IT-ADMINISTRATOR.DE

01/2012

€ 12,60 ISSN 1614-2888

iadministrator

Das Magazin für professionelle System- und Netzwerkadministration

Client-Management

4 196583 212605 01

STRATO

www. .de

Sven Stornebel
STRATO Hosting-Kunde
www.stornebel.de

Power Hosting

schon ab **5,90** €/Mon.*

Jetzt starten und 6 Monate die Grundgebühr sparen!

Den Kopf voller Ideen? Mit STRATO werden daraus erfolgreiche Websites!

- Bis zu 12 Domains, 30 MySQL-Datenbanken und unlimited Traffic
- **NEU!** Mehr Leistung: Bis zu 20.000 MB Speicher und 2 GB E-Mailspace
- 1-Klick-Installation: Wordpress, Typo3, Joomla!, xt:Commerce, Contao
- **NEU!** Günstige Partnerangebote für individuelle Text- und Designkreation

Hosting-Pakete | Online-Speicher | Webshops | V-Server

» strato.de/idee

* Preisaktion bis 31.01.2012: Alle PowerWeb-Pakete 6 Monate 0 €/mtl., danach ab 5,90 €. Einmalige Einrichtungsgebühr 14,90 €. Mindestvertragslaufzeit 12 Monate. Preise inkl. MwSt.

Servicetelefon: 0 18 05 - 055 055
(0,14 €/Min. aus dem dt. Festnetz, Mobilfunk max. 0,42 €/Min.)

EDITORIAL

Wäre es einfach, könnte es ja jeder

Liebe Leser,

vor gar nicht allzu langer Zeit war die Welt des Client-Managers perfekt: Nach jahrelangem Kampf mit unausgereiften Betriebssystemen, mäßiger Hardware und rudimentären Mechanismen der Softwareverteilung stand es plötzlich da, das homogene Netz mit stabil laufenden Windows-Clients. Der User Help Desk frohlockte und der IT-Verantwortliche blickte nicht ohne Stolz auf sein nahezu perfektes Werk. Still und zuverlässig verrichtete ein Management-System die Softwareverteilung und das Patch-Management und die Anwender erfreuten sich an robuster, leistungsfähiger Hardware. Die Geschäftsführung lobte die umfassende, tagesaktuelle Inventarisierung und die Reduktion der IT-Kosten durch das transparente Lizenzmanagement. Milch und Honig flossen in der neuen Client-Wunderwelt.

Dieser Zustand hielt etwa zehn Minuten an.

Heute stehen die Anwender plötzlich mit ihren privaten Smartphones und Tablets vor seiner Tür und die Geschäftsführung erkundigt sich nach Einsparpotenzialen durch Cloud-Computing und Desktop-Virtualisierung. Mit anderen Worten: Die perfekte Welt unseres Client-Managers ist zusammengebrochen und muss neu aufgebaut werden. Doch verzagen ist nicht angesagt, denn wie der Titel dieses Editorials schon signalisiert: Wenn es denn einfach wäre … bräuchte es keine Admins!

Glücklicherweise bringt die technologische Entwicklung dem IT-Verantwortlichen nicht nur neue Herausforderungen. Denn was vor Jahren noch State-of-the-Art in der IT war, ist heute teilweise als Freeware zu haben. So finden Sie beispielsweise in unseren Tipps, Tricks & Tools ab Seite 67 ein kostenloses Werkzeug, das Netze mit bis zu 20 Clients vollständig inventarisiert und sich zudem um das Lizenzmanagement kümmert.

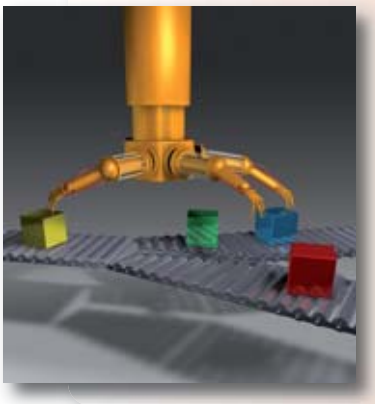
Gleichzeitig stehen neue Technologien zur Verfügung, die Anwenderberechtigungen in bisher unbekanntem Ausmaß steuern, wie unser Test des AppSense Application Managers ab Seite 28 zeigt. Und wenn Ihr Unternehmen tatsächlich vor Kollegen überquillt, die nur noch mit Tablets und ständig mobil arbeiten, könnte sich ein Blick auf Office 365, den neuen Cloud-Dienst von Microsoft, lohnen, dessen Integration ins Netzwerk Sie ab Seite 56 finden. Und wie Sie all dies Ihren Anwendern am komfortabelsten beibringen, darüber macht sich Thomas Bär in seinem Artikel zum Aufbau einer internen Schulungsumgebung ab Seite 62 Gedanken. Vielleicht ist das alles ja doch nicht so schwer.

Viel Vergnügen beim Lesen, Ihr

John Pardey
Chefredakteur

Client-Management

baramundi Management Suite 8.5



Es vergeht kaum ein Tag, an dem nicht von Schwachstellen in bestimmten Applikationen, Betriebssystemen oder Plug-Ins die Rede ist. Für den Administrator keine leichte Aufgabe, in einer heterogenen und komplexen Umgebung Schritt zu halten. Abhilfe verspricht hier die baramundi Management Suite 8.5. IT-Administrator hat sich angeschaut, was die Software im Bereich Patchverteilung für den Admin zu bieten hat.

Seite 17

SBS 2011 Essentials einrichten

Mit dem Windows Small Business Server 2011 Essentials hat Microsoft ein Angebot für Unternehmen mit bis zu 25 Mitarbeitern geschnürt. Dieser neueste Spross der Windows Familie schließt die Lücke zwischen Windows Home Server 2011 und dem Small Business Server 2011 Standard. An Funktionen muss der IT-Verantwortliche dabei gerade für kleinere Umgebungen keine Abstriche machen. IT-Administrator stellt die Möglichkeiten und Grenzen des Server-Betriebssystems vor.

Seite 52

Office 365 im Unternehmen einsetzen

Seit Mitte 2010 bietet Microsoft eine Online-Variante seiner Office- und Collaboration-Lösungen. In diesem Artikel beleuchten wir, was genau hinter diesem Angebot steckt und wo dessen Vor- und Nachteile liegen. Außerdem gehen wird darauf ein, wie eine mögliche Strategie beim Gang in die Wolke aussehen kann. So müssen sich Unternehmen etwa entscheiden, ob sie die komplette Kommunikations- und Office-Infrastruktur auslagern oder ob sie weiterhin eigene Server betreiben.

Seite 56

Vorteile automatisierter Anwendungsvirtualisierung

Durch den Wandel vom PC zur Cloud gewinnt die Desktop-Virtualisierung zunehmend an Popularität. Die Verbreitung neuer und verschiedener Kundengeräte und der Bedarf der Anwender an Mobilität beschleunigen diese Entwicklung zusätzlich. Virtualisierte und voneinander getrennte Ressourcen (Betriebssystem, Anwendungen, Benutzerdaten und -einstellungen) bieten gegenüber dem Desktopmodell den Vorteil, dass alle Schichten unabhängig voneinander verwaltet und gegebenenfalls an den erforderlichen Stellen in Verbindung mit zahlreichen Technologien eingesetzt werden können.

Seite 73

Link-Codes

Unsere Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs

Datenschleuse XXL

Die neue **Appliance SRA EX9000** von **SonicWALL** soll IT-Abteilungen in die Lage versetzen, bis zu **20.000 Remote-Zugriffe** von Geräten unter Windows und Windows Mobile, Mac OS und iOS, Android und Linux zu ermöglichen. Hierfür stellt die Appliance mit zwei Höheneinheiten und der integrierten Software **Aventail 10.6** einen Zugang her und kontrolliert diesen entweder über eine clientlose SSL-VPN-Verbindung oder clientbasiert. Mithilfe der Endpunktkontrolle und einer Authentifizierung lassen sich laut Hersteller die Identität der Anwender und der Sicherheitszustand der Geräte überprüfen. Sowohl das kürzlich vorgestellte SonicWALL Mobile Connect Client-App für iPad, iPhone und den iPod touch als auch der bereits länger verfügbare Client Aventail Connect für Android-Smartphones und -Tablets sollen den SSL-verschlüsselten Zugang zu Netzwerkressourcen von unternehmenseigenen oder von privaten Geräten der Mitarbeiter ermöglichen. Anwender oder IT-Administratoren können die Mobile Connect App über den App Store und Aventail Connect über den Android Market herunterladen. Erhältlich ist die SRA EX9000 ab sofort für 37.800 Euro. *(dr)*

SonicWALL: www.sonicwall.de

Die SonicWALL-Appliance SRA EX9000 richtet sich an große Unternehmen und ermöglicht sichere Remote-Zugriffe

Breitband-Schutz für Windows 7

Mit **Version 2.3** seines **Advanced VPN Client** erweitert **LANCOM Systems** seinen VPN-Client um eine **Breitband-Unterstützung für Windows 7**. Die neue Version überträgt die Daten bei Mobilfunkanbindungen wie LTE nun über das Windows Mobile Broadband Interface und soll so die maximale Datenübertragungsrate garantieren. Eine weitere Neuerung ist die überarbeitete Konfigurations-Oberfläche der integrierten Personal Firewall. Sie erlaubt das direkte Aktivieren und Deaktivieren von Firewall-Regeln per Mausklick. Ebenso lassen sich vordefinierte Policies erstellen. Zudem können Regeln für die Datenübertragung mit dem IPv6-Protokoll definiert werden. Die Funktion "Seamless Roaming" ermöglicht es, zwischen unterschiedlichen Netzen (beispielsweise WLAN und UMTS) zu wechseln. Online-Anwendungen überstehen dabei laut Hersteller Verbindungsunterbrechungen und -wechsel ohne Verbindungsverlust des VPN-Clients. Im Zusammenspiel mit der kommenden Version des LANCOM-Betriebssystems LCOS 8.6 soll diese Funktion von der Version 2.3 des Advanced VPN Client unterstützt werden. Zudem ermögliche der LANCOM Advanced VPN Client im Gegensatz zu üblichen IPsec und SSL-VPN-Clients nicht nur Verbindungen über WLAN, ISDN, analoge oder DSL-Modems, sondern auch direkt über LTE, UMTS und GPRS. Der Client lässt sich laut Hersteller mit allen aktuellen 32 und 64 Bit-Windows-Systemen nutzen und ist für 99 Euro ab sofort zu haben. *(dr)*

LANCOM Systems: www.lancom.de

Netzwerkschutz 2.0

Mit der Appliance **XTM 330** will **WatchGuard Technologies** Unternehmen mit bis zu 50 Anwendern **Schutz vor aktuellen Bedrohungen** bieten. Auch kleinere Firmen setzen verstärkt auf den mobilen Zugang zu Informationen im Netzwerk und integrieren Kommunikationsmittel wie Smartphone und Tablets in den Datenaustauschprozess. Um das eigene Netz dabei vor Angriffen zu sichern, soll die neue Appliance erweiterte Funktionen wie Applikationskontrolle, Gateway-Antivirus oder Web-Blocker bieten. So unterstützt die Plattform den clientlosen Netzwerkzugriff mittels Single Sign-on. Auf diese Weise soll sich die Authentifizierung der Nutzer schnell abwickeln und die Einhaltung von Gruppenregeln effektiv absichern und überwachen lassen. Erweiterte Management- und Logging-Funktionen erlauben laut Hersteller die Kontrolle auf Basis von Berichten. Unternehmen sollen detaillierte Einblicke zur Internetnutzung sowie zum Einsatz verschiedener Anwendungen erhalten. Die XTM 330 eignet sich zudem für Managed Security Service Provider (MSSP), die ihren Kunden eine leistungsfähige Lösung mit geringem Aufwand auf Administrationsseite anbieten möchten. Die Appliance ist ab sofort verfügbar. Der Listenpreis startet ab 1.046 Euro. *(dr)*

WatchGuard Technologies: www.watchguard.de

Die Appliance XTM 330 von WatchGuard Technologies soll KMUs vor aktuellen Bedrohungen schützen

Sensible Daten angetreten!

