IT-ADMINISTRATOR.DE

08/2009

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Hochverfügbarkeit

LANCOM

. . . connecting your business

Made
in
Germany

Das beste WLAN aller Zeiten!

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

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

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

INNOVATIONSPREIS-IT
KATEGORIESIEGER
2009
initiative mittelstand
STORAGE/NETZWERKE

LANCOM OAP-310agn

LANCOM
Systems

www.lancom.de

EDITORIAL

Always on my mind

Liebe Leser,

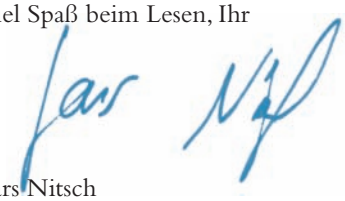
als ich vor gut zehn Jahren meinen Job als Admin einer kleinen Hausverwaltung antrat, war mir das Thema Hochverfügbarkeit kein Begriff. Was damals auch kein größeres Problem darstellte: Zwar existierte im Netzwerk ein zentraler Rechner unter Windows NT, der den nicht einmal zehn Angestellten als Fileserver diente. Fiel dieser aus, mussten die Anwender den Geschäftsbrief eben auf dem PC zwischenspeichern. Die Mieterdatenbank war lokal installiert; traten damit Probleme auf, musste halt der entsprechende Aktenordner herhalten. Das Internet hatte seinen Höhenflug noch vor sich, so dass eine Downtime der kleinen statischen Webseite nur Wenige interessierte.

Bei meinem Ausscheiden aus der Immobilienbranche Anfang 2008 stellte sich die Lage anders dar: Im Zentrum des Netzwerks stand ein Windows Small Business Server 2003, der neben seiner Tätigkeit als Datenspeicher die Rolle des Exchange-und Datenbankservers innehatte. Es gab per VPN verbundene mobile Mitarbeiter und der dynamische Webauftritt informierte Mietinteressenten über freie Wohnungen. Bei einem Ausfall des Servers drehte die komplette Belegschaft Däumchen, der wirtschaftliche Schaden war greifbar.

Besonders in kleineren Umgebungen wird das Thema Hochverfügbarkeit oft hintangestellt. Speziell hier ist die Vernachlässigung des Themas jedoch brisant, da es nur wenige oder sogar nur den einen Server gibt, der noch dazu mehrere Rollen wahrnimmt. Oft sind es Kostengründe, die Verantwortliche davon abhalten, sich nach einer hochverfügbaren Plattform umzusehen. Zudem sind die Versprechen der einzelnen Hersteller nicht immer transparent und die Frage, ob die Uptime in einer kleineren Büroumgebung nun 99,97 oder 99,98 Prozent betragen sollte, hat eher akademischen Charakter.

Trotzdem ist der Mehrzahl der IT-Verantwortlichen klar, dass Hochverfügbarkeit auch für KMUs täglich wichtiger wird. In dieser Ausgabe erfahren Sie in unserem Test der Open Source-Software OSCAR ab Seite 22, wie sich die kostenlose Cluster-Lösung im produktiven Einsatz schlägt. Wer lieber auf bekannte Marken zurückgreift, liest ab Seite 36, welche Cluster-Funktionen das neue Windows Server 2008 R2 gerade in virtuellen Umgebungen zu bieten hat.

Viel Spaß beim Lesen, Ihr



Lars Nitsch
Volontär IT-Administrator

Liefertermin:
Mitte Oktober 2009

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2009!

180 Seiten Praxis-Know-how + Tools-CD
rund um das Thema

Virtualisierung

zum Abonnenten-Vorzugspreis* von

nur € 29,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

administrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0809

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

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

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

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

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

INHALT

IT-Administrator – Ausgabe August 2009

Hochverfügbarkeit

Im Test: OSCAR 6.03

Um in Unternehmen hochkomplexe und damit rechen- und zeitintensive Aufgaben zu bewältigen, die von einem Rechner alleine nicht zu bewerkstelligen sind, ist oftmals ein den Anforderungen entsprechender Cluster die erste Wahl von IT-Verantwortlichen. Inzwischen bietet auch der Open Source-Bereich eine Fülle an Lösungen für Hochverfügbarkeit und Rechenleistung im Verbund. IT-Administrator hat die freie Cluster-Lösung OSCAR einem Test unterzogen.

Seite 22

Hochverfügbarkeit mit Windows Server 2008 R2

Mit Windows Server 2008 R2 erscheint in rund zwei Monaten die nächste Servergeneration von Microsoft. Das Betriebssystem hat unter anderem eine neue Hochverfügbarkeitsoption für das Windows Server Failover Clustering an Bord, welche erstmals mit der aus NT-Zeiten stammenden "Shared-Nothing"-Architektur bricht: Cluster Shared Volumes (CSV). Weitere Neuigkeiten wie SAN Fault Tolerance, Verbesserungen beim Validation Tool sowie bei der Verwaltung von Print Servern sollen die Administration des Servers noch einfacher gestalten. In diesem Artikel stellen wir Ihnen einige der neuen Features mit dem Schwerpunkt Hochverfügbarkeit vor.

Seite 36

Themenübersicht

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

Die "TeraStation Duo" von Buffalo speichert bis zu 2 TByte und sichert die Daten in RAID 1

NAS mit Webzugriff

Buffalo Technology erweitert sein Produktportfolio um die **TeraStation Duo**. Das **NAS-Gerät** speichert je nach Ausführung 1 oder 2 TByte an Daten. Die Übertragungsraten des Netzwerkspeichers belaufen sich dabei auf bis zu 65 MByte/s. Per RAID 1 lassen sich die Daten vor Verlust schützen, was jedoch naturgemäß die Speicherkapazität halbiert. Eine Hot-Swap-Unterstützung ermöglicht daneben das Tauschen von Festplatten im laufenden Betrieb. Die "Backup-Replication-Funktion" erlaubt darüber hinaus den Anschluss einer weiteren TeraStation Duo via USB oder LAN und eine Nachbildung aller Daten auf diesem zusätzlichen Netzwerkspeicher. Neben der Festplattenverschlüsselung bis AES 128 Bit gehören außerdem ein eingebauter Print-Server, ein DLNA-zertifizierter Medienserver sowie ein eingebauter BitTorrent-Client zur Grundausstattung der TeraStation Duo. Via WebAccess kann der User standortunabhängig vom PC, Mac oder auch iPhone auf den NAS-Speicher zugreifen. In der 1-TByte-Ausführung kostet die TeraStation Duo 569 Euro. Die 2-TByte-Variante ist für 699 Euro erhältlich. *(dr)*

Buffalo Technology: www.buffalo-technology.com

Spamschutz am Gateway

Net at Work Netzwerksysteme stellt die neue Version 7.0 seiner **Anti-Spam-Lösung NoSpamProxy für Windows Server** vor. NoSpamProxy 7.0 soll Unternehmen mit umfangreicheren Konfigurationsmöglichkeiten und optimierten Filterfunktionen noch mehr Sicherheit vor Spam und Malware bieten. Im Gegensatz zu herkömmlichen Anti-Spam-Lösungen benachrichtigt NoSpamProxy betroffene Absender automatisch über die Ablehnung einer E-Mail und verhindert dadurch das versehentliche Aussortieren oder Löschen wichtiger Nachrichten. Zu den Neuerungen von Version 7 gehören eine One-Click-Installation, verschlüsselter E-Mailversand und umfangreiche Reporting-Funktionen. Zudem lassen sich dank einer neuen Archivschnittstelle am Gateway E-Mails in Dateiform archivieren, wobei der Administrator die Möglichkeit hat festzulegen, welche Mails archiviert werden. Aufgrund der modular aufgebauten Funktionen, der sogenannten Rollen, ist NoSpamProxy 7.0 laut Hersteller noch besser skalierbar und bietet eine deutlich gesteigerte Performance. Die Lösung ist für Windows Server ab Version 2003 geeignet und schützt alle nachgelagerten E-Mailserver. Das Einsteigerpaket für 25 User kostet 575 Euro inklusive einem Jahr Software-Wartung, integriertem Virenschutz und Updates. *(dr)*

Net at Work: www.nospamproxy.de

Verkehrskontrolle im Tunnel

Stonesoft stellt die **IPS-Appliance StoneGate IPS 1030** vor. Das Gerät im Rack-Format richtet sich an kleine Umgebungen und Außenstellen und basiert auf der Plattform IPS 5.0 des Herstellers. Mit der neuen SSL-Überwachungsfunktion können IT-Administratoren auch verschlüsselten Datenverkehr innerhalb von SSL (Secure Sockets Layer)- und TSL (Transport Layer Security)-Tunneln überwachen und ihn vor unerwünschten Inhalten schützen. Das System erkennt und stoppt dabei Attacken auf Client-Webbrowser innerhalb eines SSL-Tunnels und schützt laut Anbieter Workstations und interne Netzwerke auf diese Weise noch effizienter vor schädlichen Webservern. Auf der Serverseite identifiziert und blockiert das IPS ebenfalls Angriffe innerhalb eines SSL-Tunnels, um Server vor Gefährdungen durch unberechtigte Benutzer zu schützen. Hierfür erkennt das System mehr als 160 Protokolle und Applikationen wie MySQL, MS SQL, TFTP oder Oracle sowie über 3.000 Angriffsignaturen. Ein Layer-2-Firewall soll zudem direkte Angriffe auf das Netzwerk unterbinden. Der Datendurchsatz soll 200 MBit/s beziehungsweise im Rahmen der HTTPS-Analyse 40 MBit/s betragen. Ab 4.950 Euro ist die Appliance zu haben. *(dr)*

Die Appliance "StoneGate IPS 1030" schützt auch vor Angriffen in verschlüsselten Datenströmen

Stonesoft: ww.stonesoft.com/de/products_and_solutions/ips/

Keine Downtimes durch Storage-Virtualisierung

Im "ESVA-F60" von Infortrend ist pro Modul Platz für 16 SAS-Festplatten. Insgesamt werden bis zu 112 Harddisks unterstützt.

Von **Infortrend** kommt mit **ESVA** (Enterprise Scalable Virtualized Architecture) ein neues Speichersystem auf den Markt, das im Netzwerk bis zu 112 TByte an Daten bereitstellen kann. Die **Storage-Plattform verfügt über Virtualisierungsfunktionen** und ist über den "Scale-up"-Mechanismus in der Lage, Daten zu migrieren und neuen Plattenplatz bereitzustellen, ohne dass es dabei zu Ausfallzeiten kommt. Die Systeme basieren auf dem FC- oder iSCSI-SAN-Protokoll. Drei der insgesamt fünf Modelle verfügen über eine FC-Anbindung mit einem Datendurchsatz von 8 GBit/s. Die Variante "ESVA-F20" lässt sich mit SATA-II-Festplatten bestücken, während in den Modellen "F40" und "F60" jeweils SAS-Laufwerke zum Einsatz kommen. Die Ausführungen "E20" und "E60" sind für den iSCSI-Anschluss mit 1 GBit/s gedacht. Alle Geräte verfügen über Funktionen zum Thin Provisioning sowie Load-Balancing und erlauben Array-basierte Snapshots. Die Systeme arbeiten mit Windows Server 2008, Solaris, Linux, IBM-AIX und HP-UX zusammen. Außerdem sind sie in den wichtigsten Virtualisierungs-Umgebungen wie VMware oder Microsoft Hyper-V lauffähig. Allerdings lässt sich ESVA aufgrund der virtualisierten Speicherverwaltung nicht in bestehende Storage-Strukturen einbinden und ist auch nicht mit der Hersteller-eigenen Eonstor-Linie kompatibel. Je nach Modell und Ausstattung ist die Lösung zu einem Preis ab 29.000 Euro erhältlich. *(ln)*

Infortrend: http://esva.infortrend.com/

Dünner Ersatz für den Desktop

Wyse Technology erweitert sein Portfolio an Thin Clients um die Modelle **R90LW** und **R90LEW**. Beide **Thin Clients** basieren auf Windows Embedded Standard, der nächsten Generation von Windows XP Embedded. Mit dem neuen Betriebssystem ist der Desktop-Ersatz mit dem Internet Explorer 7.0 ausgestattet und unterstützt DirectX 9, Microsofts .NET Framework 3.5 sowie VMware View. Ferner soll das integrierte Energiemanagement für eine genaue Kontrolle des Stromverbrauchs sorgen. In beiden Modellen stecken 2 GByte Flash zum Speichern von Betriebssystem und lokalen Funktionen sowie 1 GByte RAM; diese Elemente lassen sich jedoch auf maximal 4 GByte Flash und 2 GByte RAM aufstocken. Je nach Ausführung schlägt als Prozessorherz ein AMD Sempron mit einer Frequenz von 1,0 beziehungsweise 1,5 GHertz. Die Modellvariante "LEW" verfügt zusätzlich zu den sechs externen über vier interne USB 2.0-Steckplätze sowie einen parallelen Port und bietet außerdem die Möglichkeit, eine PCIe 1.1a-Karte anzuschließen. Die Rechner sind ab sofort zu einem Preis ab 556 Euro verfügbar. *(ln)*

Der Thin Client "R90LW" von Wyse unterstützt bereits den neuen Windows Embedded Standard

Wyse: www.wyse.de/products/hardware/thinclients/

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

Ab sofort bietet **Fujitsu Technology Solutions** mit dem **PRIMERGY TX100 S1** ein Server-Modell an, das sich an kleine und mittlere Unternehmen richtet. Der Server bietet einen integrierten Speicher mit bis zu 4 TByte und die Leistung und Datensicherheit von RAID 0/1. Ein optionales Band-Laufwerk für Backup- und Archivierungssysteme sorgt zudem für erhöhte Datensicherheit. Für rund 600 Euro ist der Rechner erhältlich. *(dr)*

http://de.ts.fujitsu.com

Version 6.3 der Client-Managementsoftware **DX-Union** des IT-Dienstleisters **MATERNA** ist ab sofort verfügbar. DX-Union ist eine modulare Lösung für das integrierte Workplace-Management. Die wichtigsten Module betreffen dabei das Software-Management, die Inventarisierung und das Benutzer-Management. Mit der neuen Version 6.3 übernimmt die Software unter anderem nun auch die Provisionierung von Virtualisierungskomponenten. Über diesen Mechanismus lässt sich ein Server, wie zum Beispiel Citrix XenApp, mittels Presentation Server ausstatten und bereitstellen. Für 11 Euro pro Modul ist die Suite zu haben. *(dr)*

www.dx-union.de

Belkin hat sein Portfolio an Netzwerkkomponenten überarbeitet und bietet unter der Bezeichnung **F5D51** vier neue Switches an. Die Modelle verfügen über fünf beziehungsweise acht Ethernet-Ports und kommen jeweils als 100 MBit- und GBit-Ethernet-Variante auf den Markt. Alle Anschlüsse sind Auto-Sensing- und Vollduplex-fähig. So soll unter Volllast ein Durchsatz von 2.000 MBit/s pro Port möglich sein. Auch an der Energieeffizienz hat der Hersteller geschraubt: Je nach Länge des Kabels wird der Energiebedarf automatisch angepasst. Leere Ports werden nur mit so viel Spannung versorgt, dass sie eine angeschlossene Gegenstelle erkennen. Abhängig von Port-Anzahl und Netzwerkgeschwindigkeit sind die Switches ab 20 Euro erhältlich. *(ln)*

www.belkin.com/de/

Für den Einbau im Serverschrank stellt **Synology** mit der **Rack Station RS409** einen neuen NAS-Server vor. Der Netzwerkspeicher ist für vier SATA-Festplatten ausgelegt und unterstützt dabei bis zu 2 TByte pro Magnetspeicher, so dass sich eine maximale Speicherkapazität von 8 TByte ergibt. Außerdem ist das Gerät mit einem 1,2 GHertz Prozessor, 256 MByte Arbeitsspeicher, zwei GBit-LAN-Ports, zwei USB 2.0 Anschlüssen sowie einer eSATA Schnittstelle ausgestattet. Als Firmware kommt "Disk Station Manager 2.1" zum Einsatz und stellt unter anderem Active Directory-Integration und RAID-gestützte Datensicherung bereit. Das NAS-Modul kostet ohne Festplatten 785 Euro. *(ln)*

www.synology.com/deu/

Switches für die Schiene

Mit den **Industrial Switches ALL8908 und ALL8906** stellt **ALLNET** zwei neue Netzwerkprodukte für den Einsatz im industriellen Umfeld vor. Die Switches sind speziell für die **Hutschienenmontage** (DIN Rail) entwickelt und verfügen über ein robustes, IP30 konformes Aluminiumgehäuse. Dieses soll den Einsatz in Umgebungen mit erweitertem Temperaturbereich von -10 bis +70 Grad Celsius und einer Luftfeuchtigkeit von bis zu 90 Prozent ermöglichen. Die wichtigsten Informationen zum Betriebszustand der Switches werden über drei an der Front der Geräte angebrachte Leuchtdioden signalisiert. Die Geräte verfügen je nach Modell über acht 10/100 MBit/s RJ45 Ports (ALL8908) oder über sechs 10/100 MBit/s RJ45 und zwei zusätzliche 100FX-Ports (ALL8906). Dabei unterstützen die Switches bis zu zwei separate Netzteile in einem Spannungsbereich von zwölf bis 48 Volt. Daneben stehen Standardfunktionen wie Full/Half-Duplex und Store-and-Foreward Switching sowie eine Non-Blocking-Architektur und Auto MD/MDI-X Ports zur Verfügung. Reicht ein Gerät nicht mehr aus, lassen sich die Switches kaskadieren und bieten zudem einen Alarmkontakt zur Überwachung der Stromversorgung. Damit kann auch der Linkstatus jedes einzelnen Ports kontrolliert werden. Das Modell ALLNET ALL8908 ist für 251 Euro erhältlich, die Variante ALL8906 für 293 Euro. *(dr)*

ALLNET: www.allnet.de/produkte_industrial_switches.html

Halten Industrieumgebungen aus und melden Port-Fehler: Die Industrial Switches ALL8908 und ALL8906 von ALLNET

Genügsame Netzwerkswitches

SMC bietet zwei neue und **stromsparende Fast-Ethernet-Switches** für das Rack an. Die Modelle **EZ Switch 10/100 SMC-EZ1024DT** und **SMC-EZ1016 DT** sollen den Stromverbrauch im Volllastbetrieb um bis zu 21 Prozent und bei ausgeschalteten Netzwerk-PCs um bis zu 59 Prozent senken. Die 16- und 24-Port Switches arbeiten mit SMCs intelligenten "Green Saving"-Algorithmen. Diese erkennen den Verbindungsstatus und die Kabellänge automatisch und sorgen so für einen energieoptimierten Betrieb. Sobald ein eingehendes Signal erkannt wird, wechseln die Switches aus dem Energiesparmodus in den Normalbetrieb. Leistung und Stabilität werden durch diese Energiesparfunktion laut Hersteller nicht beeinträchtigt. Die Green Saving-Switches erkennen zudem die für die Kabellänge notwendige Stromleistung, so dass durch kurze Kabelverbindungen zusätzliche Energieeinsparungen möglich werden. Bei einer Kabellänge von unter 20 Metern könne jeder Switch bis zu 12 Prozent Strom einsparen. Erhältlich sind die beiden Stromsparer ab sofort. Das 16-Port-Modell SMC-EZ1016DT kostet 57 Euro. Die 24-Port-Ausführung SMC-EZ1024DT ist für 83 Euro zu haben. *(dr)*

SMC: www.smc.com

Neues für die schlanken Rechner

IGEL Technology hebt die Firmware seiner **Linux-basierten Thin Clients** auf den **Release-Stand 4.01.100**. Neben chinesischen Regions- und Sprachoptionen und einem neuen Energiemanagement mit Standby-Funktionalität integriert der Hersteller die Softwareclients zu zahlreichen Server Based Computing-Lösungen, darunter VMware View 3.1 und ICA 11 für Citrix XenDesktop- sowie Citrix XenApp-Umgebungen einschließlich HDX-Unterstützung. Für Anwender bietet sich dabei besonders die Fähigkeit der Universal Desktop Thin Clients an, Multimediainhalte aus dem virtuellen Desktop am Thin Client beschleunigt wiederzugeben. Auch die Nutzung von lokal am Thin Client angeschlossenen Geräten wie etwa Smartphones, Webcams oder Scanner in virtuellen Desktops von Citrix und VMware ist nun dank USB-Redirection möglich. Über die Energiesparfunktion Suspend to RAM lassen sich die Thin Clients zudem binnen Sekunden in den Standby-Zustand versetzen und genauso schnell wieder aufwecken. Das neue Linux-Firmware-Paket steht ab sofort zum Download bereit. *(dr)*

IGEL Technology: www.myigel.com

Aufgebohrte Sicherheitszentrale

McAfee präsentiert mit dem **ePolicy Orchestrator 4.5** die neueste Version seiner **Security-Management-Plattform**. Sie soll Verbesserungen hinsichtlich Skalierbarkeit, Benutzerfreundlichkeit und Integration mit System-Management-Tools bieten, um konsistentere Sicherheitsprozesse zu gewährleisten. Eine neue Architektur ermöglicht dabei ein verbessertes Policy-Management und Reporting für Remote- und Roaming-Endpunkte. Load-Balancing-Fähigkeiten und Failover sollen zudem für eine verbesserte Uptime sorgen, während sich Sicherheitsrichtlinien nun auf Benutzern statt auf Systemen basierend einrichten lassen. Die Integration mit HP Openview Service Desk und BMC Remedy Action Request System ermöglicht außerdem einen Kreislaufprozess zum Management von Sicherheitsvorfällen. Schließlich sollen Navigationsfähigkeiten wie Drag and Drop, kundenspezifisch angepasste Toolbars, Suchgruppierung und eine Systemsuche den ePolicy Orchestrator einfacher in der Bedienung machen. Ab sofort ist die neue Version als Teil der McAfee-Suiten erhältlich. Für Nutzer mit Wartungsvertrag ist das Upgrade dabei kostenfrei. *(dr)*

McAfee: www.mcafee.de

phion Gipfelkonferenz 2009, 25. bis 26. Mai, Alpbach/Tirol

Die Großen lernen von den Kleinen

von Daniel Richey

Trotz wirtschaftlich angespannter Lage konnte sich der Security-Hersteller phion auch 2009 nicht über einen Mangel an Gipfelstürmern beklagen. Rund 500 Teilnehmer machten sich Ende Mai auf den Weg ins idyllische Alpbach in Tirol, um sich über neue Trends im Security-Umfeld sowie neue Produkte von phion zu informieren. In zwei Tagen und 29 Sessions klärte der Hersteller über die Technologie hinter seinen Produkten auf und ging auf zahlreiche Best-Practice-Ansätze zur Konfiguration ein. Zudem zeigte Andreas Kurz von cirosec die Gefahren bei Webapplikationen auf.

Überleben der Effizienten

Es sind zwei Aspekte, die unterschiedlicher kaum sein könnten. Doch sie treiben laut Dr. Wieland Alge, dem Geschäftsführer von phion, die IT-Branche derzeit um. So veränderten zum einen die allgegenwärtige Wirtschaftskrise das Handeln nachhaltig. Dadurch dreht sich für Alge auch bei der IT-Sicherheit alles um Effizienz. Besonders die großen Unternehmen lernten von mittelständischen Firmen, wie das Thema Security richtig angegangen würde. Seien doch die Mittelständler schon seit jeher auf eher überschaubare Budgets angewiesen.

Neben diesen wirtschaftlichen Beweggründen sah der phion-Geschäftsführer als zweiten Aspekt auch neue Trends in der IT-Sicherheit, die zu einem Umdenken zwingen. Demnach ließen sich die Gefahren nicht mehr quantitativ, sondern nur noch qualitativ messen. Steigende Prozentangaben über Angriffe beispielsweise machten keinen Sinn mehr. Besonders mit dem Mythos, dass sich organisatorisch Sicherheit erreichen ließe – also etwa durch Vereinbarungen mit den Mitarbeitern – müsse aufgeräumt werden. So sei es etwa der Sicherheitstechnik in modernen Fahrzeugen zu verdanken, dass weniger Menschen auf den Straßen sterben und nicht einem gesteigerten Sicherheitsbewusstsein der Autofahrer.

Web Application Security

Ein neues Thema im Bereich der Web Application Security präsentierte Andreas Kurz, IT-Sicherheitsberater bei cirosec: Das Cross Site Request Forgery (CSRF). Andere Begriffe hierfür sind XSRF, Session Riding oder URL Command Attack. Darunter ist ein unbemerktes Ausführen von Aktionen im Kontext eines angemeldeten Nutzers zu verstehen. Das können Passwortänderungen, Einträge in Foren oder die Teilnahme an Internet-Auktionen sein. Der Angreifer nutzt beispielsweise einen Server im Internet, auf den auch das potenzielle Opfer zugreift. Kontaktiert nun der User den Server, antwortet dieser mit einer legitimen HTML-Seite, in die jedoch Schadcode eingebettet ist. So lässt sich laut Kurz etwa über einen Image-Link Code auf einer anderen Webseite im Kontext des Browser ausführen. Dies könne etwa eine Banküberweisung sein, wenn der Nutzer parallel sein Online-Banking-Portal geöffnet hat beziehungsweise sich die entsprechenden Cookies noch im Browser-Cache befinden.

Neben Angriffen auf Online-Banking seien besonders Passwortänderungen sehr beliebte Ziele. Handle es sich dann um statische HTML-Codes ohne zusätzliche Zufallswerte, funktioniere der Angriff. Erkennen lassen sich Cross Site Request Forgerys laut Kurz über die Referer. Stammt die Anfrage von einem anderen Server, sollte der Request schlichtweg nicht ausgeführt werden. Doch auch dieser Wert lässt sich über den Browser manipulieren. Einige Seiten führen zudem bei falschen Referern die Aktion trotzdem aus und zeigen nur eine Warnmeldung.

phion-Produkte und Schmankerl

Neben den Security-Vorträgen informierten sich die Teilnehmer in zahlreichen Break-Out-Sessions über die Administration der phion-Produkte. Dabei stiegen die technisch versierten Referenten tief in die Details ein und standen den Zuhörern Rede und Antwort. Als Ergänzung zu den technischen Sessions erfreute phion die Teilnehmer schließlich mit zwei besonderen Schmankerln: Alexander Huber vom bekannten Kletter-Duo Huber-Buam zog das Publikum mit seinen Ausführungen zum Extremklettern in seinen Bann. Faszinierende Bilder und Videos zeigten die Bergsteiger an Steilwänden und auf Gipfeln in aller Welt – zumeist ohne Sicherung. In ein etwas bodenständigeres, wenn auch ebenso interessantes Thema führte Dr. Markus Hengstschläger als Biologe und Moderator bei einem österreichischen Radiosender ein. Er entführte die Zuhörer eine Stunde lang auf humoristische Weise in die Evolutionsbiologie und erklärte, weshalb Vielfalt für das Überleben einer Art notwendig ist. Ein Ansatz, der sich sicher auch auf Betriebssysteme übertragen lässt.

ITANet Schirmherrschaft:

REALTECH

IT-Administrator-Workshops am 21. August und 30. September

Neue Server im Doppelpack

von John Pardey

Gleich zwei spannende Termine zu wichtigen neuen Servern bietet der IT-Administrator seinen Leser im August und September: Am 21. August werfen wir gemeinsam mit Dozent Ulf B. Simon-Weidner einen Blick auf den Windows Server 2008 R2. Dieser Workshop findet am Vortrag der ice:2009 in Lingen/Emsland statt und steht Lesern wie auch ice-Teilnehmern offen. Und welche Neuerungen der Exchange Server 2010 bringt, zeigt unser September-Workshop in Hamburg.

Quelle: Yoyo - Pixelio.de

Zwei neue Bewohner im Rack: Windows Server 2008 R2 und Exchange 2010

Wie schon im vergangenen Jahr kooperiert der IT-Administrator mit Nicki Wruck, dem Organisator und Veranstalter der ice:2009 und eröffnet ein spannendes Wochenende mit einem Workshop am Vortag der Konferenz. Unser Aufwärmprogramm startet am 21. August um 13 Uhr (siehe auch Kasten "Agenda Workshop 21. August").

Ein Experte zeigt Windows Server 2008 R2

Die Redaktion freut sich sehr, für diesen Nachmittag Ulf B. Simon-Weidner als Dozenten gewonnen zu haben. Als renommierter Autor des IT-Administrator, langjähriger fester Bestandteil der ice-Agenda und MVP für Directory Services übernimmt er die Aufgabe, den Teilnehmern die neuen Möglichkeiten des Windows Servers 2008 R2 darzulegen.

Viele der neuen Features des R2 zeigt Simon-Weidner anhand einer Live-Demo. Er führt die Teilnehmer in die Active Directory-Neuerungen ebenso ein wie in das vereinfachte Active Directory-Scripting (AD-Powershell). Anschließend widmet er sich der Frage, was der neue Recycle-Bin für das Recovery des AD bringt und welche Fallstricke Administratoren generell bei der Wiederherstellung des Active Directory meiden sollten. Diese und weitere spannende Themen wie etwa DirectAccess, BranchCache oder die neue Version von Hyper-V bilden die Basis für

iTANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13 Uhr: Begrüßung

13.15 Uhr: Neuerungen in Windows Server 2008 R2 (Teil 1)
- Übersicht über Windows Server 2008 R2
- Management und Best Practices
- Active Directory Verwaltung - eine neue Konsole und Powershell
- Dateien und Drucken

Dozent: Ulf. B. Simon-Weidner

14.45 Uhr: Pause

15 Uhr: Neuerungen in Windows Server 2008 R2 (Teil 2)
- Hyper-V mit Cluster Shared Volumes
- Active Directory-Objekte wieder herstellen - wie sieht das in der Praxis aus?
- Windows Server 2008 R2 und Windows 7: BranchCache und DirectAccess
- Praxiserfahrungen: Der Weg zu Windows Server 2008 R2

Dozent: Ulf. B. Simon-Weidner

17.30 Uhr: Ende des Workshops

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

Teilnahmegebühren:
Für IT-Administrator-Abonnenten und ice:2009-Teilnehmer kostenlos.

Anmeldung bis zum 15. August unter
www.it-administrator.de/workshops

Workshop "Windows 2008 R2" am 21. August

einen informativen Workshopnachmittag und einen gelungenen Einstieg in das ice-Wochenende.

Exchange 2010 im September unter der Lupe

Neben dem zweiten Release des Windows Server 2008 steht aus dem Hause Microsoft ein weiteres zentrales Produkt vor der Veröffentlichung: Exchange 2010. Grund genug im Rahmen einer unserer Workshops auch auf dieses Produkt einen intensiven Blick zu werfen. Am 30. September in Hamburg stellt Walter Steinsdorfer den Lesern des IT-Administrator die Neuerungen vor. Steinsdorfer ist MVP für Exchange und betreut zudem die deutsche Exchange User Group.

Der erste Teil des Workshops, der wie gewohnt um 13 Uhr beginnt, dreht sich um zentrale Verbesserungen und neue Features des Exchange Servers. Themen wie das neue Storage-Design, die Archivierung oder auch Hochverfügbarkeit stehen dabei im Fokus (siehe auch Kasten "Agenda Workshop 30. September"). Darüber hinaus beschäftigt sich Steinsdorfer mit möglichen Migrationspfaden zu Exchange 2010 und den Hürden, die auf diesem Weg zu überwinden sind.

Im weiteren Verlauf des Nachmittags wenden wir uns schließlich Fragen des E-Mailmanagements zu. Zum einen diskutieren wir mit den Teilnehmern Features, die Exchange 2010 für diesen Aufgabenbereich bereitstellt, werfen aber auch ein Blick auf gesetzliche Vorgaben, die es im Zusammenhang mit dem Betrieb eines Mail-Servers zu beachten gilt.

Beide Workshops stehen ab sofort zur Registrierung offen und wir würden uns freuen, Sie in Lingen und Hamburg begrüßen zu dürfen.

iLaNet
Die System und Netzwerk User Group

Die Agenda des Workshops

13 Uhr: Begrüßung

13.15 Uhr: Die Neuerungen in Exchange 2010
- Das neue Storage-Design und Archivfunktionen
- Outlook Web Access
- Exchange-Remoteverwaltung
- Federated Trusts
- Hochverfügbarkeit
- Neuerungen im Hub-Transport-Dienst
- Migration zu Exchange 2010

Dozent: Walter Steinsdorfer

14.45 Uhr: Pause

15 Uhr: Partnervortrag Gingcom

16 Uhr: E-Mailmanagement mit Exchange 2010
- Vorteile des E-Mailmanagement
- Compliance-Regelungen, die es zu beachten gilt
- Automatisierung und Archivierung
- Regeln und Schutz von E-Mails

Dozent: Walter Steinsdorfer

17.30 Uhr: Ende des Workshops

Ort: Fast Lane Institute for Knowledge Transfer GmbH
Gasstraße 4a, 22761 Hamburg

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos.

Anmeldung bis zum 21. September unter
www.it-administrator.de/workshops

Workshop "E-Mailmanagement mit Exchange 2010" am 30. 09.

Bereits zum achten Mal öffnet die ice (Intelligent Communities for Europe) [1] am 22. August ihre Pforten. Und wie gewohnt hat Organisator Nicki Wruck dafür gesorgt, dass IT-Verantwortliche, Administratoren und Entwickler ein spannendes Programm vorfinden – und das zum Nulltarif. Allerdings waren die 250 Plätze in Lingen in weniger als 30 Tagen vergeben. Nur Leser des IT-Administrator haben noch die Chance auf einen der begehrten Plätze.

Um eine von fünf Eintrittskarten zur längst ausgebuchten ice:2009 am 22. August in Lingen/Emsland zu gewinnen, schicken Sie eine E-Mail mit dem Betreff "ice:2009" an redaktion@it-administrator.de. Einsendeschluss ist der 10. August. Die Gewinner werden von der Redaktion unmittelbar benachrichtigt und erhalten je einen Platz auf der ice:2009.

[1] ice:2009
www.ice-lingen.de

Gewinnen Sie eine Eintrittskarte zur ice:2009

4. Heinlein Mailserver-Konferenz 2009, 1. bis 3. Juli, Berlin

Rechtssicher und spamfrei

von Daniel Richey

Quelle: Heinlein

Auf der 4. Mailserver-Konferenz drehten sich die Themen um rechtliche Aspekte und Spam

Typischerweise kämpfen Mailserver-Administratoren an mehreren Fronten: Sie müssen Sorge dafür tragen, dass der E-Mailverkehr ohne Ausfälle funktioniert, die Nachrichten frei von Spam und Viren sind und all das rechtssicher vonstattengeht. In großen Unternehmen steht für diese Bereiche genügend Personal und Technik zur Verfügung, während kleinere Unternehmen oft schon froh sind, dass ihre Infrastruktur ohne größere Ausfälle funktioniert. Entsprechend aufgebaut waren die Themen auf der 4. Mailserver-Konferenz des Linux-Support-Dienstleisters Heinlein in Berlin.

Rechtlich gesehen bewegen sich Mailserver-Administratoren sowie Arbeitgeber oft am Rande der Legalität oder in Grauzonen. So verwunderte es nicht, dass der erste Konferenztag sich ausschließlich mit juristischen Themen befasste. Zahlreiche Rückfragen der Teilnehmer zeugten vom großen Interesse und Aufklärungsbedarf. So räumten denn auch vier Anwälte in ihren Vorträgen mit so manchen Rechtsmythen und Missverständnissen auf. Vilma Niclas, Rechtsanwältin aus Berlin, zeigte auf, was alles für einen rechtssicheren E-Mailverkehr nötig ist. So gelten etwa beim elektronischen Geschäftsverkehr die gleichen Aufbewahrungsfristen wie bei postalischen Nachrichten – sechs Jahre beziehungsweise zehn Jahre bei Buchungsbelegen. Anstatt auf Datenträgern gespeichert könnten E-Mails dabei auch ausgedruckt archiviert werden.

Viele Fallstricke bei E-Mails

Grundsätzlich gilt bei Werbemails das Opt-In-Verfahren, bei dem der Empfänger dem Versand ausdrücklich zustimmen muss. Gibt es bereits einen Geschäftskontakt, dürfen Unternehmen jedoch unter bestimmten Voraussetzungen auch ohne vorherige Zustimmung Werbenachrichten in eigener Sache versenden. Dies gilt für bis zu zwei Jahre, sofern der Kunde dem Erhalt nicht widersprochen hat. Auch bei Newslettern muss der Empfänger ausdrücklich zustimmen, da die allermeisten Newsletter letztendlich auch Werbung sind. Am besten eignet sich laut Vilma Niclas das Double-opt-in-Verfahren. Dabei melden sich die Nutzer an und erhalten eine Bestätigungsmail, die angeklickt werden muss. Nicht vergessen sollten die Verantwortlichen natürlich das Impressum – sowohl im Newsletter als auch in regulären E-Mails.

Eine Alternative, die jedoch höchstens bei Kleinstunternehmen sinnvoll angewendet werden kann. Ebenfalls wichtig zu wissen ist für die Verantwortlichen, unter welchen Umständen das eigene Unternehmen Werbung oder Newsletter versenden darf. Denn schnell drohen für Werbemails ohne Zustimmung der Empfänger Abmahnungen sowie bis zu 50.000 Euro Geldbuße.

Auf besonders große Hürden treffen Administratoren, wenn sie mit Postfächern arbeiten, in denen sich auch private E-Mails befinden. Daher warnte Rechtsanwalt Thomas Feil davor, die private Mailnutzung am Arbeitsplatz als Unternehmen zu dulden. Denn dadurch würde der Arbeitgeber selbst zum Telekommunikationsanbieter und müsse die strengen gesetzlichen Datenschutzregeln beachten. Befinden sich etwa in einem E-Mailaccount auch private Nachrichten, dürfe das Unternehmen nicht ohne weiteres Einsicht in das Postfach nehmen – auch wenn der Mitarbeiter längere Zeit krank und damit abwesend sein sollte. Insgesamt könne ein Unternehmen bei geduldeter Privatnutzung gar nicht alle Rechtsvorschriften einhalten. Der beste Weg führe daher über Betriebsvereinbarungen, die die Privatnutzung klar regeln oder am besten ganz verbieten.

