05/2011 € 12,60 ISSN 1614-2888

IT-ADMINISTRATOR.DE

iladministrator

Magazin für professionelle System- und Netzwerkadministration

NEU am Kiosk

Server-based Computing

4 196583 212605 05

Intelligente Technologien für einen smarten Planeten

Was bedeuten 27.383 Berechnungen pro Sekunde für diesen Stromzähler?

Sie bedeuten, dass dieser Zähler 24-mal am Tag abgelesen wird statt einmal im Monat. Für die Verbraucher bedeutet es mehr Transparenz, was ihren Energieverbrauch angeht. Und die Versorgungsunternehmen sehen, wie Energie genutzt wird. eMeter arbeitet mit IBM zusammen und nutzt dabei Power Systems™, IBM Anwendungs- und Servicemanagement-Lösungen, um es Versorgungsunternehmen zu ermöglichen, Daten von über 20 Millionen intelligenten Zählern stündlich abzulesen – und übertrifft damit die Benchmarks der Branche mehr als viermal.[1] Ein smartes Unternehmen braucht intelligente Software, Systeme und Services.

Machen wir den Planeten ein bisschen smarter. **ibm.com**/meter/de

Hier werden die Daten sichtbar gemacht, die mit eMeter in einem durchschnittlichen Haushalt pro Jahr abgelesen werden.

[1]Basierend auf den veröffentlichten Benchmark-Resultaten vom 13.09.2010. Quelle: IBM Presseerklärung http://www-03.ibm.com/press/us/en/pressrelease/29315.wss und eMeter Presseerklärung http://www.emeter.com/2009/emeter-demonstrates-industry%E2%80%99s-most-scalable-smart-grid-management-capability/. IBM, das IBM Logo, ibm.com, das Bildzeichen des Planeten und IBM Power Systems sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Andere Namen von Firmen, Produkten und Dienstleistungen können Marken oder eingetragene Marken ihrer jeweiligen Inhaber sein. O&M IBM CA 12/10

EDITORIAL

Bist du aber groß geworden!

Liebe Leser,

wohl jede Generation kennt diesen Spruch nur allzu gut aus der eigenen Kindheit – ist die wieder einmal gestiegene Körpergröße doch immer ein beliebtes Thema auf Familienfeiern. Dass nicht nur Kinder, sondern auch Magazine in die Höhe wachsen können, beweist nun die aktuelle Mai-Ausgabe des IT-Administrator. Das Heft ist nämlich größer geworden, oder eben besser gesagt: höher. Unterm Strich bedeutet das für Sie acht Seiten mehr Platz für praxisnahe Inhalte – zwei ganze Artikel. Diese finden Sie übrigens in unserem neuen Inhaltsverzeichnis jetzt noch übersichtlicher sortiert.

Im Rahmen unserer Layout-Anpassung ist es natürlich auch an der Zeit, Danke zu sagen. So dürfen wir uns weiterhin über treue Leser und steigende Abonnenten-Zahlen freuen. Immer mehr von Ihnen engagieren sich zudem in unseren sozialen Netzwerken auf Xing, Facebook und Twitter. Sie verfolgen online, was der IT-Administrator zu bieten hat und geben hilfreiches Feedback zu unseren Inhalten. Das zeigt uns, dass Sie unser Heft gerne lesen und in Ihrem Arbeitsalltag darauf bauen – ein Ansporn für uns, noch besser zu werden.

Aber nun zu unserem Schwerpunktthema im Mai. Die zurückliegende CeBIT hat bewiesen: Das Thema Cloud Computing ist längst bei den Firmen und Anbietern angekommen. War die Cloud vor ein paar Jahren noch ein großes Hype-Thema, ist inzwischen Pragmatismus eingekehrt. Wo sie sinnvoll nutzbar ist und dem Unternehmen Geld und Arbeit spart, warum nicht!? Auch die Anbieter sind dazu übergegangen, das Thema differenzierter anzugehen. Nicht mehr alles muss in die Cloud und wird in zehn Jahren in der Cloud sein, sondern nur noch das, was das Unternehmen wirklich weiterbringt. Gut so.

Natürlich bedeutet Cloud Computing nicht nur fußballfeldgroße Rechenzentren auf der grünen Wiese, sondern auch eigene, kleine Rechenwölkchen – die Private Clouds. Hier helfen Virtualisierungs- und Terminalserverlösungen weiter, die sich gerade in großen Umgebungen auf mehrere Server verteilen. Lesen Sie in dieser Ausgabe, wie Sie RemoteApps unter Windows Server 2008 verteilen und wie sich Veränderungen der Terminalserver-Infrastruktur auf die Performance auswirken. Daneben zeigen wir Ihnen, auf welchem Weg Sie Postfächer über verschiedene Exchange-Strukturen hinweg verschieben. In unseren Tests beweisen das neue Xen Desktop 5 sowie der 2X Application Server ihr Können.

Viel Spaß beim Lesen,
Ihr

Daniel Richey
Stellv. Chefredakteur

Server-based Computing

Im Test: Citrix XenDesktop 5

Mit XenDesktop 5 hat Citrix im Dezember 2010 die jüngste Version der hauseigenen Infrastruktur zur Bereitstellung virtueller Desktops vorgelegt. Dieses Release bricht mit der Tradition der Vorgängerversionen und setzt auf eine von Grund auf neugestaltete Architektur. IT-Administrator hat sich angesehen, welche Neuerungen dies für Sie als Administrator mit sich bringt.

Seite 24

Terminaldienste mit X2go bereitstellen

Freie Terminallösungen gibt es inzwischen wie Sand am Meer, doch längst nicht jedes Open Source-Werkzeug bietet den gewünschten Komfort und die notwendige Funktionalität. X2go, eine bislang vergleichsweise wenig beachtete Lösung, verfügt über einen ausgesprochen großen Funktionsumfang. In diesem Workshop setzen wir eine X2go-Umgebung mit Basissystem und Clients auf und richten anschließend eine Infrastruktur mit mehreren X2go-Servern ein.

Seite 30

AKTUELL

PRODUKTE

PRAXIS

WISSEN

RUBRIKEN

Microsoft RemoteApps einrichten

Mit den RemoteApps bieten die Terminaldienste unter Windows Server 2008 und 2008 R2 die Möglichkeit, einzelne Anwendungen auf einem Client so darzustellen, als seien sie lokal installiert. Der Workshop führt Sie Schritt für Schritt durch die Einrichtung und zeigt auf, wie mit dem Remotedesktopgateway auch von extern ein sicherer Zugriff möglich ist.

Seite 36

Einstieg in das Cloud Computing

Durch die sich ständig erweiternde Palette an Produkten und Dienstleistungen zahlreicher Anbieter wurde der anfängliche Cloud-Hype von konkreten, nützlichen Angeboten abgelöst. Cloud Computing repräsentiert ein Servicemodell, bei dem auf Ressourcen wie Rechenleistung, Speicherplatz, Applikationen und andere Arten von Services on Demand zugegriffen wird. Auf Basis des Pay as you Go-Modells werden dabei nur die Ressourcen berechnet, die zu einem Zeitpunkt auch tatsächlich genutzt werden. Dieser Beitrag zeigt Wege auf, wie Unternehmen sich dieser Technologie sinnvoll annähern.

Seite 74

Themenübersicht

Leistungsfähige Microserver

Speziell für den Einsatz im **Web-Hosting** stellt **Dell** die dritte Generation seiner **Microserver** vor. Die neuen Microserver der **PowerEdge C5000-Serie** mit dem **PowerEdge C5125** und dem **PowerEdge C5220** ermöglichen die Verwendung von dezidierten Servern überall dort, wo eine Multi-Core-Architektur und eine umfangreiche Virtualisierung für den entsprechenden Einsatz überdimensioniert sind. Bei den Microservern der PowerEdge C5000-Serie passen acht bis zwölf Server in ein 3 HE hohes Chassis. Die Server sind hot-pluggable, womit ein Wechsel im laufenden Betrieb möglich ist. Das Management erfolgt über das standardisierte Intelligent Platform Management Interface (IPMI 2.0). Zur Auswahl stehen zwei Varianten: Der PowerEdge C5125 verfügt über eine 1S AMD AM3 CPU (Athlon II, Phenom II) auf einer "Buenos Aires"-Plattform (AM3-Sockel). Sein Intel-Pendant ist der PowerEdge C5220, der mit einer 1S Intel Sandy Bridge CPU auf Basis der "Bromolow"-Plattform (H2-Sockel) agiert. Beide Modelle haben neben vier DDR3-UDIMMS zwei 3,5-Zoll- beziehungsweise vier 2,5-Zoll-Laufwerke im SATA- oder SSD-Format. Bei der Intel-Version kommen optional auch SAS-Platten zum Einsatz. Zur Ausstattung gehören außerdem zwei GbE-Ports und iKVM (integrated Keyboard, Video, Mouse). Die Server verfolgen das "Individually Servicable Nodes"-Konzept, was bedeutet, dass sie einzeln

Richten sich an den Web-Hosting- und Cloud-Bereich: Die Microserver aus der PowerEdge C5000-Reihe

wartungsfähig sind. Die Stromversorgung und Kühlung der Server erfolgt zentral im Chassis. Dabei handelt es sich bei beiden Geräten um eine hocheffiziente Dual-Hot-Plug-Stromversorgung mit 1.400 Watt. Der Preis lag zu Redaktionsschluss noch nicht vor. *(dr)*

Dell: www.dell.com

Storage für den kleineren Geldbeutel

Die bisherigen Modelle **sayFUSE Backup** (Fast Universal Storage Engine) und **sayFUSE Smart Server** sind nun als Modelle **sayFUSE Backup 2000M** und **sayFUSE Smart Server 2000M** verfügbar. Mit diesen Varianten adressiert sayTEC Anwender mit kleineren IT-Budgets, die dennoch nicht auf die Vorteile und wesentlichen Funktionen der sayTEC-Lösungen verzichten möchten. Diese Modelle haben keinen TFT-Touchscreen und konnten laut Hersteller auch dadurch im Preis reduziert werden. sayFUSE Backup 2000 bietet zudem statt 4 GByte nur 2 GByte Speicher. Dagegen liefert das neue Modell sayFUSE Backup 3000M 4 GByte ECC-Speicher und soll damit eine hohe Datenintegrität gewährleisten. Bei den sayFUSE Smart Server Modellen 3000 und 3000M erhalten Anwender 16 GByte RAM, das ist doppelt so viel wie bei den Modellen 2000 und 2000M. sayFUSE Backup soll die Vorteile von Tape Backup und Disk Backup kombinieren. Die vollautomatische Komplettlösung für Datensicherung, Restore und Archivierung integriert die Backup Hardware, den Backup Server sowie die Backup- und Medien-Management Software in einem System und verwendet als Backupmedien Festplatten. Die sayFUSE Backup-Modellreihe startet mit einem Preis ab 3.900 Euro für sayFUSE 2000, das Modell 2000M kostet ab 4.900 Euro und das neue Modell 3000M ab 5.500 Euro. Der Preis für sayFUSE Smart Server 2000 beginnt bei 5.300 Euro, mit TFT-Touchscreen als Modell 2000M kostet er ab 5.700 Euro. Die Modelle 3000 und 3000M stehen ab 6.500 Euro beziehungsweise 6.900 Euro im Angebot. *(dr)*

sayTEC: www.saytec-solutions.de

Grüne Switches von D-Link

D-Link erweitert die **EasySmart Switch-Familie** um zwei neue GBit-Modelle mit integrierter D-Link Green-Technologie. Der **16-Port Switch DGS-1100-16** und das **24-Port Gerät DGS-1100-24** sind nach dem neuen **Energy Efficient Ethernet-Standard** (IEEE) genormt. Der Energieverbrauch passt sich demnach automatisch der Auslastung im Netzwerk an. Daten werden dabei in kürzester Zeit mit höchster Geschwindigkeit übertragen; die Ports benötigen nur während der Übermittlung Strom. Findet keine Datenübertragung statt, fallen die Ports automatisch in einen Schlafmodus, dessen Energiekonsum nahezu 0 Watt beträgt (Idle-Mode). Für den

Die neuen D-Link-Switches der DGS-1100-Reihe sollen besonders stromsparend arbeiten

Anschluss ans Netzwerk bieten die Geräte 16 beziehungsweise 24 GBit-RJ-45-Ports. Eine QoS- (Quality of Service) Priorisierung nach 802.1p sorgt mit vier Queues für die Sicherstellung der Übertragungsqualität. Daneben ist eine Segmentierung des LAN mit VLAN gemäß 802.1Q VLAN in bis zu 32 statische Gruppen sowie ein automatisches Surveillance-VLAN möglich. Die neuen 'EasySmart' Layer 2 Gigabit-Switches sind ab sofort im Fachhandel erhältlich. Der DGS-1100-16 mit 16 Ports kostet 215 Euro, für das 24-Port Modell DGS-1100-24 liegt der empfohlene Verkaufspreis bei 269 Euro. *(dr)*

D-Link: www.dlink.de

Schutzwall für KMUs

Netgear lässt mit der **UTM150** das neue Flaggschiff seiner **ProSecure UTM-Produktfamilie** vom Stapel. Die Appliance für Unified Threat Management schützt in klein- und mittelständischen **Unternehmen bis zu 150 Anwender** vor Gefahren aus Internet und E-Mail. Als All-In-One-Gerät kombiniert das Modell den Funktionsumfang von Proxy Firewall, VPN (IPSec und SSL), Anti-Virus, Anti-Spyware, Anti-Spam, Intrusion Prevention (IPS) und URL-Filterung. Der Administrationsaufwand soll durch grafische Reporting-Funktionen sowie automatisierte Updates für Software und Malware-Signaturen entscheidend reduziert werden. Die Appliance kann daneben dem Produktivitätsverlust der Mitarbeiter vorbeugen, indem sie unsachgemäße Online-Aktivitäten verhindert. Das unerwünschte und riskante Surfen auf bestimmten nicht-arbeitsrelevanten Internetseiten wie Social Media- oder Entertainment-Plattformen lasse sich demnach bereits auf Netzwerkebene unterbinden. Über die einfache Einrichtung von VPNs sollen zudem mobile Mitarbeiter oder externe Niederlassungen von einem zentralen Sicherheitskonzept profitieren. Die Netgear ProSecure UTM150 ist ab sofort verfügbar. Inklusive eines Abonnements für einen einjährigen Schutz vor Internet- und E-Mail-Gefahren ist die UTM150 für 1.369 Euro erhältlich. *(dr)*

Netgear: www.prosecure.netgear.de

Bietet UTM-Schutz für bis zu 150 Nutzer: Die Netgear-Appliance UTM150

Hochleistungs-NAS im Schrank

Synology stellt mit der **RS2211+** und **RS2211RP+** zwei neue hochleistungsfähige **RackStations** für den Business-Bereich vor. Die **2 HE 10-Bay NAS-Server** sind auf 22 Festplatten erweiterbar und bieten eine Übertragungsgeschwindigkeit von 12 GByte/s via InfiniBand. Die RackStations unterstützen in Verbindung mit den Erweiterungsmodulen RX1211/RX1211RP eine maximale Gesamtkapazität von 66 TByte. Die RackStations sind mit einem 1,8 GHz Dual-Core-Prozessor ausgestattet und verbrauchen laut Anbieter dank CPU-Untertaktung lediglich 115,5 Watt im Betrieb und im Festplatten-Ruhemodus mit 49,5 Watt 42 Prozent weniger Energie. Die Erweiterungsmodule RX1211/ RX1211-RP sparen durch den Tiefschlafmodus bis zu 90 Prozent Energie. Als Betriebssystem liefert der Hersteller den für den Business-Einsatz optimierten DiskStation Manager 3.1 (DSM 3.1) mit. Mit dem iSCSI-Support in DSM 3.1 bieten die RackStations eine nahtlose Speicherlösung für Virtualisierungsserver wie VMware vSphere, Citrix XenServer und Microsoft Hyper-V. Zusätzlich sind die Lösungen im Business-Umfeld mit Windows ADS und ACL kompatibel. Das Modell RS2211+ wird zu einem Preis von 1.499 Euro, die Variante RS2211RP+ für 2.005 Euro angeboten. *(dr)*

Synology: www.synology.com/enu/products/RS2211+/

Die Synology RackStations takten ihre CPU bei Bedarf herunter, um Strom zu sparen

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

Diskeeper stellt seine gleichnamige Software in der **Version 2011** vor. Die neue Funktion Instant Defrag soll dabei Dateien sofort defragmentieren, noch bevor sie gelesen werden können. Zusammen mit der IntelliWrite-Fragmentierungsverhinderung laufe so jedes System stets mit bestmöglicher Systemleistung – unabhängig von der anfallenden Last. Eine Engine zur Konsolidierung des freien Speicherplatzes soll sicherstellen, dass eine Fragmentierung des freien Speichers die Funktion Instant Defrag nicht behindert. Verbesserte Analyseberichte sind zudem über Registerkarten schnell zugänglich und zeigen die Leistungsvorteile, die mit der Defragmentierung erzielt wurden. Die Small Business Edition kostet mit einer Server- und fünf Rechnerlizenzen 550 US-Dollar. *(dr)*

www.diskeeper.com

Der Cloud Web-Security-Anbieter **Zscaler** kündigt mit **Zscaler Mobile** eine Erweiterung seiner Web- und E-Mail-Security-Lösung an. Zscaler Mobile bietet mobilen Endgeräten über die Zscaler-Cloud beim Zugriff auf das Internet Schutz vor Malware-Attacken. Unterstützt werden dabei Geräte unter iOS, BlackBerrys sowie Devices, auf denen die Proxy-Einstellungen konfigurierbar sind. Android-Geräte will der Hersteller künftig ebenfalls unterstützen. Verteilen lassen sich die Einstellungen auf iPhones beispielsweise über einen 2D-Barcode, den die Nutzer abfotografieren können. Für einen bis drei US-Dollar pro Nutzer und Monat ist das Angebot erhältlich. *(dr)*

www.zscaler.com/de/

sepago gibt die Verfügbarkeit von **Profile Migrator 2.0** bekannt. Die neue Version wartet mit einer GUI-gesteuerten Migration auf. Nach der Bereitstellung der Projektdefinition werden Benutzereinstellungen und -daten unbeaufsichtigt von Quellsystemen eingesammelt und in neu angelegte Profile und Verzeichnisse auf dem Zielsystem geschrieben. Dabei erlaubt das Tool nicht nur den Umzug der Konfiguration des Betriebssystems, sondern auch die Übernahme von Einstellungen anderer Anwendungen wie etwa dem Office 2010-Paket. Außerdem können Administratoren vor und nach der Migration Skripte ausführen und den Umzugs-Helfer in Desktop Management-Suites wie SCCM integrieren. Lizenzen schlagen mit 15 Euro pro Benutzer (mehrere Profile sind erlaubt) zu Buche. *(ln)*

www.profilemigrator.com/d

JAM Software stellt Version 2.0 des Monitoring-Tools **ServerSentinel** vor. Das aktuelle Release unterstützt ab sofort unterschiedliche Hardware-Sensoren, etwa zur Kontrolle von Raumtemperatur und Luftfeuchtigkeit, überwacht Systeme im Netzwerk per SNMP und kann Ordnergrößen kontrollieren. Die Messwerte der Sensoren zeigt die Lösung in einer Diagramm- oder Listenansicht an. In der neuen Version ist es möglich, die Daten innerhalb der Liste zu gruppieren oder zu filtern. Nicht zuletzt sind mit dem Programm nun auch Einträge in die Windows-Ereignisanzeige möglich. ServerSentinel V2 ist je nach Anzahl der Lizenzen ab 42 Euro pro Installation erhältlich. *(ln)*

www.jam-software.de/serversentinel/

Flotte Bürohelfer

Lenovo bringt zwei neue **Rechner für Geschäftsanwender** auf den Markt: Die **Workstation ThinkStation E30** und den **Desktop-PC ThinkCentre M81**. Intel Core-Prozessoren der zweiten Generation unterstützen die Rapid Boot Technologie für schnelles Hoch- und Herunterfahren. Die ThinkStation E30 baut auf ihrem Vorgänger, der ThinkStation E20, auf. Sie ist wahlweise verfügbar mit der Intel Core-Prozessortechnologie der zweiten Generation oder mit bis zu vier Kernen für besonders schnelle Leistung bei einem Intel Xeon-Prozessor. Beide Geräte – die ThinkStation E30 und der ThinkCentre M81 – profitieren von der **Intel Turbo Boost-Technologie**, die bei besonders leistungsintensiven Aufgaben die Prozessorgeschwindigkeit erhöht. Neben dem herkömmlichen Festplattenspeicher kann die ThinkStation E30 auch mit 80 GByte oder 160 GByte SSD-Festplatten ausgestattet werden. Zur Erstellung und Wiedergabe von 2D- und 3D-Inhalten bietet die Workstation wahlweise NVIDIA Quadro- oder NVS-Grafik. Zusätzlich ermöglichen die SATA III- und die USB 3.0-Technologie schnelle Datenübertragungen in bis zu zwei- respektive zehnmal höherer Geschwindigkeit als SATA II und USB 2.0. Der ThinkCentre M81 Desktop-PC ist als Tower und im kleinen Formfaktor erhältlich. Er kommt mit Intel Core-Prozessoren der zweiten Generation, bis zu 160 GByte SSD-Speicher und wahlweise mit Intel HD-Grafik oder diskreter ATI Radeon-Grafik. Ebenso wie die ThinkStation E30 verfügt der Desktop über SATA III und USB 3.0. Für übersichtlicheres und produktiveres Arbeiten können Nutzer über eine diskrete Grafikkarte zudem bis zu vier voneinander unabhängige Monitore gleichzeitig betreiben. Die ThinkStation E30 ist ab Ende Mai zu einem voraussichtlichen Startpreis von rund 659 Euro verfügbar; der ThinkCentre M81 ist ab sofort zu einem voraussichtlichen Startpreis von zirka 630 Euro verfügbar. *(dr)*

Die ThinkStation E30 von Lenovo ist auch mit 160 GByte SSD-Speicher verfügbar

Lenovo: www.lenovo.de

Revolution im Ethernet

Mit dem **Brocade VDX 6720 Datacenter Switch** präsentiert der Anbieter das **erste Ethernet Fabric**. Die ersten Modelle dieser neuen Produktreihe von 10 GBit Ethernet-Switches sind nach Herstellerangaben für virtualisierte IT-Infrastrukturen optimiert und bauen auf der Virtual Cluster Switching-Technologie auf. Die Geräte integrieren sich in Layer 2 Ethernet-Netzwerke und ermöglichen die **erste echte Ethernet Fabric**. Die Brocade VDX 6720 Datacenter Switches machen das Spanning Tree Protocol überflüssig und ermöglichen es, Netzwerkschichten zusammenzulegen. Dadurch entsteht ein **flaches, Multi-Pathing-fähiges und deterministisches Netzwerk**. Die Brocade VDX 6720 Switches sind als Ein- oder Zwei-Rack-Einheiten erhältlich und per "Ports on Demand"-Lizenzierung von 16 auf 60 Ports erweiterbar. Die Geräte liefern eine Wire-Speed-Performance von 10 GBit/s zwischen den Ports, verfügen laut Hersteller über eine geringe Latenz von 600 Nanosekunden und arbeiten verlustfrei (Lossless Ethernet). So lassen sich alle Arten von Datenverkehr übermitteln, inklusive traditionellem IP, iSCSI, CIFS, NFS und Fibre Channel over Ethernet. Die Brocade VDX 6720 Datacenter Switches sind ab sofort verfügbar. Der Verkaufspreis beginnt bei 10.700 US-Dollar. *(jp)*

Brocade: www.brocade.com

Browser-basierte Gruppendynamik

Kerio Technologies baut sein Portfolio um **Kerio Workspace** aus. Die serverbasierte Software ermöglicht Anwendern die **gemeinsame und plattformübergreifende Nutzung** von Dokumenten, Dateien, Notizen, Diskussionen und Multimedia-Inhalten über einen gängigen Webbrowser. Mit Kerio Workspace können Mitarbeiter in Teams gemeinsam ihre Projektnotizen, Ideen, Dateien oder Diskussionen verwalten. Dabei können sie die Lösung sowohl als zentralen Speicherort für ihre Dateien und Kommentare nutzen als auch über die Oberfläche der Software sehr einfach komplexe Seiten mit Informationen, Grafiken, verknüpften Dokumenten und weiteren Elementen erstellen. Durch die Vergabe geeigneter Zugriffsrechte ist die sichere Nutzung von Texten, Bildern, Video und Dateien gewährleistet; Inhalte können per Suchfunktion gefunden werden. Dateien lassen sich aus Kerio Workspace heraus mit der passenden Desktopanwendung öffnen und bearbeiten. Der Desktopclient sorgt dafür, dass alle Änderungen automatisch auf Kerio Workspace gespeichert werden. Benutzer benötigen dazu lediglich einen Webbrowser. Eine Newsfeed-Funktion informiert Teams zudem direkt über Projektfortschritte und das Feedback von beteiligten Mitarbeitern. Updates lassen sich automatisch per E-Mail kommunizieren, so dass Mitarbeiter stets auf dem neuesten Stand bleiben. Kerio Workspace für Windows XP ab SP2, Debian Linux ab der Version 5, Ubuntu 8.04 oder 10.04 LTS sowie Mac OS X ab der Version 10.6 ist ab sofort in 16 Sprachen erhältlich.

Der Desktop-Client von Kerio Workspace läuft unter Windows XP SP2 und neuer sowie ab Mac OS X 10.6. Die Preise von Kerio Workspace beginnen bei 120 Euro für fünf Benutzer. Zusätzliche Nutzer kosten je 24 Euro. *(dr)*

Kerio Technologies: www.kerio.de

Kerio Workspace erlaubt die Online-Zusammenarbeit und soll dabei einfacher zu nutzen sein als andere Tools

Zentralverwaltung für Nutzerrechte

ScriptLogic gibt die Verfügbarkeit von **Privilege Authority Professional** bekannt. Mit dieser Software können IT-Administratoren **Zugriffsrechte an Benutzer** vergeben, ohne dass diese als lokale Administratoren angemeldet werden müssen. Privilege Authority Professional arbeitet nahtlos mit dem Microsoft Active Directory zusammen. IT-Verantwortliche behalten so die vollständige Kontrolle über die Administrationsrechte des PCs, gewähren dem User aber spezifische und limitierte Zugriffsrechte. Die Lösung beinhaltet dabei gebräuchliche Regeln, damit Clients für gängige Aufgaben gewappnet sind. Sie ermöglichen dem User beispielsweise den Zugriff auf Systemeigenschaften, die Ausführung von iTunes und des BlackBerry Desktop-Installers, die Installation eines Adobe Flash Players oder die Ausführung des Adobe Readers. Benutzerdefinierte Regeln, die an die speziellen Bedürfnisse des Unternehmens angepasst sind, können ebenfalls implementiert werden. Im Community Forum können Privilege Authority-Anwender Regeln mit Kollegen austauschen. Der Preis beträgt 107,50 Euro für ein Minimum von zehn zu verwaltenden Arbeitsplätzen. *(dr)*

Für die Nutzung in Privilege Authority Professional können Admins Richtlinien online mit Kollegen austauschen

ScriptLogic: www.scriptlogic.com/products/privilegeauthority/

Herrscher im Reich der großen Daten

Der Storage-Hersteller **EMC** lüftet den Vorhang für seine neue **Isilon Scale-Out NAS-Hard- und -Software**. Diese sind speziell auf die Bewältigung großer Datenmengen, die aus unterschiedlich strukturierten Datentypen bestehen, ausgelegt. Bei den neuen Isilon-Hardwaresystemen **können Anwender die Festplattenkonfiguration selbst bestimmen** und Solid-State-Drive- (SSD) mit SAS- oder SATA-Laufwerken kombinieren. Des Weiteren steht mit OneFS 6.5 eine neue, um zahlreiche Funktionen erweiterte Version des von Isilon entwickelten Betriebssystems zur Verfügung. Das Upgrade soll die Leistung der in Rechenzentren eingesetzten Storage-Systeme verbessern. Mit Sync -IQ 3.0 bietet Isilon darüber hinaus eine aktualisierte Version seiner Replizierungssoftware an, die den zwischen zwei Datensicherungen liegenden Zeitraum verkürzen soll. Sämtliche neuen Produkte sind ab sofort am Markt erhältlich. Der Listenpreis für die beiden neuen Hardwaresysteme liegt pro Knoten bei der S200 bei 40.770 Euro und bei der X200 bei 19.440 Euro. OneFS 6.5 ist bereits standardmäßig auf die neuen S200- und X200-Systeme aufgespielt. Die Kosten für SyncIQ 3.0 belaufen sich auf 3.495 Euro pro Knoten. *(jp)*

Isilon: http://de.isilon.com/

Die Isilon S200 erlaubt die Kombination verschiedener Speichermedien in einem NAS

Alle Linux-Server im Griff

Novell bringt mit **SUSE Manager** ein **Administrations-Werkzeug für Linux-Server** auf den Markt. Das Tool, das auf dem Open Source-Projekt Spacewalk 1.2 beruht, ermöglicht die Verwaltung von physikalischen, virtuellen und Cloud-basierten Servern von einer zentralen Konsole aus. Die Software unterstützt dabei neben SUSE Linux Enterprise Server auch Red Hat Enterprise Linux. Die Lösung besteht in der Basisversion aus einem Management-Modul, das sich unter anderem zur Verteilung von Updates und Patches nutzen lässt und zudem das Ausrollen von Programmen erlaubt. Um diese Aufgabe zu automatisieren, lassen sich Server in Gruppen einteilen. Rollenbasierte Zugangsregeln sollen dafür sorgen, dass nur berechtigte Nutzer Zugriff auf die Konfiguration der Server erhalten. Verwalten lassen sich nicht nur physikalische Server, sondern alle Gastsysteme, die in Virtualisierungs-Umgebungen von VMware, Xen, KVM und Hyper-V zum Einsatz kommen. Als zusätzliche Pakete sind ein Provisioning- sowie ein Monitoring-Modul erhältlich. Die erstgenannte Erweiterung erlaubt die Bare Metal-Installation von Serverbetriebssystemen mittels AutoYaST, Kickstart und PXE-Boot. Hier soll es ebenfalls kein Problem sein, die entsprechenden Server als virtuelle Maschinen in Betrieb zu nehmen. Das Monitoring-Modul schließlich überwacht laufend den Systemzustand und verständigt bei Überschreiten individuell gesetzter Grenzwerte den Administrator. Außerdem ist es möglich, über selbst definierte Sonden oder Lösungen von Drittherstellern weitere Systemdaten auszulesen. Der SUSE Manager Server, der auch als virtuelle Appliance ausgeliefert wird, kostet 13.500 US-Dollar. Hinzu kommen knapp 100 US-Dollar pro Modul und überwachtem Server. *(ln)*

Der SUSE Manager von Novell verwaltet auch Server unter Red Hat Enterprise Linux und in virtualisierten Umgebungen

Novell: www.novell.com/products/suse-manager/

IT-Administrator Workshop "Update Virtualisierung 2011"

Vorwärts immer, rückwärts nimmer

von John Pardey

IT-Administrator Trainings-Partner: Global Knowledge

ITANet Workshop-Partner: VEEAM

Die Server-Virtualisierung tritt nach großen Erfolgen bei der Konsolidierung der Rechenzentren in eine neue Phase: Management, Monitoring und Netzwerkanbindung rücken in den Fokus der IT-Verantwortlichen. Gleichzeitig sind die Entwicklungen in der Desktop-Virtualisierung so rasant vorangeschritten, dass sich diese Technologie aufmacht, ihre Nische zu verlassen. Unsere Workshops im Frühsommer in Frankfurt und Leipzig bringen Sie auf den aktuellen Stand der Virtualisierung.

Das Versprechen der ersten Welle der Server-Virtualisierung, die Hardware-Infrastruktur zu konsolidieren und so erheblich die Kosten zu reduzieren, setzten viele IT-Verantwortliche erfolgreich in die Praxis um. Parallel dazu entwickelten zahllose Hersteller neue Produkte, um Storage, Netzwerk oder auch Clients mit ähnlichen Resultaten zu virtualisieren.

Aktuelle Herausforderungen der Virtualisierung

Vielfach übersehen wird dabei, dass die Virtualisierung von x86-Servern noch eine sehr junge Technologie ist. Mit wachsender Komplexität zeigten sich erste Kinderkrankheiten. So ist das Monitoring solcher Server oft unvollständig und die Verwendung von virtuellen Switches birgt Sicherheitsrisiken. In unserem Workshop greift Dozent Nico Lüdemann diese Themen auf und stellt dar, in welche Richtung aktuelle Lösungsansätze für diese Probleme gehen. Dabei thematisiert er auch den weit verbreiteten parallelen Betrieb physikalischer und virtueller Server und dessen spezielle Herausforderungen.

Besonders verlockend scheint die Virtualisierung in Sachen Desktop, denn die schlichte Masse an Rechnern an den Arbeitsplätzen lässt auf besonders hohe Einsparpotentiale schließen. Zudem eröffnen sich Wege, um die ärgerlichen Dauerbrenner Patchmanagement, Softwareverteilung oder Geräteunabhängigkeit in den Griff zu bekommen. Der Workshop stellt den Teilnehmern den aktuellen Stand der Technologie dar und will aufzeigen, welche Wege der Client-Virtualisierung sich für welchen Einsatzzweck eignen. Außerdem stellt er den potentiellen Einsparungen die zu erwartenden Kosten gegenüber. Abschließend werfen wir noch einen Blick auf den aktuellen Stand des Client-Managements in diesem Umfeld.

Zwei Termine zur Auswahl

Für alle IT-Verantwortlichen, die Virtualisierung am Server oder Client betreuen, bietet unser Workshop ein Update neuer Erkenntnisse und Möglichkeiten. Neu ist ab 2011, dass wir jeden Workshop an zwei Terminen anbieten. Die beiden inhaltlich identischen Workshops finden diesmal am 8. Juni in Frankfurt und am 7. Juli in Leipzig statt. Alle Informationen zur Anmeldung und zum Workshop finden Sie im Kasten "Workshop Update Virtualisierung 2011". Die Anmeldung ist jeweils bis eine Woche vor dem Workshop-Termin möglich. Wir würden uns freuen, Sie begrüßen zu dürfen.

ITANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.15 Uhr: Server-Virtualisierung aktuell

- Herausforderung Management: Blinde Flecken des Monitorings und neue Werkzeuge für die Verwaltung virtualisierter Server
- Abschied vom virtuellen Switch: Neue Wege der Anbindung virtueller Maschinen an das Netzwerk
- Gemeinsame Verwaltung physikalischer und virtueller Server: Stolperfallen, Methoden, Tools

Dozent: Nico Lüdemann

14.45 Uhr: Pause

15.00 Uhr: Partnervortrag:
Veeam Backup – mehr als nur Backup!

Dozent: Dirk Hannemann (Frankfurt)
Matthias Frühauf (Leipzig)

15.45 Uhr: Pause

16.00 Uhr: Desktop-Virtualisierung aktuell

- Virtuelle Applikationen versus gehosteter Desktop
- Lokale Virtualisierung für mobile Anwender
- Vor- und Nachteile, Kosten
- Wie passt das alles ins Client-Management?

Dozent: Nico Lüdemann

17.30 Uhr: Ende der Veranstaltung

Ort

8. Juni 2011, Frankfurt/M.:
Global Knowledge Germany Training GmbH,
Hungener Straße 6, 60389 Frankfurt

7. Juli 2011, Leipzig:
Commundo Tagungshotel Leipzig,
Zschochersche Straße 69, 04229 Leipzig

Teilnahmegebühren

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

Anmeldung bis zum 1. Juni (Frankfurt/M.) beziehungsweise 1. Juli (Leipzig) unter
www.it-administrator.de/workshops/

Workshop Update Virtualisierung 2011

baramundi
software AG

Cleveres Client Management kann Ihre IT verändern!

baramundi Management Suite – und professioneller IT-Services

Cleveres Client Management kann Ihre IT – und Ihr Unternehmen – verändern: Ressourcen besser nutzen, Budgets optimieren, Daten applikationsübergreifend nutzen, für perfekte Sicherheit sorgen. Vor allem aber automatisieren Sie Routineaufgaben wie Softwareverteilung und sparen so Zeit und Geld.

Intelligente automatisierte Installationen und smartes Verteilen von Software stehen im Mittelpunkt unserer Arbeit. Mit der baramundi Management Suite managen viele Unternehmen ihre IT-Infrastruktur. Auch in Systemen mit mehreren tausend Arbeitsplätzen an teilweise über hundert Standorten. Ob Windows XP oder Windows 7 – mit der baramundi Management Suite installieren und warten Sie Ihre IT-Landschaft schneller und zuverlässiger.

Wir stellen Ihnen gerne unser langjähriges Fachwissen zur Verfügung. Sprechen Sie mit uns über Ihre Ansprüche und Anforderungen!

IT einfach clever managen

Client, System, Storage und Device Management

Reduzieren Sie Ihren Aufwand bei der Konzeption, Implementierung, Migration sowie den Betrieb Ihrer komplexen IT-Systeme.

Als unabhängiger IT-Dienstleister haben wir uns auf IT-Outsourcing sowie Konzeptionierung, Realisierung und Durchführung komplexer IT-Projekte spezialisiert. Praxisnahe IT-Beratung sowie die Erarbeitung von Teillösungen und die Übernahme von Gesamtprojekten von der Konzeption, über Testinstallationen bis hin zum Rollout und anschließendem Support zu ihren Serviceleistungen runden das Dienstleistungsportfolio ab und sorgen für einen reibungslosen Ablauf Ihres IT-Betriebes.

Als baramundi Competence Center verfügen wir über ein sehr großes Know-how im Umgang mit der baramundi Management Suite und unterstützen Sie gerne bei der Implementierung der Suite und Durchführung Ihrer IT-Projekte.

GIB
Gesellschaft für Informationstechnik und -Beratung mbH

baramundi software AG
Beim Glaspalast 1
86153 Augsburg
Fon: +49 (821) 5 67 08 - 380
Web: www.baramundi.de
E-Mail: request@baramundi.de

GIB-MBH
Mühltalerstr. 52
40221 Düsseldorf
Fon: + 49 (211) 90 23 26 2
Web: www.gib-mbh.de
E-Mail: info@gib-mbh.de

Im Test: 2X VirtualDesktopServer 9

Virtuelle Desktops nach Maß

von Jürgen Heyer

Über Virtual Desktop-Infrastrukturen einzelne Applikationen oder ganze Arbeitsplätze im Netzwerk bereitzustellen, ist längt kein Zauberwerk mehr. Statt jedoch bei der Veröffentlichung von Anwendungen nur einen Weg anzubieten, wartet der 2X VirtualDesktopServer mit einer beeindruckenden Funktionsbandbreite auf: Die Unterstützung für Terminalserver von Microsoft und Citrix, VDI und Public Desktops auf unterschiedlichen Client-Plattformen eröffnet einen breiten Spielraum für eine individuelle Gestaltung. IT-Administrator hat sich die verschiedenen Varianten im Test einmal genauer angesehen.

Viele Anbieter von Virtualisierungs-Lösungen setzen nur auf einen der führenden Hypervisoren. 2X hingegen stellt als Entwickler von Software für Thin Clients und Server-based Computing mit dem VirtualDesktopServer (VDS) in nur einem Produkt vielfältige Möglichkeiten bereit, um Applikationen und komplette Desktops auf Endgeräte zu bringen. Nicht umsonst bewirbt 2X seinen Application Server, der in VDS enthalten, aber auch als eigenes Produkt erhältlich ist, als erste Alternative zu Citrix. In Kombination mit dem Windows Terminalserver und Citrix selbst stehen dem Administrator umfassende Möglichkeiten zur individuellen Anwendungs- und Desktopveröffentlichung zur Verfügung.

Das 2X-Flaggschiff VDS unterstützt darüber hinaus praktisch alle gängigen Hypervisoren, um neben den Terminaldiensten auch virtuelle Desktops (VDI) bereitzustellen. Sehr breit aufgestellt ist zudem die Clientunterstützung mit einer beachtlichen Vielzahl an Agenten für unterschiedliche Betriebssysteme. Wer den Bedarf hat, beispielsweise auf einem Linux-System Windows-Desktops zu veröffentlichen oder wer per iPhone zugreifen will, kann dies mit 2X VDS realisieren.

Zu Beginn des Tests stand uns die Version 9 als sehr fortgeschrittene Public Beta zu Verfügung. Kurz vor Testende konnten wir noch die offiziell freigegebene Version in Augenschein nehmen. Ziel von VDS ist es letztendlich, den verschiedenen Anwendern genau den benötigten Umfang an Applikationen oder ganze Desktopumgebungen auf genau der Plattform an die Hand zu geben, die leistungsmäßig gefordert und angemessen ist. Indem VDS diverse Funktionalitäten in einem Produkt vereint, hat der Administrator nur eine Konsole zu bedienen. Darüber hinaus ist auf Anwenderseite nur ein Client im Einsatz, egal, auf welchem Weg die Bereitstellung erfolgt. Das macht die Lösung sehr wartungsfreundlich.

Redundanz des Publishing-Servers

Bei der Einrichtung von VDS ist zu beachten, dass diese unter Windows Server 2008 R2 als lokaler Administrator erfolgen muss. Als wir es anfangs als Domänen-Administrator versuchten, wurden wir mit einer Abbruchmeldung konfrontiert, die leider nicht auf die Ursache des Problems schließen ließ. Das Handbuch verlangt in diesem Zusammenhang nur

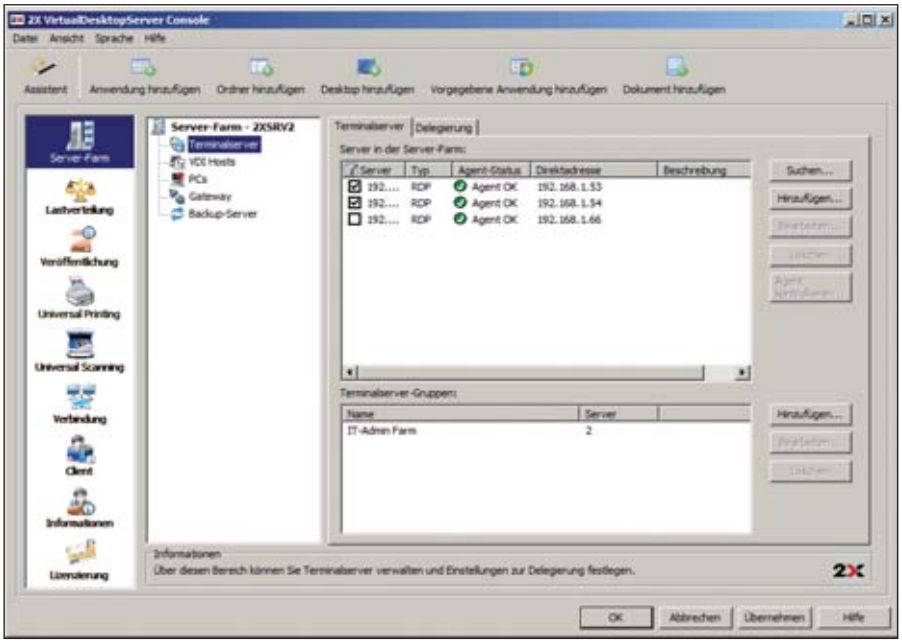


Bild 1: Sehr übersichtlich präsentiert sich der Bereich von VDS, wo die zur Serverfarm gehörigen Server einzutragen sind

allgemein Administratorrechte und erst eine Nachfrage beim Support brachte uns weiter. Wer noch unter Windows Server 2003 installiert, wird auf dieses Problem nicht stoßen.

Der Server, auf dem VDS zuerst installiert wird, fungiert standardmäßig als Master Publishing-Server (Broker). Dies bedeutet, dass alle Client-Anfragen zuerst zu diesem Server gelangen, der sie dann an das eigentliche System weitergibt, über das die gewünschte Applikation beziehungsweise der Desktop bereitgestellt wird. Das heißt aber auch, dass bei Ausfall des Publishing-Servers die gesamte Bereitstellung ausfallen würde. Um hier Redundanz zu schaffen, lassen sich ein oder mehrere Backup-Server definieren, die dann die Verteilung übernehmen. Sollte der Master Publishing-Server auf Dauer ausfallen, kann jederzeit ein Backup-Server zum Master hochgestuft werden.

Damit die Backup-Server im Normalbetrieb nicht nur weitgehend untätig auf einen Ausfall des Masters warten, können sie zusätzlich als sogenannte Secure Client Gateways genutzt werden. Diese dienen dazu, vor allem in Umgebungen mit erhöhten Sicherheitsanforderungen und in durch Firewalls segmentierten Netzwerken, den gesamten Datenverkehr über einen Port (Standard ist Port 80) zu tunneln und auf Wunsch zusätzlich mit SSL zu verschlüsseln. Standardmäßig werden SSL2 und SSL3 unterstützt, eine Beschränkung auf SSL3 ist möglich. Der Gateway-Zugriff lässt sich zusätzlich über MAC-Adressen filtern, indem der Administrator entweder eine Ausschlussliste (Alle Adressen außer ...) oder eine Einschlussliste (Nur die Adressen ...) pflegt.

Mit einem Klick zurück zu den Standardeinstellungen

Sehr von Vorteil für die Umsetzung individueller Sicherheitsanforderungen ist die Möglichkeit, dass alle genutzten Ports für RDP, Citrix, die Verwendung von Secure Client Gateways, den Einsatz von SSL/TLS und die Kommunikation mit den Agenten geändert werden können. Zu begrüßen ist ferner, dass der Administrator an allen Stellen, wo sich die Ports ändern lassen, eine Schaltfläche zur Rückkehr auf die Standardeinstellungen vorfindet – hat er sich einmal verkonfiguriert, ist es kein Problem, wieder zum Normalzustand zurückzukehren.

Auf allen Systemen, die VDS für die Applikations- beziehungsweise Desktopbereitstellung nutzen können soll, ist der 2X Publishing-Agent zu installieren. Dies kann über ein Setup erfolgen, ebenso aber remote über die weiter unten beschriebene VDS-Konsole. Diese erlaubt es zudem, bereits installierte Agenten auf Erreichbarkeit und Funktion zu prüfen sowie gegebenenfalls zu deinstallieren oder auf eine neuere Version zu aktualisieren.

Eine Stärke von VDS ist die Lastverteilung, wahlweise per Round Robin oder Ressourcen-basiert. Gerade bei der Nutzung vieler verschiedener Applikationen ist in der Regel die Ressourcen-basierte Vorgehensweise effizienter, bei der VDS die Anzahl der Benutzer-Sitzungen, den Arbeitsspeicher und die CPU-Last als Indikatoren verwendet und neue Sitzungen entsprechend zuweist. Trotzdem stellt VDS auf Wunsch getrennte Sitzungen bevorzugt auf dem gleichen Server wieder her.

Um die Anzahl der Sitzungen in Grenzen zu halten, ist es möglich, diese auf eine pro Benutzer zu beschränken. Zusätzlich gibt es für spezielle Anforderungen noch weitere Optionen für eine individuelle Verteilung, deren Beschreibung hier aber zu weit führen würde. Gefallen hat uns, dass VDS jederzeit eine detaillierte Übersicht zum aktuellen Stand der Lastverteilung und zur Verteilung der Sitzungen liefert. Zudem fiel uns positiv auf, dass das Konfigurationsprogramm die Aktualisierung der Publishing-Agenten auf den Terminalservern vorschlug, als wir im Verlauf des Tests vom Betastatus auf die erste offiziell freigegebene Version aktualisierten.

Mächtige Kommandozentrale

Erfreulich übersichtlich zeigte sich uns die VDS-Konsole, die alle Einstellmöglichkeiten in einer Oberfläche vereint. Auf der linken Seite findet der Administrator ein Menü mit den neun Hauptrubriken (Server-Farm, Lastverteilung, Veröffentlichung, Universal Printing, Universal Scanning, Verbindung, Client, Information und Lizenzierung).

Gruppen für Priorisierung und Verfügbarkeit

In der Rubrik "Server-Farm" hat der Administrator alle Server einzutragen, von denen Desktops oder Applikationen verteilt werden sollen. Das können Terminalserver sein, entweder von Microsoft oder Citrix, Virtual Desktop Hosts (VDI-Hosts) und dedizierte PCs, um diese über RDP zu veröffentlichen. Weiterhin gibt der Administrator hier die schon erwähnten Secure Client Gateways sowie vorhandene Backup-Server an. Innerhalb der erfassten Terminalserver ist zur Unterteilung eine Gruppierungs-Funktion implementiert, um beispielsweise bestimmte Applikationen oder Desktops nur über einen Teil der Server zu veröffentlichen.

Dies bedeutet auch, dass nicht alle Terminalserver identisch konfiguriert sein müssen. Vielmehr kann der Administrator etwa für eine spezielle Applikationsbereitstellung eine Servergruppe definieren und diese wiederum nur an eine bestimmte Benutzergruppe freigeben. Damit hat er die Möglichkeit, eventuelle Lizenzvorgaben besser zu kontrollieren und die Lizenzen effizienter zu verwenden. Weiterhin kann er bei Bedarf Benutzergruppen priorisieren, indem er eine Applikation für eine Gruppe nur über wenige Terminalserver zur Verfügung stellt, für eine andere Gruppe aber über zusätzliche, so dass diese selbst bei einer hohen Auslastung auf jeden Fall eine Sit-

Systemvoraussetzungen

Publishing Server und Secure Client Gateway unter Windows Server 2003/2008 (R2) Standard oder Enterprise, Terminalserver-Agent unter Windows Server 2003/2008 (R2) Standard oder Enterprise mit aktivierten Terminalservices. Der 2X-Client ist verfügbar für Windows Server 2003, Windows XP, Vista, 7, CE Embedded, Mac ab 10.5.x, außerdem für die 32-Bit-Linux-Distributionen Ubuntu 8.04/8.10/9.04/9.10, OpenSuse 11.1, Fedora Core 9/11, CentOS 5.2, VectirLinux 6.0 und Android sowie iOS.

zung bekommen. Sofern ein Benutzer auf mehreren Serverfarmen über Berechtigungen verfügt, kann er sich durchaus gleichzeitig zu mehreren verbinden.

Flexible Zusammenarbeit mit Hypervisoren

Hinsichtlich der VDI-Hosts erweist sich der 2X VDS als überaus flexibel, da praktisch alle gängigen Hypervisoren wie Microsoft Hyper-V, VMware vSphere, ESX, ESXi, Parallels Virtuozzo Containers, Citrix XenServer und Oracle Virtualbox unterstützt werden. Im Test nutzten wir die Konfiguration für den Betrieb mit VMware vCenter sowie ESXi. Diese ist vergleichsweise komplex, war aber letztendlich dennoch schnell eingerichtet. 2X stellt für diesen Zweck eine virtuelle Appliance (vApp) mit einer Ubuntu-Installation zum Download zur Verfügung, die anschließend via vSphere-Client zu importieren ist.

Weitere VDI Agent Appliances sind für Citrix XenServer und Virtual Iron verfügbar. Im Test mussten wir an der Appliance selbst nichts konfigurieren, sie holte sich mittels DHCP automatisch passende IP-Adressen. Beim Anlegen des VDI-Hosts in der Konsole sind dann diverse Eingaben erforderlich wie der Hypervisor-Typ, die genaue Version, die IP-Adresse, der genutzte Port und die Zugangsdaten (Benutzer/Passwort), was auch gleich getestet werden kann. Ist der VDI-Agent wie in unserem Test auf der Appliance installiert, wird zudem deren IP-Adresse benötigt. Weiterhin kann der Administrator die Höchstanzahl der aktivierten Gäste festlegen und das Format des RDP-Druckers vorgeben.

Da gerade bei der Konfiguration mit einem vCenter nicht alle laufenden virtuellen Maschinen als VDI-Gast genutzt werden sollten, kann der Administrator die Nutzung für jede VM einzeln sperren. Weiterhin hat er die Möglichkeit, über eine Pool-Definition mehrere Gäste zu gruppieren und dann die Pools nur bestimmten Benutzergruppen zur Verfügung zu stellen. Bei der Filterung anhand von Benutzern und Gruppen greift VDS auf Wunsch auf das Active Directory zu, so dass die Gruppenadministration am besten dort erfolgt. Alternativ ist eine Filterung über Clients und IP-Adressen verfügbar. Insgesamt hat uns die hier gebotene Flexibilität überzeugt.