Nogacom veröffentlicht Version 3.8 von **NogaLogic**, seiner **Software zur Datenklassifizierung**. Die Neuerungen des aktuellen Release beziehen sich vor allem auf die **Identifizierung sensibler Daten**. Dazu hat der Hersteller sein Werkzeug mit einem Dashboard ausgestattet, das einen Snapshot über den Zustand und die Beschaffenheit von sensiblen Daten liefert und Auskunft über Informationen erteilt, die möglicherweise ungeschützt sind. Zudem zeigt es, in welchen Repositories sensible Daten gespeichert sind. Der Nutzer soll so erkennen können, ob es sich dabei um ungeeignete oder ungeschützte Speicherorte handelt. Mit neuen Report-Features will der Hersteller einen noch höheren Detaillierungsgrad innerhalb der sensiblen Daten liefern. Dies schließt Reporte ein, die Auskunft geben über ungeeignete Berechtigungen auf sensible Daten, detaillierte Informationen zur Verbreitung von sensiblen Daten via E-Mail innerhalb der Unternehmens oder nach außen, Versionen und Kopien von sensiblen Dokumenten und ebenso über Teile von sensiblen Inhalten, die in andere Dokumente kopiert wurden. Policy Management-Funktionen sollen es schließlich ermöglichen, sensible Informationen einfach zu verschieben, zu kopieren und zu markieren. Die Lizenzkosten für NogaLogic beginnen bei rund 35.500 Euro. Dieses Paket beinhaltet drei Konnektoren (Active Directory, Filesystem, ODBC) und eignet sich für eine Million Dokumente. *(ln)*

Um sensible Daten zu schützen, gilt es, diese überhaupt erst einmal zu identifizieren. NogaLogic 3.8 widmet sich dieser Aufgabe.

Nogacom: www.nogacom.com

Die Harten für den Garten

Von **ZyXEL** kommt mit Modell **NWA3550-N** ein neuer **Access Point** nach N-Standard für den **Einsatz im Außenbereich**. Bei dem Gerät handelt es sich um einen Access Point mit 2T2R MIMO-Technologie. Es verfügt über vier N-Type Antennenanschlüsse und eine GBit-Schnittstelle und lässt sich wahlweise als AP-Controller, Managed AP und Standalone AP betreiben. Der Zugriffspunkt funkt mit einer Brutto-Datenrate von 300 MBit/s und ist aufgrund der Zertifizierung EN 60601-1-2 für den Einsatz in medizinischen Umgebungen geeignet. Das Outdoor-Gehäuse ist gegen Strahl- und Spritzwasser geschützt, arbeitet in einem erweiterten Temperaturbereich von -40 °C bis +60 °C und besteht aus schwer entflammbarem und halogenfreiem Material. Die Verwaltung erfolgt über eine grafische Managementschnittstelle. Backup-Redundanz und sichere Tunnels zwischen Controller und managed Access Point will der Hersteller integriert haben, so dass jederzeit abhörsichere Verbindungen möglich sind. Das Gerät verfügt zudem über einen integrierten RADIUS-Server, der den Einsatz eines Stand Alone RADIUS-Servers überflüssig macht. Die Stromversorgung der Netzwerkkomponente kann je nach Bedarf und Einsatzort auch über Power over Ethernet nach IEEE 802.at erfolgen. Der Access Point ist ab sofort zum Preis von rund 610 Euro erhältlich. *(ln)*

ZyXEL: www.zyxel.com/de

Mit dem NWA3550-N rundet ZyXEL sein Portfolio um einen Access Point für den Einsatz im Freien ab

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

Belkin stellt den **WLAN-Travel Router GO N300 DB** vor. Das kompakte Dual-Band-Gerät verwandelt Internetanschlüsse wie in Hotels in einen WLAN-Hotspot, über den mehrere Geräte gleichzeitig auf das Internet zugreifen können. Seinen Strom bezieht der Mini-Access Point über USB und kommt damit ohne separates Netzteil aus. Der Datendurchsatz soll bei 150 MBit/s auf beiden Funkbändern mit 2,4 und 5 GHz liegen, während die Kommunikation dank WPA2 vor Lauschern geschützt ist. Für rund 50 Euro ist der Access Point zu haben. *(dr)*

www.belkin.de

Sourcefire erweitert sein Produkt-Portfolio um die **Next-Generation Firewall** (NGFW). Die Appliance-Serie basiert auf dem IPS des Herstellers und nutzt die FirePOWER-Plattform. Die Firewalls sollen unter anderem sinnvolle Policy-Empfehlungen und automatische Anpassungen an die Sicherheitsbedürfnisse der Kunden in Echtzeit bieten. Das Modell 3D8140 NGFW beispielsweise setzt dabei 10 GBit/s an Firewall-Traffic durch und ist für 155.000 US-Dollar zu haben. Im ersten Halbjahr 2012 will der Hersteller dann auch Modelle für kleinere Umgebungen anbieten. *(dr)*

www.sourcefire.com

Cortado veröffentlicht Version 8.6 seiner Druck-Software **ThinPrint RDP Engine**. Das neue Release unterstützt Finishing-Optionen von Druckern wie etwa Lochen, Heften und Binden und soll mit dem Feature SpeedCache die Druckausgabe beschleunigen. Dies gelingt, indem Bildelemente, die sich in einem Druckjob wiederholen, nicht für jede Seite neu zum Ausgabegerät übermittelt werden. Außerdem ermöglicht die Lösung mobiles Cloud Printing direkt aus einer Session heraus. Dies sieht konkret so aus, dass der Anwender sich in der Session befindet, sein Dokument in die Cloud druckt und anschließend die Ausgabe an einem beliebigen Drucker startet, der sich in einem WLAN etwa im Hotel oder Besprechungsraum befindet. Voraussetzung ist ein Cortado-Workplace- oder Cortado-Corporate-Server-Account. Die RDP Engine ist ab 950 Euro erhältlich. *(ln)*

www.thinprint.de

Jaspersoft bringt mit **Jaspersoft 4.5** eine neue Version seiner **Software zur Analyse großer Datenmengen** auf den Markt. Bestandteil der Lösung sind diverse neue Funktionen. So kann der Nutzer in wenigen Schritten Drag & Drop-Analysen und Berichte für große Datenmengen jeglicher Art (zum Beispiel aus Apache Hadoop-, NoSQL- und Analysedatenbanken) erstellen. Zu den Features des aktuellen Release zählen außerdem eine erweiterte Analyse-Benutzeroberfläche, eine verbesserte In-Memory-Engine mit intelligenter Push-Down-Abfrage für gesteigerte Performance sowie nativer Zugriff ohne lange Latenzzeiten auf nicht-relationale Daten. Eine optimierte Excel-Ausgabe und erweiterte REST-APIs runden das Funktionsangebot von Jaspersoft 4.5 ab, das ab 4.000 Euro erhältlich ist. *(ln)*

www.jaspersoft.com/de

Bissiges Antivirus

GFI Software bringt **GFI VIPRE Antivirus Business 5.0** auf den Markt, eine **netzwerkbasierte Antiviren-Lösung**. Die neue Version beinhaltet zahlreiche Verbesserungen und neue Features. Während des Installationsprozesses kann der Administrator das Tool zur Entfernung inkompatibler Software verwenden, um vorhandene Agenten anderer Antiviren-Lösungen sicher zu löschen. Als Teil des Installationsprozesses konfiguriert VIPRE Business automatisch die Windows-Firewalls auf den einzelnen Clientsystemen, um eine reibungslose Kommunikation der Agents mit der Server-Software zu gewährleisten. Die Software eliminiert zudem die Notwendigkeit einer manuellen Datenbank-Konfiguration. Hierfür bringt das Antivirus eine integrierte Datenbank mit, welche die Installation beschleunigen und das Management vereinfachen soll. VIPRE Business kann dabei auch mit einer bestehenden Microsoft SQL-Datenbank eingesetzt werden. Der Virenschutz bietet eine zusätzliche Kommunikationsschicht für Administratoren und IT-Dienstleister, die multiple Installationen bei Kunden verwalten müssen. Die größere Variante VIPRE Business Premium bietet zusätzlich eine bidirektionale Firewall zur Verfolgung des Netzwerkverkehrs, ein Host Intrusion Prevention System (HIPS) zur Überwachung verdächtiger Aktivitäten sowie einen Web-Filter zum Blocken unerwünschter Inhalte, bösartiger Skripte, Phishing Sites und anderer schädlicher URLs. GFI VIPRE Antivirus Business ist ab sofort verfügbar. Die Preise liegen bei 12,30 Euro je Nutzer bei 100 Usern. *(dr)*

GFI Software: www.gfisoftware.de

Kontaktfreudiges NAS

LaCie präsentiert den **12big Rack Storage Server**. Der **Netzwerkspeicher** verfügt über neue Soft- und Hardware. So bietet der Storage-Server eine vierfache LAN-Anbindung und arbeitet mit dem Betriebssystem Windows Storage Server. Im Inneren arbeitet ein Intel Quad Core Xeon-Prozessor mit 4 GByte RAM, der für genug Leistung für das Ausführen paralleler Tasks und für bis zu 250 Benutzer sorgen soll. E/A-Anschlüsse für die Anbindung externer Speichergeräte und die Integration als JBOD-Array sorgen zudem laut Hersteller für eine Skalierbarkeit bis zu 144 TByte. Der Hardware-RAID-Controller unterstützt die RAID-Modi 0, 1, 5, 10, 50 sowie 60. Fünf freie PCIe-Steckplätze ermöglichen die Anbindung an 10-GBit-Ethernet, Fibre Channel oder InfiniBand. Der LaCie 12big Rack Storage Server ist mit 9 TByte, 12 TByte, 24 TByte und 36 TByte Kapazität für rund 8.200 Euro erhältlich. *(dr)*

LaCie: www.lacie.com

Mehr APIs und Skripte beim Monitoring

ManageEngine gibt die Verfügbarkeit von Version 9.0 des **OpManager** bekannt. Die neueste Ausgabe der Software zur **Überwachung großer Netzwerkumgebungen** bietet neben einem erweiterten Benutzer-Interface zahlreiche neue Funktionen. So etwa lassen sich IT-Workflows nun automatisieren: Die IT Workflow Engine mit Drag & Drop-Oberfläche soll Administratoren dabei helfen, Probleme schneller zu identifizieren und die Zeit bis zu deren Behebung zu verringern. Zudem bietet die Engine Out-of-the-Box-Unterstützung für Aktionen, Überprüfungen und Planung. Die Monitoring-Suite hat außerdem mehr Dienste zur Überwachung virtualisierter Umgebungen an Bord. So etwa enthält die Einbindung für Microsoft Hyper-V nun mehr als 70 Werte zur Verfügbarkeit und Performance von Hyper-V-Hosts und -Guests. Mehr Schnittstellen sollen zudem für eine einfache Integration bestehender Helpdesk- und Management-Lösungen sorgen. Durch die Erstellung eigener Skripte lassen sich Netzwerke noch individueller überwachen – unterstützte Skripte sind nun unter anderem PowerShell, Linux shell script, VBScript, JavaScript, CScript, Perl und Python. Die Preise für das Monitoring-Werkzeug beginnen bei etwa 1.500 Euro. *(ln)*

ManageEngine: www.manageengine.de/opmanager

Auch bei Version 9.0 des Monitoring-Tools OpManager darf eine App zum Zugriff vom Smartphone aus nicht fehlen