Deutschland als Cybercrime-Versuchsfeld

Über die Entwicklungen in der Cyberkriminalität klärte André Dornbusch, Kriminalkommissar beim Bundeskriminalamt, auf. Insgesamt befassen sich rund 40 Beamte im Referat "SO 43" mit der Ermittlung und Auswertung von Online-Verbrechen. Nach den Erkenntnissen der Ermittler ist Deutschland dank seiner hohen Sicherheitsstandards ein Versuchsland für Cyberkriminelle geworden. So gebe es Malware und Angriffsformen, die speziell auf deutsche Rechner und deren Sicherheitsmechanismen abgestimmt würden. Seien diese hier erfolgreich, könnten sie quasi überall angewendet werden.

Die E-Mail als klassisches Transportmittel für Phishing-Versuche und Schädlinge spielt nach Aussagen des Kriminalkommissars dabei schon länger kaum mehr eine Rolle. Vielmehr dienen heute geschickt platzierte aktive Inhalte auf Webseiten der Verbreitung von Trojaner und Co. In der Untergrundwirtschaft finde dabei eine starke Malware-Fokussierung durch Spezialisten statt. Hinzu komme, dass 53 Prozent der 2008 gefundenen Schwachstellen nicht gepatcht wurden. Antiviren-Software sei dabei auch nicht mehr das Maß aller Dinge als Schutz. Nur durchschnittlich vier Prozent der im Umlauf befindlichen Schadsoftware würde laut IBM-X-Force-Report von aktuellen Antiviren-Programmen entdeckt.

Spammer im Visier

Spamhaus ist einer der bekanntesten Antispam-Dienstleister. Carel van Straten erläuterte in seinem Vortrag, auf welche Techniken die Spambekämpfer zurückgreifen und wie sich diese von Unternehmen nutzen lassen. Besonders bemerkenswert war für van Straten die Tatsache, dass Spammer heutzutage meist besser international aufgestellt sind als viele große Firmen. So verteilen sich die Botnetze schnell über mehrere Länder und beziehen zahlreiche Provider mit ein. Doch auch die Nutzerbasis von Spamhaus kann sich sehen lassen: 1,5 Millionen Nutzer greifen auf die Filterungsdaten der Briten zurück. Diese Verantwortung mache es für Spamhaus schwierig, restriktive Filterungsmethoden einzusetzen. Ganze Länder lassen sich etwa nicht so einfach blockieren. Aus diesem Grund spiele die Qualität der Daten eine entscheidende Rolle.

Insgesamt stellt der Dienstleister vier verschiedene Blocklisten zur Verfügung: SBL (Nameserver-Einträge von Spam-URLs), XBL (einzelne IP-Adressen), PBL (Filter-Policies) sowie die Drop-Liste mit IP-Adressen, zu denen am besten gar keine Verbindung hergestellt wird. Die in Spam-Hinsicht auffälligsten Länder sind nach Spamhaus-Zahlen derzeit Brasilien (16,3 Prozent), Indien (11 Prozent), Russland (7,6 Prozent), Türkei (6,7 Prozent) und Polen (5,5 Prozent). Diese Länder hätten gemein, dass in ihnen erst kürzlich großflächig Breitband für Privatnutzer zur Verfügung stünde. Die Nutzer dort haben laut van Straten noch keine große Erfahrung mit Sicherheitsmaßnahmen. Nächstes Jahr könnte Polen aus den Top-5 fallen, da sich die Online-User dort zunehmend schützten. Dafür mache sich Algerien auf den Weg.

An Technologien machen Peer-to-Peer-Botnetze zunehmend die Kontrollserver überflüssig. Bislang konnten Provider oder Ermittlungsbehörden gezielt diese "Command and Control"-Server abschalten und damit ganze Botnetze lahmlegen. Doch nun verteilen sich diese Kontrollfunktionen ebenfalls über viele Rechner in unterschiedlichen Ländern. Ein weiterer Trend ist das Fast-flux-Hosting: Dabei werden beispielsweise Phishing- oder Schadcode-Webseiten auf zahlreichen kompromittierten Rechnern gehostet, damit zumindest ein paar davon funktionieren. Die Liste ändert sich dabei alle paar Minuten. Damit machen laut van Straten auch Abuse-Beschwerden bei Providern keinen Sinn, da sich die IP-Adressen Provider-übergreifend laufend ändern.

Best Practices

Eine umfassende Übersicht, wie Administratoren mit ihren Mailservern in Bezug auf Spam umgehen sollten, gab Peer Heinlein als Geschäftsführer von Heinlein Support. So seien Backscatter-Mails heute eines der größten Probleme im Spamumfeld. Mit diesen Nachrichten antworten Mailserver auf den Erhalt von E-Mails, wenn etwa der Empfänger unbekannt oder abwesend ist. Doch nehmen Mailserver Nachrichten dabei oft erst an und versuchen anschließend, die Mail intern zuzustellen. Klappt dies nicht, erzeugen Sie eine Antwortmail an die Absenderadresse. Wurde diese jedoch durch Spammer gefälscht, landet dieser Backscatter bei völlig Unbeteiligten. Daher sollten laut Heinlein die Mailserver noch während der Zustellphase – also während des SMTP-Dialogs – bereits prüfen, ob ein Empfänger valide ist. So erhält der einliefernde Mailserver direkt die Rückmeldung und bricht die Übertragung gegebenenfalls ab.

Auch erhalten Absender eine direkte Rückmeldung, dass ihre Nachricht herausgefiltert wurde. Ansonsten besteht die Gefahr, dass Spam-Nachrichten in spezielle Ordner aussortiert werden und die Nutzer False Positives darin nicht wiederfinden. Absender und Empfänger wissen dann nichts von der verlorengegangenen Nachricht und das Unternehmen hat im Zweifelsfall diese E-Mail rechtlich gesehen angenommen. Um sicherzustellen, dass die eigenen E-Mails nicht versehentlich von den Empfängern als Spam identifiziert werden, sollten Unternehmen zudem auf korrekte Reverse-Lookups achten. Das bedeutet, die IP-Adresse des sendenden Mailservers löst korrekt auf die Domain in der HELO-Nachricht auf und beweist damit ihre Zugehörigkeit zum Netzwerk des Absenders. Zum Abschluss wies Peer Heinlein noch auf ein besonderes Anliegen hin, was IT-Sicherheit anbelangt. So fokussierten sich Unternehmen viel zu sehr auf die Redundanz von IT-Geräten. Doch wenn es um den Administrator gehe, sei oft Not am Mann. Hier auf gut ausgebildetes Personal zu setzen mit vernünftigen Vertretungsregeln im Krankheits- oder Urlaubsfall sei wesentlich zielführender, als massiv in immer neue Hardware zu investieren.

IDC Dynamic IT Conference 2009, 25. Juni, Frankfurt/M.

Hürdenlauf zwischen zwei Welten

von John Pardey

Ende Juni lud das renommierte IT-Marktforschungsunternehmen IDC nach Frankfurt ein, um dort gemeinsam mit führenden Herstellern im Rahmen einer eintägigen Konferenz aktuelle Fragestellungen des Rechenzentrums zu diskutieren. Im Fokus standen dabei "dynamische IT-Infrastrukturen", die auf Basis der Virtualisierung einen hohen Automatisierungsgrad aufweisen und durch optimierte Ressourcenauslastung helfen, Kosten zu reduzieren. Doch mit diesem Ziel vor Augen liegt ein hürdenreicher Weg vor IT-Verantwortlichen, der vor allem durch das gemeinsame Management virtueller und physikalischer Systeme beschwerlich ist.

Den Auftakt der Konferenz bildete ein Vortrag von Thomas Meyer, Vice President bei IDC. Meyer stellte zunächst anhand aktueller Marktforschungsergebnisse die Stimmungslage von IT-Verantwortlichen im Jahr 2009 dar und es zeigte sich, dass die Notwendigkeit der Kostenreduktion in den Rechenzentren "dramatisch" anstieg. Dabei verändern die IT-Organisationen jedoch nur in Ausnahmefällen ihre gewählte Strategie. Sie neigen eher dazu, geplante Projekte zeitlich nach hinten zu schieben.

Ein Gewinner dieser allgemeinen Bestrebungen nach Kostenreduktion ist eindeutig die Virtualisierung. Mehr als 40 Prozent der befragten Unternehmen wollen hier mehr investieren, auch um auf diesem Wege die Gesamtkosten zu senken. Zu den Verlierern der Krise lässt sich laut Meyer die "Green IT" zählen, hier finden sich kaum Unternehmen, die aktuell bereit sind, ihre Investitionen zu steigern.

Hier wird aber auch die Unschärfe des Begriffes "Green IT" einmal mehr offenbar, denn dieselbe Gruppe von Befragten geht davon aus, über Virtualisierungslösungen ihre Energiekosten zu senken.

Bild 1: Dr. Klaus von Rottkay, Microsoft Deutschland, denkt laut über das RZ von morgen nach

Management ist der Schlüssel

Im weiteren Verlauf zeigte Meyer detaillierte Analysen, wohin die Reise der Virtualisierung geht: 2008 fanden zum ersten Mal mehr virtuelle Maschinen ihren Weg in die Rechenzentren als herkömmliche Serversysteme. Ein Trend, der sich in den nächsten Jahren noch verstärken wird, der aber auch zeigt, dass Management-Tools für rein virtuelle Umgebungen, aber besonders auch in gemischten Landschaften, eine zentrale Rolle spielen, um die Hoffnung, auf Basis der Virtualisierung Kosten zu reduzieren, erfüllen zu können.

Und hier scheint es aktuell noch an Problembewusstsein zu fehlen: Denn, wie Dr. Klaus von Rottkay, Director Business Group Server & Tools bei Microsoft Deutschland, anführte, planen zwar, wie bereits erwähnt, vier von zehn Unternehmen Mehrausgaben für die Virtuali-

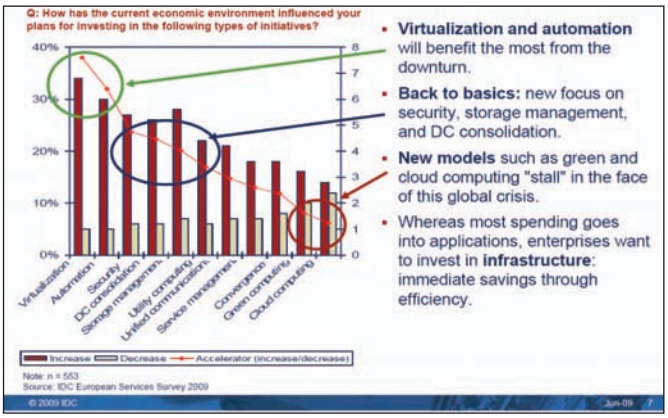


Bild 2: Die angespannte wirtschaftliche Lage führt nach IDC-Umfragen zu steigenden Ausgaben für Virtualisierung und Automation

sierung, jedoch nur 24 Prozent sind auch bereit, in entsprechende Managementtools zu investieren. Denn ohne diese Werkzeuge, so stellte auch Meyer klar, werden die Verwaltungskosten für Serversysteme weiter ungebremst steigen. Dies wirkt sich insbesondere durch eine neue Form der "Mobilität" aus. Gemeint sind hier nicht Anwender im Außendienst, die am Laptop arbeiten, sondern die hochbeweglichen virtuellen Maschinen. In Umfragen gab ein nicht geringer Anteil der IT-Verantwortlichen an, ihre virtuellen Maschinen bewegten sich täglich oder sogar stündlich. Hier müssen zukünftig, so Meyer, Policy-basierte Mechanismen greifen, die diese neue Mobility steuern.

Das RZ der Zukunft

Dass die Virtualisierung aber auch heute schon einen Mehrwert für die Unternehmen darstellt, führte Peter Dümig, Consultant bei Dell, am Beispiel Hochverfügbarkeit an. Diese lässt sich auf Basis virtualisierter Server viel einfacher einrichten, als dies früher mit Clustern der Fall war. Doch auch laut Dümig ist der Weg in das dynamische Rechenzentrum noch weit, dennoch lassen sich heute schon dessen Eckpfeiler abstecken: das RZ der Zukunft basiert auf Standards, insbesondere x86-Hardware. Es ist virtualisiert und automatisiert und seine Steuerung erfolgt auf Basis von Policies. Zudem ist es in hohem Grade Prozess-orientiert. So sei denn auch die "Cloud" im Grunde nichts anderes als ein hochoptimiertes Rechenzentrum.

Eine weitere Hürde auf dem Weg dorthin führte Michael Jones, Director Data Center bei Novell, den Teilnehmern vor Augen. Nach Jones Angaben spielen in 70 Prozent aller RZ Windows und Linux als Serverbetriebssystem eine Rolle. Und die noch immer nicht in ausreichendem Maße vorhandene Interoperabilität der beiden Welten ziehe eine hohe Komplexität nach sich, die zur Folge hat, dass in dergestalten Infrastrukturen bis zu 70 Prozent der IT-Budgets in Wartungskosten fließen. Zwar habe die Initiative von Microsoft und Novell für eine verbesserte Zusammenarbeit der Systeme erste Früchte getragen, doch es bleibe hier noch viel Arbeit auf dem Weg zum Rechenzentrum von morgen.

Im Test: Double-Take für Hyper-V

Spieglein, Spieglein im RZ

von Jürgen Heyer

Analog zum Schutz von virtuellen Systemen unter VMware durch Replikation ist Double-Take einer der ersten Anbieter, der eine entsprechende Lösung auch für die Windows 2008 Hyper-V-Plattform präsentiert. IT-Administrator hat das brandneue Double-Take für Hyper-V genauer untersucht, was anfangs aufgrund einiger Bugs allerdings nicht ganz einfach war. Mit unseren Hinweisen konnten wir dann der Entwicklungsabteilung von Double-Take bei der Fehlersuche und Produktoptimierung einige wertvolle Ratschläge geben, damit das ansonsten zuverlässige Programm auf einem deutschsprachigen Server reibungslos funktioniert.

Double-Take hat sich in den letzten Jahren überwiegend im Windows-Umfeld als zuverlässiger Lieferant für stabile Replikationslösungen zur Erhöhung der Datensicherheit etabliert. Neben intelligenten Recovery-Produkten für physikalische Systeme bietet Double-Take Varianten für virtuelle Systeme und für VMware Virtual Infrastructure (ESX Server) an. Daher lag es nahe, auch eine Version für die Windows 2008 Hyper-V-Plattform zu entwickeln.

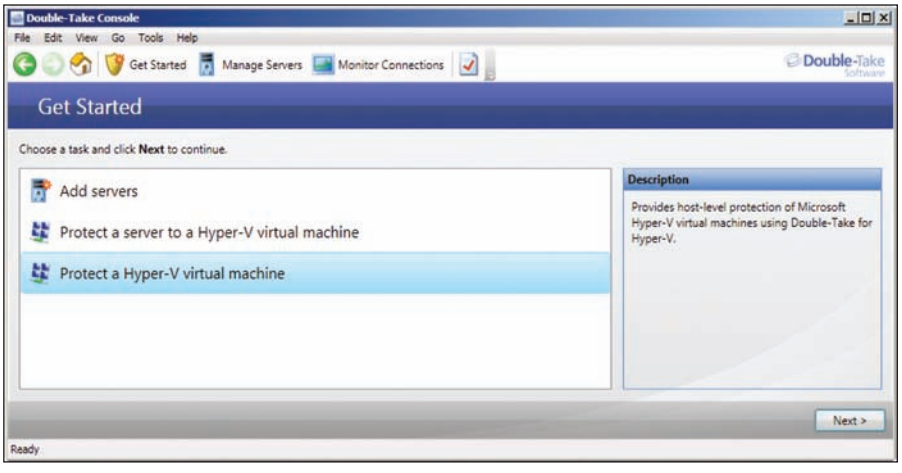


Bild 1: Drei Assistenten reichen, um die Funktionalität von Double-Take für Hyper-V abzubilden

Sicherheit durch Replikation

Von der Grundfunktion her arbeiten alle Double-Take-Produkte ähnlich: Sie replizieren Teile oder auch einen kompletten Server im laufenden Betrieb kontinuierlich auf ein zweites System beziehungsweise an eine zweite Lokation, um bei einem Ausfall des Primärsystems die Daten oder Anwendungen über das Sekundärsystem fast verzugslos wieder bereitzustellen. Die Replizierung erfolgt über das Netzwerk. Bei den Quell- und Zielservern handelt es sich stets um völlig eigenständige Systeme ohne gemeinsame Komponenten, so dass es keinen Single Point of Failure gibt. Teure Investitionen in SAN-Umgebungen oder Cluster sind nicht nötig. Für eine Replizierung ist so durchaus Standard-Hardware mit lokalen Raid-Platten-Einheiten geeignet.

Double-Take für Hyper-V (DTHV) deckt funktional zwei Grundszenarien ab. Das eine ist die Absicherung eines physikalischen Servers durch eine virtuelle Maschine (VM) unter Hyper-V, wobei sich durchaus mehrere physikalische Server auf ein zentrales Hyper-V-System replizieren lassen. Der Vorteil besteht darin, dass im Normalfall für den Betrieb die volle Leistung eines eigenständigen Servers zur Verfügung steht und ein Hyper-V-System als Backup für mehrere dieser Server dient, was letztendlich ein kostengünstiges Ausfallkonzept ermöglicht. Das zweite Szenario stellt die Replizierung von Hyper-V-VMs auf einen anderen Hyper-V-Host dar. Dabei ist keine 1:1-Beziehung zwischen zwei Hyper-V-Hosts erforderlich, es lässt sich vielmehr für jede VM das Zielsystem individuell festlegen. Ein Unternehmen kann also bei Bedarf eine ganze Hyper-V-Farm aufbauen, in der die VMs nach einem vorgegebenen Muster repliziert werden. Selbstverständlich ist es auch möglich, nur für wichtige VMs eine Replizierung einzurichten.

Übersichtliche Installation

Die Installation von DTHV selbst erwies sich als unproblematisch. Wahlweise kann ein Administrator nur die Server- oder auch die Clientkomponenten auf den Systemen einrichten. Er sollte darauf achten, aus dem Installationsmenü tatsächlich die DTHV-Version zu wählen, da das normale Double-Take zusätzlich in der Auswahlliste zu finden ist. Letztendlich wird es bei der Hyper-V-Variante ebenfalls als Basisdienst mit benötigt. Die Clientkomponente stellt letztlich die Steuerkonsole dar, die wir für den Test auf einem eigenen Arbeitsplatz installierten, wobei hier mindestens Windows XP SP2, Windows 2003 SP1 oder Windows 2008 vorausgesetzt werden.

Die Installationsroutine öffnet auf Wunsch automatisch die benötigten Ports 6320, 6332 und 135 auf der Firewall des Servers, zusätzlich ist es erforderlich, die Netzwerkerkennung auf den Hyper-V-Hosts zu aktivieren. Weiterhin legt die Routine in der lokalen Benutzerverwaltung drei Double-Take-Gruppen an. Hier ist es wichtig, mindestens einen Benutzer in die Gruppe der Double-Take-Admins aufzunehmen, mit dem die Authentifizierung innerhalb der Konsole erfolgt. Für den Test von DTHV standen uns zwei Server mit Dual- und Quadcore-Prozessoren mit ausreichend Plattenkapazität sowie Arbeitsspeicher zur Verfügung, auf denen wir Windows Server 2008 Enterprise deutsch sowie DTHV installierten, dessen Oberfläche allerdings stets in Englisch ist.

Angepasste Ablagestruktur für VMs

Standardmäßig schlägt der Hyper-V-Manager für die Anlage virtueller Maschinen ein gemeinsames Verzeichnis für die Festplattendateien vor sowie ein weiteres Verzeichnis, in dem er für jede VM einen Unterordner für die Konfiguration, Snapshots und weitere Daten anlegt. Mit dieser Struktur kann DTHV nicht umgehen. Die Software verlangt, dass für jede VM ein eigener Ordner gegebenen-

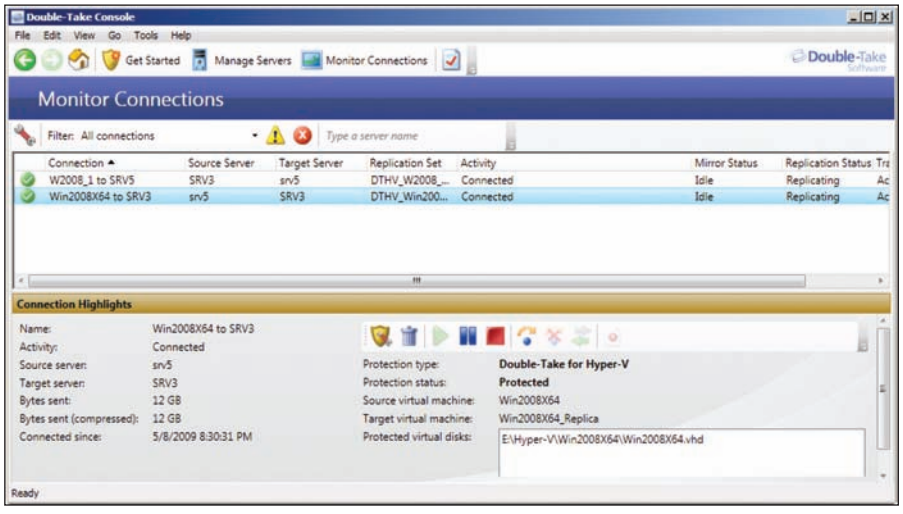


Bild 2: Double-Take für Hyper-V listet die aktiven Replikationsverbindungen übersichtlich auf

Bei der Entscheidung für den Test von Double-Take für Hyper-V hatten wir vorab mit der zuständigen Presseagentur gesprochen, da wir uns nicht sicher waren, ob wir besser die schon länger auf dem Markt befindliche Version für VMware oder eben die brandneue Variante für Hyper-V testen sollen. "Die Hitraten auf den Webseiten von Double-Take für das Hyper-V-Produkt zeigen ein deutlich größeres Marktinteresse" war die für uns ausschlaggebende Antwort. Dass dies zu einer etwas zeitintensiven, aber ebenso interessanten und fruchtbaren Produktevaluierung führen würde, hätten wir vorher nicht gedacht. Interessant und fruchtbar deshalb, weil sich der Support von Double-Take als überaus engagiert zeigte, regelmäßig über die Fortentwicklung berichtete und so einen Einblick in die zu bewältigenden Probleme gewährte. Dabei haben die Entwickler Mails sogar sonntags beantwortet. Ein Level 3-Supportspezialist, der direkt mit der Entwicklung kommunizierte, hatte sich der Thematik angenommen.

Bereits kurz nach der Installation zeigte sich das erste unüberwindbare Problem, dass der Assistent mit einer wenig aussagekräftigen Fehlermeldung die Einrichtung einer Replikation verweigerte. Da das gleiche Problem vorher schon einmal auf einem französisch-sprachigen Server aufgetreten war, tippte der Supporter auf ein generelles Problem mit unterschiedlichen Sprachversionen und lieferte eine modifizierte DLL-Datei, die den Fehler tatsächlich beseitigte. Die DLL-Datei mussten wir manuell in mehreren Verzeichnissen ersetzen, da keine Patchroutine existierte. Nun ließen sich Replikationen einrichten, die auch synchronisierten. Beim Failover-Test traten allerdings erneut Probleme auf. Egal ob wir die integrierte Failover-Funktion nutzten oder den Quellserver abrupt ausschalteten – auf dem Zielserver wurden unter Hyper-V keine virtuellen Maschinen registriert und gestartet. Dieses Verhalten war bei Double-Take noch nicht beobachtet worden und so lieferten wir umfangreiche Logdateien und Verzeichnisinhalte, nach deren Auswertung Double-Take den Fehler schließlich nachvollziehen konnte.

Innerhalb einer Woche lieferte der Hersteller einen komplett neuen Build, der allerdings wieder einen Bug im Assistenten hatte, ähnlich wie der erste Fehler. Weitere drei Tage später erreichte uns ein fehlerfreier Build, mit dem wir dann alle Funktionen testen konnten. So waren wir fast live dabei und zumindest die ersten hierzulande, die DTHV in komplett lauffähigem Zustand betreiben konnten. Aus den Gesprächen mit dem Spezialisten konnten wir deutlich heraushören, dass Microsoft nach wie vor nicht alles offenlegt und manche Dinge wohl einfach getestet werden müssen. Wenn es dann Unterschiede zwischen den Sprachversionen gibt, fallen diese erst relativ spät auf und führen genau zu solchen Effekten. Im vorliegenden Fall lag es wohl an automatischen Übersetzungen, die Windows zum Teil durchführt, zum Teil aber auch nicht. So setzt Windows beispielsweise die Bezeichnungen Betriebssystem-naher Verzeichnisse (Programme - Program Files, Benutzer - Users) oder Gruppen (Administratoren - Administrators) intern um, um eigentlich solche Namensprobleme zu lösen.

Selbst wenn in diesem Fall das Produkt nicht auf Anhieb lief, wollten wir es nicht gleich als "Bananensoftware" abstempeln, die erst beim Kunden reift. Es ist offensichtlich nicht so einfach, für solch ein komplexes Betriebssystem wie Windows einen systemnahen Zusatz zu programmieren, vor allem, weil auch Microsoft selbst lange benötigt hat, um die Hyper-V-Basis auf den Markt zu bringen, noch kurzfristige Änderungen durchgeführt hat und zu guter Letzt nicht alle Schnittstellen offenlegt. Zum Testzeitpunkt war zudem schon die nächste Hürde in Form von Windows 2008 R2 in Sicht, die erneut Anpassungen erfordern wird.

Reifungsprozess

falls mit Unterordnern angelegt wird, in dem sich die Festplatten-Dateien befinden. Der Administrator muss also für jede neue VM die Standardeinstellungen von Hyper-V abwählen und manuell einen neuen Ordner festlegen. Hintergrund dafür ist, dass DTHV für diesen Ordner eine Replikation auf den zweiten Server ebenfalls wieder in eine korrespondierende Verzeichnisstruktur einrichtet und so sicherstellt, dass alle notwendigen Dateien synchronisiert werden. Die erforderliche Struktur ist also eher mit der zu vergleichen, wie sie auch VMware verwendet.

Der Einsatz unterschiedlicher Hardware ist wie in unserem Fall mit verschiedenen Servern mit Dual- und Quadcore-Prozessoren für DTHV kein Problem. Bezüglich der Verwendung unterschiedlicher Netzwerkkarten und der Möglichkeit, unter Hyper-V auch mehr als nur eine Netzwerkkarte zu verwenden und mehrere virtuelle Switches zu konfigurieren, fragt DTHV bei der Einrichtung einer Replikation grundsätzlich die Zuordnung ab. Der Administrator muss also angeben, auf welche Karte im Zielsystem er die für die jeweilige VM verwendete Netzwerkkarte abbilden will.

Replikation und Failover

Die gesamte Bedienung läuft über die so genannte "Double-Take Console" ab, die relativ übersichtlich aufgebaut ist. Ein Assistent unterstützt hier sinnvoll bei der Einrichtung und bietet drei Optionen an. Mit der ersten sind alle Systeme mit DTHV-Installation zu erfassen. Für den Zugriff sind die Credentials für einen Benutzer anzugeben, der sich in der schon erwähnten DT-Admin-Gruppe befindet. Wir haben hierfür einen zentralen Domänenbenutzer gewählt. Unschön wirkt, dass eine eventuelle Fehlermeldung nicht direkt auf das tatsächliche Problem hinweist. Befindet sich beispielsweise der gewählte Benutzer nicht in der genannten Gruppe, so meldet DT immer einen unbekannten Benutzer oder ein falsches Passwort.

Konfiguration mit Hindernissen

Sind mindestens zwei Hyper-V-Server erfasst, lässt sich die erste Replikation einrichten. Dazu fragt der Assistent das Quell-System ab, listet dann die dort eingerichteten VMs zur Auswahl auf, anschließend den Zielserver sowie einen Pfad für die Ablage der Replika-Dateien. Im Test war allerdings bereits nach der Abfrage des Quell-Servers

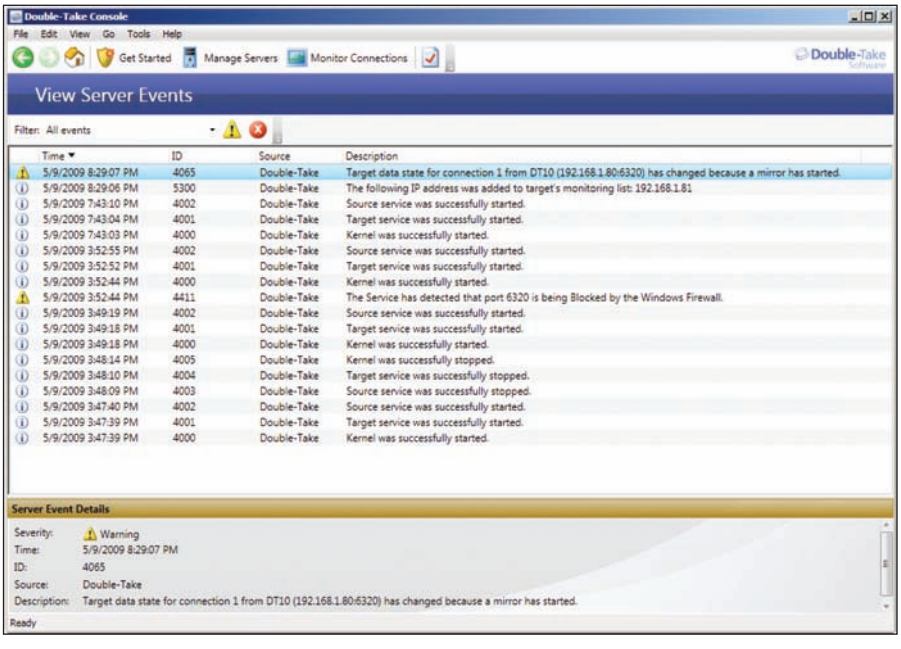


Bild 3: Eine detaillierte Ereignisanzeige erleichtert eine Nachverfolgung der durchgeführten Aktionen sowie eine bessere Fehlersuche

Leistungsstarke Hardware mit Dual- oder Quadcore-Prozessor mit Windows Server 2008 Standard, Enterprise oder Datacenter in der 64-Bit-Version mit installiertem Hyper-V-Service, mindestens 4 GByte Hauptspeicher. Nicht unterstützt werden Windows Server 2008 ohne Hyper-V, geclusterte Windows 2008 Hyper-V Hosts sowie der Hyper-V Server 2008. Wer physikalische Server schützen will, kann mit 32- oder 64-Bit-Maschinen mit Windows Server 2003 ab SP1 und mit Windows Server 2008 arbeiten. Um auf einer physikalischen Maschine für eine bessere Integration bei einem Failover die Hyper-V Integrationsdienste zu installieren, ist bei Windows Server 2003 SP2 Voraussetzung. Weitere Bedingungen für den Betrieb sind WMI und .NET in einer zum Betriebssystem passenden Version, wobei die Installationsroutine dies prüft und wie in unserem Fall das Service Pack 1 von .NET 3.51 automatisch nachinstalliert.

Systemvoraussetzungen

Schluss, DTHV antwortete stets mit einem eher irreführenden Hinweis, so dass wir hier nicht weiterkamen. Daher wendeten wir uns an unseren deutschen Ansprechpartner, der einen direkten Kontakt zu einem Level 3-Spezialisten bei Double-Take in den USA herstellte. Daraus entstand eine intensive Zusammenarbeit mit dem Hersteller, die wir im Kasten "Reifungsprozess" beschrieben haben.

Nachdem etwa zehn Tage später eine überarbeitete Version vorlag, konnten wir nun Replikationen nach Belieben einrichten. Dabei müssen bei zwei Servern nicht alle Aufträge in eine Richtung zeigen, sondern für eine sinnvolle Lastaufteilung ist es möglich, dass auf jedem Server einige VMs produktiv laufen und die beiden Systeme sich gegenseitig absichern. Fällt einer aus, übernimmt jeweils der andere die ausgefallenen VMs. Es ist nur darauf zu achten, dass beide Server gerade von der Arbeitsspeicherbestückung her in der Lage sind, alle VMs auch betreiben zu können. Beim Arbeiten mit der DTHV-Konsole fällt auf, dass die Fortschrittsangaben nicht genau stimmen, wenn mehrere Replikationen parallel laufen.

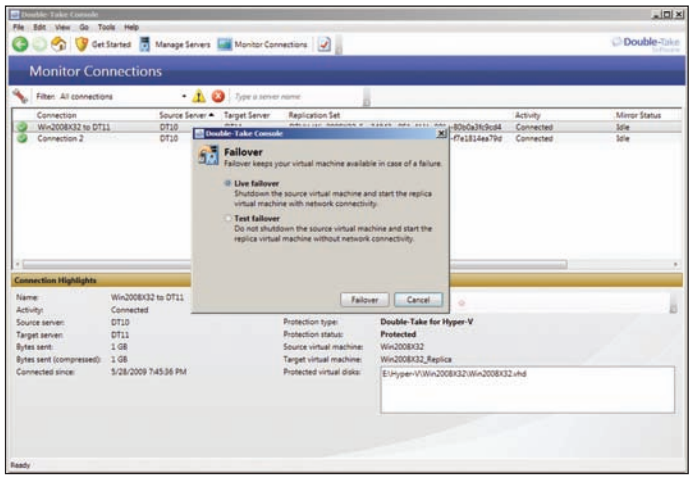


Bild 4: Ein Failover lässt sich manuell auslösen, auch zum Test ohne Netzwerkverbindung und ohne die produktive Maschine herunterzufahren

Statt für jede Verbindung die übertragene Datenmenge und den prozentualen Fortschritt getrennt anzuzeigen, bildet die Software hier vielmehr Summen und gibt diese aus.

Failover und Failback ohne Probleme

Nachdem alle konfigurierten Replikationen synchron waren, wollten wir das Verhalten bei einem Failover prüfen. Hierzu verwendeten wir in einem ersten Schritt die vorbereitete Failover-Funktion. Diese fragt ab, ob tatsächlich ein Live-Failover durchgeführt oder für einen Test die Ziel-VM ohne Netzwerkkonnektivität hochgefahren werden soll. Wir entschieden uns für einen Live Failover. Dazu fährt DTHV die Quell-VM herunter, deregistriert diese, registriert zugleich auf dem Ziel-Server eine neue Hyper-V-VM mit identischem Namen sowie einem Zusatz "_Replica" und fährt diese hoch. Anschließend ist der Server aus Benutzersicht wieder voll verfügbar.

Ist nun nach einem Failover ein Failback gefragt, um beispielsweise nach Reparatur der ausgefallenen Hardware die VMs wieder zu verteilen, so lässt sich das recht komfortabel realisieren. Hierzu besteht die Möglichkeit, eine Replikation in umgekehrte Richtung anzustoßen. Dazu muss Doubletake allerdings die ursprüngliche Quell-VM löschen, sofern das Verzeichnis noch existiert, denn letztendlich wird unabhängig von den alten Quelldaten wieder ein komplett neuer Spiegel aufgebaut. Ist dieser synchron, kann der Administrator wieder einen Failover zurück auf den alten Quell-Server anstoßen, so dass es letztendlich zu einer Wiederherstellung des Ursprungszustands kommt. Dieses Szenario funktionierte im Test problemlos, ein Failback lief genauso komfortabel ab wie ein Failover.

Nicht so elegant verhielt sich DTHV allerdings, wenn nach einem Ausfall eines Hyper-V-Servers dieser gar nicht mehr aufgebaut, sondern durch eine Neuinstallation ersetzt werden sollte. Das Problem ist, dass sich einmal eingerichtete Replizierungen nur dann problemlos löschen lassen, wenn die beiden beteiligen Server von der Konsole aus erreichbar, also online sind. Andernfalls verschwindet die Verbindung zwar augenscheinlich aus der Konsole, schlummert aber immer noch im Hintergrund und es sind manuelle Bereinigungen in der Registry notwendig. So ist es ratsam, die Registry nach den verwendeten Systemnamen und IP-Adressen zu durchsuchen und die verwaisten Einträge zu löschen. Hier besteht noch Optimierungsbedarf.

Absicherung physikalischer Maschinen

Neben dem Schutz von VMs testeten wir abschließend die noch verbleibende, dritte Option des Assistenten, eine Replikation von einem physikalischen Server auf eine Hyper-V-VM. Unser abzusichernder Server lief unter Windows 2008 und DTHV bot bei der Einrichtung der Replikation an, schon zu Be-

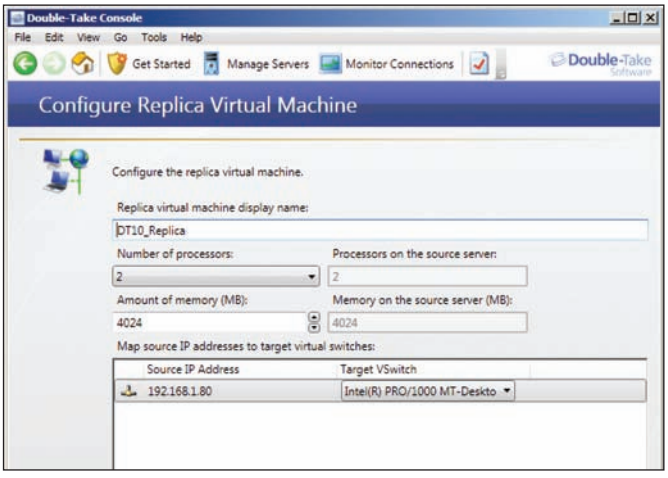


Bild 5: Bei der Absicherung einer physikalischen Maschine schlägt DTHV für die zu erstellende VM geeignete Kenngrößen vor, die der Administrator anpassen kann.

ginn die Integrationsdienste für Hyper-V zu installieren, damit später im Failover-Fall nichts mehr nachinstalliert werden muss. Hierzu nutzt das Programm etwas andere Prozesse wie bei der Hyper-V-Replikation, die auf Anhieb fehlerfrei laufen. So sahen wir bereits bei der Einrichtung der Verbindung, dass auf dem Zielsystem eine entsprechende VM im Hyper-V-Manager angelegt wird, die ausgeschaltet ist. Es lässt sich einstellen, ob die VM bei Ausfall beziehungsweise Nichterreichbarkeit des physikalischen Servers automatisch gestartet werden soll oder nicht.