Nicht uninteressant dürfte die Möglichkeit sein, den Zugriff sowohl auf VDI-Hosts als auch auf die Terminalserver über einen Zeitplaner für bestimmte Zeiträume zu unterbinden. Dabei können aktuelle Sitzungen wahlweise ihren Status beibehalten, getrennt oder zurückgesetzt werden. Die Ausschlusszeiten lassen sich permanent, täglich, wöchentlich, alle zwei Wochen, monatlich oder jährlich festlegen. Die Definition beispielsweise von Wartungsfenstern ist also kein Problem.

Bild 2: VDS und der Application Server sind in einem Setup zusammengefasst, die Lizenz entscheidet über den Nutzungsumfang

Eine untergeordnete Rolle dürfte die Option spielen, dedizierte PCs zu veröffentlichen. Für bestimmte Konfigurationen, die sich beispielsweise aufgrund spezieller Hardwareanforderungen nicht virtualisieren lassen, mag dies aber sinnvoll sein. In diesem Fall ist auf dem PC RDP zu aktivieren und der VDS-Agent zu installieren.

Grafische Darstellung des Farm-Designs

Vorteilhaft für eine Gesamtübersicht ist die Möglichkeit, sich jederzeit das aktuelle Farm-Design grafisch anzeigen zu lassen. Zusätzlich bietet 2X den so genannten VirtualInfrastructureDesigner (VID) an, ein Tool, um eine VDS-Umgebung mit grafischer Unterstützung zu entwerfen. Für den Betrieb des VID ist ein installiertes Visio 2003 oder höher Voraussetzung. Im Test ließ sich der VID anfangs nicht starten, sondern brach selbst auf unterschiedlichen Systemen immer mit einer Fehlermeldung ab. Zusammen mit dem Support wurde das Problem analysiert und schnell stellte sich heraus, dass der Grund in der Sprachversion lag. Wir nutzten stets ein deutsches Windows, 2X dagegen verwendet intern englische Versionen. Daraufhin beseitigte 2X das Problem innerhalb weniger Tage und wir konnten mit einem funktionierenden VID weitertesten.

Beim Aufruf des VID fragt ein Assistent die Komponenten und deren IP-Adressen ab, die für eine Anwendungs- und Desktopbereitstellung eingesetzt werden sollen. Daraus wird eine logische Ansicht erstellt. Der Administrator kann per Drag & Drop noch weitere Komponenten ergänzen. Ein Klick auf eine der Komponenten listet deren Eigenschaften auf, um sie bei Bedarf noch genauer anpassen zu können. Das Resultat ist eine Konfigurationsdatei, die sich in VDS importieren lässt. Genauso ist es möglich, die Konfiguration einer laufenden VDS-Umgebung zu exportieren, in den VID zu laden, dort zu verändern und anschließend wieder in VDS zu importieren.

In der Konsolen-Rubrik "Veröffentlichung" kann der Administrator die Ports zu den Agenten hin anpassen und steuern, inwiefern der Abruf der Anwendungsliste eine Benutzerauthentifizierung erfordert. Weiterhin unterstützt VDS eine Zwei-Faktor-Authentifizierung via Deepnet oder SafeNet. Integriert ist eine Authentifizierung via SafeID, FlashID, MobileID, QuickID, GridID und SecureID. Gut ist hier die Möglichkeit, bei Nutzung dieser Funktion dennoch bestimmte Benutzer oder Clients von diesem Verfahren wieder auszuschließen.

Kompletter Desktop oder einzelne Applikationen

Für die Veröffentlichung von Ressourcen findet der Administrator in der VDS-Konsole eine Symbolleiste mit den verschiedenen Möglichkeiten sowie einen Assistenten, der die Einrichtung weiter vereinfacht. Bei genauerer Betrachtung zeigt sich zwischen dem Assistenten und den direkten Möglichkeiten, eine Anwendung, einen Ordner, einen Desktop, eine vorgegebene Applikation oder ein Dokument hinzuzufügen, gar kein so großer Unterschied. In allen Fällen fragt VDS komfortabel die benötigten Angaben über mehrere Fenster hinweg ab. Der Administrator wird in jedem Fall geführt.

Die genannten Möglichkeiten zur Veröffentlichung sind von der Bezeichnung her überwiegend selbsterklärend. Bei den vorgegebenen Anwendungen sind in VDS einige systemnahe Applikationen wie der Internet Explorer oder Teile der Systemsteuerung fest hinterlegt, weiterhin kann der Administrator aus den installierten Anwendungen oder einer einzelnen Anwendung wählen. Bei der installierten Anwendung wiederum veröffentlicht VDS alle zusammengehörenden Einzelprogramme, so wie sie im Startmenü zu finden sind. Etwas genauere Angaben sind bei der Veröffentlichung einer einzelnen Anwendung erforderlich. Hier muss der Administrator den Speicherort der ausführbaren Datei direkt angeben. Sowohl bei Desktops als auch bei den Anwendungen kann der Administrator Farbtiefe und Fenstergröße in der Konsole fest vorgeben oder von den Einstellungen auf Clientseite abhängig machen.

Standardmäßig richtet VDS neben einer Menüstruktur im weiter unten beschriebenen 2X-Client für jede Ressource eine Verknüpfung im Start-Ordner des Anwender-PCs ein. Es ist aber möglich, Verknüpfungen auf dem Desktop oder im Autostart-Ordner anzulegen. Sofern für eine Applikation die Anzahl der gleichzeitigen Aufrufe beispielsweise aufgrund einer Lizenzvorgabe beschränkt ist, lässt sich auch dies hinterlegen und im Falle der Lizenzüberschreitung mit verschiedenen Aktionen wie "Benutzer warnen und nicht starten" oder "Administrator warnen und starten" verknüpfen. Natürlich stellt es kein Problem dar, den Aufruf einer Applikation generell auf eine Instanz zu beschränken.

Statt wie zuvor beschrieben Zugriffe auf Serverebene anhand Benutzer, Client oder IP-Adresse zu filtern, unterstützt VDS dies auch auf Ressourcenebene. So kann der Administrator individuell vorgeben, wer welche Anwendung oder welchen Desktop aufrufen können soll und wer nicht. Die angezeigten Verknüpfungen werden stets entsprechend angepasst. Im Test haben wir die verschiedenen Möglichkeiten durchgespielt und waren überrascht, wie einfach dies funktioniert und welche umfangreichen Möglichkeiten der Administrator zur individuellen Konfiguration hat. Sobald er etwas ändert, wird dies auf Clientseite mit der Aktualisierung der Ansicht angepasst.

Schnell wurde uns allerdings klar, dass in einer produktiven Umgebung eine genaue Vorplanung der zu veröffentlichenden Ressourcen erforderlich ist, damit sich zum einen eine übersichtliche Struktur ergibt und zum anderen verschiedene Terminalserver und VDI-Hosts bedarfsgerecht ausgelegt werden. Eine wichtige Voraussetzung dazu ist auch eine entsprechende Gruppierung beispielsweise via Active Directory. Gerade am Anfang ist es sicher sinnvoll, erst mit der Veröffentlichung weniger Ressourcen zu beginnen und den Umfang dann sukzessive zu erweitern.

Breiter Clientsupport

Geradezu erschlagend ist die Clientunterstützung von VDS: Neben dem normalen Windows-Client gibt es auch einen für Linux und Mac, der für verschiedene Distributionen (siehe Kasten "Systemvoraussetzungen") freigegeben ist. Weiterhin sind Clients für iOS (iPad, iPhone) sowie für Android verfügbar, um den Zugriff via Smartphone zu ermöglichen. Im Windows-Umfeld gibt es einen XP Embedded-Client sowie eine Version für Windows CE. Zwei weitere portable Clients für U3 und PortableApps runden das Angebot ab. Das breite Clientangebot erlaubt es so beispielsweise, dass sich via VDS veröffentlichte Windows-Desktops auf einem Linux-System oder einem iPad nutzen lassen.

Die Clientinstallation auf den verschiedenen Plattformen ist im Handbuch eingehend beschrieben. Gerade der Windows-Client besitzt eine Vielzahl an Einstellungen, um dessen Look and Feel wie die Fenstergröße oder den Umgang mit den lokalen Ressourcen individuell anzupassen. Sofern mit Proxies gearbeitet wird, lassen sich hierfür die Einstellungen eingeben. Auf jeden Fall ist vor der ersten Benutzung mindestens eine Verbindung

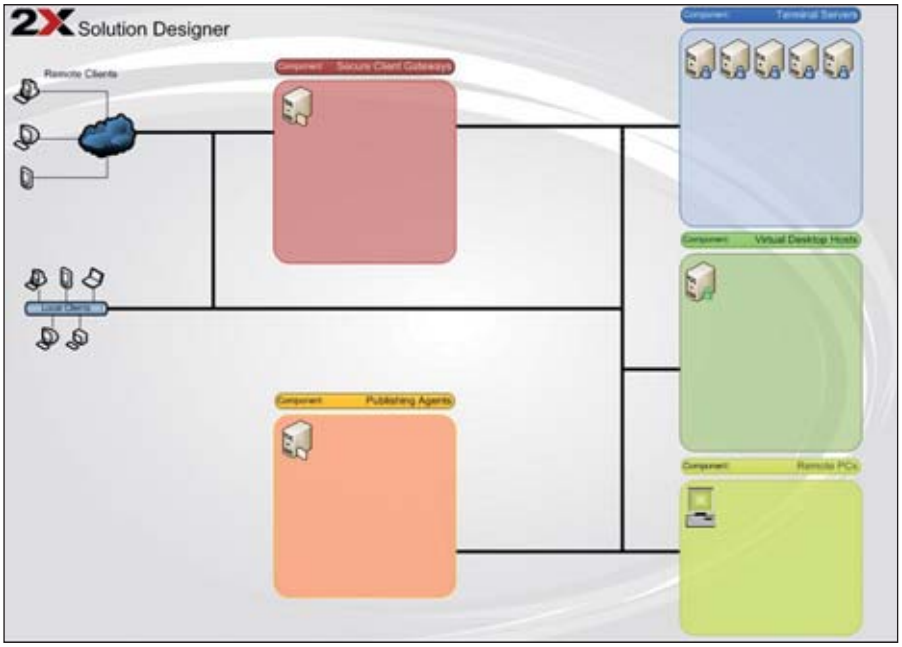


Bild 3: Die aktuelle Konfiguration präsentiert VDS auf Wunsch in einer übersichtlichen Grafik. Ein Klick auf eine Komponente zeigt die entsprechenden Eigenschaften an.

1&1. DOPPELT HOSTET BESSER.

1&1 DUAL H

DOPPELT SICHER DURCH GEO-REDUNDANZ!

Niemand kann sich Ausfallzeiten seiner Website leisten … Darum bietet 1&1 Dual Hosting jetzt die ultimative Sicherheit der Geo-Redundanz: Ihre Website wird parallel in zwei unserer Hightech-Rechenzentren an verschiedenen Orten gehostet. Fällt Ihre Internet-Präsenz im ersten Rechenzentrum unerwartet aus, läuft sie automatisch im zweiten Rechenzentrum weiter. Selbstverständlich ohne Datenverlust.

MEMBER OF united internet

OSTING

Kein anderer Webhoster überzeugt durch so viel Kompetenz, Know-how und Qualität wie 1&1:

Bei 1&1 treffen über 20 Jahre Webhosting-Erfahrung auf modernste Technik in deutschen Hochleistungs-Rechenzentren. Mehr als 1.000 IT-Profis entwickeln unsere hochwertigen Lösungen permanent weiter. **NEU:** Jetzt bietet Ihnen 1&1 mit 1&1 Dual Hosting als weltweit erster Webhoster die doppelte Sicherheit der Geo-Redundanz. Und das alles zu unschlagbar günstigen Preisen!

Doppelt sicher:
Redundante Rechenzentren!

Top-Performance:
High-End Server!

Superschnell:
210 GBit/s Anbindung!

Umweltschonend:
Grüner Strom!

Zukunftssicher:
1.000 eigene Entwickler!

NEU!

1&1 DUAL UNLIMITED

- 12 Domains inklusive
- UNLIMITED Webspace
- UNLIMITED Traffic
- UNLIMITED FTP-Accounts
- UNLIMITED MySQL Datenbanken (je 1 GB)
- UNLIMITED E-Mail Postfächer (je 2 GB)
- UNLIMITED 1&1 Click & Build Apps (freie Wahl aus 65 Applikationen)
- 1&1 WebAnalytics
- 1&1 Online Office
- PHP5, PHP Dev, Zend Framework, Ruby, SSI, SSH-Zugang, git Versionsmanagement
- NEU: 99,99% Verfügbarkeit
- NEU: Geo-redundante Infrastruktur

1&1 DUAL UNLIMITED

14,99 €/Monat*

~~29,99 €/Monat~~

50% Rabatt:
6 Monate 14,99 €/Monat, danach 29,99 €/Monat*

Weitere Pakete auf der nächsten Seite.

Alle Hosting-Lösungen im Überblick sowie viele weitere Sparangebote unter:

1&1

0 26 02 / 96 91 **0800 / 100 668**

www.1und1.info

* Mindestvertragslaufzeit 12 Monate. Einrichtungsgebühr 14,90 €. Preise inkl. MwSt.

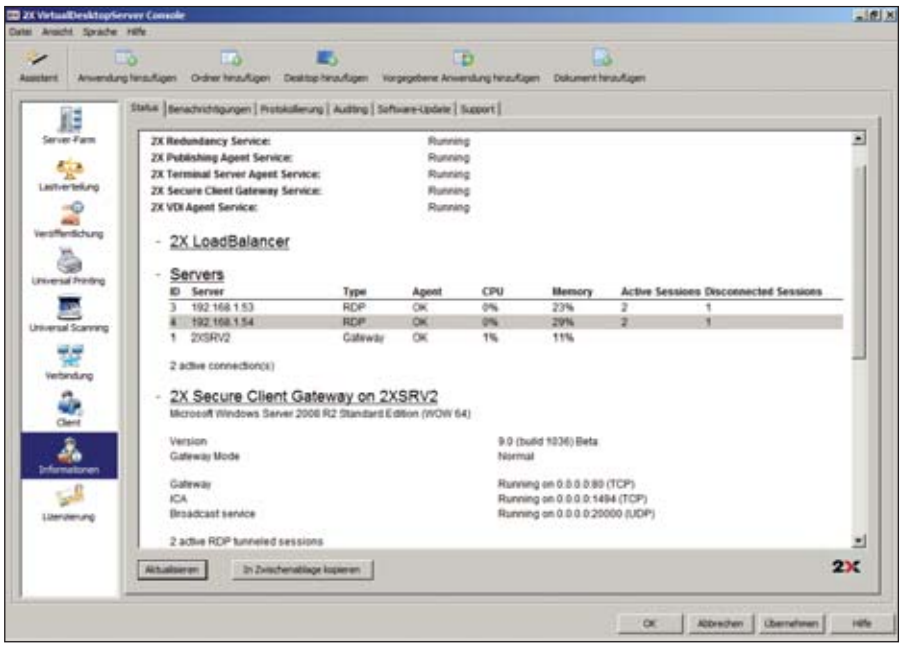


Bild 4: Eine informative Übersicht verrät jederzeit die aktuelle Last und deren Verteilung innerhalb der Farm

zu einer VDS-Farm anzulegen, damit der Client weiß, wo er einen VDS-Server oder ein Secure Client-Gateway findet.

Bezüglich der Verbindungseigenschaften kennt der Client drei Betriebsmodi. Bei der Direktverbindung wird VDS am wenigsten belastet, denn der Client fragt dort nur kurz an und bekommt einen Terminalserver zugewiesen, zu dem er sich dann direkt verbindet. Im Modus "Regulärer Gateway" läuft die gesamte Kommunikation über ein Secure Client Gateway ab, ebenso bei der Einstellung "SSL-Verbindung", bei der aber noch zusätzlich verschlüsselt wird. Der Client ist so aufgebaut, dass sich mehrere Verbindungen anlegen lassen. Auf diesem Weg sind mehrere Farmen erreichbar, so dass ein Administrator nicht alle Veröffentlichungen in eine Farm packen muss, falls das sinnvoller ist.

Beim Aufruf des Clients wird die an der VDS-Konsole vorgegebene Menüstruktur mit den freigegebenen Applikationen und Desktops angezeigt. Wie schon erwähnt, sind die Objekte auch im Startmenü oder optional auf dem Desktop mit eingebunden. Ein Doppelklick auf eine Anwendung startet diese "seamless", also ohne Rand so wie eine lokal aufgerufene Applikation. Letztendlich merkt der Anwender kaum, dass er eine Anwendung auf einem Terminalserver aufruft und nicht lokal.

Neben den beschriebenen normalen Clients ist es weiterhin möglich, Thin Clients mit PXE-Boot zu nutzen. Hierzu bietet 2X ein ThinClientOS zum Download an, das dann über ein Secure Client Gateway den Zugriff auf die von VDS bereitgestellten Ressourcen ermöglicht. Wichtig für diese Funktion ist es, dass auf dem Secure Client Gateway das PXE-Booting aktiviert ist.

Neben der Bereitstellung über die verschiedenen Clients bietet VDS einen Zugriff über ein Webportal an, genannt 2X Access Portal. Auch hier lassen sich verschiedene Farmen eintragen. Das Portal kann auf einem VDS-Server oder an anderer Stelle eingerichtet werden. Den Installationsablauf empfanden wir als etwas hakelig, da in den Voraussetzungen nur der IIS und das .NET-Framework 2.0 genannt sind, es sich dann aber auf unserem Windows Server 2008 R2 im Laufe des Setups herausstellte, dass doch noch einzelne Rollendienste wie ASP.NET, Verwaltungsskripte und statischer Inhalt fehlten. Statt nur einmal die Voraussetzungen zu prüfen und dann eine komplette Aufstellung aller fehlenden Komponenten zu liefern, wurde eine nach der anderen reklamiert, was jedes Mal Abbruch und Neustart des Setups erforderte.

Die Oberfläche des Access-Portals wird für die Auswahl der Applikationen und Desktops dynamisch aufgebaut und berücksichtigt die Filtermöglichkeiten, so dass jeder Anwender genau die Icons zu den Ressourcen sieht, für die er berechtigt ist. Über einen Administrator-Login gelangen berechtigte Nutzer zu einer Seite mit Einstellungen, um das Portal zu konfigurieren.

Produkt
Programm für Server-basiertes Computing mit Terminalserver- und Hypervisor-Unterstützung.

Hersteller
2X
www.2x.com/de/

Preis
VDS Small Business (ein Server, 80 Desktops, ein Gateway) kostet 900 Euro, VDS Professional (zwei Server, 160 Desktops, zwei Gateways) schlägt mit 2.550 Euro zu Buche und VDS Enterprise (drei Server, unlimitierte Desktops und Gateways) ist für 5.150 Euro zu haben.

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

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

Veröffentlichung von Applikationen und Desktop	9
Clientunterstützung	9
Administration der Zugriffsrechte	8
Absicherung der Datenkommunikation	9
Hypervisorunterstützung	9

Dieses Produkt eignet sich

optimal für den Einsatz in heterogenen Umgebungen, wo Desktops und Applikationen von verschiedenen Quellen an unterschiedliche Benutzergruppen bereitgestellt werden sollen. Je komplexer die Umgebung ist, desto besser kann VDS seine Stärken ausspielen.

bedingt für reine Terminalserver-Umgebungen mit einheitlicher Bereitstellung. Hier reicht gegebenenfalls auch der Betrieb einer nativen Windows Terminalserver-Farm.

nicht für Umgebungen, die ausschließlich mit lokalen Ressourcen arbeiten und in denen keine Anwendungen oder Desktops zu veröffentlichen sind.

2X VirtualDesktopServer 9

Terminalserver mit Mehrwert

Beim Einsatz von Terminalservern bietet VDS ähnlich wie Citrix einigen Mehrwert gegenüber der nativen TS-Nutzung. Selbstverständlich unterstützt VDS die neuen Funktionen von RDP7 wie Umleitung des Media Players mit Video und Audio sowie eine erweiterte Bitmap-Beschleunigung. Neben der Funktion Universal Printing hat VDS ein Universal Scanning im Angebot. Twain-kompatible Anwendungen können so Scan-Hardware auf entfernten Clients verwenden, ohne dass am Server Gerätetreiber installiert werden müssen.

Möglich ist ferner ein Multimonitor-Betrieb, und in Verbindung mit einem Terminalserver unter Windows Server 2008 R2 sowie einem Windows 7-Client wird Aero Glass unterstützt. Bereits erwähnt wurden die diversen Filterfunktionen nach Benutzern, Gruppen und IP- sowie MAC-Adressen, die vor allem bei unterschiedlichen Nutzergruppen und komplexen Umgebungen sehr nützlich sind. Die Anmeldung wird durch ein konfigurierbares Single Sign-On vereinfacht. Neben dem automatischen Durchreichen der Systeminformationen lässt sich auch ein beliebiger anderer Anwender mit Benutzername hinterlegen.

Erfreulich umfangreich und gut verständlich ist die verfügbare Dokumentation. Neben dem zentralen Handbuch gibt es diverse zusätzliche Dokumente wie beispielsweise Beschreibungen zur Einrichtung der VDI Agent Appliances, des Web-Portals und des Einsatzes von Deepnet zur Zwei-Faktor-Authentifizierung.

Fazit

Insgesamt hat der 2X VDS im Test voll überzeugt. Dem Hersteller ist es gelungen, einen beachtlichen Funktionsumfang mit einer wirklich einfachen Bedienung zu kombinieren. Der VirtualDesktopServer von 2X vereint die Veröffentlichung von Applikationen und Desktops über Microsoft Terminalserver sowie Citrix und die Bereitstellung von virtuellen Desktops in einem Produkt. Darüber hinaus lassen sich die Desktops eigenständiger PCs veröffentlichen. Beeindruckend ist der sehr breite Hypervisor-Support für praktisch alle namhaften Produkte. Mindestens ebenso beeindruckend ist die Client-Palette, die neben Windows- und Linux-Systemen auch einen allgemeinen Java-Client sowie die Unterstützung für Android und iOS umfasst.

Als sehr effizient erschien uns die zentrale Konsole, über die alle Administrationsschritte erfolgen. Gefallen hat uns weiterhin, dass sich mit VDS mehrere Terminalserver-Farmen sowie VDI-Hosts administrieren und für unterschiedliche Benutzerzugriffe gruppieren lassen. Damit ist die Betreuung einer überaus heterogenen Umgebung mit unterschiedlichsten Anforderungen der einzelnen Anwender von einem zentralen Punkt aus gegeben. Die Einrichtung mehrerer Publishing-Server im Master-/Backup-Prinzip sorgt für eine hohe Verfügbarkeit. Die Nutzung von Secure Client Gateways, bei denen der gesamte Datenverkehr über einen Port getunnelt und bei Bedarf verschlüsselt wird, prädestiniert das Produkt für den Einsatz in Umgebungen mit erhöhten Sicherheitsanforderungen. *(ln)*

Im Test: XP Unlimited Enterprise

Terminalserver light

von Thomas Bär

XP Unlimited ist eine Software-Erweiterung für Windows-Computer, um auf diesen einen mehrfachen Zugriff über das Remote Desktop Protocol zu ermöglichen. XP Unlimited bietet im Vergleich zu den herkömmlichen Microsoft-Terminalservern ähnliche Funktionen und stellt eine einfache Lösung für Server based-Computing dar. Die Software wandelt dabei gewöhnliche PCs mit Windows XP Professional, Vista oder Windows 7 in Terminalserver um. Ergänzende Funktionen wie eine Anwendungsverwaltung und -freigabe, verschlüsselter Zugriff per SSL und Lastverteilung werten das kostengünstige Produkt auf. Unser Test nimmt unter die Lupe, ob sich die vielversprechenden Features in der Praxis bewähren.

Arbeitsstationen, die auf einen mit XP Unlimited (XPU) zum Server gewordenen PC zugreifen, müssen lediglich über eine RDP-Client-Software verfügen. Diese wird bei aktuellen Windows-Versionen mitgeliefert oder lässt sich bei älteren Windows-Betriebssystemen wie Windows 9x, NT oder 2000 als Download nachrüsten. Alle gängigen Betriebssysteme, von Unix über Mac OS bis hin zu verschiedensten Linux-Distributionen, unterstützen das Microsoft RDP-Protokoll. XPU verfügt zusätzlich über einen eigenen RDP-Client, der bei den Features Load Balancing, SSL-Gateway und nahtlose Desktopintegration zu verwenden ist.

XPU ist in der sogenannten "Classic Version" auf Windows XP Professional, Vista ab Business und Windows 7-Betriebssystemen lauffähig. Der Hersteller bietet Lizenzen für 5, 10 oder unlimitierte Benutzer. Die Anzahl zugewiesener Programme pro Benutzer und die Zugriffe auf Programme sind nicht eingeschränkt. Die "Enterprise Version" unterstützt zusätzlich Windows Server 2003, 2008 und die entsprechenden SBS-Varianten. Die Benutzerkonten können direkt aus dem Active Directory einer Domäne übernommen werden. Zusätzlich stehen Features wie Lastenverteilung bei mehr als einem Server und SSL-Verschlüsselung zur Verfügung.

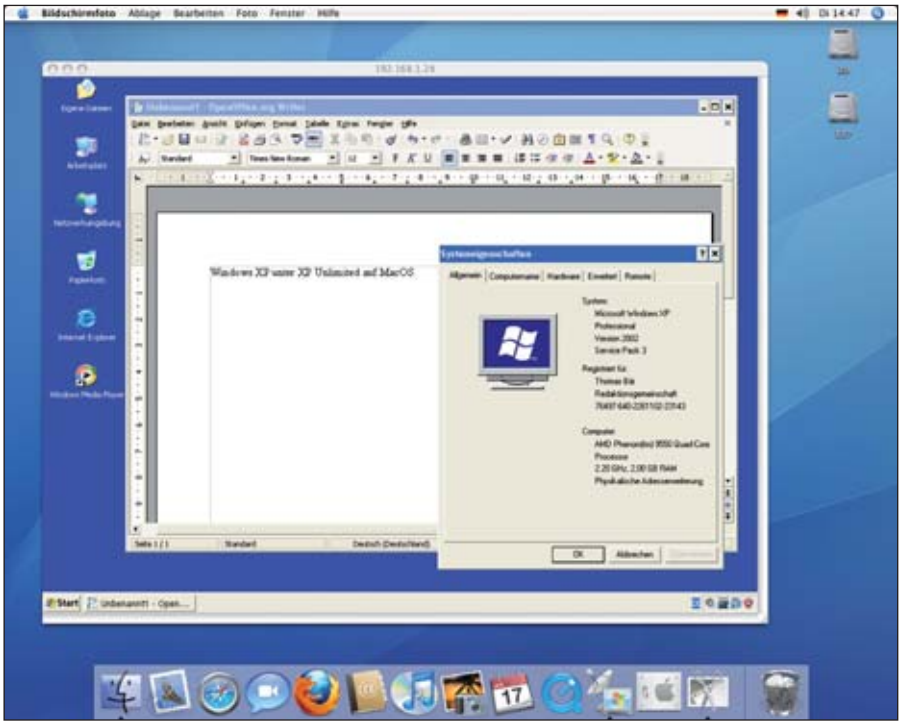


Bild 1: Dank der Verfügbarkeit von RDP-Client-Programmen sind XPU-Server über die Betriebssystemgrenzen hinweg faktisch überall einsetzbar – wie hier unter Mac OS

Systemvoraussetzungen

Computer mit Pentium III-Prozessor mit 500 MHz oder besser (empfohlen: Pentium 4 mit 2,4 GHz), 512 MByte Arbeitsspeicher (empfohlen: 1 GByte), rund 100 MByte freier Festplattenspeicher, Microsoft Windows XP Professional oder höher, Microsoft Internet Explorer 5.5 oder höher, Ethernet-Netzwerkadapter, installiertes TCP/IP-Netzwerkprotokoll.

Installation mit vielen Auffälligkeiten

Gemäß der insgesamt guten, auch in Deutsch verfügbaren Dokumentation müsste der Installationsvorgang eigentlich spielend einfach sein. In der Produktbeschreibung heißt es zudem überschwänglich, dass selbst Laien mit XPU ohne Schwierigkeiten zurechtkommen. Genau der Dokumentation folgend luden wir zunächst die 60-Tage-Testversion für maximal drei gleichzeitige RDP-Verbindungen von der Homepage des Herstellers. Während die meisten Softwareproduzenten einen einzigen Installer programmieren, findet der XPU-Neuanwender auf der Homepage verschiedene Versionen: Zwei Downloads für Windows XP, zwei

Downloads für Windows Vista und so weiter. Da die Software selbst ebenfalls in zwei Editionen, der Classic- und Enterprise-Variante, angeboten wird, steigert sich die Download-Liste auf insgesamt recht unübersichtliche 13 Einträge.

Für den ersten Test wollten wir eine Classic-Installation für Windows Vista in der 32-Bit-Form einsetzen. Der Download der nur knapp 20 MByte großen Datei war schnell erledigt und ein Doppelklick sollte, gemäß der Anleitung, nach dem Entpacken das Setup starten. Dies passierte jedoch nicht. Interessanterweise wurde stets eine Softwarekomponente für einen nicht mehr an den PC angeschlossenen USB-Scanner aktiviert. Dieses Phänomen wurde dem deutschen Distributor per E-Mail mitgeteilt, aber bis zum Abschluss der Testphase erhielten wir hierzu keine Antwort. Andere Fragen beantwortete der Deutschlandvertrieb innerhalb kürzester Zeit und stets kompetent.

Wir wichen auf einen 32 Bit Windows XP SP3-Rechner ohne Domänenzugehörigkeit aus. Hier verlief der Installationsvorgang ohne Schwierigkeiten und war nach wenigen Minuten erfolgreich abgeschlossen. Eine weitere Testinstallation, ebenfalls unter Windows XP SP3, diesmal jedoch in der Enterprise-Edition für Active Directory-Domänen, ergab erneut Auffälligkeiten. Der Installer pochte auf einen Neustart, da angeblich ein Installationsvorgang noch nicht abgeschlossen worden sei. Nach Abschluss der Installation, die mit einem weiteren Neustart endete, wurde seltsamerweise ein

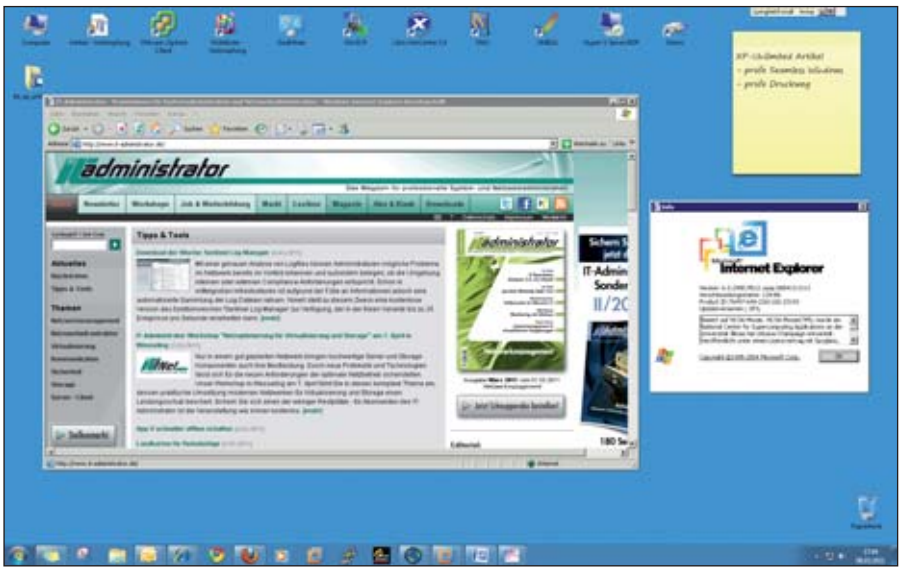


Bild 2: Mit Seamless Windows fühlt sich ein Internet Explorer 6 unter Windows 7 beinahe echt an. Leider landen Downloads nicht im Dateisystem des Client, sondern auf dem XPU-Hostrechner.

Benutzerkonto vorgeschlagen, dessen Kennwort uns unbekannt war. Diesen Account hatte der Installer automatisch angelegt. Eine Auswahl der Domäne war zunächst nicht möglich und die in der "Verwaltung" der "Systemsteuerung" zu findende Management-Oberfläche von XPU war nicht vorhanden. Einen Neustart später ließ der PC wieder eine Domänenanmeldung zu. Die Verknüpfung auf die Verwaltungsoberfläche jedoch mussten wir uns manuell anlegen.

Nach diesem Installationsdurcheinander mit vielen Fragezeichen zeigte sich XPU von einer äußerst funktionellen und stabilen Seite. Alle RDP-Zugriffe von verschiedenen Clients, seien es nun Thin Clients, Windows-PCs oder MacOS-Computer, auf den "XP Unlimited Server" verliefen problemlos und zügig. Direkt nach der Installation war ein Zugriff über RDP auf die XPU-Maschine über das Netzwerk möglich. Der Installer fügte die Gruppe "Domänen-Benutzer" der lokalen Gruppe "Remotedesktop-Benutzer" hinzu. Jeder reguläre Benutzer aus dem Active Directory konnte sich somit per RDP auf dem Computer anmelden.

Im RDP-Fenster findet sich die von den Remotedesktopdiensten gewohnte Anmeldemaske. Nach der Eingabe von Benutzernamen und Passwort erscheint für einige Augenblicke ein kleines Hinweisfenster, dass die Benutzereinstellungen geladen werden. Lediglich an dieser Stelle und bei der Abmeldung ist die Bezeichnung "XP Unlimited" zu lesen. Ansonsten ist das Look & Feel für den Anwender identisch mit einem ausgewachsenen Terminalserver. Das Start-Menü von Windows in der RDP-Sitzung trägt ebenfalls den Schriftzug "Windows Terminal Server". Einschränkungen hinsichtlich des Mappings von Client-Laufwerken in die Sitzung, der Verwendung von Smart-Cards und des Zugriffs auf die serielle Schnittstelle gibt es von Seiten XPU nicht.

Terminalserver mit Einschränkungen und Erweiterungen

Der erste Blick des Administrators fällt nicht selten auf den Task-Manager von Windows. Wie bei einem Terminalserver, so weist auch das Client-Betriebssystem verschiedene Benutzer in unterschiedlichen Sitzungen aus. Identisch mit dem Server wird im Task-Manager auch der Benutzer einer Applikation ausgewiesen. Für den Administrator ist es so ein Leichtes, exakt zu identifizieren, welche Instanz einer Software zu welchem Anwender gehört.

Bei aller Ähnlichkeit liegt es natürlich nahe, über die Terminaldienste-Verwaltung von Microsoft auf den "XPU Terminalserver" zuzugreifen. Dass es sich bei XPU nicht um einen Microsoft-konformen Terminalserver handelt, merkt der Administrator an dieser Stelle, denn der Zugriff

Die Lizenzfrage

XP Unlimited von IP Consult ist ein Zusatzprogramm zu Microsoft Windows. Es bietet oder ersetzt nicht eine ausreichende Lizenzierung durch Microsoft. XP Unlimited selbst enthält keine Lizenzen von Microsoft für Betriebssysteme oder den Zugriff auf Terminal Services. Gemäß den Microsoft-Lizenzverträgen zu Windows XP und Windows Vista heißt es, dass eine unbeschränkte Anzahl von Verbindungen über das Remote Desktop Protocol zulässig ist. "Für eine entsprechende betriebssystemseitige Lizenzierung wenden Sie sich bitte an Ihren IT-Berater", heißt es in der Produktbeschreibung von XP Unlimited.

über die Management-Oberfläche von Microsoft ist nicht möglich. Die für die Steuerung von Terminalservices benötigten Softwarekomponenten bringt XPU selbst mit, dazu später mehr.

Wenn es sich nicht wirklich um einen Terminalserver handelt, wie steht es dann mit den Anforderungen für die Applikationen? In der Produktdokumentation heißt es hierzu, dass XPU deutlich mehr Anwendungen zur Verfügung stellen kann, als es mit Microsoft Terminal Services möglich ist. Programme auf einem XPU-Server müssen überhaupt nicht "Terminalserver"-kompatibel sein, um per Server based-Computing genutzt zu werden. Alle getesteten Anwendungen, beispielsweise Open Office, funktionierten wie gewohnt. Eine offizielle Liste der unterstützten Applikationen bietet der Hersteller nicht und verweist auf die 60-Tage-Testversion seiner Software, die ausreichend Zeit für eine Teststellung bietet.

Nicht alle Softwarehersteller erlauben den gleichzeitigen Einsatz ihrer Software durch verschiedene Benutzer auf einem einzigen Rechner. Hier hilft nur der Blick in die Softwarelizenzbestimmungen des jeweiligen Herstellers, um etwaige Lizenzverstöße zu umgehen. Während die Remote Desktop-Technik für eine Vielzahl von Applikationen ausreichend ist, so können Programme, die auf einen direkten Grafikkartenzugriff angewiesen sind, über diesen Weg nicht bereitgestellt werden. Auch wenn es sich um Windows XP als Betriebssystem handelt, so funktionieren diese Programme nicht über RDP.

Applikationseinstellungen und Zugriffsrechte

Wie bereits erwähnt, fanden wir die Management-Software von XPU in unserer Testinstallation nicht am erwarteten Ort. Nach kurzer Suche entdeckten wir sie im Standard-Programmpfad von Windows. Die Verwaltungssoftware besteht aus elf Registern mit Optionen und erklärt sich dank guter Dialogtexte weitgehend von allein. Soll beispielsweise die Anmeldung über die Domäne beendet werden, so ist im Register "Domäne/Arbeitsgruppe" durch den Administrator lediglich die Option "Lokaler Server" auszuwählen. Felder wie "Name des Domänen-Administrators" oder "Domänenname" sind selbstsprechend.

Eines der wichtigsten Register ist "Applikationen". Hier steuert der Administrator, ob ein Benutzer den Desktop zu sehen bekommt und welche Applikationen er starten darf. Die Zuordnung lässt sich sowohl für Domänen-Benutzer als auch lokale Benutzer vornehmen. Die Zuweisung geschieht auf Basis von Benutzergruppen durch einfaches Anklicken. Programmpfade muss der Administrator nicht manuell eingeben. In dem Programmfenster wird durch das Drücken der Taste F3 der Windows Explorer zur Auswahl geöffnet. Sollen mehrere Programme einer Benutzergruppe zugewiesen werden, so bestimmt der Administrator, welche Software gestartet wird und welche durch ein kleines Menü in der Sitzung zur Auswahl steht. Konstellationen, in denen Benutzern lediglich der Zugriff auf den Browser gegeben werden soll, sind mit fünf Mausklicks erledigt und sofort einsetzbar. Einstellungen der Software kann der Administrator importieren, exportieren, speichern und laden.

Der Thematik "Drucken" nähert sich XPU über mehrere Seiten. Das Ansprechen der lokal installierten Drucker ist für jeden Anwender ohne zusätzliche Konfiguration sofort möglich. Einsatzszenarien von Schulungsräumen oder Büros, in denen sich drei Benutzer einen Windows-PC nebst Drucker teilen, sorgen beim Administrator für keinerlei Kopfzerbrechen. Netzwerkdrucker spricht Windows von Haus aus "pro Benutzer" an – diese sind somit ohne Abweichung vom Standard verwendbar. Über die Integration eines PDF-Writers besteht zudem die Möglichkeit, die Ausdrucke der Benutzer in Dateien zwischenzuspeichern.

Nahtlos auf dem lokalen Desktop

Der Hersteller von XP Unlimited liefert mit *xpuWin32client.exe* eine eigene RDP-Client-Software für Windows-Computer mit. Die "32" im Titel beschränkt die Software nicht auf 32-Bit-Versionen von Windows. Sowohl unter Windows 7 x64 als auch unter einem deutlich in die Jahre gekommenen Windows Me 16/32-Betriebssystem startet die Datei. Seamless Windows, die nahtlose Integration einer Terminalserverapplikation in den Desktop des lokalen Betriebssystems, ist mit XPU grundsätzlich möglich. Wird die Client-Software auf Windows XP oder höher mit gesetztem Optionshäkchen "Seamless" gestartet, so erscheint eine Applikation ohne den RDP-Rahmen direkt auf dem lokalen Desktop. Ein kleines, graues Menü am rechten Bildschirmrand erlaubt den Wechsel zwischen den Programmen in der Terminalsitzung.

Produkt
Software zur zentralen Bereitstellung von Applikationen über das RDP-Protokoll.

Hersteller
IP Consult BV
www.xpunlimited.com

Preis
XP Unlimited Classic für 5 Benutzer: 196 Euro
XP Unlimited Classic für 10 Benutzer: 226 Euro
XP Unlimited Classic unbegrenzte Nutzerzahl: 279 Euro
XP Unlimited Enterprise unbegrenzte Nutzerzahl: 577 Euro

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

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

Installation	5
Einrichtung	8
Mehrbenutzerfähigkeit	8
Applikationsbereitstellung	7
Desktopintegration	5

Dieses Produkt eignet sich

optimal für Unternehmen, die schnell und einfach Remotedesktopdienste auf Standardhardware bereitstellen und im Sinne der "Green IT" die Laufzeit von PCs als Thin Clients verlängern möchten.

bedingt für Unternehmen, die bereits andere Terminalserver-Lösungen mit der dazugehörigen Management-Software im Einsatz haben.

nicht für Unternehmen, in denen die Lizenzbestimmungen den multiplen Benutzerzugriff auf Applikationen verbieten.

XP Unlimited Enterprise

Die "Seamless"-Windows sind eine sehr schöne und für den Anwender intuitive Sache – bis zu einem gewissen Punkt. Speichert beispielsweise ein Anwender einen Download auf dem "Desktop", so erscheint die heruntergeladene Datei nicht auf dem lokalen Client-Desktop, sondern auf dem unsichtbaren Desktop des XPU-Servers. Die Zuordnung von Dateinamenerweiterungen, der Suffix – beispielsweise ".xls" für Microsoft Excel – ist über den XPU-Client leider nicht möglich. Andere am Markt befindlichen Lösungen, die die Terminalservices von Microsoft erweitern, beispielsweise ProPalms TSE oder H&H NetMan, sind hierzu in der Lage. Es bleibt für den Benutzer somit die Problematik des mehrfachen Desktops.

Webbrowser und andere Goodies

XPU in der Enterprise-Version bietet einen integrierten Webserver, über den Benutzer des Microsoft Internet Explorer per ActiveX-Erweiterung direkt auf RDP-Sessions zugreifen. Um die Funktion zu aktivieren, muss lediglich im Register "Webserver" die Option "Webserver aktivieren" angehakt werden. Weitere Einstellungen besitzt die Software nicht. Das Webinterface bietet beinahe dieselben Konfigurationsmöglichkeiten wie ein lokaler RDP-Client: Bildschirmauflösung, Mapping von Geräten und Laufwerken, Geschwindigkeitsoptionen. Lediglich das Abspeichern der Einstellungen ist nicht erlaubt, ebenso der Zugriff über HTTPS auf den Webserver. Verschlüsselte Verbindungen sind ausschließlich über das integrierte SSL-Gateway möglich. Sind mehrere XPU-Server an einem Standort vorhanden, so lassen sich diese mit den Bordmitteln der Software in einen Load Balancing-Verbund verwandeln.

Es gibt Situationen, in denen beispielsweise Netzwerkdienste getestet werden müssen oder eine große Anzahl von ähnlichen Benutzern angelegt werden muss. Dies gestaltet sich mit den von Windows zur Verfügung gestellten Mitteln mühevoll. Der Hersteller IP Consult bietet hierfür das kostenlose Tool "Generate Users and Groups" an, mit dessen Hilfe der Administrator bis zu 999 Benutzer oder Benutzergruppen anlegen und wieder löschen kann.

Fazit

XP Unlimited ist ohne Frage eine spannende Software, die sich als kleine Alternative zum Terminalserver gut einsetzen lässt. Das Aufgabengebiet ist jedoch auf einige Spezialgebiete – beispielsweise Schulungsumgebungen oder die bereits genannte Zwei- bis Dreifach Nutzung in einem Büro – begrenzt. Die aktuell getestete Version ist seit Oktober 2010 auf dem Markt, eine neue Version bereits in Planung. Künftig soll die Integration zwischen Client und dem Remote-Desktop verbessert werden, beispielsweise durch ein vereinfachtes Drucken und die optimierte Ordner-Ansicht auf dem Server. Weiterhin plant der Hersteller die Bereitstellung verschiedener Versionen der Client-Software für Windows 32, Windows 64, Linux 32, Linux 64 und Mac OS. Ein Druck-Steuerprogramm, Verwaltungstools für das SSL-Gateway und eine "Lizenzvermietung" für einen begrenzten Zeitraum runden die positive Aussicht für XP Unlimited ab. *(jp)*

Im Test: Citrix XenDesktop 5

Runderneuerte Desktop-Schmiede

von Christian Knermann

Mit XenDesktop 5 hat Citrix Ende 2010 die jüngste Version der hauseigenen Infrastruktur zur Bereitstellung virtueller Desktops vorgestellt. Dieses Release bricht mit der Tradition der Vorgängerversionen und setzt auf eine von Grund auf neugestaltete Architektur. IT-Administrator hat sich angesehen, welche Neuerungen dies für Sie als Administrator mit sich bringt.

Seit der Markteinführung hat Citrix XenDesktop kontinuierlich Verbesserungen erfahren. Mit einer Frequenz von teilweise weniger als sechs Monaten kamen neue Versionen auf den Markt. Wenngleich viele Funktionen hinzukamen und sich die GUI der Administrationskonsolen mehrfach änderte, blieb die grundlegende Architektur dabei stets gleich. Um das Management der Desktops kümmerte sich der Desktop Delivery Controller (DDC), der bis hin zu XenDesktop 4 im Kern eigentlich auf einem zweckentfremdeten XenApp Terminalserver basierte. Mehrere DDCs ließen sich zwecks Lastverteilung und Verfügbarkeit in eine Farm integrieren.

Die Grundlage einer solchen Farm bildete die Independent Management Architecture (IMA), die bereits zu Anfang des Jahrtausends mit Citrix MetaFrame eingeführt worden war. IMA umfasst eine Datenbank und mehrere Windows-Dienste, über die teilnehmende Server Informationen zum Status der Farm austauschen. Als naher Verwandter von MetaFrame nutzten auch die DDCs diese Architektur. Nach Angaben des Herstellers reichte dies zwar aus, um mehrere tausend Desktops zu verwalten. Da IMA aber nie für diesen Zweck konzipiert worden war, ließ sich die Lösung nicht bis auf fünfstellige Zahlen von Desktops skalieren. So bricht XenDesktop 5 mit der bisherigen Technik und bringt eine komplett neu entwickelte Infrastruktur mit.

Überarbeitete Architektur

Die Site tritt nun als oberste Organisationseinheit an die Stelle der Farm. Eine Site umfasst einen oder mehrere Virtualisierungshosts zur Bereitstellung von Desktops. Diese werden in sogenannten Catalogs, Gruppen gleichartiger VMs, zusammengefasst. Eine "Desktop Group" bildet dabei eine Zuordnung von Maschinen zu Benutzer-Accounts im Active Directory. Als Verbindungsbroker zwischen Clients und den Desktop-VMs fungiert weiterhin der DDC, dessen Unterbau sich allerdings deutlich verändert hat (siehe Bild 1). Der DDC spricht direkt mit einem SQL Server. Innerhalb der SQL-Datenbank wird die Konfiguration der Site zentral vorgehalten. Zur Verwaltung nutzen Administratoren das "Desktop Studio", eine MMC-basierte Konsole. Über diese lassen sich die Catalogs und Desktop Groups verwalten. Zusätzlich existiert mit dem "Desktop Director" ein einfacheres Webfrontend für typische Support-Aufgaben. Über dieses Interface ist es zwar nicht möglich, Desktops zu erstellen oder zu löschen, Helpdesk-Mitarbeiter können aber auf einfache Weise Echtzeit-Informationen zu laufenden Verbindungen anzeigen und beispielsweise hängende Sitzungen zurücksetzen.

Um das Erstellen gleichartiger Desktops kümmern sich die neuen "Machine Creation Services". Die MCS verwenden eine virtuelle Maschine als Vorlage, von der sie einen Snapshot erstellen und auf einen separaten Storage-Bereich kopieren (siehe Bild 2). Der Hersteller empfiehlt, hierzu eine NFS-Freigabe zu verwenden, da der XenServer in diesem Fall Thin Provisioning nutzt. So wird nur der tatsächlich notwendige Speicherplatz belegt. Die Snap Copy dient als Basis für beliebig viele gleichartige Desktops. Dies wird möglich, indem der eigentliche Snapshot als Master-Image schreibgeschützt abgelegt wird. Sämtliche VMs erhalten zwei weitere Disks – eine Diff Disk, in der sämtliche Änderungen am Master Image abgelegt werden, sowie eine Identity Disk, die pro Maschine persistent deren Identität im Active Directory speichert. Gegenüber den VMs erscheinen diese Disks transparent als eine Festplatte. Clients authentisieren sich gegenüber dem DDC, der Verbindungen zu den

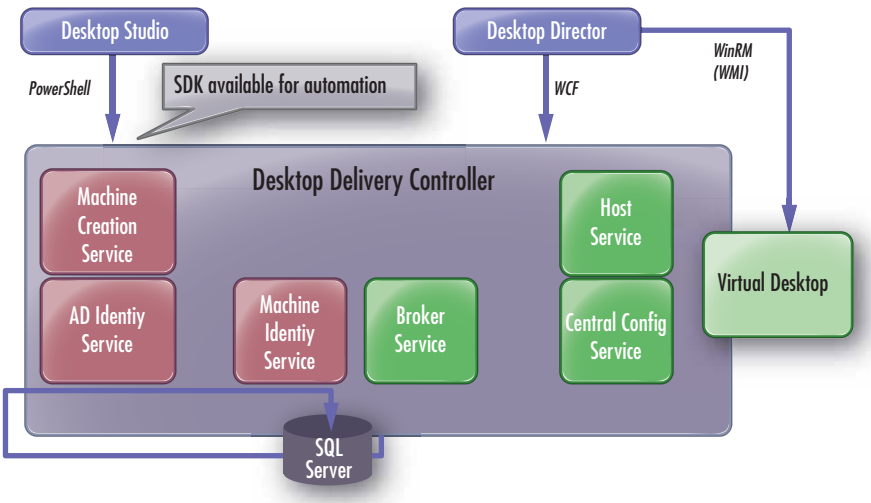


Bild 1: Der Desktop Delivery Controller steht im Mittelpunkt der XenDesktop-Infrastruktur

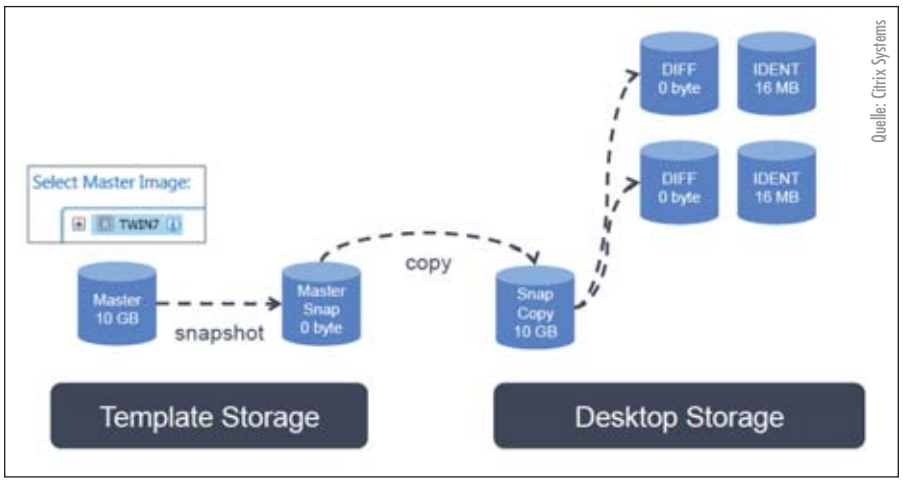


Bild 2: Die Machine Creation Services kümmern sich um die Erstellung von Desktops

Desktops vermittelt. Daraufhin kommt über das Remote-Protokoll ICA eine direkte Kommunikation zwischen Client und Desktop zu Stande.