Multimedia für alle

Mit dem Service Pack 1 für Windows 7 und Server 2008 R2 hat Microsoft den Multimedia-Beschleuniger **RemoteFX** eingeführt. Damit die Nutzer von **Rangee-Thin Clients** ebenfalls in den Genuss der Vorteile von RemoteFX kommen, unterstützen ab sofort alle Rangee Thin Clients auf Basis von **Windows Embedded** die Technologie. Und auch Geräte mit Rangee Linux können die Grafikfunktionen von RemoteFX dank eines **Software-Moduls von FreeRDP** nutzen. FreeRDP ermöglicht zudem mit einem Rangee Linux-basierten Thin Client, einen zweiten Bildschirm als erweiterten Bildschirm in einer Windows-Session zu nutzen. Das Modell Rangee 3505 etwa erlaubt die Drehung des zweiten Bildschirms (L-Scale). Diese Funktion bietet sich an, um beispielsweise gleichzeitig Dokumente im Hochformat zu bearbeiten und die Buchungssoftware auf dem Standardmonitor zu nutzen. Für die Nutzung von RemoteFX ist zum einen eine Virtualisierung mittels Hyper-V erforderlich. Zum anderen setzt die Technologie eine leistungsstarke Grafikkarte auf Server-Seite voraus. *(dr)*

Rangee: www.rangee.com

Fernwartung leicht gemacht

TeamViewer gibt den Startschuss für Version 7 seiner gleichnamigen **Software für Online-Meetings und die Fernsteuerung von PCs**. Was den Remote-Zugriff betrifft, will der Hersteller den Umgang mit dem neuen Release vereinfacht haben. So ist es bei der Dateiübertragung nun möglich, Files per Drag & Drop in beide Richtungen und in beliebige Ordner zu verschieben. Dies beinhaltet das Verschieben einer Datei in eine Outlook-E-Mail, wo diese automatisch als Anlage angehängt wird. Eine Erweiterung gab es auch bei der Unterstützung mehrerer Monitore: Sind am entfernten Computer mehrere Bildschirme angeschlossen, so lassen sich diese nun übersichtlich auf mehreren lokalen Monitoren anzeigen. Zudem kann der Nutzer individuelle Verbindungseinstellungen für einzelne Fernwartungspartner speichern und muss diese bei einer erneuten Sitzung nicht nochmals vornehmen. Mit der neuen Screenshot-Funktion lässt sich jederzeit der aktuelle Bildschirminhalt dokumentieren. Online-Meetings können mit TeamViewer 7 jetzt mit wenigen Mausklicks aufgesetzt werden. Teilnehmer greifen dabei optional flashbasiert über ihren Webbrowser zu – eine Installation der Software ist nicht erforderlich. Meetings lassen sich im Voraus anlegen und mit Microsoft Outlook planen. Der Präsentator kann Einladungen verschicken, die bereits alle notwendigen Informationen zur Teilnahme beinhalten. Für die professionelle Nutzung von TeamViewer sind verschiedene Lizenzen zu einmaligen Kosten ab rund 500 Euro erhältlich. *(ln)*

TeamViewer: www.teamviewer.com/de

Ausgebaut: TeamViewer 7 verfügt bei der Fernwartung und für Online-Meetings über eine Vielzahl neuer Funktionen

Funktionsreicher SOHO-Router

TP-LINK baut sein Portfolio mit Modell **TL-WR842ND** um einen **Router für den Einsatz in kleinen Büros** aus. Das Gerät funkt nach den Standards IEEE 802.11b/g/n und erreicht laut Hersteller mit Hilfe der MIMO-Technologie eine Brutto-Datenrate von 300 MBit/s. Für einzelne Abteilungen lassen sich per Knopfdruck bis zu vier separate Netzwerke mit eigenen SSIDs und Passwörtern erzeugen. Um die Datensicherheit weiter zu erhöhen, unterstützt die Netzwerkkomponente gleichzeitig bis zu fünf VPN-Verbindungen mit verschiedenen Verschlüsselungs- und Authentifizierungsalgorithmen (IPSec mit IKE, DES/3DES/AES, MD5/SHA1). Zu den erweiterten Sicherheitsfunktionen zählen Network Address Translation, VPN Pass-Through, PPTP, L2TP sowie IPSec. An WAN-Modi kommt das Gerät mit Dynamic IP, Static IP, PPPoE, PPTP, C2TP und BigPort zurecht. Für die optimale Verteilung der verfügbaren Bandbreite soll die QoS-Funktion sorgen. Über den USB 2.0-Port kann der Nutzer über den integrierten Media Server Multimedia-Dateien im Netzwerk zum Empfang bereitstellen. Über den ebenfalls eingebauten Printserver lässt sich auch ein Drucker netzwerkweit ansprechen. Der Multifunktions-WLAN-Router ist ab sofort zum Preis von rund 30 Euro erhältlich. *(ln)*

Mit bis zu vier verschiedenen SSIDs und maximal fünf gleichzeitigen VPN-Tunneln bietet der TL-WR842ND von TP-LINK recht viel für wenig Geld

TP-LINK: www.tp-link.com/de

Schutzpatron für vSphere

Das neue **Veeam Backup & Replication v6** soll eine **verbesserte Datensicherung unter VMware vSphere** ermöglichen. Die neue Version bietet nach Herstellerangaben dabei eine verbesserte Architektur für einfache Implementierung und Verwaltung von Backups in Unternehmen mit vielen Niederlassungen und verteilten Standorten. Backup, Replikation und Wiederherstellung über Weitverkehrsnetze wurden deutlich beschleunigt. Die Wiederherstellung auf Datei-Ebene (Instant File-level Recovery) wird um eine Web-basierte Wiederherstellung direkt in die ursprüngliche virtuelle Maschine hinein erweitert. Dazu sei weder eine direkte Netzwerkverbindung noch ein separater Agent auf der Gast-VM nötig. Außerdem unterstützt die Software nun **Windows Hyper-V**. Unternehmen, die neben VMware auch den Hypervisor von Microsoft einsetzen, benötigen damit lediglich eine Installation und nur eine Administrationskonsole. Unterstützt werden sowohl Windows Server Hyper-V als auch Microsoft Hyper-V Server aus der gleichen Backup-Infrastruktur heraus. Die neue Version 6 ist ab sofort für VMware vSphere und Windows Hyper-V verfügbar. Die Preise sind für beide Versionen identisch, zudem können die Lizenzen kostenlos zwischen den Hypervisoren getauscht werden. Ab Februar gelten dann neue Preise pro CPU-Socket: 910 Euro für die Enterprise Edition und 580 Euro für die Standard Edition. *(dr)*

Veeam: www.veeam.de

1&1 WEBHOSTING

Das beste Hosting für Profi-Websites:

- ✓ **Maximale Verfügbarkeit:** Georedundanter Betrieb – parallel in räumlich getrennten Rechenzentren!
- ✓ **Superschnell:** 275 GBit/s Anbindung!
- ✓ **Umweltschonend:** Grüner Strom!
- ✓ **Zukunftssicher:** 1.000 Entwickler bei 1&1!

1&1 DOMAINS

- Domain-Umzug
- Schnelle Domain-Aktivierung
- DNS-Verwaltung
- Domain-Umleitung
- E-Mail-Adresse zur Weiterleitung

~~0,49~~ €/Monat* .de .eu **0,29 €/Monat***

.de-Domain 1 Jahr für 0,29 €/Monat, danach ab 0,49 €/Monat.*

Weitere Domains mit Sparvorteil unter 1und1.info

1&1 DUAL PERFECT

- **6 DOMAINS INKLUSIVE**
- **5 GB** Webspace
- **UNLIMITED** Traffic
- 20 FTP-Accounts
- 10 MySQL-Datenbanken (je 1 GB)
- **UNLIMITED** Click & Build Apps (Auswahl aus 65 Applikationen)
- Zend Framework
- PHP6 (beta), PHP5, Perl, Python
- 24/7 Profi-Hotline

~~9,99~~ €/Monat* **0,– €/Monat***

1&1 Dual Perfect 6 Monate 0,– €, danach 9,99 €/Monat.*

Weitere Pakete mit 6-Monats-Sparvorteil unter 1und1.info

Internet made in Germany

*.de und .eu Domain 12 Monate 0,– €/Monat, danach .de 0,49 €/Monat, .eu 1,49 €/Monat. 1&1 Dual Perfect und 1&1 Perfect Shop 6 Monate 0,– €/Monat, danach 1&1 Dual Perfect 9,99 €/Monat, 1&1 Perfect Shop 19,99 €/Monat. Einmalige Einrichtungsgebühr 9,60 € (entfällt bei Domain-Paketen). 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

DAS SICHERSTE HOSTING

6 MONATE 0,– €/Monat*

1&1 PERFECT SHOP

- **1.000 ARTIKEL**
- 100 Warengruppen
- Marketing-Tools
- PayPal
- eBay-Tool
- **UNLIMITED** Click & Build Apps (Auswahl aus 65 Applikationen)

~~19,99 €/Monat*~~

0,– €/Monat*

1&1 Perfect Shop 6 Monate 0,–€, danach 19,99 €/Monat.*

Weitere E-Shops mit 6-Monats-Sparvorteil unter 1und1.info

1&1 bietet alles rund ums Thema Hosting bequem aus einer Hand:

- ✓ Domains
- ✓ Hosting
- ✓ E-Shops
- ✓ Online Office
- ✓ Suchmaschinen-Werbung
- ✓ Online Speicher
- ✓ MailXchange u. v. m.

1&1

Jetzt informieren und bestellen:

0 26 02 / 96 91

0800 / 100 668

www.1und1.info

Im Test: DeskCenter Management Suite 9.3

Client-Pflegedienst

von Thomas Bär

Die Vorzüge eines zentralisierten IT-Managements ergeben sich bereits in mittleren Unternehmen und besonders bei größeren Installationen. Alle Informationen über die IT-Infrastruktur sind so an einem Ort konzentriert und IT-Verantwortliche müssen nicht mühselig aus verschiedenen Datenquellen Infos zusammentragen, um eine Entscheidung fällen zu können. System-Management-Lösungen wie DeskCenter offenbaren stets den Blick auf den Ist-Zustand des Gesamtsystems in Echtzeit. Aber auch Aufgaben des administrativen Tagesgeschäfts, wie die Verteilung von Software, die Erfassung der IT-Komponenten, Patch-Management oder auch Fernwartung für den Support müssen diese Werkzeuge bieten. Die DeskCenter-Suite erhebt als Werkzeug für Systemadministratoren den Anspruch, deren tägliche Arbeit zu unterstützen und zu vereinfachen. Unser Test untersucht, wie gut DeskCenter dies gelingt.

Die DeskCenter Management Suite mag erst einige Jahre alt sein, das Wissen rund um das Systems-Management der beteiligten Produkt-Manager und -Entwickler nähert sich jedoch der zweiten Dekade. Programmlösungen dieser Art fallen ja nicht vom Himmel und es ist sehr viel Erfahrung notwendig, um ein Komplettpaket zur Verwaltung von Clients im Unternehmen zu schnüren. Neben den reinen Anforderungen des Systems Managements bietet die Software des Leipziger Herstellers einen integrierten User Help Desk, der das Portfolio in Richtung Service Desk ein wenig abrundet. Mit Ausnahme weniger Komponenten – hier sei auf die Fernwartung mit VNC und auf den Asset-Lizenz-Katalog "DNA" hingewiesen – ist DeskCenter eine Eigenentwicklung ohne eingekaufte Zusätze. Die Suite benötigt lediglich WMI, MDAC und Microsoft Windows Scripting Host auf den Client-Rechnern. Dies sind allesamt Standardkomponenten von Microsoft Windows und somit eigentlich immer vorhanden. Auf der Serverseite wird ein aktueller Windows-Server, Microsoft SQL Server, auch als Express-Variante, benötigt.