Bei unserem Test erfolgte die automatische Übernahme reibungslos und der Server war für die Anwender nach wenigen Sekunden Ausfall wieder verfügbar. Allerdings vermissten wir hier die Möglichkeit eines Failbacks. Angenommen, der ausgefallene Server ist wieder funktionstüchtig und soll die Arbeit erneut übernehmen, dann sieht Double-Take hierfür keinen automatischen Prozess vor, was das Ganze recht aufwändig macht. So können die beiden Systeme für eine Datenübernahme nicht gleichzeitig laufen, da beide mit gleichem Namen und eventuell sogar gleicher IP-Adresse im Netz sichtbar sind. Hier lässt Double-Take den Anwender allein und dieser kann sich selbst überlegen, wie er eventuell mittels Backup und Restore die Daten überträgt. Laut Double-Take soll aber eine Failback-Funktion in einer der nächsten Versionen hinzukommen.

Fazit

Microsofts Hyper-V-Technologie ist noch nicht lange verfügbar und Double-Take hat seine Hyper-V-Unterstützung nur wenige Monate später veröffentlicht. Der prinzipielle Ansatz von Double-Take für Hyper-V überzeugt auf der ganzen Linie, hinsichtlich Zuverlässigkeit und Funktionalität ist aber noch Optimierungsbedarf erkennbar, so dass wir empfehlen, vor einem produktiven Einsatz noch einige Patches und Updates abzuwarten. So lassen sich bestehende Replizierungen nur dann problemlos löschen, wenn beide Seiten online sind. Andernfalls bleiben Registry-Einträge zurück, die der Nutzer vorsichtig manuell löschen muss. Bei der Replizierung einer physikalischen Maschine auf eine VM ist ein Failback nicht vorgesehen. Auch sind die Handbücher noch nicht vollständig.

Wir kamen insgesamt zu dem Eindruck, dass Hyper-V und darauf aufbauende systemnahe Produkte wie DTHV noch mit Vorsicht zu genießen sind, weniger aufgrund von Bugs in der zusätzlichen Software, sondern vielmehr, weil Hyper-V selbst immer noch im Wandel ist. So wird beispielsweise der zum Testzeitpunkt nur als Beta verfügbare Windows 2008 Server R2 von DTHV (noch) nicht unterstützt, da dortige Änderungen erst abzuwarten sind. Dazu kommt, dass Microsoft nach wie vor nicht alle Schnittstellen offenlegt und vor allem die Entwickler von solch systemnaher Software wie DTHV viel Arbeit investieren müssen, um ihr Produkt genau anzupassen. Wir können jedem Administrator nur empfehlen, umfassende eigene Tests und Pilotinstallationen vor einem geplanten Einsatz durchzuführen, um zu prüfen, inwiefern die Lösung die eigenen Anforderungen erfüllt und ob alles fehlerfrei läuft. *(ln)*

Produkt
Programm für die Replikation virtueller Maschinen unter Hyper-V zur Erhöhung der Verfügbarkeit.

Hersteller
Double-Take
http://de.doubletake.com/

Preis
Double-Take für Hyper-V kostet inklusive einem Jahr 7x24-Support abhängig von der OS-Version des Hyper-V Hosts in der Standard Edition 1.995 Euro, in der Enterprise Edition 2.995 Euro und in der Datacenter Edition 4.995 Euro für unlimitierte VMs.

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

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

Installation	8
Bedienung/Übersichtlichkeit	7
Failover	9
Failback	7
Dokumentation	6

Dieses Produkt eignet sich

optimal für Unternehmen, die einen kostengünstigen und wirksamen Ausfallschutz für mehrere physikalische Maschinen oder ihre Hyper-V-VMs benötigen.

bedingt, wenn nur eine physikalische Maschine oder nur sehr wenige Hyper-V-VMs abzusichern sind. Dann sollten Kosten und Aufwand genau geprüft werden.

nicht, wenn ein Unternehmen auf eine andere Virtualisierungslösung als Hyper-V setzt oder es auf Hochverfügbarkeit nicht ankommt.

Double-Take für Hyper-V

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 Test: OSCAR 6.03

Cluster zum Nulltarif

von Dr. Holger Reibold

Um in Unternehmen hochkomplexe und damit rechen- und zeitintensive Aufgaben zu bewältigen, die von einem Rechner alleine nicht zu bewerkstelligen sind, ist oftmals ein den Anforderungen entsprechender Cluster die erste Wahl von IT-Verantwortlichen. Inzwischen bietet auch der Open Source-Bereich eine Fülle an Lösungen für Hochverfügbarkeit und Rechenleistung im Verbund. IT-Administrator hat die freie Cluster-Lösung OSCAR getestet.

Das Prinzip ist eigentlich simpel: Steht kein Hochleistungsserver zur Verfügung, so schnüren IT-Verantwortliche je nach Anforderungen und Kapazitäten verfügbare Rechner zu einem Rechnerverbund, um das Potenzial der einzelnen Systeme zu bündeln. Je schneller die Netzwerkverbindungen zwischen den einzelnen Systemen sind, umso leistungsfähiger wird das Gesamtsystem. Das Hauptziel liegt in der Regel in der Erhöhung der Rechenkapazität oder der Verfügbarkeit gegenüber einem einzelnen Computer.

Prinzipiell lässt sich dabei zwischen Hardware- oder Software-Clustern unterscheiden. Die einfache Form eines Hardware-Clusters ist als "aktiv/passiv" bekannt. Andere Varianten werden beispielsweise als Cascading Cluster bezeichnet. Software- oder auch Application-Cluster sind meist in der Lage, einen kontinuierlichen Betrieb zu realisieren. Alles, was Sie für den Aufbau eines Clusters benötigen, ist eine bestimmte Anzahl an Rechnern, die quasi das Hardware-Rückgrat bilden und eine Software für die Steuerung und Konfiguration der Umgebung.

Die Open-Source-Lösung: OSCAR

Wenn Sie mit dem Gedanken spielen, einen Cluster aufzubauen, so stellt sich unweigerlich die Frage, welches die optimale Lösung ist. Hardware-Cluster sprengen häufig das Budget. Daher sind softwarebasierte Lösungen in der Regel die bessere Wahl. Als eines der interessantesten Projekte gilt OSCAR [1], ein Projekt der Open-Cluster-Group. Die Organisation versucht, die Entwicklungen rund um freie Software für den Cluster-Einsatz zu koordinieren und neue Entwicklungen anzustoßen. OSCAR steht übrigens für "Open Source Cluster Application Resources". Nach Angaben der Entwickler war OSCAR von Anfang an so konzipiert, dass sich mit dem freien Werkzeug auch mit relativ wenig Erfahrung in diesem Bereich professionelle Cluster realisieren lassen. In den USA ist OSCAR ein weit verbreitetes Werkzeug, in Europa hingegen kommt es vergleichsweise selten zum Einsatz.

Im OSCAR-Paket sind alle Tools für den Aufbau und die Programmierung eines High-Performance-Clusters, kurz HPC, integriert. Ein weiterer Punkt spricht für den Einsatz von OSCAR: Es enthält fertige Pakete, die für den Einsatz auf gängigen Linux-Plattformen vorbereitet sind. Administratoren, die bereit sind, sich tiefer in die Materie einzuarbeiten, können mit OSCAR auch eigene Umgebungen mit spezifischen Eigenschaften realisieren.

Unterstützte Plattformen

Plattform	Architektur	Status
Red Hat Enterprise Linux 5 / CentOS 5	x86	Volle Unterstützung
Red Hat Enterprise Linux 5 / CentOS 5	x86_64	Volle Unterstützung
Debian 4	x86	Volle Unterstützung
Debian 4	x86_64	Volle Unterstützung
Ubuntu 8.04	x86	Volle Unterstützung
Ubuntu 8.04	x86_64	Volle Unterstützung
Debian 5	x86_64	Experimentell
Fedora Core 9	x86	Experimentell
Open Suse 10	x86	Experimentell

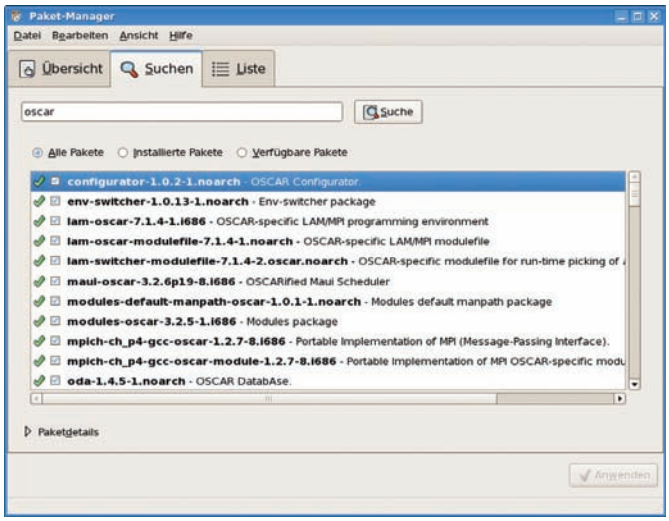


Bild 1: Ist die CentOS-Systemkonfiguration um die Repository-Informationen für den Download von OSCAR erweitert, gestaltet sich die Installation über den Paketmanager einfach

OSCAR setzt auf einer Standard-Linux-Installation auf. Eine Standardinstallation verwendet die MPI-Implementierung (Message Passing Interface). Inzwischen gibt es verschiedene solcher Implementierungen. Eine der Stärken des OSCAR-Systems ist es, dass es die verschiedenen Varianten unterstützt und somit auch mit anderen Umgebungen problemlos kommunizieren kann, die ebenfalls eine MRI-Variante verwenden. Aktuell ist Version 6.0.3 von Ende Mai 2009.

Bestandteile von OSCAR

In einem OSCAR-System gibt es zwei Modi: Client und Server. Prinzipiell lässt sich ein Cluster mit einem Prozessor und Betriebssystem (homogener Cluster) und mit verschiedenen Prozessoren und Betriebssystemen (heterogener Cluster) erzeugen. Das OSCAR-System besteht ähnlich einem Baukasten aus mehreren Paketen, die sich in drei Kategorien einteilen lassen:

- Core-Pakete: Diese Komponenten werden für den Aufbau und den Betrieb eines Clusters benötigt. Sie werden überwiegend mit dem Installer eingerichtet.
- Zusatzpakete: Hierbei handelt es sich um Erweiterungen der Kernfunktionalität, die überwiegend von den OSCAR-Entwicklern stammen.
- Pakete von Dritt-Anbietern: Für OSCAR stehen verschiedene Erweiterungen von Drittentwicklern zur Verfügung.

OSCAR verfügt mit der System-Installations-Suite, kurz SIS, über ein spezielles Cluster-Installationswerkzeug. Dieses System vereinfacht die Installation und kommt aus mehreren Gründen zum Einsatz:

- SIS ist ein qualitativ hochwertiger Open-Source-Installer, der hervorragend mit Produktionsumgebungen arbeitet.
- Für den Einsatz des Installers ist kein Client-Knoten erforderlich.

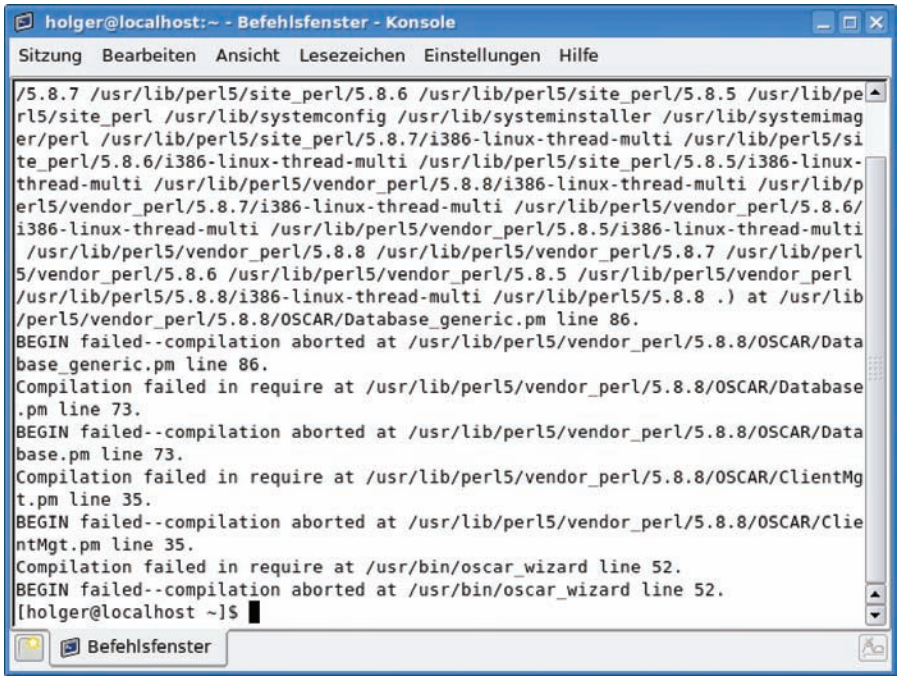


Bild 2: In der Praxis treten immer wieder Probleme bei der Installation von Version 6.x auf, die mit dem Download-Archiv von OSCAR5.x so nicht auftreten

- Die SIS verfügt über eine zentrale Datenbank, die die Daten der einzelnen Knoten verwaltet. Dazu gehören beispielsweise die IP-Adresse und der Image-Name.

OSCAR sollte sich auch problemlos auf Klon-Plattformen ausführen lassen, die auf einer der oben genannten Plattformen basieren. Sie können es beispielsweise problemlos auf dem RHEL-Klon CentOS ausführen.

Systemvoraussetzungen

Um einen OSCAR-Server aufsetzen zu können, muss das Serversystem folgende Systemvoraussetzungen erfüllen:

- Pentium oder höher
- Netzwerkadapter mit TCP/IP-Unterstützung
- Befinden sich Cluster-Knoten außerhalb des lokalen Netzwerks, wird ein zweiter Netzwerkadapter benötigt
- Mindestens 4 GByte freier Speicherplatz (davon 2 GByte unter "/" und 2 GByte unter "/var")

Als Client können Sie die in der Tabelle "Unterstützte Plattformen" erwähnten Systeme nutzen. Sie sollten außerdem über ein CD-ROM-Laufwerk oder aber über ein PXE-aktiviertes BIOS verfügen.

OSCAR in Betrieb nehmen

Die Inbetriebnahme von OSCAR ist theoretisch relativ einfach. Eine Standardinstallation auf einer der oben aufgeführten Linux-Varianten in einer Workstation-Version genügt in der Regel vollkommen, um als Basis für ein OSCAR-System eingesetzt werden zu können. Wichtig, wenn Sie mit Version 6.x arbeiten wollen: Das zukünftige OSCAR-System benötigt einen Internetzugang, da es keine klassischen Downloads mehr für OSCAR gibt, sondern der Zugriff direkt über ein Online-Repository erfolgt.

Auf Seiten des Servers sind für die Speicherung der OSCAR-Images circa 2 GByte an Speicherplatz erforderlich. Die Daten werden standardmäßig in das Verzeichnis */var/lib/systemimager* gelegt. Sie benötigen in etwa 2 GByte pro Image. In der Regel erfüllen alle Systeme diese Anforderungen. Um OSCAR installieren zu können, sind Root-Rechte erforderlich. Verschaffen Sie sich also zunächst mithilfe von *su* die notwendigen Berechtigungen. Als Nächstes gilt es, das System für die Verwendung des Online-Repositorys einzurichten. Die Vorgehensweise ist davon abhängig, mit welchem System Sie arbeiten.

Um mit einem CentOS- beziehungsweise RHEL-basierten System zu arbeiten, meldeten wir uns als Root an und fügten die folgende Datei dem Verzeichnis */etc/yum.repos.d* hinzu:

```
# CentOS-OSCAR.repo
#
# If the mirrorlist= does not work
  for you, as a fall back you can
  try the
# remarked out baseurl= line inste-
  ad.
#
[oscar]
name=CentOS-$releasever - OSCAR
baseurl=http://bison.csm.ornl.gov/re
  pos/rhel-5-{arch}
gpgcheck=0
```

Anschließend ersetzten wir *{arch}* durch die tatsächlich verwendete Architektur, also i386 oder x86_64. Als Nächstes stellten wir mit dem Befehl *yum update* si-

Bild 3: Der OSCAR-Einrichtungsassistent führt durch die notwendigen Schritte

cher, dass unser System auf dem neuesten Stand ist. Um das OSCAR-RPM zu installieren, führten wir als Root folgenden Befehl aus:

```
yum install oscar
```

Alternativ lässt sich auch der Paketmanager von RHEL/CentOS verwenden.

Im nächsten Schritt galt es, die Datei */etc/oscar/oscar.conf* zu prüfen. Konkret prüften wir insbesondere die OSCAR-Schnittstelle und die Netzwerkschnittstelle, um danach als Root folgenden Befehl auszuführen:

```
oscar-config –setup-distro {distro}-
  {version}-{arch}
```

Beim Einsatz eines Debian 4 oder eines Ubuntu-basierten Systems müssen die folgenden Zeilen der */etc/apt/sources.list* hinzugefügt werden:

- Für x86_64 Systeme: *deb http://bison.csm.ornl.gov/repos/debian-4-x86_64/etch/*
- Bei x86-Systemen: *deb http://bison.csm.ornl.gov/repos/debian-4-i386/etch/*

Nun folgt der Befehl *aptitude update,* um sicherzustellen, dass das System auf dem neuesten Stand ist. Die OSCAR-Pakete für Debian-basierte Systeme installieren IT-Verantwortliche über *apt-get install oscar.* Auch unter Debian muss nun die OSCAR-Konfigurationsdatei */etc/oscar/oscar.conf* geprüft und abschließend folgender Befehl ausgeführt werden:

```
oscar-config –setup-distro {distro}-
  {version}-{arch}
```

Die letzte Alternative ist ein Betrieb unter Fedora Core 9: Hier muss der Anwender die folgende Datei dem Verzeichnis */etc/yum.repos.d* hinzufügen:

```
# CentOS-OSCAR.repo
#
# If the mirrorlist= does not work
  for you, as a fall back you can
  try the
# remarked out baseurl= line
  instead.
#
[oscar]
name=CentOS-$releasever - OSCAR
baseurl=http://bison.csm.ornl.gov/
  repos/fc-9-i386
gpgcheck=0
```

Schließlich ersetzen Sie *{arch}* wieder durch die jeweilige Plattformeigenschaft. Die eigentliche Installation erfolgt auch hier wieder mit dem Befehl *yum install oscar.* Nach der Installation folgt die Prüfung der OSCAR-Konfigurationsdatei und folgender Befehl schließt die Installation ab: *oscar-config -setup-distro fedora-9-i386.*

Hürde Cluster-Installation

Mit den bisherigen Schritten nahmen wir OSCAR in Betrieb und widmeten uns nun der Cluster-Installation. Wie bereits erwähnt, steht für die Cluster-Installation ein eigener Installer zur Verfügung. Um diesen zu starten, wechselten wir in das Wurzelverzeichnis der OSCAR-Installation und führten folgende Befehle aus:

```
oscar-config –bootstrap
system-sanity
oscar_wizard install
```

Der Befehl *oscar-config -bootstrap* führt verschiedene Einrichtungs- und Konfigurationsschritte durch. So werden damit beispielsweise verschiedene Pakete auf dem Server installiert, auch alle OSACR-Serverpakete, die Dateien */etc/hosts* und */etc/exports* werden aktualisiert und es erfolgt ein Neustart der Systemdienste, die OSCAR benötigt.

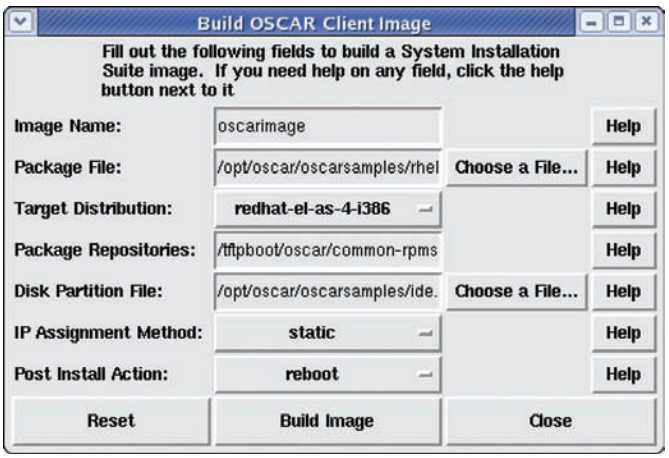


Bild 4: Das Anlegen eines Client-Images ist mithilfe des Einrichtungsassistenten einfach

Bei der Ausführung des oscar-config-Befehls kam es auch bei einer Plattform wie CentOS, die laut Angaben des OSCAR-Entwicklerteams zu den voll unterstützten Umgebungen gehört, leider immer wieder zu Abbrüchen des Installationsvorgangs. In der OSCAR-FAQ [2] finden sich verschiedene Problemlösungen, doch helfen die nicht immer weiter. Lässt sich die Ursache nicht lokalisieren und beheben, bleibt nur der Weg über die Version 5.x. Deren Installation und Konfiguration verlief unproblematischer. OSCAR gibt beim Aufruf des Assistenten auf der Konsole eine Unmenge an Informationen aus. In der Protokolldatei */var/log/oscar/oscar_wizard.log* lasen sich möglicherweise Hinweise für einen möglichen Abbruch der Installation finden.

Ein erfolgreich ausgeführter oscar-wizard-Befehl startete den eigentlichen OSCAR-Einrichtungsassistenten, der uns durch die acht Schritte für die Einrichtung einer Cluster-Umgebung führte. In Zukunft wird es auch einen neunten Schritt geben, der bislang noch die Bezeichnung "Step 0" trägt und dann der Verwaltung der Repositories dienen soll.

Bild 5: Die Testfunktion im OSCAR-Einrichtungsassistent gibt grünes Licht

Die Schritte im Überklick:

1. Der erste Schritt trägt die Bezeichnung "Select OSCAR Packages To Install": Mit einem Klick auf diese Schaltfläche öffneten wir einen Auswahldialog, der uns die Auswahl von Nicht-Kern-Paketen des OSCAR-Systems erlaubte.
2. Es folgt "Configure Selected OSCAR Packages": Für verschiedene Pakete stehen eigene Konfigurationsoptionen zur Verfügung. Auf diese griffen wir nun zu und passten diese an.
3. Mit einem Klick auf die Schaltfläche "Install OSCAR Server Packages" installierten wir alle ausgewählten Serverpakete mit den angepassten Optionen.
4. Der Schritt "Build OSCAR Client Image" erlaubte es uns, ein Client-Image mithilfe des OSCAR-System-Installers zu erzeugen. Dieses Image wird dann an die Knoten als Teil der Cluster-Installation übermittelt.
5. Nachdem die Client-Images erzeugt worden waren, legten wir unter "Define OSCAR Clients" fest, welches die Clients sein sollten. Hier liessen sich beispielsweise deren Hostnamen oder IP-Adressen angeben.
6. Anschließend bestimmten wir unter "Setup Networking" die MAC-Adressen der Clients, damit die zugehörigen Systeme bei deren späteren Systemstart automatisch in das System eingebunden werden. In diesem Schritt bestimmten wir auch den Installationsmodus. Bislang gibt es drei Modi: systemimager-rsync als Standardmodus, systemimager-multicast und systemimager-bt.
7. Nachdem wir alle Cluster-Knoten mit dem notwendigen Image versorgt und einen Neustart durchgeführten hatten, schlossen wir mit einem Klick auf "Complete Cluster Setup" die Installation ab und nahmen die Umgebung in Betrieb.
8. Schließlich stellte uns der OSCAR-Einrichtungsassistent eine Testfunktion ("Test Cluster Setup ") zur Verfügung, mit der wir die Installation und Konfiguration prüften.

Cluster-Administration

Nachdem wir die Installations- und Konfigurationshürden genommen hatten, wendeten wir uns im nächsten Schritt dem Management der Umgebung zu. Die Verwaltung der Umgebung wird dank des Managementassistenten zum Kinderspiel. Der Assistent besitzt eine einfache GUI, dank derer sich die meisten administrativen Aufgaben leicht erledigen lassen. Über die GUI können sich beispielsweise folgende Aktionen ausführen lassen:

- Client-Images erstellen
- Neue Knoten hinzufügen und bestehende Cluster-Knoten löschen

Produkt
Software für die Cluster-Bildung auf Linux-Basis.

Hersteller
Open Source

Preis
Kostenlos

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

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

Cluster-Bildung	9
Konfiguration	8
Flexibilität	7
Bedienung	9
Systemintegration	7

Dieses Produkt eignet sich

optimal für den Aufbau eines Linux-basierten Clusters beliebiger Größe.

gut für KMUs, die mit wenig Linux-Vorkenntnissen und geringem Budget eine HA-Lösung aufbauen wollen.

nicht für den Einsatz in heterogenen Umgebungen.

OSCAR 6.03

- Cluster-Funktionalität testen
- Überwachung der Umgebung

Wichtig vor dem Start dieses Assistenten: Die eigentliche Cluster-Konfiguration muss mit dem Einrichtungsassistenten abgeschlossen sein. Den Managementassistenten starteten wir mit folgendem Befehl:

```
/usr/bin/oscar-wizard manage
```

Der Assistent führte uns durch den kompletten Managementprozess. So ließen sich beispielsweise über die Schaltfläche "Download Additional OSCAR Packages" die bereits erwähnten Zusatzpakete für die OSCAR-Umgebung herunterladen.

Fast schon kinderleicht war das Hinzufügen neuer Knoten, hierzu genügte uns ein Klick auf "Add OSCAR Clients". Anschließend bestimmten wir die IP-Adresse beziehungsweise den Hostname und hinterlegten dann die MAC-Adresse, damit der Client beim seinem Systemstart automatisch in den Cluster-Verbund aufgenommen wird.

Auch die Management-GUI stellt eine Testfunktion zur Verfügung. Mithilfe des Network-Boot-Managers legten wir außerdem einfach fest, wie sich Clients verhalten, wenn diese über das LAN booten. Sobald der Cluster mit den ersten Clients hochgefahren war, lieferte uns die Monitoring-Funktion der Management-GUI eine Übersicht über den Status der einzelnen Knoten. Administratoren, die tiefer in die Umgebung einsteigen wollen, können OSCAR auch über die Konsole verwalten. Hierfür stehen weit mehr Funktionen und Optionen zur Verfügung, als sie die GUI zu bieten hat.

Fazit

OSCAR genießt nicht umsonst einen ausgezeichneten Ruf unter den freien Lösungen für den Aufbau eines Clusters. Wenn die Installations- und Konfigurationshürden einmal gemeistert sind, belohnt das System den IT-Verantwortlichen mit einer Benutzerfreundlichkeit, die ihres gleichen sucht und ist somit gerade auch für den Einstieg in die Welt der Cluster sehr gut geeignet. *(jp)*

Links

[1] OSCAR-Projektseite
http://svn.oscar.openclustergroup.org/trac/oscar/wiki

[2] OSCAR-FAQ
http://svn.oscar.openclustergroup.org/trac/oscar/wiki/faq#Installation

Im Test: *Elastic Computing Platform von Enomaly*

Noch nicht ganz auf Wolke 7

von Thomas Weyergraf

Quelle: Ioannis Kounadeas - Fotolia.com

Noch ist nicht alles sonnig beim Cloud-Management

Alle möglichen Hersteller versuchen inzwischen, das Thema Cloud Computing zu besetzen. Doch um ganze Netzwerke aus verschiedenen Servern auf eine Cloud-Infrastruktur zu migrieren, sind neben ausgefeilten Virtualisierungstechniken vor allem hoch entwickelte Administrationswerkzeuge notwendig. Eine solche Managementlösung für virtuelle Cloud-Infrastrukturen bietet die Elastic Computing Platform (ECP) der kanadischen Firma Enomaly. Obwohl recht jung – Enomaly wurde 2004 gegründet – rühmt sich das Unternehmen mit einer ganzen Reihe namhafter Referenzkunden, darunter Schwergewichte wie Intel oder die Deutsche Bank. IT-Administrator hat ECP getestet und wichtige Aspekte der Plattform genauer betrachtet.

In der Cloud reicht es nicht mehr, einer virtuellen Maschine (VM) virtuell CPU, Arbeitsspeicher, Netzwerkanbindung und Plattenkapazität zuzuweisen. Galt die Migration von virtuellen Serverinstanzen von einem physikalischen Server auf einen anderen bislang als netter Bonus hinsichtlich der Ausfallsicherheit und Lastverteilung, so wird diese im Cloud-Umfeld zur unverzichtbaren Arbeitsgrundlage. Zudem muss die gesamte Infrastruktur verwaltet werden: Komplette Netzwerke, Storage-Pools und Cluster physikalischer Server, die den ausfallsicheren Betrieb der Gast-VMs gewährleisten. Eine vollständige, einfache und vor allem sichere Remote-Administration einer Cloud-gestützten Serverinfrastruktur ist für jede entsprechende Softwarelösung eine Herausforderung.

Management auf Basis von libvirt

ECP ist Linux-basierend und wird unter der GNU Affero GPL als Open Source angeboten. Nach Angabe einer gültigen E-Mailadresse auf der Downloadseite von Enomaly erhielten wir per E-Mail einen Link zum Download. Neben einigen Zusatzpaketen, die vornehmlich der Anpassung auf verschiedene Linux-Distributionen dienen, findet sich unter dem Namen "Enomalism Core" die eigentliche Software. Dieses Paket steht für eine ganze Reihe von Linux-Distributionen, wie Ubuntu, Centos, RedHat und Fedora zur Verfügung. ECP baut, wie im Open Source-Umfeld nicht unüblich, auf den Ergebnissen anderer Open Source-Projekte auf. Von entscheidender Bedeutung ist, dass ECP auf "libvirt", einem Toolkit, das maßgeblich von RedHat entwickelt wird, basiert. Mittels libvirt werden die verschiedenen Virtualisierungslösungen unter Linux, wie etwa Xen, KVM, Qemu oder OpenVZ, mit einer einheitlichen, netzwerkgestützten und sicheren Softwareschnittstelle versehen, die übergeordneten Managementlösungen wie ECP einen vereinfachten Zugriff bieten. Derzeit entwi-

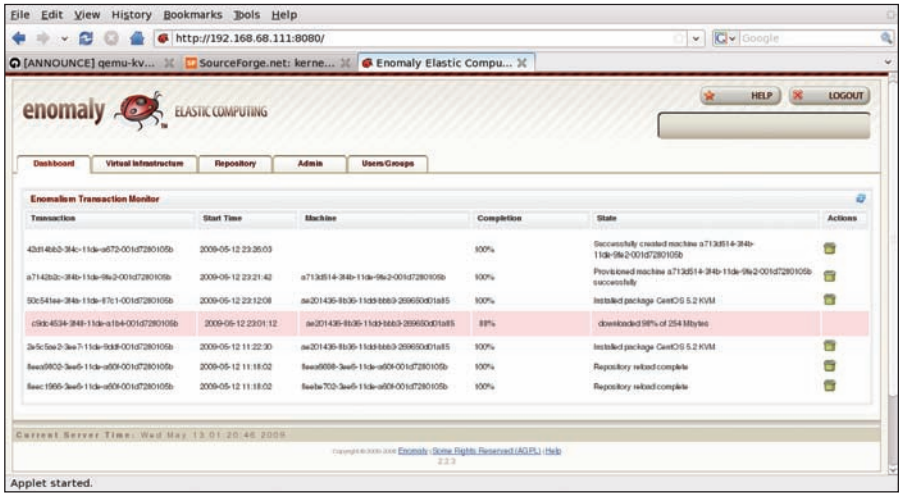


Bild 1: Die ECP-Oberfläche mit offenem Dashboard

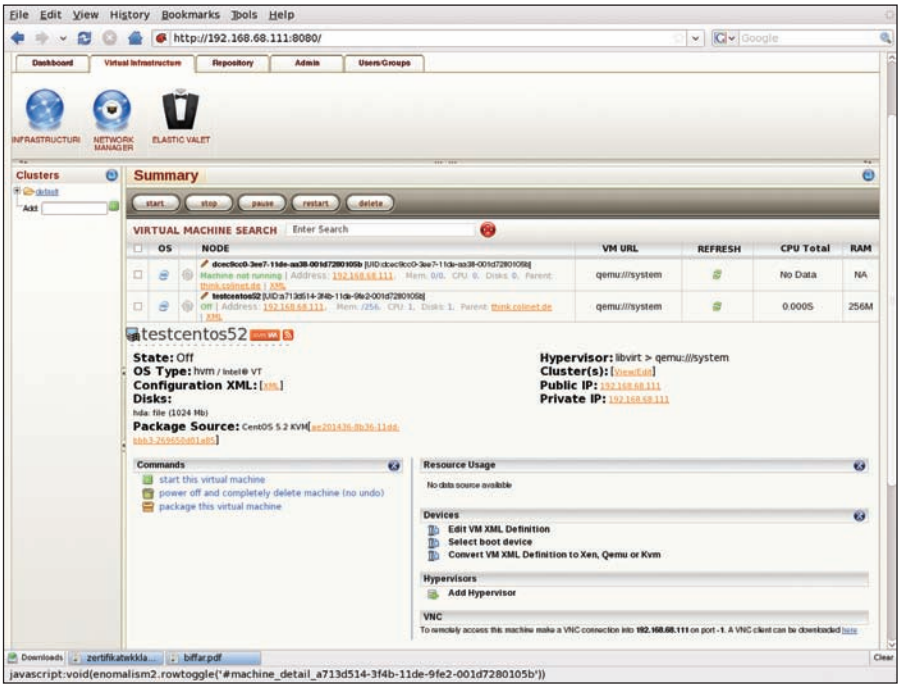


Bild 2: Die Darstellung einer laufenden VM in unserer Testumgebung ist äußerst detailliert

ckelt sich libvirt zu einem Defacto-Standard im Linuxumfeld, was den Umgang mit Virtualisierern angeht. Zudem lassen sich mit libvirt Netzwerkinfrastrukturen und Storage-Anbindungen für die verschiedenen Virtualisierer verwalten. Durch + libvirt verwendet ECP die Virtualisierungstechniken Xen und QEMU/KVM, über die wir im IT-Administrator in der Vergangenheit umfassend berichteten.

Installation

Um ECP auf einer passenden Distribution zu betreiben, müssen IT-Verantwortliche neben dem Enomalism-Paket noch eine ganze Reihe zusätzlicher Pakete installieren, die jedoch meist aus dem Repository des Host-Linux bedient werden können. ECP ist weitgehend in der Skriptsprache Python implementiert und legt alle möglichen Daten in einer eigenen MySQL-Datenbank ab. Den Installationsprozess durchliefen wir weitgehend manuell: Zusatzpakete spielten wir mit dem Package-Manager der Distribution ein und bereiteten diese entsprechend von Hand in den betreffenden Config-Files für ECP vor. Mittels Package-Manager spielten wie auch das eigentliche Enomalism-Paket ein, um im Anschluss einige Konfigurationsskripte durchlaufen zu lassen, die ECP mitbringt.

Zudem mussten in einer ECP-eigenen Konfigurationsdatei einige Einstellungen vorgenommen werden. Mittels eines Skripts starteten wir ECP erstmalig und konnten es fortan mit einem Browser auf Port 8080 bedienen. Der erste Besuch forderte zum Abschluss der Installation auf und bot anschließend die Möglichkeit, sich als Administrator "admin" mit Passwort "password" anzumelden. Alles in allem ist die Installation für einen Administrator problemlos zu bewältigen, bietet aber nicht zuletzt aufgrund der weit reichenden Abhängigkeiten viele Fehlerquellen. Wünschenswert wäre ein Installationsskript, was die notwendigen Einzelschritte automatisiert und Warnhinweise enthält.

An anderer Stelle verhält sich ECP dafür unerwartet automatisch: Im Verlauf des Tests installierten wir ECP auf einem Centos-Host, den wir zuvor bereits für libvirt und Netzwerkbridges konfiguriert hatten. Als ein ECP-Skript (*virt-network.sh*) versuchte, die Netzwerkkonfiguration automatisch vorzunehmen, stolperte es über die vorhandene Konfiguration und hinterließ diese in einem unbrauchbaren Zustand, ohne jedoch irgendwelche Konfigurationsdateien permanent zu ändern. Neben der Installationsanleitung auf der Enomaly-Homepage steht eine alternative Anleitung [2] zur Verfügung, die einige nützliche Hinweise enthält.

ECP im Betrieb

Nach erfolgreichem Login präsentierte sich ECP mit einem sehr aufgeräumten Webinterface, dass neben Buttons für Hilfe und zum Ausloggen fünf Tabs darstellt, unter denen sich die Managementfunktionen von ECP finden. Nach dem Login wird der Tab "Dashboard" dargestellt, der eine Liste von Transaktionen in ECP liefert. Dargestellt werden alle Kontrolloperationen an Virtuellen Maschinen, Repository-Bewegungen und Log-Einträge.

Cloud Computing

Im Prinzip ist die Cloud der nächste, logische Schritt nach der Virtualisierung. Während letztere für die Trennung von Server und eigentlicher Hardware gesorgt hat, lässt Cloud Computing das Rechenzentrum an sich gleich ganz verschwinden und ersetzt es durch entsprechende Internet-basierte Services. Dies ist mitnichten reine Zukunftsmusik – so hat beispielsweise Amazon Cloud-Services im Angebot: Die Amazon Elastic Compute Cloud. Anwender können sich virtuelle Server unterschiedlicher Ausbaustufen auf Stundenbasis mieten [1].

Die versprochenen Vorteile ähneln dabei denen der Virtualisierung: Effizientere Hardwareauslastung, Ausfall der Anschaffungskosten für eigene Serverhardware samt Infrastruktur, einfachere Administration. Derzeit kann Cloud Computing diese Versprechen nur in einem eng umrissenen Anwendungsszenario einlösen. Vor allem die verfügbaren – und vor allem bezahlbaren – Internetbandbreiten, die für die Kommunikation der Clients mir einer Cloud-Infrastruktur benötigt werden, reichen derzeit bei weitem nicht aus. Selbst wenn dem so wäre, die anfallenden Kosten für die Cloud-Nutzung kalkulieren sich auf der gleichen Grundlage wie ein lokales Rechenzentrum – abgesehen natürlich vom offensichtlichen Unterschied in der Anschaffung. Oder provokant formuliert: eine Kilowattstunde Energieverbrauch in einer Cloud muss genauso bezahlt werden wie die Kilowattstunde eines lokalen Servers. Bei aller Skepsis hinsichtlich Cloud Computing birgt das Konzept einige interessante Aspekte.