Lizenzierung wieder mit Concurrent User-Modell

XenDesktop ist in vier verschiedenen Varianten erhältlich [1]. Die "VDI Edition" unterstützt ausschließlich virtuelle Desktops. Diese dürfen auf einem XenServer, Hyper-V oder VMware-Host laufen. Als "Express Edition" ist diese Funktionalität für bis zu zehn virtuelle Desktops kostenfrei zu haben. Die "Enterprise Edition" integriert auch physische Maschinen. Zusätzlich ist in dieser Edition die Terminalserver-Lösung XenApp enthalten, so dass Desktops darüber mit zusätzlichen Applikationen versorgt werden können. Die "Platinum Edition" schließlich ergänzt das Portfolio um weitere Citrix-Produkte, darunter Monitoring und Statistik mittels EdgeSight oder Optimierung des WAN-Zugriffs über den Citrix Branch Repeater.

Das Lizenzmodell hat Citrix in der Vergangenheit mehrfach überarbeitet. Ursprünglich war XenDesktop wie von XenApp bekannt auf der Basis gleichzeitiger Benutzung (Concurrent Use, CCU) zu lizenzieren. Der Versuch, auf namentlich benannte Benutzer oder Endgeräte (Named User/Device) umzustellen, wurde vom Markt nicht mit Freuden aufgenommen. Entsprechend hat Citrix in einem ersten Schritt für die VDI Edition das Concurrent User-Modell wieder eingeführt. Seit Januar 2011 ist für alle Editionen die CCU-Option wieder verfügbar. Im Rahmen des sogenannten Trade-Up-Programms haben Bestandskunden außerdem die Möglichkeit, vorhandene XenApp-Lizenzen gegen XenDesktop einzutauschen [2].

Da sich die Preise für Named User/Device und CCU-Lizenzen deutlich unterscheiden, ist je nach Szenario abzuwägen, welche Option die günstigere ist. Als Richtwert ist davon auszugehen, dass sich die Lizenzierung pro Named User/Device erst dann rechnet, wenn mehr als 50 Prozent aller namentlich benannten Benutzer gleichzeitig auf virtuellen Desktops oder Terminalservern arbeiten wollen.

Installation in Active Directory-Domäne

Für unsere Testinstallation nutzten wir eine Active Directory-Domäne sowie einen Pool mehrerer Virtualisierungshosts unter Citrix XenServer 5.6 FP1. Darin installierten wir eine Windows 7-VM und einen Windows Server 2008 R2 als DDC. Die XenDesktop-Images luden wir aus dem MyCitrix-Portal herunter. Wir meldeten uns als Domänen-Administrator an unserem virtuellen Server an und verbanden das XenDesktop 5 ISO-Image. Daraufhin startete per Autorun der Installationsassistent. Dieser erkannte das Server-Betriebssystem und bot entsprechend die Installation der XenDesktop Server-Komponenten an. Als weitere Option standen die "Extras" zur Wahl. Neben Links zu den Release Notes und der Online-Dokumentation kann dort das Desktop Studio einzeln installiert werden. Zu den Extras zählt zudem die Management-Lösung für die Zero Clients vom Typ Xenith des Herstellers Wyse.

Wir starteten das Setup mit der Option "Install XenDesktop". Im nächsten Schritt wurden uns daraufhin sämtliche Komponenten der XenDesktop-Infrastruktur angeboten. Standardmäßig sind alle Bausteine ausgewählt. Alternativ ist es hier natürlich möglich, einen bereits vorhandenen SQL-Server zu nutzen oder den Web-Access separat zu installieren. Wir beließen es für den Test aber bei der Standardauswahl und installierten alle Komponenten. Der Assistent bot daraufhin an, die nötigen Anpassungen der Windows Firewall für den Lizenzserver vorzunehmen.

Im folgenden Dialogschritt wurde uns eine Zusammenfassung der anstehenden Aktionen angezeigt. Neben den eigentlichen Komponenten umfasste dies sämtliche Voraussetzungen wie das .NET Framework oder den Webserver IIS. An dieser Stelle wurde eine wesentliche Verbesserung gegenüber dem Installationsprozess von XenDesktop 4 sichtbar. Administratoren der Vorgängerversionen dürften sich noch daran erinnern, dass die Installation oftmals abgebrochen werden musste und erst in mehreren Anläufen gelang, da fehlende Voraussetzungen nicht vorab erkannt wurden und manuell erfüllt werden mussten. Dies gehört nun der Vergangenheit an: Nachdem wir über die Schaltfläche "Install" die Einrichtung gestartet hatten, kümmerte sich der Assistent automatisch um die Installation der benötigten Windows-Komponenten. Nach der Einrichtung aller Komponenten war zu unserer Überraschung kein Neustart des Servers erforderlich. Wir verließen den Assistenten über die Schaltfläche "Close".

Neuerungen in XenDesktop 5.0

- Komplett neue Architektur (ohne IMA)
- Unterstützung für Windows Server 2008 R2 auf dem DCC
- Rollenbasiertes Setup
- Deutlich vereinfachte Administration mit dem Desktop Studio
- Schnelle Bereitstellung von Desktops mit den MCS

Daraufhin startete das Desktop Studio automatisch mit einer aufgeräumten Oberfläche und vier Optionen zur Konfiguration des DDC. Der Punkt "Quick Deploy" dient der besonders schnellen Basiskonfiguration einer Gruppe von Desktops mit Standardwerten. Mit "Join existing deployment" tritt der DDC einer bestehenden Site bei. Das "Desktop Deployment" führt detailliert durch die Einrichtung virtueller Desktops und bietet dabei weitere Möglichkeiten. Mit dem "Application deployment" werden die sogenannten VM Hosted Apps konfiguriert. Dahinter verbirgt sich die Option, einzelne Anwendungen aus einem virtuellen Desktop zu veröffentlichen. Ein solcher "Mini-Terminalserver" macht immer dann Sinn, wenn eine Anwendung aus Gründen von Kompatibilität oder Leistungsanforderungen nicht auf einem Terminalserver untergebracht werden kann. Doch bevor wir uns der weiteren Konfiguration widmeten, kümmerten wir uns zunächst um den Lizenzdienst und die Vorbereitung der Vorlage für unsere Desktops. Über das MyCitrix-Portal luden wir eine Eval-Lizenz herunter und starteten anschließend die License Managment Console, um die Lizenz zu laden.

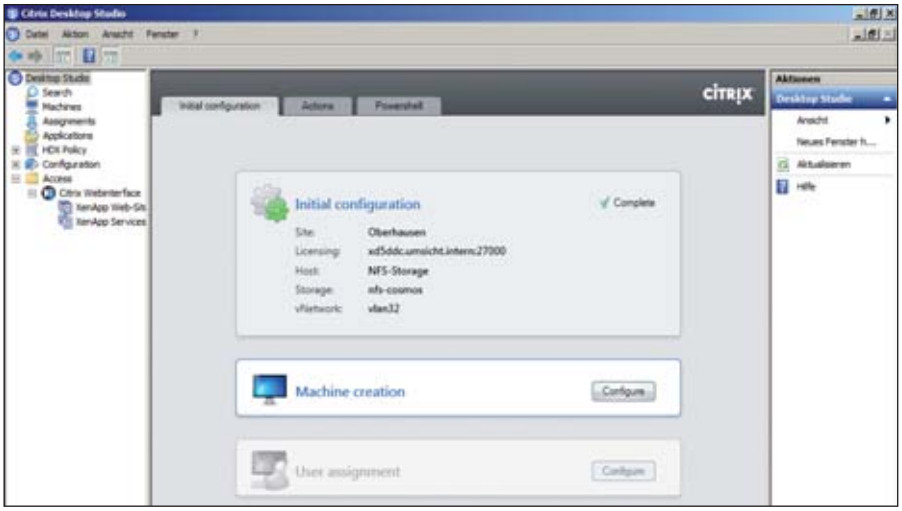


Bild 3: Das Desktop Studio führt mit wenigen Schritten durch die Einrichtung

Virtual Desktop Agent mit eingeschränktem Funktionscheck

Im Anschluss luden wir das XenDesktop ISO-Image in unsere Windows 7-VM. Der Assistent erkannte das Client-Betriebssystem, entsprechend stand neben den "Extras" nur die Installation des VDA zur Wahl. Letztere Option bot wiederum zwei Wege, "Quick Deploy" oder "Advanced Install". Wir entschieden uns für die erweiterte Installation. Neben dem eigentlichen VDA beinhaltet die Setup Routine auch die XenApp Plug-Ins, mit denen ein virtueller Desktop seinerseits als Terminalserver Client agieren kann. Auf diese Option verzichteten wir aber zunächst. Im folgenden Dialog konnten wir unseren DDC eintragen und den Eintrag über die Schaltfläche "Check" testen. Dies betrifft allerdings nur die grundlegende Überprüfung, ob der Zielserver per DNS aufgelöst werden kann. Eine funktionale Prüfung, ob der DDC ordnungsgemäß installiert und konfiguriert ist, findet hier nicht statt.

Der Assistent bot nun an, die Windows Firewall automatisch anzupassen und die VM für den Einsatz als virtuellen Desktop zu optimieren. Weiterhin wurde standardmäßig die Remoteunterstützung aktiviert, da das Spiegeln von Sitzungen zu Supportzwecken nicht über das ICA-Protokoll, sondern über Microsofts RDP erfolgt. Zu guter Letzt wurde das Windows Remote Management aktiviert, damit im Betrieb Echtzeitdaten zum Zustand der Desktops zur Verfügung stehen. Es folgte die eigentliche Installation des VDA, die unter anderem den Citrix Universal Printer Driver sowie Treiber für den Citrix Remote USB-Bus einrichtete. Zum Abschluss der Installation war ein Neustart fällig.

Flexible Desktop-Verteilung

Nachdem wir geprüft hatten, dass die VM ohne Probleme neu gestartet war, fuhren wir sie herunter. Daraufhin konnten wir die Konfiguration auf dem DDC fortsetzen. Um einen möglichst detaillierten Überblick über die Funktionalität zu erhalten, entschieden wir uns hier für die erweiterte Konfiguration im Rahmen des "Desktop Deployment". Der Prozess erforderte drei Schritte: Die grundlegende Konfiguration, die Erzeugung von Desktop-VMs sowie die Zuordnung von Benutzern.

Zunächst definierten wir einen Namen für unsere Site. Bei der Konfiguration der Datenbank verließen wir uns auf die Standard-Werte. Da auf dem lokalen SQL Server Express noch keine entsprechende Datenbank vorhanden war, bot uns der Assistent an, dies automatisch zu erledigen. Daraufhin konnten wir die Verbindung zu unseren XenServern angeben. Dazu verwendeten wir den FQDN des Pool Masters und passende Anmeldeinformationen. Wir akzeptierten zudem die Standardeinstellung und überließen XenDesktop das Erstellen von virtuellen Maschinen. Im nächsten Schritt konnten wir über die Schaltfläche "Add…" einen Speicherort für die VMs hinzufügen. Dazu nutzten wir eine NFS-Freigabe, die wir zuvor im XenCenter an die Virtualisierungshosts angebunden hatten. Die abschließende Zusammenfassung bestätigten wir mittels "Finish", womit die Basiskonfiguration abgeschlossen war.

Weiter ging es mit der Einrichtung eines ersten Catalogs im Rahmen der "Machine creation" (siehe Bild 3). Im entsprechenden Assistenten mussten wir zunächst den Typ der virtuellen Desktops festlegen. Uns standen hierfür fünf Typen zur Auswahl [3]: Die Variante "Pooled" wird durch die Machine Creation Services aus einem Master Image erzeugt. Die Option "Random" bedeutet dabei, dass Benutzer wahlfrei mit einem Desktop verbunden werden. Melden sie sich ab und wieder an, landen sie auf einer anderen VM. Im Fall von "Static" werden die Benutzer bei der ersten Anmeldung einem Desktop fest zugeordnet. Nach Angaben des Herstellers adressiert Letzteres vor allem Anwendungen, deren Lizenzbestimmungen eine fixe

The power to do more

Vermeiden Sie kostspielige Fehler. Erweitern Sie Ihr System um einen Dell Server.

Mit einem Dell Server können Sie Ihren E-Mail-Verkehr effizienter verwalten, Dateien schneller finden, Sicherungen beschleunigen und Fehler bei Ihren alltäglichen IT-Aufgaben vermeiden. Ein Dell Server ist einfach zu installieren und zu warten, kostet etwa genauso viel wie ein Desktop-PC und ist eine echte Bereicherung für Ihr Unternehmen.

8 Gründe für ein Upgrade **www.dell.de/FIRSTSERVER**

PowerEdge™ T110

Ihr idealer erster Server

Preise ab

419 € 499 € inkl. MwSt.

zzgl. MwSt.

Preise zzgl. Versand 75 € (89 € inkl. MwSt.)
Angebot gültig bis zum 24.5.2011

- Mit optionalen Intel® Xeon E3 Serie Prozessoren der zweiten Generation
- Windows Server 2008 R2 Foundation Edition -auswählbare Erweiterungen
- Bis zu 32 GB RAM
- Max. 4 x 3.5'' Festplatten

Empfohlene Erweiterungen:

3 Jahre ProSupport*, Vor-Ort-Service am nächsten Arbeitstag

Windows Small Business Server 2011

Windows Server 2008 Foundation

Rufen Sie uns an für ein Server-Angebot: 0800 533 55 40 71
Mo-Fr 8-19 Uhr (bundesweit zum Nulltarif aus dem dt. Fest- und Mobilfunknetz)

Angebot gültig bis: 24.5.2011

intel inside Xeon

Leistungsstark. Intelligent.

Zuordnung von Anwendern und Desktops fordern. Für beide Varianten gilt, dass Desktops nach Abmeldung des Users auf den Ursprungszustand des Masters zurückgesetzt und Änderungen verworfen werden. Sollen Benutzer dauerhaft Änderungen an ihrer VM vornehmen dürfen, hilft der Typ "Dedicated" weiter. Auch in diesem Fall werden die Desktops von den MCS aus einem Master-Image generiert. Änderungen, etwa die Installation einer Anwendung durch den Anwender, werden persistent gespeichert.

Mit dem Typ "Existing" werden bestehende virtuelle Maschinen in XenDesktop eingebunden. XenDesktop nutzt die Funktionen der jeweiligen Virtualisierungsinfrastruktur, um die VMs nach Bedarf zu starten oder herunterzufahren. Das Management der Maschinen hat aber ansonsten über klassische Softwareverteilung zu erfolgen. Der Typ "Physical" integriert vorhandene physische Maschinen. Dabei kann es sich um einen Blade-PC oder einen beliebigen Büro-PC handeln, solange auf der Maschine der VDA installiert ist. In diesem Fall vermittelt XenDesktop lediglich ICA-Verbindungen zu den Maschinen. Die komplette Verwaltung inklusive dem Starten der Systeme hat mit anderweitigen Methoden zu erfolgen.

Sofern zur Verwaltung der virtuellen Desktops die bereits aus früheren Versionen bekannten Citrix Provisioning Services zum Einsatz kommen, ist der Typ "Streamed" die richtige Wahl. Dies empfiehlt sich vor allem für größere Szenarien, in denen eine gemeinsame Lösung zur Bereitstellung von virtuellen Desktops und Terminalservern gefragt ist. Wir entschieden uns im Rahmen unseres Tests für die Variante "Pooled / Random". Daraufhin konnten wir das Master-Image als Vorlage für unsere virtuellen Desktops bestimmen. Zur Auswahl standen sämtliche VMs in unserem Pool sowie deren Snapshots. Nach Auswahl der Quell-Maschine war gefragt, wie viele Desktops auf Basis der Vorlage erstellt werden sollen. Dabei bot sich die Möglichkeit, die Anzahl der vCPUs und den Hauptspeicher abweichend vom Master-Image einzustellen. Wir akzeptierten die Standard-Werte und überließen es dem DDC, neue AD-Konten für die virtuellen Desktops anzulegen. Dazu konnten wir eine Organisationseinheit im AD als Ziel bestimmen und ein Namensschema für die Accounts vorgeben. Das Zeichen "#" steht dabei als Platzhalter für Ziffern und erlaubt, die Desktops mit führenden Nullen zu nummerieren. Zuletzt blieb, einen Namen für den Catalog zu vergeben und den Assistenten mittels "Finish" abzuschließen. Daraufhin erzeugte der Assistent einen Snapshot der Master Maschine im NFS-Speicher und legte die gewünschten VMs inklusive AD-Konten an. Damit konnten wir uns dem Zuweisen von Benutzern widmen.

Schnelles User Assignment

Die Zuordnung ist denkbar schnell erledigt und beschränkt sich auf die Auswahl eines Catalogs und einer Benutzergruppe. Dazu verwendeten wir eine Gruppe von Testbenutzern in unserem AD. Mit der Vergabe eines Namens für die Desktop Group war die Konfiguration vollständig. Soll das Webinterface separat bereitgestellt werden, sind zusätzliche Schritte zur Installation und Konfiguration erforderlich [4]. Da wir das Webinterface aber mit dem DDC per Assistent installiert hatten, waren die Websites für den Zugriff auf unsere Umgebung bereits automatisch konfiguriert. Wir installierten das Citrix Online Plug-In auf einem Client-Rechner und konnten uns über die URL *http://{Servername}/Citrix/DesktopWeb* mit dem Webinterface verbinden. Das WI präsentiert sich ebenfalls in neuer Optik, nachdem die dunkle Oberfläche der Vorgängerversion nicht ohne Kritik geblieben war.

Nach Anmeldung eines Testbenutzers fand sich nur ein Desktop in der Auswahl wieder, mit dem automatisch eine Verbindung aufgebaut wurde. In der Desktop-Sitzung stand am oberen Bildschirmrand eine Menüleiste bereit, mit der wir die Sitzung in den Vollbild-Modus versetzen und zum lokalen Desktop zurückkehren konnten (siehe Bild 4). Über das Menü "Einstellungen" konnten wir die HDX-Flash-Beschleunigung aktivieren. Da sowohl in der VM als auch auf dem lokalen Client ein Flash-Player vorhanden war, konnten wir Flash-Inhalte zum Client umleiten und lokal rendern lassen. Dies sorgte für eine ruckelfreie Wiedergabe, funktionierte aber nur für Inhalte, die innerhalb der VM mit dem Internet Explorer wiedergegeben wurden. Mit dem Firefox funktioniert dies noch nicht. Zudem muss der Client selbst eine direkte Verbindung zum Flash-Medium aufbauen können.

Bild 4: Der Desktop Receiver dient der Kommunikation mit den virtuellen Desktops

Über den "Universal Printer Driver" wurden sämtliche Drucker des Clients automatisch in die Desktop-Sitzung verbunden. Druckaufträge ließen sich von dort ohne Probleme an den Client schicken. Dabei konnten wir über den nativen Druckertreiber auf dem Client sämtliche Funktionen, wie Schachtsteuerung und Duplex-Modus, nutzen. Verbanden wir einen neuen Drucker mit dem Client, wurde dieser umgehend ohne Neuanmeldung in der Remote-Sitzung sichtbar. Parallel dazu konnten wir als Administrator mittels Desktop Director unter der URL *http://{servername}/DesktopDirector* den Status der laufenden Sitzung überwachen.

Produkt
Infrastrukturlösung zur Virtualisierung von Desktops und Anwendungen.

Hersteller
Citrix Systems
www.citrix.de

Preis
Die VDI-Edition kostet für den Named User/Device 44 US-Dollar. Für den Concurrent User werden 89 Dollar fällig. Die Enterprise-Variante ist für 103 Dollar beziehungsweise 229 Dollar zu haben. Für die Platinum-Version fallen 160 Dollar beziehungsweise 320 Dollar an.

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

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

Funktionsumfang	8
USB-Unterstützung	6
Grafik-Performance	7
Linux-Client-Support	7
Installation und Inbetriebnahme	7

Dieses Produkt eignet sich

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

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

nicht für Unternehmen, die alternative Betriebssysteme wie Linux als virtuellen Desktop bereitstellen wollen.

Citrix XenDesktop 5.0

Update von VMs leicht gemacht

Um den Update-Prozess zu testen, installierten wir zusätzliche Anwendungen in unserer ursprünglichen VM, die als Vorlage gedient hatte. Anschließend fuhren wir die Maschine wieder herunter und starteten im Desktop Studio per Rechtsklick auf den Catalog die Aktion "Update Machine". Es war lediglich erforderlich, ein neues Master-Image auszuwählen und im nächsten Schritt die "Rollout strategy" festzulegen. "None" bedeutet, dass das Update erst zur Anwendung kommt, wenn ein Anwender freiwillig seine Sitzung beendet. "Send message" fordert ihn mit einer frei definierbaren Nachricht auf, dies zu tun. "Restart immediately" beendet laufende VMs und bringt das Update sofort zur Anwendung. Wir entschieden uns für die vierte Option, zuerst eine Nachricht zu senden und dann nach einer einstellbaren Frist neu zu starten. Anschließend kopierte der Assistent zunächst einen Snapshot des Master in den NFS-Speicher, benachrichtigte den Endanwender und startete nach der gewählten Zeitspanne die VMs mit dem aktualisierten Image neu.

Ebenso einfach war es möglich, mit der Aktion "Rollback update" wieder auf einen früheren Stand zurückzukehren. Kommt der Update-Prozess häufig zur Anwendung, sammeln sich allerdings die älteren Stände im NFS-Speicher an. Ein direkter Zugriff auf den Speicher, um dort aufzuräumen und ältere Stände zu löschen, ist aus dem Desktop Studio heraus nicht möglich. Sollen alte Versionen entsorgt werden, muss dies mit den Methoden der unterliegenden Virtualisierungslösung erfolgen.

Fazit

Mit XenDesktop 5 hat Citrix die Installation und die Handhabung gegenüber den Vorgängerversionen wesentlich vereinfacht. So ist es möglich, mit relativ geringem Aufwand eine Infrastruktur aufzusetzen und erste Desktops bereitzustellen. Die neuen MCS vereinfachen den Administrationsaufwand signifikant. Nichtsdestotrotz will der Schritt in den produktiven Betrieb sorgfältig geplant sein. Durch die Verteilung der Komponenten auf unterschiedliche Server und die Kombination mit XenApp Terminalservern lassen sich nahezu beliebig große und komplexe Umgebungen aufbauen [5].

Sollen XenDesktop und XenApp strategisch eingesetzt werden, ist die Ausfallsicherheit eines der wichtigsten Kriterien. Dies gilt im Fall von XenDesktop insbesondere für die SQL-Datenbank, der in der neuen Architektur gesteigerte Bedeutung zukommt. Ist die Datenbank nicht erreichbar, laufen zwar bestehende Sitzungen weiter. Es ist in diesem Fall aber nicht mehr möglich, die Site zu administrieren oder neue Verbindungen aufzubauen. Entsprechend sollte der SQL-Server abgesichert werden. Dies gelingt, indem der Server als VM über die Hochverfügbarkeitsoptionen der unterliegenden Virtualisierung abgesichert wird. Weiterhin bieten sich auf Datenbankebene die Microsoft Cluster Services oder SQL Mirroring an [6].

Unabhängig davon erlaubt XenDesktop 5 einen schnellen Einstieg in das Thema Desktop-Virtualisierung. So ist es durchaus möglich, erste Desktops in wenigen Stunden bereitzustellen. Für die Benutzer wird dank USB-Unterstützung und Flashbeschleunigung kaum mehr ein Unterschied zu physischen Desktops spürbar. Einzig höhere Grafik-Anforderungen bleiben derzeit noch unbefriedigt. Die 3D-Beschleunigung namens "HDX 3D for Professional Graphics" gab es unter XenDesktop 4 bereits. Im neuen Release soll diese Funktion erst mit einem zukünftigen Update nachgereicht werden [7]. *(dr)*

[1] XenDesktop-Varianten
B4T11

[2] Citrix Trade Up-Programm
B4T12

[3] Varianten der virtuellen Desktops
B4T13

[4] Setup mit separatem Webinterface
B4T14

[5] Modulare XenDesktop-Architektur
B4T15

[6] Microsoft Cluster Services und SQL-Mirroring
B4T16

[7] Update für HDX 3D
B4T17

Link-Codes

Installation und Konfiguration von Terminal-Diensten mit X2go

Ungeahnter Komfort

von Dr. Holger Reibold

Quelle: Visty - Fotolia.com

Freie Terminallösungen gibt es inzwischen wie Sand am Meer, doch längst nicht jedes Open Source-Werkzeug bietet den gewünschten Komfort und die notwendige Funktionalität. X2go, eine bislang vergleichsweise wenig beachtete Lösung, bringt beides in einem ausgesprochen großen Umfang mit. In diesem Workshop setzen wir eine X2go-Umgebung mit Basissystem und Clients auf und richten anschließend eine Infrastruktur mit mehreren X2go-Servern ein.

Das X2go-System macht sich insbesondere die NX-Bibliotheken für die Übertragung der Daten zunutze. Dabei können die lokalen Fähigkeiten eines X-Servers genutzt werden, was zu einer spürbar besseren Darstellungsgeschwindigkeit führt. Für den Remote-Zugriff lassen sich sowohl über das Netzwerk bootbare Thin Clients als auch Desktop-Clients (für Windows, Mac OS X und GTK beziehungsweise QT) verwenden. Eine weitere Besonderheit: Sie können Desktop-Sitzungen per Live-Authentifizierung, Passwort, USB oder Smart Card von Arbeitsstation zu Arbeitsstation mitnehmen, ohne dabei eine Anwendung beenden zu müssen. X2go unterstützt auch Kompressions-, Caching- und Verschlüsselungstechniken, womit auch der Zugriff über das Internet auf ein Remote System problemlos möglich ist. X2go unterstützt außerdem lokale USB-Speichergeräte und die Sound-Ausgabe.

X2go fit für den Unternehmenseinsatz

X2go [1] bietet auch mehrere Funktionen, die gerade für den unternehmensweiten Einsatz wichtig sind. Sie können beispielsweise lokale Geräte zentral administrieren. Und aufgrund der modularen Architektur lässt sich X2go einfach in eine bestehende Infrastruktur integrieren; auch das Zusammenspiel mit einem LDAP-Server ist dabei möglich. Die Software ist flexibel, so dass Sie sie als einfache Basisinstallation ohne LDAP-Authentifizierung über ein klassisches Thin Client-System verwenden können, aber auch als vollintegriertes Administrationswerkzeug samt Client-Überwachung.

Der Zugriff auf den X2go-Server kann entweder mit einem herkömmlichen Client von einem Windows- oder Linux-System erfolgen oder über eine Thin Client-Lösung, die mittels Preboot Execution Environment (PXE) bootet und die Client-Software via Network File System (NFS) vom Server lädt. Entscheiden Sie sich für die Boot-Variante, präsentiert der Client die Cardview, in der verschiedene Einstellungen wie die Auflösung angepasst, die Sound-Ausgabe de-/aktiviert und der Fenstermanager ausgewählt werden können. Wenn Sie die Umgebung zunächst einer Evaluierung unterziehen wollen, ist insbesondere die One-Variante interessant für Sie. Der einzige Haken: Das Projekt ist miserabel dokumentiert.

Installation des Basissystems

X2go ist bislang nur über das Debian-Repositorium zu beziehen. Lediglich die Mac OS X- und Windows-Clients stehen als direkte Downloads über die Projekt-Website zur Verfügung. Sollten Sie also nicht mit Debian, sondern einer anderen Linux-Variante arbeiten, müssen Sie zunächst die Einstellung Ihres Paketmanagers entsprechend erweitern.

Wenn Sie beispielsweise mit (K)Ubuntu arbeiten, so müssen Sie ein neues Repositorium abonnieren, da X2go bislang nicht in den Ubuntu-Repositorien zu finden ist. Um eine Ubuntu-Installation um ein Repository zu erweitern, in dem auch die X2go-Komponenten enthalten sind, öffnen Sie das Menü "System / Systemverwaltung / Software-Paketquellen". Auf der Registerkarte "Andere Software" fügen Sie dazu folgenden Repository-Eintrag hinzu:

```
deb http://x2go.obviously-
  nice.de/deb/lenny main
```

Für die Server-Installation suchen Sie im Paketmanager den Eintrag "X2go". Der Paketmanager sollte Ihnen eine umfangreiche Liste mit über 20 Einträgen präsentieren. Beachten Sie, dass die aktuelle Version 3.0.1.1 ist. Wenn Sie in einer Sin-

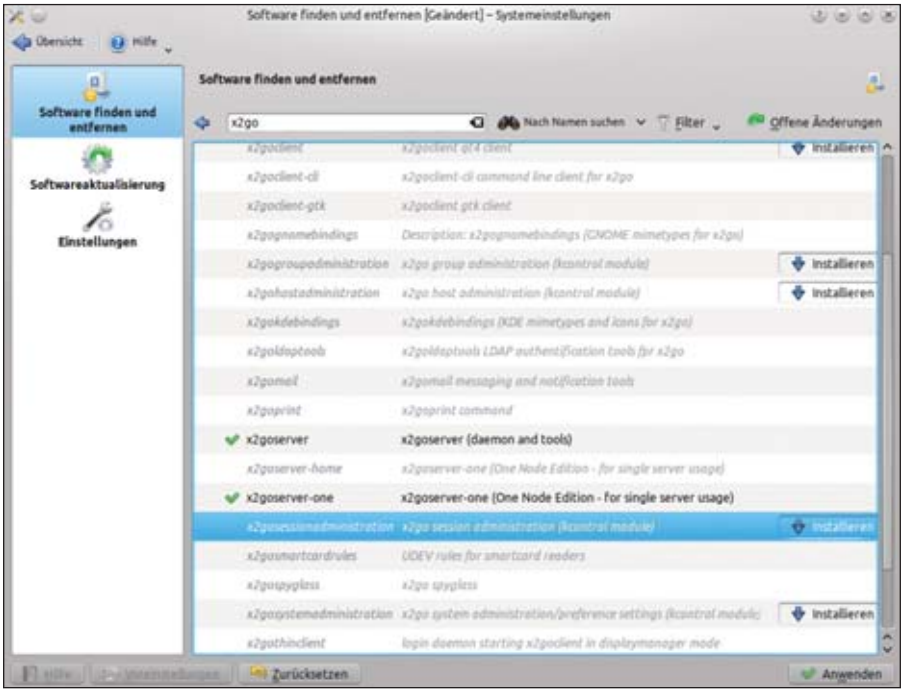


Bild 1: Nachdem Sie Ihren Paketmanager mit den Repository-Einstellungen gefüttert haben, stehen die verschiedenen X2go-Pakete zur einfachen Installation zur Verfügung

gle-Host-Umgebung arbeiten, sollten Sie die Variante "x2goserver-one" installieren. Diese Variante ist für den Einsatz auf virtuellen Maschinen und einzelnen Servern optimiert. Standardmäßig wird mit der One-Variante auch ein X2go-Client installiert. Stellen Sie außerdem sicher, dass die Komponenten "SSHFS" und "FUSE" installiert sind.

Prinzipiell können Sie jetzt mit einem X2go-Client auf den Server zugreifen. Für die Installation des X2go-Clients greifen Sie am einfachsten wieder zum Paketmanager. Er stellt Ihnen auch verschiedene weitere Module zur Verfügung.

Über den CUPS-Adapter "X2goprint" erweitern Sie das System um Druckfunktionen, die speziell für Netzwerkverbindungen mit niedriger Bandbreite, wie etwa Internet-Verbindungen, konzipiert sind. Innerhalb einer typischen Netzwerkumgebung benötigen Sie diese Funktionalität eher nicht, außer Sie wollen auch die Drucker verwenden, die direkt mit den (Thin-) Clients verbunden sind. Der Druckdienst X2goprint kann mit den X2go-Varianten "One", "Home" und "X2goserver" (dem vollständigen Server-Paket) verwendet werden. Bevor Sie den X2go-Druckdienst installieren können, müssen Sie sicherstellen, dass ein zentraler CUPS-Server netzwerkweit verfügbar ist. Es bietet sich natürlich an, den CUPS-Server auf dem X2go-System zu installieren. Sie müssen außerdem auf jedem X2goserver-System den Druckdient X2goprint installieren:

```
# apt-get install cups-x2go
```

Mit dem Druckdient X2goprint wird ein neuer Benutzer hinzugefügt, der die Datei */etc/sudoers* erweitert. Nach der Installation des Dienstes können Sie dem CUPS-System einen neuen Drucker mit Bezeichnung "x2goprinter" hinzufügen – wählen Sie den Drucker "Virtual x2goprinter" aus. Für die Konfiguration des Druckers verwenden Sie die Konfigurationsdatei */etc/cups/cups-x2gon.conf*.

Installation einer vollständigen X2go-Umgebung

Wenn Sie in den vollen Genuss der Leistungsfähigkeit des X2go-Systems gelangen wollen, müssen Sie die vollständige Version des X2go-Servers installieren und diese an Ihre Bedürfnisse anpassen. Eine vollständige X2go-Server-Installation ist dann erforderlich, wenn Sie in Ihrer Infrastruktur mehrere Terminalserver verwenden wollen. Diese werden dann in einer Server-Gruppe zusammengefasst. In einem solchen Szenario wird auch eine PostgreSQL-Server-Installation benötigt, um die X2go-relevanten Session-Informationen zu speichern. Für die Verwaltung der Benutzer ist außerdem ein LDAP-Server notwendig. Die vollständige Version des Servers installieren Sie mit dem Befehl # *apt-get install x2goserver*. Auch bei dieser Installationsvariante müssen Sie sicherstellen, dass die SSFHS- und FUSE-Komponenten installiert sind.

Der nächste Schritt dient dem Anlegen einer X2go-Benutzergruppe, der Sie all die Benutzer zuweisen müssen, die das Terminalsystem nutzen wollen. Diese Benutzergruppe trägt standardmäßig die Bezeichnung x2gousers. Um dieser X2go-Benutzergruppe nun die gewünschten User zuzuweisen, verwenden Sie folgenden Befehl:

```
# adduser benutzername x2gousers
```

Wenn Sie die File Sharing-Funktionen von X2go nutzen wollen, müssen Sie die bereits erwähnten SSHFS-Komponenten mit # *apt-get install sshfs* installieren. Wichtig ist hierbei, dass Sie die Benutzer, die diese Funktionalität nutzen dürfen, der Gruppe "fuse" zuweisen.

Als Nächstes installieren Sie den PostgreSQL-Server (die Verwendung einer MySQL-Datenbank ist bislang leider nicht möglich). Zur Datenbankinstallation führen Sie folgenden Befehl aus, vorausgesetzt beide Server werden auf dem gleichen System ausgeführt:

```
# apt-get install postgresql
```

In dieser Datenbank werden die Session-Informationen gespeichert. Für die eigentliche Installation der Datenbank steht Ihnen ein einfaches Shell-Skript zur Verfügung. Wechseln Sie zunächst ins Verzeichnis "/usr/lib/x2go/script". Dort führen Sie das Skript aus: # *./x2gocreatebase.sh*.

Sollten Sie in Ihrem Unternehmen bereits einen PostgreSQL-Server betreiben und diesen nutzen wollen, ist auch das problemlos möglich. Dazu müssen Sie den X2go-Server wissen lassen, wohin er die Daten schreiben soll:

```
# echo -n {Adresse_des_PostgreSQL-
  Servers} > /etc/x2go/sql
```

Sie sollten die passwortlose Authentifizierung mithilfe von SSH-Schlüsseln erlauben. Geben Sie dabei keine Paraphrase an:

```
# mkdirhier /root/.x2go/ssh/.pg
# ssh-keygen -t das -f
  /root/.x2go/ssh/.pg/id_dsa
```

Um den öffentlichen Schlüssel auf den PostgreSQL-Server zu kopieren, verwenden Sie den Befehl *ssh-copy-id*. Alternativ können Sie den Schlüssel auch wie folgt übermitteln:

```
# cat id_dsa-pub >
  ~postgres/.ssh/authorized_keys
```

Es ist lediglich noch ein Verbindungstest erforderlich, den Sie mit folgendem Kommando durchführen:

```
# ssh -i /root/.x2go/ssh/.pg/id_dsa
  postgres@server
```

Installation und Konfiguration der LDAP-Tools

In größeren Umgebungen bietet es sich an, die X2go-Benutzer mithilfe eines LDAP-Servers zu verwalten. Auch hierfür stellt Ihnen X2go mit den X2go-LDAP-Tools die passenden Werkzeuge zur Verfügung. Prinzipiell können Sie alle Verzeichnisdienste verwenden, die die Schemata InetOrgPerson, PosixAccount und optional SambaAccount unterstützen. Für die Installation der LDAP-Tools verwenden Sie bitte folgendes Kommando:

```
# apt-get install x2goldaptools
  \x2gouseradministration
  x2gohostadministration
  \x2gosystemadministration
  x2gogroupadministration
```

Dabei wird – sofern noch nicht geschehen – auch OpenLDAP installiert. X2go verwendet den Hostnamen für die Identifikation von Drittsystemen. Daher müssen Sie sicherstellen, dass der Hostname, die Umgebungsvariable sowie Auflösungsdienste die gleichen Werte liefern: *# echo $HOSTNAME*. Geben Sie alle Hostnamen und IP-Adresse der Host-Datei */etc/hosts* an:

```
# echo "192.168.1.1 x2goserver.local
  x2goserver" > /etc/hosts
```

Wenn Sie den OpenLDAP-Server auch für die Verwaltung der Samba-Accounts verwenden wollen, dann ist außerdem noch die Installation der SMB-Erweiterung erforderlich.

Zu den X2go-LDAP-Tools gehört auch ein einfaches Skript mit der Bezeichnung "genconf", das eine neue LDAP-Konfiguration erzeugt und Änderungen an bestehenden Konfigurationsdateien vornimmt. Sie sollten das Skript allerdings nur in Verbindung mit einer Neuinstallation eines LDAP-Servers ausführen. Um das Skript zu starten, wechseln Sie in das Verzeichnis "/usr/share/x2goldaptools/config/" und nutzen diesen Befehl:

```
#./genconf {LDAP_URL} {organisation}
  {land} {domain} {netbiosname}
  {Optionaler Wert: LDAPMASTER_URL}
```

Das Skript akzeptiert neben dem Hostnamen des LDAP-Servers den Firmenbeziehungsweise Organisationsnamen, das Land, die Domain und den Netbios-Namen der Samba-Konfigurationsdatei. Bei der Option LDAPMASTER_URL handelt es sich um einen optionalen Schlüssel für die LDAP-Server-Replikation. Das genconf-Skript generiert neue Konfigurationsdateien in das etc-Verzeichnis.

X2go-Thin-Client in Betrieb nehmen

Nachdem Sie eine vollständige X2go-Server-Installation aufgesetzt haben, können Sie sich als Nächstes der Installation der (Thin-) Clients widmen. Indem Sie den X2go-Client als Display-Manager verwenden, erhalten Sie in Kombination mit einer Boot-Umgebung eine einfach zu verwaltende Lösung für Ihr gesamtes Netzwerk. Die X2go-Boot-Umgebung unterstützt sowohl USB-Speichermedien als auch CD-ROM-Laufwerke.

Für eine derartige Installation benötigen Sie in etwa 300 MByte freien Speicherplatz. Zunächst müssen Sie allerdings für

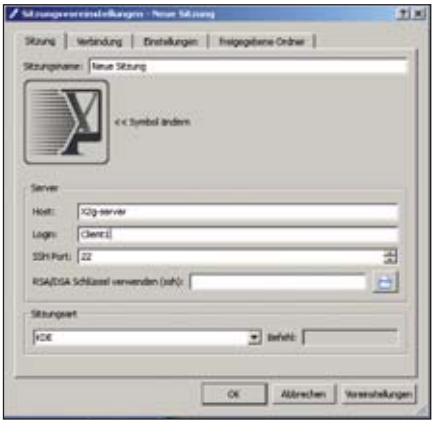


Bild 2: Die Kontaktaufnahme vom Linux-Desktop-Client zum X2go-Server erfordert das Anlegen der Sitzungsvoreinstellungen

die Installation der notwendigen Netzwerkdienste sorgen:

```
# apt-get install dhcp3-server
  atftpd nfs-kernel-server
  debootstrap
```

Sie benötigen ein beliebiges Verzeichnis, in das die Boot-Umgebung installiert wird. Das könnte beispielsweise "/opt/x2gothinclient" heißen und Sie müssen es zunächst mit *# mkdir /opt/x2gothinclient* anlegen. Nun erwecken Sie dieses Verzeichnis mithilfe des Befehls *debootstrap* zum Leben:

```
# debootstrap –arch i386 lenny
  /opt/x2gothinclient/
  http://ftp2.de.debian.org/debian
```

Das Kommando *debootstrap* installiert ein Debian-System von Grund auf neu, und zwar in dem hier spezifizierten Verzeichnis. Der Befehl lässt sich aus einem laufenden System heraus auf einer anderen Partition oder auch in einem Verzeichnis auf dem aktuellen System verwenden. Fügen Sie als Nächstes den Nameserver-Eintrag hinzu:

```
# cp /etc/resolv.conf /opt/x2gothin-
  client/etc/resolv.conf
```

Sie benötigen außerdem verschiedene Netzwerklaufwerke:

```
# vi /opt/x2gothinclient/etc/net-
  work/interfaces:
  auto lo
```

```
  iface lo inet loopback
```

Auch der Hostname und ein Eintrag in der Hostdatei /etc/hosts ist erforderlich:

```
# echo x2gothinclient > /opt/x2got-
  hinclient/etc/hostname
# echo "127.0.0.1 localhost"
  >/opt/x2gothinclient/etc/hosts
```

Nun muss X2go noch in die Host-Datei eingetragen werden:

```
# echo "192.168.1.1 x2goserver.ser-
  ver.de x2goserver"
>/opt/x2gothinclient/etc/hosts
```

Und Sie müssen den Zugriff auf das X2go-Repository angelegen:

```
# echo "deb http://x2go.obviously-
  nice.de/deb/ lenny main"
>/opt/x2gothinclient/etc/apt/
  sources.list
```

Sehr wichtig ist bei dieser Client-Installation, dass Sie alle Arbeiten auf die Boot-Umgebung beschränken und die Befehle nicht auf das übrige System anwenden. Das könnte im ungünstigsten Fall dazu führen, dass ein Zugriff darauf unmöglich wird. Das stellen Sie mit folgendem Kommando sicher:

```
# chroot /opt/x2gothinclient
  /bin/bash
```

Damit die Umgebung funktionieren kann, benötigen Sie die beiden Verzeichnisse */proc* und */dev*:

```
# mount -t proc none /proc
# mount -t devpts none /dev/pts/
```

Da *debootstrap* keinen Kernel installiert hat, der für das Starten der Boot-Umgebung benötigt wird, holen Sie das nach:

```
# aptitude update
# aptitude install syslinux locales
  linux-image-486
```

Da Sie vermutlich eine andere Tastaturbelegung als us_US verwenden wollen, müssen Sie diese entsprechend konfigurieren: *# dpkg-reconfigure locales*. Das System startet nun über das Netzwerk und Sie müssen "initramfs", das die für den Systemstart benötigten Dateien enthält, wie folgt anpassen:

```
# vi /etc/initramfs-tools/
  initramfs.conf
```

Mit *# update-initramfs -u -v* wenden Sie die neue Konfiguration an und generieren initramfs neu.

Um die Client-Installation abzuschließen, sind noch zwei weitere Schritte erforderlich. Das Thin Client-Paket installiert einen System-Daemon, der X2goclient als Display Manager startet. Er ruft außerdem einen Daemon auf, der für das automatische Mounten von lokalen Speicherlaufwerken sorgt:

```
# apt-get install x2gothinclient-
  system
# cd /usr/share/x2gothinclient-
  system/script
# ./x2gothinclient_install.sh
```

Damit ist die Installation der Boot-Umgebung abgeschlossen. Bevor Sie die chroot-Umgebung jedoch verlassen, sollten Sie die beiden Verzeichnisse */proc* und */dev* aushängen:

```
# umount /proc/
# umount /dev/pts/
```

Mit dem exit-Befehl verlassen Sie die Boot-Umgebung.

Zusammenspiel mit weiteren Servern

X2go spielt hervorragend mit verschiedenen Servern zusammen, hierzu gehört auch ein DHCP-Server, der die Clients mit IP-Adressen versorgt. Wenn Sie bereits einen DHCP-Server in Ihrer Infrastruktur betreiben, so müssen Sie sicherstellen, dass Sie für die Boot-Umgebung einen spezifischen Adressraum verwenden. Um Adresskonflikte zwischen bestehenden Komponenten und der Boot-Umgebung zu verhindern, bietet es sich an, der X2go-Umgebung einen eigenen Adressraum zuzuweisen. Dazu editieren Sie die DHCP-Konfigurationsdatei über *# vi /etc/dhcpd/dhcpd.conf*. Weisen Sie jetzt der Umgebung beispielsweise folgende Konfiguration zu:

```
option domain-name "server.de";
option domain-name-servers
  192.168.1.1;
# X2go Thin Client-Adressbereich
subnet 192.168.0.0 netmask
  255.255.255.0 {
range 192.168.0.100 192.168.0.199;
filename "/pxelinux.0";
next-server 192.168.0.250;
}
```

Damit die geänderte Konfiguration greift, müssen Sie mit */etc/init.d/dhcp3-server restart* einen Neustart des DHCP-Servers durchführen. Wurde einem X2go-System per DHCP eine IP-Adresse zugewiesen, wird ein Kernel per TFTP bereitgestellt. Damit das funktioniert, muss ein Atftpd zur Verfügung stehen und entsprechend konfiguriert werden, denn nur so kann der benötigte Kernel auch gefunden werden. Stellen Sie daher sicher, dass der Atftpd verfügbar ist und durch ein Init-Skript (nicht inet.d) gestartet wird:

```
# vi /etc/default/atftpd
USE_INETD=false
OPTIONS="–daemon –port 69 –tftpd-
  timeout 300 –retry-timeout 5
  –mcastport
1758 –mcast-addr 210.192.10.0-255
  –mcast-ttl 1 –maxthread 100
  –verbose=5 /tftpboot"
```

Sie benötigen zudem ein öffentlich schreibbares Verzeichnis zur Ablage des Kernels.

```
# mkdir /tftpboot
# chmod 755 /tftpboot
```

Wenn Sie den inet.d auf Ihrem System verwenden, sollten Sie sicherstellen, dass der Daemon nicht ausgeführt wird. Außerdem müssen Sie die Atftpt-Konfigurationsdatei erzeugen und editieren:

```
# mkdir /tftpboot/pxelinux.cfg
# touch
  /tftpboot/pxelinux.cfg/default
# vi /tftpboot/pxelinux.cfg/default
# cp
  /opt/x2gothinclient/usr/lib/sysli-
  nux/pxelinux.0 /tftpboot/
```

Wichtig ist dabei, dass Sie die IP-Adresse folgendermaßen anpassen:

```
label linux
kernel vmlinuz
append root=/dev/nfs
  nfsroot=192.168.1.1:/opt/
  x2gothinclient ro
initrd=initrd.img ip=dhcp
```

Das Root-Dateisystem der Boot-Umgebung wird mithilfe von NFS gemounted. Der Vorteil ist offensichtlich: Der Zugriff ist über das Netzwerk möglich. Sie müssen als Nächstes das benötigte Verzeichnis durch das Editieren der NFS-Konfigurationsdatei exportieren:

```
# vi /etc/exports
/opt/x2gothinclient
  192.168.1.0/24(ro,async,
  no_root_squash)
```

Nun starten Sie den NFS-Daemon neu:

```
# /etc/init.d/nfs-kernel-server
  restart
```

Konfiguration der Clients

Wenn Sie Thin Clients verwenden, so ist noch eine Anpassung der Client-Konfiguration erforderlich. Dazu führen Sie folgenden Befehl aus:

```
# vi
  /opt/x2gothinclient/etc/default/x2
  gothinclient
```

Passen Sie gegebenenfalls die IP-Adresse an:

```
x2goclient -pgp-card -
  ldap="192.168.1.1:389:o=server,c=d
  e" -external-login=/ramdrive/
  logins -no-menu -maximize
  -link=lan -kbdlayout= de -kbd-
  type=pc105/de -set-kbd=1
  -geometry=fullscreen
  -add-toknown-hosts -read-exports-
  from=/ramdrive/export
  -add-to-known-hosts
```

Damit ist der Thin Client einsatzbereit und kann im Display Manager-Modus ausgeführt werden. Neben dem Thin Client bietet sich außerdem der Einsatz eines Desktop-Clients an, der für Linux, Mac OS X und Windows über den Download-Bereich der Projekt-Site zur Verfügung steht. Die Funktionalität der drei Clients ist identisch. Zur Installation des Windows-Clients laden Sie sich die aktuelle Version des X2go-Clients 3.01.x herunter. Der Client verfügt über einen Installationsassistenten, mit dem Sie das Zielverzeichnis bestimmen. Nach der Installation erfolgt der Aufruf über die Windows-Startleiste. Der Session-Einrichtungsdialog verlangt zunächst die Angabe des X2go-Servers und des Log-In-Typs. Mit dem Auswahlmenü "Sitzungsart" bestimmen Sie, ob Sie mit der KDE-, Gnome- oder einer anderen Desktop-Umgebung arbeiten.

Bild 3: Für die X2go-Version 2.x gibt es auch ein KDE-Kontrollmodul, das beispielsweise Sitzungen verwalten kann. Es arbeitet aber leider nicht mit der aktuellen Version 3.0.x zusammen.

Auf Seiten des Clients legen Sie außerdem auf der Registerkarte "Verbindung" fest, ob der Zugriff auf den Server beispielsweise über das LAN oder WAN erfolgt. Für die Darstellung und Nutzung des Clients sind die Konfigurationsmöglichkeiten der Registerkarte "Einstellungen" zuständig. Hier können Sie beispielsweise die Auflösung und das Tastatur-Layout bestimmen sowie die Audio-Unterstützung aktivieren. Über das Konfigurationssymbol der Client-Symbolleiste greifen Sie auf die Einstellungen für die Verwendung eines LDAP-Servers und die Druckeinstellungen zu. Um die Verbindung zu einer X2go-Serverkonfiguration herzustellen, klicken Sie im Client auf das Icon neben der Sitzungsbezeichnung. Der Client fordert Sie zur Eingabe von Benutzernamen und Passwort auf. Mit einem Klick auf "OK" stellen Sie die Verbindung zum Terminal-Server her.

Für X2go 2.x gibt es auch verschiedene Backend-Module, die Sie als KDE-Kontrollmenü für die Verwaltung von Sessions, Benutzern, Gruppen und Geräten verwenden können. Doch diese sind bislang nicht in Version 3 verfügbar. Ob und falls ja, wann sie in der aktuellen Version aufgelegt werden, scheint zumindest ungewiss.