Unkomplizierte Installation

Für den Produkttest stellte uns der Hersteller eine vorkonfigurierte VMware ESX5i-Umgebung zur Verfügung. Auf dem dort virtualisierten Windows Server 2008 R2 mit zwei CPUs mit je zwei Kernen wurde mit 8 GByte zugewiesenem Arbeitsspeicher sowohl der Domänencontroller mit allen Server-Diensten als auch die Datenbank und die komplette DeskCenter-Suite betrieben. In der Praxis ist eine solche Konfiguration natürlich kaum empfehlenswert, da die Freigabe mit den Softwarepaketen somit auf einem Domänencontroller liegen würde – für einen Softwaretest ist dies jedoch kein Problem. Das Share mit den Paketen könnte zudem von einfachen NAS-Filern bereitgestellt werden, es ist nicht erforderlich, dass die Freigabe auf dem Server liegt, der als DeskCenter-Installation genutzt wird. Auf die ebenfalls vorkonfigurierten virtuellen Maschinen griffen wir im Test kaum zurück. Stattdessen nutzten wir physikalische Client-Computer aus unserer Testumgebung.

Wir spielten dennoch die Installationsschritte kurz exemplarisch durch, um uns einen Eindruck von der Qualität des Installationsassistenten zu machen. Dieser richtet in wenigen Schritten die Software komplett ein. Steht kein Microsoft SQL-Server im Netzwerk zur Verfügung, so bietet der Installationsassistent an, die kostenfreie 2008er Express-Edition aufzuspielen. Sofern die Web-Komponenten von DeskCenter genutzt werden sollen, ist die Aktivierung des Internet Information Server (IIS) in Windows erforderlich. Bei Bedarf können sich Administratoren und Systemverwalter die Konsole von DeskCenter lokal auf ihren Workstations installieren oder per Remote Desktop über den Server arbeiten.

Systemvoraussetzungen

Aktueller Windows-Server mit Microsoft SQL Server 2005 Express oder höher. Die Dienste der Software können aus Performancegründen auf einzelne Server verteilt werden. Kleinere Installationen sind auf einer einzigen Hardware möglich. Clientseitig ergeben sich die Anforderungen aus der zu verteilenden Windows-Version und den verteilten Anwendungsprogrammen.

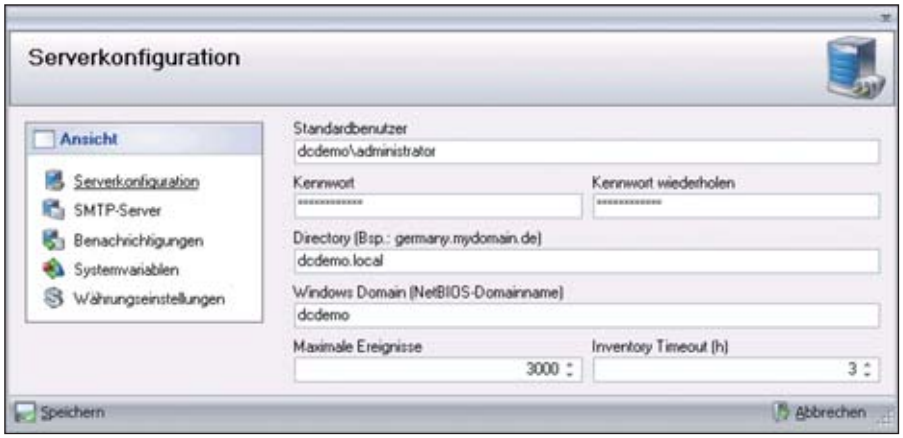


Bild 1: Die Installation und Konfiguration der DeskCenter Management Suite ist mit wenigen Mausklicks und einigen Stammdaten zügig erledigt

Zügige Grundkonfiguration mit gewohnter Oberfläche

Die Oberfläche von DeskCenter gefällt auf Anhieb – kein Wunder, ist doch die Ähnlichkeit zu den aktuellen Microsoft Office-Varianten mit ihren Ribbons kaum zu übersehen. Menü- und Untermenü-Struktur sind auf den ersten Blick erkennbar. Das Hauptmenü der Software ist symbolhaft durch einen Kreis dargestellt – ebenfalls wie von Office bekannt. Alle wichtigen Befehle für den Systemverwalter sind entweder im stets rechts gehaltenen Aktions-Menü oder über das Kontextmenü aufrufbar. Sofern sinnvoll möglich, steht mit der "F1"-Taste ein kontextsensitives Handbuch zur Verfügung – manchmal sind die Hilfetexte jedoch so kurz geraten, dass der Blick in die PDF-Handbücher notwendig ist. Für die wichtigsten Aufgabengebiete, beispielsweise die Verteilung von Microsoft Windows XP, gibt es im Hauptmenü ein PDF-Tutorial, in dem der Sachverhalt Schritt für Schritt und mit Hintergrundinformationen betrachtet wird.

Die ersten Schritte unter "Serverkonfiguration" erklären sich von selbst. Zunächst muss ein administrativ berechtigter Benutzer-Account durch den Systembetreuer hinterlegt werden. Mit diesem Account werden die Installationsschritte auf den Client-Computern durchgeführt sowie eine Vielzahl weiterer Kommandos. Im Test war dies das Konto des Standard-Domänen-Administrators. Leider greift dieses Konto nicht für alle Aktionen – wird beispielsweise ein VB-Skript-Kommando ausgeführt, das in die Konsole des Administratoren eingebunden ist, so geschieht dies im Kontext des aktuell angemeldeten Benutzers und nicht in der Rolle des in den Stammdaten hinterlegten Administrators. Sofern der Systembetreuer stets mit ausreichend hohen Rechten angemeldet ist, mag das kein Problem sein. Es widerspricht nur dem Grundsatz, Konten möglichst keine Admin-Rechte zuzuweisen.

Die Module der Suite informieren die IT-Mannschaft per E-Mail über Änderungen in der Systemlandschaft. Glücklicherweise ist dies nur eine optionale Einstellung und erlaubt zudem eine feinere Steuerung wie "Erfolg melden", "Änderungen melden" oder "Lizenz läuft in n Tagen ab melden". Hier hinterlegten wir im Test die SMTP-Informationen eines E-Mailservers bei einem Provider. Dass es sich bei dem Icon mit dem Briefumschlag um den Befehl "teste die E-Mail-Einstellung" handelt, erkannten wir auf Anhieb – ansonsten hätte es der Tool-Tipp-Text getan. Insgesamt betrachtet ist die Installation und die Konfiguration der Software einfach und dürfte selbst auf leistungsschwacher Hardware in rund einer Stunde abgeschlossen sein. Das Einspielen von Installationsdateien für die Betriebssystemferninstallation (OS Deployment) und für die Verteilung von Programmen (Softwarepakete) dauert naturgemäß länger.

Offline/Online-Suche nach dem Inventar

Die Grundformel für ein effektives IT-Management ist simpel: "Keine Inventardaten – keine effektiven Entscheidungen". Da kaum eine Umgebung auf der sprichwörtlichen grünen Wiese im Zusammenspiel mit DeskCenter aufgebaut werden dürfte, müssen zunächst die Informationen der Umgebungen in die Datenbank gelangen. Das "One-Step-Inventory" ist ein Offline-Inventarisierungsmodul, das sich beispielsweise über einen USB-Stick direkt auf einem PC ausführen lässt. Die gesammelten Daten werden nicht direkt an die Datenbank geschickt, sondern zunächst lokal auf dem Datenträger gespeichert und erst auf ein manuelles Kommando an die Suite übergeben. Neben Inventardaten zur Hardware-Ausstattung über WMI arbeitet die Software mit einem angepassten Dateiscan – bekannte Applikationen können so anhand der Existenz von Dateien entdeckt und korrekt zugeordnet werden. Dank dem Parameter "/silent" ist auch eine Ausführung über die Kommandozeile, beispielsweise aus einem Anmeldeskript heraus, generell möglich. Zur Inventarisierung ist keine Installation einer Agenten-Komponente erforderlich – sofern Veränderungen laufend dokumentiert werden müssen, ist dies jedoch sinnvoll.

Gewöhnlich wird die Datenbank der Suite laufend mit Informationen durch eine kleine Agenten-Komponente (SDI) auf den Clients versorgt ("Live Inventarisierung"). Dieser Agent, je nach Konfiguration durch ein frei anpassbares Symbol im Task-Tray sichtbar, versorgt in frei konfigurierbaren Abständen die Suite mit Informationen. Mit Blick auf die Betriebssicherheit sehr günstig gelöst: Der Agent fragt aktiv bei dem für ihn definierten Server nach. Liegt dort ein Kommando vor – beispielsweise die Softwareinstallation – so führt der Agent den Befehl aus. Kommandos werden somit nicht gepusht, sondern für den Agent bereitgestellt.

Die ermittelten technischen Daten wie CPU-Typ, Festplattengröße oder eingesetzte Speicherbausteine werden für den schnellen Blick in einer kompakten Übersicht dargestellt. Diese ist für die Aufgabenstellungen im Support auf das Wichtigste begrenzt. Unter "Systemdetails" geht es dann in die tausenden von Werten bis hin zur gesetzten Systemvariablen. Der Primärschlüssel im Konzept von Desk-

Center ist nicht etwa die MAC-Adresse oder ein generierter UI – es ist der NetBios-Rechnername.

Technische Daten allein machen jedoch noch lang kein IT-Management aus. Das kaufmännische Asset Management erfasst alle weiteren Informationen, die für eine vollständige Verwaltung entscheidend sind. Diese Daten können jedoch nicht per WMI oder Dateiscan ermittelt werden. Kaufmännische Daten werden in die so genannten "Asset Sets" eingepflegt. Dazu zählen unter anderem Daten zu Kostenstellen, Verträgen, Garantien, Servicepartnern oder Abschreibungszeiträumen. Vorhandene Daten können Systembetreuer durch die offene SQL-Datenbank importieren, manuell erfassen oder mittels externer Schnittstellen mit anderen Systemen und Datenbanken, beispielsweise auch SAP, synchronisieren.

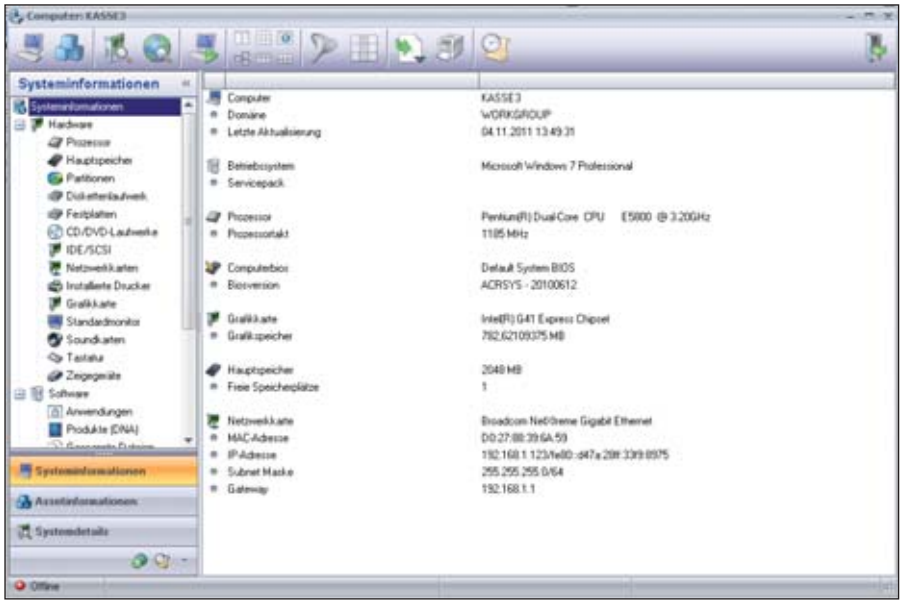


Bild 2: Die übersichtliche Zusammenfassung der Inventardaten ohne allzu viel Ballast dürfte vor allem die Mitarbeiter im Support erfreuen

Regelgestützte Software-Verteilung

Die erste zu lösende Aufgabe mit der Suite besteht in der Verteilung von Windows 7 im Testnetzwerk. Lizenzschlüssel, Gestaltung der Partitionen, zu installierende Windows-Funktionen – all dies nimmt der Administrator in selbsterklärenden Dialogen im Register "OS Deployment" vor. Der Rechnername kann entweder fix vergeben werden, als fortlaufende Nummer kreiert oder aus bereits bekannten Informationen, wie der MAC-Adresse, abgeleitet werden.