Der nächste Tab "Virtual Infrastructure" bietet den Zugang zum Cloud-Management. ECP fasst physikalische Systeme zu "Clustern" zusammen, auf denen wiederum virtuelle Maschinen betrieben werden. Der Tab "Virtual Infrastructure" bietet seinerseits drei weitere Tabs: Über "Infrastructure" haben Administratoren Zugang zum Management der Cluster und den darauf laufenden virtuellen Maschinen. Hier lassen sich Cluster erzeugen, ändern und löschen. Auch virtuelle Maschinen können hier gestartet, gestoppt, erzeugt, gelöscht und detailliert administriert werden bis hin zum Remote-Zugang via VNC.

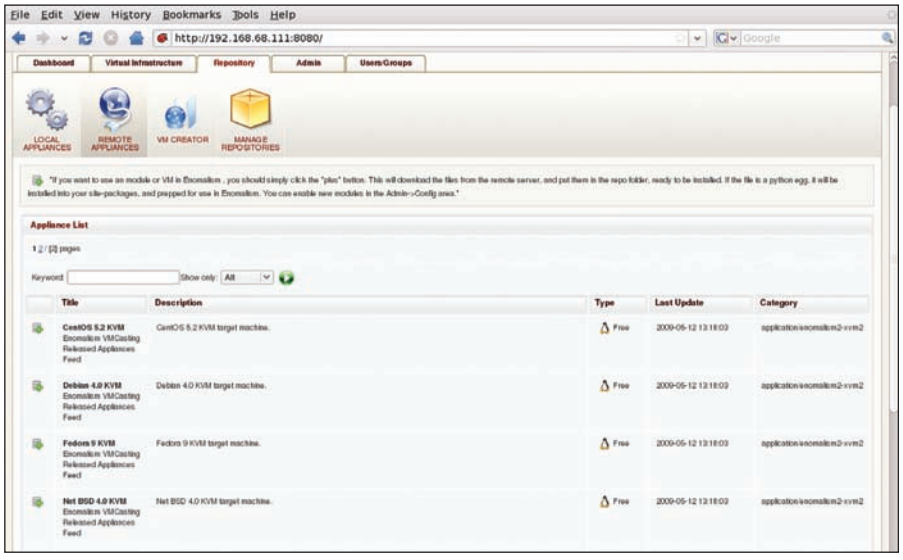


Bild 3: Das Remote-Repository der Testumgebung

ECP präsentiert die umfassenden Informationen übersichtlich und strukturiert die administrativen Funktionen sauber. Wem die angebotenen Konfigurationsmöglichkeiten nicht ausreichen, dem bietet ECP die Möglichkeit, die XML-Konfigurationsdatei direkt zu bearbeiten. Das ist vor allem dann sehr sinnvoll, wenn QEMU/KVM als Virtualisierungstechnologie zum Einsatz kommt. Insbesondere das QEMU-Frontend kennt eine schier unendliche Zahl von Kommandozeilenparameter, die so ziemlich jeden Aspekt einer VM konfigurieren können. Dies vollständig in einem Webinterface aufzubereiten, wäre nicht nur ein schwieriges Unterfangen, sondern würde auch zu einem wahren Interface-Monster führen. ECP umschifft diese Klippe zugunsten der Einfachheit geschickt: Exotischere Optionen werden einfach im XML-Configfile gesetzt. Wird im Infrastructure-Tab keine individuelle Maschine abgerufen (siehe Bild 2), so wird ähnlich dem Dashboard eine Liste der laufenden physikalischen und virtuellen Maschinen geboten.

Unflexibles Netzwerkmanagement

Mit dem Tab "Network Manager" unter "Virtual Infrastructure" kann der Administrator die Netzwerkkonfiguration für die virtuellen Maschinen in der Cloud konfigurieren. ECP setzt zum Netzwerkmanagement auf Linux Ethernetbridges, die jede normale Linux-Distribution bietet. Entsprechend legt ECP neue Netzwerke als Bridge-Devices an, erwartet einen Namen für das Netzwerk, eine verfügbare IP-Range und den Cluster, zu dem das Netz gehören soll.

Sonderlich flexibel ist ECP in Sachen Netzwerkkonfiguration derzeit noch nicht. Es fehlt zum Beispiel eine Möglichkeit, Einfluss darauf zu nehmen, welches physikalische Ethernetinterface welcher Bridge zugewiesen wird. Eine explizite Möglichkeit, Storage-Netzwerke aus ECP heraus zu konfigurieren, fehlt derzeit völlig.

Provisioning und virtuelle Appliances

Der letzte Tab unter "Virtual Infrastructure" heißt "Elastic Valet" und dient dem Bereitstellen (Provisioning) von virtuellen Maschinen. ECP bietet vorgefertigte Pakete, aus denen virtuelle Maschinen erzeugt werden können. Mit Hilfe dieser Pakete erlaubt Elastic Valet ein einfaches Einrichten selbst mehrerer VMs in einem Schritt. Der Administrator wählt einfach das Paket, aus dem die VMs erzeugt werden sollen (etwa Centos), gibt an, auf welchem Cluster diese laufen sollen und deren Anzahl. Elastic Valet sorgt anschließend dafür, dass die virtuellen Maschinen auf den richtigen Systemen in der Cloud erzeugt werden. Über den Fortschritt der Bereitstellung kann sich der Benutzer durch das Dashboard informieren.

Neben "Virtual Infrastructure" bietet der nächste Tab "Repository" die Verwaltung eben dieser Pakete an. Grundgedanke ist, virtuelle Maschinen als Appliances zu behandeln, die als Pakete vorliegen und aus diesen VMs für die Cloud zu erzeugen. Im Prinzip ist das eine Fortführung der bekannten Packages aus den Repositories einer normalen Linux-Distribution. Entsprechend bietet ECP die Möglichkeit, neue Appliance-Pakete aus im Internet zugänglichen, externen Quellen zu laden und dem eigenen, lokalen Repository hinzuzufügen – eben ganz ähnlich, wie ein laufendes Linux aus Paketen Software installiert und Updates bezieht.

Unter Repository findet der Anwender zwei Tabs namens "Local Appliances" und "Remote Appliances" – beide bieten Listen von den verfügbaren Appliances, einmal im lokalen Repository und einmal für die konfigurierten externen Quellen. Zur Verfügung stehen Appliances für Cen-

Links

[1] Amazon Cloud Services
aws.amazon.com/ec2/

[2] Installationsanleitung für ECP
www.howtoforge.com/kvm-virtualization-with-enomalism-2-on-a-fedora-10-server -

tos-, Debian- und Fedora Linux-Distributionen sowie eine NetBSD-Appliance. Wem die angebotenen Appliances nicht ausreichen, kann mit dem Tab "VM Creator" einfach eigene Appliances anfertigen, indem man Namen und benötigten Plattenplatz angibt sowie eine Datei mit einem ISO-Image der Installations-CD. So lassen sich zum Beispiel Windows-VMs einrichten, zu denen Enomaly aus lizenzrechtlichen Gründen keine vorgefertigten Appliances anbieten kann.

Mit dem letzten Tab unter Repositories, "Manage Repositories", lassen sich externe Appliance-Quellen konfigurieren. Als Default stehen zwei Enomaly-Repositories zur Verfügung – eins bietet Appliances an, über das Zweite liefert Enomaly Updates und neue Zusatzmodule für ECP aus. Die beiden letzten Tabs des ECP-Interfaces bieten mit "Admin" die Möglichkeit, ECP selbst zu konfigurieren und mit "User/Groups" ein Benutzer- und Rechtemanagement für die ECP Anwender. Hervorzuheben ist, dass man Rechte zu Teilaufgaben, wie etwa das Provisioning, sehr feingranuliert vergeben kann.

Fazit

Enomalys ECP besticht durch seine Einfachheit, den logischen Aufbau und vor allem die übersichtliche Präsentation. Ein Administrator mit grundlegender Erfahrung zum Thema Virtualisierung unter Linux kommt auf Anhieb mit ECP zurecht. Mit Clustern lassen sich lokale und entfernte Server einfach in Pools verwalten und bieten eine übersichtliche Anbindung zukünftiger Services, wie etwa die eingangs erwähnte Amazon Elastic Cloud. ECP baut in den wichtigsten Funktionen auf Technologien aus dem Linux-Umfeld, wie etwa libvirt. Damit wird ECP zukünftig von deren Entwicklungen profitieren können – etwa die Unterstützung neuer Virtualisierungstechniken.

Die Verwaltung der virtuellen Maschinen als Appliance-Pakete samt Download aus dem Internet ist zusammen mit "Elastic Valet" zum Provisioning eine gelungene und einfache Lösung. Nachteilig ist die umständliche Installationsprozedur, die allerdings für den Betrieb irrelevant ist. Einige Systemskripte von ECP könnten noch etwas Entwicklung vertragen – wie etwa das erwähnte Netzwerksetup. Unbedingt integriert werden sollte ein SAN-Management. Netzwerk-Storage spielt schon heute eine große Rolle, die durch Virtualisierung und Cloud-Computing noch erheblich betont wird. Wer nach einer einfachen Möglichkeit sucht, seine Linux-basierte, virtuelle Infrastruktur zu verwalten, sollte einen Blick auf ECP werfen. *(jp)*

Produkt
Programm zum Management virtualisierter Infrastrukturen

Hersteller
Enomaly Inc.
http://www.enomaly.com

Preis
Kostenlos – Open Source

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

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

Oberfläche und Bedienung	10
Basiert auf relevanten Open Source-Projekten	8
Installationsprozedur	1
Netzwerkkonfiguration	3
Integration von SAN	3

Dieses Produkt eignet sich

optimal für den schnellen und intuitiven Einstieg in das Cloud-Management.

bedingt für komplexe Virtualisierungsinfrastrukturen aufgrund der sehr einfach gehaltenen Netzwerkkonfiguration.

nicht als Komplettlösung zum Management auf Grund des fehlenden SAN-Managements.

Elastic Computing Platform

Neuerungen in Exchange Server 2010

Messaging der nächsten Generation

von Walter Steinsdorfer

Der Exchange-Server ist in vielen Unternehmen das Arbeitstier, wenn es um den Kontakt zur Außenwelt geht. Mit Version 2010 hat Microsoft seinen Mailserver wieder auf Vordermann gebracht und einige interessante Features eingeführt. Diese machen das Arbeiten nicht nur komfortabler, sondern auch schneller. IT-Administrator zeigt, was Sie alles vom neuen Exchange-Server erwarten dürfen, aber auch welche Einschränkungen der Mailserver mit sich bringt.

In der neuen Version 2010 von Microsoft Exchange Server hat sich viel getan – obwohl seit dem Release der aktuellen Version gerade einmal zweieinhalb Jahre vergangen sind. Im Gegensatz zu Exchange Server 2007, wo zumindest zu Testzwecken eine 32-Bit-Variante zur Verfügung stand, ist die derzeit aktuelle Beta-Version nur als 64-Bit-Variante erhältlich. Das schränkt auch die möglichen Betriebssysteme ein, die Sie verwenden können. Generell lässt sich Exchange 2010 nur auf Windows Server 2008 installieren; eine Installation auf Windows Server 2003, auch in der 64-Bit-Variante, ist nicht möglich. Auch auf der momentan nur als Beta vorliegenden Version Windows Server 2008 R2 kann das Setup erfolgreich abgeschlossen werden, obwohl dieses Betriebssystem (noch) nicht offiziell unterstützt wird.

Da es sich bei Exchange 2010 noch um eine Beta-Version handelt, lässt sich diese nicht in eine vorhandene Exchange-Organisation beziehungsweise einen Active Directory (AD)-Forest mit Exchange installieren. Sie müssen also zumindest für die Vorabversion eine eigene Active Directory-Umgebung erstellen. Eine Migration innerhalb der vorhandenen Organisation wird erst mit der RTM-Version von Exchange Server 2010 zur Verfügung stehen, wobei der Umzug von Exchange 2003 und 2007 möglich ist. Eine direkte Migration von Exchange 2000 soll dagegen nicht funktionieren und die Exchange 2007-Server müssen hierfür über das aktuellste Service Pack verfügen.

Installation des neuen Mailservers

Bevor Sie mit dem Setup beginnen, müssen Sie noch sicherstellen, dass sich die PowerShell v2 CTP 3, WinRM CTP3 sowie das .NET-Framework 3.5 (am besten mit Service Pack 1) auf dem Rechner befinden. Probleme gibt es in den meisten Fällen, wenn IPv6 über die Netzwerkeinstellungen deaktiviert ist. Häufig lässt sich dann die installierte Hub-Transport-Rolle nicht starten oder das Setup verweigert die Installation der Rolle gänzlich. Um das Problem zu vermeiden, lassen Sie einfach den Haken gesetzt. Auch wenn IPv6 in Ihrem Netzwerk noch keine Rolle spielt, ergeben sich hieraus keine weiteren Schwierigkeiten. Lediglich ein gelbes Hinweisschild in der Anzeige neben der Uhr weist gegebenenfalls auf das fehlende IPv6-Netzwerk hin, allerdings kann das ohne Beachtung bleiben. Nach der Installation der genannten Pakete können Sie das Setup starten. Die Installation verläuft ähnlich wie bei Exchange 2007, große Unterschiede sind nicht auszumachen. Wie bei der Vorgängerversion führt Sie ein Assistent durch das Menü, wenn Sie das graphische Setup auswählen. Dabei lassen sich bis auf "Edge" alle Rollen auf einem Server aufsetzen. Das gilt auch für die Installation eines Database Availability-Clusters. Bei der Auswahl "typische Installation" werden – wie schon bei Exchange 2007 – die Rollen Hub-Transport, Client Access und Mailbox installiert. Nach der Prüfung der Systemvoraussetzungen kopiert das Setup die Dateien und richtet die Dienste ein. Sollte es sich um den ersten Exchange Server in Ihrer Installation handeln, findet noch die Schemaerweiterung statt. Auch eine skriptgesteuerte Installation ist wie bei Exchange 2007 möglich. Sie unterscheidet sich ebenfalls kaum von ihren Vorgängern in der vorliegenden Beta-Version.

Verbindungen zu anderen Organisationen

Nach der Installation der Serverrollen werden Sie beim ersten Aufruf der Konsole kleinere Unterschiede ausmachen: So startet die Exchange-Managementkonsole und verbindet sich mit "On-Premesis". Das ist immer Ihre Exchange-Installation

in Ihrem AD-Forest. Hier finden Sie schon die erste grundlegende Änderung: Eine Verbindung zu anderen Exchange-Organisationen ist nun innerhalb der Konsole möglich. Über sogenannte "Federated Trusts" lassen sich Verbindungen zu anderen Exchange-Organisationen herstellen. Ein Austausch von Frei/Gebucht-Zeiten oder auch ganzen Kalenderinhalten ist damit organisationsübergreifend ohne größere Umstände möglich. Mit Outlook Web Access oder mit Outlook 2007 können diese dann wie interne Kalender nebeneinander dargestellt werden.

Daneben haben Sie die Möglichkeit, einen Teil der Postfächer oder auch alle auf Microsoft-Servern zu hosten. Microsoft nennt diese Plattform "Business Productivity Online Standard Suite" (kurz BPOS), zu der praktischerweise gleich ein Migrationsassistent mitgeliefert wird. Über BPOS können neben Exchange auch Sharepoint oder Office Communication Server online zur Verfügung gestellt werden.

Ausbau der Performance

Bereits mit Exchange 2007 hat Microsoft in der Skalierbarkeit von Mailboxservern einen Sprung nach vorne gemacht. Durch die Möglichkeit, auf 64-Bit-Plattformen zu arbeiten, steht deutlich mehr Speicher als Cache zur Verfügung. Eine weitere erhebliche Verbesserung wird nun mit Exchange 2010 eingeführt: Bislang war es noch immer notwendig, möglichst schnell drehende Festplatten für die Exchange-Datenbanken und Transaktionsprotokolle zu verwenden. Denn um eine gute Leistung für die Datenbanken zu erzielen, benötigen transaktionsorientierte Datenbanken, zu denen neben Exchange übrigens auch SQL und das Active Directory zählen, möglichst viel Input- und Output-Operationen pro Sekunde (I/O). Doch für gewöhnlich liegen die angeforderten Daten in der Datenbank auf den unterschiedlichsten Bereichen der Festplatte verstreut. Mit Exchange 2010 ändert sich dieser Umstand nun und die Elemente werden möglichst "intelligent" so in der Datenbank verteilt, dass der Schreib-Lesekopf der Festplatte nicht mehr so viele Sprünge machen muss, um an die Daten zu kommen.

Eine schnelle SATA-Festplatte schafft etwa 300 I/Os, wenn die Daten hintereinander liegen, beim sogenannten "Random"-Zugriff oft nur um die 50 I/Os. Insofern kann sich die Datenrate allein durch die intelligente Anordnung der Datenbankdateien stark erhöhen. Eine weitere Änderung betrifft die zu lesenden Elemente: Sind aus einer Reihe von zehn Elementen zum Beispiel die Elemente 1, 3, 6, 7, 10 auszulesen, muss der Schreib-Lesekopf nicht zu jedem dieser Elemente neu positioniert werden. Der Server liest einfach alle Elemente von 1 bis 10 aus und verwirft die nicht benötigten Teile im RAM. Der Geschwindigkeitsvorteil fällt dabei so deutlich aus, dass sich auch für größere Umgebungen statt den schnellen SCSI- oder SAS-Festplatten die deutlich günstigeren SATA-Festplatten eignen. Die bisher immer nachts ablaufende Wartung, in der auch die Onlinedefragmentierung untergebracht ist, findet nun rund um die Uhr als Hintergrundtask mit niedriger Priorität statt.

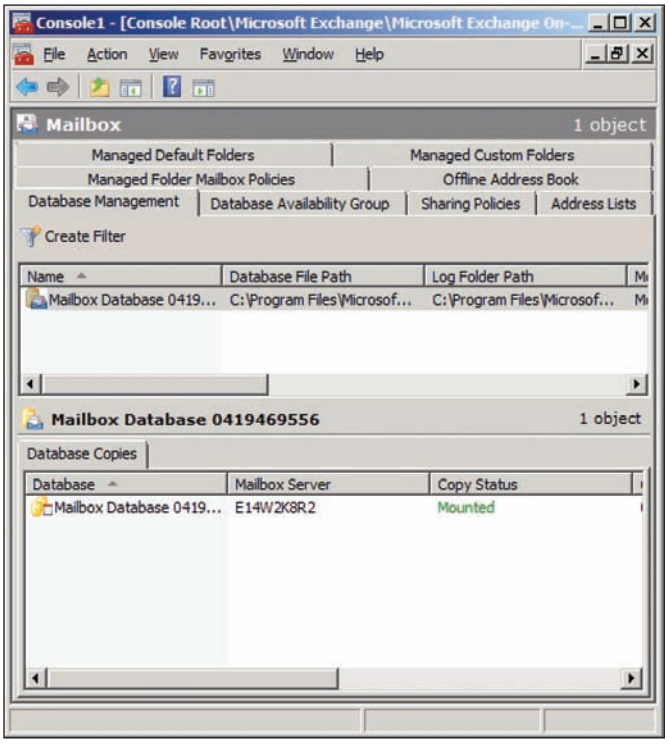


Bild 1: Bei Exchange 2010 sind Datenbanken nun Objekte der Exchange-Organisation

Hochverfügbarkeit komplett erneuert

Der Exchange Server 2010 bricht mit sämtlichen Hochverfügbarkeitsmethoden, die bis dahin unter Exchange bekannt waren. Es gibt ab Version 2010 nur noch die "Database Availability Group", kurz DAG. Also fallen Local Continuous Replication, Standby Continuous Replication, Clustered Continuous Replication und auch das Single Copy Cluster weg. Microsoft wird ab Exchange 2010 so nur noch eine Form der Hochverfügbarkeit unterstützen.

Die DAG kann jeweils bis zu 16 Mailboxserver enthalten, also bis zu 16 Kopien der gespiegelten Datenbanken. Wie bei der Clustered Continuous Replication (CCR) erfolgt das Einspielen der Logfiles entweder verzögert oder sofort. Zudem lassen sich, im Gegensatz zu Exchange 2007, alle Rollen auf den geclusterten Mailboxservern installieren. Einen Wermutstropfen gibt es dennoch: Die DAG lässt sich nur auf der Windows Server 2008 Enterprise-Edition einrichten, da einige darin vorhandenen Ressourcen des Clusterdienstes genutzt werden. Im Gegensatz zu Exchange 2007 sparen Sie sich aber damit zumindest theoretisch zwei Server und können sich bereits mit zwei Mailboxservern eine kleine Hochverfügbarkeitslösung bauen. Der Nachteil dabei ist, dass zwar die Datenbank innerhalb von 30 Sekunden geschwenkt wird, aber die Clients davon eventuell nichts mitbekommen. Daten-

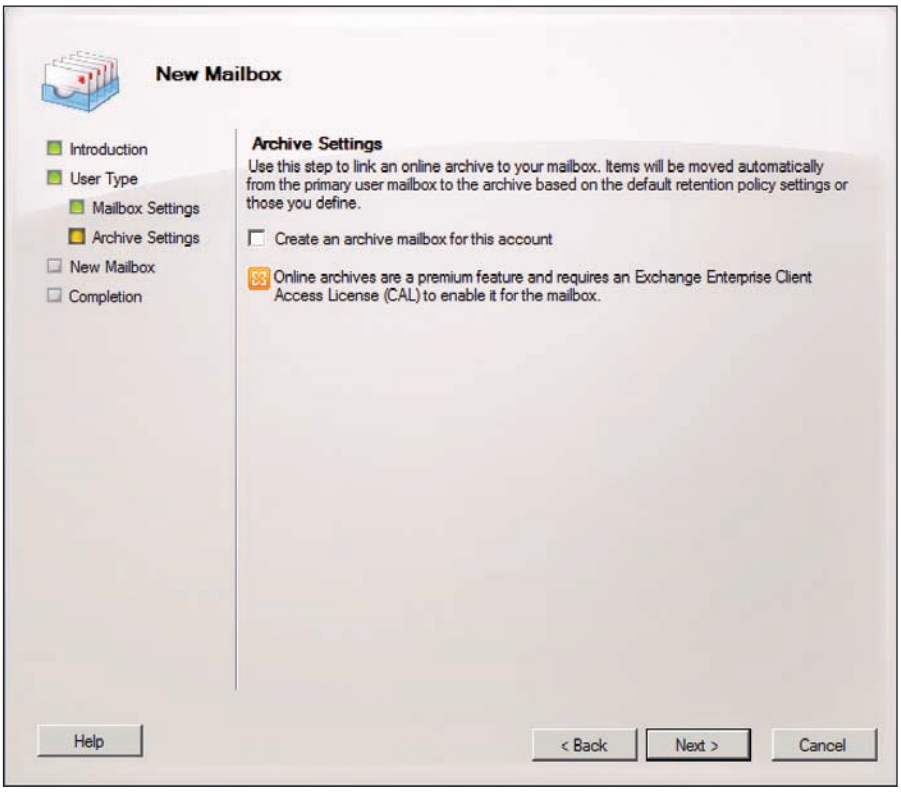


Bild 2: Die neuen Archivmailboxen lassen sich gezielt durchsuchen, um Compliance-Richtlinien zu entsprechen

banken fügen Sie in der grafischen Oberfläche oder wie gewohnt per PowerShell hinzu; die ausgewählte Datenbank wird dabei automatisch auf die Knoten in der DAG repliziert.

Ab Exchange Server 2010 werden übrigens alle Clients, auch die internen Outlook-Clients, über den CAS-Server mittels HTTPS angebunden. Nur die CAS-Serverrolle kommuniziert mit dem Mailboxserver noch über RPC beziehungsweise Mapi. Sollte nun einer der beiden Mailboxserver plötzlich ausfallen, werden die Clients nicht automatisch auf den zweiten Knoten umgeleitet. Auch bei einem Zwei-Knoten Cluster sollten Sie sich daher überlegen, einen Network-Loadbalancer vor den beiden CAS-Servern zu betreiben.

Keine Storage Groups mehr

Die Datenbanken sind übrigens kein Bestandteil einer Storage Group in Exchange 2010. Die Storage Groups hat Microsoft vielmehr entfernt und die Datenbank ist nun ein Objekt der Exchange-Organisation, innerhalb derer der Name der Datenbank eindeutig sein muss. Das spiegelt sich auch in der Konsole wieder, in der Sie das Datenbankmanagement unterhalb der Organisationskonfiguration finden. Dafür haben Datenbanken eine weitere Eigenschaft hinzubekommen: Sie können einstellen, über welche CAS-URL sich der Client mit der Datenbank verbinden soll. Das ist in größeren Umgebungen mit mehreren CAS-Servern oder Loadbalancern wichtig.

Mit Exchange 2010 führt Microsoft auch die Archivmailbox ein. In der RTM-Version wird diese Mailbox allerdings in der gleichen Datenbank liegen müssen wie die normale Mailbox des Anwenders. Immerhin hat der Hersteller damit ein Archiv geschaffen, das den Compliance-Anforderungen genügen dürfte. Das Archiv und auch die normalen Mailboxen sind nämlich von der besonderen Rolle des Compliance-Verantwortlichen nach Stichpunkten oder anderen Kriterien wie Absender oder Anhängen durchsuchbar. Als reines "Auslagerungstool", um die Datensicherungszeit in einem vertretbaren Rahmen zu halten, ist die Archivmailbox damit nicht geeignet.

Neben der Archivmailbox ist noch das Feature des Online-Mailboxumzuges hinzugekommen. E-Mailboxen können nun umgezogen werden, während der Anwender einfach weiterarbeitet. Nach Abschluss dieses Umzugs bekommt der Nutzer lediglich den Hinweis, dass er sein Outlook neu starten muss. Damit lassen sich nun auch große Migrationen über langsame WAN-Leitungen tagsüber anstatt in langen Nachtsitzungen erledigen. Leider ist dieses Feature nur bei Migrationen von Exchange 2010 Mailboxservern zu Exchange 2010 Mailboxservern verfügbar. Für die erste Migration von Exchange 2003 oder Exchange 2007 zu 2010 sollte der User also noch sein Outlook beenden.

Rights Management schützt Dokumente und E-Mails

Mit Exchange 2010 werden die Rights Management Services (RMS) in die Hub-Transport-Rolle integriert. Rights Management dient dazu, Office Dokumente über XML-basierte Zertifikate vor unberechtigten Zugriffen zu schützen und ihnen Teilrechte wie "nur lesen" einzuräumen. Weiterhin besteht die Möglichkeit, das Ausdrucken oder das Kopieren von Inhalten in RMS-geschützten Dokumenten zu verhindern. Der Rights Management-Dienst kann für Windows Server 2003 von Microsoft heruntergeladen und installiert werden, ab Windows Server 2008 ist er als Serverrolle installierbar. Als Client benötigen Sie mindestens Office 2003 Professional bzw. Office 2007 Professional Plus (mit Office Professional haben Sie nur Dokumentenleserechte). Als Client-Betriebssystem kommen XP, Windows Vista oder Windows 7 in Frage. Ab Windows Server 2008 ist das Rights Management in der Server CAL enthalten, bei 2003 war noch eine gesonderte Lizenz nötig. Dank der guten Integration des Rights Managements in die Hub-Transport Rolle können Sie E-

Mails zum Beispiel auch per Transportregel automatisch verschlüsseln. Damit bietet der Server eine gute Möglichkeit, die Vertraulichkeit zu wahren und zu verhindern, dass schützenswerte Dokumente versehentlich an den falschen Empfänger versendet werden.

Neues Rollenkonzept

Mit Exchange 2010 fällt es leichter, Teile der Administration zu delegieren und es sind auch mehr Rollen vorgesehen als in der Vorgängerversion. Die Exchange 2010-Installation erlaubt auf einfache Art und Weise die Vergabe von Berechtigungen an andere Benutzer. So ist es zum Beispiel möglich, über Outlook Web Access oder die Exchange Management Konsole Mitarbeitern außerhalb der IT Zugriff auf die Verwaltung von Verteilerlisten zu geben. Das Interface in Outlook Web Access ist relativ einfach aufgebaut, so dass kein großer Schulungsbedarf entstehen sollte. Auch das Anlegen von Benutzern oder die Verwaltung von Kontakten ist so umsetzbar. Die Verteilerlisten sind in der neuen Version auch moderierbar, also vor der Zustellung einer E-Mail an den kompletten Verteiler muss erst ein Moderator die E-Mail freigeben.

Ebenfalls angepasst hat Microsoft die Adresslisten, die sich nun hierarchisch aufbauen lassen. Damit können Sie für einzelne Firmenteile oder für getrennte Firmen in Exchange relativ leicht Trennungen vornehmen. Infolgedessen stellt Microsoft die Weiterentwicklung des "Hosted Messaging and Collaboration" (HMC) für Exchange ein. Dieses Tool für Hostingumgebungen, in denen auf einer Exchange-Plattform mehrere Firmen nebeneinander Platz fanden, wird nun wegfallen und Exchange 2010 soll alles mitbringen, um gehostete Umgebungen out-of-the-box zu installieren. Auch die PowerShell, die in Version 2 installiert werden muss, bietet Remotezugriff auf Exchange Server. Bei der Version, die Windows Server 2008 R2 in der Softwareliste zur Auswahl anbietet, handelt es sich übrigens noch um Version 1. Für kleinere Verwaltungsaufgaben und Shell-Liebhaber reicht es in Zukunft aus, die PowerShell zu installieren, um die Exchange 2010-Organisation zu verwalten.

Neues in Outlook Web Access

Auch im Webinterface von Exchange 2010 hat sich einiges getan: Die Oberfläche wurde komplett erneuert, der neue "Conversation View" für alle, die auf vielen Mailinglisten oder Verteilern stehen, wurde integriert. Diese neuen Ansicht – die auch auf Windows Mobile Devices ab der Version 6.0 installierbar ist, sobald Sie sich das erste Mal mit dem Exchange 2010 verbinden – unterstützt eine deutlich leichtere Abarbeitung von Diskussionen. Sollten Nutzer an einer Diskussion nicht mehr teilnehmen wollen, lässt sich diese auch einfach ausblenden. Nicht zuletzt können nun auch mehrere Kalender nebeneinander angezeigt werden.

Die Oberfläche wirkt deutlich moderner und bietet den direkten Zugriff auf ein Web-Administrationstool. Mit dem lassen sich bequem Benutzer oder Verteilerlisten verwalten, ohne eine Konsole zu öffnen. Des Weiteren besteht die Möglichkeit, über Outlook Web Access nun auch SMS-Nachrichten zu verschicken, sofern ein Active Sync-fähiges Handy mit dem Postfach verbunden ist. Als weiteres, durchaus bemerkenswertes Feature sind in Outlook Web Access die Favoriten hinzugekommen. Diese erleichtern die Arbeit, wenn Sie viele Ordner und Unterordner in Ihrer Inbox besitzen. Schließlich lassen sich die Archivmailbox und das Verwaltungsinterface direkt aus OWA heraus aufrufen.

Fazit

Neben den oben geschilderten Verbesserungen sind noch weitere hinzugekommen, wie zum Beispiel ein Dashboard für die SLA-Überwachung und Performance-Counter, das Einblenden mehrerer Organisationen parallel in der Konsole, die Mailtipps oder verbessertes Records Management. Alles in allem würde die ausführliche Schilderung der Neuerungen den Rahmen des Artikels sprengen, aber die aufgezeigten Neuerungen sind einen Blick wert. Es lohnt sich, ein wenig Zeit in die Installation der Beta-Version zu investieren. Wer viele Berechtigungen delegiert, eine schnelle Umschaltung bei Hochverfügbarkeit nutzen möchte oder E-Mail im Hostingbereich betreibt, wird um Exchange 2010 sicher nicht herumkommen. *(dr)*

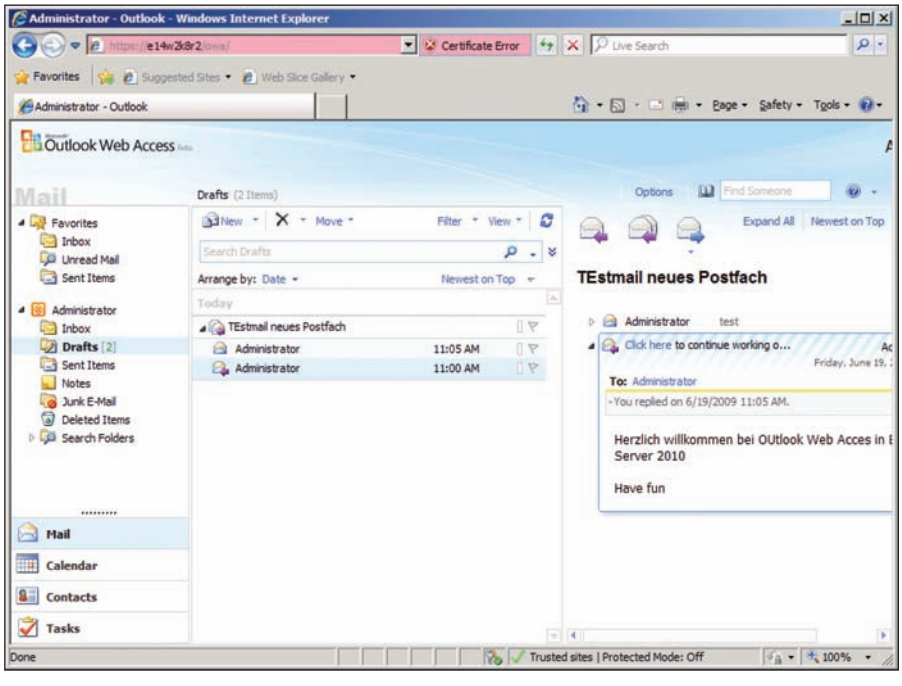


Bild 3: Die Weboberfläche ändert sich mit Exchange 2010 grundlegend und wirkt nun moderner

Hochverfügbarkeit mit Windows Server 2008 R2

Virtuelle Clusterfreuden

von Nail Own

Quelle: Scott Maxwell - Fotolia.com

Mit Hilfe von Cluster Shared Volumes lassen sich virtuelle Maschinen ohne Downtime verschieben

Mit Windows Server 2008 R2 erscheint in rund zwei Monaten die nächste Servergeneration von Microsoft. Das Betriebssystem hat unter anderem eine neue Hochverfügbarkeitsoption für das Windows Server Failover Clustering an Bord, welche erstmals mit der aus NT-Zeiten stammenden "Shared-Nothing"-Architektur bricht: Cluster Shared Volumes (CSV). Weitere Neuigkeiten wie SAN Fault Tolerance, Verbesserungen beim Validation Tool sowie bei der Verwaltung von Print Servern sollen die Administration des Servers noch einfacher gestalten. In diesem Artikel stellen wir Ihnen einige der neuen Features mit dem Schwerpunkt Hochverfügbarkeit vor.

Momentan befindet sich Windows Server 2008 R2 – bisweilen auch unter den Codenamen "Vienna" und "Windows 7 Server" bekannt – noch in der Beta-Phase und steht als Release Candidate unter [1] zum Download zur Verfügung. Ende Oktober soll das Server-Betriebssystem voraussichtlich zeitgleich mit Windows 7 auf den Markt kommen. Die Entwickler aus Redmond haben in der neuen Version besonders die Möglichkeiten des Windows Server Failover Clustering (WSFC), ehemals MSCS, stark ausgebaut.

Cluster Shared Volumes

Mit Hilfe von Cluster Shared Volumes (CSV) ist es möglich, gleichzeitige konkurrierende Lese- und Schreiboperationen auf einem Shared Volume auszuführen. Dies ist allerdings nur für die Rolle Hyper-V vorgesehen, und zwar um eine virtuelle Maschine (VM) im laufenden Betrieb von einem Hyper-V Host auf einen zweiten zu verschieben. Microsoft nennt dieses direkt mit CSV in Verbindung stehende Feature "Hyper-V Live Migration", das im Gegensatz zur nicht zu verwechselnden "Hyper-V Quick Migration" ohne Downtime auskommt.

Einsatzgebiet virtualisierte Umgebungen

Das Thema Virtualisierung in Rechenzentren ist schon seit einiger Zeit auf dem Vormarsch. Die Vorteile davon in Verbindung mit Microsoft Hyper-V-Clustering liegen klar auf der Hand: Zum einen ermöglicht es eine weitgehende Unabhängigkeit vom Betriebssystem. Außerdem müssen Applikationen in der VM nicht clusterfähig sein. Die OS-Unabhängigkeit erlaubt beispielsweise den Betrieb einer hochverfügbaren Windows XP-Installation. Die innerhalb der VM laufenden Applikationen benötigen keine Anpassung oder Sonderbehandlung für den Betrieb auf einem Hyper-V-Cluster, da die darunter liegende Architektur eines Hyper-V-Clusters völlig abstrahiert wird. Virtualisierte Lösungen erfahren zudem immer stärkeren Support: Selbst Anwendungen wie Microsoft SQL Server in der Version 2005 und 2008 sind seit kurzem vollständig für den Betrieb in einer Hyper-V VM vorgesehen [2,3].

Die Funktionsweise von CSV

Gleichzeitige Zugriffe mehrerer Hosts auf denselben Datenträger und somit das gleiche Dateisystem wurden bis dato nur von spezialisierten Cluster File-Systemen mit einem entsprechenden Distributed Lock Manager (DLM) und mehrstufigem, ausgefeiltem File Locking-Mechanismus unterstützt. Beispiele dafür sind das Oracle Cluster File System (OCFS2), RedHats Global File System (GFS2) oder VMWares Virtual Machine File System (VMFS). Allerdings benötigt ein Cluster File-System eigene Tools zur Verwaltung, Pflege und Wartung – zudem erfordert die Administration gesonderte Kenntnisse und geschultes Personal.