Fazit

Mit X2go steht Ihnen eine vorzügliche Terminalserver-Lösung samt passender Clients zur Verfügung. Auch wenn die Server-Konfiguration gelegentlich ein wenig umständlich und unübersichtlich ist, arbeitet die Umgebung in der Praxis sehr stabil. Auch bei den Desktop-Clients gibt es nichts zu meckern: Sie sind einfach in Betrieb zu nehmen und genauso einfach einzusetzen. Da die Desktop-Clients für alle wichtigsten Betriebssysteme verfügbar sind, steht einer plattformübergreifenden Nutzung von X2go nichts im Wege. *(jp)*

[1] X2go Projekt-Site
B5P11

Link-Codes

Kostenlos für IT-Administrator Abonnenten

ITANet

ITANet Workshop-Partner: VEEAM

IT-Administrator Trainings-Partner: Global Knowledge

Workshop in Frankfurt/M. und Leipzig

Update Virtualisierung 2011
am 8. Juni und 7. Juli 2011

Die Agenda:

13.00 Uhr: Begrüßung

13.15 Uhr: Server-Virtualisierung aktuell

- Herausforderung Management:
  Blinde Flecken des Monitorings und neue Werkzeuge für die Verwaltung virtualisierter Server
- Abschied vom virtuellen Switch:
  Neue Wege der Anbindung virtueller Maschinen an das Netzwerk
- Gemeinsame Verwaltung physikalischer und virtueller Server:
  Stolperfallen, Methoden, Tools

Dozent: Nico Lüdemann

14.45 Uhr: Pause

15.00 Uhr: Partnervortrag:
Veeam Backup – mehr als nur Backup!

Dozent: Dirk Hannemann (Frankfurt)
Matthias Frühauf (Leipzig)

15.45 Uhr: Pause

16.00 Uhr: Desktop-Virtualisierung aktuell

- Virtuelle Applikationen versus gehosteter Desktop
- Lokale Virtualisierung für mobile Anwender
- Vor- und Nachteile, Kosten
- Wie passt das alles ins Client-Management?

Dozent: Nico Lüdemann

17.30 Uhr: Ende der Veranstaltung

Termin: 8. Juni 2011
Ort: Global Knowledge Germany Training GmbH,
Hungener Straße 6, 60389 Frankfurt
Uhrzeit: 13.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos*.

Anmeldeschluss: 1. Juni 2011

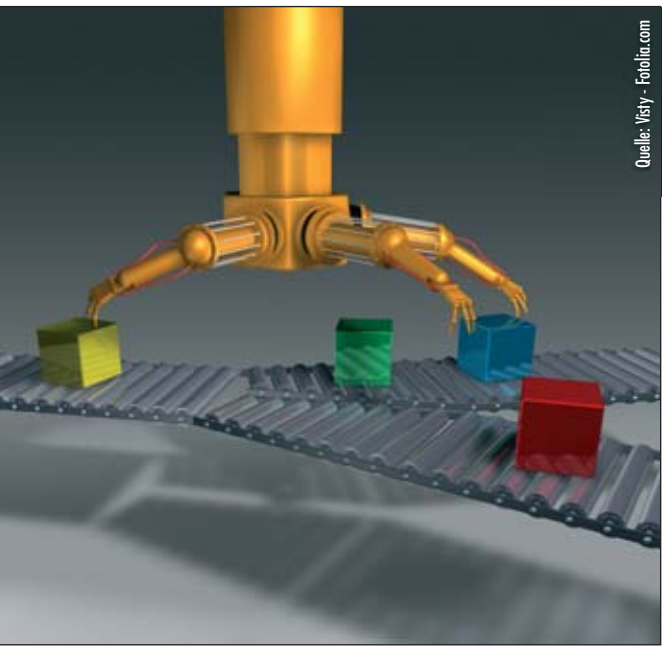
Termin: 7. Juli 2011
Ort: Commundo Tagungshotel Leipzig,
Zschochersche Straße 69, 04229 Leipzig
Uhrzeit: 13.00 bis ca. 17.30 Uhr

Teilnahmegebühren:
Für IT-Administrator Abonnenten kostenlos*.

Anmeldeschluss: 1. Juli 2011

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

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



Microsoft RemoteApps einrichten

Applikationen im Fernzugriff

von Christian Knermann

Mit den RemoteApps bieten die Terminaldienste unter Windows Server 2008 und 2008 R2 die Möglichkeit, einzelne Anwendungen auf einem Client so darzustellen, als seien sie lokal installiert. Der folgende Workshop führt Sie Schritt für Schritt durch die Einrichtung und zeigt auf, wie mit dem Remotedesktopgateway auch von extern ein sicherer Zugriff möglich ist.

Per RDP auf die komplette Desktop-Umgebung eines Servers zuzugreifen, darf bereits seit den seligen Zeiten von Windows NT als etablierte Technik bezeichnet werden. Für viele Administratoren gehört dies bei der Systemverwaltung zum Tagesgeschäft. Auch zur Versorgung von Thin Clients mit einem vollständigen Desktop ist der RDP-Zugriff ein probates Mittel. Für Anwender, die auf ihrem lokalen Client bereits ein vollwertiges Windows-Betriebssystem nutzen, führt ein zusätzlicher Terminalserver-Desktop in der Praxis aber oft zu Verwirrung. Dies gilt umso mehr, wenn lokal und remote unterschiedliche Benutzerprofile zum Einsatz kommen. "Warum sehe ich plötzlich zwei Startleisten und Desktops?" – um diese und ähnliche Support-Anfragen zu vermeiden, haben Drittanbieter-Lösungen wie Citrix XenApp das Konzept der veröffentlichten Applikationen geprägt. Mit dem Windows Server 2008 hat Microsoft begonnen, entsprechende Optionen direkt in die hauseigenen Terminaldienste einzubauen. Um die Einrichtung der RemoteApps zu demonstrieren, nutzen wir einen frisch installierten Windows Server 2008 R2, der Mitglied einer Active Directory Domäne ist.

RemoteApps vorbereiten

Über den Server-Manager starten Sie den Assistenten "Rollen hinzufügen" und wählen die Rolle "Remotedesktopdienste". In der folgenden Auswahl aktivieren Sie den "Remotedesktop-Sitzungshost" (siehe Bild 1). Dabei handelt es sich um den neuen Namen des altbekannten Terminalservers. Der Rollendienst beinhaltet automatisch die RemoteApp-Funktion. Ein Weg, auf RemoteApps zuzugreifen, führt über den "Web Access für Remotedesktop". Diesen Rollendienst fügen Sie ebenfalls hinzu. Im weiteren Verlauf wählen Sie auch die "Desktopgestaltung" zur Installation, um später auf den Clients eine möglichst einheitliche Optik von lokalen Anwendungen und RemoteApps zu erhalten. Dem ist allerdings eine Grenze gesetzt. Im Gegensatz zu Desktop-Sitzungen können einzelne RemoteApps die Transparenz-Effekte der Aero-Oberfläche nicht nutzen [1].

Nach dem obligatorischen Neustart installieren Sie die Applikationen Mozilla Firefox, Notepad++ sowie Gimp. Letztere installieren Sie benutzerdefiniert und verknüpfen alle angebotenen Dateitypen. Diese Anwendungen werden anschließend als RemoteApp dienen. Weiter geht es im Server-Manager mit dem Punkt "Rollen / Remotedesktopdienste / RemoteApp-Manager". Dort rufen Sie über das Aktionen-Feld am rechten Bildschirmrand oder per Rechtsklick in die leere Tabelle im mittleren Bereich die Aufgabe "Remote-App-Programm hinzufügen" auf. Der entsprechende Assistent kann in einem Arbeitsgang mehrere Anwendungen veröffentlichen und präsentiert dazu eine Liste der automatisch erkannten Applikationen. Firefox findet sich in der Liste nicht wieder, so dass Sie den Browser über die Schaltfläche "Durchsuchen…" manuell hinzufügen müssen. Anschließend selektieren Sie den Browser sowie Gimp 2 und Notepad++. Die Anwendungen erscheinen anschließend in der Liste der RemoteApps (siehe Bild 2).

RDP-Dateien und MSI-Pakete

Sind die RemoteApps auf dem Server definiert, müssen sie noch den Client-Com-

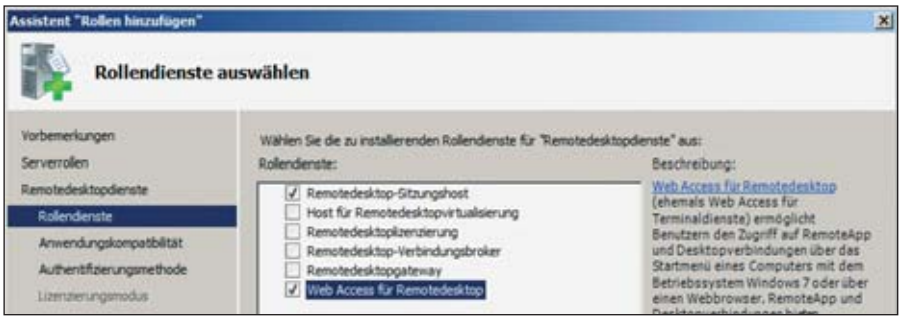


Bild 1: Das rollenbasierte Setup installiert alle nötigen Komponenten

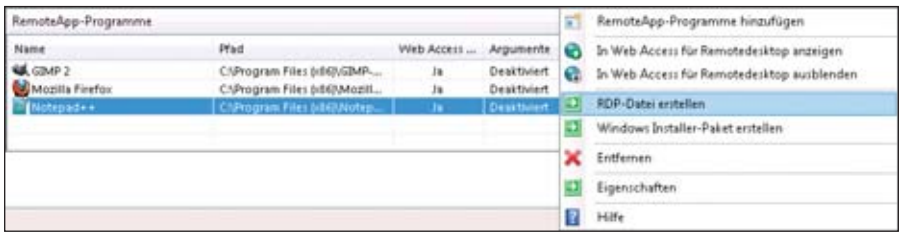


Bild 2: Der RemoteApp-Manager regelt die Bereitstellung der Anwendungen

putern bekannt gegeben werden. Ein Weg dazu führt über die Aktion "RDP-Datei erstellen". Auf diesem Weg exportieren Sie die Parameter zum Aufruf der Applikation in eine Datei vom Typ *.rdp. Diese wird standardmäßig lokal auf dem Server im Pfad "C:\Program Files\Packaged Programs" abgelegt. Von dort können Sie die Datei auf eine für die Endanwender lesbare Netzwerkfreigabe verschieben. Als Client dient in unserem Beispiel ein Windows 7-System, das ebenfalls Mitglied unserer Domäne ist. Melden Sie sich als Domänen-Benutzer an diesem Client an und öffnen Sie die RDP-Datei, wird die gewünschte RemoteApp gestartet (siehe Bild 3). Es folgt ein Anmeldedialog, in dem Sie sich mit Benutzername und Passwort authentifizieren müssen. Anschließend wird die Anwendung in einem freistehenden Fenster auf dem Desktop angezeigt, so als sei sie lokal installiert.

Mag der Weg über freigegebene RDP-Dateien für erste Gehversuche noch akzeptabel sein, gibt es doch einen für die Endanwender komfortableren Weg. Dieser führt über die Aktion "Windows Installer-Paket erstellen". Der zugehörige Assistent erfragt ebenfalls die Einstellungen für eine RDP-Datei und verpackt diese anschließend in ein Verteilungspaket vom Typ *.msi. Neben den RDP-Einstellungen enthält das Paket Informationen darüber, wie die Anwendung auf dem Client verankert werden soll. So können Sie Verknüpfungen sowohl auf dem Desktop als auch in einem frei definierbaren Startmenü-Ordner anlegen. Die Option "Clienterweiterungen für dieses Programm mit RemoteApp verknüpfen" greift zudem in die Dateitypenzuordnung auf dem Client ein. Für unsere Beispielanwendung Gimp bedeutet dies, dass alle Bildformate auf dem Client der RemoteApp zugewiesen werden, sobald das MSI-Paket installiert ist. Die RemoteApp differenziert nur mit bestimmten Dateitypen zu verknüpfen, ist leider nicht möglich. Es werden immer pauschal alle Dateiendungen belegt, die auch serverseitig der Anwendung zugeordnet sind.

Der Assistent legt das Paket ebenfalls im Pfad "C:\Program Files\Packaged Programs" ab. Von dort können Sie es manuell, per Gruppenrichtlinie oder über eine beliebige Softwaremanagement-Lösung verteilen. Wichtig ist dabei, dass das MSI-Paket nicht pro Client-Computer, sondern pro Benutzer zu installieren ist. Denn die Verknüpfungen der RemoteApps landen jeweils im benutzerspezifischen Teil des Startmenüs (siehe Bild 4). Von dort können Sie die Anwendung starten oder alternativ im Explorer auf eine Bilddatei klicken. Diese wird daraufhin an den Terminalserver übergeben und dort geöffnet.

Bild 3: Der Dialog weist darauf hin, dass die Anwendung vom Server startet

Somit haben Sie bereits eine enge Integration der RemoteApps in den Client erreicht. Was sich allerdings noch störend bemerkbar macht, ist die erneute Abfrage von Benutzername und Passwort beim Start einer RemoteApp. Wenn Sie bereits als Domänen-Benutzer am Client angemeldet sind, sollte es doch möglich sein, diese Anmeldeinformationen transparent an den Server weiterzureichen.

Single Sign-On mit Bordmitteln

Ein Single Sign-On ist mit Bordmitteln realisierbar. Allerdings müssen Sie dem Client-Computer erst noch beibringen, dass er die Anmeldeinformationen weitergeben darf. Dazu platzieren Sie das Konto Ihres Clients im Active Directory in einer Organisationseinheit, auf die Sie ein Gruppenrichtlinienobjekt anwenden. Innerhalb der Richtlinie aktivieren Sie die Option "Delegierung von Standardanmeldeinformationen zulassen", die sich im Ordner "Computerkonfiguration\Richtlinien\Administrative Vorlagen…\System\Delegierung von Anmeldeinformationen" findet. Über die Schaltfläche "Anzeigen…" können Sie eine Liste von Diensten und Servern pflegen, für die der Single Sign-On aktiv sein soll. Ein Eintrag der Form *TERMSRV/** aktiviert die transparente Anmeldung beispielsweise für sämtliche Terminalserver, *TERMSRV/*.mydomain.com* nur für die Hosts einer bestimmten Domäne. Sobald diese Einstellung aktiv ist, starten die RemoteApps ohne weitere Authentisierung. Die bis hierher beschriebene Konfiguration funktioniert sowohl für Windows Server 2008 R2 als auch für den Vorgänger Windows Server 2008 und erlaubt Endanwendern auf einfache Weise, zentral bereitgestellte Applikationen zu nutzen. Aus Sicht des Administrators fehlt es aber an Flexibilität. Sollen zusätzliche RemoteApps bereitgestellt werden, muss erst ein passendes MSI-Paket geschnürt und

Falls der Web Access auf einem separaten Server laufen oder mehrere Terminalserver integrieren soll, müssen Sie sich als Administrator am Web Access anmelden und die gewünschten Zielserver auf der Seite "Konfiguration" eintragen. Es ist möglich, wahlweise einzelne Terminalserver oder einen Verbindungsbroker als Ziel zu verwenden. Damit dies funktioniert, muss das Active Directory-Konto des Web Access Servers auf den Zielservern Mitglied der lokalen Gruppe "Terminaldienste-Webzugriffscomputer" sein. Das Funktionsprinzip des Verbindungsbrokers war bereits Gegenstand früherer Artikel [2,3] und wird hier nicht weiter ausgeführt.

Server einrichten für Web Access

verteilt werden, um die Verknüpfungen im Startmenü zu aktualisieren. Für Windows 7-Clients in Verbindung mit Windows Server 2008 R2-Terminalservern gibt es noch eine weitere Option, um die Integration ins Startmenü zu realisieren. Dazu benötigen Sie den Web Access.

Web Access ohne weitere Konfiguration

Da Sie den Web Access in unserem Beispiel direkt auf dem Terminalserver installiert haben, ist keine weitere Konfiguration erforderlich. Sie können sich im Browser mit der URL *https://{Servername}/RDWeb* verbinden. Der Server hat bei der Installation ein selbstsigniertes Zertifikat generiert. Dies sollte zunächst ausreichen. Um weitere Sicherheitswarnungen zu vermeiden, importieren Sie dieses Zertifikat in den Speicher "Vertrauenswürdige Stammzertifizierungsstellen" des Clients. Nach erfolgreicher Anmeldung an der Webseite werden Ihnen die verfügbaren RemoteApps angezeigt, die Sie mit einfachem Klick starten können. Dies funktioniert allerdings ausschließlich mit dem Internet Explorer, da dazu das ActiveX Plug-In der Remotedesktopverbindung erforderlich ist.

Der Web Access exportiert die RemoteApps zusätzlich als RSS-Newsfeed, der über die Adresse "https://{Servername}/RDWeb/Feed/webfeed.aspx" erreichbar ist. Dieser Feed bildet die Grundlage für die neuere Variante der Startmenü-Integration unter Windows 7. Auf Ihrem Client finden Sie in der Systemsteuerung unter "RemoteApp- und Desktopverbindungen" die entsprechende Option, die Integration in das Startmenü zu konfigurieren. Dazu ist im Assistenten für neue Verbindungen als Option lediglich die URL zum Feed anzugeben. Wichtig ist dabei, den vollqualifizierten Hostnamen des Web Access-Servers zu verwenden, auf den dessen Serverzertifikat ausgestellt ist. Anschließend werden die verfügbaren RemoteApps heruntergeladen. In unserem Beispiel kommt es dabei zunächst zu einem Fehler. Da der Feed ein Problem mit Sonderzeichen hat, wird unsere RemoteApp Notepad++ nicht geladen. Rufen Sie daher auf dem Terminalserver die Eigenschaften der RemoteApp auf und ändern das Attribut "Alias" von "notepad++" zu "notepad". Anschließend können Sie auf dem Client die Verbindungen aktualisieren. Nun werden alle drei RemoteApps erfolgreich geladen. Die Verknüpfungen finden sich anschließend im Startmenü wieder. Der große Vorteil dieser Art der Verteilung ist, dass der Client die Liste der RemoteApps in regelmäßigen Abständen aktualisiert. Für den Administrator entfällt somit die Notwendigkeit, jede Änderung manuell zu propagieren.

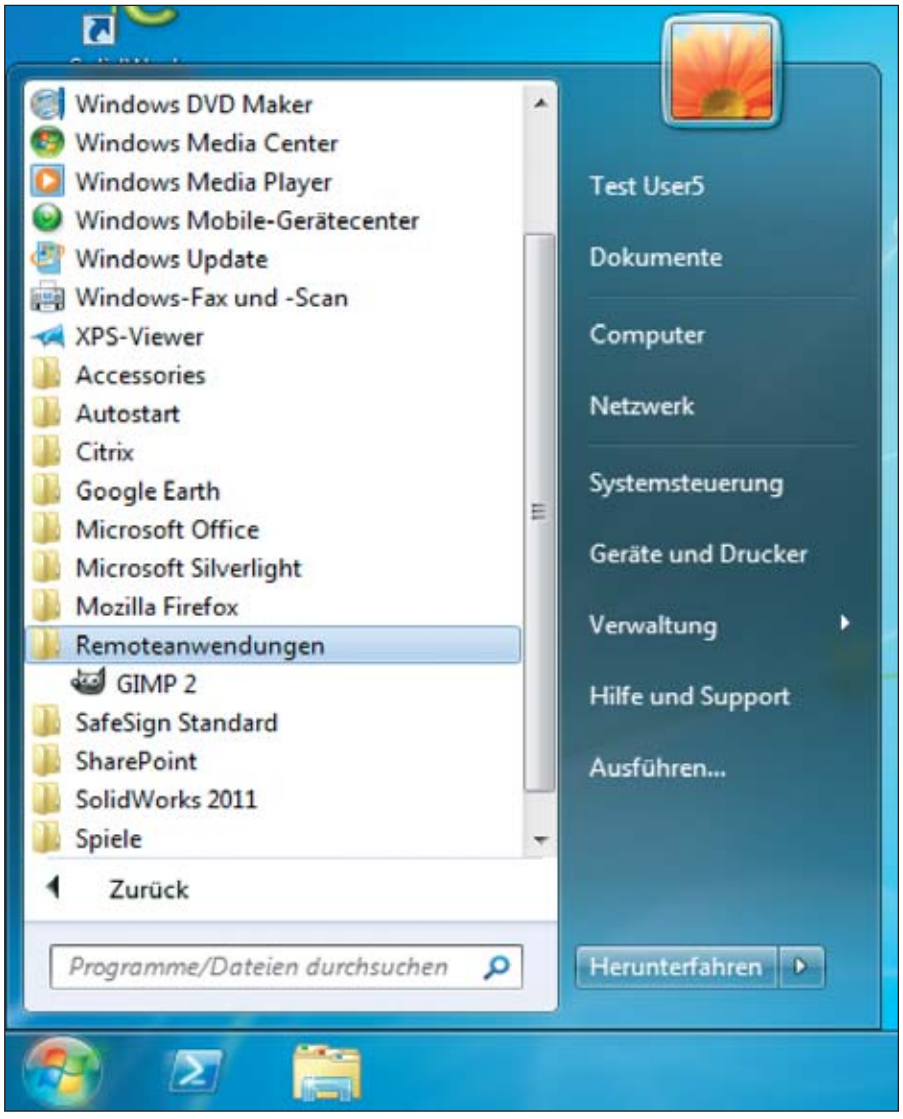


Bild 4: RemoteApps lassen sich in das Startmenü integrieren

Nachteilig ist allerdings, dass die Adresse des RSS-Feeds pro Benutzer einzurichten ist und sich diese Einstellung nicht ohne Weiteres per Gruppenrichtlinie verteilen lässt. Die automatische Konfiguration der "RemoteApp- und Desktopverbindungen" ist leider nicht trivial und funktioniert nur in Umgebungen, in denen zur Lastverteilung über mehrere Terminalserver der Remotedesktop-Verbindungsbroker zum Einsatz kommt. Dieser bietet die Option, eine Konfigurationsdatei zu exportieren. Um diese Datei automatisch an die Anwender zu verteilen, ist wiederum eine Kombination aus Gruppenrichtlinien und PowerShell gefragt. Näheres erläutert ein Blog-Beitrag unter [4]. Für kleinere Infrastrukturen bleibt also nur, MSI-Pakete zu verteilen oder die Anwender den Link zum RSS-Feed in der Systemsteuerung eintragen zu lassen. Letzteres ist zwar bei Aktualisierungen flexibler, unterstützt aber im Gegensatz zu den MSI-Paketen nicht die Verknüpfung von RemoteApps mit Dateitypen. In diesem Fall müssen Anwender also zunächst explizit die RemoteApp starten und dann innerhalb der Anwendung die gewünschte Datei öffnen.

Benutzerzuweisung ohne Sicherheitsgewinn

Damit bei einer größeren Anzahl an RemoteApps die Übersicht in Web Access und Startmenü nicht verloren geht, findet sich in den Eigenschaften einer jeden RemoteApp ab Windows Server 2008 R2 die Registerkarte "Benutzerzuweisung". Dort lässt sich die Anzeige der Verknüpfung zur jeweiligen Anwendung auf bestimmte Benutzergruppen beschränken. Benutzern, die nicht Mitglied in einer dieser Gruppen sind, wird die RemoteApp nicht mehr angeboten. Dabei ist zu beachten, dass es sich bei dieser Funktion nicht um ein Sicherheitsmerkmal handelt.

Hat ein Anwender, dem die Anwendung nicht angezeigt wird, Zugriff auf eine RDP-Datei, die direkt auf die Anwendung verweist, kann er sie dennoch starten. Ist es im Hinblick auf die IT-Sicherheit gefordert, dass ein Anwender bestimmte Applikationen nicht starten darf, so bleibt also nur, diese Applikationen über Dateisystemberechtigungen auf dem Server zu schützen oder die Applikationen für verschiedene Benutzergruppen auf mehrere Server zu verteilen. Somit ist die Benutzerzuweisung lediglich ein Hilfsmittel zur Strukturierung der Anzeige.

Sichere App-Nutzung übers Internet

Was im internen Unternehmensnetz funktioniert, sollte auch für mobile Nutzer und Heimarbeitsplätze auf sichere Weise nutzbar sein. Dazu bietet sich die Möglichkeit, den Web Access mit dem Remotedesktopgateway zu kombinieren. Das Gateway tunnelt RDP-Verbindungen SSL-gesichert, so dass für den Zugriff auf die RemoteApps von extern nur Port TCP-443 freigegeben werden muss. Im produktiven Betrieb ist es nicht empfehlenswert, von außen direkte Zugriffe auf einen Host zu erlauben, der seinerseits mit dem Active Directory direkt kommuniziert. Eine Alternative ist es, Sicherheitslösungen wie den Microsoft ISA Server einzusetzen [5]. Im Rahmen unseres Workshops soll uns der direkte Zugriff genügen. Installieren Sie dazu einen weiteren Server in Ihrer Domäne. Auf diesem System fügen Sie über den Server-Manager die Rollendienste "Remotedesktopgateway" und "Web Access für Remotedesktop" hinzu. Abhängigkeiten, wie der Webserver IIS und der RPC-über-http-Proxy, werden automatisch ebenfalls selektiert. Im nächsten Schritt können Sie ein Serverzertifikat importieren oder ein selbstsigniertes generieren. Wir entscheiden uns in unserem Beispiel für letztere Option. Für den produktiven Betrieb sollte aber in jedem Fall ein Zertifikat einer bekannten Zertifizierungsstelle zum Einsatz kommen.

Anschließend können Sie eine Autorisierungsrichtlinie definieren. Diese bestimmt, welche Benutzer das Gateway nutzen dürfen. Sie gestatten allen Domänen-Benutzern, eine Verbindung herzustellen. Im nächsten Dialogschritt versehen Sie die Richtlinie mit einem Namen und legen die zulässigen Anmeldemethoden fest. Belassen Sie es dabei beim Standard, der Anmeldung per Kennwort. Damit bleibt nun noch zu wählen, auf welche Ressourcen die Anwender zugreifen dürfen. Beschränken Sie den Zugriff auf die Domänen-Gruppe der "Terminalservercomputer". Die folgenden Schritte können Sie mittels "Weiter" überspringen und schließlich die Installation der Komponenten starten.

Nach der Installation können Sie im Server-Manager unter "Rollen\Remotedesktopdienste\Remotedesktopgateway-Manager\{Servername} (Lokal)\ Richtlinien" die Autorisierungsrichtlinien noch deutlich feinteiliger justieren. Über die Verbindungsautorisierungsrichtlinie können Sie beispielsweise die Regeln verschärfen, so dass Sie den Zugriff nicht nur auf eine Gruppe von Anwendern einschränken, sondern zusätzlich nur Clientcomputer erlauben, die in der Domäne bekannt sind. Analog gelten diese Überlegungen für die Ressourcenautorisierungsrichtlinien. Hier ließe sich definieren, dass die Domänen-Benutzer nur auf bestimmte Terminalserver zugreifen dürfen, während eine weitere Richtlinie den Administratoren Zugriff auf alle Systeme gewährt.

Fügen Sie nun Ihr Gateway auf dem Terminalserver der lokalen Gruppe der "Terminaldienste-Webzugriffscomputer" hinzu und tragen Sie im Gegenzug den Terminalserver im Web Access des Gateway-Servers als RemoteApp-Quelle ein. Zu guter Letzt hinterlegen Sie das Gateway im RemoteApp-Manager des Terminalservers mit seinem vollqualifizierten Namen in den Bereitstellungseinstellungen. Um Fehler im Rahmen der Tests zu vermeiden, exportieren Sie das selbstsignierte Zertifikat des Gateways und importieren es in den Zertifikatsspeicher eines weiteren Clients. Diesen nutzen Sie nun, um von extern per HTTPS auf das Gateway zuzugreifen. Starten Sie nach erfolgreicher Anmeldung am Web Access eine RemoteApp, so kommt die Verbindung mittelbar über das Gateway auf TCP-Port 443 zustande. Es ist keine direkte Verbindung auf TCP-Port 3389 mit dem Terminalserver erforderlich.

Da externe Benutzer an ihren Clients oftmals mit lokalen Accounts arbeiten, funktioniert es nicht, die lokalen Anmeldeinformationen an den Server zu übermitteln. In diesem Szenario hilft Ihnen der zuvor beschriebene Single Sign-On-Mechanismus nicht weiter. Zusätzlich zur Anmeldung am Web Access fordert auch der Terminalserver zu einer Anmeldung mit Benutzername und Passwort auf. Dies lässt sich mit dem sogenannten Web Single Sign-On vermeiden. Dazu müssen Sie lediglich auf dem Terminalserver im RemoteApp-Manager die Einstellungen für die digitale Signatur ändern, so dass der Terminalserver RDP-Dateien signiert ausliefert. Da wir in unserem Beispiel mit einem selbstsignierten Zertifikat arbeiten, müssen Sie dieses auf unserem externen Client natürlich auch importieren. Kommen im produktiven Betrieb Zertifikate einer etablierten PKI zum Einsatz, was nochmals dringend empfohlen sei, erübrigt sich dieser Konfigurationsaufwand.

Greifen Sie nun über Ihr Gateway auf den Terminalserver zu, reicht die einmalige Anmeldung am Web Access aus. Die Anmeldeinformationen werden an den Terminalserver weitergereicht, so dass kein weiterer Prompt mehr erscheint. Sofern in größeren Umgebungen ein Verbindungsbroker zum Einsatz kommt, um mehrere Server zu einer Farm zusammenzufassen, sind weitere Konfigurationsschritte erforderlich, um Web Single Sign-On zu aktivieren [6].

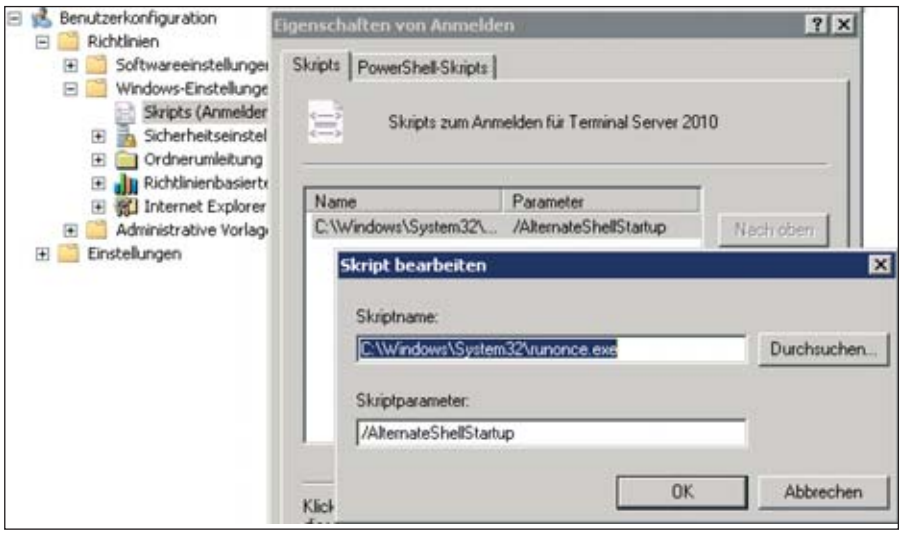


Bild 5: Werden Benutzerprofile nicht richtig initialisiert, hilft eine Gruppenrichtlinie weiter

Typische Fallstricke vermeiden

Ohne einen vollständigen Desktop können Benutzer nur die jeweilige RemoteApp beenden, aber nicht explizit die im Hintergrund laufende Desktop-Sitzung abmelden. Dies führt im Betrieb nach kurzer Zeit dazu, dass auf dem Terminalserver zahlreiche Sitzungen im Zustand "Verbindung getrennt" verbleiben und unnötig Ressourcen sowie Lizenzen verbrauchen. Abhilfe schafft eine Gruppenrichtlinie, die Sie den Benutzern zuweisen. Die gewünschte Option befindet sich unter "Benutzerkonfiguration / Richtlinien / Administrative Vorlagen… / Windows-Komponenten / Remotedesktopdienste / Remotedesktopsitzungs-Host / Sitzungszeitlimits / Zeitlimit für getrennte Sitzungen festlegen". Hier können Sie eine Zeitspanne zwischen einer Minute und fünf Tagen wählen. Nach Ablauf dieser Frist werden getrennte Sitzungen abgemeldet. Falls eine Sitzung nicht vom Anwender selbst, sondern durch einen Abbruch der Netzwerkverbindung getrennt wird, sollte dem Benutzer noch genügend Zeit eingeräumt werden, sich wieder mit der Sitzung zu verbinden und seine Arbeit zu beenden. In der Praxis empfiehlt es sich daher, diese Einstellung nicht zu restriktiv zu wählen.

Ein weiteres Problem kann auftreten, wenn sich neue Benutzer, die noch kein Benutzerprofil haben, an einer RemoteApp anmelden. Das Benutzerprofil wird in diesem Fall erst zum Zeitpunkt der Anmeldung an der RemoteApp erzeugt, dabei aber leider nicht korrekt initialisiert. Symptome dieses Problems sind in der Praxis von Fall zu Fall unterschiedlich und daher schwer zu erkennen. So kann sich das Problem beispielsweise darin äußern, dass RemoteApps neuen Benutzern im Standard-Fensterdesign angezeigt werden, obwohl auf dem Terminalserver die Desktopgestaltung aktiviert war. Bei der weiteren Arbeit mit der RemoteApp zeigt sich dann, dass diverse Funktionen nicht benutzbar sind. So reagiert beispielsweise der PDF-Druckertreiber PDFCreator mit abstrusen Fehlermeldungen. Startet ein neuer Benutzer dagegen einen Desktop statt der RemoteApp, wird das Profil korrekt initialisiert. Sowohl Desktopgestaltung als auch der Druckertreiber sind verwendbar. Grund für dieses Verhalten ist, dass einzelne RemoteApps nur eine eingeschränkte Desktop-Umgebung starten [7].

Natürlich kann es keine dauerhafte Lösung sein, Benutzer erst zur Anmeldung an einem Desktop zu veranlassen, damit einzelne Anwendungen verwendbar sind. Ein einfacher Ausweg besteht darin, den Befehl

```
C:\Windows\System32\runonce.exe
  /AlternateShellStartup
```

während der Benutzeranmeldung auszuführen. Der Aufruf kann in ein Logon-Skript verpackt werden. Unter Windows Server 2008 R2 ist es ebenso möglich, den Befehl direkt per Gruppenrichtlinie abzusetzen. Dazu wenden Sie wiederum ein GPO auf unsere Benutzer an. Die nötige Einstellung finden Sie unter "Benutzerkonfiguration / Richtlinien / Windows-Einstellungen / Skripts (Anmelden/Abmelden) / Anmelden". Dort können Sie direkt den Pfad und den nötigen Skriptparameter hinterlegen (siehe Bild 5). Dieser Workaround eignet sich insbesondere für Szenarien, in denen Benutzer auf dem Terminalserver keinen kompletten Desktop nutzen sollen und verschiedene Benutzerprofile auf Client und Server zum Einsatz kommen.

Fazit

Mit den RemoteApps und dem Remotedesktopgateway bieten die Bordmittel des Windows Server 2008 R2 inzwischen Funktionen, wie sie zuvor den Lösungen von Drittanbietern vorbehalten waren. Bis die entsprechenden Rollen laufen, haben Administratoren allerdings zahlreiche Konfigurationsschritte zu meistern. Kommt zusätzlich der Verbindungsbroker zum Einsatz, um mehrere Server zu einer Farm zusammenzufassen, wird das Ganze nochmals komplexer. Mit dem offiziellen Windows Server 2008 R2 Remote Desktop Services Resource Kit [8] erhalten Administratoren Hilfestellung aus erster Hand, um auch umfangreichere Szenarien zu meistern. *(dr)*

[1] RemoteApps und die Aero-Oberfläche
B5P41

[2] Artikel "Nah und doch fern – Desktop-Virtualisierung mit dem Windows Server 2008 R2"
in IT-Administrator Nr. 4/2010

[3] Artikel "Unsere kleine Farm – Terminaldienste unter Windows Server 2008 (2)"
in IT-Administrator Nr. 10/2008

[4] Konfigurationsdatei automatisch an Anwender verteilen
B5P44

[5] TS-Gateway mit ISA-Server nutzen
B5P45

[6] Single Sign-On mit Verbindungsbroker
B5P46

[7] Eingeschränkte Desktop-Umgebung bei RemoteApps
B5P47

[8] Windows Server 2008 R2 Remote Desktop Services Resource Kit
B5P48

Link-Codes

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

Neuerungen und Migration zu Small Business Server 2011

Serverpaket mit Umzugshelfer

von Thomas Joos

Raul Franganillo Fernandez – Fotolia.com

Small Business Server 2011 Standard ist der direkte Nachfolger von SBS 2008 und bietet aktuelle Servertechnologien in 64-Bit-Versionen. SBS 2011 baut auf Windows Server 2008 R2 Standard Edition auf und unterstützt bis zu vier Prozessoren sowie maximal 32 GByte RAM. Weitere Bestandteile sind Exchange Server 2010 SP1 Standard Edition, SharePoint Foundation 2010 und Windows Server Update Services 3.0 SP2. In diesem Workshop gehen wir auf die Lizenzierung des Server-Betriebssystems ein, erläutern die Unterschiede zwischen den verschiedenen Editionen und legen dann im Detail die Schritte dar, die bei der Migration auf den Small Business Server 2011 nötig sind.

Benutzer haben auch in der neuen Version von Small Business Server 2011 (SBS 2011) die Möglichkeit, über das Internet per Remote Web Access auf lokale Daten im SBS-Netzwerk zuzugreifen. Die Oberfläche dazu hat Microsoft optimiert. Administratoren können über den Browser eine RDP-Sitzung auf dem SBS-Server starten und so aus der Ferne Verwaltungsaufgaben durchführen.

Die Installation von SBS 2011 verläuft ähnlich wie bei den Vorgängerversionen. Alle Serverfunktionen sind auf einer DVD zusammengefasst und werden bei der Installation automatisch eingerichtet. Microsoft hat die aktuelle Version zudem mit einigen neuen Tools für die Migration von Vorgängerversionen ausgestattet. Hier bietet die Lösung wesentlich bessere Unterstützung als SBS 2008. Ansonsten beinhaltet SBS 2011 keine größeren Neuerungen im Vergleich zu SBS 2008.

Lizenzen und Versionen

Im Netzwerk dürfen Sie nur einen Server mit SBS 2011 installieren und mit einer Lizenz ist auch nur der Betrieb eines einzelnen physikalischen Servers erlaubt – Sie müssen alle Bestandteile von SBS 2011 (Windows Server 2008 R2, Exchange Server 2010, SharePoint Foundation 2010, Windows Server Update Services 3.0) auf einer Maschine installieren. Eine Aufteilung dieser Funktionen ist nicht erlaubt. An SBS 2011 lassen sich maximal 75 Anwender anbinden.

Bei der Lizenzierung von Small Business Server 2011 hat sich im Vergleich zu seinem Vorgänger am Grundprinzip wenig verändert: Um einen Small Business Server zu lizenzieren, müssen Sie zunächst eine Serverlizenz erwerben. Diese Lizenz berechtigt zum Installieren von Small Business Server 2011. Zusätzlich benötigen Sie CALs für den Zugriff. Wollen Sie die Active Directory-Rechteverwaltung (RMS) nutzen, müssen Sie diese gesondert lizenzieren, das gilt auch für die Remote Desktop-Dienste. Möchten Sie Enterprise-Funktionen von Exchange Server 2010 nutzen, müssen Sie zusätzlich zu den SBS-CALs für diese Anwender Enterprise-CALs lizenzieren. Zu den Enterprise-Features gehören die Archivierung von Postfächern über das neue Archivierungspostfach, Suchmöglichkeiten zwischen verschiedenen Postfächern, Verschlüsselung des Journals, E-Mail-Transportrichtlinien und -Schutz auch für Outlook 2010 und die Verwendung der Rechteverwaltung innerhalb von Exchange. Weder die Standard-CAL noch die Enterprise-CAL von Exchange Server 2010 oder SBS 2011 enthalten eine Outlook-Lizenz.

Sie können mit den SBS-Clientlizenzen auf andere Server im Netzwerk zugreifen, auf denen Windows Server 2008 R2, Exchange Server 2010 oder SQL Server 2008 R2 installiert ist. Allerdings darf die Anzahl der Zugriffe nicht die Anzahl der Client-Lizenzen übersteigen. Die Server-Lizenzen für alle anderen Produkte müssen Sie jedoch kaufen – nur die CALs sind integriert, mit Ausnahme von Remote Desktop-CALs. Alle Applikationen von Small Business Server 2011 müssen Sie auf dem ersten Server installieren. Sie können auf SBS 2011 keine Sprachpakete aufspielen wie bei Windows Server 2008 R2. Mehrere Sprachen werden von SBS 2011 nicht unterstützt.

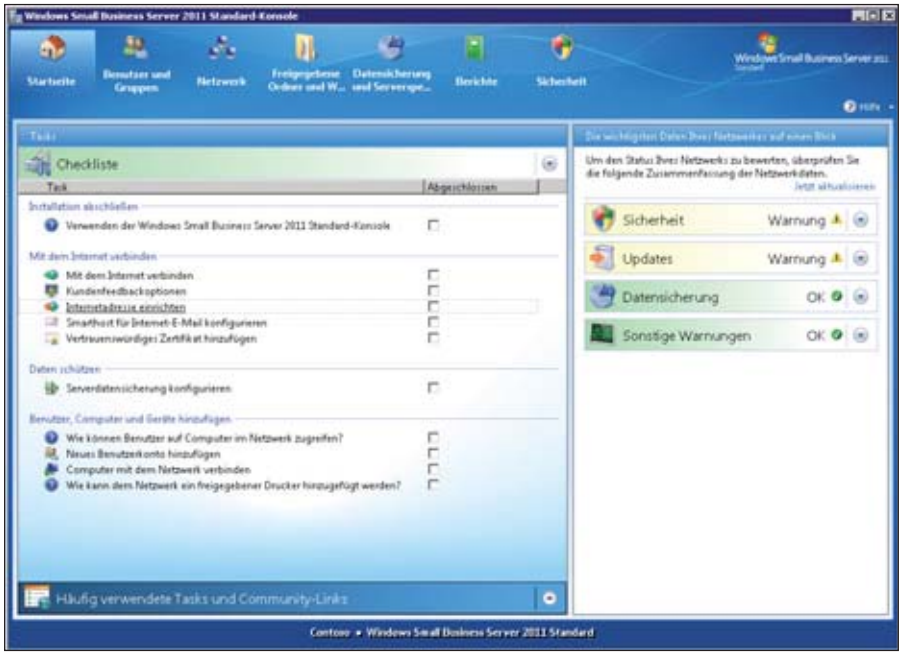


Bild 1: Die Konsole von SBS 2011 zeigt auf ihrer Startseite wichtige Systeminformationen und anstehende Aufgaben an

Essentials vs. Standard

Für kleine Unternehmen bietet Microsoft eine kleinere Edition an, die vom Funktionsumfang aber eher Windows Home Server als SBS 2011 Standard entspricht. Es fehlen die Funktionen von Exchange und SharePoint. Der Server baut zwar ebenfalls auf Windows Server 2008 R2 auf, hat ansonsten aber wenig mit SBS 2011 Standard zu tun. Unternehmen können bis zu 25 Benutzer anbinden. SBS 2011 Essentials steht ebenfalls nur als 64-Bit-Version zur Verfügung. SBS 2011 Essentials bietet vor allem eine zentrale Datenablage und die Möglichkeit, über Konnektoren die Clientcomputer zu sichern und sie zu überwachen. Die Lizenzierung unterscheidet sich etwas von SBS 2011 Standard: Sie benötigen nur eine Serverlizenz. Benutzerlizenzen sind für SBS 2011 Essentials nicht notwendig.

Die Verwaltung baut, wie SBS 2011 Standard, auf einer einheitlichen Management-Oberfläche auf. Ein Vorteil ist die Möglichkeit, zusätzliche Add-ins zu installieren, die von anderen Softwareherstellern stammen können. Solche Add-ins gab es bereits für Windows Home Server, den direkten Vorgänger von SBS 2011 Essentials. Add-ins lassen sich in die zentrale Verwaltungsoberfläche einbinden. Wie auch die Standard-Version verwendet Essentials eine Active Directory-Domäne, und muss Domänencontroller sein. Über diese Konstruktion läuft auch die Sicherung der Client-Computer und deren Wiederherstellung.

Premium Add-on für SBS 2011

Microsoft bietet für beide SBS-Editionen ein Premium-Add-on an, das vom Funktionsumfang der Premium Edition von SBS 2008 entspricht. Erwerben Unternehmen dieses Add-on, dürfen sie einen zusätzlichen Server mit Windows Server 2008 R2 installieren. Dabei ist es nicht notwendig, dass sich der zweite Server physisch am selben Standort wie der SBS befindet – der Server muss jedoch Mitglied der Small Business Server-Domäne sein. Der zweite Server darf Domänencontroller der Domäne sein, außerdem ist bereits eine Lizenz für SQL Server 2008 R2 for Small Business in das Paket integriert. Anwender, die auf den SQL-Server zugreifen wollen, benötigen allerdings eine zusätzliche Benutzerlizenz mit der Bezeichnung SBS 2011 Premium Add-on-CAL. Nur für den Fall, dass Sie den zusätzlichen Server als Hyper-V-Host oder zusätzlichen Domänencontroller betreiben, sind keine CALs notwendig.

Migration mit Bordmitteln

Small Business Server 2011 unterstützt Administratoren wesentlich besser bei der Migration als Vorgängerversionen. Bevor Sie vom Quell-Server mit SBS 2003/2008 umziehen, ist es wie immer empfehlenswert, eine vollständige Sicherung des Servers in der Windows SBS-Konsole oder über Ihr Datensicherungsprogramm vorzunehmen. Gibt es bei der Migration Probleme, können Sie mit diesem Backup den Quell-Server wiederherstellen.

Vor der Migration steht die Aktualisierung

Wollen Sie zu SBS 2011 migrieren, ist es notwendig, dass Sie zunächst den Quell-Server mit SBS 2003/2008 auf den neu-

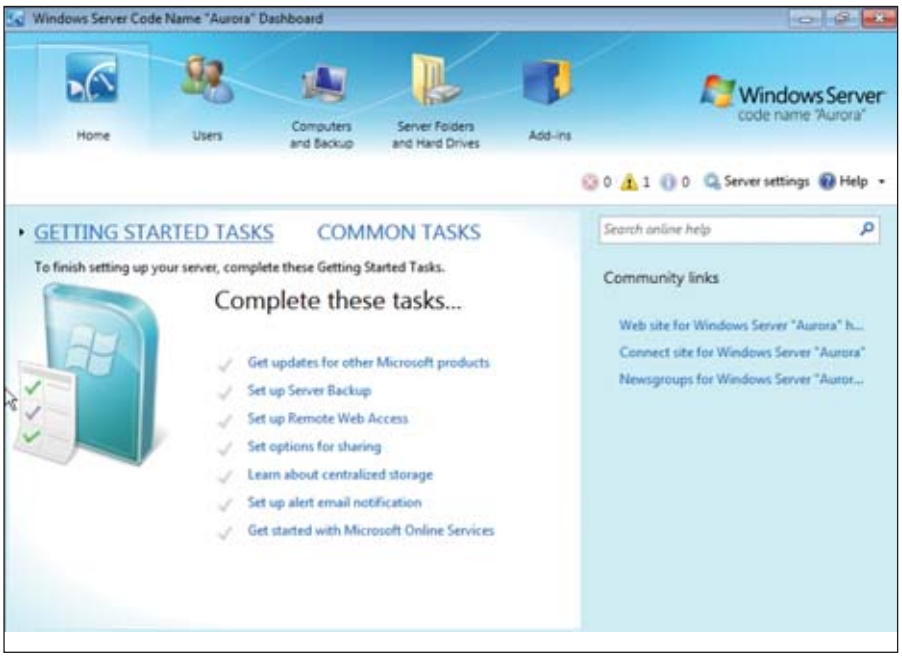


Bild 2: SBS 2011 Essentials ähnelt in Umfang und Erscheinungsbild eher Windows Home Server

esten Stand bringen. Im Technet existieren unter [1] für eine Migration von SBS 2003 und unter [2] für eine Migration von SBS 2008 ausführliche Anleitungen für den Umbau. Für den Fall, dass Sie den Server auf einer neuen Hardware aufsetzen, finden Sie hier [3] diverse Hilfestellungen. Bevor Sie die eigentliche Migration beginnen, sollten Sie den SBS-Server zudem auf vorhandene Konfigurationsfehler überprüfen. Dazu verwenden Sie den kostenlosen Small Business Server 2003 Best Practices Analyzer (BPA) von der Seite [4]. Auch für SBS 2008 gibt es diesen BPA [5].

Exchange für die Migration vorbereiten

Auch die Exchange-Komponente des SBS-Servers sollten Sie vor der Migration optimieren. Führen Sie am besten vorher eine Datensicherung durch sowie eine Offline-Defragmentierung der Exchange-Datenbanken. Außerdem sollten die Anwender ihr Postfach aufräumen. Dazu gehören das Leeren des Papierkorbs und das Archivieren von alten E-Mails. Je kleiner die Exchange-Datenbank ist, umso schneller läuft die Migration ab. Diese Vorgehensweise ist bei SBS 2003 und bei SBS 2008 identisch.

Für die Offline-Defragmentierung muss die Bereitstellung der Datenbanken aufgehoben oder der Dienst Microsoft Exchange-Informationsspeicher beendet sein. Um eine Offline-Defragmentierung durchzuführen, verwenden Sie das Befehlszeilentool Eseutil mit der Option "/d" und dem Pfad zur Datenbank. Das Tool legt vor dem Defragmentierungsvorgang eine temporäre Kopie der Datenbankdatei an, defragmentiert sie und kopiert nach dem Vorgang die Datei zurück. Aus diesem Grund sollte auf dem Datenträger genug Platz sein, mindestens das Doppelte der Größe der Exchange-Datenbankdateien. Die Syntax in der Befehlszeile für eine Offline-Defragmentierung lautet zum Beispiel:

```
eseutil /d  C:\Programme\Exchsrvr\
  MDBDATA\priv1.edb
```

Sie finden das Tool in SBS 2003 im Verzeichnis "C:\Programme\Exchsrvr\bin". Hat Eseutil mit der Defragmentierung begonnen, öffnet es die Datenbank und legt eine Kopie an. Während der Defragmentierung werden automatisch defekte Bereiche der Datenbank gelöscht. In SBS 2008 gehen Sie genauso vor. Die Datenbankdateien liegen hier aber im Verzeichnis "C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group". Eseutil finden Sie im Verzeichnis "C:\Program Files\Microsoft\Exchange Server\Bin". Rufen Sie über das Kontextmenü eine Befehlszeile mit Administratorrechten auf und wechseln Sie in das Verzeichnis "C:\Program Files\Microsoft\Exchange Server\Bin". Um in SBS 2008 eine Defragmentierung durchzuführen, verwenden Sie zum Beispiel folgenden Befehl:

```
Eseutil /d "C:\Programme\Microsoft\
  Exchange Server\Mailbox\First Sto-
  rage Group\Mailbox Database.edb"
```

Installieren des Migrations-Tools für SBS 2011

Bevor Sie nun die Migration durchführen können, müssen Sie den Quell-Server mit SBS 2003/2008 noch mit einigen Erweiterungen ausstatten. Dazu nutzen Sie das Migrations-Tool von SBS 2011 von der DVD. Damit Sie das Werkzeug nutzen können, müssen Sie auf dem Quell-Server bei SBS 2003 zuerst das .NET Framework 2.0 SP1 [6] installieren. In SBS 2008 sollte diese Umgebung bereits vorhanden sein. Sie benötigen aber auch in SBS 2008 den Microsoft Baseline Configuration Analyzer 2.0. Laden Sie sich die 64-Bit-Version unter [7] herunter und installieren Sie diese auf dem Server mit SBS 2008. Bei SBS 2003 installieren Sie die 32-Bit-Version.

Haben Sie diese Vorbereitungen getroffen, spielen Sie das Tool zum Vorbereiten der Migration über die SBS 2011-DVD auf dem Server mit SBS 2003/2008 auf. Damit Sie den Helfer einsetzen können, müssen Sie sich mit einem Benutzerkonto anmelden, das den Gruppen Domänen-Admins, Organisations-Admins und Schema-Admins zugeordnet ist. Legen Sie die SBS 2011-DVD in das SBS 2003/2008-Laufwerk und starten Sie den Installationsassistenten. Wählen Sie die Option "Tool zum Vorbereiten der Migration installieren".