Wie beinahe alle Systems Management-Lösungen nutzt auch die DeskCenter Management Suite das PXE-Verfahren, um jedem startenden PC im Netzwerk ein Boot-Image zukommen zu lassen. Gibt es einen Auftrag zur Installation, so leitet das PXE-Image den traditionellen Installationsvorgang über WindowsPE ein, ansonsten würde das bereits installierte System von der Festplatte starten.

Der einfachste Weg, um an die benötigten Treiber eines Computers zu gelangen, ist der Einsatz eines kleinen Tools namens "EasyExtrakt" auf einer Referenz-Installation. Welche Treiber übernommen werden sollen und ob die generischen Windows-Treiber ebenfalls ausgelesen werden dürfen, legt der Systembetreuer durch die Auswahl einiger Checkboxen fest. Das so entstandene Treiberpaket wird über die DeskCenter-Konsole eingelesen und steht fortan zur Auswahl. Eine Treiberdatenbank, die der Hersteller pflegt, oder ein großer Treiberpool, aus dem sich die Installer herauspicken, was sie brauchen, gibt es hier nicht. Das sorgt zwar für eine ordentliche 1:1-Buchhaltung von Treiberpaketen zu PC-Reihen, erhöht aber den manuellen Aufwand für die IT. Sehr angenehm für den Administrator ist die Möglichkeit, von der gewählten Konfiguration gleich ein Boot-Image durch die Suite erzeugen zu lassen. Für Computer, die nicht per PXE erreicht werden können, vielleicht die einzige Möglichkeit, dennoch ordentlich installiert zu werden.

Im Test zahlten wir jedoch Lehrgeld: Wer denkt schon daran, dass eine Broadcom-Netzwerkkarte nicht im Treiberumfang von Windows 7 enthalten ist? Wir nicht und so blieb der Client-PC, ein aktueller Acer Veriton – der den Systemstart per PXE begann und versuchte, die Installation von Windows 7 durchzuführen –, im Abschnitt "Kopieren" ohne weiteren Kommentar längere Zeit stehen. Erst nachdem wir den NIC-Treiber als Teil des PXE-Grundpakets mit auf den Weg gaben, wurde die Installation komplett durchgeführt. Hierzu sind glücklicherweise nur sehr wenige Mausklicks erforderlich. Eines ist der Systematik der Windows-Installation im Unattended-Modus geschuldet: Nachdem der Client-Rechner mit der Installation begonnen hat, hat der Administrator in seinem System-Management nur noch wenige Informationen über das, was aktuell geschieht ("fire and forget"). Erst wenn sich ein Client-PC ungewöhnlich lange nicht zurückmeldet, offenbart er so, dass etwas nicht stimmt. Es zeigt sich einmal mehr, dass für jede Rechner-Charge zunächst ein Test zwingend notwendig ist. Ein logische Kaskade im Sinne eines Release-Managements mit Versionierung der Konfiguration, Definition von Testumgebungen und Freigabe durch einen Release-Verantwortlichen haben die Entwickler von DeskCenter derzeit nicht eingearbeitet.

Die Softwareverteilung mit der Suite basiert in erster Linie auf dem bekannten MSI-Paketformat. Erlaubt ist jedoch auch das Ausbringen aller ausführbaren Softwarepakete wie zum Beispiel EXE-Dateien, Batchdateien und Skripte. Außerdem wird die Verteilung von VMware ThinApp-Paketen mittels der Thinreg-Methode unterstützt. Installationen können durch den Administrator manuell oder regelbasiert initiiert werden. Eine Regel könnte beispielsweise lauten "Adobe Flash Player 10.1.82.76 soll installiert werden, wenn auf dem System der Adobe Flash Player mit einer Version vor 10.1.82.76. installiert ist." Diese Regeln können sowohl auf Computer- als auch

Vorteilspreis für IT-Administrator Abonnenten

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Training Windows Server Best-Practice

München, 21. März 2012 – Hamburg, 15. Mai 2012

Quelle: 123RF

Themen des Trainings:

Active Directory: So läuft's rund. Praxis aus 12 Jahren
- Active Directory und DNS - Virtuelle DCs
- Replikation - Sicherheit - Lieblingsfehler
- Ausblick: Neuerungen im Active Directory unter Windows Server 8

Wiederbelebung: Disaster Recovery für das Active Directory
- Was kann denn kaputtgehen?
- Backup-Methoden: Was geht und was nicht?
- Restore ist mehr als Backup: Praxisdemos

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

Referent: Nils Kaczenski

Termin: 21. März 2012
Ort: ExperTeach Training Center München, Wredestr. 11, 80335 München

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 7. März 2012

Termin: 15. Mai 2012
Ort: ExperTeach Training Center Hamburg, Esplanade 6, 20354 Hamburg

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 2. Mai 2012

Trainings-Partner:

ExperTeach

Teilnahmegebühren:
Für IT-Administrator Abonnenten Euro 145,- (zzgl. 19% MwSt.), für Nicht-Abonnenten Euro 195,- (zzgl. 19% MwSt.).
Die Teilnehmerzahl ist auf 25 begrenzt.

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

Benutzer-Objekte angewendet werden. Sofern eine Software über keine parametergestützte Verteilung verfügt, bleibt nur die eigene Paketerstellung mit dem optionalen und kostenpflichtigen "DeskCenter Package Studio". Das Package-Studio protokolliert die Installation und bildet aus dem Delta der Vor- und Nachher-Betrachtung ein Industriestandard-MSI-Paket.

Die Lizenzen stets im Blick

Lizenzmanagement ist in jedem Unternehmen unabhängig von der Größe ein immer wichtigeres Thema. Die Lizenzbestimmungen der Hersteller werden immer komplexer und für den Administrator zunehmend schwerer zu durchschauen. Abhängig vom Lizenzvertrag können Zweit- und Mehrfachnutzungsrechte gewährt werden, teilweise sind auch Upgrade- oder Downgrade-Rechte eingeschlossen und nicht zuletzt erschweren zum Beispiel einzuhaltende Bindungsfristen die alltägliche Arbeit. Die Software-Erkennung wurde ja bereits durch die Inventarisierung vorgenommen – nicht nur auf WMI-Basis, denn der Datei-Scan sichert das Ergebnis.

Jetzt besteht die Kunst darin, die ausgelesenen Informationen mit den Lizenz-Bedingungen des Herstellers und den Bestandsinformationen in Einklang zu bringen. Mit dem "Software Asset DNA Modul" wird ein einfacheres Lizenzmanagement mit einer Datenbank zur Softwareerkennung mit über 100.000 Produkteinträgen ermöglicht. Die Übersicht der Softwareprodukte enthält wichtige Details zu den Produkten, etwa ob die Software lizenzpflichtig ist, um was für eine Software es sich handelt, welche Lizenzarten zur Verfügung stehen, wer der Hersteller ist und welche Upgrade-Pfade und -Rechte es gibt. Die mit einer Repaketierung von Software einhergehende Änderung des eingetragenen Herstellers oder der Produktbezeichnung gleicht die Datenbank aus. Ein aktivierbares "Application Metering" erlaubt zudem die tatsächliche Nutzung zu ermitteln und erleichtert so die korrekte Lizenzierung im Terminalserver- und VM-Umfeld.

Fazit

Die DeskCenter Management Suite ist eine insgesamt leistungsfähige Software für das Systems Management in mittleren bis größeren Unternehmen. Die typischen Anforderungen des Tagesgeschäfts bewältigen Administratoren mithilfe der Software ohne Schwierigkeit. Während sich die Marktbegleiter aktuellen Themen wie VDI oder der möglichst hohe Automatisierung von Prozessen widmen, ist die DeskCenter Management Suite noch eher traditioneller ausgerichtet und orientiert sich an den alltäglichen Bedürfnissen des Administrators. Betriebssystem-Verteilung, Migrations-Aufgaben oder einfache Softwareverteilung – alles ist mit dem Werkzeug gut möglich. Automatisierte Aktualisierungen von Softwarepaketen unter Berücksichtigung von Ausstattungsmerkmalen der Hardware oder ein Self-Service zur Eigeninstallation mit Genehmigungsprozess und Verrechnung auf die Kostenstelle sind hingegen nicht die Welt der Suite. Die Software spricht eher die Handwerker unter den Administratoren an denn die Prozessdesigner und Entwickler unter den Systembetreuern. Da sich VBS- oder C#-Programme direkt einbinden lassen, könnte aber auch die zuletzt genannte Gruppe mit der Suite erfolgreich arbeiten. *(jp)*

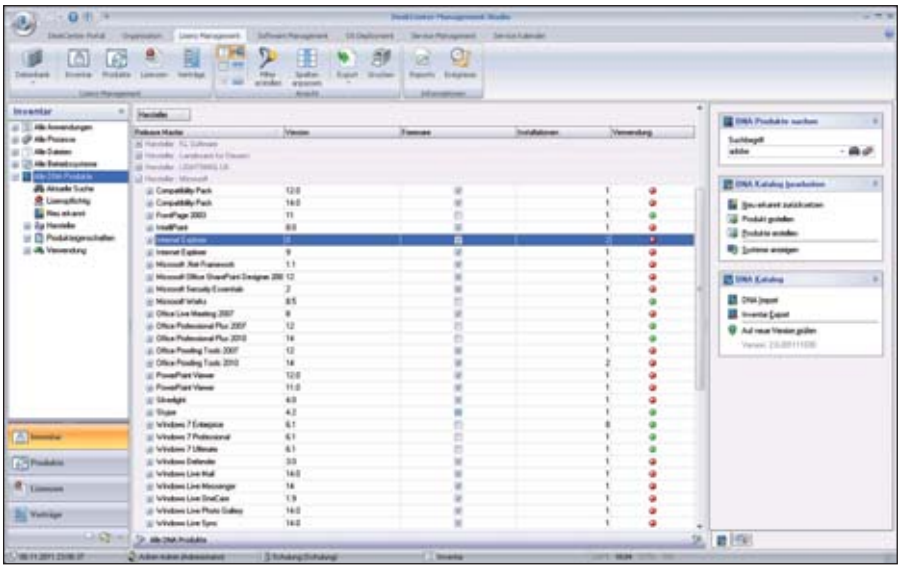


Bild 3: Dank der DNA-Lizenz/Software-Datenbank ermittelt DeskCenter sehr genau das Softwareinventar und bringt dieses mit Lizenzinformationen in Einklang

Produkt

Software für das System- und Lifecycle-Management Windows-basierter Client-PCs.

Hersteller

DeskCenter Solutions AG
www.deskcenter.com

Preis

Je nach gewählten Funktionen und Modulen variieren die Preise. Die Basislizenz kostet 12,95 Euro pro Clientrechner, Betriebssystemverteilung ebenfalls 12,95 Euro, Softwareverteilung 14,95 Euro, Software-Asset-Management 11,95 Euro.

Alternativ empfiehlt sich die Nutzung des "Enterprise Pakets" zu 65 Euro je Clientlizenz, in diesem Paket kommt es zu einem 30 Prozent Preisnachlass im Vergleich zu den Einzellizenzen.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Einrichtung und Bedienung	9
Betriebssystemverteilung	7
Softwareverteilung	7
Lizenz-Analyse	9
Inventar- & Asset-Management	8

Dieses Produkt eignet sich

optimal für Unternehmen des Mittelstands, die eine schnell einsetzbare und auf das Wesentliche fokussierte Systems Management-Lösung suchen.