Ganz im Gegensatz dazu CSV: Unter der Haube arbeitet auf dem sogenannten "Coordinator Node" ein File System Kernel Filter-Treiber [4], um die Zugriffe per "Distributed File Access for Hyper-V" zu regeln. Der Coordinator unterscheidet bei Zugriffen zwischen Schreibvorgängen, die das Dateisystem beeinflussen – zum Beispiel bei Änderungen von Attributen – und

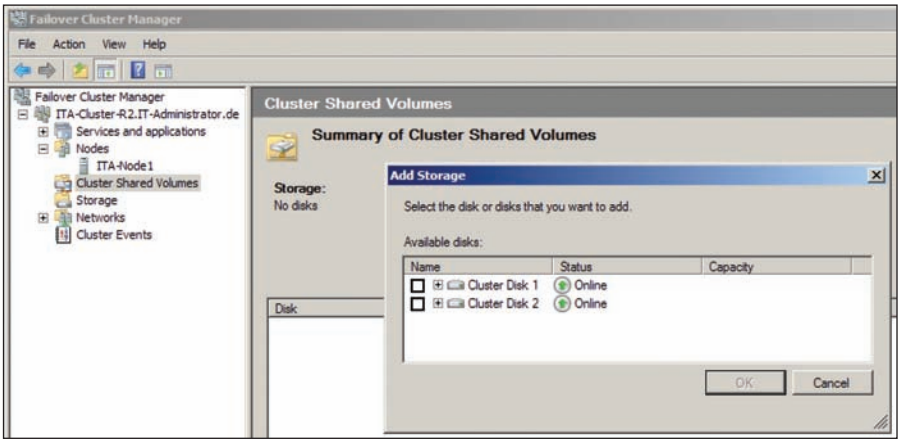


Bild 1: In der "Failover Cluster Management Console" aktivieren Sie die Cluster Shared Volumes (CSV). Danach können Sie Cluster-Datenträger hinzufügen.

Schreibvorgängen, die keiner Änderung der Struktur bedürfen. Ist Letzteres der Fall, sendet der Coordinator die Adresse der beschreibbaren Blöcke an den Node, der dann einen direkten Schreibvorgang via "Block-Level Access" durchführt.

Der Besitzer der Datenträger-Ressource verwaltet auf diese Art die Zugriffe auf eine CSV-Disk und wahrt die Konsistenz des Dateisystems, während alle Nodes im Cluster über folgenden Pfad darauf zugreifen: *{SystemDrive}\ClusterStorage*.

CSV läuft auf einem üblichen Windows NTFS-Dateisystem ohne proprietäre Software oder spezielles Datei-System. Die gängigen NTFS-Wartungs- und Disaster Recovery-Maßnahmen lassen sich weiterhin anwenden. Lediglich zur Anfertigung von Sicherungen der VMs mittels Volume Shadow Copy (VSS) ist ein neuer API-Aufruf namens "PrepareVolumeForSnapshotSet" nötig. Auch bei der Hardware gibt es keine besonderen Voraussetzungen, um CSV zu nutzen: Wie schon beim Hyper-V-Clustering mit Windows Server 2008 muss ein Shared Storage-Device vorhanden sein, das via iSCSI, Fibre Channel oder SAS an die Server angebunden ist und standardmäßig SCSI-3 Persistent Reservation (SCSI-3 PR) unterstützt. Abgesehen davon spielt lediglich die Prozessor-Architektur der Nodes eine Rolle: Sie darf beispielsweise innerhalb eines Clusters nicht von unterschiedlichen Herstellern sein. Empfehlenswert für eine möglichst schnelle Live-Migration ist eine gute Netzwerkanbindung der Nodes, im Idealfall GBit-Ethernet oder besser.

Betrieb von CSV

Dieser einheitliche Dateisystem-Pfad gilt für alle Nodes im Cluster und bietet einen "Single Name Space". Damit ist ein eigener Laufwerksbuchstabe nicht mehr nötig und stellt somit keinen limitierenden Faktor mehr für die Anzahl an VMs eines Hyper-V-Clusters dar. Der Failover einer VM führt außerdem nicht dazu, dass diese offline geht, ebenso bedingt der Failover einer VM nicht mehr einen Besitzerwechsel der Disk-Ressource. Ein Windows Client, der auf eine so eingerichtete Ressource zugreift, erfährt von einem Failover somit gar nichts: Offene Netzwerkverbindungen bleiben erhalten und es kommt zu keinem Abbruch bestehender TCP-Verbindungen oder -Sessions.

Live-Migration im Detail

Bei einem Failover eines Hyper-V-Gasts erstellt das Betriebssystem eine VM auf dem passiven Node und kopiert via Ethernet den gesamten Speicherinhalt des RAM vom aktiven auf den passiven Node. Änderungen am Inhalt des Speichers, die während dieses Vorgangs geschehen, werden im Anschluss daran inkrementell solange iterativ auf den passiven Node kopiert, bis ein konsistenter Zustand ohne Deltas des aktiven und passiven Nodes erreicht ist. Danach stoppt die ursprüngliche VM und die neu erstellte nimmt den Betrieb auf. Abschließend werden die Clients innerhalb des TCP-Timeouts auf die nun aktive VM geleitet und die ursprüngliche VM auf dem ursprünglichen Node gelöscht. Dieser Vorgang wirkt sich nicht auf Clients aus, die mit einer VM verbunden sind. Die Verfügbarkeit der VM und der Applikationen darin bleibt davon unberührt. Ein Failover ist bei Version R2 auf Basis einer einzelnen VM möglich: Der physikalische Datenträger ist nicht mehr wie bisher die kleinste verschiebbare Einheit. Dadurch ist es möglich, mehrere Virtual Hard Disks (VHD) als Repräsentanz einer VM auf dem gleichen Datenträger abzulegen und diese einzeln auf beliebige Nodes zu verteilen. Das spart letzten Endes auch Speicherplatz auf den LUNs und hilft dabei, Performance-Engpässe auszugleichen.

Einsatzszenarien für Cluster Shared Volumes

Die Installation einer speziellen Software, eines Treibers oder eines Agenten innerhalb einer VM ist nicht notwendig für die Funktionalität von CSV. Die Zugriffe auf einen virtuellen Datenträger laufen für den virtualisierten Gast völlig transparent ab. Dies stellt einen echten Vorteil gegenüber Lösungen anderer Hersteller dar, da CSV bei der Version 2008 R2 fester Bestandteil des Betriebssystems ist. Eine Einschränkung bringt Hyper-V Live-Migration jedoch mit sich: Es wird ein funktionierender Knoten vorausgesetzt. Eine Live-Migration beim Totalausfall eines aktiven Knotens ist nicht möglich. Somit ist zwar ein manueller Failover einer VM und die damit verbundene Live-Migration im regulären Betrieb oder während eines Wartungsfensters problemlos möglich. Ein Failover bei Ausfall des Nodes führt allerdings zu einer Quick Migration. Anwendungsfälle für eine Live-Migration sind daher beispielsweise:

- Hardwareerweiterung eines Nodes oder Tausch einiger Komponenten
- Microsoft Updates, die einen Reboot benötigen
- Verteilung von VMs auf weitere Nodes aus Lastgründen

Ein Two-Node-Cluster kann immer nur eine Live-Migration zur gleichen Zeit

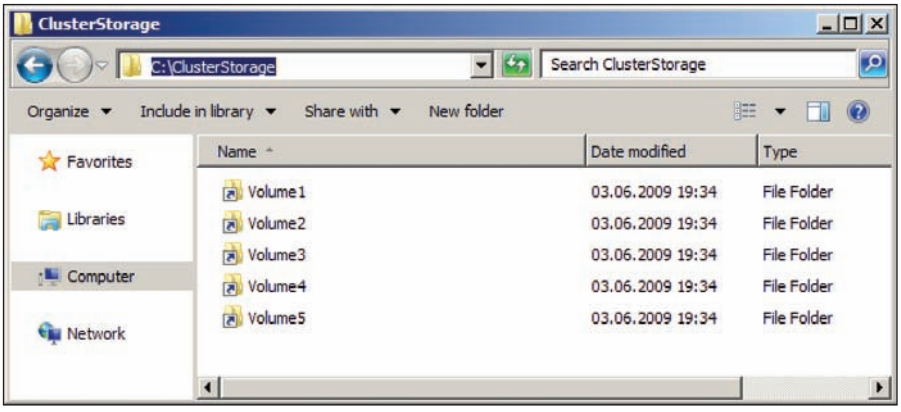


Bild 2: So stellt der Windows Explorer unter Windows Server 2008 R2 die Shared Volumes dar. Der Zugriff ist von allen Nodes aus über einen einheitlichen Dateipfad möglich.

ausführen. Die Anzahl der Live-Migrations entspricht der Anzahl der Nodes geteilt durch zwei: Bei einem 16 Node Cluster lassen sich acht Live-Migrations von Aktiv- zu Passiv-Node gleichzeitig durchführen.

Weitere R2 Cluster Features

CSV ist sicherlich eines der interessantesten Features beim Windows Server Failover Clustering mit der Version R2 des Windows Server 2008. Es gibt aber noch weitere Neuerungen, wie etwa SAN-Fault-Tolerance über dynamische I/O Redirection oder ein vereinfachtes Drucker-Management.

SAN-Fault-Tolerance

Falls auf dem aktiven Node die Pfade zum Storage nicht mehr erreichbar sind, kann der CSV I/O-Traffic über Server Message Blocks auf den Netzwerkverbindungen zu weiteren Nodes umgeleitet werden, welche noch gültige Pfade zum Storage aufrechterhalten. Dabei kommt es nicht zu einem Failover einer VM. Das verringert die Anzahl an Single Points of Failure hinsichtlich des SAN-Aufbaus: Den Ausfall einiger Fibre Channel-Komponenten kann der Cluster nun automatisch ausgleichen, bis die Teile in einem Wartungsfenster getauscht werden. Selbst der Storage-Pfad des Coordinator Node, der beim Hyper-V-Clustering mit CSV die Zugriffe auf den Storage regelt, lässt sich im Fehlerfall abfedern. Damit ist es erstmals möglich, anstehende I/Os über einen Public- oder Heartbeat-Netzwerkpfad auf eine SAN umzuleiten und das unabhängig von der Storage Architektur, sei es FC, SAS oder iSCSI.

Failover Cluster Validation

Microsoft hat mit Windows Server 2008 die Notwendigkeit abgeschafft, dass Cluster-Hardware in der Windows HCL (Windows 2000) oder dem Windows Catalog (Windows 2003) gelistet sein muss, um uneingeschränkten Support zu erhalten. Wie schon bei vorhergehenden Windows Cluster-Versionen spielen die Latenzzeiten der Netzwerkverbindung und der Storage-Komponenten eine wichtige Rolle. Darüber hinaus ist die Qualität der verwendeten Hardware und der eingesetzten Treiber maßgebend für einen stabilen Clusterbetrieb. Dazu hat Microsoft mit dem Validate Tool, einer Fortführung des Tools "Cluster-Prep", eine Möglichkeit in die Failover Cluster Management Console integriert. Damit kann ein Cluster-Administrator jederzeit am Server direkt prüfen, ob die Hardware und die Treiber wie vorgesehen zusammenarbeiten. Die Cluster-Validierung wurde in der Version R2 verbessert und prüft nun auch die eingerichtete Cluster-Konfiguration, die ein Administrator vorgenommen hat und gibt dazu Best Practise-Empfehlungen ab. Damit lässt sich über eine Archivierung der generierten Berichte eine Dokumentation der jeweils gesetzten Einstellungen vornehmen. Wer vor der Anschaffung der Cluster-Hardware sicherstellen will, dass eine Validierung der verwendeten Hardware problemlos durchläuft, greift auf das Failover Cluster Configuration Program (FCCP) zurück. FCCP-Hardware wird bereits vom Hersteller auf Windows Cluster Kompatibilität getestet, sprich validiert.

Printer Driver Isolation

Mit Version R2 von Windows Server 2008 wird sich bei Printservern einiges ändern,

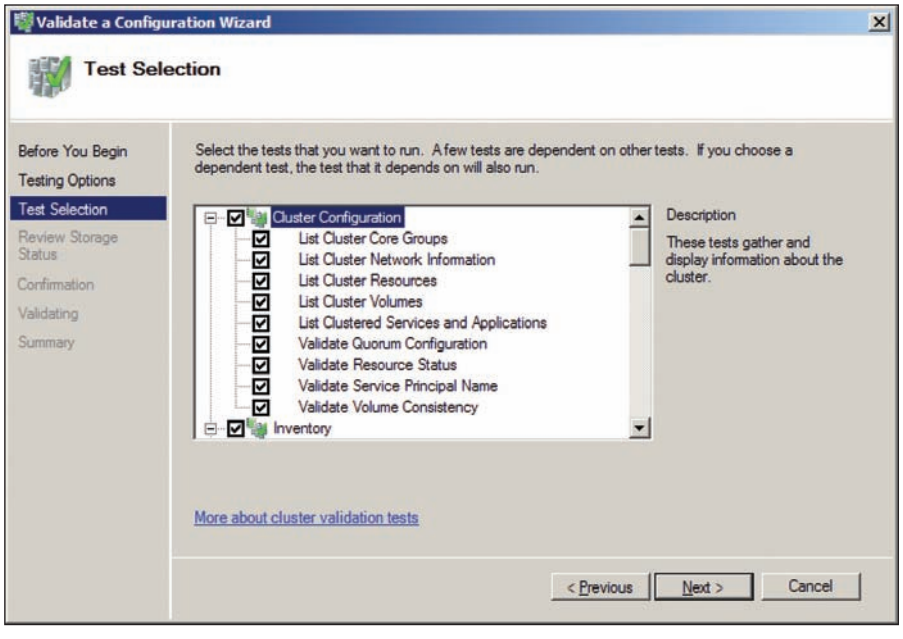


Bild 3: Das "Validation Tool" bietet in Version R2 neue Tests zur gesetzten Konfiguration eines Clusters an

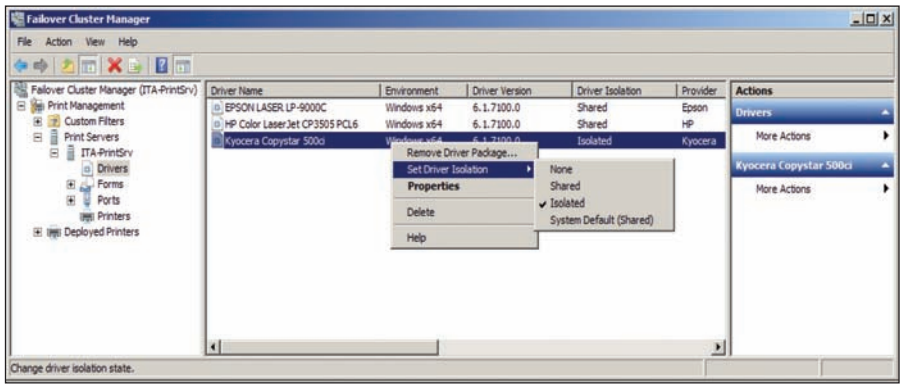


Bild 4: "Printer Driver Isolation" lässt sich für jeden installierten Druckertreiber über den Failover Cluster Manager auswählen

um die Stabilität der Spooler Komponente zu steigern und damit die Verfügbarkeit zu erhöhen. Ein Administrator hat die Möglichkeit, einzelne Druckertreiber zu isolieren und in eigenen Prozessen ausführen zu lassen. Damit führt ein fehlerhafter Druckertreiber nicht mehr zum Absturz des gesamten Spooler-Prozesses oder gar des Print-Servers. Driver Isolation erfordert dafür angepasste Treiber; alle mitgelieferten "Inbox"-Treiber für Windows 7 und Windows Server 2008 R2 unterstützen die Funktion bereits. Folgende Modi sind damit möglich und vom Systemverwalter konfigurierbar: "None", "Shared" und "Isolated". Im Shared-Modus teilen sich die Druckertreiber einen gemeinsamen Host Prozess außerhalb des Spoolers. Im Isolated-Modus läuft jeder entsprechend konfigurierte Druckertreiber in einem eigenen Host Prozess. Es ist ebenso möglich einen Treiber zu isolieren, der vom Hersteller in den Treiberdateien nicht eindeutig als kompatibel ausgewiesen wurde – das sollte ein Administrator aber vorab außerhalb des produktiven Betriebs testen. Das Feature ist zu 100 Prozent clusterfähig und wird auch als "Sandboxing Printer Drivers" bezeichnet.

Print Backup und Restore Manager (PrintBRM)

Eine weitere Neuerung, die das Verwalten von Druck-Servern betrifft, ist die Ablösung des Tools "Print Migrator" (PrintMig) zum Sichern, Wiederherstellen und Migrieren von Druckertreibern. PrintMig erhält einen Nachfolger für die Kommandozeile: "PrintBRM" (Print Backup/Restore Manager). Im Gegensatz zu PrintMig benötigt PrintBRM keinen separaten Download, es befindet sich seit Windows Vista unter dem Pfad *{systemroot}\System32\Spool\Tools*. Wie der Assistent, der sich über die GUI des Print Management Snap-Ins aufrufen lässt, sichert es die Treiber und die dazugehörigen Dateien sowie die Print Processors und die Language Monitors. Im Unterschied zum Print Migrator fällt das Tool auch unter 64-Bit Systemen unter einen uneingeschränkten Support.

Fazit

Die neuen Möglichkeiten von Server 2008 R2 in Bezug auf das Failover-Clustering sind eine logische Weiterführung der Features von Windows Server 2008. Microsoft hat an vielen Punkten Verbesserungen vorgenommen und neue Möglichkeiten implementiert. CSV stellt hier eine echte Innovation dar, die mit bewährten Methoden auf elegante Weise einen immensen Mehrwert bei der Virtualisierung bietet. Bleibt abzuwarten, wie sich die Kompatibilität und Stabilität der finalen RTM-Version im Zusammenspiel mit gängiger Applikations-Software und Server-Hardware in der Praxis erweist. In Verbindung mit den angebotenen Hochverfügbarkeitslösungen für den Enterprise-Bereich von Windows Server 2008 R2 könnte Microsoft ein großer Wurf gelingen, wie es sich auch bei der Clientversion Windows 7 abzeichnet. *(ln)*

Links

[1] Download des Release Candidate von Windows Server 2008 R2
www.microsoft.com/windowsserver2008/en/us/R2-Download.aspx

[2] Microsoft Support Policy für SQL Server 2005 und 2008
http://support.microsoft.com/kb/956893/en-us/

[3] Microsoft Support Policy für einzelne Produkte in Bezug auf Virtualisierung
http://support.microsoft.com/kb/957006/en-us/

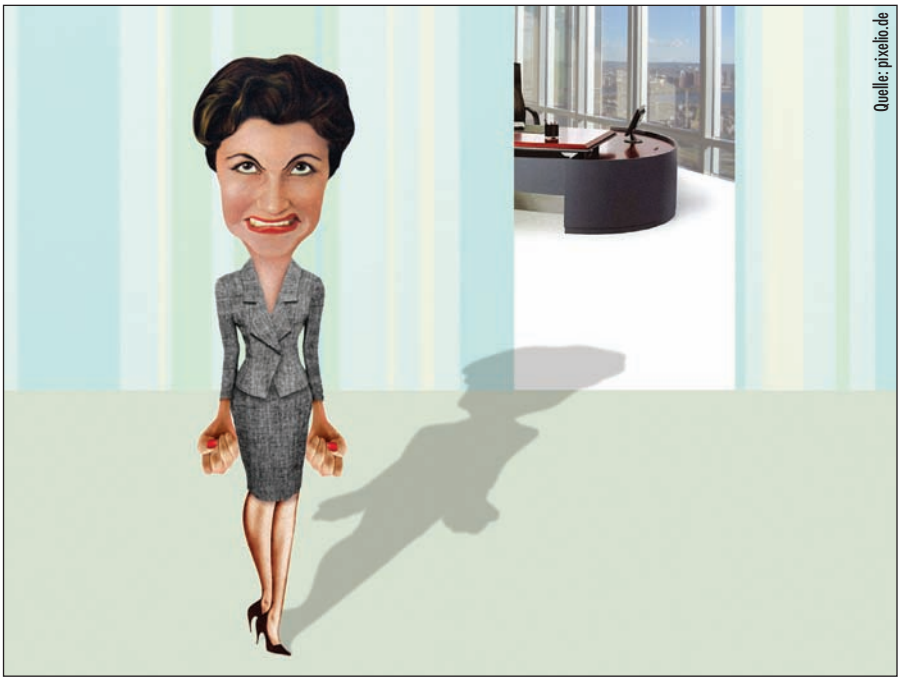
[4] Cluadmin.de – Filtertreiber im Cluster
www.cluadmin.de/filtertreiber-im-cluster-p88/

Active Directory-Replikation meistern (1)

Verteilte Ordnung

von Florian Frommherz und Nils Kaczenski

Active Directory ist das Rückgrat moderner Windows-Netzwerke. Meist versieht es klaglos seinen Dienst und toleriert einzelne Serverausfälle oder auch einen großen Netzwerk-Umbau. Hin und wieder jedoch steht der Administrator vor Problemen mit dem Datenabgleich – der Replikation der gemeinsamen Datenbank. Unser Workshop beleuchtet Hintergründe, Technik und Praxis der komplexen AD-Replikation.



Frau Ellen Bogen hat kürzlich geheiratet und nun zusätzlich den Namen ihres Mannes angenommen – alle wissen Bescheid, nur das Active Directory nicht

Das Active Directory (AD) basiert auf dem Lightweight Directory Access Protocol (LDAP), das den Zugriff auf große Objektmengen, die sich in Unternehmen meist als hierarchische Struktur darstellen, bereitstellt. Schon der Grundentwurf des "NT Directory Service", wie der Dienst zunächst Microsoft-intern hieß, hatte ehrgeizige Ziele: Er sollte die zentrale Anmeldung (Single Sign-on) an allen Servern und Workstations ermöglichen, gleichzeitig aber mit älteren Clients kompatibel bleiben. Mechanismen zur Lastverteilung und Ausfallsicherheit sowie die Integration von Anwendungsdaten betonten die Eignung für große Unternehmen. Den Administratoren sollten Funktionen wie ein zentrales Client-Management bei gleichzeitig dezentraler Verwaltbarkeit zugutekommen. Und schließlich band Redmond seine detaillierte Berechtigungssteuerung in den Dienst ein, der schon bei den Dateidiensten Maßstäbe gesetzt hatte.

Den technischen Kern des AD bildet ein ausgefeiltes Replikationssystem, das den Anwendern ermöglicht, die logische Domänenstruktur unabhängig von der Netzwerktopologie zu betreiben. Das AD beruht auf einer selbsterzeugenden Multi-Master-Replikation: Alle Domänencontroller (DC) einer Domäne haben denselben lesenden und schreibenden Zugriff auf die Verzeichnisdatenbank. Fällt ein DC aus oder fügt der Administrator einen hinzu, so berechnet AD selbst die günstigste neue Replikationsstruktur, um alle DCs mit den aktuellen Daten zu versorgen. Auf diese Weise ist der Dienst skalierbar von kleinen Umgebungen bis zu weltweiten Konzernnetzen.

In einer solch verteilten Datenbank können jedoch viele Konflikte bestehen, wenn Änderungen nicht zusammenpassen, die Administratoren verschiedener Standorte vornehmen – daher umfasst AD Behandlungsroutinen für typische Administrationsfehler. Legen zwei entfernt voneinander arbeitende Administratoren etwa neue Benutzerobjekte mit denselben Namen an, so benennt AD automatisch eins der Konten um und vermeidet so die Kollision. Ähnlich geht es in anderen Fällen vor – siehe dazu den Kasten "Konflikte vermeiden".

DNS als Rückgrat des AD

Eine funktionierende Namensauflösung ist die wichtigste Voraussetzung für Active Directory – und gleichzeitig die häufigste Fehlerquelle. Seit Windows 2000 versucht ein Windows-Computer stets, Namen zunächst über DNS aufzulösen. Scheitert dies, so versucht er andere Methoden wie die NetBIOS-Namensauflösung und WINS.

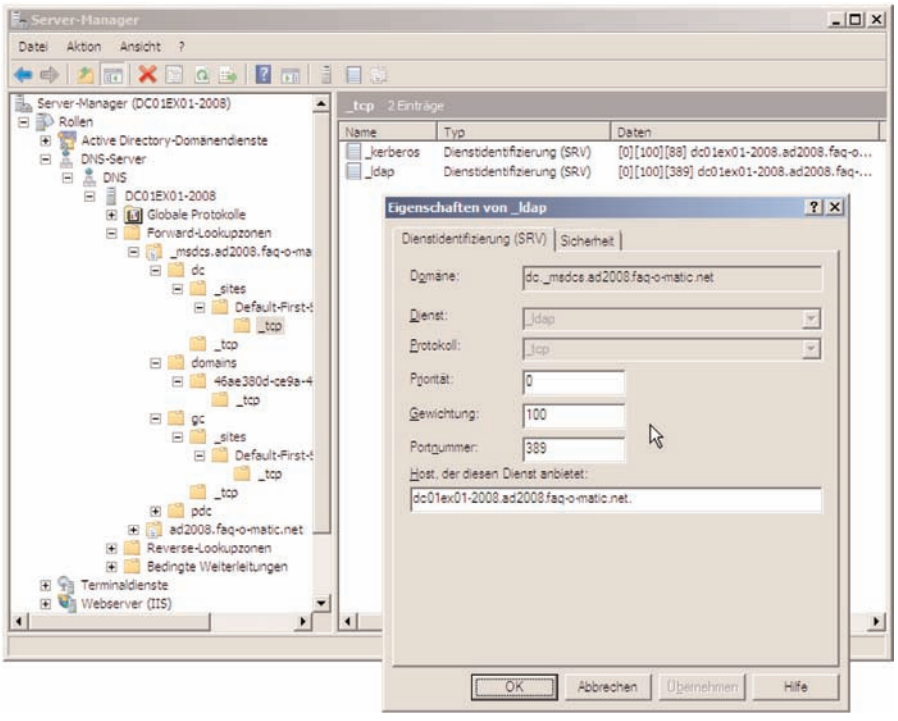


Bild 1: Zentral gepflegt: Active Directory legt zahlreiche Einträge im DNS an, über die Clients die zugehörigen Dienste finden

Jede AD-Domäne benötigt einen internen DNS-Namen und die dazugehörige Datenbank ("Zone") auf einem DNS-Server. Meist empfiehlt es sich, den DNS-Server auf allen Domänencontrollern zu betreiben und die Zone auf "Active Directory-integriert" zu schalten, sodass ihre Daten direkt im AD liegen. Auf diese Weise unterliegt auch DNS der Multi-Master-Replikation, wodurch alle Clients auf die aktuellen Daten zugreifen können. Die Clients (und Mitgliedsserver) sollten jeweils zwei der DNS-Server in ihrer IP-Konfiguration zugewiesen bekommen, für PCs am besten per DHCP. Dann tragen sie sich selbst in die DNS-Datenbank ein und können die Namen aller anderen Netzwerkteilnehmer nachschlagen. Achtung: Ein PC, der Mitglied einer Domäne ist, sollte niemals einen externen DNS-Server eingetragen bekommen, also etwa den Server des Providers. Sonst würde er diesen erfolglos nach der Domäne fragen und so Fehler verursachen. Sollen Clients DNS-Namen im Internet auflösen können, so definiert man im internen DNS-Server eine Weiterleitung ("Forwarder") auf einen externen Server.

Für die Domänencontroller selbst empfiehlt sich in den meisten Netzwerken eine "kreuzweise" Konfiguration: Jeder DC, der auch DNS-Server ist, erhält in seiner IP-Konfiguration als primären DNS-Server einen anderen DC und erst als sekundären Eintrag einen Verweis auf sich selbst. So lässt sich einer möglichen "Inselbildung" vorbeugen, in der ein DC nur seine eigenen Daten kennt und aus der Replikation herausfällt. Zudem vermeidet dies Timeout-Probleme beim Neustart eines DC, denn DNS startet normalerweise erst nach den AD-Diensten, was sonst zu Wartezeit und Fehlermeldungen führt. Die nötigen Einträge zu den einzelnen AD-Diensten nehmen die DCs selbst im DNS vor. Klappt dies einmal nicht, so hilft meist der Neustart der Anmeldedienste über folgende Befehlssequenz:

```
ipconfig /registerdns &&
  net stop netlogon && net start
  netlogon
```

Aufbau der Replikationstopologie

Um seine mächtige Replikationstechnik auszunutzen, teilt das AD seine Datenbank in mehrere Partitionen ein, so genannte "Namenskontexte" (Naming Context, NC). Der bekannteste ist der Domänen-Namenskontext, in dem sich alle produktiven Objekte der jeweiligen Domäne befinden. Diese Partition repliziert sich vollständig zwischen allen DCs derselben Domäne.

Separate Replikationstopologien baut AD für seine Konfigurationspartition und für das Schema auf. Im "Configuration NC" speichert das AD Informationen zur Replikation und auch Applikationen können sich hier eintragen, so etwa Exchange. Die Konfigurationspartition replizieren alle DCs des gesamten AD-Forest, denn sie ist domänenüber-

Konflikte vermeiden

Active Directory kann viele Replikationskonflikte erkennen und beheben. Die wichtigsten Mechanismen:

- Objektnamenskonflikt: Erzeugen zwei Admins an verschiedenen Servern etwa zur selben Zeit mehrere Objekte mit demselben Namen, so benennt AD das "jüngere" Objekt um. Dazu hängt es an den Namen die Zeichenfolge "CNF:" (für Conflict) sowie die intern eindeutige Kennung (Globally Unique Identifier, GUID) an. Es empfiehlt sich, in großen Umgebungen regelmäßig nach solchen Namen zu suchen und die Objekte manuell zu bearbeiten. Hierfür können Sie in der benutzerdefinierten Suche der AD-MMC den Suchstring "(name=*CNF*)" nutzen.
- Attributwertkonflikt: Ändert ein Administrator den Nachnamen eines Benutzerobjekts auf "Müller" und gleichzeitig ein anderer denselben Namen auf "Meyer", so übernimmt AD die zeitlich letzte Änderung. Der andere Wert wird kommentarlos überschrieben. Erst Windows Server 2008 bietet dafür eine Protokollfunktion auf Attributebene, die aber zunächst aktiviert werden muss. Dazu definieren Sie in der Default Domain Controllers Policy zunächst allgemein die Überwachung für den Verzeichnisdienstzugriff. Danach schalten Sie über die Kommandozeile die Werteverfolgung ein:
  `auditpol /set /subcategory:"directory service changes" /success:enable`
- Verwaister-Container-Konflikt: Legen Sie in der OU "Vertrieb" ein neues Objekt an, während ein Kollege gerade die OU "Vertrieb" löscht, so verschiebt AD das neue Objekt bei der nächsten Replikation in den Container "LostAndFound" (standardmäßig ausgeblendet). Ein so "verwaister" Benutzer kann sich also anmelden, befindet sich aber nicht im richtigen Verwaltungsbereich der Domäne.

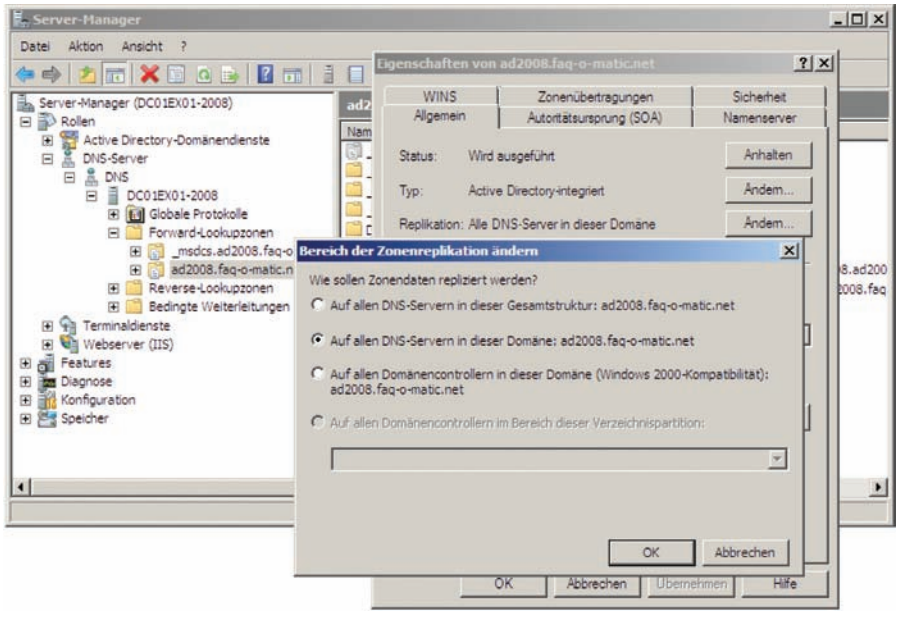


Bild 2: Für Applikationspartitionen des AD (hier die DNS-Partition) kann der Administrator den Replikationsbereich selbst festlegen

greifend gültig. Gleiches gilt für das Schema, also die Datenbankdefinition, die festlegt, wie Objekte und Attribute beschaffen sind. Mit "ADSI Edit" können Sie sich diese speziellen Partitionen einmal ansehen. In Windows Server 2008 ist das Programm bereits enthalten, auf früheren Versionen installieren Sie es aus den Support Tools nach. Führen Sie auf dem obersten Knoten einen Rechtsklick aus und wählen Sie "Verbinden". Das Programm fragt Sie dann nach dem Namenskontext, den Sie unter "Bekannten Namenskontext auswählen" aus der Liste auswählen.

In Windows Server 2003 hat Microsoft einen weiteren Partitionstyp eingeführt: Applikations-Namenskontexte. So ist es dem AD möglich, Daten bestimmter Anwendungen separat von den "technischen" AD-Daten zu replizieren. Von Haus aus liegen DNS-Daten in solch einer Partition, doch Administratoren können auch eigene "Application Partitions" erzeugen. Die Replikation der DNS-Partition können Sie über das GUI festlegen. Rufen Sie dazu im DNS-Snap-In per Rechtsklick die Eigenschaften der DNS-Zone auf. Unter "Allgemein" nutzen Sie dann den Button "Ändern" für die Replikation, um die Einstellung zu bearbeiten. Für andere Applikationspartitionen müssen Sie, falls die jeweilige Applikation kein Verwaltungstool hat, das Werkzeug *NTDSUtil* nutzen. Näheres dazu finden Sie bei Bedarf in Microsofts TechNet [1].

Um die Replikationstopologie zu erzeugen, benötigt das AD Informationen zum Aufbau des Netzwerks. Diese holt es sich nicht selbst, sondern der Administrator muss einige Rahmendaten zur Verfügung stellen. Entscheidend sind dabei die LAN-Standorte, aus denen das Netz besteht, und die Qualität der WAN-Verbindungen dazwischen: Netzwerke mit "schnellen" Verbindungen betrachtet AD als "Standorte" (Sites). Als weitere Anforderung kommen eindeutige IP-Subnetze hinzu: Ein IP-Netzwerkbereich (etwa 192.168.1.0/24) muss vollständig zu einem Standort gehören; Adressen dieses Bereichs dürfen an anderen Standorten nicht vorkommen. Umgekehrt kann eine Site aber durchaus mehrere IP-Subnets beherbergen.

Die Leitungsgeschwindigkeit zwischen Standorten geben Sie nicht etwa in Bits pro Sekunde an, sondern nur relativ zueinander als abstrakten "Kostenwert". Dieser ist numerisch; als Standard gibt AD den Wert 100 vor. Eine langsame Verbindung bekommt hohe Kosten (beispielsweise 200 oder 1.000), eine schnelle dementsprechend niedrige. Gibt es nun mehrere mögliche Verbindungen zwischen zwei Standorten, so wählt AD die mit den geringsten Kosten. Sollte diese nicht verfügbar sein, nimmt AD den Weg mit den nächst höheren Kosten – ähnlich einer Routing-Tabelle (näheres hierzu beleuchten wir im zweiten Teil des Workshops).

Verteilung von Änderungen im AD

Die Replikation der Änderungen verwirklicht Active Directory über Benachrichtigungen, sogenannte "Change Notifications", die die direkten Replikationspartner erhalten. Direkte Replikationspartner sind hierbei andere Domänencontroller, die sich in der Site des Quelldomänencontrollers befinden. Welcher DC direkt mit welchem anderen repliziert, bestimmt ein Active Directory-interner Dienst, der Knowledge Consistency Checker (KCC), über den Aufbau der Replikationstopologie.

Der Quell-Domänencontroller sendet nach Ablauf einer kurzen Wartezeit seine Change Notification an seine direkten Replikationspartner. Die Wartezeit ist wichtig, um nicht bei jeder Änderung eine separate Benachrichtigung senden zu müssen, sondern im Falle mehrerer Änderungen in einem kurzen Zeitintervall eine Benachrichtigung für alle Änderungen versenden zu können. Die Wartezeit beträgt für Windows Server 2003 und Server 2008 15 Sekunden, während Windows 2000 ganze fünf Minuten wartet. Für darauffolgende Änderungen wird die Wartezeit verkürzt – hier werden lediglich drei Sekunden in Windows Server ab 2003 oder 30 Sekunden in Windows 2000 gewartet. Benachrichtigte DCs können daraufhin Änderungen an den NCs über den Quell-Domänencontroller abfragen.

Deshalb ist bei der AD-Replikation auch von einer "Pull"-basierten Replikation die Rede. Änderungen an den Namenskontexten werden nicht per "Push" an die Replikationspartner gesendet, sondern vom Quelldomänencontroller zur Verfügung gestellt.

Steuerung der Replikation

Das Sicherstellen der Replikation und das effiziente Verteilen von Neuigkeiten ist Aufgabe des KCC. Der KCC läuft als Dienst in einem Intervall von 15 Minuten auf allen Domänencontrollern und prüft die Konfiguration in "Active Directory-Standorte und Dienste" und der darin hinterlegten Parameter, um daraufhin eine Replikationstopologie für alle verfügbaren Domänencontroller zu erstellen. Aus dieser Replikationstopologie ist zu entnehmen, welcher Domänencontroller Aktualisierungen von welchen anderen Domänencontrollern empfangen kann.

Der KCC versucht stets, einen bidirektionalen Ring von Domänencontrollern zu erstellen, in dem sich Ringnachbarn über Änderungen informieren und die Replikation initiieren. Eine Replikationstopologie wird pro Namenskontext erstellt. In großen Gesamtstrukturen mit mehreren Domänen bedeutet dies, dass für die Domänenpartitionen und die forestweiten Partitionen getrennte Replikationspläne erstellt werden müssen. In übersichtlicheren Gesamtstrukturen mit nur einer Domäne kann es sich der KCC leicht machen: da alle Domänencontroller dieselben NCs besitzen, genügt eine Topologie für alle Namenskontexte.

Um der Replikationsdaten Herr zu werden und die von anderen Domänencontrollern empfangenen Aktualisierungen der Namenskontexte einpflegen und prüfen zu können, bedarf es eines Mechanismus, Änderungen anhand ihrer Reihenfolge sortieren zu können. Schließlich soll es nicht passieren, dass DC1 die aktuellen Änderungen von DC2 repliziert und DC3 später einen älteren Stand der Objektdaten nach DC1 repliziert und die Neuerungen überschreibt, weil DC3 selbst noch nicht die neuesten Änderungen von DC2 empfangen hat.