Unter manchen Umständen erhalten Sie während der Installation des Migrationstools eine Fehlermeldung. In diesem Fall finden Sie unter [8] ausführliche Anleitungen zur Fehlerbehebung. In SBS 2008 etwa startet das Vorbereitungstool nicht automatisch, sondern Sie müssen es über die Programmgruppe "Windows Small Business Server Tools" manuell starten. Als Nächstes überprüft der Assistent den Server auf Probleme, die die Migration verhindern können. Findet der Assistent Knackpunkte, beheben Sie diese und lassen Sie den Scan-Vorgang erneut durchführen, bis keine Probleme mehr auftauchen. Klicken Sie erst dann auf "Weiter".

Automatisierte Migration mit Antwortdatei

Im Rahmen der Vorbereitung des Quell-Servers erstellen Sie eine Antwortdatei. Diese Datei ist notwendig, um auf einem neuen Server SBS 2011 zu installieren und den Server mit dem Quell-Server mit SBS 2003/2008 zu verbinden. Im neuen Fenster für die Antwortdatei füllen Sie die notwendigen Daten aus, die Sie dann später

Sonderfall SBS 2003: Benutzer und Gruppen zu SBS 2011 verschieben

Installieren Sie SBS 2011 im Migrationsmodus, tritt der Server der bestehenden Domäne mit SBS 2003/2008 als Domänencontroller bei. Das heißt, alle Benutzerkonten im AD sind auch in SBS 2011 vorhanden. Allerdings zeigt die Konsole von SBS 2011 die Benutzer noch nicht an, wenn Sie von SBS 2003 migrieren. Sie müssen diese daher extra in die Konsole migrieren. Das Gleiche gilt für Sicherheitsgruppen und die Verteilerlisten, die Sie in SBS 2003 nutzen. Für diese Migration benötigen Sie das Tool *GroupConverter.exe* aus dem Verzeichnis "C:\Program Files\Windows Small Business Server\bin". Auf der zweiten Seite des Assistenten sehen Sie alle Gruppen, die im Active Directory des SBS 2003 vorhanden sind. Wählen Sie die Gruppen aus, die Sie zu SBS 2011 übernehmen wollen. Nach der Übernahme können Sie nicht benötigte Gruppen einfach löschen, genau wie Gruppen, die Sie lokal in SBS 2011 angelegt haben. Die Konvertierung besteht generell darin, dass der Assistent den Gruppen verschiedene Attribute im Active Directory zuweist, damit diese in der SBS-Konsole von SBS 2011 verfügbar sind.

in einer Datei speichern. Den Benutzernamen, den Sie in der Antwortdatei hinterlegen, verwendet SBS 2011 auch für den Verzeichnisdienstwiederherstellungsmodus, wenn Sie Daten im Active Directory wiederherstellen müssen. Speichern Sie die Antwortdatei unter dem Namen *sbsanswerfile.xml*. Kopieren Sie die Datei auf einen USB-Stick, den Sie dann mit dem Ziel-Server für SBS 2011 verbinden.

Die Installation von SBS 2011 erfolgt im Migrationsmodus auf einer getrennten Maschine. Im Rahmen der Migration nimmt der Installationsassistent den neuen Server mit SBS 2011 in die Domäne des alten SBS mit auf. Achten Sie darauf, dass Sie den Quellserver spätestens nach 21 Tagen aus dem Netzwerk entfernen – ansonsten fährt der Quell-Server nach dieser Zeitspanne ständig automatisch herunter. Der Installationsassistent verschiebt alle Betriebsmasterrollen (FSMO) auf den neuen Server. Der Ziel-Server wird außerdem zum globalen Katalog konfiguriert. Auch die DHCP-Funktion übernimmt der Assistent vom Quell- auf den Zielserver. Haben Sie während der Installation die erstellte Antwortdatei per USB-Stick oder als CD im Server eingelegt, findet der Installationsassistent von SBS 2011 diese automatisch und startet die Servermigration, ohne dass Sie diese bestätigen müssen. Gibt es in der Antwortdatei Tippfehler, erhalten Sie eine entsprechende Fehlermeldung und können die richtigen Daten eingeben.

SBS 2011 legt während der Installation Protokolldateien im Verzeichnis "%programfiles%\Windows Small Business Server\Logs" ab. Öffnen Sie dieses Verzeichnis, um nach Fehlern während der Installation zu suchen. Erhalten Sie während der Installation der SBS-Komponenten eine Fehlermeldung, öffnen Sie mit der Tastenkombination "Shift+F10" eine Befehlszeile. Mit dem Kommando

```
notepad "C:\Program Files\Windows Small
  BusinessServer\Logs\
  SBSSetup.log"
```

öffnen Sie die Logdatei, die genauere Angaben zum Fehler enthält. Während der Installation müssen Sie sonst keine weiteren Daten übernehmen. Der neue Server wird Mitglied der bestehenden Domäne mit SBS 2003/2008 und als neuer Domänencontroller im bestehenden SBS-Netzwerk integriert.

Datenübernahme nach der Installation

Sie können für die Migration der Daten nicht das standardmäßige Administrator-Konto in SBS 2011 verwenden. Legen Sie ein neues Benutzerkonto an, das über Domänen-Administratorrechte verfügt, um den Assistenten zu starten. Verwenden Sie bereits ein anderes Konto als Administrator, können Sie den Assistenten direkt nach der Installation auf dem Server mit SBS 2011 starten. Melden Sie sich für die Migration mit dem neuen Benutzerkonto an und starten Sie die SBS-Konsole.

Bevor Sie die Administrationsaufgaben durchführen, sollten Sie dafür sorgen, dass die Daten des Active Directory vom alten auf

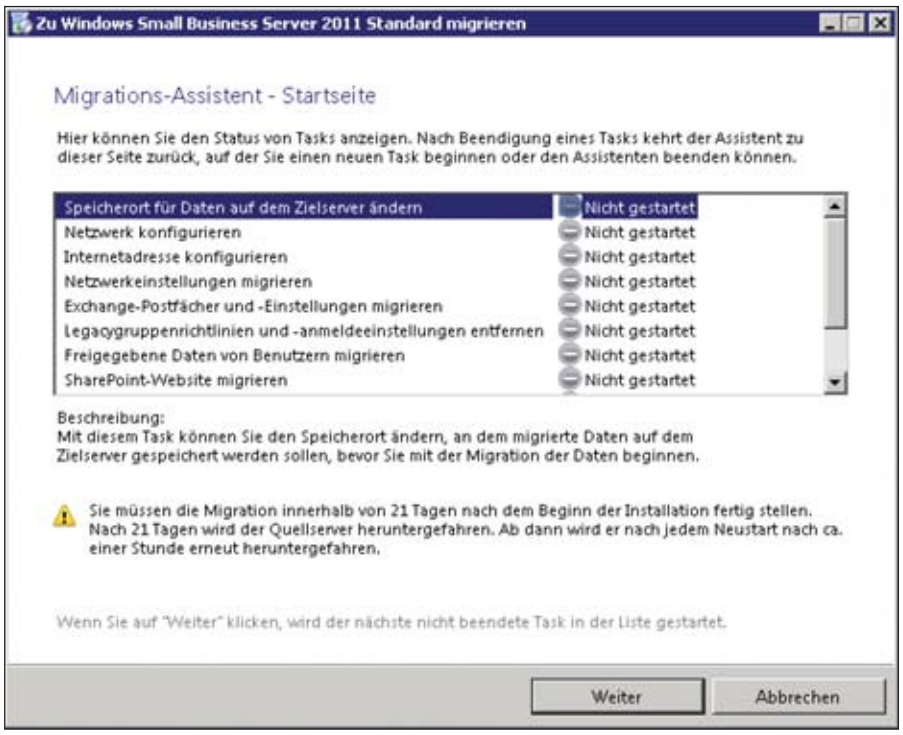


Bild 3: Auch die eigentliche Datenübernahme zu SBS 2011 erfolgt über den Migrationsassistenten

den neuen Server replizieren. Öffnen Sie dazu eine Befehlszeile mit Administratorrechten und geben Sie den Befehl *repadmin /syncall /P* ein. Klicken Sie dann in der SBS-Konsole auf den Link "Zu Windows SBS migrieren" im Bereich "Server migrieren". Es startet der Assistent zur Migration. Führen Sie für die Migration alle Aufgaben durch und setzen Sie diese anschließend auf abgeschlossen.

Auf der ersten Seite des Assistenten sehen Sie, welche Aufgaben Sie konfigurieren können. Hier und auf den weiteren Seiten können Sie für jeden Migrationsschritt entsprechende Assistenten starten, Hilfen abrufen oder den Migrations-Task als abgeschlossen markieren. Der Assistent versucht außerdem automatisch, Portweiterleitungen auf dem Router oder der Firewall zum SBS einzutragen. Sie können diese Weiterleitungen aber auch manuell durchführen:

- Port 25: SMTP für E-Mail
- Port 80: HTTP
- Port 443: HTTPS
- Port 987: HTTPS für SharePoint über den Remote-Webarbeitsplatz
- Port 1723:VPN (wenn eingesetzt)

Sobald Sie im Migrations-Assistenten den Bereich für die Übernahme der Exchange-Postfächer und öffentlichen Ordner erreichen, müssen Sie außerhalb des Assistenten Daten übernehmen. Haben Sie den SBS 2011 im Migrationsmodus installiert, funktioniert der E-Mailverkehr zwischen Postfächern auf den beiden SBS-Servern automatisch. Bei der Migration der Exchange-Daten und -Konnektoren vom alten Server zum neuen Server mit SBS 2011 gehen Sie in folgender Reihenfolge vor:

1. Konfigurieren Sie die Konnektoren für den Empfang und Versand von E-Mails.
2. Konfigurieren Sie anschließend den POP3-Konnektor.
3. Verschieben Sie die öffentlichen Ordner.
4. Verschieben Sie das Offline-Adressbuch.
5. Verschieben Sie die Postfächer.

Dateien und Freigaben auf SBS 2011 migrieren

Eine wichtige Aufgabe bei der Migration ist die Übernahme der Dateien und der Freigaben von SBS 2003/2008 auf den neuen Server mit SBS 2011. SBS 2011 arbeitet mit Grenzwerten für die Dateifreigaben für Anwender. Achten Sie daher darauf, dass die Daten, die Sie vom Quell-Server für die einzelnen Benutzer übernehmen, nicht diese Grenzwerte überschreiten. Microsoft empfiehlt die Übernahme der Daten mit *rococopy.exe*, das zu den Bordmitteln von SBS 2011 gehört. Geben Sie dazu das Kommando

```
Robocopy \\{Quell-Server}\Users
  \\{Ziel-Server}\UserShares /E
  /COPY:DATSOU /R:10 /LOG:
  C:\migration.txt
```

ein. Wollen Sie keine Daten kopieren, sondern nur die bestehenden Freigaben und Rechte vom Quell- auf den Ziel-Server übertragen, benötigen Sie die Registry. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie auf dem Quell-SBS die Registry durch Eingabe von *regedit*.
4. Navigieren Sie zu "HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\LanmanServer\Shares".
5. Exportieren Sie diesen Schlüssel über das Kontextmenü.
6. Wollen Sie nicht alle Freigaben übernehmen, öffnen Sie die exportierte Datei und löschen Sie die Einträge der Freigaben, die Sie nicht übernehmen möchten.
7. Kopieren Sie die Datei auf den Ziel-Server und klicken Sie doppelt auf die Datei, um sie auf dem Ziel-Server zu importieren. Achten Sie aber darauf, dass der Import die Einträge der vorhandenen Freigaben auf dem Ziel-Server überschreibt.
8. Starten Sie nun den Server neu.
9. Überprüfen Sie in der SBS-Konsole auf dem Server über den Menüpunkt "Freigegebene Ordner und Websites", ob die Freigaben vorhanden sind. *(ln)*

Link-Codes

[1] Migration von SBS 2003 zu SBS 2011
B5P71

[2] Migration von SBS 2008 zu SBS 2011
B5P72

[3] Migration von SBS 2011 auf eine neue Hardware
B5P73

[4] SBS 2003 Best Practices Analyzer
B5P74

[5] SBS 2008 Best Practices Analyzer
B5P75

[6] Microsoft .NET Framework 2.0 Service Pack 1 (x86)
B5P76

[7] Microsoft Baseline Configuration Analyzer 2.0
B5P77

[8] Fehlerbehebung bei Update-Problemen
B5P78

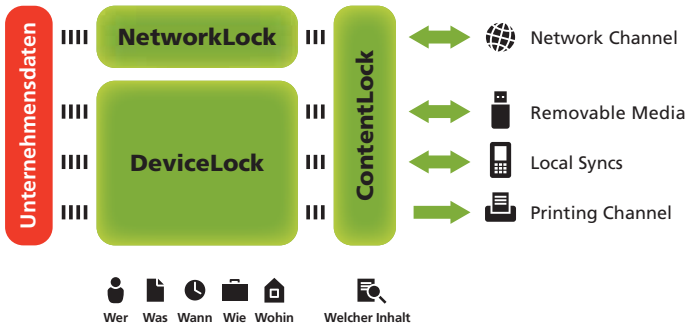
Teilt ihre Gedanken mit der ganzen Welt

genau wie ihre Passwörter.

Mitarbeiter sind auch nur Menschen.
Da kann es passieren, dass Ihre Firmendaten in sozialen Netzwerken landen. Oder verloren gehen. Oder manipuliert werden. Schützen Sie sich davor!

- Kontrolle sämtlicher PC-Schnittstellen, inkl. Webmail, FTP, Facebook & Co.
- Schutz vor Datenbeschädigung und -verlust durch Unachtsamkeit oder Vorsatz
- Individuelle Justierbarkeit
- Für kleine, große und größte Netzwerke
- Über 4 Mio. Installationen
- Referenzen in hochsensiblen Branchen
- Neu! Jetzt mit vollständiger Content- und Kontext-Prüfung

Die Datenflusskontrolle der DeviceLock Endpoint DLP-Suite



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

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security

Performance-Messung für Terminalserver- und VDI-Infrastrukturen

Vom Tuk-Tuk zum Sportwagen

von Matthias Wessner

Eine sehr wichtige Frage für eine Terminalserver- oder Virtual Desktop-Infrastruktur ist die Evaluierung und Messung realistischer Performance-Daten. In der Projektphase werden dazu typischerweise verschiedenste Whitepapers zu Rate gezogen und IT-Verantwortliche müssen sich mit Begriffen wie Prozessor-Warteschlangenlänge oder auch Interrupts pro Sekunde herumschlagen. Auch die verschiedensten Schwellenwerte, die erreicht oder nicht überschritten werden sollten, begegnen dem Projektverantwortlichen häufig. Doch die Relevanz dieser Werte für aktuelle Hardware wie etwa SSD-Festplatten oder OctaCore-Prozessoren bleibt fraglich. Hier schafft eine realistische Performance-Messung mit der freien Version des Vitual Session Indexer Abhilfe, dessen Einsatzgebiete und Funktionsweise dieser Beitrag vorstellt.

Betrachten wir zum Beispiel die Standard-Schwellenwerte des Citrix Ressource Manager, stellen wir fest, dass laut diesen Schwellenwerten bereits Systeme mit einer relativ geringen Benutzerlast überlastet sein sollten wie ein Tuk-Tuk (eine dreirädrige Mischung aus Mofa und Auto) in Bangkok mit zehn Personen. Seltsamerweise schnurrt das System aber noch wie eine Oberklassen-Limousine vor sich hin. Dies liegt daran, dass zum Beispiel der Standard-Schwellenwert weder für Context Switches noch für einen Pentium III-Prozessor ausgelegt ist.

Auch zeigen sich in der Praxis immer wieder Systeme, die trotz einer dauerhaften CPU-Last von 80 Prozent eine extrem gute Performance liefern oder im Gegensatz dazu Umgebungen, die vermeintlich nichts tun, aber dennoch sehr träge reagieren. Damit ist auch das wichtigste Schlüsselwort für eine gute Performance-Messung genannt: Reagieren. Denn objektiv betrachtet interessiert es nicht, wie hart die CPU buckeln muss oder was deren prozentuale Auslastung ist – Hauptsache das System antwortet in einer angemessenen Zeit. Insofern wäre es doch gut, wenn es ein Performance-Messtool gäbe, welches das Antwortzeitverhalten und nicht nur die CPU, den Speicher und die Festplatten-I/O misst.

Leistungsmessung mit VSI und VRC

Und dieses Tool gibt es: Der Virtual Session Indexer, kurz VSI [1]. Dieses auch als Freeware erhältliche Werkzeug misst das Antwortzeitverhalten innerhalb einer Benutzersitzung, unabhängig davon, ob es sich um ein Desktopbetriebssystem in einer Hosted Desktop-Umgebung oder einen Terminalserver handelt. Das Tool wurde insbesondere dazu entwickelt, bei der Beantwortung der Frage zu helfen, ob und mit welchem Hypervisor die Virtualisierung von Terminalservern zu empfehlen ist. Noch vor drei Jahren wäre diese Form der Virtualisierung nur für extrem gering ausgelastete Systeme als geeignet eingestuft worden. Aber die Zeiten ändern sich und Software (hier die Hypervisoren) und Hardware sind zum einen leistungsfähiger und zum anderen – etwa durch die native Unterstützung der Virtualisierung von Betriebssystemen durch die Hardware – besser aufeinander abgestimmt.

Die Funktionsweise des Programms besteht darin, Benutzeranmeldungen und Benutzeraktionen auf einem Terminalserver zu erzeugen. Dabei startet es zum Beispiel Outlook unter Verwendung einer lokalen PST-Datei (um Fremdeinwirkungen auszuschließen – es wäre für den Test völlig kontraproduktiv, wenn zum Beispiel der Exchange-Server nicht mit den Antworten hinterherkommt und deshalb der Terminalserver eine vermeintliche Sättigung meldet). Zwischendurch misst die Software immer wieder das Antwortzeitverhalten und belastet den Terminalserver mit zusätzlichen Sitzungen. Überschreiten drei der Sitzungen einen Schwellenwert (2000 ms), wird ausgewertet, wie viele Sitzungen insgesamt angemeldet sind und die Anzahl der Sitzungen als Index ausgegeben.

Da die Testreihen in den standardisierten Tests "eingefroren", also unveränderlich sind, sind die Ergebnisse mit allen anderen VSI-Messungen vergleichbar. Der ermittelte Index muss dabei natürlich nicht der Anzahl der echten Anwender entsprechen, da sich deren Verhalten und damit das Lastverhalten von dem simulierten unterscheiden kann. So können sich die Zahl der gleichzeitigen Sitzungen in der Praxis noch oben oder auch unten verschieben – entsprechend dem Benutzer und dem daraus resultierenden Lastverhalten.

Mit Software allein lässt sich noch nichts messen, dazu ist noch eine entsprechende Testumgebung notwendig. So hat sich Login Consultants mit PQR zusammenge-

schlossen und das Project VRC (Virtual Reality Check) [2] ins Leben gerufen, das die optimale Konfiguration für die verschiedenen verfügbaren Virtualisierungs-Layer erforschen soll.

Messverfahren in VSI

Zunächst lohnt sich ein Blick darauf, wie in dem Verfahren gemessen beziehungsweise wie der Index bestimmt wird: Der Index in der ersten VSI-Version nannte sich "Optimal Performance Index" (OPI) und beruhte auf dem Antwortzeitverhalten der zwei Aktionen "Maximieren von Word" und "Datei öffnen"-Dialog. Bei OPI wurde eine Sättigung erreicht, wenn bei drei Sitzungen die entsprechenden Aktionen länger als 2.000 ms benötigten. Das Problem war, dass die 2.000 ms auch noch Aktionen von "AutoIt", welches zur Automatisierung der Aufgaben genutzt wurde, einbezogen. Daher gab es mit der Version 2.0 eine neue Messmethode, VSIMax genannt. Auch hier gilt der Schwellenwert von 2.000 ms, die Latenz von AutoIt spielt allerdings dabei keine Rolle mehr. Zusätzlich wurden weitere Aktionen hinzugefügt, wie der Druckdialog, der "Suchen und Ersetzen"-Dialog und das Starten des Taschenrechners. Diese Aktionen beanspruchen das System stärker und deuten somit besser auf den Grad der Auslastung hin.

Um eventuelle, Hypervisor-spezifische Zeitabweichungen näher zu untersuchen, kam ein externer Server mit einem Microsoft SQL Server auf einem Baremetal HP-Server der Enterprise-Klasse zum Einsatz. Dieser wurde über ein 1 GBit-LAN angebunden, wobei die Netzwerklatenz unter 1 ms lag. Durch die gute Anbindung und Ausstattung des Servers wurde ausgeschlossen, dass die Einbeziehung einer externen Ressource sich negativ auf das Gesamtergebnis auswirkte. Der SQL-Server wurde genutzt, da die SQL-Zeitstempel als sehr genau gelten. Unter Einbeziehung dieses neutralen Schiedsrichters liefen weitere Tests mit den folgenden Ergebnissen:

- Hyper-V meldet, dass entsprechende Aktionen 10 ms schneller fertig sind, als sie es in der Realität sind. AutoIt meldet also zum Beispiel 200 ms und die externe SQL-Zeit 210 ms.
- Der VMware-Hypervisor verhielt sich ähnlich und meldete sogar 20 ms schnellere Aktionen. Die Differenz war dabei immer konstant.
- Anders verhielt sich der XenServer, bei dem prozentuale Unterschiede gemessen wurden, wobei die Abweichung 10 Prozent vom gemessenen Wert betrug. Eine Aktion, die zum Beispiel 220 ms dauerte, wurde mit 200 ms gemeldet und eine mit 440 ms mit 400 ms.

Diese Abweichungen mussten natürlich behoben werden, um die Messungen ordnungsgemäß durchzuführen. Das Release 2.0 von VSI integriert einen Mechanismus, der alle zwei Minuten die Abweichungen mit einer externen Uhr vergleicht und dann die Ergebnisse anpasst. Eine durchgängige Überprüfung bei jeder Aktion wäre ein zu großer Overhead, da mehr als 1.000 Events pro Durchlauf ausgeführt werden. Seit VSI 2.0 bietet das Werkzeug also ein Selftuning bezüglich der Zeitdifferenzen, wobei hierzu ein externer SQL-Server benötigt wird. Das Citrix XenServer-Team hatte auch noch den Hinweis gegeben, dass der Eintrag "/USEUPTIMER" in der *Boot.ini* das Verhalten von virtuellen Windows-Betriebssystemen auf einem XenServer bezüglich des Timings verbessern kann. Die Einbindung eines externen Zeitgebers ist aber nur bei dem Performance-Vergleich zweier Hypervisoren notwendig, da die Abweichungen ansonsten relativ sind.

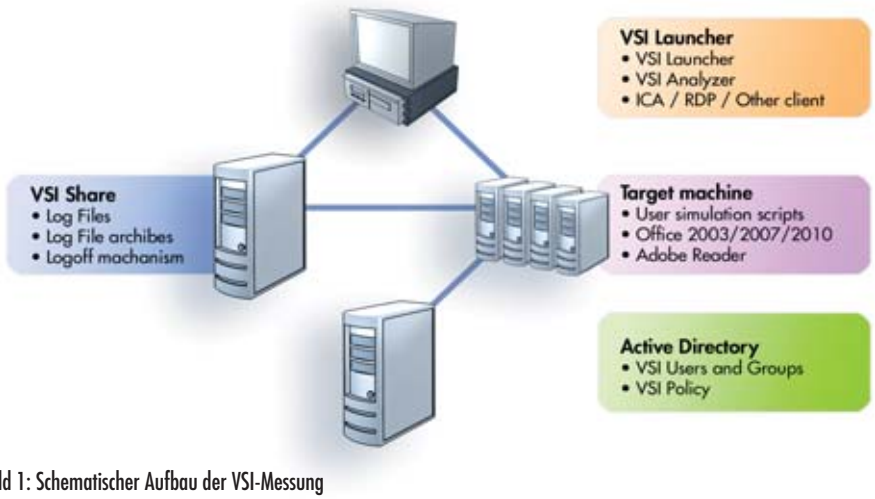


Bild 1: Schematischer Aufbau der VSI-Messung

Ergebnisse des VRC-Projekts

Die Phase 1 des VRC-Projekts startete Testreihen mit den drei Hypervisoren von Microsoft, Citrix und VMware (Hyper-V 1.0, XenServer 5.0 und ESX 3.51). Unter diesen wurde die Last mit Windows Terminal-Servern gemessen, wobei unterschiedlichste Konfigurationen getestet wurden. Hauptsächlich lässt sich sagen, dass Hyper-V 1.0 weit von den anderen beiden Konkurrenten abgeschlagen wurde und ESX mehr in VDI-Umgebungen und XenServer mehr in Terminalserver-Umgebungen Vorteile zeigte. Tiefer wollen wir an dieser Stelle aber nicht auf die Messergebnisse eingehen, da diese Messungen noch mit der Version 1.0 von VSI erfolgten. Das Ergebnis unter dem Strich war, dass sich Terminalserver mittlerweile virtualisieren lassen. Da aktuelle Hardware mehr Performance bietet als ein 32 Bit-Betriebssystem nutzen kann, macht es Sinn, 32 Bit basierende Terminalserver-Umgebungen zu virtualisieren, um die Leistung aktueller Hardware zu nutzen.

Die Phase 2 unterzog Hyper-V 2.0, vSphere 4.0 und XenServer 5.5 dem Leistungstest. Das herausragende Ergebnis war, dass Hyper-V 2.0 mit den anderen beiden Hypervisoren mithalten konnte. Das heißt, dass sich mittlerweile auch Terminalserver-Infrastrukturen auf Hyper-V performant bereitstellen lassen. Ein weiteres Ergebnis zeigte, dass vSphere mit Prozessoren mit aktiviertem Hyperthreading nicht so gut zu Recht kam wie die anderen beiden. Kurze Zeit nach der Veröffentlichung der Ergebnisse hat VMware einen Hotfix für vSphere bereitgestellt, der dieses Manko beseitigte. Hier nun einige weitere Ergebnisse aus den Messungen:

- Das Deaktivieren von ASLR, einem Sicherheitsfeature von Windows, bringt einen Vorteil von circa vier Prozent.
- Office 2007 SP2 hat einen dramatischen Performance-Vorteil verglichen zu SP1.
- Internet Explorer 7 und 8 haben die gleichen Performance-Werte.

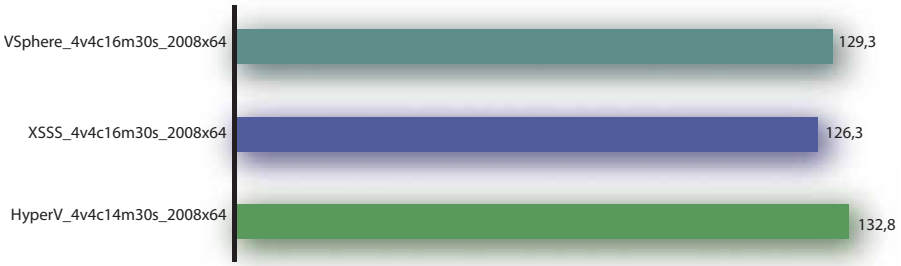


Bild 2: In Phase 2 des VRC-Projekts zeigte Hyper-V in der Version 2.0 deutlich verbesserte Leistungsdaten

- XenApp CPU-Management hat einen sehr positiven Einfluss auf ausgelastete Systeme.
- Die XenServer XenApp-Optimierung hat auf aktueller Hardware keine Auswirkungen mehr, da die Software vMMU jetzt die Hardware steuert.
- Hardware-basierte vMMU hat dramatische Vorteile zu Software-basierter vMMU.

Die folgenden Einstellungen haben sich auf einem vSphere-Hypervisor als positiv herausgestellt, wenn Terminalserver-Workloads betrieben werden sollen:

1. *esxcfg-advcfg --set 0 / Numa/PageMigEnable*
2. *esxcfg-advcfg --set 10000 / Cpu/HaltingIdleMsecPenalty*

Ein weiteres wichtiges Ergebnis war, dass die Virtualisierung von 64 Bit-Betriebssystemen nicht mehr Performance bringt, sondern dass hier eine Baremetal-Installation die höhere Benutzerdichte leisten kann.

Phase 3 des Projektes VRC untersuchte insbesondere die Bereitstellung von Hosted Desktop-Umgebungen und führte einen Vergleich zu Terminalserver-basierten Infrastrukturen durch. In dieser Phase kam dann auch VSI 3.0 zum Einsatz, das insbesondere in Bezug auf das Handling optimiert wurde und somit den einfachen Einsatz ermöglichte. Weiter wurde VSIMax 2.0 auf die Version 2.1 aktualisiert, in der auch Festplattenengpässe besser in die Auswertung eingehen.

Phase 3 hat deutlich gezeigt, dass in einer VDI-Umgebung insbesondere Disk-I/Os eine besondere Rolle spielen. Während der Anmelde-Phase finden sehr viele Read-I/Os statt, die sich dann während des normalen Betriebes hauptsächlich in Write-I/Os wandeln. Demnach zeigt sich eingangs ein sehr hoher Read-I/O-Bedarf und dann zu 80 Prozent ein Write-I/O-Bedarf. Betrachten wir unterschiedliche Storage-Hersteller, können Read-I/Os sehr gut von Caching-Mechanismen abgefangen werden, da hier viele I/Os identisch sind (zum Beispiel das Laden eines Betriebssystems). Viel schwieriger wird es da mit Write-I/Os, da diese auch unterschiedlichste Ausprägungen zeigen. Es kommt also bei einer VDI-Infrastruktur sehr stark auf die I/O-Kapazitäten des Storage an. Dies wandelt die Anforderungen an die Storage-Provider innerhalb der Firmen. Wenn derzeit Storage-Platz angefordert wird, wird meistens nur das Volumen genannt und wie ausfallsicher es sein muss und nicht wie viel I/Os es leisten muss – in einer VDI-Infrastruktur ist das ein kritischer Faktor.

Ein weiterer wichtiger Aspekt ist das Tuning der VDI-Workstations, viel wichtiger als zum Beispiel bei Terminalserver-basierten IT-Infrastrukturen. Was denken Sie, wann unter anderem der höchste I/O bei Windows 7 erzeugt wird? Dann, wenn Windows 7 idle ist, also eigentlich nichts zu tun hat. Dann starten automatisch Aufräum- und Optimierungsprozesse, die aber in einer VDI-Infrastruktur meist unerwünscht sind. Geben Sie einmal auf der Kommandozeile den Befehl *AT* ein und Sie sehen, wie viele Scheduled Tasks Windows 7 so mitbringt.

Weitere Optimierungen konnten durch die Deaktivierung von ASLR (16 Prozent), das Deaktivieren vom VM Logging (4 Prozent) sowie Konfigurationen anhand weiterer Ergebnisse der Phase 3 (insgesamt 16 Prozent) erreicht werden. So lässt sich in der optimierten Umgebung gegenüber einer Umgebung mit der Standardkonfiguration eine um 40 Prozent verbesserte Performance erreichen.

Selber messen mit VSI

Um selbst einen Test durchzuführen, registrieren Sie sich unter [1] für einen freien Download von VSI. Die Version 3.0 lässt sich sehr einfach installieren und Sie benötigen drei Komponenten: mindestens einen Launcher, die Target-Maschinen und einen Analyzer. Der Launcher, von dem Sie die Sitzungen starten, kann ein normaler Client sein. Die Target-Maschinen sind Terminalserver oder eine VDI-Umgebung, auf die die Sitzungen losgelassen werden. Auf diesen Maschinen wird dabei auch ein Teil Software installiert. Die freie Version unterstützt jedoch nur englische Betriebssysteme und ein spezielles Anwendungsset, wobei Sie nur Microsoft Office 2003 oder 2007 mit (Terminalserver-fähigem) Lizenzschlüssel beisteuern müssen.

Den Analyzer können Sie problemlos mit auf dem Launcher installieren. Für den Analyzer benötigen Sie noch das MSChart AddOn für .NET. Zusätzlich kann VSI 3.0 das Active Directory entsprechend vorbereiten, so dass Testkonten angelegt, entsprechende OUs erzeugt und Gruppenrichtlinien erstellt werden. Alle Funktionen von VSI bietet jedoch nur die kostenpflichtige Version.

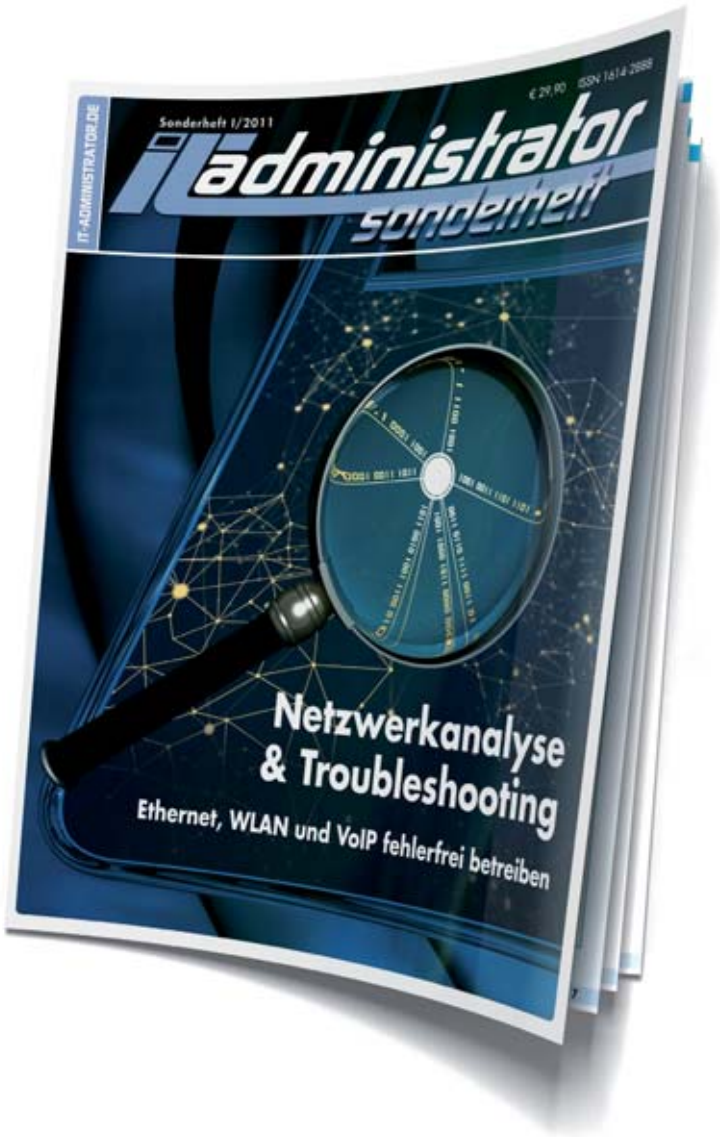
Der große Unterschied von VSI zu anderen Performance-Mess-Tools ist, dass Sie per Knopfdruck die Ergebnisse für VSIMax herausbekommen. Führen Sie dann Änderungen an der Konfiguration des getesteten Systems durch, ermitteln Sie durch einen erneuten Test mit VSI anhand des Indexes VSIMax, ob sich die Änderungen positiv oder negativ auswirken. *(jp)*

Matthias Wessner ist Principal Architect bei Login Consultants, einem auf Virtualisierung, Migration, Desktop Deployment und Application Delivery spezialisierten IT-Dienstleister.

[1] VSI-Homepage
B5P51

[2] Projekt Virtual Reality Check
B5P52

Link-Codes



Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft I/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iadministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____
und bestelle das IT-Administrator Sonderheft I/2011 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft I/2011 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0511

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

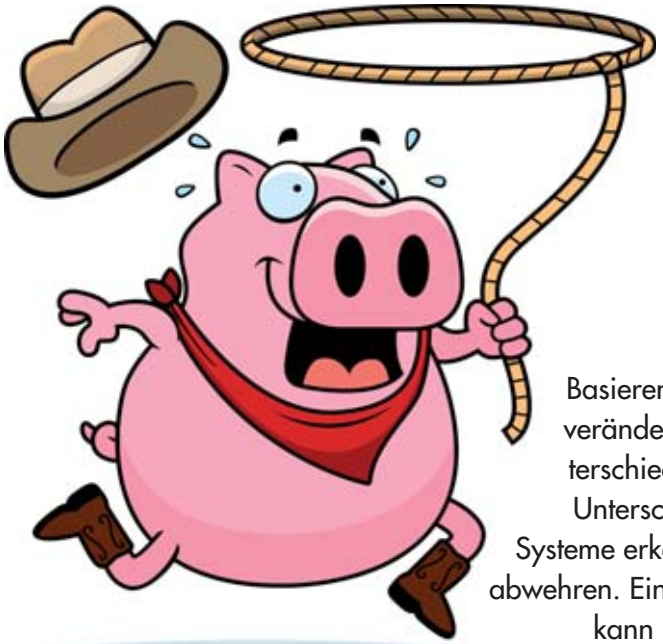
Tel: 06123/9238-251
Fax: 06123/9238-252

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



Quelle: Cory Thoman - 123RF

Open Source-IDS Snort aufsetzen

Schweinchen auf Datenjagd

von Florian Thiessenhusen

Basierend auf Open Source ist Snort ein kostenfreies und jederzeit veränderbares Intrusion Detection- und Prevention-System. Im Unterschied zu herkömmlichen Angriffserkennungssystemen wird der Unterschied zwischen IDS und IPS transparent. Intrusion Detection Systeme erkennen Angriffe, Intrusion Prevention Systeme können diese abwehren. Ein IPS muss logischerweise auf einer Art IDS basieren. Snort kann beides sein, abhängig von der Konfiguration. Wie Sie das System einrichten, lesen Sie in diesem Workshop.

Firewalls sind in der Sicherheitsbranche längst zu einem Standard geworden. Der Begriff wird jedoch häufig mit "ab Werk sicher" gleichgesetzt. Dabei wird außer Acht gelassen, wie diese Firewall funktioniert und welcher Verkehr wie tief (auf dem OSI-Schichtenmodell) untersucht wird. Selbst eine Firewall, die auf Schicht 4 arbeitet, kann nicht das komplette TCP-Paket untersuchen. So ist es möglich, dass beispielsweise ein verwundbarer, weil zum Beispiel nicht richtig gepatchter Webserver (der richtigerweise per Port 80 oder 443 aus dem Internet angesprochen wird) mit Schadcode angegriffen wird, ohne dass die Firewall etwas dagegen tun kann. Denn diese verrichtet nur ihren Job: die Weiterleitung von Paketen, basierend auf konfiguriertem Regelwerk.

Um also Datenverkehr in der Tiefe untersuchen zu können, muss eine Komponente den Traffic auf der Applikationsschicht prüfen können. Aktuell gibt es wenige Firewall-Hersteller, die das nicht können. Da werden den eigenen Firewalls IDS- und IPS-Funktionen verpasst, die dann auf ausgewählten und weitverbreiteten Ports wie POP3, SMTP oder HTTP Angriffe und Schadcode erkennen und blockieren sollen. Kombiniert mit einer Gateway-Antivirus-Komponente nennt sich dies zum Beispiel "Unified Thread Management". Hersteller entwickeln diese Schnittstellen zumeist nicht selbst, sie werden von anderen kommerziellen Anbietern eingekauft. Andere Hersteller benutzen dafür selbst auch Snort. Bei der Beschaffung solcher oder ähnlich gelagerter Produkte sollten Sie darauf achten, dass IDS und IPS voneinander getrennt sind und der eigentliche Hersteller der IDS/IPS-Lösung bekannt ist.

Open Source versus kommerzielle Angebote

Nahezu alle kommerziellen Lösungen arbeiten signaturbasiert. Das heißt, die IDS/IPS-Lösung ist nur so schlau wie die Signatur. Es gibt keine oder eingeschränkte Möglichkeiten, eigene Filter oder Anomaliemuster zu definieren. Die Industrie gibt Ihnen als Unternehmen damit vor, was eine Anomalie ist und was nicht.

In der Folge können manche Unternehmen selbst einfachste Anforderungen an ihr kommerzielles IDS nicht umsetzen. Zum Beispiel versuchen viele Firmen, Datenverkehr spezieller Anwendungen, die auf Port 80 (HTTP) nach außen kommunizieren, zu unterbinden. Port 80 an sich abzuschalten ist keine Option, das IDS/IPS bietet – bis auf die üblichen Verdächtigen wie ICQ oder Skype – keine weitere Konfiguration an. Mit Snort bauen Sie sich hingegen Ihren eigenen Filter, basierend auf den im Netzwerk aktiven Applikationen. Ein weiteres Argument ist, dass viele Administratoren nicht mit Linux als Betriebssystem und dessen Verwaltung per Konsole arbeiten möchten. So bietet Snort eine grafische Oberfläche an, auf die wir im weiteren Verlauf dieses Workshops eingehen werden.

Drei Einsatzvarianten

Für IDS/IPS-Lösungen kommen im Kern nur drei verschiedene Implementierungen in Frage: Gateway-, Netzwerk- und Host-basiert. Die Gateway-basierte Implementierung ist die gängigste. Am Übergang von einer vertrauenswürdigen (LAN) zu einer potenziell gefährlichen Netzwerkzone (DMZ, WAN) sollte ein IDS/IPS in jedem Fall positioniert sein. Aufgrund der weiten Verbreitung wird sich dieser Workshop mit dieser Art näher beschäftigen.

In großen und verteilten Netzwerken bietet es sich hingegen an, viele Sensoren zu verteilen, die an zentralen oder dezentralen Punkten Netzwerk-basiert Daten sammeln, die durch ein IDS/IPS ausgewertet werden. Der Aufwand des Betriebes und der Implementierung ist sehr groß und in der Praxis sind solche Installationen

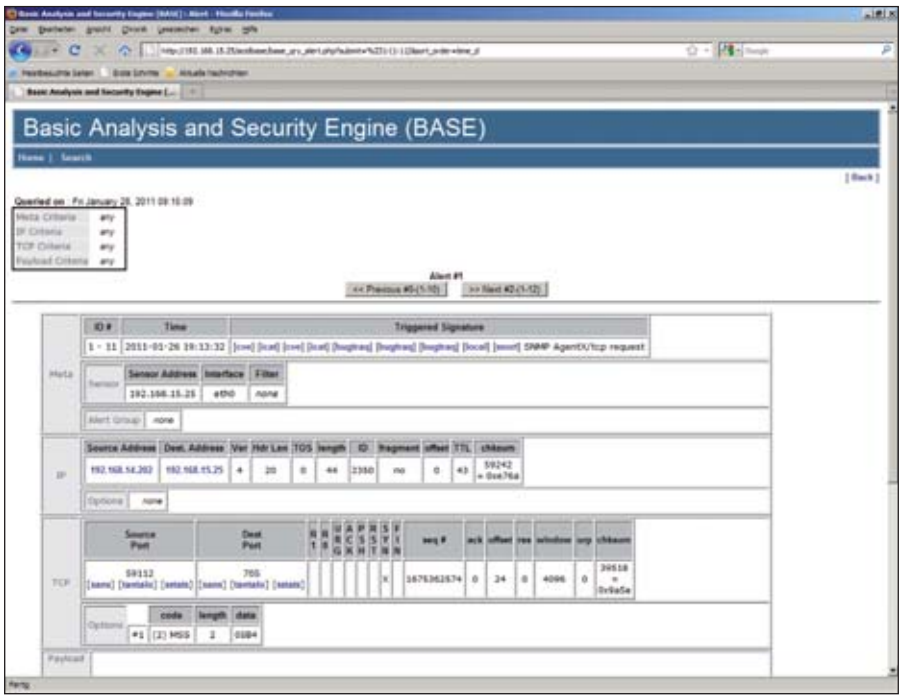


Bild 1: Die webbasierte Anzeige der Alarme in der "BASE"

verhältnismäßig selten anzutreffen. Viele Gefahren für ein Netzwerk kommen von innen, wenn auch nicht immer bewusst. Etliche Security-Hersteller haben sich deshalb darauf spezialisiert, die Endpoints und deren aus- und eingehenden Datenverkehr, also Desktops, Notebooks und auch Server, ebenfalls Host-basiert auf Anomalien zu untersuchen. Die Verwaltung ist ebenfalls sehr aufwändig und der Nutzen steht durchaus in Frage.

Installation auf dem Gateway

Auch Snort basiert grundsätzlich auf vorkonfigurierten Regelsätzen. Diese lassen sich von Snort.org manuell sowie automatisiert herunterladen. Dafür ist jedoch eine Anmeldung erforderlich. Die in diesem Workshop dargestellten Schritte zur Installation basieren auf einer XORP-Version aus dem Debian-Stable Repository. Die Snort-Version ist 2.7.0 – originale Regelsätze von Snort gibt es jedoch erst ab der Version 2.8 (die aktuellste Snort-Version ist 2.9). Um also auf einem Debian-System ein aktuelles Snort betreiben zu können, müssen Sie dieses selbst kompilieren oder auf den Debian "testing" oder "unstable" Mirror wechseln, um die Vorteile der Paketverwaltung zu nutzen. Jedoch reichen die unter 2.7.0 vorinstallierten, wenn auch älteren Regeln für die meisten Aspekte aus. Es bleibt zudem immer die Möglichkeit, eigene Regeln zu schreiben.

Nachfolgend führen wir Sie durch die klassischste aller Snort-Installationen auf dem Gateway. Jedoch sei angemerkt, dass dies nur die Installation eines IDS, also Intrusion Detection Systemes, darstellt. Unser Ziel ist es, verdächtigen Datenverkehr internetseitig zu erkennen. Wir gehen für unseren Workshop von einem Internetzugang aus, der idealerweise ein eigenes Subnetz mit öffentlichen IP-Adressen bereitstellt. Häufig kommen in der Praxis 8er-Netze zum Einsatz, die abzüglich der Broadcastadressen sechs öffentliche IP-Adressen verwalten. Ein meist vom ISP zur Verfügung gestellter Router baut die Internetverbindung auf und leitet ankommende Anfragen abhängig vom ARP-Cache beispielsweise an die Firewall weiter, ohne den Verkehr näher zu untersuchen. Die Firewall ihrerseits nutzt WAN-seitig konfigurierte, öffentliche IP-Adressen und leitet Anfragen an LAN- und DMZ-Hosts weiter – abhängig von NAT, ARP und Firewall-Konfiguration. Auf dieser Stufe findet die Paketuntersuchung statt. Ein IDS/IPS sollte dabei nahezu ungefilterten Datenverkehr untersuchen.

Im Unterschied zur Ausgangslage kann auch noch ein Hub vor dem Router platziert werden. Ein Hub ist kostengünstig und hat den Vorteil, dass er eingehende Anfragen an alle Ports schickt, ohne zu wissen, wo sich der Zielhost befindet. In LANs sollten Switches Hubs vorgezogen werden, da diese eine eigene Datenbank pflegen, welcher Host an welchem Port angeschlossen ist. In diesem Fall machen wir uns diese sicherheitskritische Funktionalität des Hubs zu Nutze und schließen dort das Snort-System sowie den Router an (alternativ ginge auch ein Switch mit Mirrorport, aber ein Hub ist für solche Zwecke mehr als geeignet und wesentlich günstiger).

Um nun die notwendigen Pakete zu installieren, beginnen Sie mit dem Kommando

```
# apt-get install mysql-server
```

Merken Sie sich die eingegebenen Authentifizierungsdaten gut. Weiter geht es mit

```
# apt-get install apache2
# apt-get install php5
# apt-get install snort-mysql
```

Es erscheint ein Assistent, den Sie erstmal durchklicken können. Auf die Frage, welches das "Home-Net" ist, geben Sie für unser Beispiel 192.168.0.0/16 an. Dieses Netz stellt das zu Beschützende dar. Diese Einstellung lässt sich später noch ändern.

Acidbase stellt die Weboberfläche für das Snort-Logging dar und benötigt somit Zugriff auf die Datenbank. Im Laufe der Installation mit

```
# apt-get install acidbase
```

werden Sie nach dem MySQL-Passwort (siehe oben) und dem Base-Passwort gefragt. Auch hier empfiehlt sich, die Daten aufzuschreiben. Acidbase ist jedoch nicht mit Abschluss der Paketinstallation fertig eingerichtet, vielmehr müssen Sie noch

Systemvoraussetzungen

Das Snort-System benötigt zwei Interfaces: eines zum Empfang der Daten und eines als Management-Interface. Das Interface, das direkt am Hub angeschlossen wird, läuft im Promiscuous Mode. Des Weiteren wird ein aktuelles Debian-Release (aktuell Lenny) genauso vorausgesetzt wie ein Editor (vim). Das Zielsystem ist ein in MySQL loggendes Snort, das durch eine webbasierte Lösung überwacht wird. Des Weiteren sind zwei Netzwerkinterfaces vorhanden, optimalerweise läuft die Hardware physisch und nicht virtuell.

das Datenbankschema importieren. Dies geschieht über das Webinterface, das Sie vorher noch konfigurieren sollten. Öffnen Sie hierfür die entsprechende Datei mit dem Editor über den Befehl

```
# vi /etc/apache2/sites-available/
  default
```

Ganz am Ende der Datei fügen Sie nun folgenden Inhalt ein beziehungsweise übernehmen diesen aus der Datei */etc/acidbase/apache.conf*:

```
<IfModule mod_alias.c>
  Alias /acidbase "/usr/share/
  acidbase"
</IfModule>

<DirectoryMatch /usr/share/
  acidbase/>
  Options +FollowSymLinks
  AllowOverride None
  order deny,allow
  deny from all
  allow from all
  <IfModule mod_php4.c>
    php_flag magic_quotes_gpc Off
    php_flag track_vars On
    php_value include_path
  .:/usr/share/php
  </IfModule>
</DirectoryMatch>
```

Anschließend folgen Sie dem Hinweis aus dem Acidbase-Setup und konfigurieren das Snort-spezifische Datenbanklayout:

```
# cd /usr/share/doc/snort-mysql
# zcat create_mysql.gz | mysql -u
  snort -D snort -p{Passwort}
```

Das Passwort muss ohne Leerzeichen angefügt werden und stellt das Acidbase-Passwort dar. Geben Sie nun die beiden Kommandos

```
# rm /etc/snort/db-pending-config
# dpkg –configure –pending dpkg-
  reconfigure snort-mysql
```

ein. Der Snort-Assistent startet anschließend erneut. Versichern Sie sich, dass das Interface, das von Snort überwacht wird und am Hub angeschlossen ist, auf "Promiscuous" eingestellt ist. Achten Sie dabei darauf, dass es sich um das Interface ETH1 handelt. ETH0 ist das Interface, von dem aus Sie per SSH oder Webmanagement zugreifen. ETH1 sollten Sie in diesem Zusammenhang auch nicht konfigurieren, etwa mit der Vergabe einer IP-Adresse.

In gleichem Assistent wird auch die Datenbankverbindung abgefragt. Diese geben Sie ein und lassen Snort die Verbindung überprüfen. Um ETH1 beim Hochfahren auch starten zu können, konfigurieren wir noch ein Startskript mit dem Befehl

```
# mv /etc/rc2.d/S20snort
  /etc/rc2.d/_S20snort
# vi /etc/init.d/runsnort.sh
```

und fügen den folgenden Inhalt in *runsnort.sh* ein

```
Ifconfig eth1 up -arp
/etc/init.d/snort start

# chmod 750 /etc/init.d/runsnort.s
# ln -s /etc/init.d/runsnort.sh
  /etc/rc2.d/S95runsnort
```

Abschließend testen wir Snort mit

```
# snort -i eth1 -v
```

Jetzt sollten eine Menge Pakete über die Konsole rauschen. Um die Ergebnisse zu sehen, prüfen wir die installierte Webkonsole (Acidbase). Auf dem Willkommensbildschirm wird vor einer unvollständigen Installation gewarnt: "Database appears to be incomplete/invalid". Mit einem Klick auf "Create BASE AG" schließen Sie die Installation ab. Erfolgsmeldungen sollten nun eingeblendet werden und die Lösung wartet anschließend auf Alerts von Snort. Um Snort zu testen, reicht ein NMAP-Scan von einem externen System auf eine vom Router bereitgestellte öffentliche IP-Adresse:

```
# Nmap -sS {SNORT-IP}
```

Das Logfile *# Nmap -sS {SNORT-IP}* zeigt die in Bild 2 dargestellten Ergebnisse.