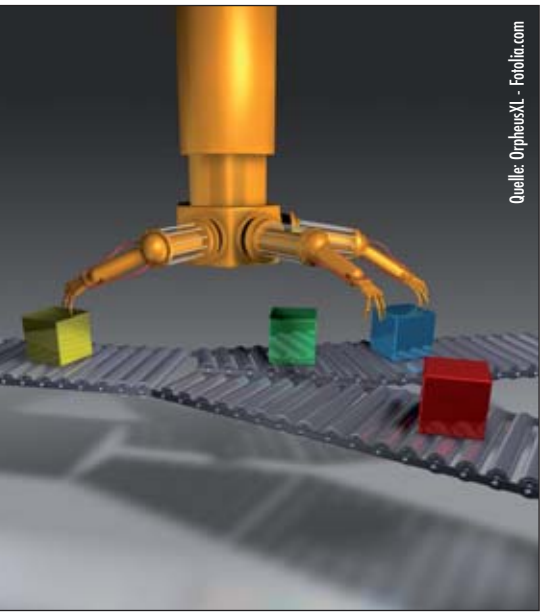
bedingt für Firmen, die schon ein Systems Management im Einsatz haben und nur einzelne Bestandteile suchen.

nicht für kleine Unternehmen, bei denen es kaum zu Änderungen in der Software- und Betriebssystemausstattung kommt.

DeskCenter Management Suite 9.3

Im Test: baramundi Management Suite 8.5

Hilfreicher Lückenfüller


Quelle: OrpheusXL - Fotolia.com

von Thomas Bär

Es vergeht kein Tag, an dem nicht von Schwachstellen in bestimmten Applikationen, Betriebssystemen oder Plug-Ins die Rede ist. Für den Administrator keine leichte Aufgabe, in einer heterogenen und komplexen Umgebung Schritt zu halten. Abhilfe verspricht hier die baramundi Management Suite, die in der neuen Version 8.5 IT-Verantwortlichen ein Modul zum Patch-Management bietet. IT-Administrator hat sich angeschaut, was die Software im Bereich Patchverteilung leistet.

Software auf dem neuesten Stand zu halten, ist seit jeher eine wichtige Systemmanagement-Aufgabe. Die Management Suite 8.5 von baramundi, kurz bMS 8.5, will daher als System- und Client-Lifecycle-Management-Lösung alle aktuellen IT-Management-Anforderungen von Administratoren abdecken. Von der Betriebssystem-Ferninstallation über Software-Verteilung, Bereitstellung von Geräte- und Systemtreibern, Fernwartung, Inventarisierung, Kiosk-Modus für die selbstständige Softwareinstallation durch Benutzer, Zugriffskontrolle für Geräte, Sicherung und Wiederherstellung von Benutzer-Daten bis hin zur Verwaltung von Citrix-Terminalservern wird die Administration in einer einzigen Konsole zusammengefasst. Der Vorteil einer integrierten Systemmanagement-Lösung wie der bMS 8.5 für den Administrator liegt auf der Hand. Er muss sich nur mit einer einzigen Software auseinandersetzen und beispielsweise können Inventardaten 1:1 für Support- und Administrationsaufgaben weitergenutzt werden, ohne sie erneut erfassen zu müssen.

Updates flexibel und punktgenau

Wie die meisten System- und Client-Lifecycle-Management-Lösungen am Markt deckt auch baramundi beim Patch-Management in erster Linie Microsoft-Produkte ab. Da Microsoft-Programme und insbesondere Windows in beinahe allen Unternehmen zum Einsatz kommen, ist die Integration verständlich und notwendig. Doch im Vergleich zum WSUS von Microsoft bietet das baramundi Patch-Management die Möglichkeit, definierbare Regelwerke einzupflegen, nach denen die Aktualisierungen gesteuert werden. Der Administrator entscheidet somit selbst, wann welche Updates, die einen Neustart der Maschine erfordern, tatsächlich installiert werden. Die Installationen laufen im Hintergrund ab und die benötigten Neustarts werden durch den Agenten auf dem Client zusammengefasst, was die Installationsdauer verkürzt.

Je nach Einstellung ist es möglich, dass das baramundi Patch-Management vollautomatisch arbeitet, ohne dass der Administrator eingreifen muss. In der Praxis ist eine genauere Steuerung jedoch meist sinnvoller. Während das Synchronisieren von Einstellungen und Updates bei Microsoft WSUS ausschließlich über OUs möglich ist, kann der Administrator bei der baramundi-Suite per Drag & Drop in der Oberfläche festlegen, welche Systeme gepatcht werden sollen. Dieses Feature ist ein deutlicher Unterschied zur Standardlösung von Microsoft, bei der Administratoren nur sehr wenige Möglichkeiten

Bild 1: Im Patch-Management der baramundi Management Suite 8.5 ist die Verteilung von sicherheitsrelevanten Aktualisierungen von Microsoft direkt integriert

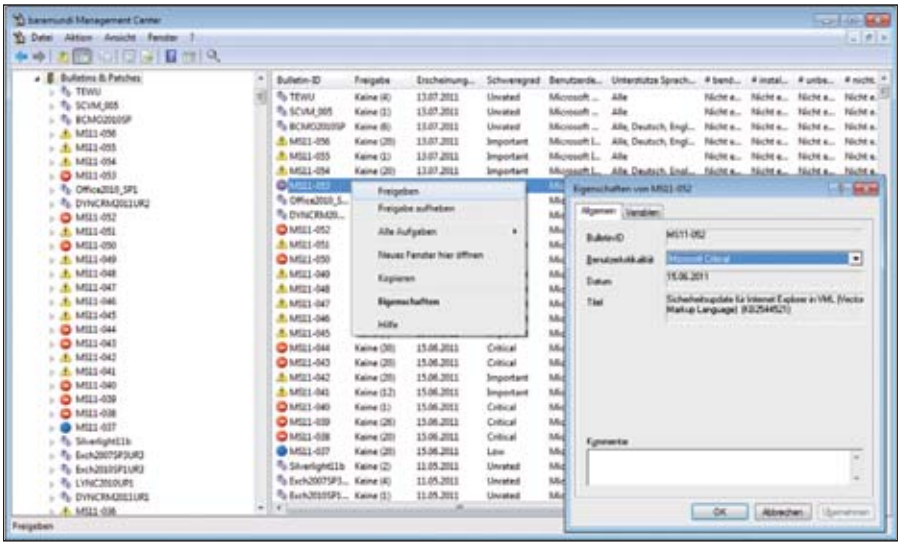


Bild 2: Die allgemeinen Patch-Informationen von Microsoft sind auch in der baramundi-Software direkt sichtbar

des Einwirkens haben. Beim Patch-Management mit baramundi lassen sich Patches gezielt für einzelne Rechner oder Gruppen, für ganze Domänen oder Standorte verteilen – auf Wunsch auch sofort.

Übersichtliche Patchverwaltung mit Einschränkungen

Was nützt die beste Software zur Verteilung von Updates, wenn sich der Administrator nicht sicher sein kann, dass der gewünschte Status der Client-PCs auch erreicht wurde. Im Register "Patch Baselines" des baramundi-Moduls findet sich eine Auflistung mit dem Erfüllungsgrad der Verteilung. Zur weiteren Verarbeitung oder zur grafischen Darstellung kann der Benutzer die einzelnen Zusammenfassungen wie die Anzahl von Bulletin-Meldungen, die noch nicht zugeordnet wurden, in ein Excel-Sheet exportieren. Welche Patches bereits durch welche Baseline verteilt werden und welche Sicherheits-Bulletins noch ohne Zuweisung sind, ist ebenfalls in dieser Ansicht für den Administrator einfach zu erkennen.

Alle Informationen, die Microsoft im Rahmen der Update-Bereitstellung einstellt, kann der Administrator auch bei baramundi über den Kontextbefehl "Eigenschaften" zu jedem Bulletin beziehungsweise Patch aufrufen. Die hier genannten Bezeichnungen wie "Knowledge Base" oder Bulletin-ID entsprechen ebenfalls der üblichen Beschriftung von Microsoft, was die Suche im Internet nach Kommentaren der Community weiter ermöglicht.

Leider beschränkt sich die bMS ausschließlich auf sicherheitsrelevante Patches von Microsoft. Gewöhnliche Updates wie das "Microsoft Office File Validation Add-In (KB 2501584)", das vor einigen Wochen zur Verlangsamung von Microsoft Excel 2003 beim Öffnen von Dateien im Terminal-Server-Umfeld führte, lassen sich mit der baramundi-Variante überhaupt nicht verteilen. Da nützt es wenig, wenn die Deinstallationsfähigkeiten von baramundi den Standard-Bordmitteln von Microsoft überlegen sind.

Mit Blick in das überaus aktive baramundi-Anwenderforum wird klar, dass Administratoren WSUS und bMS Patch-Management im Parallelbetrieb verwenden, sich aber durchaus die ausschließliche Verteilung über die baramundi-Suite wünschen würden. Mit einer kleinen AutoIT-Applikation hat ein Administrator den Vorgang von WSUS über den "ShutdownJobExecutor" miteinander verbunden, so dass WSUS-Updates stets beim Herunterfahren angestoßen werden. Baramundi lädt die über den Microsoft Update Service bereitgestellten Patches nicht einfach 1:1 in die baramundi Management Suite. Die Software-Aktualisierungen werden zunächst durch Mitarbeiter im Rahmen des Qualitätsmanagements geprüft und anschließend freigegeben. Somit kommt es stets zu einer zeitlichen Verzögerung, bis ein Patch zur Verfügung steht. Hinweise auf Probleme mit verspätet verarbeiteten Patches konnten wir allerdings weder im Benutzer-Forum noch im Internet entdecken.

Hilfreiche Nutzungsdaten

Aktualisiert werden muss natürlich zunächst die Software, die auch intensiv von den Anwendern oder im Serverumfeld genutzt wird. Eine Sicherheitslücke in einer ungenutzten Spezialsoftware ist als weitaus weniger dramatisch einzustufen als ein Bug in einem tagtäglich von hunderten Mitarbeitern genutzten Browser. Natürlich hat der Administrator ein Gefühl dafür, welche Programme oft und intensiver genutzt werden. Aber mit Sicherheit sagen kann es auch der beste Admin nicht. In einigen Systems- und Client-Management-Lösungen gibt es daher ein Programm, das die Softwarenutzungsaktivitäten der Anwender in einer Datenbank protokolliert. Ein solches Feature mit dem Namen "Application Usage Tracking" (AUT) gibt es auch für die baramundi Management Suite. Üblicherweise wird AUT genutzt, um die Softwarelizenzkosten im Unternehmen zu senken, indem ungenutzte Software identifiziert wird. Aus dem Blickwinkel der Sicherheit betrachtet eignen sich die Reports jedoch auch dazu, festzulegen, welche Programme am ehesten aktualisiert werden müssen, sofern neue Versionen vorgestellt werden.

Datenschutzrechtliche Bedenken

Ein Client-Computer, der zahlreiche Daten über seine eigene Verwendung an eine zentrale Datenbank meldet, und die Tatsache, dass üblicherweise ein PC sehr genau einem Benutzer zugeordnet werden kann, ruft schnell Datenschützer und Betriebs- beziehungsweise Personalräte auf den Plan. Die Analyse eines Arbeitsplatzes durch den Vorgesetzten oder Administrator ohne die Zustimmung des Mitarbeiters verstößt bereits gegen das Datenschutzgesetz, auch wenn die Beteiligten stets versichern wer-

Systemvoraussetzungen

Standard-Server mit aktueller CPU, 1,5 GByte Speicher, ausreichend Festplattenspeicher für Software-Pakete und Patches. Windows-Clients ab der Version 2000. Das Modul baramundi Patch-Management unterstützt die jeweils marktübliche Palette an Microsoft-Betriebssystemen, beginnend bei Windows 2000, XP über Server 2003, Vista und Server 2008, Windows 7 und die jüngsten Windows Server 2008 R2. Sofern eine 64-Bit-Edition vorliegt, so unterstützt baramundi auch diese, neben der Standard-x86-Ausprägung.