Verteilte Systeme begegnen diesem Problem auf unterschiedliche Arten. Für Active Directory böte sich an, einen Änderungszeitstempel als Kriterium zu verwenden – schließlich ist die Zeit auf allen Domänencontrollern und Clientcomputern der Domäne nahezu gleich, was eine zwingende Voraussetzung für das Authentifizieren mit Kerberos ist. Da Active Directory aber unter Umständen aus mehreren hundert verschiedenen Knoten in unterschiedlichen Standorten mit variierenden Latenzen bestehen kann, reichen "nahezu" synchrone Uhren nicht aus.

Beispiele für den High Watermark Vector von DC-1

Namenskontext	Replikationspartner	HWMV
Domänen-NC	DC-2	766474
Domänen-NC	DC-3	222934
Configuration-NC	DC-2	723222
Configuration-NC	DC-3	179682
Schema-NC	DC-2	758860
Schema-NC	DC-3	215320

Beispiele für den High Watermark Vector von DC-2

Namenskontext	Replikationspartner	HWMV
Domänen-NC	DC-1	866548
Domänen-NC	DC-3	222934
Configuration-NC	DC-1	823296
Configuration-NC	DC-3	179682
Schema-NC	DC-1	758860
Schema-NC	DC-3	858934

USN und HWMV steuern die Replikation

Das AD verwendet deshalb mehrere Vektoren, die bei Änderungen erhöht werden und bei der Replikation zwischen den beiden Partnern ausgewertet werden. Sie speichern dabei die Datenbankstände anderer Domänencontroller. Einer dieser Vektoren ist die "Update Sequence Number" (USN). Jeder DC hat eine eigene USN, die bei jeder durchgeführten Datenbank-Transaktion automatisch erhöht wird. Eine Objekterstellung wird ebenso als eine Transaktion gewertet wie das Ändern eines einzelnen Benutzerattributes, etwa des Nachnamens oder der "Beschreibung". Dabei wird die USN sowohl mit den in der Transaktion geänderten Attributen gespeichert als auch im Attribut "highestCommitedUSN" des Verzeichnisdienstkopfes (rootDSE) hinterlegt.

Um zu wissen, welchen Datenstand ein Domänencontroller bereits von einem anderen repliziert hat, merkt sich jeder DC die USN der Namenskontexte seiner Replikationspartner. So können

DCs, die Änderungen von ihren Partnern anfragen, den letzten Stand (USN) des Namenskontextes, den sie per Replikation mit diesem Partner erhalten haben, mit in der Anfrage senden. Partner können auf diese Weise nur die Änderungen vorbereiten und replizieren, die seit der letzten erfolgreichen Replikation vorgenommen wurden. Die USN-Stände der letzten Replikation werden im so genannten "High-Watermark Vector" (HWMV) gespeichert.

UTDV verhindert Endlosschleifen

Zu guter Letzt wird ein weiterer Vektor benötigt, der "Up-To-Dateness"-Vektor (UTDV), der dem HWMV ähnelt. Dieser Vektor speichert allerdings nicht nur die USNs der aktuellen direkten Replikationspartner. Für den Up-To-Dateness-Vektor werden alle letzten USNs jeglicher Partner gespeichert, von denen ein Domänencontroller jemals einen so genannten "Originate Change" repliziert hat – dies schützt vor Endlosschleifen bei der Verteilung von Aktualisierungen.

Die Replikation unterscheidet zwischen zwei eingehenden replizierten Änderungen: "Originate Change" bezeichnet Änderungen, die auf einem direkten Partner vorgenommen wurden und direkt von diesem Partner übernommen wurden. "Replicated Changes" sind hingegen Änderungen, die ein entfernter DC vorgenommen hat und die mit Hilfe eines direkten Replikationspartners, der die Änderungen bereits empfangen hat, repliziert wurden. Der direkte Replikationspartner hat die Änderung also nicht selbst erstellt, sondern ist nur "Mittelsmann" bei der Änderungspropagierung.

Die High-Watermark-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	HWMV
DC-1 – HWMV (USN: 2555)	Domänen-NC	DC-2	2299
	Domänen-NC	DC-3	1467
DC-2 – HWMV (USN: 2299)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2555
	Domänen-NC	DC-3	1467
DC-3 – HWMV (USN: 1467)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2555
	Domänen-NC	DC-2	2299

Die Up-To-Dateness-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	UTDV
DC-1 – UTDV (USN: 2555)	Domänen-NC	DC-2	2299
	Domänen-NC	DC-3	1460
	Domänen-NC	DC-4	765
DC-2 – UDTV (USN: 2299)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2555
	Domänen-NC	DC-3	1467
	Domänen-NC	DC-4	765
DC-3 – UTDV (USN: 1467)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2534
	Domänen-NC	DC-2	2299
	Domänen-NC	DC-4	765

Zusammenspiel der Vektoren

Wie die Vektoren zusammenspielen und welche Bedeutung sie bei der Replikation haben, wird durch ein Beispiel deutlich. Im nachfolgenden Szenario wurde ein Forest mit einer Domäne erstellt. Die Domäne hat drei Domänencontroller, DC-1, DC-2 und DC-3. DC-4, ein Test-Domänencontroller, wurde vor einiger Zeit wieder zum Mitgliedsserver heruntergestuft. Die Tabellen zeigen die HWMV und UDTV der aktiven Domänencontroller. Da der UTDV die USNs aller direkten Replikationspartner speichert, damit auch derer, die in der Zwischenzeit nicht mehr verfügbar sind, wird DC-4 ebenfalls im Vektor aufgeführt.

In unserem Beispiel wird ein Attribut eines Benutzerobjektes verändert. Frau Ellen Bogen aus der Personalabeilung hat kürzlich geheiratet und nun zusätzlich den Namen ihres Mannes angenommen. Um die Namensänderung auch korrekt im AD hinterlegen zu können, öffnet ein Administrator "Active Directory-Benutzer und Computer" und verbindet sich daraufhin – automatisch – mit DC-1. Dort trägt er den neuen Namen ein: sie heißt jetzt Frau Ellen Bogen-Schmerz. Die Änderung an Ellens Benutzerkonto hat eine Erhöhung der USN auf DC-1 zur Folge, und zwar von 2555 auf 2556. DC-1 informiert daraufhin seine beiden Replikationspartner, DC-2 und DC-3, dass Änderungen am Domänen-NC vorgenommen wurden. DC-2 erhält die Change Notification und prüft den eigenen HWMV. Als Antwort auf die Change Notification sendet DC-2, ne-

ben anderen Parametern, wie etwa die maximal erlaubte Objektzahl für die Replikation oder den betreffenden Namenskontext, seinen kompletten UTDV und HWMV an DC-1. Aus dem HWMV von DC-2 kann DC-1 erkennen, dass die Namensänderung der Benutzerin Ellen noch nicht bei DC-2 eingetroffen ist und repliziert diese daraufhin. Als Anhang an die Replikationsdaten sendet DC-1 seine neue USN mit, sodass DC-2 nun die Replikationsdaten mit Ellens neuem Nachnamen, die USN von DC-1 und seine eigene USN inkrementieren kann. Die Änderungen speichert DC-2 in seiner HWMV und UTDV, da DC-1 ein direkter Replikationspartner ist und die Replikation ein Originating Update war.

Nun fordert DC-3 die Änderungen von DC-1 an – schließlich hat auch dieser DC die Change Notification erhalten. Auch hier wird die Replikation vorgenommen und die entsprechenden Vektoren angepasst – es resultieren die geänderten HWMV- und UTDV-Werte.

Der DC-3 hat nach der Replikation alle Änderungen von DC-1 übernommen. Auch DC-3 hat seine USN erhöht (1468) und informiert nun DC-2 über die Änderungen an seinem Domänen-NC, da er nicht weiß, dass DC-2 bereits Änderungen direkt von DC-1 repliziert hat. Wie aus der HWMV-Übersicht rechts hervorgeht, kennt DC-2 alle Änderungen von DC-3 bis zur USN 1467. DC-3 hat allerdings durch das "Originating Update" von DC-1 und Ellens Nachnamen seine USN inkrementiert (1468). Dies würde bedeuten, dass die Namensänderung erneut repliziert wird. Da DC-2 aber nun seine komplette UTDV-Tabelle an DC-3 sendet, kann DC-3 erkennen, dass DC-2 zwar eine veraltete USN von ihm besitzt, in seinem UTDV für DC-1 aber die neueste Änderung von DC-1 (2556) bereits ebenfalls per Originating update repliziert hat. DC-3 muss also nichts weiter tun, als DC-2 seine neue USN (1468) schicken, damit DC-2 sie in seiner HWMV-Tabelle speichern kann.

Aus dem Beispiel lässt sich erkennen, warum es eine HWMV-Vektortabelle und eine Up-To-Dateness-Vektortabelle gibt. Während der HWMV die aktuellen Aktualisierungsstände der direkten Replikationsnachbarn speichert, schützt der UTDV vor Replikationsschleifen.

Problemerkennung

Sobald Sie einen Server zum Domänencontroller heraufstufen, versuchen die KCCs der anderen DCs eine Replikationstopologie zu erstellen und das neue Mitglied einzubinden. So einfach sich die Replikation von allein regelt, so schleichend können Probleme auftreten. Oft bemerken Sie Probleme mit der Replikation erst, wenn Benutzer anrufen und sich beschweren, dass ihr frisch geändertes Passwort plötzlich nicht mehr funktioniert und sie das alte Passwort verwenden mussten – oder dass das Adressbuch in Outlook veraltete Daten anzeigt. In beiden Fällen kann eine gestörte Replikation das schuldige Übel sein, denn wenn Änderungen nicht repliziert werden können, könnten Benutzer mit veralteten Daten konfrontiert werden.

Die geänderten High-Watermark-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	HWMV
DC-1 – HWMV (USN: 2556)	Domänen-NC	DC-2	2300
	Domänen-NC	DC-3	1468
DC-2 – HWMV (USN: 2300)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-3	1467
DC-3 – HWMV (USN: 1468)	Namenskontext	Replikationspartner	HWMV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-2	2299

Die geänderten Up-To-Dateness-Vektortabellen der Domänencontroller

	Namenskontext	Replikationspartner	UTDV
DC-1 – UTDV (USN: 2556)	Domänen-NC	DC-2	2299
	Domänen-NC	DC-3	1460
	Domänen-NC	DC-4	765
DC-2 – UDTV (USN: 2300)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-3	1467
	Domänen-NC	DC-4	765
DC-3 – UTDV (USN: 1468)	Namenskontext	Replikationspartner	UTDV
	Domänen-NC	DC-1	2556
	Domänen-NC	DC-2	2299
	Domänen-NC	DC-4	765

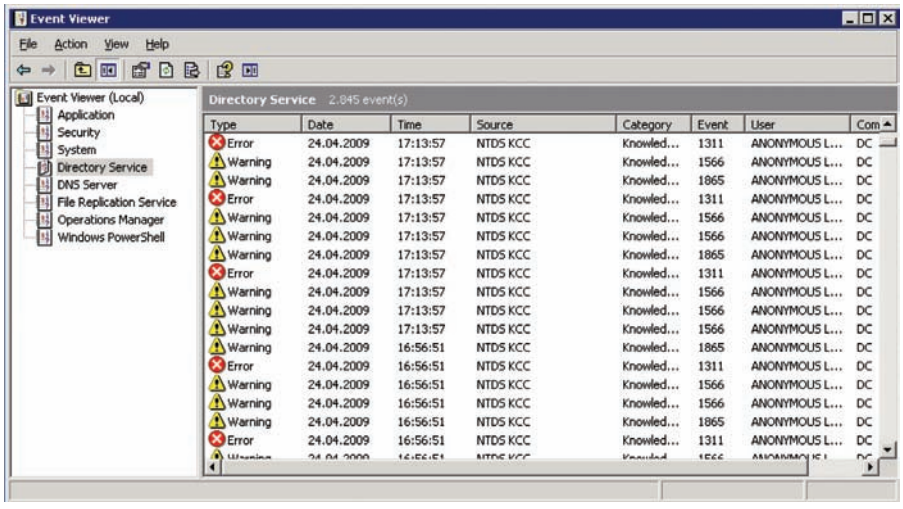


Bild 3: Die Ereignisanzeige informiert über auftretende Probleme bei der Replikation

Leider heulen im AD keine Sirenen auf, wenn mit der Replikation etwas nicht in Ordnung ist oder wird der Administrator automatisch mit einer E-Mail informiert, wenn der Datenabgleich scheitert. Zwei einfache Methoden gibt es allerdings, die Replikation zu überprüfen und sich ein Bild zu machen, ob das verteilte System rund läuft. Eine Methode basiert auf der Ereignisanzeige von Windows. Beim Heraufstufen zu einem Domänencontroller erstellt der Assistent ein neues Ereignislog namens "Verzeichnisdienst". Hier protokolliert AD alle Ereignisse. Gibt es Probleme mit der Replikation, lässt sich dies anhand dieses Ereignislogs erkennen – der KCC meldet etwa alle 15 Minuten, wenn es Schwierigkeiten mit der Erstellung der Replikationstopologie geben sollte.

Das Eventlog wird im Fehlerfall also regelrecht vollgeschrieben. Ist es allerdings ruhig um die Verzeichnisdiensteinträge, ist davon auszugehen, dass auch die Replikation erfolgreich funktioniert. Wer keine Serververwaltungssoftware wie beispielsweise System Center Operations Manager einsetzt, die Eventeinträge sammelt und die Gesundheit der Server überwacht, kann sich mit Visual-Basic- oder Powershell-Skripting oder mit bereits fertigen Tools wie EventComb [2] Ereignisse aus der Ereignisanzeige sammeln und automatisiert zustellen lassen. EventComb ist ein Programm aus dem Windows Server 2003 Resource Kit, das Ereignisanzeigen vorgegebener Computer nach Ereignissen durchsuchen kann. Gefiltert nach den Ereignis-IDs 1311, 1566 und 1865, lassen sich so zumindest die häufigsten

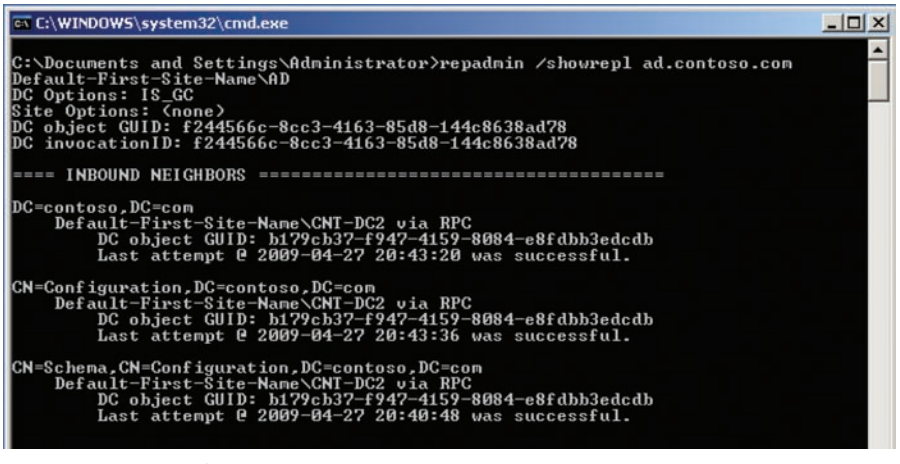


Bild 4: Repadmin zeigt für jeden Namenskontext den Status der letzten Replikation mit allen Replikationspartnern an

Replikationsprobleme sammeln. Vorsicht aber: Das Tool ist nur für recht kleine Umgebungen geeignet, in großen gerät es schnell durcheinander.

Ein zweites, wertvolles Kommandozeilenprogramm ist "repadmin" aus den Support Tools. Repadmin erlaubt es, den Status der letzten Replikation aller Namenskontexte abzufragen. Dabei zeigt es – abhängig vom DC, mit dem das Tool verbunden ist – pro Namenskontext an, mit welchen Domänencontrollern die Replikation versucht wurde und wann die letzte erfolgreiche Replikation stattgefunden hat. Aufgerufen mit dem Befehl Parameter "/showrepl" zeigt repadmin den Replikationsstatus an.

Fazit und Ausblick

In diesem ersten Teil des Workshops haben wir uns um die notwendigen Grundlagen und eine Menge Theorie gekümmert, die zum Verständnis der "Verteiltheit" von Active Directory beitragen. Wir haben uns die Replikation angesehen und erfahren, wie wir die Replikation überwachen können. Im zweiten Teil des Workshops werden wir über Standortgrenzen hinauswachsen und die Replikation über mehrere Standorte hinweg kennenlernen und ihre Konfiguration durchleuchten. *(jp)*

Florian Frommherz ist MVP für Gruppenrichtlinien und Systemingenieur bei der Controltech Engineering AG in Liestal in der Schweiz. Nils Kaczenski ist MVP für Directory Services und Consulting-Leiter der WITcom by Wahl + Co. in Hannover.

Links

[1] Verwalten von Anwendungsverzeichnispartitionen
http://technet.microsoft.com/de-de/library/cc755918.aspx

[2] EventComb – Windows Server 2003 Resource Kit Tools
www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&d

Virtual Desktop Infrastructure mit VMware View einrichten (2/3)

Welche VM hätten's denn gern?

von Andreas Badur und Dr. Jürgen Fechter

Virtualisierung bietet Unternehmen zahlreiche Vorteile und ist daher schon seit längerem ein Trend. In unserer dreiteiligen Workshopserie zeigen wir Ihnen, wie Sie die Virtual Desktop Infrastructure mit VMware View einrichten. In diesem Teil erfahren Sie, wie Sie das VMware View Portal nutzen und den View-Client ausrollen.

Um auf die Virtual Desktop Infrastructure zuzugreifen, steht unter Windows der native View Client zur Verfügung. Ansonsten können Nutzer das View Portal verwenden. Dieses unterstützt jedoch kein ThinPrint und keine USB-Redirection. Die Linux-Voraussetzungen hierfür sind ein Java-fähiger Browser, der die Java Runtime Engine 1.5 oder 1.6 verwendet, sowie das Programm "rdesktop", Version 1.5 oder höher, im Suchpfad. Die aktuelle Version von Remote Desktop finden Sie unter [1]. Selbstverständlich können Sie auch unter Windows auf das View Portal zugreifen. Hierfür muss der Browser ActiveX-Steuerelemente unterstützen und zulassen. Sollte auf der Maschine noch kein View Client vorhanden sein, wird dieser automatisch beim ersten Zugriff auf das Portal installiert. Dabei stehen ebenfalls keine USB-Redirection und Einträge im Startmenü zur Verfügung. Zudem benötigen Sie den Remote Desktop Client in der Version 6.1. Diesen finden Sie unter [2].

Unter Windows sollten Sie für den problemlosen Zugriff immer die native Installation des View Clients samt aller Optionen verwenden. VMware stellt hierfür zwei Installationsprogramme zur Verfügung: *VMware-ViewClient-{xxx}.exe* und *VMware-ViewClientwithoffline-{xxx}.exe*. Letzteres enthält die Erweiterungen, die Sie für die Offline Desktop-Funktionalität benötigen. Dadurch lässt sich der Client nur auf physikalischen Maschinen installieren, sofern dort kein VMware ACE, VMware Player, VMware Server oder VMware Workstation vorhanden ist. Für beide Varianten wird der Remote Desktop Client in Version 6.1 empfohlen. Die Installation selbst ist sehr einfach: Führen Sie die gewünschte Datei aus, akzeptieren Sie die Lizenzbedingungen und wählen Sie die Optionen und den Pfad aus. Optional können Sie hier schon einen VCS hinterlegen, das ist aber keine Pflicht.

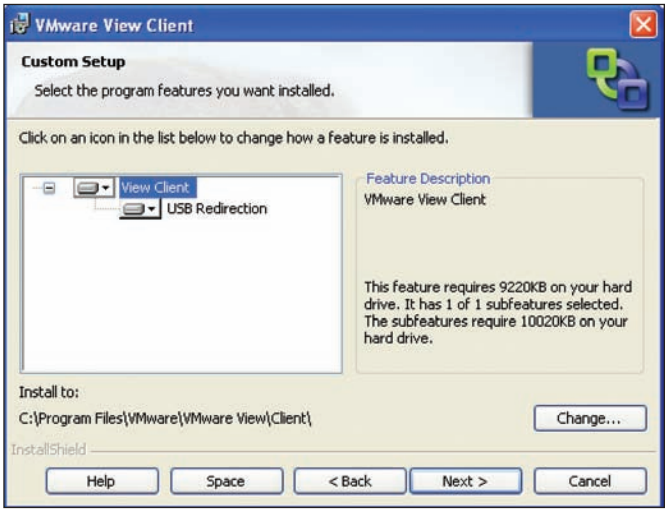


Bild 1: Die Installation des View Clients verläuft mithilfe eines Setup-Wizards

Vorbereitung eines Templates

Damit VMware View seine vollen Stärken der automatischen Pools ausspielen kann, benötigt es Templates. Dabei handelt es sich um ganz normale ESX-Templates, auf denen zusätzlich der View Agent installiert wurde. Mit den folgenden Schritten legen Sie ein Template an:

- Installieren Sie eine VM mit einem der unterstützten Betriebssysteme, etwa Windows XP Professional SP 3
- Konfigurieren Sie die Maschine entsprechend Ihren Anforderungen
- Installieren Sie im Anschluss die aktuellsten VMware-Tools
- Installieren und konfigurieren Sie alle gewünschten Applikationen, zum Beispiel den Client Ihrer CRM-Lösung, Office, alternative Browser et cetera.
- Installieren Sie den VMView Agent, idealerweise mit allen Optionen
- Entfernen Sie alle Snapshots, die auf dieser Maschine sind
- Konvertieren oder klonen Sie nun diese Maschine in ein Template. Klonen empfiehlt sich, wenn die Maschine weiterhin als Vorlage für neue Templates dienen soll. Durch diesen Vorgang wird auf der Maschine ein Sysprep durchgeführt und alle spezifischen Informationen wie die SID entfernt.

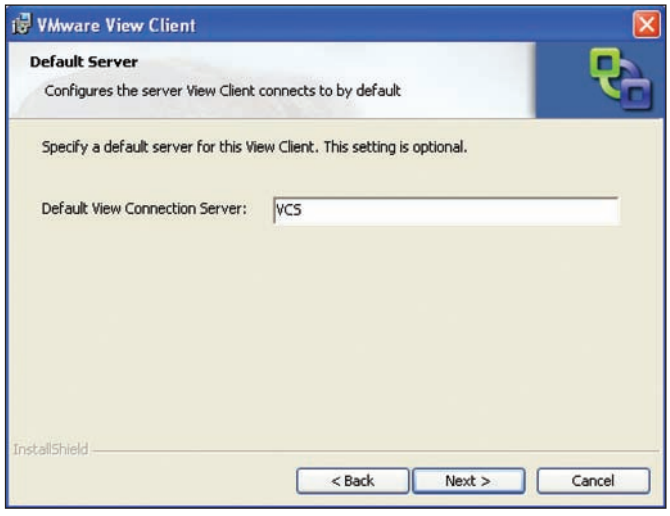


Bild 2: Beim ersten Start des View Clients können Sie einen Standardserver angeben

Grundsätzlich sollten Sie auch die Microsoft-Patches [3] installieren, um reibungslose RDP-Verbindungen zu ermöglichen.

Automatische Desktop Pools erstellen

Ein automatischer Desktop Pool enthält eine oder mehrere Maschinen, die durch den VCS automatisch aus einem Template erstellt und konfiguriert werden. Die Pools gibt es in zwei Varianten: persistent und non-persistent. Beim persistenten Desktop Pool erhält ein Benutzer immer dieselbe bisher benutzte Maschine zugewiesen. Alle persönlichen Einstellungen und Dokumente bleiben erhalten. Im Gegensatz dazu wird bei nicht-persistenten Desktop Pools der Benutzer auf einer beliebigen Maschine angemeldet. Um persönliche Einstellungen und Dokumente hier zu erhalten, müssen Sie Active Directory-Techniken wie servergespeicherte Profile oder Ordnerumleitung einsetzen.

Das Erstellen selbst ist einfach und wird durch einen Assistenten unterstützt. Klicken Sie im VCS Administrator auf "Desktop and Pools" und danach auf "Add". Wählen Sie nun den gewünschten Pooltyp aus, in diesem Fall "Automated Desktop Pool" und anschließend, ob Sie einen persistenten oder nicht-persistenten Desktop erstellen wollen. Klicken Sie danach den VCS an, der für die Erstellung und Verwaltung der VM zuständig sein soll. Auch wenn Sie nur einen in ihrer Umgebung haben, müssen Sie diesen auswählen. Im nächsten Schritt vergeben Sie eine eindeutige Pool-ID, eine Bezeichnung für den View Client und eine Beschreibung. Die Beschreibung darf maximal 1.024 Zeichen lang sein und ist nur innerhalb des View Administrators sichtbar.

Auf der nächsten Seite stellen Sie das Verhalten des Pools ein: Stellen Sie den Status auf "enabled", ist der neue Pool sofort für alle berechtigten Benutzer verfügbar. Ergänzend können Sie festlegen, wie die einzelne VM reagieren soll, wenn niemand eingeloggt ist, sowie, ob getrennte Benutzer automatisch abgemeldet werden sollen. Unterbinden oder erlauben Sie nun den Benutzern, ihren virtuellen Desktop selbst zurückzusetzen, worunter VMware den Reboot der VM versteht. Wenn Sie vorher "non-persistent" ausgewählt haben, stehen hier zwei Optionen mehr zu Verfügung: "Power off and delete virtual machine after first use" und "Allow multiple sessions per user". Bei ersterer wird eine VM direkt nach dem Abmelden des Benutzers wieder gelöscht und bei letzterer darf der Benutzer mehrere VMs desselben Pools verwenden. Allerdings wird beim Löschen der VM das entsprechende Active Directory-Computerobjekt nicht aus dem Verzeichnisdienst entfernt.

Klicken Sie auf "Next" und Sie erhalten die Maske, wie in Bild 3 zu sehen. Der untere Teil erscheint erst, wenn Sie auf "Advanced Settings" geklickt haben. Die Felder bedeuten im Einzelnen:

- "Provisioning": Default ist "enabled"; dies bedeutet, dass der Pool sofort die entsprechende Anzahl Desktops erstellt, sobald Sie diesen Assistenten beendet haben
- "Number of Desktops": Legt die Anzahl der Desktops fest, die dieser Pool erstellen soll. Wenn Sie die Checkbox "Enable Advanced Number of Desktop Setttings" in den erweiterten Einstellungen aktivieren, ist dieses Feld deaktiviert

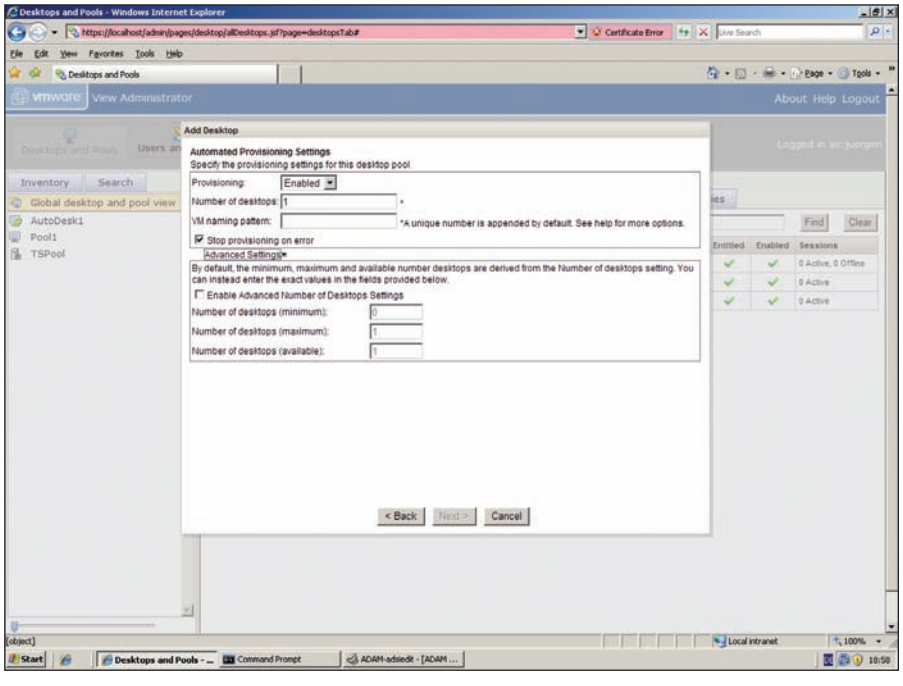


Bild 3: Das Automated Desktop Provisioning erlaubt ein Anlegen von vordefinierten Desktops

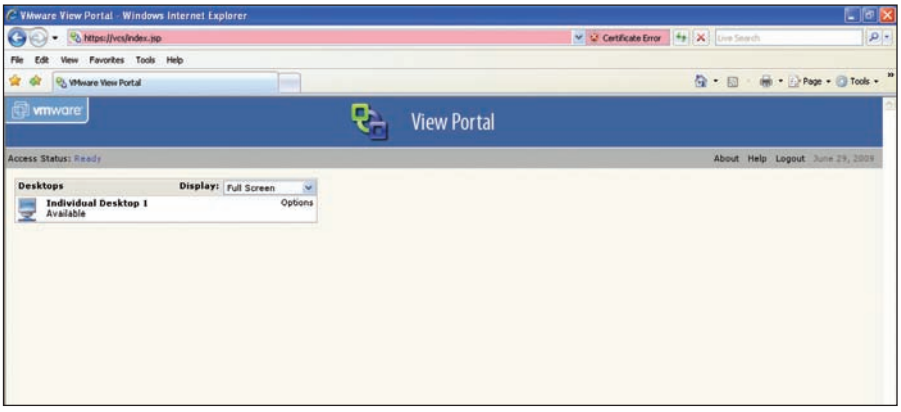


Bild 4: Die Auswahl von Desktop-Pools im View Portal

- "VM Naming Pattern": Hier hinterlegen Sie ein Schema für die Namen der VMs. Dieser Namen wird auch für den Hostnamen und das entsprechende Computerkonto übernommen. Lesen Sie dazu auch den Kasten "Namensmuster"
- "Stop provisioning on error": Mit dieser Option werden keine neuen Maschinen erzeugt, wenn Fehler beim Erstellen von VMs auftraten. Der Haken sollte immer gesetzt sein

Es empfiehlt sich, die "Advanced Settings" zu benutzen, da Sie hier das Verhalten des Pools und damit auch die Belastung der ESX(i)-Hosts feiner verwalten können. Dies geschieht über die drei Werte "Number of Desktops (minimum)", "Number of Desktops (maximum)" und "Number of Desktops (available)". Ersterer ist die Mindestanzahl an VMs, die dieser Pool beinhaltet. Analog dazu legen Sie mit dem zweiten Wert die maximale Anzahl VMs des Pools fest. Der letzte Wert ist der interessanteste: Hiermit legen Sie fest, wie viele nicht zugeordnete VMs den Benutzern jederzeit zur Verfügung stehen sollen. Wird dieser Wert unterschritten, werden sofort neue VMs erstellt.

Auf den nachfolgenden Seiten können Sie nun das gewünschte Template, einen Ablage-Ordner innerhalb des VCS und den Host oder Cluster, auf dem die Maschinen laufen sollen, festlegen. Es werden nur Cluster mit maximal acht Hosts unterstützt und angezeigt. Wählen Sie anschließend einen Ressource Pool aus, in dem die neuen VMs laufen sollen und definieren Sie die Datastores, in denen die VMs abgelegt werden. Für Cluster wird hier nur Shared Storage angezeigt. Danach können Sie noch wählen, ob Sie die Option "customization spezification" anwenden möchten. Sie können auch die neu erstellten Desktops nachträglich bearbeiten, indem Sie einerseits Einstellungen an den VMs selbst vornehmen oder diese beispielsweise manuell in die Domäne aufnehmen. Eleganter ist es natürlich, die "customizations" zu verwenden.

Bevor der Pool nun angelegt wird, erhalten Sie nochmals eine Übersicht aller vorgenommenen Einstellungen angezeigt. Kontrollieren Sie diese genau, denn wurde der Pool einmal erzeugt, können Sie Einstellungen wie Pooltyp oder Pool-ID nicht mehr ändern. Finden Sie dabei einen Fehler, können Sie jederzeit mit dem Knopf "Back" einige Schritte zurückgehen. Ist alles in Ordnung, klicken Sie auf "Finish" und der Pool wird gespeichert und gegebenenfalls bereits die ersten VMs erzeugt.

Customizations anlegen

"Customization spezifications" sind Definitionen, die mehrere Einstellungen enthalten, mit denen eine neue VM, die aus einem Template erstellt wurde, angepasst wird. Dadurch können Sie nur ein Template haben und mit Hilfe dieser Definitionen unterschiedlichste Ergebnisse erzielen. Um so eine Definition anzulegen, sind mehrere Schritte erforderlich: Klicken Sie im VCS auf "Edit / Customization Specifications / New", um eine neue Definition anzulegen. Wählen Sie nun "Windows" in der Klappbox aus, vergeben Sie einen Namen und optional eine Beschreibung. Anschließend geben Sie den Namen und die Organisation ein, die in der Maschine hinterlegt werden sollen. Wählen Sie dabei eine der beiden Optionen:

- "Use the virtual machine name": Der Hostname ist derselbe, den die VM bekommt (empfohlen)
- "Use a specific name": Hier können Sie ein eigenes Label definieren; stellen Sie sicher, dass "Append a numeric value to ensure uniqueness" aktiviert ist, damit die Namen eindeutig bleiben.

Geben Sie jetzt die Lizenz für das Betriebssystem ein; es empfiehlt sich der Einsatz von Volumenlizenzen. Nach der Angabe des Administratorpasswords wählen Sie die gewünschte Zeitzone aus. Optional können Sie nun einen oder mehr Befehle eingeben, die ausgeführt werden, wenn sich der erste Benutzer anmeldet.

Im nächsten Schritt legen Sie fest, wie Sie die Einstellungen für die Netzwerkkarte vornehmen wollen. "Typical Setting" wird hier empfohlen, damit Sie später die erstellten Maschinen nicht nochmals manuell anpassen müssen. Wählen Sie nun, ob die Maschine automatisch zu einer Domäne hinzugefügt werden soll. Hierfür wird ein Benutzer mit Passwort mit entsprechenden Rechten benötigt. Aus Sicherheitsgründen verwenden Sie für diese Aufgabe einen eigenen Benutzer. Sie sollten zudem den automatischen Domänen Join verwenden, um alle Vorteile des automatischen Desktop Pools nutzen zu können. Stellen Sie nun noch sicher, dass der Haken "Generate New Security ID (SID)" gesetzt ist. Mit einem Klick auf "Finish" schließen Sie die Konfiguration ab und haben mit diesen einfachen Schritten eine Modifikationsdefinition angelegt, die Sie in den Eigenschaften eines automatischen Desktoppools verwenden können. Wenn Sie sich gut mit Sysprep auskennen, können Sie, anstatt einen Namen und eine Be-

schreibung einzugeben, auch den Haken "Use Custom Sysprep Answer File" setzen und im nächsten Abschnitt eine eigene *sysprep.inf*-Datei importieren.

Zugriffe durch Nutzer erlauben

Damit Nutzer auf diesen Pool zugreifen können, müssen Sie die sogenannten "Entitlements" konfigurieren. Wählen Sie im linken Teil des View Administrators den entsprechenden Pool aus und klicken dann im rechten auf "Entitlements". Es öffnet sich eine Übersicht, welche Domänenbenutzer und -gruppen bereits Zugriff haben. Über die Schaltfläche "Add" erscheint ein Suchfenster, mit dem Sie das AD nach Benutzern und Gruppen durchsuchen können. Wählen Sie das Gewünschte aus (Mehrfachselektionen sind möglich) und klicken Sie auf "OK". Ob Sie alles richtig gemacht haben, können Sie ganz einfach testen, in dem Sie sich auf einem Rechner anmelden, der die View Client-Software installiert hat. Starten Sie diese, geben den Namen des VCS ein und melden Sie sich mit einem Benutzer an. Nun sollten Sie den eben erzeugten Desktop-Pool angezeigt bekommen. Wenn nicht, ist dieser Benutzer nicht in den Entitlements dieses Pools freigeschaltet worden oder ist kein Mitglied einer dort hinterlegten Gruppe. Überprüfen Sie in dem Fall nochmals die Einstellungen. Sehen Sie nun den Pooleintrag, wählen Sie diesen per Doppelklick aus und Sie werden sofort mit einer freien VM verbunden. Je nachdem, welche Konfiguration Sie vorgenommen haben, kann es sein, dass eine neue VM erstellt werden muss. Dies können Sie im VI überprüfen.

View Composer

Im folgenden Abschnitt unseres Workshops zeigen wir Ihnen, wie Sie den View Composer (VCP) installieren, um mit Linked Clone Desktops zu arbeiten. Der VCP ist ein Dienst, der auf der Maschine des VC läuft. Einmal installiert, konfiguriert und aktiviert verrichtet er seine Aufgaben unauffällig im Hintergrund. Für die Installation müssen Sie zunächst die Datenbank auf den Einsatz des VCP vorbereiten. Wir gehen in unserem Beispiel davon aus, dass ein SQL Server Express auf dem VCS läuft. Falls Sie einen SQL-Server auf einem anderen Server benutzen wollen, passen Sie die Schritte entsprechend an. Installieren Sie zuerst SQL Server Management Studio Express auf dem vCenter Server. Die Software finden Sie unter [4].

Erstellen Sie nun eine neue Datenbank, indem Sie sich mit dem Management Studio an der Datenbank anmelden. Geben Sie dazu als Servernamen "{vCenter-Servername}\SQLEXP_VIM" ein und wählen als Authentifizierung "Windows Authentifizierung". Klicken Sie danach mit der rechten Maustaste auf "Databases" und "New Database". Geben Sie als Datenbankname "VIM_LinkedClone" und unter Optionen die Sortierung "SQL_Latin1_General_CP1_CI_AS" ein. Alles andere kann auf den Standardeinstellungen bleiben. Damit der VCP korrekt arbeiten und kommunizieren kann, benötigen Sie einen Domänenbenutzer mit den Rechten eines Domänenadministrators. Haben Sie für das VC bereits einen angelegt, können Sie diesen weiter verwenden. Beachten Sie bitte den Kasten "View Composer-Benutzerrechte", falls Sie eine eigene Rolle im VCS definieren möchten.