Parallel wird dieser Alarm auch im Webinterface Acidbase aufgelistet. Damit ist Snort fertig eingerichtet.

Fazit

Ein IDS/IPS muss nicht teuer sein. Mit ein wenig technischem Verständnis können Sie ein komplett kostenloses System basierend auf Snort aufsetzen – eine sehr gute Alternative ist es allemal. Für etwas unerfahrene Administratoren oder Systemverantwortliche empfiehlt sich eine Installation, wie wir sie in diesem Artikel vorgeschlagen haben – in Form eines IDS, um Erfahrung zu sammeln. Ein sehr großer Vorteil von Snort ist auch die Möglichkeit, eigene Regeln zu programmieren, was bei den meisten kommerziellen Systemen nicht funktioniert. *(dr)*

Florian Thiessenhusen ist IT-Security Consultant bei der adMERITia AG. Seinen Blog finden Sie unter: blog.port389.de

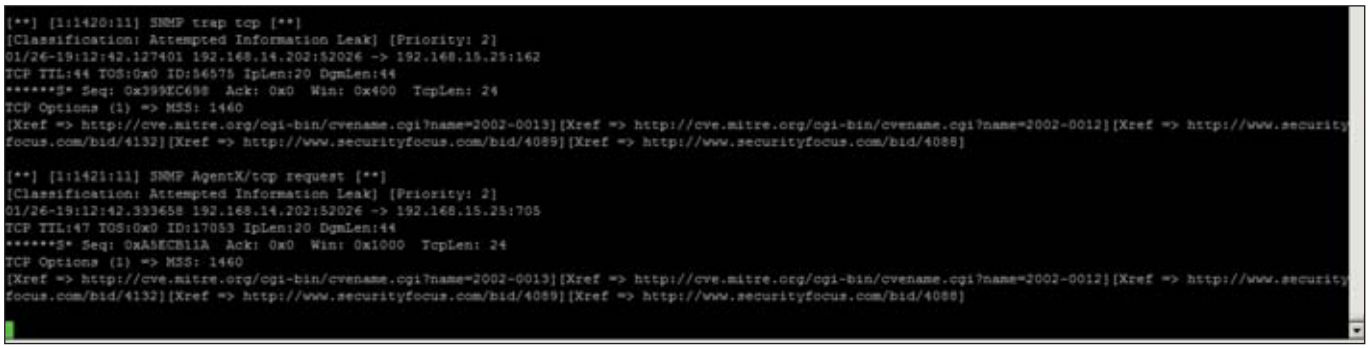


Bild 2: Die Ausgabe des Logfiles durch den Befehl *Nmap -sS*

Verschieben von Postfächern in Exchange Server 2010 SP1

Umzugslaster fürs E-Mailkonto

von Thomas Joos

Das Verschieben von Exchange-Postfächern ist vor allem im Rahmen einer Migration oder eines Hardware-Wechsels ein häufiger Vorgang. Microsoft hat mit Version 2010 die Möglichkeit dieses Verfahrens deutlich verbessert und einige Änderungen an den Abläufen vorgenommen. Außerdem existiert im SP1 weiterhin die Möglichkeit, Postfächer auch zwischen verschiedenen Exchange-Organisationen zu verschieben. In diesem Workshop zeigen wir Ihnen, welche Vorbereitungen Sie vor dem Verschieben treffen müssen und wo mögliche Stolperfallen beim Bewegen der Postfächer lauern.

Sowohl einzelne als auch mehrere Postfächer lassen sich von einer Postfachdatenbank in die andere oder auf einen weiteren Exchange-Server mit Mailbox-Serverrolle verschieben. Dazu verwendet Exchange 2010 keine RPC-Verbindung zwischen den Servern mehr, sondern den neuen Postfachreplikationsdienst (Mailbox Replication Service, MRS). Dieser Dienst läuft auf allen Clientzugriffservern (CAS). Anwender können während des Verschiebens problemlos weiterarbeiten, ohne dass Daten verloren gehen. Auch ist es möglich, Postfächer zwischen verschiedenen Exchange-Versionen zu verschieben – allerdings können in diesem Fall Anwender nicht immer online mit ihrem Postfach weiterarbeiten. Die Tabelle "Versionsunterschiede beim Verschieben von Postfächern" verrät Ihnen, zwischen welchen Versionen Sie in Verbindung mit Exchange 2010 Postfächer verschieben können und in welchen Editionen die Anwender dabei weiterarbeiten können. Das Verschieben sollten Sie immer von Exchange 2010 aus starten.

Damit das Verschieben von Postfächern funktioniert, sind mehrere offene TCP-Ports notwendig. Die Kommunikation zu diesen Ports muss zwischen den Exchange-Servern und den Domänencontrollern möglich sein. Der Tabelle "Beim Verschieben von Postfächern benötigte TCP-Ports" können Sie eine Auflistung der entsprechenden Ports entnehmen.

Verbindet sich ein Client per MAPI mit einem Clientzugriffserver, also mit Outlook im internen Netzwerk oder über Outlook Anywhere über das Internet, spielt das RPC-Protokoll mit seinen dazugehörigen Ports eine wichtige Rolle. Zwischen dem Clientzugriffserver findet eine Verbindung zwischen dem Port 135 und einem dynamischen Portbereich statt. Vor allem beim externen Zugriff kann es sinnvoll sein, den dynamischen Bereich einzugrenzen, da Sie ansonsten zahlreiche Ports in Firewalls oder Routern öffnen müssen. Wie diese Eingrenzung mit Hilfe von Registry-Änderungen funktioniert,

Versionsunterschiede beim Verschieben von Postfächern

Verschieben von/zu	Verschieben möglich	Anwender können weiterarbeiten
Exchange Server 2010 (SP1) zu Exchange Server 2010 (SP1)	Ja	Ja
Exchange Server 2007 SP2/SP3 zu Exchange Server 2010 (SP1)	Ja	Ja
Exchange Server 2007 SP1 zu Exchange Server 2010 (SP1)	Nein	Nein
Exchange Server 2003 SP2 zu Exchange Server 2010 (SP1)	Ja	Nein
Exchange Server 2010 (SP1) zu Exchange Server 2007 SP2/SP3	Ja	Nein
Exchange Server 2010 (SP1) zu Exchange Server 2003 SP2	Ja	Nein

Benötigte Ports	
Port (TCP)	**Beschreibung**
808	Kommunikation durch den Mailbox Replication Service
53	DNS
135	RPC
389	LDAP
3268	LDAP, globaler Katalog
1024 und höher	Wenn Sie den Port der Datenbanken nicht statisch festgelegt haben, sind alle Ports über 1024 notwendig
88	Kerberos
445	Microsoft-DS Dienst
443	HTTPS

können Sie unter [1] im Microsoft Technet nachlesen.

Postfächer innerhalb der Exchange-Organisation verschieben

Öffnen Sie zum Verschieben die Exchange-Verwaltungskonsole und navigieren Sie zu "Empfängerkonfiguration/Postfach". Klicken Sie mit der rechten Maustaste auf das Postfach, das Sie verschieben wollen, und wählen Sie den Befehl "Neue lokale Verschiebungsanforderung oder Neue Remote-Verschiebungsanforderung". Verwenden Sie "Neue lokale Verschiebungsanforderung", um das ausgewählte Postfach in eine andere Datenbank innerhalb derselben Gesamtstruktur zu verschieben. Mit "Neue Remoteverschiebungsanforderung" verschieben Sie das ausgewählte Postfach in eine andere Gesamtstruktur. Damit das funktioniert, müssen Sie aber verschiedene Vorbereitungen treffen, auf die wir später noch ausführlich eingehen.

Platzbedarf von Transaktionsprotokollen einrechnen

Bei diesem Vorgang können Sie auch mehrere Postfächer markieren und auf einen Rutsch verschieben. Auf der ersten Seite des Assistenten wählen Sie die Postfachdatenbank aus, in die Sie die Postfächer verschieben wollen. Beim Bewegen von zahlreichen Postfächern erzeugt Exchange erhebliche Mengen an Transaktionsprotokollen sowohl auf den Quell- als auch auf den Zielservern. Selbst bei Servern mit genügend Festplattenplatz ist so die Kapazitätsgrenze schnell erreicht. Vor allem beim Verschieben über Nacht kann Ihnen am nächsten Tag eine Überraschung blühen, wenn der Vorgang abgebrochen wurde, da die Transaktionsprotokolle die Festplatten geflutet haben. Um diesem Problem aus dem Weg zu gehen, sollten Sie entweder nicht zu viele Postfächer auf einmal verschieben, dafür sorgen, dass genügend Festplattenplatz verfügbar ist, oder in den Eigenschaften der beteiligten Postfachspeicher die Umlaufprotokollierung aktivieren. Letztgenannte Funktion beschränkt die Zahl der abgelegten Transaktionsprotokolle.

Beim Verschiebevorgang kopiert Exchange das Postfach zunächst auf den Zielserver und vergleicht dieses dann mit dem Quell-Postfach. Erst danach löscht der Assistent das Quell-Postfach. Es besteht also zu keiner Zeit die Gefahr eines Datenverlustes, da das Quell-Postfach bis zum Schluss vorhanden ist. Auch wenn Sie den Verschiebevorgang abbrechen, gehen keine Daten verloren. Haben Sie das Service Pack 1 für Exchange 2010 installiert, können Sie bereits während der Erstellung des Archivs eine andere Datenbank auswählen. Bei Postfächern, für die Sie bereits die Archivierung aktiviert haben, können Sie das Archiv auch nachträglich verschieben:

1. Öffnen Sie die Exchange-Verwaltungskonsole.
2. Klicken Sie auf den Punkt "Empfängerkonfiguration".
3. Klicken Sie mit der rechten Maustaste auf das Postfach, dessen Archiv Sie verschieben wollen, und wählen Sie "Neue lokale Verschiebungsanforderung".
4. Im unteren Bereich des Fensters stehen Ihnen die Möglichkeiten zur Verfügung, nur das Archiv, nur das Postfach oder beides in eine andere Datenbank zu verschieben.

Regeln für fehlerhafte Nachrichten festsetzen

Auf der Menü-Seite "Verschiebungsoptionen" legen Sie fest, was mit fehlerhaften Nachrichten geschehen soll:

- Postfach auslassen: Bei dieser Option verschiebt Exchange keine Postfächer mit fehlerhaften Nachrichten. Microsoft empfiehlt diese Option.
- Die fehlerhaften Nachrichten auslassen: Wählen Sie diese Option nur dann aus, wenn die Verschiebungsanforderung beim vorherigen Versuch keinen Erfolg hatte. In diesem Fall müssen Sie dann noch die maximale Anzahl auszulassender Nachrichten festlegen. Möglich ist hierbei ein Wert von -1 bis 2.147.483.647. Wählen Sie -1, um eine unbegrenzte Anzahl fehlerhafter Nachrichten auszulassen.

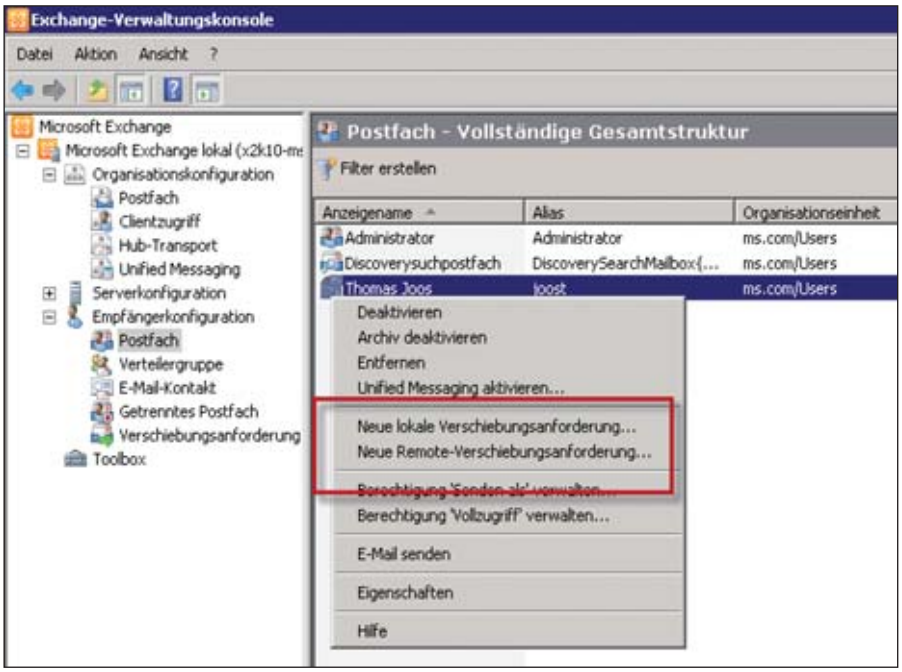


Bild 1: Dem Menüpunkt zum Verschieben von Postfächern in Exchange 2010 hat Microsoft eine recht komplizierte Bezeichnung verpasst

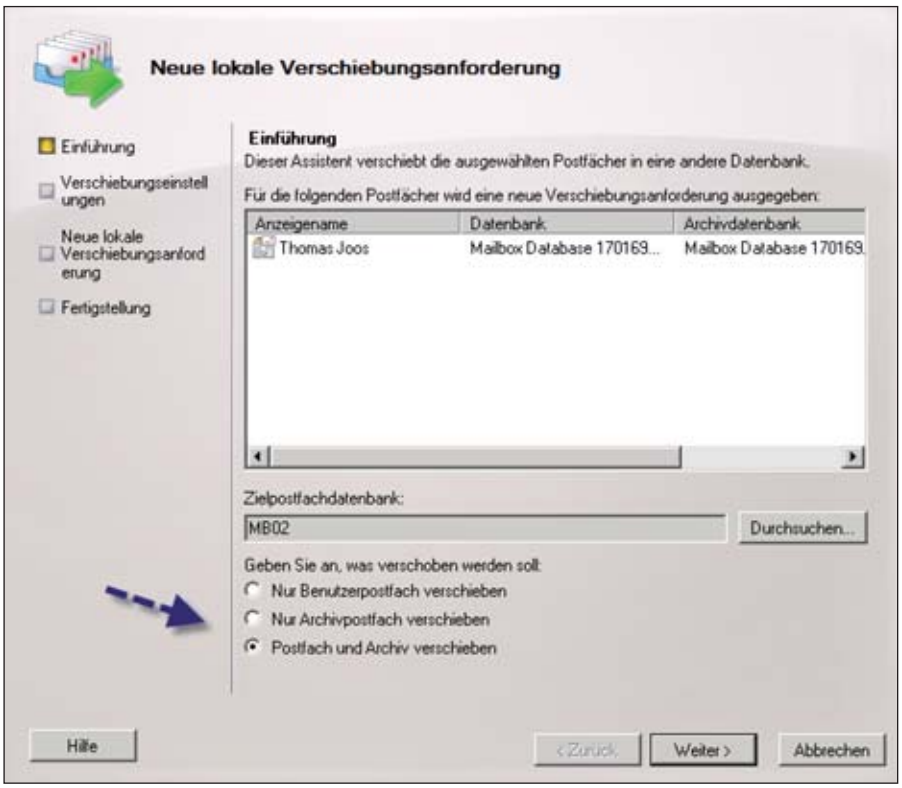


Bild 2: Mit der Installation des Service Pack 1 für Exchange 2010 lassen sich das Benutzerpostfach und das Archiv auf Wunsch auch einzeln verschieben

Klicken Sie auf der nächsten Seite auf "Neu", um die Verschiebungsanforderung zu erstellen. Exchange verschiebt das Postfach und Sie sehen über den Menüpunkt "Verbindungsanforderung", welche Arbeiten der Server durchgeführt hat beziehungsweise wie der aktuelle Stand beim Verschieben ist. Über die Eigenschaften einer Verbindungsanforderung sehen Sie den Status des Vorgangs und können sich defekte Nachrichten anzeigen lassen. Während des Verschiebevorgangs können Benutzer wie schon erwähnt weiter mit dem Postfach arbeiten. Nur wenn der Vorgang abgeschlossen ist und der Anwender eine Aktion durchführen will, mit der Outlook eine Verbindung zum neuen Server benötigt, erscheint eine Fehlermeldung und der Anwender muss Outlook neu starten. Startet der Benutzer nach dem Verschiebevorgang seinen Mailclient neu, verbindet sich Outlook automatisch mit dem neuen Server.

Achten Sie beim Verschieben darauf, dass die Größe der Postfächer nicht die Grenzwerte überschreitet, die auf dem Zielpostfachspeicher gesetzt sind. Ist ein Postfach zu groß, verschiebt Exchange dieses nicht auf den Zielserver. Die Grenzwerte für Postfachspeicher sehen Sie auf der Registerkarte "Grenzwerte", wenn Sie in der Exchange-Verwaltungskonsole über "Organisationskonfiguration\Postfach" die Eigenschaften der Datenbank aufrufen.

Verschieben mit der Shell

Zum Verschieben von Postfächern in der Exchange-Verwaltungsshell verwenden Sie das CMDlet "New-MoveRequest". Bevor Sie ein Postfach über die Exchange-Verwaltungsshell verschieben, können Sie mit der Option "WhatIf" testen, was beim Verschieben passieren würde, ohne den Vorgang tatsächlich zu starten. Ein Beispiel für diesen Befehl sieht so aus:

```
New-MoveRequest -Identity
  thomas.joos@contoso.com -Target-
  Database mailbox02 -WhatIf
```

Tatsächlich verschieben Sie das Postfach dann mit dem Befehl

```
New-MoveRequest -Identity
  thomas.joos@contoso.com
  -TargetDatabase mailbox02
```

Mit dem Befehl

```
Get-Mailbox -Database mailbox01 |
  New-MoveRequest -TargetDatabase
  mailbox02 -BatchName "mb01tomb02"
```

können Sie sämtliche Postfächer einer Datenbank in eine komplett andere Datenbank verschieben.

Verschieben von Postfächern zwischen Organisationen

Mit Exchange 2010 besteht die Möglichkeit, Postfächer zwischen Exchange-Servern unterschiedlicher Organisationen zu verschieben. Auch die Vorgängerversionen Exchange 2003/2007 unterstützen diese Funktion. Über den Menüpunkt "Neue Remoteverschiebungsanforderung" verschieben Sie das ausgewählte Postfach in eine andere Exchange-Organisation. Exchange 2010 unterstützt dabei zwei Arten von Verschiebungsvorgängen für Remotepostfächer:

1. Verschieben von Postfächern innerhalb von Exchange 2010-Organisationen: Bei diesem Szenario verfügen Sie über eine Exchange 2010-Organisation und eine zweite Organisation mit mindestens einem Exchange 2010-Clientzugriffsserver.
2. Verschieben von Postfächern bei Verwendung einer älteren Exchange-Version: In diesem Fall verfügen Sie über eine Exchange 2010-Organisation und eine zweite Organisation mit Exchange 2003 SP2 oder Exchange 2007 SP2/SP3. Auch ein Mischbetrieb ist hier möglich.

Versionsunterschiede von Exchange beachten

Ist in der Organisation mit den älteren Exchange-Versionen kein Exchange 2010-Clientzugriffsserver installiert, können Sie zum Verschieben der Postfächer nicht die Exchange-Verwaltungskonsole verwenden, sondern benötigen die Exchange-Verwaltungsshell. Zudem ist zu beachten, dass Exchange 2010-Clientzugriffserver nur über eine entsprechende Anpassung und nur mit einer angepassten URL auf Exchange 2003-Backend-Server zugreifen können. Migrieren Sie von Version 2003 auf Exchange 2010, sollten Sie für Anwender, die noch ein Postfach unter Exchange 2003 haben, eigene Frontend-Server einsetzen, keine Exchange 2010-CAS-Server.

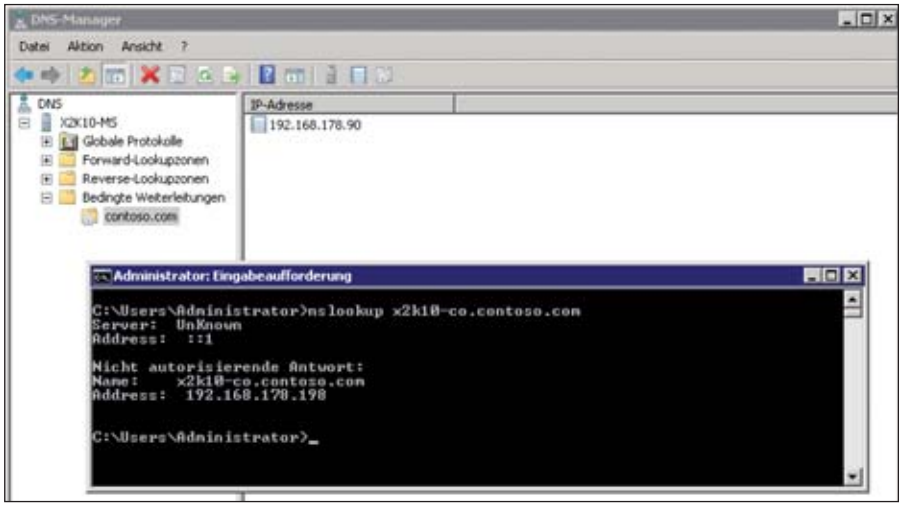


Bild 3: Für die korrekte Auflösung verschiedener Gesamtstrukturen sollten Sie bedingte Weiterleitungen verwenden

Beim Verschieben zwischen Organisationen gehen unter Umständen Berechtigungen Dritter für den Postfachzugriff verloren. Das ist vor allem dann der Fall, wenn der entsprechende Benutzer nicht in der Ziel-Organisation vorhanden ist. Der Postfachreplikationsdienst (MRS) versucht über das Attribut "msExchMailboxGUID", Postfach- und Postfachordnerberechtigungen beizubehalten. Die Sicherheits-IDs (SID) in den Zugriffssteuerungseinträgen ersetzt Exchange dabei. Ohne zugewiesene SID gehen die Berechtigungen verloren. Damit Sie ein Verschieben über verschiedene Gesamtstrukturen durchführen können, müssen Sie sich mit der Exchange-Verwaltungskonsole erst mit der anderen Gesamtstruktur verbinden. Damit das funktioniert, aktivieren Sie die Remoteverwaltung der PowerShell:

1. In der anderen Organisation müssen Sie in der Befehlszeile zunächst mit *winrm quickconfig* die Remoteverwaltung aktivieren.
2. Zudem ist die Namensauflösung in beiden Organisationen sicherzustellen. Der schnellste Weg dafür ist, in der DNS-Verwaltung auf den DNS-Servern der beiden Organisationen eine bedingte Weiterleitung für die jeweilige Organisation anzulegen.

Namensauflösung kontrollieren

Es muss sichergestellt sein, dass sich die beiden Exchange-Server gegenseitig mit ihrem DNS-Namen auflösen können. Nachdem Sie die Namensauflösung überprüft haben, starten Sie die Exchange-Verwaltungskonsole und klicken mit der rechten Maustaste auf den obersten Menüpunkt der Konsole Microsoft Exchange. Wählen Sie die Option "Exchange-Gesamtstruktur hinzufügen" aus. Geben Sie im neuen Feld einen Anzeigenamen ein und den FQDN des Exchange-Servers der Ziel-Organisation, in der Sie die Remoteverwaltung mit *winrm quickconfig* aktiviert haben. Entfernen Sie den Haken bei "Anmeldung mit Standardanmeldenamen" und authentifizieren Sie sich an der fremden Gesamtstruktur. Eine Vertrauensstellung ist dazu nicht unbedingt notwendig, die bedingte DNS-Weiterleitung reicht aus. Klicken Sie auf "OK" und lassen Sie Exchange die Verbindung aufbauen. Für den Verbindungsaufbau benötigen Sie natürlich die Authentifizierungsdaten eines Administratorkontos in der Organisation. Anschließend sehen Sie die Organisation in der Exchange-Verwaltungskonsole und arbeiten mit den hinterlegten Rechten.

Sollte die Verbindung nicht funktionieren, geben Sie in der Befehlszeile den Befehl *WinRM enumerate winrm/config/listener* ein. Stellen Sie sicher, dass ein Listener mit dem Port 5985 aktiv ist und auf alle IP-Adressen des Servers gebunden ist. Selbstverständlich darf der Port nicht durch eine Firewall blockiert sein. Standardmäßig schaltet Exchange den Port in der Windows-Firewall frei. Setzen Sie eine weitere Firewall zwischen Client und Server ein, sollten Sie diesen Port offen lassen. Für die Authentifizierung verwenden die Konsole und die Shell das Kerberos-Verfahren.

Öffnen Sie bei Problemen in der IIS-Verwaltung auf dem Exchange-Server das virtuelle Verzeichnis "/PowerShell". Überprüfen Sie, ob "Kerbauth" als Modul hinterlegt ist. Stellen Sie sicher, dass dieses Modul nicht für die Standardwebseite aktiviert ist, sondern nur für das virtuelle PowerShell-Verzeichnis. Klicken Sie dazu auf das virtuelle Verzeichnis in der IIS-Verwaltung und dann auf "Module". Auch das Modul "WSMan" muss für das

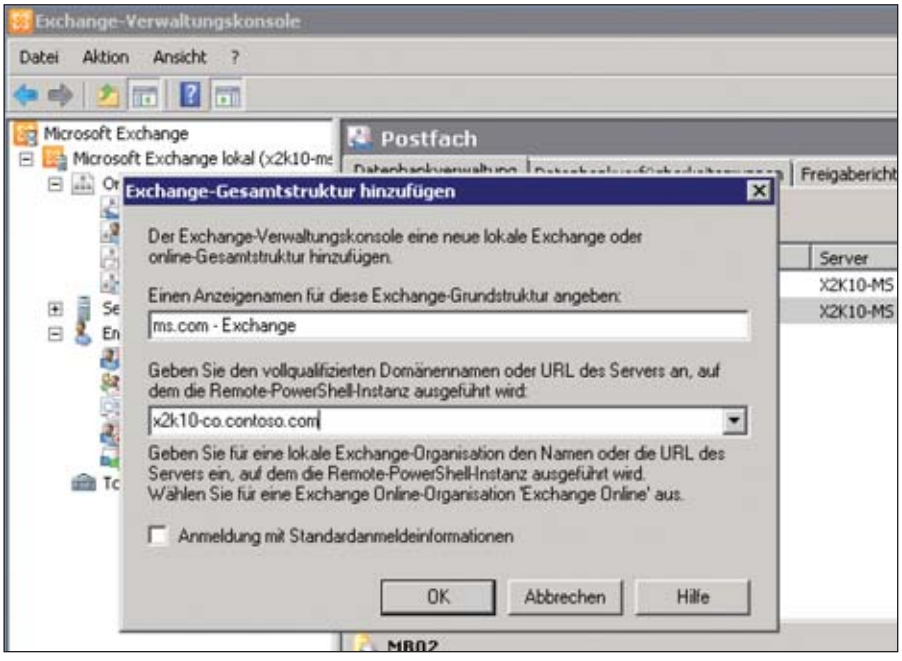


Bild 4: Um eine neue Exchange-Gesamtstruktur hinzuzufügen, sind die korrekten Anmeldeinformationen vonnöten

Liefertermin:
Ende Oktober 2011

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2011!

180 Seiten Praxis-Know-how rund um das Thema

SharePoint 2010 für Administratoren

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft II/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

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/2011 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

☐ **Ja**, ich bestelle das IT-Administrator Sonderheft II/2011 zum Preis von **€ 29,90** inkl. Versand und 7% MwSt.

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0511

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

virtuelle Verzeichnis aktiviert sein und in der Liste erscheinen. Auf dem Server können Sie in der Exchange-Verwaltungsshell testen, ob ein bestimmter Benutzer berechtigt ist, sich über das Netzwerk über eine Remote-Powershellsitzung zu verbinden. Geben Sie dazu den Befehl

```
(Get-User {Benutzername}).Remote-
  PowershellEnabled
```

ein. Erhalten Sie als Ausgabe "false", darf der Benutzer keine Verbindung aufbauen, erhalten Sie "true", ist die Verbindung gestattet. Wollen Sie den Verbindungsaufbau für den Benutzer gestatten, verwenden Sie den Befehl

```
Set-User {Benutzername}
  -RemotePowerShellEnabled $True
```

Überprüfen Sie in den Eigenschaften des virtuellen Verzeichnisses "/PowerShell", ob der korrekte Pfad in den Grundeinstellungen eingetragen ist. Der Pfad lautet in der Standardinstallation "C:\Program Files\Microsoft\ExchangeServer\V14\ClientAccess\PowerShell". In manchen Fällen kann die Verwaltungskonsole die Verbindung auch dann nicht aufbauen, wenn Sie auf dem Server mehrere Webseiten aktiviert haben und die Standardwebseite nicht verfügbar ist. Auch die Konfiguration einer automatischen Ordnerumleitung zu "https://{Servername}/owa" resultiert häufig in solchen Fehlern. Die PowerShell setzt den Port 80 für die Remoteverbindung voraus. Ist der Port nicht vorhanden oder mit einer anderen Webseite verknüpft, lässt sich Exchange nicht über das Netzwerk verwalten.

Stellen Sie sicher, dass für die Standardwebseite in den Bindungen für Port 80 kein Hostname eingetragen ist und der Port auch mit der Seite verbunden ist. Auf dem virtuellen Verzeichnis PowerShell darf kein SSL aktiviert sein. Überprüfen Sie in der IIS-Verwaltung über "Anwendungspools" auch, ob alle notwendigen Exchange-Anwendungspools gestartet sind, vor allem der Pool "MSExchangePowerShellAppPool". Ein weiteres Problem beim Starten der Verwaltungsprogramme tritt auf, wenn die Variable "ExchangeInstallPath" nicht in den Systemvariablen auf dem Exchange-Server gesetzt ist oder auf das falsche Verzeichnis zeigt. Um das zu überprüfen, rufen Sie die Eigenschaften von "Computer" im Startmenü auf und wechseln auf die Registerkarte "Erweitert":

1. Klicken Sie hier auf die Schaltfläche "Umgebungsvariablen".
2. Stellen Sie sicher, dass im unteren Bereich bei Systemvariablen die Variable "ExchangeInstallPath" auf den Pfad "C:\Program Files\Microsoft\Exchange Server\V14" zeigt beziehungsweise auf den Pfad, in dem Sie Exchange installiert haben.

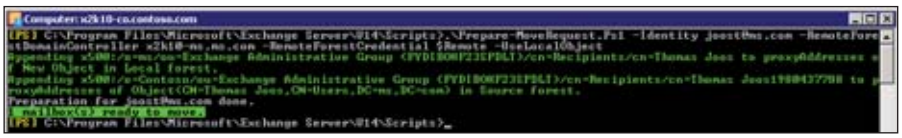


Bild 5: Vor dem Verschieben von Postfächern zwischen Exchange-Organisationen sind einige Vorbereitungen zu treffen

Wollen Sie Benutzerkonten und die dazugehörigen Postfächer von der Quellstruktur in die Zielstruktur übernehmen, sollten Sie vor der Übernahme der Postfächer die Benutzerkonten mit dem Active Directory Migration Tool (ADMT) übernehmen. Außerdem benötigen Sie ein Skript, das die notwendigen Exchange-Attribute übernehmen kann.

Zielorganisation per Skript vorbereiten

Beim Gesamtstruktur-übergreifenden Verschieben von Postfächern muss die Ziel-Organisation über ein E-Mail-aktiviertes Benutzerobjekt verfügen, das mit dem Postfach in der Quell-Organisation übereinstimmt. Die E-Mail-aktivierten Benutzer müssen außerdem die folgenden Bedingungen erfüllen:

- Das Attribut "msExchMailboxGUID" muss sowohl mit dem Postfach als auch mit dem E-Mail-aktivierten Benutzer übereinstimmen.
- Bei Verwendung von Archivpostfächern müssen die Attribute "msExchArchiveGUID" und "msExchArchiveName" in beiden Gesamtstrukturen für das Archivpostfach übereinstimmen.
- Das Attribut "mailNickname" wird bei der Erstellung des E-Mail-aktivierten Benutzers erstellt und muss in beiden Gesamtstrukturen übereinstimmen.
- Der E-Mail-aktivierte Benutzer in der Ziel-Organisation muss über eine SMTP-Adresse innerhalb des Namensraums für E-Maildomänen verfügen.

Bevor Sie ein Postfach von der Quell-Organisation zur Ziel-Organisation verschieben, sollten Sie zunächst überprüfen, ob die Exchange-Attribute für die entsprechenden Benutzerkonten in der Ziel-Organisation vorhanden und aktuell sind. Haben Sie keine anderen Werkzeuge für die Synchronisierung der Attribute, können Sie auch mit dem internen Skript *PrepareMoveRequest.ps1* arbeiten. Dieses finden Sie im Verzeichnis "Program Files\Microsoft\ExchangeServer\V14\Scripts". Damit Sie das Skript verwenden können, müssen in der Quell-Organisation Server mit Exchange 2003, Exchange 2007 oder Exchange 2010 vorhanden sein. In der Ziel-Organisation ist Exchange 2010 erforderlich. Sie sollten das Skript in der Exchange-Verwaltungsshell des Servers in der Ziel-Organisation durchführen. Das Skript hat verschieden Schalter, die Sie der Tabelle "Optionen des Skripts *PrepareMoveRequest.ps1*" entnehmen können.

Sie benötigen für das Ausführen des Skripts also Administratorrechte in der Ziel-Organisation und in der Quell-Organisation. Für die Quell-Organisation sind die beiden Rollen "Exchange Server Administrators" und "Exchange Recipient Administrators" notwendig, in der Zielorganisation bedarf das Konto mindestens der RBAC-Rollen "Move Mailboxes", "Mail Recipients" und "Mail Recipient Creation". Die Ausführung des Skripts nehmen Sie am besten so vor, dass Sie die Anmeldedaten an der lokalen Organisation (Ziel-Organisation) und der Remote-Organisation (Quell-Organisation) in Variablen eingeben. Öffnen Sie dazu die Exchange-Verwaltungsshell und geben Sie den Befehl *$local = get-credential* ein. Sind Sie bereits mit einem Konto angemeldet, das über genügend Rechte verfügt,

benötigen Sie diesen Befehl nicht. Anschließend geben Sie die Daten eines Administratorbenutzers der Ziel-Organisation ein. Verwenden Sie den gleichen Befehl mit der Variablen *$remote = get-credential*. Sie benötigen Administratorrechte in der Quell-Organisation, da das Skript die Ziel-Adresse als X500-Adresse in das Objekt der Quell-Organisation schreibt. Wechseln Sie dann in das Verzeichnis "Program Files\Microsoft\Exchange Server\V14\Scripts" und tippen Sie den folgenden Befehl ein:

```
.\Prepare-MoveRequest.Ps1 -Identity
  {E-Mail-Adresse eines Benutzers in
  der Quell-Organisation} -RemoteFo-
  restDomainController {FQDN eines
  DC in der Quell-Organisation} -Re-
  moteForestCredential $Remote -Use-
  LocalObject
```

Anschließend bereitet das Skript den Benutzer für den Verschiebevorgang vor und stellt sicher, dass das Benutzerkonto in der Ziel-Organisation über die notwendigen Attribute verfügt, um einen Verschiebevorgang zu starten. Ist bereits ein Objekt vorhanden, passt der Befehl das Konto durch die Option "-UseLocalObject" an. Ist kein passendes Konto vorhanden, legt das Skript einen Benutzer an. Bei dem neuen Benutzerkonto handelt es sich um einen neuen, deaktivierten E-Mail-aktivierten Benutzer.

Wollen Sie mehrere Benutzerkonten auf einmal vorbereiten, empfiehlt Microsoft, die E-Mailadressen in einer CSV-Datei aufzunehmen. Wie Sie dabei vorgehen, entnehmen Sie einem weiteren Technet-Beitrag [2].

Optionen des Skripts *PrepareMoveRequest.ps1*

Option	Eingabe	Beschreibung
Identity	Notwendig	Diese Option ermöglicht die Identifizierung des Quell-Postfachs, das Sie verschieben wollen.
RemoteDomain-Controller	Notwendig	Hier geben Sie einen Domänencontroller in der Quell-Organisation ein.
RemoteForest-Credential	Notwendig	Hier geben Sie die Anmeldedaten eines Administrators der Quell-Organisation ein, der das Recht hat, Daten zu kopieren und Daten zu schreiben.
LocalForest-Credential	Optional	Mit dieser Option können Sie die Anmeldedaten in der Ziel-Organisation eingeben, wenn der Benutzer, mit dem Sie arbeiten, nicht die notwendigen Rechte hat.
TargetOU	Optional	Hier können Sie die OU in der Ziel-Organisation eingeben, in der das Skript das Benutzerkonto anlegen soll.
LinkedMailUser	Optional	Diese Option erlaubt die Werte Strue und Sfalse. Der Wert ist standardmäßig auf Sfalse gesetzt. Mit Strue erstellt das Skript ein verknüpftes E-Mail-aktiviertes Konto mit dem Benutzer in der Quell-Organisation
Mailbox-DeliveryDomain	Optional	Diese Option legt die E-Mail-Domäne für das Benutzerkonto fest. Standardmäßig verwendet das Skript die Standarddomäne in der Ziel-Organisation.
UseLocalObject	Optional	Diese Option entdeckt Konflikte innerhalb des Benutzerkontos und kann ein bereits existierendes Objekt entsprechend konvertieren.

SIDHistory mit ADMT übernehmen

Beim Anlegen des neuen Benutzers in der Ziel-Organisation übernimmt das Skript verschiedene Attribute für das Zielobjekt. Allerdings kann das Skript keine SIDHistory übernehmen. Dies bedeutet, dass Sie das neue Benutzerkonto zunächst nicht für eine Migration verwenden können, da keine Dateizugriffsberechtigungen funktionieren. Wollen Sie das neue Benutzerkonto auch für die Anmeldung und den Zugriff auf Dateifreigaben im Netzwerk verwenden, ist nach der Verwendung des Skripts *Prepare-MoveRequest.ps1* noch der Einsatz des Active Directory-Migrationstools (ADMT) vonnöten. Achten Sie aber darauf, dass erst die Version 3.2 des ADMT auch Domänen mit Windows Server 2008 R2 unterstützt.

Übernehmen Sie Daten aus der Quell-Organisation mit dem ADMT in die Ziel-Organisation, ist auch die SIDHistory vorhanden. Microsoft empfiehlt die Verwendung von *Prepare-MoveRequest.ps1* und dann erst die Übernahme durch das ADTM. Führen Sie zuerst das ADMT aus, legt dieses den neuen Benutzer zwar an, allerdings ist dann das Skript nicht dazu in der Lage, die Exchange-Attribute zu übernehmen – zumindest dann, wenn Sie kein Service Pack 1 für Exchange 2010 installiert haben. Durch die Installation von Service Pack 1 für Exchange 2010 erhält *Prepare-MoveRequest.ps1* noch die Option "OverwriteLocalObject". Diese neue Option ermöglicht es, bereits angelegte Benutzerkonten zu aktualisieren. Verwenden Sie die neue Option, kann das Skript die Attribute von der Quell-Organisation kopieren. Das funktioniert jedoch nur dann, wenn das Benutzerkonto in der Ziel-Organisation eine Adresse aus der Quell-Organisation hat, die auf das entsprechende Quell-Benutzerkonto zeigt. Sie müssen dazu OverwriteLocalObject zusammen mit der Option "UseLocalObject" verwenden.

Aktivieren des MRSProxy-Dienst

Damit Sie Postfächer zwischen Exchange-Organisationen verschieben können, sollte in jeder Organisation ein Clientzugriffserver mit Exchange 2010 stehen, da der Vorgang über diese Server abläuft, oder genauer gesagt über den MRSProxy-Dienst. Dieser Dienst ist standardmäßig installiert, aber deaktiviert. Damit Sie diesen nutzen können, müssen Sie ihn zunächst aktivieren. Arbeiten Sie mit Clientzugriffservern in einem NLB-Verbund, aktivieren Sie den Dienst auf allen Servern des Verbundes. Sie können testen, ob der MRSProxy läuft, wenn Sie sich mit der Webseite "https://{Servername des Clientzugriffservers}/ews/mrsproxy.svc" verbinden. Findet der Internet Explorer die Seite nicht, ist der Dienst deaktiviert. Um den Dienst zu aktivieren, passen Sie die Steuerdatei *web.config* des Clientzugriffsdienstes an. Öffnen Sie dazu auf dem entsprechenden Clientzugriffserver die Datei *web.config* im Verzeichnis "{Exchange-Installationspfad}\V14\ClientAccess\ExchWeb

\EWS\". Sichern Sie die Datei aber vor der Bearbeitung. Suchen Sie nach folgender Passage:

```
<!- Mailbox Replication Proxy Server
  configuration ->
<MRSProxyConfiguration
IsEnabled="false"
MaxMRSConnections="100"
DataImportTimeout="00:01:00" />
```

Ändern Sie den Wert "IsEnabled" auf "true" ab und speichern Sie die Datei. Bei der Kommunikation arbeiten die Server in der Ziel- und Quell-Organisation über HTTPS und benötigen dazu das Serverzertifikat des jeweilig anderen Servers. Aus diesem Grund muss das Zertifikat von einer vertrauenswürdigen Stammzertifizierungsstelle ausgestellt sein.

Abschließendes Verschieben des Postfachs durchführen

Nach der erfolgreichen Verbindung der beiden Organisationen in der Exchange-Verwaltungskonsole und den beschriebenen Vorbereitungen können Sie eine neue Remoteverschiebungsanforderung starten und unter dem Menüpunkt "Verschiebungsoptionen" verschiedene Einstellungen festlegen:

- Quellgesamtstruktur: In diesem Feld wird die Quellgesamtstruktur mit den zu verschiebenden Postfächern angezeigt.
- Zielgesamtstruktur: Wählen Sie die Zielgesamtstruktur aus der Liste aus. Die Gesamtstruktur muss dazu in der Exchange-Verwaltungskonsole verbunden sein, wie auf den vorangegangenen Seiten beschrieben.
- FQDN des Proxyservers für den Postfachreplikationsdienst in der Quellgesamtstruktur: Hier geben Sie den vollqualifizierten Domänennamen des Servers ein, auf dem sich der Proxy für den Postfachreplikationsdienst befindet. Dabei handelt es sich um einen Clientzugriffserver in der Remotegesamtstruktur. Beispiel: x2k10ms.microsoft.com.
- Anmeldeinformation der folgenden Quellgesamtstruktur verwenden: In diesem Feld geben Sie die Authentifizierung ein, wenn Sie keine Vertrauensstellung erstellt haben.
- Zielzustellungsdomäne: Hier geben Sie den vollqualifizierten Domänennamen der externen E-Mailadresse ein, die nach Abschluss der Verschiebungsanforderung in der Quellgesamtstruktur für den E-Mail-aktivierten Benutzer erstellt wird. Nach Abschluss des Verschiebungsvorgangs stempelt der Ziel-Exchange-Server diese Adresse als externe E-Mailadresse des E-Mail-aktivierten Benutzers.
- Zieldatenbank: Hier geben Sie die Postfachdatenbank ein, in der Exchange das Postfach erstellen soll. Da in Exchange 2010 die Datenbanken einmalig in der Organisation sind und keine feste Verbindung mehr zu einzelnen Servern haben, reicht es, den Namen der DB ohne den Servernamen anzugeben.

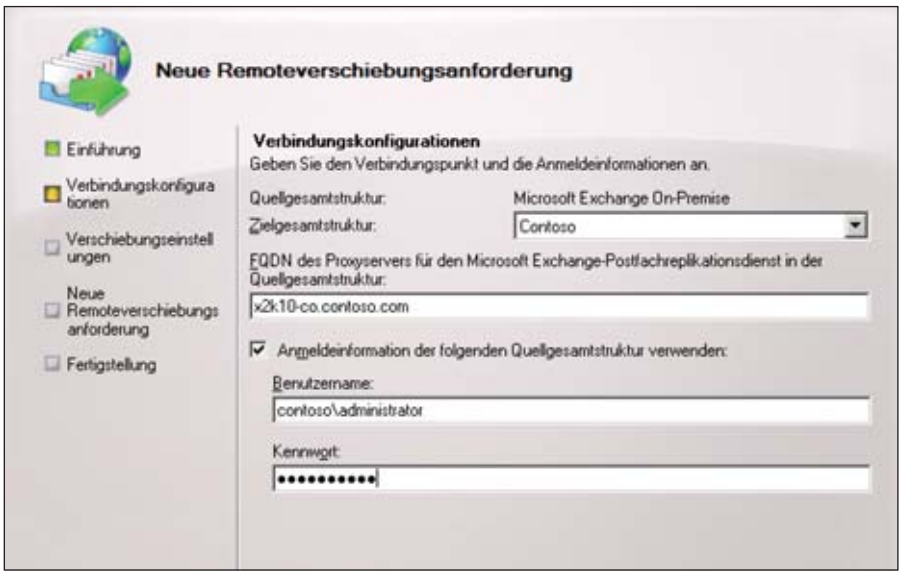


Bild 6: Das abschließende Verschieben von Postfächern zwischen Organisationen

Überprüfen Sie die Einstellungen für die Remoteverschiebungsanforderung und klicken Sie auf "Neu". Wie beim internen Verschieben können Sie auch zwischen Organisationen Postfächer in der Exchange-Verwaltungsshell verschieben. Befindet sich in einer der Organisationen noch kein Exchange 2010-Clientzugriffserver, ist das Verschieben nur in der Verwaltungsshell möglich. Im Folgenden zeigen wir Ihnen ein Beispiel für einen solchen Vorgang:

```
New-MoveRequest -Identity {Benutzer
  in der Ziel-Organisation} -Remote-
  Legacy -TargetDatabase {Name der
  Ziel-Datenbank}" -RemoteGlobalCa-
  talog {FQDN eines DC in der Quell-
  Organisation} -RemoteCredential
  $Remote -TargetDeliveryDomain
  {Name der Ziel-Domäne}
```

Während des Verschiebens des Postfachs aktiviert der Assistent per E-Mail das Benutzerkonto in der Ziel-Organisation. Ist das Benutzerkonto selbst im AD deaktiviert, bleibt es auch deaktiviert. Das Konto in der Quell-Domäne wird durch den Assistenten per Mail deaktiviert und in einen E-Mail-aktivierten Benutzer mit einer E-Mailadresse in der Ziel-Organisation konvertiert. *(ln)*

[1] "Configuring Static RPC Ports on an Exchange 2010 Client Access Server" B5P91

[2] "Prepare Mailboxes for Cross-Forest Moves Using the Prepare-MoveRequest.ps1 script in the Shell" B5P92

Weitere Links zum Thema:

"Understanding Federation" B5P93

"Deploy Exchange 2010 in a Cross-Forest Topology" B5P94

"Exchange Provisioning using ILM 2007 and FIM 2010" B5P95

Problembehandlung bei fehlenden Nutzerattributen B5P96

MRSProxy Service starten B5P97

"Managing Move Requests" B5P98

Link-Codes

Inventarisierung mit Spiceworks 5.0

Würzige Netzwerkverwaltung

von Thomas Drilling

Große Unternehmen brauchen und verwenden Werkzeuge zum Verwalten, Inventarisieren und Analysieren der im Firmennetz eingesetzten Hard- und Software oder für das Einrichten von Helpdesks zum Verarbeiten von Support-Anfragen. Zwar mangelt es in diesem Sektor sicher nicht an leistungsfähigen Tools, die meisten aber sind teuer und kompliziert. Spiceworks dagegen ist kostenlos und richtet sich vor allem an kleine bis mittelgroße Unternehmen. In diesem Workshop gehen wir auf die Inbetriebnahme des Werkzeugs ein und zeigen, wie Sie nach dem ersten Scan-Vorgang schnell an die erfassten Daten kommen.

Spiceworks eignet sich laut dem gleichnamigen texanischen Hersteller für kleine und mittelständische Unternehmen mit bis zu 1.000 Clients. Die Software arbeitet vollständig webbasiert und hat sich eine besonders einfache und intuitive Bedienung zum Ziel gesetzt. Die Unternehmensgründung ist unmittelbar mit dem Produkt verknüpft, das seit seinem Start im Jahr 2006 eine rasante Entwicklung vorweisen kann und heute eine große internationale Community besitzt. Eine Reihe von Assistenten und Werkzeuge unterstützen auch weniger versierte Nutzer beim Erfassen, Administrieren oder Analysieren ihrer IT-Umgebung.

Spiceworks ist weder Free- noch Shareware, wird vom Hersteller aber trotzdem kostenlos angeboten. Zur Finanzierung blendet er Werbebanner in die GUI ein. Unter Kennern haben sich insbesondere die Versionen 3.1 und 4.0 einen guten Ruf erworben. Wir nutzen als Grundlage für diesen Workshop die aktuelle Version 5.0. Deren Funktionsumfang ist über die Jahre mittlerweile so weit gediehen, dass sich das Tool durchaus mit Software vom Kaliber HP OpenView messen kann – und das bei weitaus einfacherer Bedienung.

Haupteinsatzbereich von Spiceworks ist das Inventarisieren sämtlicher Server, Arbeitsplätze und sonstiger Geräte im Netzwerk und der auf den einzelnen Maschinen installierten Software. Sie können somit jederzeit und schnell die auf einem beliebigen Server vorhandene Software oder dessen Hardware-Komponenten abfragen. Darüber hinaus liefert die Management-Plattform auf Wunsch noch tiefer gehende Informationen oder zeigt Warnungen und Event-Hinweise an. So kann der Nutzer etwa jederzeit feststellen, welchen Release-Stand die auf einem ausgewählten Server oder Desktop installierte Software hat und wann die letzten Updates eingespielt wurden.

Innovative Verwaltung über den Browser

Das Spiceworks-Framework besteht aus einem Management-Server und der Client-Software, die vollständig browserbasiert arbeitet. Die GUI besteht also ausschließlich aus dynamischen Web-Seiten – eine Windows-Verwaltungskonsole gibt es nicht – und ist sehr innovativ aufgebaut. Das Design orientiert sich an der Gestaltung moderner Webseiten. Die innere Architektur der Lösung ähnelt hingegen anderen Vertretern dieser Softwaregattung: Ein zentraler Management-Server sammelt die Daten von allen überwachten Geräten und speichert diese in einer Datenbank. Bei der Abfrage der Geräte verwendet das Werkzeug unter Windows WMI. Spiceworks erkennt aber auch Linux- und Mac-Rechner sowie Router, VoIP-Telefone und IP-fähige Drucker. Bei der Inventarisierung können Sie eine IP-Range definieren und gegebenenfalls User-Accounts vorgeben, mit denen sich der Scanner an den betreffenden Geräten anmeldet.

So nehmen Sie Spiceworks in Betrieb

Das Setup von Spiceworks 5.0 ist schnell erledigt. Nach dem Download der 29 MByte großen EXE-Datei starten Sie die Installation durch einen einfachen Doppelklick. Daraufhin startet ein Assistent den Standard-Browser und führt in einer Web 2.0-Applikation durch das weitere Setup. Legen Sie nun den gewünschten Nutzernamen und das Passwort fest und bestätigen Sie Ihre Eingaben. Auf dem folgenden Start-Screen haben Sie die Möglichkeit, in die Module "Inventory", "Help Desk" oder "Configuration Backup" zu verzweigen – der Menüpunkt "Inventory" dürfte für die meisten Nutzer mit Abstand der wichtigste sein.