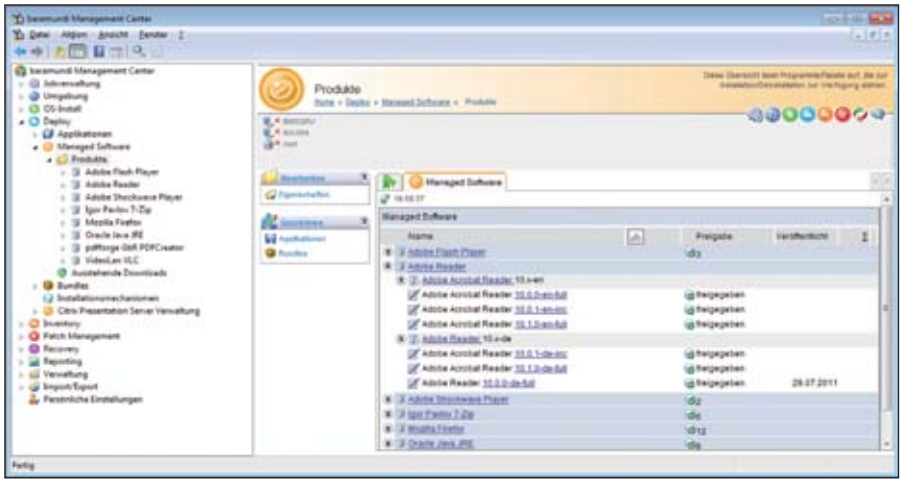


Bild 3: Managed Software – fertig konfektionierte Softwarepakete von baramundi entlasten den Administrator und stellen ebenfalls eine Form der Aktualisierung dar

den, dass alles in guter Absicht und ohne negative Auswirkungen für den Betroffenen verlaufen wird. Um dieser Problematik von Haus aus zu entgehen, lassen sich die gesammelten Daten bei AUT nur eingeschränkt darstellen. So ist beispielsweise das Datum der tatsächlichen letzten Nutzung für den Administrator nicht ersichtlich. Reports wie "Nicht genutzte Applikationen" berücksichtigen, je nach Konfiguration, einen großen Zeitraum wie 30 bis 90 Tage.

Eine missbräuchliche Nutzung der Daten – beispielsweise eine unerlaubte Leistungsmessung durch den Vorgesetzten – ist bei einer längeren Zeitspanne nicht möglich und Detailinformationen wie Tagesarbeitszeit und Zeitpunkt der Nutzung werden nicht gespeichert. Wird die Mitarbeitervertretung im Unternehmen frühzeitig über die Möglichkeiten von AUT in Kenntnis gesetzt und die Parameter gemeinsam bestimmt, dürfte es auch mit den Daten für eine effektive Software-Aktualisierung keine Probleme geben.

Vorgefertigte Pakete zur Softwareverteilung

Neben dem klassischen Patch-Management sind auch weitere Komponenten der baramundi Management Suite direkt oder indirekt mit der Aktualisierung von Programmen im Unternehmen betraut. Erst mit der aktuellen Version 8.5 stellte baramundi im Sommer dieses Jahres eine Neuerung vor: Managed Software. Dahinter verbirgt sich die Bereitstellung von weit verbreiteten Programmen, die bei der Mehrzahl der Kunden sowieso zum Einsatz kommen dürften. Der Hersteller liefert diese Software fertig als Paket aus und hat die Verteilungsmechanismen der Sammlung bereits im Vorfeld geprüft. Faktisch dürfte sich bisher jeder Administrator mit der Erstellung von Paketen für Java, Acrobat Reader oder Mozilla Firefox in der bMS auseinandergesetzt haben.

Diese Aufgabenstellung entfällt nun für Administratoren, die Software mit der bMS 8.5 verteilen. Derzeit bietet der Hersteller die Anwendungen Adobe Reader, Flash Player, Shockwave Player, Mozilla Firefox, Sun Java JRE und PDFCreator als fertige Pakete zum Download an. Wichtige Details, wie beispielsweise die Einstellungen dahingehend, dass diese Programme nicht versuchen, über die üblichen Wege mit dem Update-System ihres Herstellers in Verbindung zu treten, haben die Paket-Designer von baramundi bereits berücksichtigt. Der Flash-Player beispielsweise, der als Managed-Software über bMS verteilt wurde, bittet somit nicht regelmäßig um die Freigabe zum Update durch den Benutzer. Vielmehr automatisiert, überprüft und testet baramundi die Softwarepakete und stellt diese den Administratoren über die Online-Datenbank zum automatisierten Verteilen bereit. Die Pakete eignen sich sowohl zur Erstinstallation, zum Update und zur Deinstallation und sind jeweils in den Sprachen Deutsch und Englisch sowie für alle von der bMS unterstützten Windows-Plattformen verfügbar. Microsofts Sicherheitsupdates werden weiterhin über das baramundi Patch-Management-Modul verwaltet – hier wird der Hersteller keine Änderung vornehmen. Weitere Software-Produkte möchte baramundi als Managed Software in naher Zukunft je nach Kundenwunsch anbieten.

Smarter Automatismus

Bei genauer Betrachtung ist das Patch-Management das gezielte Ausbringen von Korrekturen in Form kleiner Programmänderungen. Software-Hersteller generieren für ihre Programme Patches und stellen diese zum Download bereit. Während Microsoft, Apple oder Oracle hierfür ganze Aktualisierungsmechanismen entwickelt haben, so gibt es viele kleinere Softwarelösungen, bei denen der Austausch einer Datei und eine Änderung in der Registry den "Patch" an sich darstellen. Für diese Programme – die nicht selten speziell für ein Unternehmen oder in Eigenregie entwickelt wurden – bietet sich ebenfalls die Softwareverteilung von baramundi an.

Mit dem baramundi Package Studio erzeugt der Administrator Transformationsdateien (MST), mit denen sich jedes MSI anpassen lässt. Alte Setups können bei Bedarf in das modernere Windows Installer-Format über-

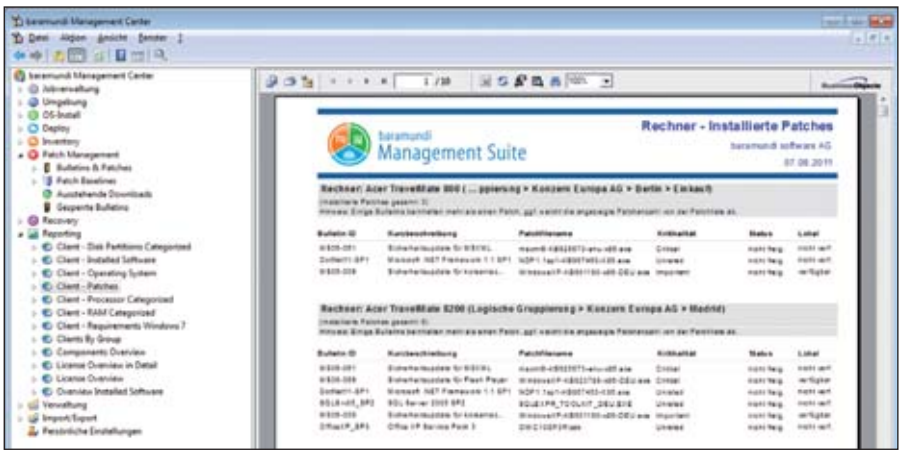


Bild 4: Welchen Client-Systemen fehlen welche Patches und warum – ein Report gibt im Klartext Auskunft

führt werden oder die MSI-Pakete direkt, beispielsweise für einen Patch-Vorgang, erstellt werden. Das baramundi Package Studio basiert auf dem bekannten AdminStudio von Flexera Software, das für seine Repackage-Fähigkeiten bekannt ist. Installationsschritte werden dabei während des Setups aufgezeichnet und machen die aufwendige Erstellung von Snapshots überflüssig.

Neben der Paket-Erstellung gibt es bei baramundi noch eine weitere Technik, die sich sehr gut für Software-Aktualisierungen einsetzen lässt: baramundi Automate. Mit dieser Automatisierung erstellt der Administrator so genannte Response-Dateien für automatische Installationen, Konfigurationen oder sonstige automatisierte administrative Aufgaben über eine grafische Skriptsprache. Praktisch verhält sich eine solche Automate-Datei wie ein Vorgang, der durch den Benutzer selbst durchgeführt wird. Problematisch könnte sich in diesem Zusammenspiel allerdings die User Account Control (UAC) unter Windows Vista oder Windows 7 zeigen. Doch auch daran haben die Entwickler gedacht. So wird die UAC, die für die Erhöhung der Sicherheit bei Windows zuständig ist, temporär deaktiviert und das Keyboard und die Maus des Benutzers auf Wunsch blockiert, während das Skript abläuft.

Selbst nichtstandardisierte Oberflächen wie in Java-Applikationen lassen sich über baramundi Automate steuern. Zur Oberflächenautomatisierung greift die Software üblicherweise auf die Windows-API zu – die Programmierschnittstelle, die es Entwicklern erlaubt, Software für Windows zu entwickeln. Für Automate-Benutzer sind hier ausschließlich die Dialogfensterelemente von Bedeutung. Für diese werden die Namen der Fenster, Rahmen oder Controlls automatisch ermittelt. Eine zweite Schnittstelle ist die MSAA (Microsoft Active Accessibility), diese wurde in der jüngeren Vergangenheit für die Automatisierung optimiert und wird ebenfalls von baramundi für die Kommunikation mit der Benutzeroberfläche genutzt.

Die in der baramundi Management Suite gebräuchlichen Variablen stehen in Automate ebenfalls zur Verfügung. So lassen sich Sprachvarianten, besondere Client-Einstellungen oder Setup-Pfade pro Client dynamisch aus Variablen generieren. Der Befehlsumfang des baramundi Automation Studios umfasst Datei-Operationen, Shortcuts erstellen, Registry-Werte setzen und bearbeiten, Dienste steuern, Benutzer und Benutzergruppen anlegen, löschen und bearbeiten und Freigaben erstellen, löschen oder verbinden. Die Befehle werden dabei nicht eingegeben, sondern per Drag & Drop aus der Auswahl in den Skriptablauf gezogen.

Bandbreitensteuerung gegen Datenstau

Im April 2011 gab baramundi bekannt, dass in der Lösung nun der so genannte "baramundi Background Transfer" zur Bandbreitensteuerung zum Einsatz kommt. Hierbei handelt es sich um die von Microsoft als BITS bekannte Technik, die dafür sorgt, dass Updates und Down-loads von Applikationen mit einer geringeren Priorität transportiert werden als die Nutzdaten der Anwender. Baramundi entkoppelt zudem die Übertragung der für eine Installation notwendigen Dateien von der Einrichtung selbst.

Der Transfer findet zunächst, für den Benutzer transparent, im Hintergrund statt. Wie viel verfügbarer Restspeicherplatz auf dem Zielsystem zur Verfügung steht, sieht der Administrator in der Oberfläche der bMS. Die Technik der Bandbreitensteuerung im Hintergrund wird sich insbesondere in verteilten Umgebungen mit verschiedenen Standorten und WAN-Leitungen positiv auswirken.

Fazit

Die Summe der Fähigkeiten der baramundi Management Suite macht klar, dass integrierte System- und Client-Management-Systeme dem Administrator bei der Aktualisierung der Software gute Dienste leisten können. Dank dieser Programme ist der Administrator in der Lage, die größte Schwachstelle im Netzwerk, den Client-PC und den Benutzer, mit vertretbarem zeitlichen und finanziellen Aufwand in den Griff zu bekommen. Auch ohne Fernwartungssitzung oder Vor-Ort-Einsatz kann die baramundi-Software die Aktualisierungen vornehmen. Die komplette Übernahme der WSUS-Funktionalität scheint, zumindest was die Forum-Benutzer angeht, auf der Kundenwunschliste zu stehen. Ohne Frage ist es für den Administrator zudem eine Vereinfachung, wenn er sich nicht mehr selbst um die Paketierung für eine Softwareverteilung kümmern muss – keine Anpassungen des Installationsvorgangs für unterschiedliche Windows-Versionen, kein aufwändiges Testen des Pakets und keine Erprobung der Deinstallation. Ein weiterer Pluspunkt für die bMS. *(dr)*

Produkt
Management Suite zur Patch- und Softwareverteilung.