Zulässige Namensmuster

Standardmäßig wird ein bis zu 13 Zeichen langes Präfix benutzt, um alle Desktops eines Pools als zusammengehörig zu identifizieren. Ein numerisches Suffix wird angehängt, um die einzelnen Desktops desselben Pools unterscheiden zu können.

Dieses Verhalten können Sie verändern, in dem Sie ein eigenes Schema hinterlegen. Insgesamt dürfen die Namen nicht länger als 15 Zeichen werden.

Muster mit einfachem Zähler

Pool1-{n}-Desktop: Während der Erstellung wird {n} durch eine fortlaufende Zahl innerhalb desselben Desktoppools ersetzt, ergibt also Pool1-1-Desktop, Pool1-2-Desktop, …

Muster mit Zähler mit fester Länge

Pool2-{n:fixed=3}: Hiermit legen Sie die Länge der Zahl fest. Es wird mit führenden Nullen aufgefüllt, ergibt also Pool2-001, Pool2-002,…

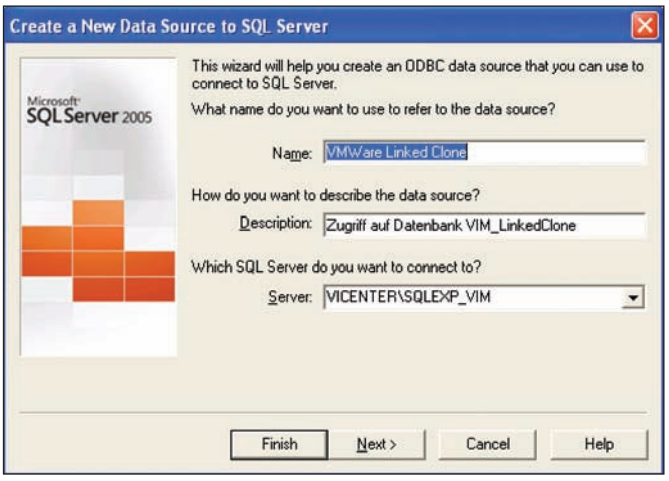


Bild 5: Der SQL Client-Assistent mit den benötigten Werten

Zusätzlich benötigen Sie eine ODBC-Datenquelle. Diese richten Sie unter "Systemsteuerung / Verwaltung / Datenquellen" ein. Klicken Sie dabei auf "System DSN", "Add" und "SQL Native Client". Ein Konfigurationsassistent erscheint. Auf der zweiten Seite des Assistenten lassen Sie alles unverändert. Setzen Sie auf der dritten Seite nun den Haken "Ändern der Standarddatenbank" und wählen die Datenbank "VIM_LinkedClone" aus. Auf der letzten Seite bleiben die Standardwerte.

Nachdem Sie die Datenbank erstellt haben, installieren Sie *VMware-viewcomposer-xxx.exe* auf dem VC-Server. Die Standardeinstellungen können beibehalten werden. Auf der Seite "Database Information" tragen Sie anschließend den Namen der zuvor eingerichteten ODBC-Verbindung, den separat angelegten Domänenbenutzer und das passende Kennwort ein. Der Benutzer muss in der Notation {Domäne}\{Benutzerkennung} eingetragen werden. Notieren Sie sich unbedingt die Nummer des SOAP-Ports. Während der ersten Installation des VCP werden ein SSL–Zertifikat und ein RSA-Schlüsselpaar zur codierten Speicherung des Passworts in der Datenbank erstellt. Wenn Sie die Installation wiederholen, können Sie wählen, ob Sie den Schlüssel und das Zertifikat beibehalten oder neu erstellen möchten.

Rufen Sie nun das Interface des View Administrators auf und wechseln auf die Konfigurationsansicht. Klicken Sie auf Ihren VC-Server und auf "Edit". Setzen Sie den Haken bei "Enable View Composer", tragen den zuvor notierten SOAP-Port ein und klicken auf "Add". Geben Sie hier nun ebenfalls die Daten des neu angelegten Domänenadministrators ein. Ein Klick auf "Add" und einer auf "OK" und schon ist die globale Konfiguration von VCB abgeschlossen.

Erstellen einer Master-VM

Die Master-VM ist die VM, von der alle virtuellen Desktops eines Pools abgeleitet werden. Erstellen und konfigurieren Sie Ihre VM nach Ihren Anforderungen; stellen Sie aber sicher, dass

- die VM ein Mitglied der Domäne ist, in der die virtuellen Desktops aufgenommen werden sollen.
- die Netzwerkeinstellungen wie etwa Proxys korrekt konfiguriert sind. Es muss unbedingt DHCP zum Einsatz kommen.
- die Systemplatte am Virtual Device Node SCSI (0:0) angeschlossen ist.
- alle Laufwerke nur eine Partition enthalten. Mehrere virtuelle Laufwerke werden aber unterstützt.
- die Energieoptionen des Betriebssystems auf "Immer an" stehen.
- der View Agent installiert ist und läuft.

Damit aus dieser VM nun eine Master-VM wird, sind drei einfache Schritte notwendig. Geben Sie in der Konsole *ipconfig /release* ein, um die erhaltene IP-Adresse zurückzugeben. Fahren Sie danach die VM herunter und warten Sie, bis sich diese ausgeschaltet hat. Erstellen Sie nun einen Snapshot und geben ihm den Namen "Baseline Configuration 1". Verändern Sie übrigens nie die Master-VM, indem Sie diese etwa in ein Template konvertieren, bevor oder während der VCP Linked Clone Desktops erstellt. Der VCP-Dienst setzt voraus, dass die Master-VM in einem statischen und unveränderten Zustand ist.

Erstellen eines Linked Clone Desktop Pools

Da die Einrichtung eines Desktop Pools für Linked Clone Desktops ebenfalls im View Manager über "Automated Desktop Pool" erfolgt, werden hier nur die Abweichungen zu den Pools mit Standarddesktops erläutert. Wählen Sie einen persistenten Desktop aus und setzen Sie auf der Seite "VirtualCenter Server" den Haken "Use linked clone technology". Bei "Desktop/Pool Settings" ist jetzt eine neue Option namens "Refresh OS disk on logoff" sichtbar. Hiermit steuern Sie, wie oft die Systemplatte anhand der Master-VM aktualisiert werden soll. Sie können das immer, nie, alle X Tage oder in Abhängigkeit des Füllgrades des Datastores machen. Diese Option erscheint nur bei persistenten Desktops. Für nicht-persistente Desktops macht es keinen Sinn, da die VM am Ende der Benutzung ohnehin wieder zerstört wird. Stellen Sie für diesen Workshop hier "Never" ein. Wählen Sie nun auf den nächsten Seiten Ihre Master-VM und den Snapshot "Baseline Configuration 1" aus.

Wenn Sie für den VCP eine eigene Rolle im VC anlegen möchten, brauchen Sie über die Rechte des "View Administrators" hinaus folgende Rechte:

- Datastore: Browse Datastore, File Management
- Virtual Machine – Inventory: Move
- Virtual Machine – Configuration: alle Optionen
- Virtual Machine – State: alle Optionen
- Virtual Machine – Provisioning: Clone, Allow Disk Access
- Global: Enable Methods, Disable Methods

Beachten Sie, dass dieser Benutzer ebenfalls lokaler Administrator auf dem Server sein muss, auf dem der VCP-Dienst läuft. In unserem Beispiel ist das der Server des VCS.

View Composer-Benutzerrechte

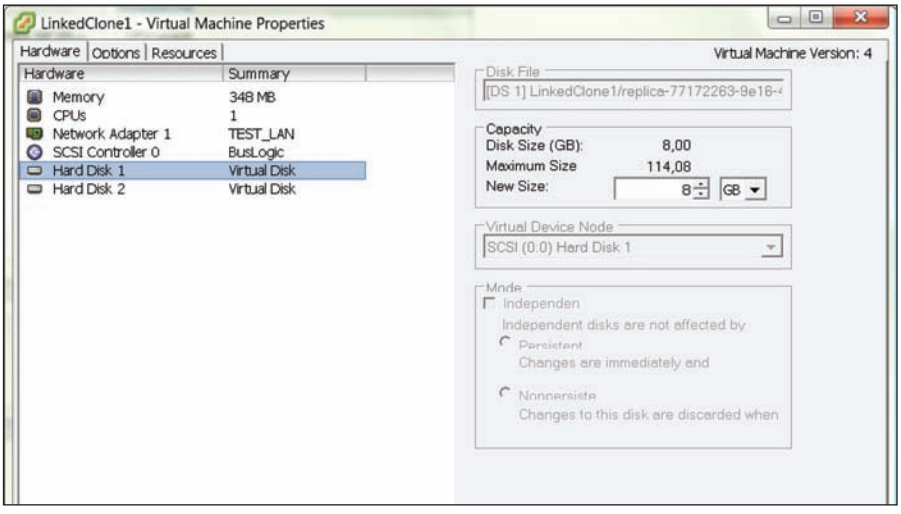


Bild 6: Anzeige der verwendeten Replica über die Eigenschaften der virtuellen Maschine

Sie haben auch die Möglichkeit, jeden erstellten Desktop automatisch mit einer weiteren virtuellen Festplatte versehen zu lassen, die die Benutzerdaten enthält. Aktivieren Sie dazu unter "User Data" die Option "Redirect User Data to a separate disk", bestimmen Sie die Größe und einen noch verfügbaren Laufwerksbuchstaben. Die Daten dieser Platte werden von keiner Aktion des VCP-Dienstes beeinflusst. Beim Einsatz der Option "Store user data on the same disk as the OS" ist dies nicht der Fall; da sind die Daten bei jeder Anpassung der Master-VM weg. Die Datastores haben auch die neue Einstellmöglichkeit "Storage Overcommit". Damit können Sie steuern, wie aggressiv das System neue VMs den Datastores hinzufügt. Je aggressiver die Stufe ist, umso weniger Platz wird für das individuelle Wachstum der einzelnen VMs reserviert, aber umso mehr VMs passen auf den Datastore. Als Letztes wählen Sie einen Domänenadministrator aus, damit die neuen Maschinen der Domäne hinzugefügt werden können. Sie können ebenfalls eine OU angeben, in die die Computerkonten der VMs verschoben werden sollen.

Sofort nachdem der Pool fertiggestellt ist, generiert der VCP-Dienst ein Replikat der Master-VM. Aus technischer Sicht handelt es sich dabei um das Master-Image, welches in Beziehung zu den Differenzimages der einzelnen Desktops steht. Es wird pro Datastore ein Replikat angelegt. Sobald die Replikation fertig ist, werden je nach Provisioning-Einstellungen ein oder mehrere Desktops erstellt. Öffnen Sie die Einstellungen eines Desktops und klicken auf "Hard Disk 1". Rechts oben sehen Sie, welches Replikat diese Platte verwendet. Benutzen Sie den Datastore-Browser, um die tatsächliche Dateigröße zu überprüfen. Sie sollte nur wenige MByte groß sein. Die Benutzung dieser Desktops unterscheidet sich für den Anwender nicht zu den Desktops der Standardpools.

Refreshing, Recomposing und Rebalancing

VMware unterscheidet drei Arten, einen Linked Clone Desktop zu bearbeiten: Sie führen ein "Recomposing" durch, wenn Sie einen anderen Snapshot derselben Master-VM oder den Snapshot einer anderen Master-VM dem Pool zuordnen. In beiden Fällen wird ein neues Replikat erstellt. Mit der Dauer der Nutzung der Desktops durch die Anwender wächst das Differenzimage jeder Desktop-VM an. Um die Größe zu reduzieren, führen Sie einen sogenannten "Refresh" durch. Dabei wird das Differenzimage an Hand des ursprünglichen Replikats neu erstellt. Da hier kein neues Replikat erstellt wird, ist dieser Vorgang schneller als das "Recomposing". Sie können dies manuell, automatisiert in verschiedenen Zeitintervallen oder in Abhängigkeit von der Systemplattengröße ausführen. Mittels "Rebalancing" lässt sich die Verteilung der erstellten Desktops auf den Datastores angleichen. Für alle drei Maßnahmen gilt: Sie können nur bei persistenten Desktops angewendet werden und die Daten auf einer Benutzerdatenplatte werden nicht beeinflusst.

Fazit

Im zweiten Teil unserer Workshopserie haben wir Ihnen gezeigt, wie schnell und einfach Sie mit VMware View persönliche Desktopsysteme zur Verfügung stellen. Trotz der Vielzahl der Komponenten ist ein grundlegendes Setup schnell erstellt – vor allem, wenn es bereits passende Templates der Gastsysteme gibt. Daneben haben Sie erfahren, wie Sie den View Composer aufsetzen. Der dritte und abschließende Teil der Serie hat dann die Nutzung der ThinApp-Applikationsvirtualisierung sowie der Images zum Thema. *(dr)*

Andreas Badur und Dr. Jürgen Fechter sind Mitarbeiter des Systemhauses science+computing ag und arbeiten dort als Consultants beziehungsweise IT-Architekten. Sie arbeiten im Competence Center "Microsoft Infrastructure Solutions", welches Virtualisierungslösungen einschließt.

Links

[1] Remote Desktop Sourcen
www.rdesktop.org

[2] RDP Client Version 6.1
http://microsoft.com/downloads/details.aspx?familyid=6E1EC93D-BDBD-4983-92F7-479E088570AD

[3] Patches für RDP-Verbindungen
http://support.microsoft.com/kb/323497 und
http://support.microsoft.com/kb/884020

[4] SQL Server Management Studio Express
www.microsoft.com/downloads/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

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

Microsoft Windows

Immer, wenn ich **unter Windows Server 2008 einen Reboot** durchführen möchte, meldet sich das bekannte Fenster, das nach den **Gründen für den Neustart** fragt und sich nicht so einfach wegklicken lässt. Ich würde aber gerne auf diese wissbegierige Anfrage verzichten. Kann ich die Box irgendwie abschalten?

Um die Nachfrage nach den Ursachen eines Neustarts dauerhaft abzuschalten, öffnen Sie zunächst die MMC. Dort wählen Sie "File / Add Remove Snapin" aus und fügen den "Group Policy Management Editor" hinzu. Nun wählen Sie das gewünschte Group Policy Object (GPO), beispielsweise "Default Domain Policy", und bestätigen alle Dialoge mit "OK". Im Verzeichnisbaum navigieren Sie zu "Computer Configuration / Policies / Administrative Templates / System". Jetzt wählen Sie rechts in der Liste "Display Shutdown Event Tracker" aus und setzen den Eintrag auf "disabled". Beachten Sie hierbei, dass die Einstellung für die gesamte Domäne gilt, wenn Sie das GPO "Default Domain Policy" bearbeitet haben. Alternativ können Sie den Wert auch auf "enabled" setzen, in der Dialogbox aber zusätzlich die Option "Server Only" ankreuzen, um den Reboot-Dialog auf Windows-Clients zu umgehen. *(ln)*

Beim Navigieren mit dem Windows Explorer wäre es ab und zu sehr praktisch, wenn ich **direkt aus dem Kontextmenü die Eingabeaufforderung** im entsprechenden Verzeichnis öffnen könnte. Gibt es vielleicht einen entsprechenden Eintrag in der Registry, mit dem ich die Kommandozeile mit einem Rechtsklick starten kann?

Wie Sie schon vermutet haben, können Sie das Kontextmenü über einen Eintrag in der Registry verändern. Bewegen Sie sich in der Registrierungsdatenbank zum Eintrag "HKEY_LOCAL_MACHINE \ Software \ Classes \ Folder \ shell" und erzeugen Sie dort mit der rechten Maustaste einen neuen Schlüssel mit der Bezeichnung "cmd". Mit einem weiteren Rechtsklick im rechten Fenster auf den neu erzeugten Schlüssel und der Auswahl der Option "ändern" setzen Sie den Wert etwa auf "Eingabeaufforderung hier öffnen" – dies ist der Wortlaut des neuen Eintrags im Kontextmenü. Innerhalb dieses neu erzeugten Schlüssels generieren Sie nun einen weiteren Schlüssel mit der Bezeichnung "command". Hier hinterlegen Sie als Wert folgendes:

```
CMD.EXE /S /K pushd "%1"
```

Schließen Sie den Registry Editor und starten Sie zusätzlich den Windows Explorer neu. Nun sollte Ihr Kontextmenü um einen Eintrag reicher sein und Sie können die Kommandozeile stets im gewünschten Verzeichnis öffnen. *(ln)*

Ich habe gehört, dass **Windows 7** über ein integriertes Tool verfügt, mit dem sich **Image-Dateien ohne Zusatzprogramme auf DVD brennen** lassen. Da ich derzeit die Beta des neuen Betriebssystems ausprobiere, würde mich interessieren, ob ich dieses Tool über die Kommandozeile starten kann.

Der Name der kleinen Hilfsdatei ist *isoburn.exe*. Diese lässt sich über den Windows Explorer mit einer kleinen GUI, aber auch über die Eingabeaufforderung bedienen. Geben Sie hierzu

```
isoburn.exe /Q F: "C:\{Verzeichnis-
  name}\Imagedatei.iso"
```

ein. In diesem Fall wäre das Laufwerk "F" der DVD-Brenner, der zweite Pfad stellt den Ablageort des Image-File dar. Der Schalter "/Q" bewirkt, dass das Brennen des Abbilds sofort beginnt. Ohne diesen Zusatz müssen Sie den Brennvorgang noch manuell bestätigen. *(ln)*

Mozilla / Firefox

Beim Surfen mit Mozilla Firefox habe ich immer mehrere Tabs offen. Um eine Reihe von Tabs schnell zu schließen, bevorzuge ich die Tastatur und verwende die **Kombination "Strg+W"**. Dabei passiert es mir leider manchmal, dass

ich auch den letzten Tab schließe und Firefox damit ebenfalls beende. Gibt es irgendeine Möglichkeit, **den letzten Tab stets geöffnet zu halten?**

Wenn Sie nicht wollen, dass sich mit dem Schließen des Tabs ganz links auch Firefox verabschiedet, können Sie dies in den erweiterten Einstellungen des Browsers konfigurieren. Geben Sie dazu in der Adressleiste *about:config* ein und navigieren Sie zum Eintrag "browser.tabs.closeWindowWithLastTab". Dessen Wert ändern Sie mit einem Doppelklick von "true" auf "false". Ab sofort können Sie so oft "Strg+W" drücken, wie Sie wollen: Ein Tab bleibt immer offen und erhält Firefox so am Leben. *(ln)*

Firefox 3.5 kommt mir zwar um einiges schneller vor als die Vorgängerversion, trotzdem würde ich mir den Seitenaufbau manchmal noch zügiger wünschen. Kann ich auf irgendeine Weise noch **mehr aus dem Browser herausholen?**

Auf jeden Fall sollten Sie einen Blick auf zwei Einstellungen in der erweiterten Konfiguration werfen. Nach der Eingabe von *about:config* in der Adresszeile sehen Sie sich den Eintrag "network.http.pipelining" an und setzen diesen auf "true". Beim Eintrag "network.http.pipelining.maxrequests" sollten Sie den Zahlenwert erhöhen, "8" ist beispielsweise ein sinnvoller Wert. Pipelining ermöglicht mehrfache gleichzeitige Datenanfragen und sollte den Seitenaufbau merklich beschleunigen. Sind Sie mit einer älteren Firefox-Version unterwegs, sollten Sie zudem den Eintrag "network.http.pipelining.firstrequest" auf "true" setzen und außerdem den Parameter "nglayout.initialpaint.delay" mit "0" hinterlegen. Insgesamt sollte der Browser nun etwas flotter sein. *(ln)*

CITRIX

Seit geraumer Zeit benötigt die Access Management Console für den Start ungewöhnlich lange. Gibt es hierfür einen Grund und lässt sich **diese Verzögerung vermeiden?**

Die Access Management Console (AMC) in Version 4.5.x, 4.6.x oder 5.x wurde als Microsoft .NET-Applikation konzipiert. Citrix fügt der AMC eine Authenticode-Signatur bei, die für zusätzliche Sicherheit sorgt. Wird die AMC von einem Rechner ohne Internet-Zugang ausgeführt, so führt dies zu einer Verzögerung während des Starts. Windows selbst ist nicht in der Lage, die Authenticode-Signatur auf Gültigkeit zu prüfen. Dieses Problem lässt sich auf zwei Arten lösen: Sie können den Computer mit dem Internet verbinden und so die Überprüfung der Signatur ermöglichen – der Startvorgang beschleunigt sich. Außerdem ist es möglich, die Überprüfung der Signatur für die Microsoft Management Console zu deaktivieren. Als Voraussetzung für die Deaktivierung muss .NET Framework 2.0 mit Patch KB936707, Microsoft .NET Framework 2.0 SP1 oder .NET ab Version 3.0 installiert sein. Folgender Workaround funktioniert sowohl bei 32-Bit- als auch bei 64-Bit-Windows-Systemen:

1. Erstellen Sie die Datei *mmc.exe.config* in *c:\windows\system32*
2. Fügen Sie folgende Zeilen ein:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<runtime>
<generatePublisherEvidence enabled="false" />
</runtime>
</configuration>
```

3. Starten Sie die Access Management Console neu. Der Ladevorgang sollte nun wesentlich schneller erfolgen, weil die Überprüfung der Authenticode-Signatur übersprungen wird. *(Citrix/ln)*

Tools

Spätestens seit Conficker ist jedem IT-Verantwortlichen die Bedrohung durch **Malware** bewusst, die **USB-Wechseldatenträger** nutzt, um Systeme zu infizieren und sich zu verbreiten. Besonders die Autorun-Funktion von Windows kann hier zum Problem werden, wenn sie die eventuell auf dem USB-Stick vorhandenen Schädlinge automatisch lädt. Hat ein Unternehmen keine zentrale Lösung – wie etwa ein Data Leackage Prevention-Werkzeug –, um USB-Zugänge zum Netzwerk zu kontrollieren, gilt es, die Malware auf anderem Wege zu stoppen.

Das bereits im März veröffentlichte Tool **Panda USB Vaccine** liegt nun in einer aktualisierten Form vor und sperrt den automatischen Start von Programmen auf Wechseldatenträgern. Das Werkzeug deaktiviert die Autorun-Funktion auf PCs beziehungsweise auf einzelnen USB-Sticks und schützt somit vor infizierten Datenträgern sowie umgekehrt USB-Sticks vor infizierten Rechnern. Panda USB Vaccine behebt somit unkompliziert eine Windows-Sicherheitslücke, die Administratoren zwar mit Windows-Bordmitteln beheben können, doch das kostenlose Programm bietet deutlich mehr Komfort. Lauffähig ist das Schutzprogramm unter Windows XP und Vista (und nach Herstellerangaben auch schon unter Windows 7) sowie Windows Server 2003. Die nun vorliegende Version von "USB VAccine.exe" wurde in folgenden Punkten aktualisiert beziehungsweise ergänzt:

- Unterstützung der "Impfung" von NTFS-Datenträgern.
- Die Ausführung von "USBVaccine.exe" ruft einen Installer auf, der die Konfiguration des Autostart-Verhaltens von USB Vaccine

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

beim Windows-Start möglich macht.
- Konfigurationsoption, um das Tray-Icon zu verstecken.
- Konfigurationsoption während des Setups, um neue USB-Datenträger beim Anschluss an den Rechner zu impfen. *(jp)*

Quelle: http://acs.pandasoftware.com/marketing/promo/USBVaccine.zip

Es gibt Situationen, in denen die Konfiguration von **Presentation Server/XenApp** mit Webinterface und Programm Neighborhood Agent einfach nicht so funktionieren will, wie eigentlich zu erwarten war. Als aufwändige Lösung bleibt dann oft nur, den Netzwerkverkehr mit Wireshark zu scannen, um die **fehlerhafte Komponente** zu finden. Mit einem kleinen Tool fällt dieses Troubleshooting deutlich leichter.

Presentation Server / XenApp enthält den so genannten Citrix-XML-Service. Dieser Systemdienst, der standardmäßig auf Port 80 arbeitet, stellt die Konfiguration im XML-Format über HTTP bereit. Alle Anfragen und Antworten an diesen Dienst werden in XML ausgedrückt und folgen der Definition in der Datei *NFuse.dtd*. Diese wird mit allen Versionen des Web Interface ausgeliefert und ist unter *C:\inetpub\wwwroot\Citrix\XenApp\conf* abgelegt. Über den XML-Dienst erhält das Web Interface Informationen über veröffentlichte Anwendungen und Einstellungen, die für den Anwendungsstart relevant sind. Jetzt wäre es doch hilfreich, wenn man selber das WebInterface imitieren, die Serverfarm untersuchen oder nach Informationen fragen könnte. Das alles ist mit dem "XmlServiceExplorer" möglich. Durch dieses Tool gestaltet sich die Fehlerbehebung sehr viel einfacher. Bei diesem Werkzeug handelt es sich um ein grafisches Tool, um Anfragen an den XML-Dienst zu senden, die sich frei generieren lassen. Damit können Sie die ablaufende Kommunikation nach Schwachstellen und Unregelmäßigkeiten untersuchen. *(sepago/ln)*

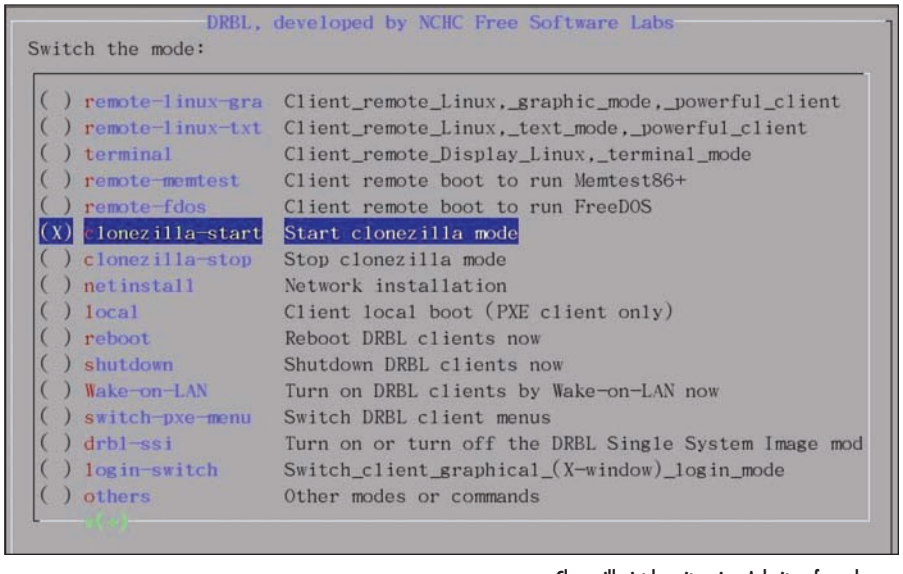
blogs.sepago.de READ | WRITE

Weitere Informationen zu diesem Werkzeug finden Sie unter *http://blogs.sepago.de/nicholas/2008/07/17/talking-to-the-xml-service/*

Meldet sich die Festplatte mit merkwürdigen Geräuschen, ist es für den Anwender an der Zeit, sich Gedanken über die Sicherung beziehungsweise Rettung der Daten zu machen. Vor der selben Aufgabe – die komplette Festplatte zu kopieren und die Daten an einem anderen Ort weiter zu nutzen – stehen IT-Verantwortliche aber auch dann, wenn ein Hardwarewechsel ansteht, sei es nun der komplette Rechner oder nur eine neue Festplatte. In beiden Fällen ist eine **1-zu-1-Kopie des Festplatteninhalts** – inklusive aller Partitionen, Dateien und natürlich Windows selbst – die ideale Lösung.

Ein kostenloses Werkzeug, das sich bei genau diesen Aufgaben als sehr hilfreich erwiesen hat, ist **Clonezilla**. Dieses leistungsfähige Tool zum Klonen kompletter Festplatten braucht sich vor kommerziellen Angeboten keineswegs zu verstecken. Nach dem Download brennen IT-Verantwortliche das ISO-Image auf eine CD-Rom und erhalten so ein bootfähiges "Clonezilla-Live-Linux". Clonezilla unterstützt die Dateisysteme ext2, ext3, reiserfs, xfs, jfs sowie FAT und NTFS. Der so erstellte Klon lässt sich auf der Ziel-Festplatte entpacken und anschließend dort weiterarbeiten als wäre nichts gewesen. Ein besonderer Vorteil von Clonezilla ergibt sich aus der Tatsache, dass das Werkzeug nur Blöcke speichert beziehungsweise wiederherstellt, die auch tatsächlich benutzt sind. Das kann sich deutlich auf die Geschwindigkeit auswirken. Das Paket liegt in zwei Varianten vor: eine installierbare Version mit Multicasting-Unterstützung oder Clonezilla Live. Herunterladen können Sie das System kostenlos als ISO- oder Zip-Datei – beide Dateien sind etwa 83 MByte groß. *(jp)*

Quelle: http://sourceforge.net/projects/clonezilla/



Clonezilla ist bereit, seine Arbeit aufzunehmen

Powermanagement im Rechenzentrum

Den Strom selbst managen

von Bodo Mainz

IT-Verantwortliche müssen neben den Stromkosten vor allem die Ausfallsicherheit im Auge behalten. Der folgende Artikel gibt einen Überblick, wie sich IT-Equipment zum einen zuverlässig gegen Stromausfälle und Spannungsschwankungen schützen und wie sich zum anderen mit modernen Komponenten für Stromverteilung und Monitoring die IT-Infrastruktur effizient und kostensparend verwalten lässt.


Quelle: Pixelio.de

Für das IT-Equipment im Rechenzentrum hat zunächst der Schutz vor Stromausfällen und Störfrequenzen oberste Priorität – schließlich können Systemausfälle und Datenverluste enorme Kosten nach sich ziehen. Hinzu kommt: IT-Geräte und Netzwerkkomponenten sind auf eine absolut saubere, das heißt sinusförmige Eingangsspannung angewiesen – schon kleine Frequenzstörungen können Schäden verursachen. Unterbrechungsfreie Stromversorgungen (USVs) überbrücken Stromausfälle, filtern schädliche Spannungsstörungen und kompensieren Spannungs- und Frequenzschwankungen.

Um in Rack-Umgebungen und Datenzentren Platz zu sparen, gibt es speziell entwickelte USV-Modelle im 19-Zoll-Format, sogenannte Rackmount (RM)-USVs. Dank ihrer hohen Leistungsdichte bieten sie dieselbe Leistung und arbeiten mit dem gleichen Funktionsumfang wie entsprechende Standgeräte. Mit wachsender Serverdichte spielt neben dem Platz die Wärmeentwicklung in Serverräumen eine große Rolle. Bei der Auswahl der einzelnen Rack-Komponenten muss daher auf eine hohe Energieeffizienz – also auf einen hohen Wirkungsgrad – und damit niedrige Verlustleistung geachtet werden. Es empfiehlt sich außerdem, bereits vor dem Einbau einer RM-USV Aspekten wie Abwärme und Kühlung Rechnung zu tragen: Die USV sollte immer so in ein Rack integriert sein, dass eine optimale Luftzirkulation gewährleistet ist. Je nach Größe der abzusichernden Last und des benötigten Schutzumfangs kommen für Rechenzentren zwei unterschiedliche USV-Typen infrage: Line-interaktive- und Online-USVs.

USV-Schutz im Rechenzentrum

Für Rechenzentren und Racks mit kleiner und mittlerer Leistungsdichte ohne sehr kritische oder sensible Verbraucher ist ein mittlerer Schutzumfang ausreichend. Die kontinuierliche Spannungsaufbereitung spielt für Systeme wie Hubs, Router, kleinere Appliance-Server oder Telekommunikationsanwendungen keine so entscheidende Rolle. Hier bieten sich Line-interaktive USVs an. Ist die Eingangsspannung in einem akzeptablen Bereich, wird sie durch die Line-interaktive USV lediglich gefiltert und dann hindurchgeleitet. Ist die Eingangsspannung außerhalb dieses Bereiches, aber noch innerhalb eines bestimmten vorgegebenen, größeren Eingangsfensters, wird sie zusätzlich automatisch ausgeregelt und ebenfalls gefiltert.

Außerhalb dieses vorgegebenen Eingangsspannungsbereiches versorgt der Wechselrichter die Last. Ein Gleichrichter wandelt die Eingangsspannung in Gleichspannung um, damit die Akkus vollgeladen bleiben, wenn die Netzspannung anliegt. Dies erfordert etwa zehn Prozent der USV-Leistung – die Komponenten bleiben kühl. Damit wer-

Die Steckdose für das RZ erfüllt weit mehr Aufgaben als eine normale Steckerleiste

den Spannungsspitzen geglättet sowie Unebenheiten und Über- beziehungsweise Unterspannungen ausgeglichen. Die Wellenform des von der Last verbrauchten Stroms wird hier allerdings nicht geändert. Line-interaktive USVs sind außerdem in ihrer Kapazität begrenzt und daher nicht geeignet, besonders leistungsstarke Verbraucher zu schützen. Der Vorteil dieser Technologie: Der Strom wird nicht permanent gewandelt – und das bedeutet weniger Energieverbrauch, weniger Abwärme, weniger Kosten. Ein Nachteil ist die Umschaltzeit von einigen Millisekunden.

Rund-um-die-Uhr-Schutz für kritisches Equipment

Racks mit mittlerer und hoher Leistungsdichte in Datenzentren mit kritischen und hochsensiblen Verbrauchern erfordern ein höheres Maß an Schutz. Permanente Verfügbarkeit und Ausfallsicherheit sind ebenso unabdingbar wie eine absolut saubere Sinusspannung. Sichergestellt wird dies mit Online-Doppelwandler-USVs. Diese wandeln die Eingangswechselspannung kontinuierlich in Gleichspannung. Ein Lader lädt bei Bedarf die Batterie, die zwischen Gleichrichter beziehungsweise Lader und Wechselrichter geschaltet ist. Anschließend wird die Gleichspannung mittels Wechselrichter wieder in eine konstante sinusförmige Wechselspannung umgewandelt. Vorteile: keine Umschaltzeiten, da der Wechselrichter im Dauerbetrieb ist und nicht erst zugeschaltet werden muss.

Des Weiteren hat die USV durch die Doppelwandlung einen reinen Sinuswellenstrom am Ausgang. Alle wichtigen Spannungsprobleme inklusive Schaltspitzen, Störspannungen, Frequenzabweichungen und harmonischen Oberwellen werden eliminiert und die Last wird mit reiner Sinusspannung versorgt. Nachteile: Online-Doppelwandler-Systeme verbrauchen mehr Energie und erzeugen auch mehr Wärme als Line-interaktive USVs.

Wegen der hohen Kosten, die Stromausfälle nach sich ziehen, müssen unternehmenskritische Anwendungen rund um die Uhr 100-prozentig abgesichert sein. Eine maximale Ausfallsicherheit erreicht ein IT-Verantwortlicher durch parallele beziehungsweise redundante Systeme. Hier kommen oft modulare Systeme, bestehend aus parallel geschalteten Einzelanlagen zum Einsatz. Inzwischen gibt es Technologien, die erlauben, dass die einzelnen Module unabhängig voneinander arbeiten. Fällt ein Modul aus, übernimmt das andere dessen Last automatisch und ohne Verzögerungszeit. Das erhöht die Ausfallsicherheit beträchtlich.

Shut-down- und Monitoring-Software

Fast alle modernen USVs werden heute mit sogenannter Shutdown- und Remote-Management-Software für alle gängigen Betriebssysteme geliefert. Die USV kommuniziert bei serieller Anbindung mit einem Gerät – meist dem Hauptserver – über die serielle Schnittstelle und meldet sofort Stromstörungen oder -ausfälle. Dort tritt dann die Management-Software nach einem festgelegten Plan in Aktion und veranlasst beispielsweise andere Systeme dazu, in der richtigen Reihenfolge alle Daten zu speichern, die Anwendungen zu schließen, das Betriebssystem herunterzufahren und sich auszuschalten. Bei Anbindung über eine Netzwerkverbindung können alle Server von der USV direkt angesprochen werden.

Bei beiden Möglichkeiten muss der Systemadministrator vorher genau wissen, welche Prozesse und Systeme voneinander abhängig sind – so wäre es beispielsweise fatal, die Firewall abzuschalten, solange ein anderes System noch mit dem Internet kommunizieren muss oder ein Speichersubsystem herunterzufahren, wenn potenziell noch File-System-Operationen stattfinden.

Stromfresser im Blick

Selbst wenn das Equipment durch USVs geschützt ist, gilt es dennoch, den Strom permanent zu überprüfen: Wo wird er hauptsächlich verbraucht? Welche Qualität hat der Strom aus dem Netz? Das macht so genannte Leistungsmesser immer wichtiger. Leistungsmesser analysieren die Stromqualität, speichern sämtliche Messwerte und erstellen auf Basis dieser Daten Qualitätsreports, die Facility-Managern oder Systemadministratoren bei der Problembehebung helfen. In den Auswertungen werden zum Beispiel Störfrequenzen wie harmo-

nische Oberwellen angezeigt, die empfindlichem Equipment schaden und so zu Systemausfällen führen können. Darüber hinaus messen die Geräte den Stromverbrauch und identifizieren "Stromfresser". In der Regel verfügen Leistungsmesser über ein webbasiertes Benutzer-Interface.

Mit PDUs den Strom effizient verteilen

Eine hohe Qualität der Stromversorgung erfordert auch eine effiziente Stromverteilung, die sich flexibel den unterschiedlichsten Anforderungen von Datenzentren und Racks anpassen lässt. Mit Power Distribution Units (PDUs), intelligente Steckerleisten auf Rack-Basis, lassen sich Stromverbrauch und Temperatur im Datenzentrum exakt messen – auf System-, Chassis- oder Rack-Ebene. Zugleich verfügen diese modernen Stromverteilungslösungen über eine Vielzahl an Optionen, um die Stromverteilung im Rack für jeden Verbraucher individuell zu überwachen und zu steuern. Dazu ist es notwendig, dass jede Steckdose einzeln abgesichert ist – die Gefahr einer möglichen Überlast auf die jeweilige Steckdose wird damit begrenzt. Idealerweise können die Ein- und Ausgänge der Stromverteilungen einzeln aus der Ferne ein- und ausgeschaltet werden. Damit lässt sich das Herunterfahren einzelner Steckdosen individuell überwachen. Auch das Hochfahren von Servern kann so kontrolliert gesteuert werden.

Praktisch ist auch die Möglichkeit, Steckdosen zu virtuellen Gruppen zusammenzufassen. So lassen sich auch Server mit mehreren Stromkabeln über einen einzigen Mausklick rebooten. Jede Steckdosengruppe benötigt dabei einen separaten Sicherungsautomaten. So beeinflusst ein überlastetes Segment nicht mehr die übrigen Segmente und der Betrieb kann schnell wiederhergestellt werden. Manche Stromverteilungslösungen verfügen zudem über Software und Schnittstellen, über die eine Vielzahl an Steckdosenleisten miteinander verknüpft werden können. Das vereinfacht das Netzwerkmanagement und reduziert die Anzahl der Netzwerkadressen, die zur Verwaltung der Steckdosenleisten im Rack nötig sind.

Heute arbeiten Hersteller unterschiedlicher Bereiche eng zusammen, sodass Systeme einfach ineinandergreifen können. Ein Beispiel dafür ist die neueste Version des IBM Systems "Director Active Energy Manager (AEM) V4.1". Der AEM liefert Anwendern einen Überblick über den tatsächlichen Stromverbrauch in Datenzentren und ist Teil von IBMs CoolBluePortfolio im Rahmen des Big-Green-Projekts. Dabei kann er den Energieverbrauch auch plattformübergreifend erfassen. Mithilfe von PDUs kann die aktuelle Version des AEM nun auch zur Energieverwaltung von Nicht-IBM-Systemen eingesetzt werden. Einige PDU-Hersteller wie Eaton haben sich darauf eingestellt – ihre PDUs unterstützen bereits AEM.

Durch diese detaillierten Einblicke in den Stromkreislauf lassen sich Datenzentren so verwalten, dass sie absolut energieeffizient arbeiten. Administratoren können Energie verschwendende Server identifizieren und Racks lokalisieren, in denen Kapazitäten für zusätzliches IT-Equipment frei sind. Je nachdem können sie dann Lasten von über- oder unterlasteten Systemen umziehen, um Hotspots zu eliminieren oder Energie zu sparen.

Überwachung der Umweltbedingungen

Hitze, Feuchtigkeit, Rauch, Wasser – die Ursachen für derlei Umwelteinflüsse im Datenzentrum können vielfältig sein. Die Folgen laufen dagegen auf dasselbe hinaus: Kritisches Equipment wird beschädigt, Daten gehen verloren, Anwendungen fallen aus. Untersuchungen zeigen, dass etwa 60 Prozent aller Hardware-Ausfälle auf Hitzeprobleme zurückzuführen sind. Gerade Datenzentren mit hoher Leistungsdichte müssen permanent überwacht werden. In Umgebungen wie Labors, Krankenhäusern, Lagerhäusern, Büchereien oder Museen sind die Umgebungsbedingen außerdem strikt festgelegt und dürfen bestimmte Werte nicht überschreiten.

Um dies unter Kontrolle zu haben, gibt es Monitore für die Rund-um-die-Uhr-Überwachung. Ungleichmäßige Luftströme, Hotspots et cetera werden damit rechtzeitig entdeckt, bevor an den Geräten Schaden entsteht. Solche Geräte messen über verteilt angebrachte Kontaktsensoren Temperatur und Feuchtigkeit an mehreren Stellen im Rack. Die Werte werden in Echtzeit an einen PC, ein internetfähiges Gerät oder ein Netzwerkmanagementsystem übermittelt. Gleichzeitig können gelistete Empfänger via E-Mail oder SNMP-Managementsysteme automatisch benachrichtigt werden, wenn die Parameter außerhalb der festgelegten Bereiche liegen. Darüber hinaus kann der Monitor bis zu 100 weitere Messstellen im Netzwerk automatisch lesen und erkennen sowie deren Status in Echtzeit auf einer einzigen Webseite abbilden.

Fazit

Mit steigenden Datenmengen erhöhen sich auch die Kosten für Energie, Kühlung und Verwaltung der IT-Infrastruktur. Umso mehr gilt es, darauf zu achten, dass das Equipment gleichmäßig ausgelastet ist und unnötiger Energieverbrauch und Überhitzung vermieden werden. Mittels moderner Monitoring- und Stromverteilungslösungen können Administratoren die Energieversorgung zentral kontrollieren und steuern. Dabei macht ein umfassendes Konzept Sinn, bei dem einzelne Systeme ineinandergreifen. Meldet der Leistungsmesser zum Beispiel ein hohes Maß an Oberwellen, muss die USV darauf ausgelegt sein, diese Art von Spannungsstörungen zu eliminieren. Stellt der Administrator mithilfe eines Rack-Monitors eine übermäßige Wärmeentwicklung fest, hilft ihm die Überwachung mittels PDUs, den dafür verantwortlichen Server zu identifizieren und rechtzeitig Anwendungen umzulagern. Das minimiert von vornherein das Ausfallrisiko und die Energiekosten im Rechenzentrum. *(jp)*

Bodo Mainz ist Geschäftsführer von Eaton Power Quality.

Schritte zur Datenbanksicherheit

Heiliger Informationsgral

von Uwe Maurer

Datenbanken stellen das Herzstück der meisten Unternehmen dar. In ihnen finden sich sensible Informationen, die für die tägliche Arbeit benötigt werden und nicht für fremde Augen bestimmt sind. Doch bei der Datenbanksicherheit hapert es oft. Dieser Beitrag zeigt auf, mit welchen Schritten Sie für Sicherheit sorgen.

Mit einigen Schutzvorkehrungen sichern Sie Ihre Datenbanken wirkungsvoll ab

Moderne Datenbanken werden immer komplexer und bieten die unterschiedlichsten Schnittstellen an: Es gibt Servicezugänge, Zugänge für Drittfirmen und für den Support, hochprivilegierte Zugänge für die Administratoren und oft zudem für Entwickler, auch auf den produktiven Systemen. Neben den normalen Benutzerzugängen greifen viele Anwendungen über spezielle Applikationskonten zu. Die Datenbanksysteme stehen relativ offen im Netz und sind für die unterschiedlichsten Angriffe und Bedrohungen frei zugänglich. Doch sind die Systeme und Komponenten selten auf einem aktuellen Patchlevel. In den meisten Fällen finden sich zudem Konfigurationsschwächen – besonders fehlerhafte Einstellungen aus der Installationsphase sind nicht selten. Damit stellen Datenbanken ein relativ leichtes Ziel für Angreifer dar.

Schutz sensibler Informationen

Um sensible Informationen zu schützen, steht als erstes eine Aufnahme der Datenbanksysteme und aller Datenbanken an. Sind diese bekannt, lassen sich Sicherheitsaudits und -reviews auf den technischen und organisatorischen Ebenen durchführen und notfalls Sofortmassnahmen einleiten. In vielen Fällen ist eine anfänglich gut konzipierte und implementierte Datenbank im Lauf der Zeit so weit "verkonfiguriert" worden, dass sich die Ursachen von Performanceproblemen kaum noch lokalisieren lassen. Die konsequente Einführung oder Überarbeitung des Change-Managements braucht allerdings Zeit und muss daher frühzeitig begonnen werden. Es müssen dabei nicht nur die Change-Fenster, sondern auch die Inhalte der Changes bekannt sein und hinsichtlich Durchführung und Ergebnis überwacht werden.

Bereits die Überprüfung und Kontrolle der Datenbank-Konfigurationen können über den Standardisierungseffekt zu Einsparungen an Zeit und Geld führen. Dasselbe gilt für die Überarbeitung des Berechtigungssystems und des User- und Rollenmanagements. Je besser die Einhaltung des Prinzips der minimalen Berechtigungen funktioniert, desto weniger können versehentliche Änderungen Zeit und Nerven kosten. Die eingesparte Zeit lässt sich darauf verwenden, um nach der Inventarisierung der Datenbanken die Identifizierung der kritischen Daten oder eine umfassende Datenklassifizierung in Angriff zu nehmen. Die extrem kritischen Daten sind meist vorher schon bekannt – für sie könnte sofort mit der Datenbank-Verschlüsselung begonnen werden.

Die entscheidenden Maßnahmen liegen in der Dokumentation der Datenhaltung und im Bereich Security Monitoring. Dabei sind in erster Linie alle hochprivilegierten Aktivitäten zu überwachen, die zu Änderungen an Zugriffsrechten führen können. Das gilt natürlich insbesondere für Drittfirmen

und Entwickler auf Produktivsystemen. Grundsatz für das Security Monitoring ist dabei die Forderung, dass die Überwachung nicht von den Überwachten selbst vorgenommen oder verändert werden darf. Dem entspricht am besten ein zentrales, übergreifendes und externes Monitoring; die Anforderungen an die Selbstüberwachung sind ansonsten nur schwer realisierbar. Erst mit einem zweckmäßigen Security Monitoring ist es möglich, laufend und effizient die notwendigen Fakten für die konkrete Beurteilung des Risikos zusammenzutragen. Fünf Sofortmaßnahmen bieten sich jedoch bereits zu Beginn an:

1. Mit relativ wenig Aufwand lässt sich die Qualität der Passwörter prüfen, um Enumerationsattacken vorzubeugen. Gründlicher wirkt allerdings die Einführung von modernen und komfortablen Authentifizierungstechniken.
2. Entfernung der Default-Einstellungen, vor allem der Default-Accounts und -Passwörter.
3. Einführung eines Prozesses für die Einhaltung von kritischen Fristen für Security-Patches.
4. Regelmäßiges Durchführen von technischen und organisatorischen Audits und konsequente Einführung eines Systems für die laufende Überwachung und die Bereitstellung von Entscheidungsdaten für die Betriebsoptimierung.
5. Überarbeitung der Anwendungssicherheit, vor allem bei Webanwendungen, und Kapselung der Datenbanksysteme mit Paketfiltern und geeigneten Proxys.

Parallel mit der Durchführung dieser Sofortmaßnahmen wird die Sicherheit der Datenbanken stufenweise auf ein angemessenes Niveau angehoben. Es hat sich in den letzten Jahren ein eigener Markt für spezielle Database-Security-Systeme entwickelt, die eine Vielzahl der geforderten Sicherheitsfunktionen konsolidiert und effizient erbringen können.

Technologien im Bereich Datenbanksicherheit

Die Aufgabenfelder für die Datenbanksicherheit sind im Wesentlichen:

1. Discovery und Analyse der Datenbanken
2. Patchen und sichere Konfiguration
3. Berechtigungssystem
4. Verschlüsselung der sensiblen Inhalte
5. Überwachung der Administration und sensibler Zugriffe
6. Prävention und Blocking-Mechanismen in Echtzeit
7. Compliance herstellen und reporten

Mittels aktivem und passivem Discovery-Scanning (Prüfung auf laufende Services im Netz) werden zunächst im Rahmen einer Datenbank-Inventarisierung die Serveradressen erkannt, auf denen sich Datenbanken befinden. Um zu vermeiden, dass ein aktives Scanning zu einer Störung der Infrastruktur führt, lesen die Systeme die Serveradressen aus dem Netztwerkverkehr der Datenbank-Kommunikation passiv aus. Für diese Aufgabe eignen sich auch bereits bestehende IDS/IPS- oder NBAD-Systeme (Network Behavior Anomaly Detection). Für die weitere Analyse der identifizierten Serversysteme werden Credentials übergeben, mit denen sich die einzelnen Datenbanken und deren Struktur analysieren lassen. Dazu werden an den Server oder an das Datenbankmanagement-System geeignete Abfragen per Data Definition Langauge (DDL) gestellt. Intelligente Datenbank-Monitoring-Systeme können anhand von Datenmustern den Benutzer bei der Interpretation der Datenbankfelder unterstützen.

Patchen und sichere Konfiguration

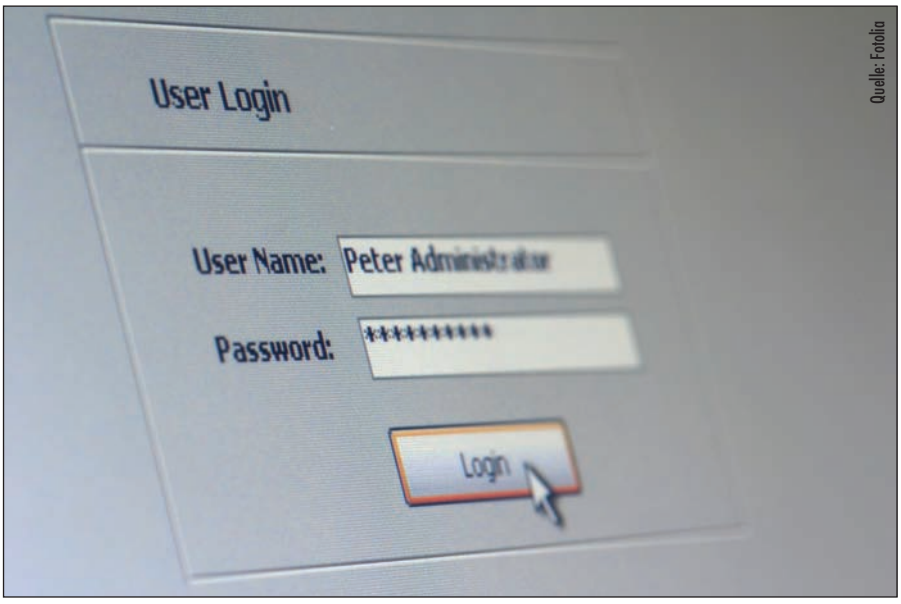
Bei fast allen Datenbankservern lohnt es sich, nach technischen Software-Schwachstellen auf den verschiedenen Ebenen, vom Betriebssystem bis zur Datenbanksoftware, zu suchen. Das kann ebenfalls in einem eigenen Arbeitsschritt von geeigneten aktiven Scanner-Systemen übernommen werden. Das Auffinden von Konfigurationsschwachstellen lässt sich teilweise mit Konfigurations- und Change-Management-Systemen durchführen, soweit diese über ausreichende Datenbank-Intelligenz verfügen. Datenbankinterne Konfigurationsfehler werden von speziellen Database-Security-Systemen über DDL-Abfragen ermittelt. Die Fehler in den Zugriffsberechtigungen können nur von geeigneten Datenbank-Auditierungs-Systemen gefunden werden. Das geschieht vor allem ebenfalls über DDL-Abfragen, meist im selben Arbeitsschritt wie das Auffinden der Konfigurationsfehler. Für die Problembehebung werden Korrekturhinweise in unterschiedlicher Qualität abgegeben.

Die Untersuchungsarbeiten bis hier sind mit relativ geringem Aufwand verbunden und in kurzer Zeit umsetzbar. Die Ergebnisse sollten aber nur von erfahrenen Datenbank-Administratoren in Zusammenarbeit mit den Security-Spezialisten umgesetzt werden. Bereits in Testprojekten können auf diese Weise wichtige verwertbare Ergebnisse erzielt werden.

Verschlüsselung und Zugriffskontrolle

Die Verschlüsselung von Datenbanken erfordert etwas mehr Aufwand. Vor allem muss sichergestellt sein, dass unter Last keine Performance-Einbußen auftreten. Eine transparente Verschlüsselung der gesamten Datenbankinhalte wirkt vor allem gegen Angriffe auf Systemebene und bei Nachlässigkeiten im Umgang mit den Speichermedien. Verschlüsselung kann zudem eine sehr gute Prävention gegen missbräuchliche Zugriffe und gegen Datendiebstahl sein, wenn sie richtig eingesetzt wird. Für eine gezielte Verschlüsselung der sensiblen Daten gilt es, diese Inhalte aber überhaupt zu identifizieren.

Gute Verschlüsselungsprodukte sind zwar begrenzt in der Lage, Aktivitäten der Datenbank-Administratoren aufzuzeichnen oder zu melden. Das Security-Monitoring der Datenbanken durch ein Audit-Modul des Datenbank-Managementsystems selbst führt jedoch sehr oft zu Performance-Problemen und wird zunehmend durch die externe Auditierung



Ungeänderte Default-Passwörter sind ein Einfallstor für Angreifer

abgelöst. Ein solches externes Database-Activity-Monitoring erfolgt über die Analyse des Netzwerktraffics. In der Datenbank-Kommunikation werden alle Abfragen und Aufrufe an die Datenbanken ermittelt und ausgewertet. Es lassen sich damit alle wichtigen Datenbanken einbeziehen und das Monitoring erfolgt weitgehend neutral gegenüber den DBMS-Herstellern. Die ermittelten Daten sind nicht von Netz-, System- oder Datenbankadministratoren beeinflussbar.

Die Grenzen dieses netzbasierten Database-Monitorings liegen dort, wo die Kommunikation anwendungsspezifisch kodiert oder verschlüsselt erfolgt. Dann bleibt nur die Unterstützung durch Host-basierte Agenten. Diese greifen die systeminterne Kommunikation ab und können zusätzlich noch die Aktivitäten auf Betriebssystem-Ebene überwachen. Die Performance-Auswirkungen der Agenten liegen bei etwa drei bis fünf Prozent CPU-Leistung. Das vollständige Monitoring der Datenbankzugriffe und des Status der Datenbanksysteme führt meist zu wertvollen Hinweisen, die von diesen sofort zur Analyse von bestehenden Problemen in den Bereichen Sicherheit, Konfiguration, aber auch Performance verwendet werden.

Prävention und Blocking-Mechanismen in Echtzeit

Wenn bei einem Zugriff eindeutige Hinweise auf einen Missbrauch oder auf mögliche negative Konsequenzen für die Datenbanken erkennbar sind, kann die Policy fordern, dass diese Zugriffe sofort unterbunden werden. Möglichkeiten bestehen auf Netzebene, teilweise auf Systemebene, vor allem auf der Datenbankebene. Diese Blocking-Maßnahmen können remote vom Database-Security-System aus oder über die Hostagenten direkt auf dem System ausgeführt werden. Response-Policies bedürfen in jedem Fall einer exakten Analyse und Planung.

Fazit

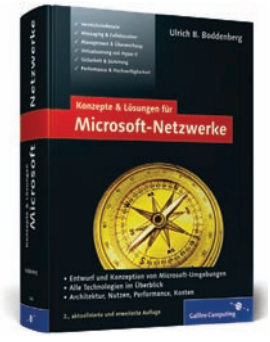
Werden die vorgenannten Technologien mit dem Wissen über die Forderungen von Compliances oder Standards kombiniert, können beim Auditieren der Datenbank oder beim Activity-Monitoring Abweichungen festgestellt und berichtet werden. Solche Berichte können vor allem für eine gute Vorbereitung von Compliance-Prüfungen eingesetzt werden. Mit den beschriebenen Techniken könnten auch automatisiert Korrekturen von Compliance-Verstößen herbeigeführt oder Abweichungen verhindert werden – die notwendige Sorgfalt vorausgesetzt.

Ein großer Teil der aufgeführten Maßnahmen kann teilweise mit vorhandenen Bordmitteln durchgeführt werden. Allerdings sind der zeitliche Aufwand und der Bedarf an speziellem Wissen über Datenbanksicherheit ohne Einsatz von Spezialsystemen relativ hoch. Die Inventarisierung der Datenbankserver ist bei einem funktionierenden Asset-Management oder einer zentralen, laufend aktualisierten CMDB vielleicht bereits umgesetzt. Die Inventarisierung der Datenbanken und deren Inhalte könnten aus einem zentralen Data-Repository ausgelesen werden. Bei einem gepflegten Schwachstellen-Management und einem Changemanagement-System kann man davon ausgehen, dass man sich auf die Datenbank-Konfigurationen und -Schwachstellen konzentrieren kann. Eine Analyse der sensiblen Inhalte und der Berechtigungssysteme der Datenbanken, wie sie für eine gezielte Datenbank-Verschlüsselung gebraucht werden, erfordert allerdings dann doch meist hohen Beratungsaufwand. Für viele Projekte besteht aber die eigentliche Schwierigkeit darin, die Performanceprobleme der herstellerspezifischen internen Audit-Möglichkeiten in den Griff zu bekommen, von den Problemen der Evidenzsicherung abgesehen.

Es ist sicher vernünftig, sich gerade in schwierigen Zeiten um die Sicherheit der zentralen und sensiblen Daten zu kümmern. Es ist daher zu erwarten, dass es in absehbarer Zeit zunehmende Compliance-Anforderungen von Seiten der Finanziers, Partner, Kunden oder sogar der Öffentlichkeit geben wird. Der vernünftige Weg im Bereich Datenbanksicherheit geht in die Richtung von konsolidierten und effizienten Spezialsystemen, mit denen schnell deutliche Sicherheitsgewinne und Betriebsvorteile bei den Datenbanken nachgewiesen werden können. *(dr)*

Uwe Maurer ist CISSP, Business Development Manager Security Operations bei Integralis.

Konzepte und Lösungen für Microsoft Netzwerke



Die zweite Auflage von Ulrich Boddenbergs Wälzer zu Microsoft-Netzwerken ist mehr als doppelt so dick wie der Vorgänger. Potenzielle Leser sollten sich allerdings über den Fokus des Buchs im Klaren sein: Der Autor balanciert auf einem schmalen Grat zwischen Konzepterklärung und technischer Anleitung. Was sich nach Unentschlossenheit anhört, ist tatsächlich eine sehr gelungene Mischung. Im Gegensatz zur ersten Ausgabe ist das Buch sehr viel technischer geworden, ohne in einer reinen Featureaufzählung zu versanden. Mit "Konzepte und Lösungen für Microsoft Netzwerke" kann eigentlich jeder etwas anfangen – der erfahrene Admin, der nach einer neuen Virtualisierungslösung sucht, ebenso wie ein technisch unerfahrener, aber IT-affiner Manager.

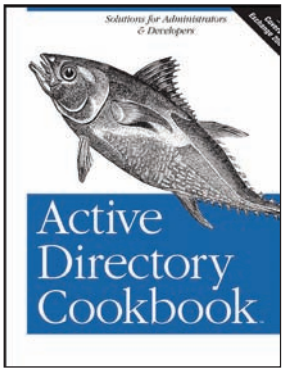
Den Anfang des Buchs machen eher theoretische Gedanken zu Entwürfen und Konzepten aus: Wie muss Hardware dimensioniert werden, welche Systeme gibt es überhaupt von Microsoft, wo sind die historischen Wurzeln. Boddenberg sieht das große Ganze, nicht nur den Server, und scheut vor klaren Ansagen nicht zurück. So hat er eine ziemlich kritische Meinung zu Storage Area Networks und IPv6, die er bei kleinen und mittleren Firmen selten gerechtfertigt sieht. Dabei schafft er es, bei vielen Aspekten so abstrakt zu bleiben, dass nicht nur reine Microsoft-Anwender etwas vom Thema haben. Trotzdem bleibt er auch konkret genug, um eine echte Hilfe im Alltag zu bieten. Ein schönes Beispiel sind seine Erklärungen zu Performance und Dimensionierung von RAID-Systemen. Wer diesen Abschnitt gelesen hat, geht deutlich aufgeklärter in die nächste Verhandlung mit dem IT-Systemhaus. Und so arbeitet sich das Buch durch Aspekte wie Verzeichnisdienste, Zusammenarbeit, Kommunikationsprotokolle, Virtualisierung, Sicherheit und Management bis zu Hochverfügbarkeit und Mobilität. Produkte werden erklärt, die Installation und Anwendung in einer Tiefe besprochen, mit der Administratoren gut klar kommen, auch wenn sie das Produkt selbst nicht kennen.

Fazit: Ein sinnvolles Buch für jeden, der Microsoft-Netzwerke einsetzen, erweitern oder optimieren will. Der Autor geht nicht bis ins letzte Detail der Produkte ein, erklärt aber genug, damit technische Manager informierte Entscheidungen treffen und Administratoren erste Erfahrungen im Einsatz sammeln können.

Elmar Török

Autor:	Ulrich B. Boddenberg
Verlag:	Galileo Computing
Preis:	69,90 Euro
ISBN:	978-3-8362-1356-1
Bewertung:	★★★★★

Active Directory Cookbook



Dass ein O'Reilly-Kochbuch dicker ist als der Standardtitel zum Thema selbst, kommt nicht oft vor. "Active Directory Cookbook" sticht aus der Kochbuch-Reihe hervor. In diesen Titeln gibt es keinen durchgängigen Fließtext: Zu einem Problem wird eine Lösung beschrieben, dann geht es mit dem nächsten Problem weiter. Die ziemlich genau 1.000 Seiten des englischsprachigen "Active Directory Cookbook" kommen durch zwei Umstände zustande: Zum einen ist Active Directory nach wie vor ein extrem umfangreiches Thema. Die meisten Administratoren haben nur mit einem winzigen Teilbereich zu tun, zumindest solange alles ordnungsgemäß läuft. Zum anderen geben die Autoren zu jedem Problem bis zu vier Lösungswege an. Der Leser hat die Wahl, ob er per graphischer Benutzeroberfläche, Kommandozeile, VBScript oder PowerShell an die Lösung herangeht.

Gerade bei der Verwaltung sehr großer Active Direcory-Verzeichnisse werden die Admins dankbar auf die Automatisierung zurückgreifen. Und durch den enormen Einsatz der Autoren gibt es auch praktisch nichts, was im Buch fehlen würde. Die Bandbreite der Kochrezepte reicht vom Erstellen der Bäume, Domänen und Vertrauensstellungen über die Manipulation von Objekten jeglicher Art, Gruppenrichtlinien und Schemas bis hin zur Exchange Integration und dem Microsoft Identity Lifecycle Manager. Was Robbie Hunter und Laura Allen nicht schaffen, ist innerhalb der Kochrezepte so etwas wie einen Lesefluss herzustellen. Die Anleitungen haben eine kurze bis sehr kurze Einführung, dann geht es an die Lösung. Spaß macht so ein Buch nicht gerade, doch durch den Verzicht auf jede überflüssige Zeile, haben auch Leser mit mittelmäßigen Englischkenntnissen keine Probleme. Ein VBScript sieht nun mal auf Deutsch und auf Englisch ziemlich ähnlich aus.

Fazit: Unverzichtbar für jeden Vollzeit Active Directory-Administrator. Schneller und klarer lassen sich die vielfältigen Probleme und Aufgaben rund um den Verzeichnisdienst nicht lösen. Für Einsteiger und Gelegenheitsadmins sind die 1.000 Seiten nur bedingt geeignet. *Elmar Török*

Autoren:	Robbie Hunter, Laura Allen
Verlag:	O'Reilly
Preis:	47,95 Euro
ISBN:	978-0-596-521103
Bewertung:	★★★★☆

www.python-forum.de

Programmierer unter sich

Phyton genießt als plattformübergreifende Skriptsprache inzwischen große Beliebtheit. Insbesondere der Einstieg fällt verhältnismäßig leicht und die Skripte laufen unter Windows, Linux und Mac OS. Entstanden ist die Sprache 1995, wobei sich die Entwickler die Rosinen aus zahlreichen Skriptsprachen herauspickten. Python selbst ist dabei klein, fast schon minimalistisch geblieben. Auf dem relativ kleinen Kern der Sprache baut dennoch eine große Zahl von Modulen auf, die Python für Anwendungen attraktiv machen: Vom Webbrowser über XML-Parsing bis zur E-Mailverarbeitung ist alles dabei. Das gilt auch für alle Schnittstellen zum Betriebssystem zur Netzwerkprogrammierung, Operationen auf dem Dateisystem, Ausführung externer Kommandos et cetera.

Inzwischen liegt Python in Version 3 (genauer: 3.1) vor und stellt die Nutzer damit vor zahlreiche Syntaxänderungen und einer bewusst fehlenden Abwärtskompatibilität zur 2er-Version. Das wirft nicht nur bei Anfängern Fragen auf, sondern stellt auch erfahrene Programmierer vor die Aufgabe, ihren Code anzupassen. Eine Möglichkeit, sich mit Gleichgesinnten über die Skriptsprache auszutauschen, bietet das Python-Forum. Dort finden die Besucher in knapp 140.000 Beiträgen Informationen zu quasi allen Aspekten der Sprache – angefangen bei der Installation und Konfiguration, über Webprojekte hin zur Datenbankprogrammierung. Über 6.000 angemeldete User stehen dabei Rede und Antwort und das meist innerhalb weniger Tage oder sogar noch am gleichen Tag.

Doch nicht nur mit rein technischen Grundlagen befasst sich das Forum. So haben die Nutzer die Möglichkeit, sich über Projekte und Ideen auszutauschen und damit die Sprache in einen praktischen Kontext zu stellen. Die Projekte befassen sich überwiegend mit unterhaltenden Themen, wie etwa der Spieleprogrammierung. Nichtsdestotrotz findet auch der geneigte Admin die ein oder andere Anregung, wenn es um die CMS-Programmierung oder die Mailverarbeitung geht. Dass es sich im Forum um wahre IT-Spezialisten handelt, beweist übrigens die Rubrik "Offtopic". Außer IT-Themen findet sich hier kaum Geplauder aus dem Alltag. *(dr)*

Das Python-Forum unterstützt Programmierer im Umgang mit der Skriptsprache

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:**

Anwenderbericht: Datensicherung bei der Wilhelm Gronbach GmbH

Gerade einmal sechs Mitarbeiter betreuen an verschiedenen Standorten mehr als 300 Rechner. Die Palette der zu sichernden Applikationen könnte vielfältiger kaum sein: Die Daten von CAD- und Office-Applikationen werden an jedem Standort auf einem eigenen Linux-Fileserver gespeichert. Die Betriebsdatenerfassung nutzt eine Microsoft SQL-Datenbank und das Qualitätsmanagement vertraut auf Oracle. Lesen Sie in unserem Anwenderbericht, mit welcher Backup-Strategie die Admins für eine unternehmensweite Datensicherung sorgen.
www.it-administrator.de/themen/netzwerk-management/fachartikel/63281.html

Nutzungspotentiale von Configuration Management

Datenbanken zum Konfigurationsmanagement (CMDB) sind Themen, die nicht nur im Rahmen von ITIL-Projekten in die IT-Abteilungen hineingetragen werden. In unserem Online-Fachartikel klären wir Begrifflichkeiten und beleuchten die Nutzenpotenziale entsprechender Systeme. Außerdem geben wir Empfehlungen zum Funktionsumfang für die Auswahl von Lösungen. Tipps aus der Praxis geben wertvolle Hinweise für die erfolgreiche Projektarbeit.
www.it-administrator.de/themen/netzwerk-management/fachartikel/63282.html

(Rechts)sichere E-Mailkommunikation

Die E-Mail ist aus dem Geschäftsalltag nicht mehr wegzudenken. Verfügbarkeit, Integrität und Vertraulichkeit sind dabei die maßgeblichen Elemente sicherer E-Mailkommunikation. Unser Online-Artikel beleuchtet den Einfluss von Verschlüsselung und Signatur auf die genannten Eckpfeiler und erklärt, in welcher Situation welche Art von Verschlüsselung möglich und sinnvoll ist.
www.it-dministrator.de/themen/kommunikation/fachartikel/63283.html

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

»Komplexität und Dynamik sind unser Alltagsgeschäft«

Carsten Lucau (31) arbeitet im IT-Team der SPH AG als Systemingenieur und IT-Administrator. Das Stuttgarter Systemhaus bietet CRM- und ERP-Systeme für den Versandhandel an. Als ASP- und SaaS-Dienstleister für seine Kunden ist das Unternehmen zwingend auf die stabile Infrastruktur seiner Rechenzentren angewiesen.

Welche Ausbildung haben Sie gemacht?

Nach der Schule entschied ich mich für das Studium der Informationstechnik an der Berufsakademie Stuttgart. Berufsbegleitend besuche ich momentan den darauf aufbauenden Masterstudiengang Wirtschaftsinformatik.

Warum sind Sie IT-Administrator geworden?

Ich hatte schon früh ein großes Interesse an der Technik. Mir macht es Spaß mit komplexen Systemen und ihren ständig wechselnden Anforderungen zu arbeiten.

Welche IT-Umgebung betreuen Sie aktuell?

Für die eigene IT von SPH sowie für das externe Projektgeschäft arbeite ich als Systemingenieur innerhalb eines IT-Teams. In unserem redundant ausgelegten Rechenzentrum betreuen wir derzeit rund 30 Server sowie etwa 50 Clients.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir nutzen Paessler, den Microsoft Systems Management Server sowie den IBM Systems Director und decken damit alle Aufgabengebiete ab.

Welche Ihrer Systeme sind hochverfügbar ausgelegt?

Da unser Geschäftserfolg von der Performance und der Verfügbarkeit unserer IT-Infrastruktur abhängt, sind alle Produktivsysteme hochverfügbar.

Welches HA-System setzen Sie ein?

Wir nutzen dafür die Bordmittel der jeweiligen Hersteller, also Windows Cluster, MS SQL-Server Mirroring et cetera.

Welches war Ihr längster Serverausfall und was war der Grund dafür?

Einer unserer älteren RAID-Controller ist vor geraumer Zeit für mehr als vier Stunden ausgefallen. Das hat den Betrieb gestört und zu Beeinträchtigungen in den Abläufen geführt.

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

In unserem Job haben wir es mit hochkomplexen Anforderungen zu tun. Es ist tagtäglich eine Herausforderung, diese mög-

Geburtstag: 15.05.1978
Familienstand: verheiratet
Hobbys: Wandern, Klettern, Bogensport

Carsten Lucau, IT-Administrator

lichst effizient mit den technisch verfügbaren Möglichkeiten der IT im Rahmen des vorgeschriebenen Budgets umzusetzen.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Für einen größeren Kunden bereiten wir eine ERP-Installation auf Basis von Microsoft Dynamics AX 2009 vor. Das ist eine komplexe Angelegenheit, die sehr viel Sorgfalt verlangt.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mit gefällt die hohe Dynamik und Verantwortung, die die Aufgaben mit sich bringen. Dazu kommen interessante Kundenkontakte und natürlich immer wieder der Umgang mit neuen Technologien.

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

Standardaufgaben, wie Updates, das Patchmanagement und die Wartung gehören nicht unbedingt zu meinen Favoriten.

Was tun Sie für Ihre Fort- und Weiterbildung?

Ich nehme regelmäßig an Schulungen beziehungsweise Zertifizierungen teil. Dann lese ich diverse Fachzeitschriften und besuche Internetportale.

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

Vor Jahren machte ich ein SQL-Update mit fehlender "WHERE"-Klausel. Danach waren mehr Sätze geändert als ursprünglich geplant. Allerdings konnte der Fehler schnell behoben werden und die Sache hatte ein Happy-End.

Was war Ihr größter Erfolg als IT-Administrator?

Auf die Konsolidierung unserer eigenen IT-Infrastruktur bin ich stolz. Davon profitieren sowohl unsere Mitarbeiter als auch unsere Kunden.

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

Ein älterer Anwender hat wegen eines nicht starten wollenden neuen PCs einen telefonischen Hilferuf abgesetzt. Nach minutenlanger Recherche kam dann heraus, dass er den an der Vorderseite angebrachten Ein/Aus-Schalter nicht gefunden hat und stattdessen wild auf dem Produktlogo des PC-Herstellers herumdrückte.

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

Eine der größten Herausforderungen sind die immer dynamischeren Anforderungen im Dienstleistungsbereich. Diesen müssen wir deutlich zeitnaher und kosteneffektiver entgegentreten. Dabei gilt es, die Vielschichtigkeit und Komplexität von Systemen mit weniger Aufwand zu verwalten, um letztendlich als serviceorientiertes Profitcenter dem Unternehmen einen Mehrwert liefern zu können.

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 9/09 erscheint am 4. September 2009

Schwerpunktthema:

Drucker- und Peripheriemanagement

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

Unsere Ausgabe im **Oktober** dreht sich um **Storage**. In einem Test nehmen wir unter anderem die SAN-Managementlösung "SANmelody" unter die Lupe. Daneben lesen Sie in unseren Workshops, worauf es bei der SAN-Konzeption ankommt und welche Neuerungen der Server 2008 R2 mitbringt.

Als Schwerpunkt im **November** folgt dann das Thema **IT-Desaster-Management**.

***Im Vergleichstest:* USB über das Netzwerk**

***Im Test:* Druckermanagement mit PaperCut**

***Workshop:* Professionelle Druckerverwaltung mit CUPS**

***Workshop:* Druckertreiberisolierung unter Server 2008 R2**

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Andreas Badur, Dr. Jürgen Fechter, Jürgen Heyer, Nils Kaczenski, Bodo Mainz, Uwe Maurer, Neil Own, Dr. Holger Reibold, Walter Steinsdorfer, Elmar Török, Thomas Weyergraf

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

Es gilt die Anzeigenpreisliste Nr. 6 vom 01.01.2009

LAC/2008

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

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

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

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

Erscheinungsweise
monatlich

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

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Internet
www.it-administrator.de

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

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

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

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

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

INSERENTENVERZEICHNIS

Das IT-Administrator Komplettprogramm!

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

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

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

Als bestehender Jahresabonnent können Sie hier upgraden:

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

Oder Sie sind Neukunde? Hier können Sie bestellen:

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

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

Temperaturen rauf – Preise runter!

1&1 Sommer-Aktion:

1&1 HOMEPAGE PERFECT

2 Domains inklusive

Wählen Sie aus: .de, .com, .net, .org, .biz, .info, .name, .at, .eu!

- 1 GB Speicherplatz
- 200 E-Mail Adressen mit je 2 GB Postfach
- 100 GB Transfervolumen/Monat
- Adobe® Photoshop Elements
- Blog und Fotoalbum
- Click & Build Applikationen (Joomla, MediaWiki,...)
- MySQL-Datenbank
- Suchmaschinen-Tools
- 24/7 Profi-Hotline
- ... und vieles mehr!

Nur bis 31.08.:

1 Jahr lang 0,– €/Monat*

Danach 6,99 €/Monat.

~~6,99 €/Monat~~

Aktuelle % Spar-Angebote

Außerdem ständig weitere Preis-Aktionen im Internet:

z. B. viele Domains jetzt supergünstig und ohne Einrichtungsgebühr!

*0,– € im ersten Jahr, danach 6,99 €/Monat. Einmalige Einrichtungsgebühr 9,60 €. 24 Monate Mindestvertragslaufzeit. Versandkosten bei Softwarebestellung 6,– €. Preise inkl. MwSt.

MEMBER OF united internet

Jetzt informieren und bestellen unter:

01805 / 001 535 14 ct/Min. dt. Festnetz, Mobilfunktarife ggf. abweichend

www.1und1.info

1&1