Beim ersten Start fragt Spiceworks, ob Sie Ihr gesamtes Netzwerk inventarisieren möchten oder nur den eigenen PC. Vor dem Netzwerk-Scan erfragt der Assistent

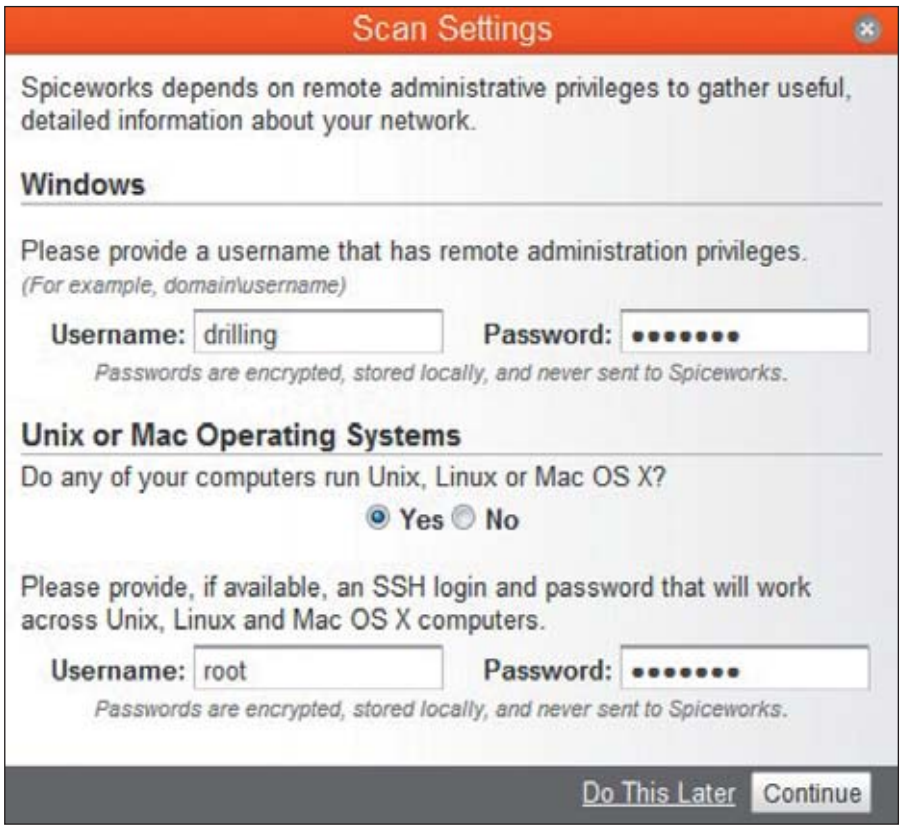


Bild 1: Mit den richtigen Credentials kann Spiceworks problemlos Windows-, Mac OS- und Linux-Arbeitsplätze ermitteln

einen Benutzer-Account nebst Passwort, der auf dem Management-Server über Remote Administration-Privilegien verfügt. Hierbei muss es sich um einen existenten Windows-Account handeln. Gibt es im Netz auch Unix-/Linux-Rechner, ist zusätzlich darunter die Option "Yes" zu markieren. Der Assistent klappt in diesem Fall weiter auf und erfragt einen Unix-Benutzer-Account, der über eine SSH-Login-Berechtigung verfügt. Danach zeigt der Assistent den zu scannenden IP-Bereich an sowie die eben spezifizierten Windows- und SSH-Konten.

Ein Klick auf "Start" leitet den Scan ein. Spiceworks trägt die eben getroffene Scan-Konfiguration außerdem automatisch in seinen Scheduler ein. Die Scan-Parameter, wie etwa die zu überprüfende IP-Range, können Sie entweder direkt an dieser Stelle mit einem Klick auf "Settings" oder im Inventory-Menü bei den Einstellungen ändern. Ein Klick auf "Network Scan" zeigt die Scheduling-Liste der aktuell gültigen Scan-Einträge. Ein vorhandener Job lässt sich wahlweise durch einen Klick auf den kleinen Pfeil rechts neben "Edit" und Auswahl des Kontextmenü-Eintrages "Edit" ändern oder Sie legen gleich einen neuen Eintrag an.

Weiter unten auf dieser Seite ist es möglich, die Scheduling-Parameter zu ändern, so dass der Status der Netzwerküberwachung mit der Häufigkeit potenziell hinzukommender Netzwerkgeräte Schritt halten kann. Nach erfolgreichem Scan können Sie sämtliche im Netzwerk identifizierten Komponenten webbasiert verwalten, Reporte über Ihre IT-Umgebung erstellen oder Fehleranalysen durchführen. Die Inventory-Seite ist damit zentrale Informationsschnittstelle zwischen Admin und den im Netzwerk installierten IT-Komponenten.

Alle Geräte im Griff

Auf der Devices-Seite finden Sie im "Environment-Summary" im unteren Drittel alle wichtigen Informationen über die Geräte in einem Netzwerk. Diese Aufstellung verteilt alle relevanten Informationen auf neun Registerkarten. So können Sie etwa im Reiter "Scan Errors" nachvollziehen, ob und an welchen Geräten im Netz der automatische Scan gescheitert ist, etwa weil die zuvor angegebenen Benutzer Accounts dort nicht existieren oder mangels ausreichender Rechte nicht funktionieren. Jede Kategorie der Devices-Sektion offenbart wiederum umfangreiche Detail-Informationen. Die Kategorie "Unknowns" erlaubt, nicht identifizierte Geräte manuell zu klassifizieren. Ein Klick auf "Workstations" bringt detaillierte Informationen zur Konfiguration eines Arbeitsplatz-PCs auf den Schirm, inklusive installierter Software, Ereignis- und Alarmmeldungen oder Log Monitoring.

Per Default zeigt der Reiter "General Info" allgemeine Informationen über den Hersteller an, nebst Seriennummer und den derzeit angemeldeten Besitzer. Im Register "Configuration" gewinnen Sie einen detaillierten Überblick über Prozessor, Betriebssystem samt Seriennummer, den letzten Reboot sowie die Speicher- und Plattenbelegung. Welche Netzwerk-Freigaben auf der betreffenden Maschine eingerichtet sind, offenbart ein Klick auf den Register-Reiter "Network Shares", während Sie aktuelle Events und Warnungen im Reiter "Events" einsehen können. Ein sehr interessantes Feature verbirgt sich im Menü rechts neben der Workstation Summary: Klicken Sie hier im Bereich "Troubleshooting" auf "Compare", besteht die Möglichkeit, mehrere Systeme miteinander zu vergleichen, was die Fehlerdiagnose erleichtert. Übrigens unterstützt Spiceworks auch das Einrichten sogenannter "Custom Groups", so dass Sie das Inventar einer bestimmten Personengruppe oder Abteilung optimal verwalten und überwachen können. Möchten Sie eine neue Gruppe anlegen, aktivieren Sie die Funktion "Create a new Group" und ordnen dann via Drag & Drop einfach die entsprechenden Geräte der neuen Gruppe zu.

Software-Management, Fernzugriff und Daten-Backup

Ein Klick auf den Reiter "Software" im Device Summary präsentiert Ihnen einen vollständigen Überblick über alle auf dieser Maschine installierten Programme inklusive der aktuellen Versions-Nummern. Klicken Sie dagegen im Hauptmenüeintrag "Inventory" auf "Software", erhalten Sie eine Liste sämtlicher im Gesamt-Netz installierten Tools und Programme. Ist eine Anwendung mehrfach installiert, zeigt Spiceworks in der Spalte "Installs" die Anzahl der Installationen an. Möchten Sie wissen, auf welchen Maschinen die jeweiligen Installationen ver-

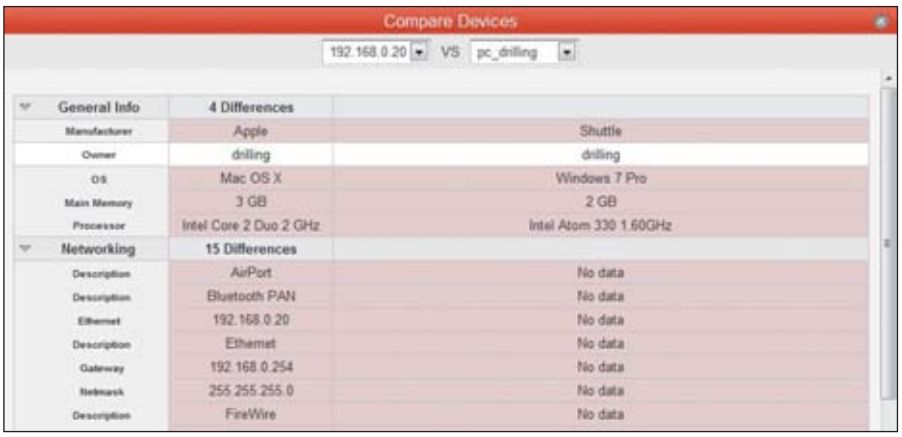


Bild 2: Spiceworks verfügt über eine nützliche Compare-Funktion, mit deren Hilfe sich die Konfiguration zweier Geräte schnell vergleichen lässt

teilt sind, klicken Sie im "Application Summary" unterhalb der Software-Liste auf den Reiter "Installed On". Neben Version und Produkt-ID beziehungsweise -Key berücksichtigt das Werkzeug übrigens auch Lizenzinformationen.

Spiceworks hat auch eine Remote Desktop-Funktionalität integriert, so dass sich Geräte via RDP-Session von einer Konsole aus fernsteuern lassen. Es ist sogar möglich, Mainboards mit vPro-Chipsatz anzusprechen und so Intels Active Management-Technologie zu nutzen. So können Sie etwa einen Rechner per Remote-Zugriff aus- beziehungsweise einzuschalten. Spiceworks lädt dazu ein Plugin nach, sobald Sie auf "Get Remote Control of Your vPro Enabled Machines. Download Plugin Now" klicken.

Daneben beherrscht das Management-Tool gängiges Wake on LAN. Wie immer muss der zu steuernde Rechner dies explizit unterstützen, was einen passenden Netzwerk-Controller nebst aktivierter BIOS-Option voraussetzt.

Das Programm ist ferner dazu in der Lage, ein automatisches Backup der lokalen Spiceworks-Daten durchzuführen, was sich mindestens vor dem Installieren eines Software-Updates anbietet. Die Funktion verbirgt sich im Menü "Inventory / Settings / Backup Configuration". Hier legen Sie zunächst das Backup-Ziel fest (Backup Location). Anschließend können Sie im Bereich "Backup Schedule" ein automatisches Backup initiieren. Ist diese Option aktiviert, führt Spiceworks vor jedem Software-Update eine automatische Sicherung durch. Natürlich steht Ihnen unter "Backup Status" jederzeit frei, ein manuelles Backup durchzuführen.

Fazit

Spiceworks ist eine äußerst passende Management-Lösung für KMUs und weist in Version 5.0 einen hohen Reifegrad auf. Viele Kinderkrankheiten wurden mittlerweile ausgeräumt und die Struktur ist über die Jahre noch klarer geworden. Die enorme Verflechtung der Software mit der Community sorgt zudem dafür, dass etwaige Fehler meist schnell behoben sind, hat aber auch den Effekt, dass Sie sich häufiger als üblich mit neuen Versionen auseinandersetzen müssen. *(ln)*

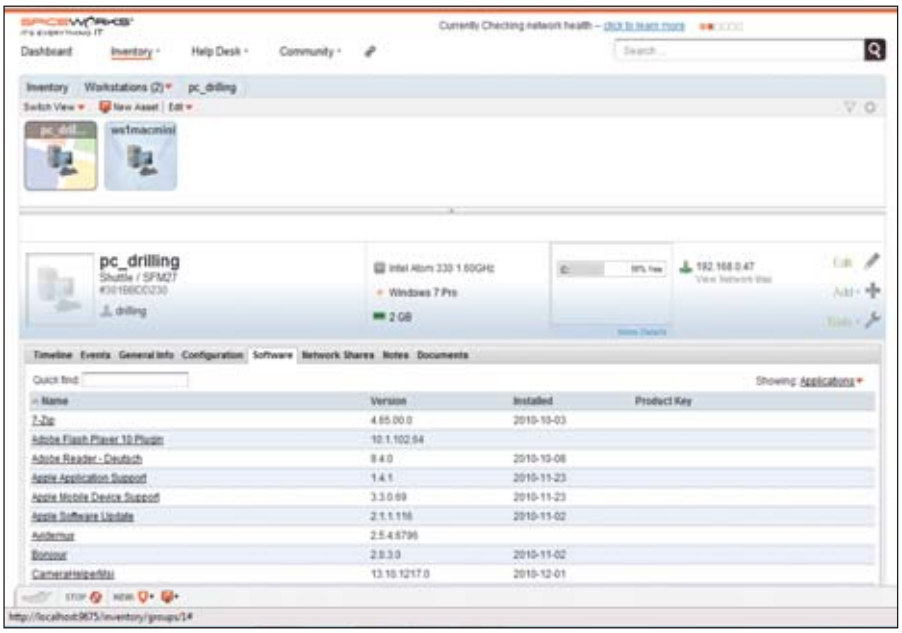


Bild 3: Im Reiter "Software" listet Spiceworks sämtliche auf der betreffenden Maschine installierten Tools und Programme auf

Tipps & Tricks ohne Gewähr

In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps, Tricks und Tools zu den aktuellen Betriebssystemen und Produkten, die in vielen Unternehmen im Einsatz sind. Wenn Sie einen tollen Tipp auf Lager haben, zögern Sie nicht und schicken Sie ihn per E-Mail an tipps@it-administrator.de.

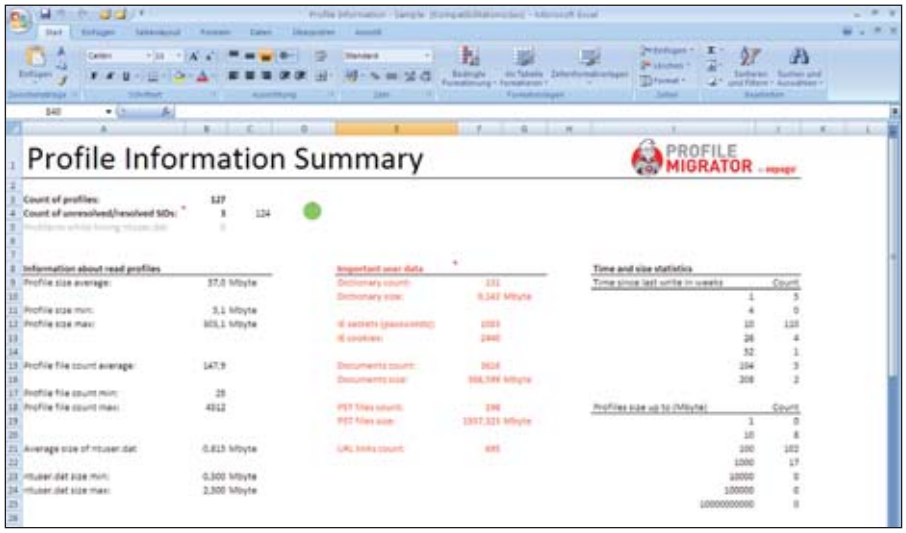
Microsoft Windows

Beim **Speichern von Office 2010-Dateien** aus Word, Excel oder Powerpoint auf ein Netzwerk-Share, das mit Distributed File System Replication (DFSR) repliziert wird, erhalten unsere User regelmäßig die **Fehlermeldung "\\server\share\test.ppt is in use. Please try again later"**. Andere Nutzer hatten die besagte Datei zu diesem Zeitpunkt jedoch sicher nicht in Verwendung. Testweise haben wir im freigegebenen Ordner eine Datei namens *test.ppt* mit 0 Byte Größe angelegt. Das Speichern der Datei auf ein lokales Laufwerk und das anschließende Verschieben auf das Netzwerk-Share funktionierten ohne Probleme, ebenso wie das Speichern aus anderen Applikationen wie dem Notepad. Beim Speichern in besagten Office-Programmen trat die Fehlermeldung aber immer wieder auf. Was kann hier die Ursache sein? Gibt es hier eventuell ein **ungünstiges Zusammenspiel von Office und DFSR**?

Auch wenn es natürlich viele Gründe für die von Ihnen beschriebene Zugriffsverletzung geben kann, liegen Sie mit Ihrer letzten Vermutung vermutlich gar nicht so schlecht. Office legt beim Speichern eine Datei nicht gleich in ihrem endgültigen Format an, sondern erzeugt zunächst eine TMP-Datei mit einem zufälligen Namen. In diese Datei schreibt die Anwendung dann alle relevanten Informationen und erst zum Schluss, beim Schließen des Dokuments, wird die Datei in den letztendlichen Dateinamen umbenannt. Wenn nun DFSR versucht, die zwischenzeitliche TMP-Datei zu kopieren, tritt die beschriebene Zugriffsverletzung auf und das File lässt sich nicht speichern. Um derartigen Konflikten vorzubeugen, schließt DFSR eigentlich standardmäßig gewisse Dateitypen aus – *.BAK, *.TMP und ~*. Nicht immer jedoch ist diese Einstellung korrekt hinterlegt oder wurde durch eine falsche Konfiguration zunichte gemacht. Gehen Sie deshalb auf den zu replizierenden Ordner und sehen Sie sich im Kontextmenü die Eigenschaften an. Im Reiter "General" finden Sie in der Zeile "File Filter" sämtliche von der Replikation auszunehmenden Dateien. In dieser Zeile müssen entweder die drei oben erwähnten Dateitypen stehen oder die Zeile muss komplett leer sein – auch dann greift der Standardausschluss. Die Ausnahmeregelung funktioniert jedoch nicht, wenn etwa nur noch ein Komma oder anderweitige sinnlose Eingaben in dieser Zeile stehen. Dann greift weder die Standard-Einstellung noch ein selbst konfiguriertes Setting. Sehen Sie deshalb zuerst an dieser Stelle nach, wenn vermehrt Zugriffsverletzungen auftauchen und Sie DFSR im Einsatz haben. *(ln)*

Roaming Profiles gibt es ja mittlerweile nun schon sehr lange und sie sind auch in unserem Unternehmen erste Wahl, um Benutzereinstellungen für Systeme gleicher Art bereitzustellen. In der Vergangenheit war es jedoch so, dass die **Profildaten im Rahmen von Migrationsprojekten verworfen** wurden – war es doch bis vor einigen Jahren nicht möglich, die Roaming Profiles-Einstellungen einfach zu übernehmen. Mittlerweile sind ja Anwendungen verfügbar, die diese Daten über Betriebs- und Programmversionsgrenzen übernehmen. Gibt es irgendeine Möglichkeit, vor der Übernahme mit einem Zusatztool zu überprüfen, ob ein **Mitnehmen der alten Profile sinnvoll** ist?

Um zu klären, ob die Übernahme von Profileinstellungen Sinn macht, müssen Sie zunächst einmal wissen, welche Daten mit welchen Volumes sich überhaupt innerhalb der Dateifreigabe für die Roaming Profiles befinden. Das ist nicht ganz so einfach, denn die Profile enthalten neben den Einstellungen für Anwendungen weitere sensible Daten, die gerne vergessen werden. Dazu gehören zum Beispiel die gespeicherten Passwörter des Internet Explorers, Cookies, Dokumente auf dem Desktop, Benutzerwörterbücher et cetera. Eine einfache Möglichkeit, vorhandene Profil-Freigaben mit hunderten oder tausenden von Profilen zu analysieren, bietet ein Powershell Skript, das einige dieser Parameter erfasst und entsprechend auswertet. Gleichzeitig kann das Skript verwaiste und veraltete Profile erkennen. Die Ausgabe erfolgt in einer Excel-Tabelle, die besonders wichtige Parameter wie etwa die Anzahl der gespeicherten Passwörter oder die Größe der PST-Dateien in einem rot markierten Sonderbereich aufführt. Das Skript selbst können Sie im Sepago-Blog herunterladen. Als weitere Voraussetzungen benötigen



Ein kostenloses Skript verrät die wichtigsten Kennzahlen bestehender Roaming Profiles-Daten und erleichtert so die Einschätzung, ob sich deren Migration lohnt

Sie noch die PowerShell 2.0, ein installiertes Microsoft Excel, lokale Administratoren-Rechte sowie Leseerlaubnis auf die Verzeichnisse, in denen die Roaming Profiles liegen. *(sepago/ln)*

Link-Code: B5PE3

blogs.sepago.de READ | WRITE

Mehr Tipps zu den Themen Exchange und Terminaldienste lesen Sie auf http://blogs.sepago.de

Neben den Virtual Hard Disks (VHD) lassen sich bei **Hyper-V** ja auch **Pass-Through Disks** konfigurieren. Diese sollen die Möglichkeit bieten, dass eine virtuelle Maschine ein **LUN direkt vom Storage zugewiesen** bekommt. Das Storage kann dabei eine lokal an Hyper-V angeschlossene Disk oder eine LUN von einem Storage Area Network sein. Was muss ich beachten, damit eine virtuelle Maschine eine Pass-Through Disk ansprechen kann?

Da Microsoft mit Windows Server 2008 R2 die Performance der VHDs massiv optimieren konnte, kommen Pass-Through Disks inzwischen hauptsächlich bei Szenarien zum Einsatz, in denen Volumes grösser als 2 TByte sein müssen. Damit eine VM eine Pass-Through Disk ansprechen kann, gilt es, einige Schritte zu beachten. Der wichtigste Punkt ist, dass die VM exklusiv Zugriff auf den Storage hat. Dazu muss die Disk aus Sicht des Hyper-V-Hosts im Offline-Status sein. Um überhaupt erst eine neue Disk verwenden zu können, müssen Sie diese zunächst auf dem Host initialisieren. Dies können Sie wie gehabt im Disk Management Snap-In (*diskmgmt.msc*) durchführen. Sobald die Disk initialisiert wurde, müssen Sie sicherstellen, dass diese danach wieder im Offline-Status ist. Wie bereits zuvor erwähnt, ist es von großer Wichtigkeit, dass der Hyper-V-Host keinen Zugriff mehr auf die Disk haben darf, wenn Sie diese als Pass-Through konfigurieren wollen. Ist die Disk vorbereitet, können Sie mit der Konfiguration der VM beginnen. In deren Einstellungen fügen Sie nun einfach eine weitere Festplatte hinzu. Anstelle einer VHD wechseln Sie nun aber auf "Physical Hard Disk" und wählen im Drop-Down die gewünschte Pass-Through Disk aus. Wenn Sie die Pass-Through Disk als Boot-Disk benötigen, so müssen Sie diese zwingend an den IDE-Controller anschließen, damit Hyper-V die Festplatte beim Startvorgang erkennt. Einzig reine Daten-Platten können vom SCSI-Controller Gebrauch machen. Diese SCSI-Disks lassen sich der VM übrigens auch im laufenden Betrieb hinzufügen. Überaus wichtig ist zudem folgender Sachverhalt: Betreiben Sie Hyper-V in einem Failover-Cluster, so ist die Konfiguration der VM-Einstellungen ausschließlich in der Failover Cluster Management Console (*CluAdmin.msc*) durchzuführen. Wer hier andere Wege wählt, riskiert, dass die Cluster Group nicht aktualisiert wird und die Pass-Through Disk nicht richtig funktioniert. Zum Schluss noch ein Hinweis zum Troubleshooting: Zwei Effekte treten häufig auf, wenn die Festplatte nicht offline war: Zum einen kann der Datenspeicher der VM erst gar nicht als Pass-Through Disk zugewiesen werden. Zum anderen hat das Gast-Betriebssystem der virtuellen Maschine dann nur Read-Only-Zugriff auf die Platte.

(Michel Lüscher/ln)

Server Talk

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

Microsoft Exchange

Beim **E-Mailzugriff über Outlook Web Access** kommt es bisweilen vor, dass der Exchange 2007- oder Exchange 2010-User eine – je nach Programmversion unterschiedliche – Fehlermeldung erhält. Die Nachricht besagt, dass der **Zugriff auf die Mailbox nicht möglich** ist. Wo kann hier das Problem liegen?

Fehler beim OWA-Zugriff auf Exchange-Konten können natürlich eine Reihe von Ursachen haben. Unter Umständen liegt das Problem aber ganz einfach daran, dass das Attribut "msExchVersion" im Nutzer-Objekt des Active Directory nicht korrekt konfiguriert ist. Exchange 2007 und 2010 benötigen hier einen Wert von mindestens 0.1 – ist das Attribut an dieser Stelle mit 0.0 gesetzt, sieht Exchange das Nutzerobjekt als "read only" an und gewährt keinen Zugriff über OWA. Um den Wert von msExchVersion zu überprüfen, geben Sie in der Exchange Management Shell folgendes Kommando ein:

```
Get-Mailbox {username}| format-list
  ExchangeVersion
```

Beträgt dieser Wert nicht mindestens 0.1, führen Sie diesen Befehl aus:

```
Set-Mailbox {Username}
 -ApplyMandatoryProperties
```

Diese Eingabe bewirkt, dass das Nutzer-Objekt mit dem korrekten Wert gestempelt wird und OWA und Exchange in Zukunft reibungslos zusammenarbeiten. *(ln)*

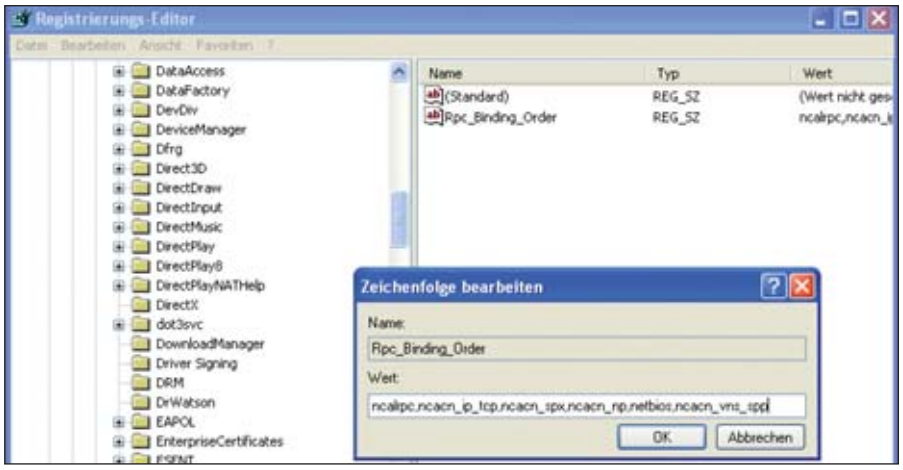
Auf dem Rechner eines Anwenders kommt es **beim Zugriff auf Exchange 2003 zu folgender Fehlermeldung**: "Der Name kann nicht aufgelöst werden. Die Verbindung mit dem Microsoft Exchange Server kann **aufgrund von Netzwerkproblemen nicht hergestellt** werden." Da der PC dieses Nutzers der einzige ist, auf dem in dieser Hinsicht Probleme auftreten, bin ich mit meinem Latein am Ende – die gängigsten Ursachen wie eine fehlerhafte DNS-Auflösung oder das Fehlen benötigter Dienste kann ich ausschließen. Haben Sie vielleicht noch einen Tipp?

Eventuell stimmen auf dem Client die Settings für das RPC-Protokoll nicht. Die Standardeinstellungen hierzu sind in dem Registry-Schlüssel "Rpc_Svr_Binding_Order" hinterlegt. Sind diese Eintragungen nicht korrekt, kann es (nicht nur bei Exchange) zu Verbindungsproblemen kommen. So überprüfen Sie die RPC-Konfiguration: Öffnen Sie die Registry mit dem Kommando *Regedit* und navigieren Sie zum Eintrag "HKLM \ Software \ Microsoft \ Exchange \ Exchange Provider". Klicken Sie im rechten Teilfenster doppelt auf "Rpc_Svr_Binding_Order". Die korrekte Zeichenfolge muss hier lauten "cacn_ip_tcp,ncacn_spx, ncacn_vns_spp". Ist diese nicht genau so hinterlegt, geben Sie sie exakt ein. Klicken Sie auf "OK" und schließen Sie den Registrierungs-Editor. Starten Sie danach alle Exchange-Dienste neu. Im Anschluss sollten keine Verbindungsschwierigkeiten mehr auftreten. *(ln)*

Auf einem älteren Mailserver haben wir noch **Exchange 2003** am Laufen. Bisher war uns nicht bewusst, dass es ein **Größenlimit für User-Mailboxen in Höhe von 16 GByte** gibt. Das Problem ist nun, dass sich das Postfach beim Überschreiten dieser Grenze gar nicht mehr öffnen lässt und der Nutzer gar keine Gelegenheit dazu hat, seine Mails zu entrümpeln. Gibt es hier irgendeinen Weg, um zumindest temporär eine Ausnahmeregelung für mehr als 16 GByte zu schaffen?

Diese Möglichkeit gibt es in der Tat, Sie können durch eine Änderung der Registry auf dem Exchange-Server die Postfachgröße auf 17 GByte ausdehnen, damit der Nutzer zumindest zum Aufräumen Zugriff erhält. Navigieren Sie dazu nach der Eingabe von *regedit* zum Schlüssel "HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ MSExchangeIS \ {Name des Exchange-Servers}\Private-{Zufälliger Hexadezimaler String}" und erstellen Sie dort einen neuen Eintrag (DWORD) mit dem Titel "Temporary DB Size Limit Extension". Klicken Sie diesen neu geschaffenen Eintrag nun doppelt und geben sie ihm den Wert "1" (Dezimal). Das "Überziehen" der Mailbox um 1 GByte ist nun möglich und der Anwender kann unwichtige Mails löschen. Außerdem sollten Sie das Postfach im Anschluss offline defragmentieren. Wie das genau geht, lesen Sie im Knowledge Base-Artikel 828070. *(ln)*

Link-Code: B5PE4



Für eine funktionierende Verbindung zu Exchange müssen auch die Einstellungen für das RPC-Protokoll in der Registry stimmen

CITRIX

Auf einigen Notebooks in unserem Unternehmen ist der aktuelle **XenClient** installiert, der meist Windows 7 in der 64-Bit-Version als Gastsystem zur Verfügung stellt. Nun würde ich gerne im XenClient eine **WLAN-Verbindung** einrichten. Diese benötigt allerdings ein Zertifikat, das mir in Form einer Datei mit der Endung *.CER vorliegt. Wie genau muss ich nun vorgehen, um das **Zertifikat innerhalb des Citrix-Hypervisors** zu installieren?

Um im XenClient ein Zertifikat zu installieren, sind lediglich die folgenden Schritte nötig: Zunächst sollten Sie das Zertifikat kopieren – dazu eignen sich Programme wie WinSCP für Windows- oder SCP für Linux/Unix-Umgebungen. Danach ist es zunächst nötig, sich mit Hilfe der Tastenkombination "Strg+Shift+T" auf dem XenClient Receiver anzumelden. Hierbei ist wichtig, Login-Daten mit Root-Rechten zu verwenden. Nun kopieren Sie das Zertifikat mit Hilfe des folgenden Kommandos von dom0 auf die virtuelle Maschine:

```
scpv4v {Zertifikat} 1.0.0.1:/root
```

Dabei ist zu beachten, mittels CD-Befehl in das Verzeichnis mit dem kopierten Zertifikat zu wechseln. Im Netzwerk-Icon des Citrix Receiver sollten Sie das Zertifikat nun problemlos auswählen können, um im Anschluss eine Verbindung mit dem WLAN herzustellen. *(Citrix/ln)*

Linux

Ich möchte auf meinen RPM-basierten Systemen **lediglich sicherheitsrelevante Updates einspielen**. Feature-Updates sind auf meinen Produktiv-Systemen nicht erwünscht. Ist dies möglich, **ohne ein zusätzliches Management-Tool** zu installieren?

Ja, das ist kein Problem. Der Paketmanager yum lässt sich über ein Plug-In entsprechend erweitern, so dass er lediglich Security-Updates installiert. Das Plug-In installieren Sie mittels

```
yum install yum-plugin-security
```

aus dem Standard-Software-Repository der meisten RPM-basierten Distributionen. Mit dem Befehl

```
yum –security list-sec
```

erhalten Sie dann eine Liste sämtlicher vorhandenen Sicherheits-Updates. Hängen Sie dem Befehl noch ein "bz" an, so sehen Sie zusätzlich auch die Bugzilla-Nummern. Wenn Sie nähere Informationen zu einem Update wünschen, so hilft das folgende Kommando weiter:

```
yum –security info-sec bz 657101
```

Hier sehen Sie dann eine Beschreibung etwa des Bugs 657101. Möchten Sie dieses Update dann einspielen, so funktioniert dies mit dem Befehl

```
yum –security update –bz 657101
```

Wollen Sie einfach alle sicherheitsrelevanten Pakete aktualisieren, so lautet der Befehl schlicht

```
yum –security update
```

(Thorsten Scherf/ln)

Die Cloud-basierte Druckerverwaltung des Printer Dashboard ermöglicht die detaillierte Fernüberwachung aller Drucker im Netz

Tools

Das **Problem ungenutzter Speicherressourcen in virtuellen Maschinen** ist in vielen Unternehmen unbekannt oder wird nicht adressiert. Die brach liegenden Speicherkapazitäten lassen sich jedoch für andere virtuelle oder physikalische Maschinen nutzen. IT-Verantwortliche, die nicht glauben, mit diesem Problem konfrontiert zu sein, könnten sich unter Umständen mit einem Tool, das den ungenutzten Speicher sichtbar macht, einer großen Überraschung gegenübergestellt sehen.

Die freie Software **vOptimizer Waste-Finder** lokalisiert überlasteten VM-Speicher und reduziert unnötige Speicherkosten. Sie erlaubt eine **effizientere Nutzung bestehender virtueller Speicherressourcen**, verbessert die VM-Performance, reduziert den Zeitaufwand für das Management virtuellen Speichers und eliminiert Risiken mangelhafter virtueller Speichermanagementpraktiken. Dazu liefert das Tool eine Übersicht über Gesamtumfang und -wert des überlasteten VM-Speichers. Darüber hinaus gewinnt die Software verschwendeten VM-Speicher zurück (Verkleinerung von VM-Disk-Dateien) für die Verwendung durch andere Applikationen. Dies erreicht der Waste-Finder durch den Scan unbenutzten Speicherplatzes zur Lokalisierung überlasteten VM-Speichers und die Vorhersage möglicher Einsparungen für VMware vCenter-Server/ESX-Hosts und alle VMs. Dies erfolgt durch zwei voll automatisierte Prozesse für die Größenanpassung und das Zurückgewinnen virtuellen Speicherplatzes. Darüber hinaus bringt das Werkzeug zwei 64k-Blockpartitionsanpassungen für die Verbesserung von VM-I/O und Speicherkostenberichte zur Erkennung von Wachstumstrends und der Projizierung von Budget-Anforderungen mit. Das Tool steht nach einer Registrierung zum freien Download bereit. *(jp)*

Link-Code: B5PE1

Das durchdachte **Management des Drucker-Fuhrparks** stellt einerseits einen Hebel für teilweise enorme Kostensenkungen in der IT dar, zum anderen kann der IT-Verantwortliche mit viel positiver Eigenwerbung bei den Anwendern rechnen, wenn Druckgeschwindigkeit und -qualität stimmen. Doch trotz weitverbreiteter Einsicht in diese Notwendigkeiten finden sich gerade in kleineren Infrastrukturen nur selten dedizierte Tools für diese Aufgaben. Doch die Cloud bewegt auch hier einiges: Eine freie Software erlaubt es IT-Verantwortlichen nun, die gesamte Druckerlandschaft per Webbrowser zu überblicken. So sollen zu niedrige Tonerstände, Papierstaus oder andere Druckprobleme und Missstände der Vergangenheit angehören.

Das frei als Software as a Service im Web verfügbare **Printer Dashboard** von thinprint steht als Drucker-Monitoring-Tool dem Administrator hilfreich zur Seite. Zur Nutzung ist lediglich eine Registrierung zur Erzeugung des notwendigen Accounts Voraussetzung. Anschließend muss der IT-Verantwortliche einen Agenten herunterladen und einrichten und schon erfolgt als erster Schritt eine Inventarisierung des Drucker-Bestandes. Dabei erlaubt es Printer Dashboard, unabhängig von Druckerhersteller oder -modell die Drucker bequem von jedem beliebigen Ort zu kontrollieren. Das Monitoring umfasst dabei selbstverständlich technische Aspekte des Druckbetriebes und meldet geöffnetes Gehäuse genauso wie Drucker im Offline-Modus oder Papierstaus. Gleichzeitig beobachtet die Software Verbrauchsmaterialien wie Papier und Toner und ermöglicht die direkte Nachbestellung. Und dank der integrierten Buchführung kennt der Administrator Papier- und Tonerverbrauch eines jeden Druckers und kann so die Kosten für jedes Gerät kalkulieren. *(jp)*

Link-Code: B4PE2

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

Drucken im Netzwerk und in VDI-Umgebungen

Um die Ecke gedruckt

von Herbert Hemke

Sowohl das Drucken selbst als auch die Administration der Druckumgebung sind im Laufe der Jahre trotz aller Anstrengungen der Anbieter von Server-based Computing-Architekturen ein Flaschenhals geblieben. In diesem Beitrag gehen wir unter anderem auf das Drucken in heterogenen Umgebungen, die Behebung von typischen Druckfehlern sowie den Einsatz von universellen Druckertreibern ein. Außerdem beleuchten wir, wie sich mit Geräten ohne eigenes Drucksystem – etwa dem iPad – überhaupt drucken lässt und ob das Drucken vielleicht sogar komplett in der Cloud stattfinden kann.

Das in die Jahre gekommene Server-based Computing (SBC) ist so aktuell wie nie zuvor – doch es hat sich grundlegend gewandelt: Während die meisten IT-Verantwortlichen früher bei SBC meist an eine Citrix-Farm mit Fat- und Thin Clients dachten, geht es heute oft um gemischte Umgebungen mit Microsoft-Terminaldiensten und virtualisierten Desktops. Neben Citrix und Microsoft spielen VMware, Oracle, Red Hat und andere Anbieter auf der Klaviatur der zentralisierten und virtuellen Desktop-Infrastrukturen (VDIs). Als Endgeräte kommen neben PCs und Terminals auch Tablets und Smartphones zum Einsatz (siehe Bild 1).

Ein wichtiger Faktor für die Zufriedenheit der Anwender sowie die Akzeptanz der Migration auf VDI ist die Geschwindigkeit beim Drucken. Diese wird ganz entscheidend von der zur Verfügung stehenden Bandbreite beeinflusst, denn Druckdaten erreichen schnell das zehnfache Volumen des Ursprungsdokuments. Mögliche Maßnahmen – gerade im Zusammenhang mit verteilten Unternehmensstrukturen – sind neben der Bereitstellung teurer Bandbreite die Komprimierung der Druckdaten, eine Bandbreitenbegrenzung oder der Einsatz von Quality of Service-Routern.

Die Treiberverwaltung

Einen wichtigen Themenkomplex bildet die gesamte Problematik der Treiberverwaltung. Hier hat sich einiges zum Guten gewendet. So können ab Windows Server 2008 R2 Treiber nicht mehr so einfach installiert werden, wenn sie nicht zuvor von Microsoft signiert wurden. Die Möglichkeit, kritische Treiber zu isolieren, erspart den Admins viele schmerzhafte Stunden der Fehlersuche (siehe "Einzelhaft für üble Treiber" in IT-Administrator 09/2009). Weiterhin bietet Windows die Möglichkeit, mit einem Update die Treiberliste aktuell zu halten. Bei Windows Server 2008 können Sie so die Zahl der nutzbaren Druckertreiber von circa 2.000 auf rund 5.000 steigern.

Soll der Vorteil einer VDI-Umgebung mit vereinheitlichten Images für einzelne Nutzergruppen und damit einhergehend die Reduzierung des Verwaltungsaufwandes zum Tragen kommen, empfiehlt sich ohnehin der Einsatz universeller Druckertreiber. Auf diese Weise lassen sich Druckertreiberkonflikte und damit Spooler- oder Server-Abstürze vermeiden sowie Storage-Ressourcen schonen.

Die UPDs (Universal Printer Driver) der Druckerhersteller setzen einen homogenen Drucker-Park eines einzigen Herstellers voraus. Die Plattform-UPDs von Microsoft, Citrix und VMware benötigen Windows und sind somit für das Drucken über Thin Clients oder direkt auf Netzwerkdruckern ungeeignet. Wenn nicht komplett auf UPDs gesetzt werden kann, stellen 64-Bit-Systeme eine Schwierigkeit dar, wenn sich noch ältere Drucker im Bestand finden. Eine Lösung bietet etwa ThinPrint V-Layer, der alle Druckertreiber auf einem Druckserver zentralisiert und ansonsten nur über einen virtuellen Treiber druckt.

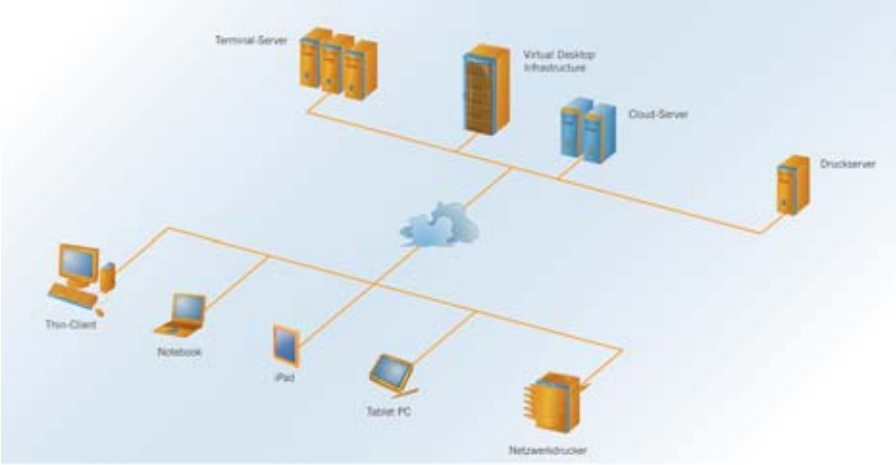


Bild 1: Heutige Druckumgebungen zeichnen sich durch eine Vielzahl an Endgeräten und Kommunikationswegen aus

Printserver in VDI-Umgebungen

Werden universelle Treiber von Citrix, Microsoft, VMware oder ThinPrint eingesetzt, dann stellt sich die Frage, wo die Übersetzung in die Sprache des Originaldruckertreibers stattfindet beziehungsweise wo die Herstellerdruckertreiber installiert und verwaltet werden. Die meisten Thin Clients mit Ausnahme von Embedded XP und Windows embedded können Druckaufträge nicht verarbeiten. Für die Übersetzung kommen also entweder PCs oder ein dedizierter Druckserver in Frage. Im Fall des PCs müssen auf jedem einzelnen Desktop die Druckertreiber installiert werden. Erste Wahl ist hier also in jedem Fall der Einsatz eines dedizierten Druckservers, der einfach und übersichtlich zu administrieren ist und mit dem sich die Netzwerkdrucker komfortabel adressieren lassen.

Die in die Herstellerlösungen von Citrix, Microsoft und VMware bereits integrierten Lösungen bieten im Zusammenspiel mit Printservern lediglich eine Basisunterstützung mit automatisch erzeugten Clientdruckern. Diese Konstellation ist tauglich für eher kleinere Unternehmen, die Windows-PCs als Clients nutzen. In komplexeren Architekturen ist aber meist der Einsatz einer Zusatzlösung anzuraten. Ebenfalls nicht mit Bordmitteln zu bewerkstelligen ist das komplexe Thema Drucken in gemischten Umgebungen.

Universal Printer Driver im Überblick

Die meisten Hersteller bieten für ihre Netzwerkdruckerpalette universelle Treiber an; nicht alle sind jedoch für den Einsatz in SBC-Umgebungen geeignet. Hier ein Überblick:

- Canon Universal Printer Driver
- Dell Open Print Driver
- Driver for Universal Print (Ricoh)
- HP Universal Printing
- Kyocera Classic Driver
- Lexmark Universal Printer Driver
- Samsung Universal Print Driver
- Universal Print Driver (Konica Minolta)
- Universal Printer Driver for BR-Script (Brother)
- Xerox Global Print Driver

Alle diese Treiber werden jeweils in einer PostScript-Version geliefert (PS- beziehungsweise BR-Script). Fast alle Hersteller stellen auch PCL-Versionen zur Verfügung (PCL5 und/oder PCL6). Alle Laserdrucker unterstützen PCL, viele zusätzlich PostScript. Für professionelles Grafikdesign geht es nicht ohne PostScript. Für Office-Anwendungen genügt PCL, zumal die Treiberkonfiguration hier oft einfacher ist. Sharp verwendet für seinen Universaltreiber das auf PostScript basierende PDF-Format. Tintenstrahl- und Nadeldrucker bieten aus Kostengründen häufig noch keine PCL- oder PostScript-Unterstützung, sondern beschränken sich auf den sogenannten Epson-Standard (ESC/P = Epson Standard Code for Printers).

Fehlerhafte Ausdrucke vermeiden

Ein Nachteil von UPDs sollte nicht unerwähnt bleiben: Bei besonderen Anforderungen, wie einem Dokument mit Quer- und Hochformat oder Halbtransparenzen in Grafiken, versagen gerade UPDs neueren Datums den Dienst. Hier punkten die Treiber mit längerer Marktreife.

Beim Drucken kann es zudem vorkommen, dass die Nutzer zwar die richtige Schrift in ihrer Anwendung ausgewählt haben, auf dem Ausdruck aber eine andere Schrift erscheint beziehungsweise falsche oder fehlende Zeichen. Eventuell stehen Zeichen auch zu weit auseinander, stoßen aneinander oder überlappen sich. Ursache hierfür ist oft, dass die Druckaufträge nicht dort gerendert werden, wo sie entstehen. Die folgenden Tipps helfen, Schriftenprobleme zu vermeiden:

Alle Schriften auf dem Druckserver installieren

Installieren Sie alle Schriften, die Ihre Nutzer verwenden, und zwar nicht nur dort, wo deren Anwendungen laufen (also auf Terminal-Servern, virtuellen Desktops oder Workstations), sondern auf allen beteiligten Druckservern. Installieren Sie immer alle Schnitte einer Schrift. Für Arial sind das beispielsweise die Normalschrift Arial (Regular) sowie die Schnitte Arial kursiv, Arial fett und Arial fett kursiv.

Schriften in Dokumente einbetten

Wollen Ihre Nutzer auch solche Dokumente drucken, die nicht in Ihrem Unternehmen bearbeitet wurden, dann können diese Dokumente unter Umständen lediglich die Information enthalten, welche Schrift in der jeweiligen Anwendung verwendet wurde. Die Schrift selbst wurde aber eventuell gar nicht mitgeliefert – zum Beispiel durch Einbettung in das Dokument. Ist die Schrift eines firmenfremden Dokumentes auf demjenigen Druckserver installiert, wo gerendert wird, dann gibt es in der Regel keine Probleme.

Umgekehrt ist es möglich, verwendete Schriften in die Datei einzubetten, die an andere Firmen gesendet werden soll. Sie können bei PDF-Dateien im Adobe Reader leicht kontrollieren, ob die Schrifteinbettung erfolgreich war. Dazu wählen Sie "Dateieigenschaften Schriften" (in englischen Versionen "Fileproperties Fonts"). Im in Bild 2 dargestellten Beispiel wurde zwar die Schrift Arial im Ursprungsdokument verwendet, diese ist aber nicht in das PDF eingebettet. Von der Schrift Calibri sind nur die wirklich im Dokument verwendeten Zeichen eingebettet (Embedded Subset), und von der Schrift HelveticaNeue-ThinCond sind alle Zeichen eingebettet (Embedded).

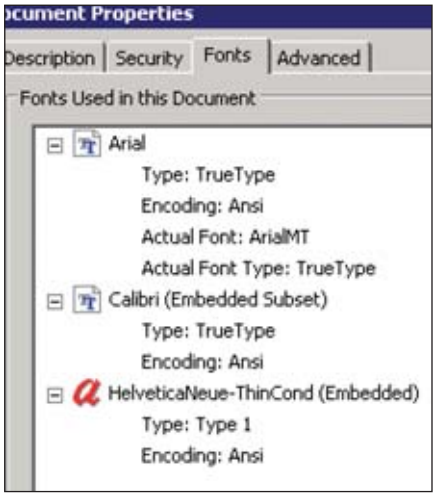


Bild 2: Mit dem Adobe Reader lässt sich leicht überprüfen, ob die Schrifteneinbettung erfolgreich war

Die Schrifteinbettung steuern können Sie beispielsweise mit dem Acrobat Distiller. Aber nicht jeder kann auf das kostspielige Flaggschiff von Adobe zurückgreifen. Unkompliziert, weil die Schrifteinbettung nicht eingestellt werden muss, sind dagegen das freie Tool PDF24 Creator sowie das ebenfalls kostenlose Microsoft-Office-Plug-In "Speichern unter PDF".

Automatische Schriftenersetzung ausschalten

Als die Ressourcen von Druckern noch eingeschränkt waren, gab es eine Funktion, die Original-Schriften nicht an den Drucker sendet, sondern im Drucker (oder vorher mit dem Treiber) durch eine mit der Firmware mitgelieferten Schrift ersetzt. So wird dadurch oft statt Times New Roman die Schrift Times gedruckt und statt Arial die etwas zierlichere Helvetica.

Obwohl die Schriften nicht völlig identisch sind, fällt die Ersetzung meist gar nicht auf. Allerdings stimmen spätestens seit Einführung der Unicode-Schriften mit Windows 2000 die Zeichensätze nicht mehr überein (Unicode-Schriften erkennt man am großen "O" im Schrift-Icon anstelle des Doppel-T). Dadurch gehen eventuell Sonderzeichen verloren. Außerdem bringen neue Windows-Versionen immer völlig neue Schriften mit.

Deshalb sollten Sie die automatische Schriftenersetzung beim Drucken in Netzwerken grundsätzlich abschalten. Diese Funktion wird allerdings von vielen Herstellern unterschiedlich bezeichnet. Häufig heißt sie "Durch Druckerschriftart ersetzen". Deaktivieren Sie diese Option beziehungsweise wählen Sie stattdessen "Als Softfont in den Drucker laden".

Professionell in VDIs drucken

Wer von VDI-Umgebungen spricht, geht häufig vom virtuellen Windows-Desktop auf der einen Seite und einem zweiten Windows-Desktopsystem auf der anderen Seite aus. Die Realität gestaltet sich aber meist vielfältiger: In der Zentrale werden in großer Anzahl Windows 7 x64-Desktops bereitgestellt, die von einem "Golden Image" gezogen werden. Einige unternehmensweit genutzte Anwendungen laufen auf Remote-Desktop- beziehungsweise XenApp-Servern und werden als Anwendung auf den virtuellen Desktops veröffentlicht. Häufig ist auch ein ERP-System angebunden. Die Druckerlandschaft ist heterogen, es sind also Drucker von unterschiedlichen Herstellern, neue Multifunktionsgeräte, Desktopdrucker und alte Schwarz-Weiß-Laserdrucker im Einsatz.

Der Benutzer greift mit unterschiedlichen Systemen auf die Anwendungen und Dokumente zu. So steht in seinem Büro vielleicht ein Thin Client, mit dem er ausschließlich auf Netzwerkdruckern ausdruckt. Zuhause dagegen nutzt er seinen PC mit lokalem Drucker und unterwegs möchte er in Hotels oder Firmenniederlassungen von seinem Laptop aus drucken. Seit kurzem ist er zudem stolzer Besitzer eines iPads und startet die ersten Versuche, das Notebook auf Reisen durch sein Tablet zu ersetzen.

Eine hierzu passende effektive Druckarchitektur könnte wie folgt aussehen: Innerhalb der Firma, wo er Thin Clients und Netzwerkdrucker nutzt, ist es am sinnvollsten, einen zentralen Druckserver einzusetzen, auf dem die Netzwerkdrucker eingerichtet sind. Sie werden dann über Policies oder Skripte maschinenbasiert in die jeweilige Session gemappt. Die Druckertreiber werden dabei von dem Druckserver über Point and Print auf die Desktops beziehungsweise Remote-Desktop-Server gezogen. Vorteil hierbei ist, dass am Clientsystem kein Konfigurationsaufwand entsteht und keine dezentralen Druckserver benötigt werden. Der Nachteil, besonders auf Remote Desktop Sessions: die Ansammlung verschiedenster Druckertreiber.

Heimarbeitsplätze sind am besten mit automatisch erzeugten Clientdruckern in den Sessions bedient. Hier wird der Drucker erkannt, der zu Hause am PC installiert ist, und auf dem virtuellen Desktop auf Basis eines virtuellen Druckertreibers erstellt. Das Rendern des Druckjobs erfolgt auf dem heimischen Windows-PC. Der Vorteil für Administratoren: Sie müssen sich nicht um die vielen verschiedenen Drucker der Mitarbeiter zu Hause kümmern und keine Hersteller-Treiber auf den zentralen Desktop-Systemen verwalten. Zu beachten ist, dass alle Drucker in allen Sessions richtig angezeigt werden, auch in der oben beschriebenen Session-in-Session-Umgebung. In der zweiten Session vom virtuellen Desktop auf einen RDS-Server muss die Druckerinformation vom Ursprungsclient, also dem Heimanwender, ausgelesen werden.

Mit einem Laptop unterwegs zu drucken, stellt schon eine Herausforderung dar, besonders, wenn der Benutzer aus Sicherheitsgründen vernünftigerweise nicht über administrative Rechte verfügt. So würde es dem Laptop-Besitzer ohne die entsprechenden Installationsrechte noch nicht einmal zum Ausdruck verhelfen, wenn neben dem Hoteldrucker eine CD mit den Treibern liegen würde. Noch schwieriger wird es für iPad-Nutzer, denn ihr System ist nicht in der Lage, zu drucken oder einen lokalen Drucker einzurichten. Zwar bietet Apple eine Lösung namens AirPrint an, doch wird der Reisende kaum im Hotel zufälligerweise auf einen geeigneten Drucker treffen, der genau diese Lösung unterstützt. Und aus einer Session heraus ist das Drucken schlichtweg unmöglich.

Druckaufträge aus der Wolke

Um iPads oder Smartphones mit einer Druckfunktion auszustatten, muss untersucht werden, wie mobile Geräte drucken, die kein eigenes Drucksystem haben. Manche Endgeräte haben zwar eine Druckmöglichkeit, aber gerade unterwegs wird der zu druckende Dateityp oder der

Unterschiede beim Drucken im LAN und in VDIs		
	VDI	**LAN**
Bereitstellen von Druckern	Druckerinformationen werden vom Client eingelesen und Drucker lokal auf den VDs installiert.	Netzwerkdrucker werden von einem Druckserver gemappt, lokale per USB angeschlossen.
Treiberinstallation	Einsatz von universellen Druckertreibern oder virtuellen Druckern, um die Treiberanzahl auf den Images möglichst klein zu halten.	Druckertreiber werden auf allen Desktops installiert, automatisch per Point-and-Print oder durch gezielte Verteilung.
Druckweg	Oft lange Wege: Von den zentralen VDs zum am Client eingerichteten Drucker oder über zentralen Druckserver an Netzwerkdrucker.	Meist kurze Wege: Direkt zum lokalen Drucker oder vom Desktop über Druckserver zum Netzwerkdrucker.
Clients	Neben klassischen Desktops Vielzahl an Clients von Zero Clients, Thin Clients bis hin zu Tablets. All diese nicht druckfähigen Geräte werden von VDI-Lösungen nicht oder nur rudimentär unterstützt.	Neben klassischen Desktop-Clients halten vermehrt Tablet-PCs Einzug ins Unternehmen. Drucken kann hier nur über spezielle Lösungen erfolgen.
Anwendungsbereitstellung	Anwendungen laufen auf entfernten Systemen, gegebenenfalls verteilt auf unterschiedlichen Systemen (VDs / Terminalserver).	Anwendungen laufen lokal.

gewünschte Drucker meistens nicht unterstützt. Eine Möglichkeit, um alles und überallhin drucken zu können, ist das Dazwischenschalten eines Druckservers. Auf diesem sind klassischerweise die Treiber installiert und dort wird der Druckauftrag gerendert.

Die Drucker müssen natürlich bekannt und vom Printserver erreichbar sein. Spontan zu drucken auf einem Drucker, der zufällig im WLAN auftaucht, ist so nicht möglich. Hierfür wird eine Cloud-Printing-Lösung benötigt: Der Anwender sendet die Druckdaten aus einer Anwendung heraus via HTTPs zu einem Cloud Printserver, der den Druckauftrag generiert und dann zum Client sendet, von wo aus er per WLAN oder Bluetooth zu einem beliebigen Drucker geschickt werden kann. Cloud Printing steht noch ganz am Anfang. Einige Lösungen werden jedoch bereits angeboten oder stehen kurz davor: Bei der Cloud-Printing-Lösung von HP – HP ePrint – erhalten alle Druckermodelle des Herstellers eine eigene Mailadresse, über die sie ihre Druckaufträge empfangen. Das hat den Vorteil, dass jeder, der die E-Mailadresse eines Druckers kennt, seine Jobs an diesen Drucker senden kann. Nachteil: Es werden nur sehr wenige Druckermodelle unterstützt. Google hat für die Anwendungen seines Chrome OS die Spezifikationen offengelegt, so dass auch andere Systeme Google Cloud Print nutzen können, etwa Office-Anwendungen für Google-Android. Als Zieldrucker sollen in einem ersten Schritt ebenfalls HP-Drucker mit E-Mailadresse dienen. Mit der Lösung Cortado Workplace fragt das Endgerät beim Drucken den Druckertyp über Bluetooth oder WLAN ab. Dieses wird dem Cloud-Dienst übermittelt, der den passenden Treiber auswählt. Gedruckt werden kann dann auf nahezu beliebigen Druckern, die in einem WLAN installiert oder die per Bluetooth adressierbar sind. Die Zieldrucker benötigen keine E-Mailadresse und müssen nicht mit dem Internet verbunden sein. Unterstützt werden momentan etwa 10.000 verschiedene Druckermodelle. *(ln)*

Herbert Hemke ist Technischer Redakteur und Consultant bei der ThinPrint AG.

Einstieg in das Cloud Computing

Himmelfahrtskommando

von René Büst

Quelle: Fixelio.de

Es besteht kaum mehr Zweifel daran, dass Cloud Computing Einzug in die Informationstechnologie der Unternehmen hält. Durch die sich ständig erweiternde Palette an Produkten und Dienstleistungen zahlreicher Anbieter wurde der anfängliche Hype von konkreten, nützlichen Angeboten abgelöst. Cloud Computing repräsentiert ein Servicemodell, bei dem auf Ressourcen wie Rechenleistung, Speicherplatz, Applikationen und andere Arten von Services on Demand zugegriffen wird. Auf Basis des Pay as you Go-Modells werden dabei nur die Ressourcen berechnet, die auch tatsächlich genutzt werden. Dieser Beitrag zeigt Wege auf, wie Unternehmen sich dieser Technologie sinnvoll annähern.

Die IT-Abteilungen der Unternehmen werden einen Wandel erfahren: Sie kümmern sich zukünftig nicht mehr darum, Systeme aufzubauen, zu konfigurieren und zu warten, sondern sie werden IT-Services unterschiedlicher Anbieter für die Bedürfnisse des Unternehmens identifizieren und miteinander verknüpfen. Einige Services werden auch weiterhin von den IT-Abteilungen über eine Private Cloud bereitgestellt, aber im Laufe der Zeit werden immer mehr Dienste von externen Anbietern angebunden.

Ein gutes Beispiel hierfür ist Cloud Storage. Eine stetig wachsende Herausforderung für Unternehmen besteht in der immensen Zunahme von zu speichernden Daten. Das führt neben den steigenden Ausgaben für Festplatten und Storagesysteme zu komplexeren und kostspieligeren Aufgaben für die Verwaltung und Wartung der gesamten IT-Infrastruktur. Die Nutzung eines Cloud Storage-Service zum Speichern und Backup der Daten ist hier ein Ansatz, der sehr kostengünstig umgesetzt werden kann. Ein weiterer Vorteil besteht darin, dass auf die Daten zu jeder Zeit und von jedem Ort zugegriffen werden kann.

Der richtige Einstieg

Cloud Computing bietet eine Vielzahl unterschiedlicher Einsatzgebiete und Einstiegsmöglichkeiten. Dazu kommen viele weitere Handlungsszenarien. An dieser Stelle gilt es aber, auf die individuellen Bedürfnisse zu schauen und zunächst die eigene Situation zu analysieren und auf Basis von Erfahrungswerten Rückschlüsse auf das eigene Unternehmen zu ziehen.

Eine bewährte Strategie kann, je nach Größe des Unternehmens, sein, zunächst eine (kleine) Private Cloud zu implementieren und diese schrittweise auf Basis der eigenen Erkenntnisse weiter den Bedürfnissen entsprechend auszubauen. Im weiteren Verlauf können dann sukzessive Dienste von Public Cloud-Anbietern, wie etwa Cloud Storage, angebunden werden.

Um den Sprung zu einem Public Cloud-Anbieter jedoch erfolgreich zu schaffen, müssen Unternehmen den Anbieter einer genauen Evaluierungsphase unterziehen, während der folgende Fragen beantwortet werden sollten:

- Ist meine aktuelle IT-Infrastruktur zu der des Anbieters kompatibel?
- Lässt sich eine Verbindung und Integration auf eine einfache, zuverlässige und sichere Art und Weise vornehmen?
- Verfügt der Anbieter über ausreichend Expertise beim Cloud Computing?
- Kann ich sicher sein, dass der Anbieter über ein ganzheitliches Risikomanagement verfügt?
- Sind die Verträge transparent?
- Entstehen Anfangsinvestitionen?
- Wie skalierbar ist die Infrastruktur des Anbieters?

Cloud Storage als erster Schritt

Der beste und vermeintlich einfachste Einstiegspunkt in das Cloud Computing ist die Nutzung eines Cloud Storage-Service. Cloud Storage hat in erster Linie den Vorteil, dass der genutzte Speicherplatz automatisch mit den Bedürfnissen mitwächst. Werden heute 10 GByte, morgen aber 100 GByte benötigt, stellt das kein Problem dar und es sind dafür keine eigenen Investitionen in neue Speichersysteme fällig.

Weitere Gründe, die für Cloud Storage als den Einstieg in das Cloud Computing sprechen, sind:

- Einfache Einrichtung und Anbindung: Stellt der Anbieter eine offene und gut

dokumentierte API bereit, kann Cloud Storage auf eine schnelle und einfache Art und Weise an die bestehende Infrastruktur angebunden werden.

- Backend-Erweiterung: Cloud Storage lässt sich dazu nutzen, die bestehende Speicherumgebung kostengünstig zu erweitern. Zudem können Unternehmen im Laufe der Zeit die Daten, die sich auf dem eigenen lokalen Speicher befinden, ebenfalls auf den Cloud Storage übertragen und somit eine flüssige Migration der Daten durchführen, um das eigene Speichersystem letztendlich abzulösen.
- Einfache Trennung zwischen sensiblen und öffentlichen Daten: Wollen Unternehmen aus der eigenen Infrastruktur heraus Daten der Öffentlichkeit bereitstellen, führt das zu weiteren Investitionen in Schutzsysteme, wie etwa eine DMZ. Viele Cloud Storage-Services haben Funktionen zur Trennung von privaten, sensiblen Daten und Daten, die der Öffentlichkeit zugänglich sein dürfen, bereits integriert.
- Anbindung an weitere Cloud Services: Cloud Storage kann dazu genutzt werden, weitere Cloud Services wie etwa Software as a Service (SaaS) oder Platform as a Service (PaaS) zu kombinieren, indem er als zentraler Speicherplatz dient, auf den alle Services auf Basis einer gemeinsamen und einheitlichen Datenbasis zugreifen.

Cloud Backup

Aufgrund der in der Regel hohen Investitionen in eigene Backup-Lösungen meiden vor allem kleine und mittelständische Unternehmen den Weg einer ganzheitlichen Backup-Strategie und setzen maximal auf gewöhnliche voll-, inkrementelle oder differenzielle Backups. In diesen Fällen findet zwar eine Sicherung in regelmäßigen Abständen statt, aber der Schutz der erstellten Backups bezüglich des physikalischen Zugriffs vor Dritten oder vor höherer Gewalt wie Feuer oder Hochwasser ist damit nicht gewährt.

Vor allem der zeitliche Verlust und der aktuelle Versionsstand sind hier nicht zu unterschätzen. Durch den Einsatz von Cloud Storage wird der Status der Daten hochverfügbar, da sich die Daten nicht mehr zentral an einem Ort, sondern verteilt über mehrere Standorte hinweg befinden. Zudem bietet Cloud Storage die Möglichkeit eines Echtzeit-Backups, womit die Daten zur Laufzeit ständig synchronisiert sind. Hier besteht der Vorteil darin, dass eine Änderung an einer Datei automatisch erkannt und mit dem Cloud Storage abgeglichen wird, wodurch mit den Änderungen an dieser Datei sofort ein Backup stattfindet.

Cloud Archivierung

Mussten früher Unmengen an Papier über viele Jahre hinweg archiviert werden, stehen IT-Manager in den letzten Jahren der Herausforderung gegenüber, die Archivierung durch IT-Systeme übernehmen zu lassen. Das größte Nadelöhr besteht in der Menge an verfügbaren Speicherplatz, der dafür benötigt wird. Trotz der in den vergangenen Jahren drastisch gesunkenen Preise für Festplattenspeicher geht es bei der Archivierung um deutlich mehr als die reine Datenspeicherung, wie etwa Compliance-Gesichtspunkte, langfristige Sicherung und Aufbewahrung. Daher gilt es vor allem für KMUs, einen Cloud Storage-

Anbieter zu identifizieren, der den Ansprüchen der jeweiligen Branche gerecht wird und der neben der Speicherung großer Datenmengen ebenfalls über ausreichend Expertise im Bereich der Datenarchivierung verfügt.

Worauf es beim Cloud Computing ankommt

Die Entscheidungsgrundlagen für ein Cloud Computing-Angebot sind individueller Natur. Zunächst gilt es, die eigenen Bedürfnisse zu identifizieren, um danach das für sich passende Angebot herauszufiltern und zu erkennen, wo Cloud Computing für das Unternehmen einen entscheidenden Vorteil bietet und wo nicht.

Grundsätzlich ist ein hybrider Ansatz, bestehend aus Private Cloud, Public Cloud, SaaS und Cloud Storage, die Strategie, die zu Beginn verfolgt werden sollte. Wie ein Ansatz im Einzelnen aussieht, ist jedoch von Unternehmen zu Unternehmen unterschiedlich und von dessen jeweiliger Größe abhängig. Große Unternehmen legen speziell auf die Bereiche Datenschutz, Datensicherheit und Risiko ein besonderes Augenmerk. Dazu gehört ebenfalls die Frage, was mit den Daten passiert, wenn das Angebot nicht mehr genutzt wird, sowie der Grad der Kontrolle. Im Falle der hybriden Lösung ist der Integrationsgrad zwischen der Cloud des Anbieters und den unternehmenseigenen Technologien von besonderem Interesse.

Drei Arten von Clouds

Private Cloud

Bei einer Private Cloud betreiben Unternehmen ihre eigenen Rechenzentren beziehungsweise haben eigene Server angemietet, nutzen die Dienste jedoch nur für ihre eigenen geschäftlichen Zwecke innerhalb ihrer privaten Netze und stellen diese der Allgemeinheit nicht zur Verfügung.

Public Cloud

In einer Public Cloud werden Dienste wie Rechenleistung oder Speicherplatz einer breiten Masse zur Verfügung gestellt. Die Aufgaben, die von einem Unternehmen in der Private Cloud verwaltet werden, übernimmt in der Public Cloud dann ein Drittanbieter.

Hybrid Cloud

Eine Hybrid Cloud repräsentiert eine Mischung aus einer Private und einer Public Cloud. Dabei nutzen Unternehmen ihre eigene Private Cloud oder ein Rechenzentrum und binden bei Bedarf weitere Dienste aus einer Public Cloud von externen Anbietern ein.

Was alle grundlegend gemein haben, ist der Wunsch nach Skalierbarkeit, Flexibilität und Reduzierung des finanziellen Aufwands, wobei ein großes Unternehmen deutlich schneller skalieren können muss als ein KMU. Letztere achten mehr auf einen zuverlässigen Support und einen Anbieter, der sich im besten Fall in der Nähe befindet und schnell erreichbar ist.

Bleiben wir aber bei unserem Beispiel aus dem Bereich Cloud Storage. Bei der Auswahl des Anbieters gilt es viele Fragen detailliert zu erläutern und zu klären. Der Cloud Storage-Service muss zunächst die typischen Eigenschaften des Cloud Computing erfüllen: hohe Verfügbarkeit, Zuverlässigkeit und Skalierbarkeit. Des Weiteren muss der Cloud Storage-Anbieter seinen Kunden eine (theoretisch) unendlich große Menge an Speicherplatz zur Verfügung stellen, die sich an die wechselnden Anforderungen des Kunden automatisch anpasst. Die Abrechnung darf hierbei nur auf Basis der tatsächlich genutzten Mengen an Speicherplatz und Datentransfer erfolgen.

Bereits an dieser Stelle sollten IT-Verantwortliche betrachten, ob die Nutzung eines Cloud Storage tatsächlich zu Kosteneinsparungen führt. Weiterhin gilt es darauf zu achten, dass der Cloud Storage über eine offene, aber vor allem gut dokumentierte API verfügt, die kompatibel zu bereits bekannten APIs am Markt ist, um den Service von außen zuverlässig ansprechen zu können. Nur so kann eine nahtlose Integration des Cloud Storage in die eigene Infrastruktur ohne Probleme erfolgen. In diesem Zusammenhang ist es ebenfalls interessant zu überprüfen, ob für das Cloud Storage-Angebot eine Dateiverwaltung existiert, mit der etwa die Rechte für einzelne Dateien auf Benutzer- und Gruppenebene vergeben werden können und somit der Zugriff auf Dateiebene gesteuert wird.

Weiterhin ist die Verfügbarkeit des gesamten Systems des Anbieters von hoher Relevanz. Cloud Storage muss eine so hohe Verfügbarkeit aufweisen, dass auf die darin gespeicherten Daten zu jeder Zeit und von jedem Ort aus plattformunabhängig zugegriffen werden kann. In diesem Zusammenhang gilt es auch die Service Level Agreements des Cloud Storage-Anbieters zu überprüfen. Bietet er nur Standard-SLAs für jeden seiner Kunden oder geht er individuell auf die Bedürfnisse der Kunden ein und erstellt ein passendes SLA zusammen mit dem Kunden? Durch ein SLA nicht beeinflussbar, aber dennoch besonders wichtig bei Cloud Storage ist die Latenz. Die Latenz ist die Reaktionszeit, die der Cloud Storage benötigt, um auf die Anfrage durch einen Benutzer zu antworten. Hier sollte darauf geachtet werden, dass der Anbieter über eine gute, stabile und schnelle Internetanbindung verfügt.

Zu guter Letzt sollte die Betrachtung auf die derzeit am häufigsten diskutierten Eigenschaften eines Cloud Storage-Dienstes, den Datenschutz und die Datensicherheit, fallen. Der Dienst muss lokale und globale rechtliche Rahmenbedingungen und Beschränkungen erfüllen. In Deutschland wäre das zum Beispiel die vollständige Einhaltung und Gewährleistung des Bundesdatenschutzgesetzes (BDSG).

Fazit

In Zukunft wird die Bedeutung abnehmen, zu wissen, wie die im Unternehmen eingesetzte IT im Detail funktioniert. Es wird vielmehr darum gehen, zu wissen, welche IT-Ressourcen einem Unternehmen zur Verfügung stehen und wie diese gewinnbringend zu verwenden sind.

Um jedoch nicht direkt allzu großen Herausforderungen gegenüberzustehen, bietet es sich an, den Einstieg zunächst einfach zu gestalten und die Cloud Schritt für Schritt zu adaptieren. In dieser Phase werden ausreichend Erfahrungen gesammelt, die aufzeigen, wie die eigenen Bedürfnisse aussehen und worauf es für das Unternehmen selbst bei einem Cloud-Angebot ankommt. *(jp)*

René Büst betreibt als IT-Consultant den Blog CloudUser.org und hat diesen Beitrag für ScaleUp Technologies erstellt. ScaleUp (www.scaleupcloud.com) entwickelt und betreibt eine Cloud Management-Plattform, die es Unternehmen ermöglicht, eine Public, Private oder Hybrid Cloud bereitzustellen.

Juristische Vorgaben zur E-Mailarchivierung (2)

Problemfall Privatmails

von Patrick Prestel und Max-Lion Keller

Rund um das Thema E-Mailarchivierung haben Unternehmen zahlreiche Gesetze einzuhalten. Insbesondere entstehen erhebliche Rechtsprobleme, wenn Unternehmen ihren Mitarbeitern die private Nutzung der geschäftlichen E-Mailadresse gestatten. Im ersten Teil unseres Beitrags wurden die Anforderungen an die E-Mailarchivierung und der Konflikt mit dem Fernmeldegeheimnis aufgezeigt. Im zweiten Teil stellen wir zunächst den Konflikt mit dem Datenschutzrecht dar. Anschließend gehen wir darauf ein, wie IT-Verantwortliche die Konflikte mit dem Fernmeldegeheimnis und dem Datenschutz lösen können.

Beginnen wollen wir unseren Beitrag mit dem Datenschutz-Konflikt bei einem Verbot der privaten Nutzung. Das TKG gilt im Falle des Verbots der privaten Nutzung zwar nicht, da der Arbeitgeber kein Dienstanbieter im Sinne des TKG ist. Aber dann gilt aber das Bundesdatenschutzgesetz (BDSG) hinsichtlich der E-Mails. Gemäß § 4 BDSG dürfen personenbezogene Daten nur erhoben oder genutzt werden, wenn dies durch den Betroffenen oder durch Gesetz oder eine andere Rechtsvorschrift gestattet ist. Diese müsste nach § 4a BDSG schriftlich und freiwillig abgegeben werden. Neben dem Aufwand, die Einwilligung einzuholen, besteht die praktische Gefahr, dass einzelne Mitarbeiter die Einwilligung nicht erteilen, so dass keine umfassende und automatisierte Archivierung möglich ist. Zudem ist die Einwilligung jederzeit widerrufbar.

Für die E-Mailarchivierung kommt innerhalb eines Betriebes § 32 BDSG als gesetzliche Rechtfertigung zur Anwendung. Dieser erlaubt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Erforderlich ist die Verwendung personenbezogener Daten dann, wenn keine objektiv zumutbare Alternative existiert. Die Erforderlichkeit ist anzunehmen, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht oder nicht angemessen gewahrt werden können. Dabei ist bei der Archivierung zu berücksichtigen, dass sich für den Arbeitgeber aus den zahlreichen gesetzlichen Vorschriften nicht nur ein Interesse, sondern eine Pflicht zur Archivierung ergibt. Deshalb kann die Erforderlichkeit im Sinne des § 32 BDSG unseres Erachtens nur zu bejahen sein.

Wege aus dem Dilemma

Wie bereits ausgeführt, bringt die Gestattung der privaten Nutzung der betriebseigenen IT-Infrastruktur durch die Mitarbeiter nicht zu unterschätzende rechtliche Komplikationen mit sich – gerade was auch die Archivierung von E-Mails anbelangt. Aus dem Grund sollten sich die Verantwortlichen gut überlegen, ob überhaupt und wenn ja, in welcher Art und Weise die private E-Mail Kommunikation am Arbeitsplatz gestattet ist. Im Folgenden zeigen wir Ihnen praxisnahe Lösungen auf und beleuchten die rechtlichen Archivierungsanforderungen bei E-Mails.

Zumindest aus juristischer Sicht scheint ein Totalverbot des Einsatzes von E-Mails zu privaten Zwecken im Unternehmen die ideale Lösung zu sein: Das Unternehmen wird nicht zum Telekommunikationsanbieter, so dass das Fernmeldegeheimnis nicht gilt. Und auch kann datenschutzrechtlich die Archivierung gerechtfertigt werden. Das Unternehmen hat dann das Recht, beliebig und unbegrenzt die E-Mails der jeweiligen Mitarbeiter zu archivieren. Das Verbot sollte im Unternehmen aus Rechtssicherheitsgründen jedoch unbedingt kommuniziert werden.

Zu beachten wäre, dass das E-Mailverbot aus Beweisgründen in jedem Fall schriftlich fixiert werden sollte. Das Verbot ist auch in der Praxis durchzusetzen. Untersagt nämlich ein Arbeitgeber die private Nutzung von E-Mails, ohne dies dann regelmäßig zu kontrollieren und zu unterbinden, kann sich das Verbot in eine Duldung "umwandeln". Der Arbeitnehmer hat nach einer Weile der Duldung (sog. betriebliche Übung) einen Anspruch auf die Leistung, hier die Privatnutzung.

Zulassung mitarbeitereigener Mobilgeräte als Alternative

Über viele Handys, insbesondere Smartphones, können Nutzer mittlerweile bequem das Internet nutzen. Bei Laptops kann etwa über einen USB-Surf-Stick die Internetverbindung hergestellt werden. In beiden

Fällen wird der Internetzugang durch den Vertragspartner des Arbeitnehmers (Handyvertrag oder Surf-Stick-Vertrag) bereitgestellt. Dann ist nicht der Arbeitgeber Anbieter nach dem TKG, sondern der Vertragspartner des Internetzugangs des Mitarbeiters. Zudem werden die privaten E-Mails nicht durch den Arbeitgeber archiviert.

Die vorbehaltlose Erlaubnis der privaten E-Mailnutzung ist aus rechtlicher Sicht dagegen alles andere als ideal. Dem Arbeitgeber ist es verwehrt, den privaten E-Mailverkehr seiner Mitarbeiter zu lesen – geschweige denn zu archivieren –, da das Fernmeldegeheimnis nach § 88 III TKG gilt. Können private E-Mails nicht von den betrieblichen unterschieden werden, ist dem Arbeitgeber auch der Zugriff auf die geschäftlichen E-Mails versagt. Der Zugriff auf den Inhalt der Mails kann für den Arbeitgeber zu einer Strafbarkeit nach §§ 206 und 202a StGB führen. In dieser Konstellation ergibt sich eine Pflichtenkollision des Arbeitgebers. Er verletzt entweder die Straftatbestände nach §§ 206, 202a StGB (Datenschutz, Fernmeldegeheimnis) oder nach 238b StGB (Buchführungspflicht).

Kompromisslösungen

Natürlich sind auch Zwischenlösungen als Kompromiss denkbar, etwa dergestalt, dass den Mitarbeitern im Einzelnen vorgeschrieben wird, auf welche Art und Weise privat über die firmeninterne IT-Infrastruktur kommuniziert werden kann. Folgende Lösungen bieten sich hierzu an:

Zugriff auf Web-Accounts

Der Arbeitgeber erlaubt den Zugriff auf eine private E-Mailadresse des Arbeitnehmers in einem Freemail-Account und verbietet den privaten E-Mailverkehr über die geschäftliche E-Mailadresse. Dadurch bleibt die geschäftliche E-Mailadresse von privaten Inhalten frei und kann ohne Konflikt mit dem Fernmeldegeheimnis archiviert werden. Verstößt der Arbeitnehmer dagegen, so verletzt er seine Treuepflicht mit der Folge, dass er nicht mehr schutzwürdig ist. Weiter sollte das private Surfen zeitlich beschränkt werden, also zum Beispiel auf die Zeiten von 08:00 Uhr bis 09:30 Uhr, von 12:00 Uhr bis 13:00 Uhr. Denn damit ist der Arbeitgeber nur in diesen Zeiträumen Anbieter nach dem TKG. Somit bleibt ihm in der übrigen Zeit die Möglichkeit, das Surfen der Arbeitnehmer zu kontrollieren.

Zuweisen einer privaten Adresse

Den Mitarbeitern kann neben einer geschäftlichen E-Mailadresse auch eine private und als solche gekennzeichnete E-Mailadresse wie Max.Muster.Privat@Firmenname.de zur Verfügung gestellt werden, verbunden mit der Auflage, dass nur Letztere zu privaten Zwecken genutzt werden darf. Der Arbeitgeber würde dann nur die E-Mails der geschäftlichen E-Mailadresse archivieren. Damit würde eine zentrale sowie effiziente Archivierung ermöglicht werden, da auf diese Weise eine Vermischung privater wie auch dienstlicher E-Mail ausgeschlossen sein würde.

Anlegen eines privaten Ordners

Jeder Arbeitnehmer legt einen Ordner "Privat" an, in den er alle privaten E-Mails verschiebt, bevor archiviert wird. Bei der Archivierung wird dieser Ordner nicht archiviert. Bei dieser Lösung darf jedoch nicht sofort beim Ein- oder Ausgang der E-Mails archiviert werden. Sondern es muss ein bestimmter Zeitpunkt vorgegeben werden, an dem archiviert wird, damit die Arbeitnehmer bis dahin ihre E-Mails verschieben können.

Kennzeichnung privater E-Mails.

Auch sind Regelungen denkbar, die dem Mitarbeiter vorschreiben würden, private E-Mails auch im Header deutlich als "privat" zu kennzeichnen. So wird es zum Teil schon von Behörden praktiziert. Manche Juristen vertreten die Auffassung, dass es in diesem Fall dem Arbeitgeber nicht verwehrt werden dürfe, immerhin den Betreff der jeweiligen E-Mail zu öffnen oder sichtbar zu machen. Dies ist jedoch abzulehnen, da jeglicher Inhalt der privaten Mail, also auch der Betreff, vom Fernmeldegeheimnis geschützt ist. Können private Mails von den betrieblichen Mails nicht unterschieden werden, ist dem Arbeitgeber auch der Zugriff auf die geschäftlichen E-Mails versagt.

Gesonderte Surfstationen

Der Arbeitgeber kann seinen Arbeitnehmern gesonderte Rechner zur Verfügung stellen, von denen aus die Arbeitnehmer auf das Internet und gegebenenfalls einen Drucker zugreifen können. Diese Rechner stehen auf einem zentralen Platz und dienen mehreren Arbeitnehmern zugleich, etwa pro Abteilung oder pro Stockwerk ein Rechner. Die Arbeitnehmer können von dort auf ihre Freemail-Accounts zugreifen, sonstige Seiten ansurfen, Dateien herunterladen, Dateien drucken et cetera. Dieser PC darf dann nicht archiviert werden. Verlässt ein Arbeitnehmer den Rechner, kann er diesen herunterfahren oder neustarten. Der Rechner sollte so konfiguriert sein, dass er bei jedem Herunterfahren ein komplettes Reset durchführt. Damit werden etwa alle heruntergeladenen Daten des Arbeitnehmers oder der Verlauf des Browsers gelöscht, so dass jeder nachfolgend nutzende Arbeitnehmer nicht die Daten seines Vorgängers sehen kann.

Einwilligung in die Archivierung

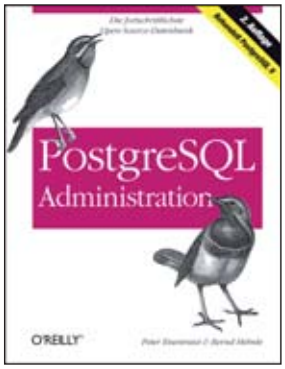
Teilweise wird die Ansicht vertreten, dass der Arbeitnehmer in die Archivierung der privaten E-Mails einwilligen kann. Damit kann der Arbeitgeber dem Arbeitnehmer die private E-Mailnutzung gewähren, wenn der Arbeitnehmer vorher die Einwilligung abgibt. Andernfalls erteilt er ihm ein Verbot zur privaten Nutzung. Begründet wird die Auffassung damit, dass der Arbeitnehmer auf den ihm gesetzlich gewährten Schutz des Fernmeldegeheimnisses verzichten kann. Die Gegenauffassung hält den Verzicht deshalb nicht möglich, da das Fernmeldegeheimnis auch für den Kommunikationspartner des Arbeitnehmers gilt. Für den Kommunikationspartner kann der Arbeitnehmer jedoch nicht "mitverzichten". Demzufolge führt diese Lösung nicht zu einer Möglichkeit, die private E-Mailnutzung und die Archivierung zu vereinen.

Fazit

Rund um das Thema E-Mailarchivierung gibt es für Unternehmen zahlreiche Gesetze und Normen einzuhalten. Insbesondere sollte genau geregelt werden, ob und wie Mitarbeiter eines Unternehmens die geschäftliche E-Mailadresse privat nutzen dürfen. Nur so lassen sich rechtliche Fußangeln umgehen und ein angenehmes Betriebsklima erhalten. *(dr)*

Rechtsassessor Patrick Prestel und Rechtsanwalt Max-Lion Keller LL.M. befassen sich mit IT-Recht in der Kanzlei Keller-Stoltenhoff, Keller, Münch (www.it-recht-kanzlei.de).

PostgreSQL Administration



Nunmehr bei Version 9 angelangt, spielt das Datenbankmanagementsystem PostgreSQL in kommerziellen Bereichen wie auch der öffentlichen Infrastruktur eine gewaltige Rolle. Auch wenn sich der Admin von heute in Bezug auf Beschreibungen zu PostgreSQL nicht mehr ausschließlich durch englische Webseiten arbeiten muss, zielt der Inhalt des Buchs "PostgreSQL Administration" in der 2. Auflage auf den stabilen und performanten Betrieb des Datenbanksystems.

In zehn Kapiteln hat sich das Autorenduo bemüht, praktische Erfahrungen für den professionellen Einsatz einzubauen, was weitestgehend gelungen ist. Auch wenn Windows-Versionen des Datenbankmanagementsystems verfügbar sind, bezieht sich der Inhalt auf Linux/Unix-Systeme und somit die Arbeit auf der Kommandozeile. Die ersten beiden Kapitel konzentrieren sich demzufolge auf die Installation und Grundkonfiguration anhand der verfügbaren Parameter. Für den Betrieb einer stabilen DB-Umgebung wird hierbei das notwendige Hintergrundwissen vermittelt.

Im Kapitel "Wartung" widmen sich die Autoren den wiederkehrenden Wartungstasks für den performanten Betrieb. Der Fokus liegt dabei sowohl auf der Defragmentierung und Reorganisierung von Tabellen und Indizes (VACUUM) wie auch Planerstatistiken (ANALYZE). Aufmerksamkeit verdient der Abschnitt "Performance-Tuning", der zahlreiche praktische Hinweise gibt, bevor die anspruchsvolle Thematik "Replikation und Hochverfügbarkeit" erfreulicherweise erschöpfend bearbeitet wird. Die Inhalte beider Kapitel tragen dazu bei, verschiedene Lösungen für eine bessere Verfügbarkeit und Leistung anzubieten.

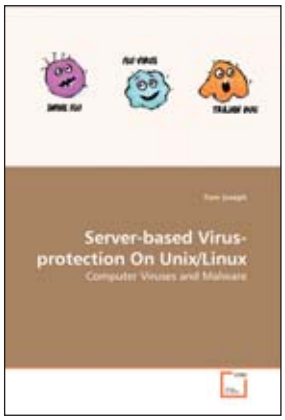
Fazit: Mit rund 370 Seiten wirkt das Buch auch aufgrund seines DIN A5-Formats erfreulicherweise handlich. Keine Schmalkost verspricht der Inhalt, der sich an erfahrene Datenbank-Administratoren richtet. Die Überarbeitung gegenüber der ersten Auflage verarbeitet aktuelle Entwicklungen (PostgreSQL 8.4, 9.0 und neue Hardware) sowie ausführlich die Möglichkeiten der Datenbankreplikation.

Der sachliche Schreibstil, der auf Schnörkel verzichtet, verhilft der Publikation zum aktuellen deutschsprachigen Referenzwerk, ohne Anspruch auf den gesamten Funktionsumfang des PostgreSQL-Systems.

Frank Große

Autor	Peter Eisentraut, Bernd Helmle
Verlag	O'Reilly
Preis	34,90 Euro
ISBN	978-3-89721-661-7
Bewertung (max. 10 Punkte)	**10**

Server-based Virus-protection on Unix/Linux



Gerade im professionellen Serverumfeld wird dem Thema Virenbefall unter Linux/Unix die berechtigte Aufmerksamkeit geschenkt, da durch die Sensibilisierung der vergangenen Jahre zumindest ein Grundbedürfnis vorhanden ist. In einer kurzen Einführung werden sowohl die Arten von Computerviren und Malware wie auch die Techniken zur Bekämpfung der Schädlinge aus theoretischer Sicht vorgestellt. Im darauffolgenden Kapitel untersucht der Autor den Einsatz von Drittanbieter-Lösungen zur Absicherung von Linux-Services, wie E-Mail, File- und Druckservern und den Einsatz beim Proxy-Server. Dabei werden Kommandozeilen-Scanner, Drittanbieter-APIs und Client-Server-Lösungen betrachtet.

Der Einsatz des Content Vectoring Protocol (CVP) als Teil von Checkpoints OPSEC wird vorgestellt und aufgrund der fehlenden Möglichkeit, einen Client weiterzuentwickeln, gegenüber dem Internet Calendar Access Protocol (ICAP) verworfen. Nach Beschreibung der Funktionsweise und Architektur von ICAP folgt die Auflistung von Softwarelösungen auf dieser Basis. Da der Autor tiefer in die Materie vorgedrungen ist, findet der Leser sowohl die technische Spezifikation wie auch die Arbeitsweise dieses Protokolls wieder.

AMaViS ist das Tool, das im Bereich des E-Mail-Virenschutzes zum Einsatz kommen soll. Die Implementierung in Sendmail und Postfix werden auf akademische Weise untersucht und der Leser darf hier kein How-To erwarten. Ebenso wird mit samba-vscan als Lösung für den Fileserver verfahren. Im Bereich der Webtransaktionen wird von einem Squid-Proxy ausgegangen. Dieser kontrolliert mit Squid-ICAP sowohl den FTP- wie auch Web-Transfer. Die Tests bescheinigen erfreulicherweise fehlerlose Ergebnisse.

Fazit: Der Leser erhält für einen relativ hohen Preis ein 109-seitiges Büchlein, welches das Ergebnis einer Diplomarbeit präsentiert. Erwartungsgemäß werden theoretische Aspekte in der Publikation in den Vordergrund gestellt, die anhand von Praxis-Erfahrungen untermauert und verglichen werden. Zahlreiche Performance-Tests belegen die Erkenntnisse. Für den Admin mit Interesse an tiefergehender Materie lesenswert, für den praktischen Einsatz aber weniger relevant.

Frank Große

Autor	Tom Joseph
Verlag	VDM Verlag Dr. Müller
Preis	51,99 Euro
ISBN	978-3639180534
Bewertung (max. 10 Punkte)	**5**

www.wsuspraxis.de

Gekonnt patchen

Immer ausgefeiltere Methoden bei Phishing und Malware lassen die Bedeutung eines effizienten Patchmanagements nahezu täglich steigen. Die zentrale Komponente des Patchmanagements ist dabei in vielen IT-Organisationen WSUS. Bei den Windows Server Update Services (WSUS) handelt es sich um eine Patch- und Updatesoftware, bestehend aus einer Server- und einer Clientkomponente. WSUS unterstützt die Administratoren, Microsoft-Updates im Netzwerk zu verteilen. WSUS lädt Updatepakete aus dem Internet und bietet sie den Windows-Clients zur Installation an. Und obwohl dieser Vorgang einfach und die WSUS-Technologie unkompliziert erscheint, treten in der Praxis der Patch-Verteilung doch immer wieder Fehler auf. Beginnend bei der Installation, über den Kontakt zu den Clients bis hin zur Sicherheit des WSUS-Servers steckt der Teufel wie so oft im Detail. Aber auch die Administration des WSUS-Servers selbst – etwa dessen Sicherung oder Aktualisierung – bedarf einiges an Know-how.

Auch wenn WSUS nicht alle Applikationen im Unternehmen patcht, stellt die Nutzung des Dienstes zumindest die ersten Schritte in Richtung eines umfassenden Patchmanagements dar. Unsere Website des Monats – wsuspraxis.de – begleitet den Administrator bei all diesen Schritten.

So stellt der Betreiber Arnd Rößner auf seiner als Blog betriebenen Webseite zahlreiche Hilfestellungen zur Inbetriebnahme, Konfiguration und Optimierung von WSUS bereit. Mit seinen regelmäßigen Blog-Einträgen hält Rößner seine Leserschaft über die aktuelle Entwicklung des WSUS auf dem Laufenden, informiert über problematische Patches und gibt Tipps und Tricks rund um den Update-Dienst von Microsoft zum Besten. Wer hier als WSUS-Admin nach der Lösung eines speziellen Problems sucht, hat über die Suche der Website gute Chancen, eine entsprechende Lösung zu finden.

Neben den laufenden Tipps der Blog-Einträge bietet wsuspraxis.de zudem eine ausführliche Anleitung für die Grundkonfiguration des WSUS-Servers. Darin beschreibt Rößner nicht nur die einzelnen Schritte der eigentlichen Installation. Er wirft zudem an passender Stelle immer wieder Hinweise zur Konfiguration und Beschaffenheit der umgebenden Infrastruktur in die Runde, die sich der Administrator zu Herzen nehmen sollte, um einen reibungslosen WSUS-Betrieb zu gewährleisten. Eine zweite ausführliche Anleitung befasst sich ebenso detailliert mit der Konfiguration der Gruppenrichtlinie "Windows Update" für die Verwendung mit Windows Server Update Services 3.0. Und zu guter Letzt stellt wsuspraxis.de dem Leser eine kleine Sammlung relevanter Links zur Verfügung. Wer also mit WSUS arbeitet, sollte die Seite regelmäßig besuchen, damit das Patchen nicht zur Flickschusterei verkommt. *(jp)*

Immer gut gepatcht: wsuspraxis.de bietet Tipps, Tricks und How-Tos

Unser Internetauftritt versorgt Sie jede Woche mit einem neuen interessanten Fachartikel. Diesen Monat erfahren Sie auf unserer Webseite mehr zu folgenden Themen:

Anwenderbericht: Umstellung auf Thin Clients bei A.T.U.

Alle PCs müssen raus – das war das Motto, das Auto-Teile-Unger für seine komplette Filial-IT ausgab. Um hohe Administrationskosten und Stromverbrauch zu senken, verwandelte A.T.U. insgesamt 4.000 PCs in Thin Clients. In unserem Anwenderbericht im Web beschreiben wir, wie das Server-based Computing beim größten deutschen KfZ-Dienstleister Einzug hielt, auf welche Thin Client-Modelle die IT-Verantwortlichen setzten und ob der Migrationsprozess reibungslos ablief.

www.it-administrator.de/themen/server_client/fachartikel/93139.html

5 GHz als Treiber für zukünftige WLAN-Netze

Tablet-PCs und Smartphones stellen immer öfter die Basis für so manche Unternehmensanwendung dar – dies belastet jedoch das bestehende WLAN und erfordert ein Aufrüsten, um das Vielfache an mobilen Usern bewältigen zu können. In unserem Beitrag im Web lesen Sie, wie Sie durch gleichzeitige Nutzung des 5 GHz- und 2,4 GHz-Bandes deutlich mehr überlappungsfreie Funkkanäle bereitstellen und mobilen Geräten so das volle Hochgeschwindigkeitsspektrum anbieten.

www.it-administrator.de/themen/kommunikation/fachartikel/93140.html

Solid State Drives und Auto-Tiering

Hohe Geschwindigkeit, fallende Preise und moderater Energieverbrauch tragen zur steigenden Verbreitung von SSDs in Highend-Speichersystemen bei. Kombiniert mit FC-, SAS- oder SATA-Platten, werden meist nur die wichtigsten Daten auf die schnellen Flash-Speicher verlagert. Unser Online-Fachartikel erklärt, wie ein solches automatisiertes Verlagern aussehen kann und wie sich dabei die Auslegung der Storage-Komponenten gestaltet.

www.it-administrator.de/themen/storage/fachartikel/93141.html

Anwenderbericht: Hochgeschwindigkeits-WLAN im Stadion

Ein WLAN mit bis zu 300 MBit/s Datendurchsatz macht eine schnelle Berichterstattung aus dem neuen Tivoli der Alemannia Aachen möglich – und legt gleichzeitig die Basis für eine Vielzahl an Diensten in Gastronomie, Service und Verwaltung. In unserem Online-Anwenderbericht erfahren Sie, welche Komponenten zur drahtlosen Datenübertragung im Stadion zum Einsatz kommen und dabei über 100 Journalisten sowie eine Fläche von 15.000 Quadratmetern mit Internetzugang versorgen.

www.it-administrator.de/themen/kommunikation/fachartikel/93142.html

Besser informiert: Fachartikel auf der Website des IT-Administrator

»Waldarbeit ist ein guter Ausgleich zum Bürojob«

Matthias Lerchbaumer (22) ist in der Linzer Zentrale der Rinder Warenhandel GmbH als Netzwerktechniker für das Server-based Computing der Firmengruppe und die entsprechende Infrastruktur verantwortlich. Autoteile und Autozubehör sind seit mehr als 40 Jahren das Kerngeschäft des international tätigen Unternehmens im österreichischen Linz/Leonding.

Warum sind Sie IT-Administrator geworden?

Ich habe eine Arbeitsstelle, an der ich meine erlernten Fähigkeiten unter Beweis stellen kann. In der IT bin ich eigentlich mehr durch Zufall gelandet und dann recht schnell in die jetzigen Aufgaben hineingewachsen.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Die Waldarbeit ist ein guter Ausgleich zum Bürojob. Entspannung finde ich auch bei meinem anderen Hobby, der Restauration von Oldtimertraktoren. Diese wunderbaren alten Maschinen wieder zum Laufen zu bringen und mit ihnen zu fahren, ist ein tolles Erfolgserlebnis.

Nehmen Sie Ihre Arbeit auch in den Urlaub, ins Wochenende mit?

Manchmal lässt sich das nicht vermeiden. Doch meistens gelingt mir die Trennung von Beruf und Privatleben recht gut.

Welche Aspekte Ihres Berufs machen Ihnen am meisten Spaß und welche weniger?

Als Netzwerktechniker habe ich eine abwechslungsreiche Tätigkeit, die mir viel Spaß macht. Weniger schön finde ich die doch überwiegend sitzende Tätigkeit und die Belastung der Augen.

Warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Es ist eine verantwortungsvolle Aufgabe, die viel eigenständiges Arbeiten ermöglicht. Darüber hinaus ist es befriedigend, die Kollegen bei ihrer Arbeit zu unterstützen.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Derzeit arbeiten wir an der Erstellung einer allgemeinen Produktdatenbank, welche die User mit Hilfe von Masken verändern und erweitern können. Diese Produktdatenbank soll in Zukunft sowohl die Erstellung von eigenen Katalogen ermöglichen als auch als Datenquelle für den Online-Katalog der Website dienen. Die grafischen Elemente für dieses Projekt steuere ich auch bei.

Mit welcher aktuellen IT-Technologie würden Sie gern einmal arbeiten?

Als Grafik-affiner Mensch würde mich die Arbeit mit Photoshop CS 5 reizen. Im IT-Bereich wäre es schön, zumindest auf einem Server mit Windows Server 2008 arbeiten zu können.

Wie denken Sie, arbeitet ein Administrator in 10 Jahren?

Wahrscheinlich werden viele Aufgaben in den Unternehmen noch stärker Datenbank-basiert sein, was den persönlichen Kontakt zu den Anwendern weiter reduziert.

In welchen Bereichen setzt Ihr Unternehmen Server-based Computing ein?

Unsere ausländischen Töchterfirmen sowie Anwender in Österreich greifen remote auf das Lagerverwaltungsprogramm zu, das auf unserem Terminalserver in der Firmenzentrale läuft. Auch Programme zur Produktverwaltung sowie andere Applikationen, die unternehmensweit im Einsatz sind, residieren auf dem zentralen Host in Linz.

Halten Sie Server-based Computing für eine zukunftssichere Technologie?

Ja, ich glaube dieses Konzept wird sich behaupten. In Zukunft werden schnellere Internet- und Netzwerkverbindungen mehr Datendurchfluss ermöglichen. Dann werden auch multimediale Anwendungen, beispielsweise interaktive Grafiken, optimaler über Server-based Computing nutzbar sein.

Welche besonderen Herausforderungen und welchen Nutzen hält diese Technologie bereit?

Als Herausforderung sehe ich vor allem die Bedienung und Wartung des zentralen Servers, da bei einem Ausfall sämtliche Clients in ihrer Arbeit stark eingeschränkt sind. Wenn die Systeme ordnungsgemäß laufen, beschränken sich Wartungsarbeiten allerdings lediglich auf den oder die Server. Um zahlreiche, oft weit voneinander entfernt arbeitende Clients muss man sich nicht kümmern.

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?

Geburtstag: 31.05.1988
Familienstand: ledig
Hobbys: Oldtimertraktoren restaurieren, Radfahren, Lesen, Natur

Matthias Lerchbaumer, IT-Administrator

Ausbildung und Tätigkeit

- Höhere Lehranstalt für Wirtschaftliche Berufe in Freistadt (Österreich), Zweig Kommunikations- und Mediendesign
- Quereinstieg in die IT-Administration
- Heute Netzwerktechniker mit Verantwortung als IT-Administrator (Netzwerk- und Serverwartung, EDV User Support, Druckerinstallation und -wartung, Installation und Wartung von PCs und Notebooks, Wartung Mailsystem, Wartung Firmenwebsite, Wartung der internen Datenbanken (Oracle und SQL-Server), Datensicherung und andere technische Aufgaben
- Teilverantwortung für das Marketing wie etwa Betreuung der Firmenwebsite, Verantwortung für alle grafischen Umsetzungen, darunter Produktfotos

Betreute Infrastruktur

- Dezentrale IT-Landschaft mit drei Terminalservern, drei Datenbankservern, zwei Applikationsservern, virtueller Mailserver mit VMware, Windows Server 2003
- rund 40 Clients in Linz, dazu etwa acht mobile im Außendienst
- weitere Arbeitsplätze in den Niederlassungen in Deutschland, Tschechien, Slowakei, Ungarn und Slowenien
- Datenverkehr der Tochterfirmen läuft komplett über die Server in Linz
- Warenlager in der Slowakei mit Funkterminals wird von Linz aus betreut

Die Ausgabe 6/11 erscheint am 1. Juni 2011

Schwerpunktthema:

Virtualisierungs-Management und Automatisierung

Im Test: Xaganti for ESX

Im Test: NetIQ Aegis

Workshop: Hyper-V über die PowerShell verwalten

Systeme: Neuerungen in Microsoft System Center Virtual Machine Manager 2012

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

Die Ausgabe im **Juli** hat sich zum Schwerpunkt das Thema **Hochverfügbarkeit** gesetzt. In unseren Tests werfen wir unter anderem einen Blick auf Marathon everRun MX. In den Workshops lesen Sie, wie Sie Citrix XenServer 4 mit der Hochverfügbarkeitserweiterung Remus gegen Ausfälle absichern.

Als Schwerpunkt im **August** folgt dann das Thema **Systemmanagement**.

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), *Stellv. Chefredakteur*
daniel.richey@it-administrator.de

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, René Büst, Thorsten Butz, Thomas Drilling, Frank Große, Herbert Hemke, Jürgen Heyer, Thomas Joos, Max-Lion Keller, Christian Knermann, Patrick Prestel, Dr. Holger Reibold, Florian Thiessenhusen, Matthias Wessner

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

Es gilt die Anzeigenpreisliste Nr. 8 vom 01.01.2011

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik, Gero Wortmann
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

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

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

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

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
All-Inclusive Jahresabo (mit Sonderheften + Jahres-CD) Inland: € 184,64
All-Inclusive Studentenabo Inland: € 117,14
All-Inclusive Jahresabo Ausland: € 199,64
All-Inclusive Studentenabo Ausland: € 124,64
E-Paper-Einzelheftpreis: € 9,45
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-
(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99
(zugleich Anschrift aller Verantwortlichen)
Web: www.heinemann-verlag.de
E-Mail: info@heinemann-verlag.de

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

. . . connecting your business

Made
in
Germany

WLAN mit Hochverfügbarkeitsgarantie? Von LANCOM!

Mit der LANCOM Smart Controller-Architektur sorgen wir für maximale Ausfallsicherheit im WLAN: was immer passiert, das Funknetz steht weiter zur Verfügung.

Davon profitieren kleine WLANs genauso wie Netze mit Tausenden von Access Points, der Hotspot genauso wie die Installation im Freien. Und: Wireless LANs von LANCOM skalieren perfekt – so wächst Ihr Netz ganz einfach mit Ihren Bedürfnissen.

Setzen auch Sie auf WLAN von der deutschen Nummer EINS! Exzellenter Service, kostenlose Updates & Investitionsschutz inklusive.

LANCOM
Systems