Hersteller
Baramundi Software
www.baramundi.de

Preis
Abhängig von gewählten Modulen und Anzahl beginnend ab 9,70 Euro bis 22,50 Euro pro Client und Jahr. Baramundi bietet seine Lösung als Suite oder als einzelne Komponenten an. Es wird nicht nach Servern, sondern in erster Linie nach Arbeitsplätzen lizenziert.

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

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

Funktionsumfang der Suite	7
Patch-Management	6
Managed Software	8
Softwareverteilung	7
Paketierung und Automatisierung	7

Dieses Produkt eignet sich

optimal für Unternehmen, die viele Software-Aktualisierungen selbst erstellen müssen und eine große Anzahl von Windows-Clients zu versorgen haben.

bedingt für Unternehmen, die bereits mit Microsoft WSUS alle Sicherheitsanforderungen im Bereich Patching abdecken können.

nicht für kleine Unternehmen oder Firmen, die bereits eine andere Client-Lifecycle-Management-Software im Einsatz haben.

baramundi Management Suite 8.5

Bestellen Sie jetzt

das IT-Administrator

Sonderheft 1/2012!

180 Seiten Praxis-Know-how rund um das Thema

Exchange 2010

Migration, Betrieb und Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft 1/2012 für € 24,90. Nichtabonnenten zahlen € 29,90. IT-Administrator All-Inclusive Abonnenten "zahlen" für Sonderhefte nur € 19,90 - diese sind im Abonnement dann automatisch enthalten. Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.*

Liefertermin:
Ende März 2012

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 I/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0112

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

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

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

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

Im Test: LogMeIn Pro 4.1

Fernzugriff nach Maß


Quelle: 123RF

von Jürgen Heyer

Der klassische Fernzugriff ist für viele Administratoren das Mittel der Wahl, wenn es um die Arbeit mit Servern oder Wartung und Support von Client-Rechnern geht. Klassische Lösungen wie Remote Desktop bieten jedoch nur einen begrenzten Funktionsumfang und dienen eher dem Zugriff über ein lokales Netzwerk. LogMeIn Pro verspricht hier einen wesentlich flexibleren Fernzugriff auch über das Internet. Im Test musste die Software ihr Können beweisen.

Solange sich ein Konsolenfernzugriff auf das Intranet beschränkt, ist die Windows-Standardfunktion "Remote Desktop" für den Administrator ein durchaus adäquates Mittel für die Verwaltung von Clients und Servern. Für das Monitoring stehen zudem in der Regel diverse zentrale Tools bereit, die neben den üblichen Aufgaben wie der Überwachung der Verfügbarkeit zum Beispiel auch die Softwareverteilung übernehmen. Die Erreichbarkeit im eigenen Netz ist dank einer internen Namensauflösung oder klar strukturierter IP-Adressen unproblematisch. Anders sieht die Situation aus, wenn der Zugriff über das Internet erfolgt, ohne dass ein eigener VPN-Tunnel hierfür zur Verfügung steht. Dann bietet sich ein Dienst wie LogMeIn Pro an, der die Verbindungen steuert und die Verschlüsselung sowie das Routing übernimmt. LogMeIn betreibt dazu eine Internet-weite Gateway-Plattform, auf der sich jeder Kunde registrieren muss. Wer sich bereits mit dem Thema beschäftigt hat, weiß, dass es neben LogMeIn noch eine ganze Reihe anderer Anbieter von Fernsteuerdiensten via Internet gibt. Ein entscheidender Vorteil von LogMeIn Pro besteht im großen Funktionsumfang des Produktes an sich und darin, dass LogMeIn darüber hinaus noch andere Tools im Portfolio hat, die sich je nach Bedarf ergänzen und kombinieren lassen.

Zugriff aktiv oder passiv

LogMeIn Pro vereint zwei grundlegende Fernsteuerungsverfahren in sich. Die eine Arbeitsweise besteht darin, dass der Dienst analog zu Remote Desktop den Fernzugriff auf Systeme (Hosts) quasi im eigenen Zuständigkeitsbereich, also mit bekannten Anmeldeparametern, aber an einem beliebigen Ort im Internet ermöglicht. Das kann ein Server in einer Außenstelle ebenso sein wie ein Arbeitsplatz-PC, den jemand vom Home Office aus erreichen möchte. Hierbei muss sich ein Administrator oder Anwender über einen Account auf einer zentralen Webkonsole bei LogMeIn einloggen. Von dort aus kann er dann alle Hostsysteme erreichen, die mittels dieses Accounts installiert wurden, und sich dort anmelden, sofern er systemseitig die Berechtigung besitzt.

Beim zweiten Verfahren fungiert der Host – egal ob Server oder Arbeitsplatz-PC –

Bild 1: Das Dashboard fasst die wichtigsten Informationen auf einer Seite zusammen, ein Klick in einen Bereich verzweigt zu den Detailinformationen

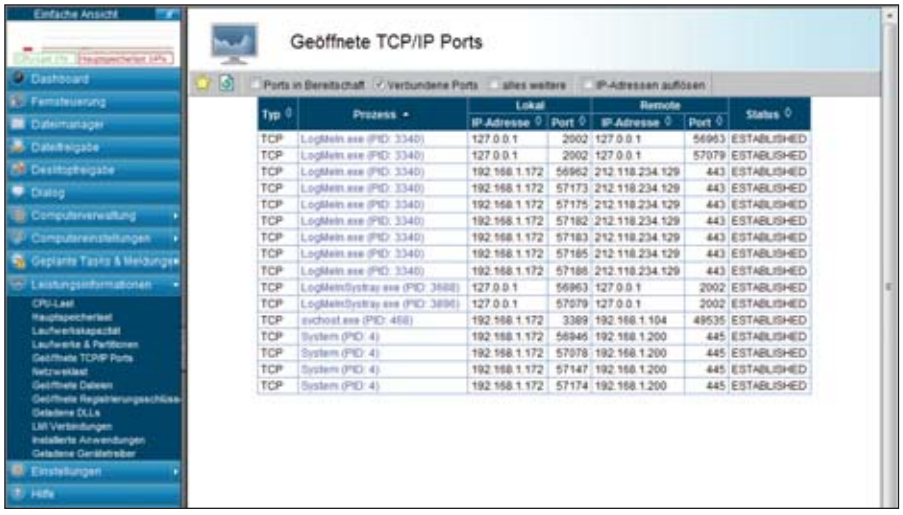


Bild 2: LogMeIn Pro liefert umfassende Monitoring- und Leistungsinformationen, darunter auch die offenen TCP/IP-Ports

als Initiator, indem ein dort angemeldeter Administrator oder Anwender den Desktop für eine beliebige Gegenstelle freigibt. Die Übermittlung der Freigabeinformationen erfolgt in der Regel per E-Mail in Form einer URL. Die Freigabe kann entweder nur zur Betrachtung beispielsweise für Schulungszwecke oder inklusive Fernsteuerung für den Supportfall genutzt werden. Dazu später mehr. Eine deutliche Arbeitsvereinfachung bietet LogMeIn Pro dadurch, dass neben der reinen Fernsteuerung noch diverse Zusatzfeatures zur Verfügung stehen. Dies sind ein Dateimanager, eine gezielte Dateifreigabe und diverse Monitoring- sowie Management-Funktionen, die bereits einen guten Überblick über ein System geben, statt dass sich ein Administrator jedes Mal auf den Desktop aufschalten muss, um über die einzelnen Bordmittel mühsam Systeminformationen auszulesen.

Erstkonfiguration mit kleinem Stolperstein

Der Einstieg in LogMeIn Pro ist denkbar einfach und beginnt mit einer Registrierung auf der LogMeIn-Homepage mit einer E-Mailadresse und der Festlegung eines Passwortes. Abgeschlossen wird die Registrierung durch Bestätigung eines Links, den LogMeIn anschließend an die angegebene E-Mailadresse schickt. Es besteht nun die Möglichkeit, einen Agenten herunterzuladen, was dann sinnvoll ist, wenn das genutzte System zukünftig fernsteuerbar sein soll. Nach der Installation des Agenten findet der Administrator in der Taskleiste ein Icon, über das er eine übersichtliche GUI mit mehreren Registern öffnet. Hier sollte er sich zuerst mit den Konfigurationsoptionen beschäftigen, aufgeteilt auf die drei Register "Allgemein", "Sicherheit" und "Erweitert", um das Verhalten des Agenten auf Verbindungsanfragen einzustellen.

Auf der Seite "Allgemein" lassen sich diverse Grundeinstellungen ändern, wie beispielsweise, ob bei einer Interaktion die Eingaben des Hostbenutzers oder des Gastes Vorrang haben. Auch lässt sich hier vorgeben, ob und in welchem Umfang der Hostbenutzer bei einer Aufschaltung zustimmen muss, sowie was passiert, wenn der Hostbenutzer nicht reagiert. Unübersichtlich empfanden wir, dass es nicht klar ist, für welchen Fernsteuermodus die Einstellungen tatsächlich greifen. So gelten die Optionen zur Zustimmung des hostseitigen Benutzers nur dann, wenn der Zugriff vom eingangs erwähnten Webportal aus erfolgt. Bei einer vom Host aus initiierten Desktopfreigabe per E-Mail und Link muss die dort sitzende Person zwingend zustimmen und ein Zugriff ist auch nur dann möglich, wenn jemand am Host angemeldet ist.

Auf der Seite "Sicherheit" findet sich eine Schaltfläche für die detaillierte Benutzersteuerung. In dieser können für lokale und Domänenbenutzer explizit Detailrechte auf die einzelnen Funktionen von LogMeIn (unter anderem Anmelden, Konfiguration, Dateisystem, Fernsteuerung, Whiteboard) festgelegt werden. Auf diese Weise lassen sich auch die Einstellungen schützen, so dass ein Administrator die LogMeIn-Konfiguration für den späteren Benutzer unveränderbar vorschreiben kann. Per Standard ist für Administratoren Vollzugriff eingerichtet.

Eine zusätzliche Sicherheitsebene lässt sich über ein "Persönliches Passwort" einrichten. Dieses ist es bei einer Remoteanmeldung dann zwingend einzugeben. Darüber hinaus unterstützt LogMeIn den Schutz mittels RSA SecurID ebenso wie die IP-Adressfilterung. Durch die Verwendung von Profilen lassen sich einfach verschiedene Regelsets festlegen, die je nach Aktivierung zur Anwendung kommen oder nicht. In einem Profil lassen sich mehrere Regeln eintragen, die nacheinander abgearbeitet werden. IP-Adressen und -Bereiche können dabei explizit erlaubt oder verboten werden. Weiterhin ist ein Schutz vor Denial-of-Service- und Authentisierungsangriffen implementiert. Das Registerblatt "Erweitert" enthält schließlich noch diverse Detaileinstellungen wie die Vorgaben bei einer Proxy-Nutzung, die Angabe des Ablageortes für die Logdateien und die Möglichkeit, eine Fernsteuersitzung aufzuzeichnen, falls dies für Revisionszwecke erforderlich ist.

Einladungen per E-Mail verteilen Dateien

Wie erwähnt kann der Administrator vom Host aus über den Agenten selbständig Verbindungen initiieren. Hierbei handelt es sich um die Datei- und Desktopfreigabe zu einem beliebigen anderen System im Internet. Dabei gibt der Anwender seinen aktuellen Desktop entweder nur zur Betrachtung oder zur Bedienung durch den entfernten Benutzer frei. Die Dateifreigabe ermöglicht es einem Benutzer, aus der Ferne einzelne Dateien herunterzuladen. Das eignet sich weniger für die Übertragung großer Datenmengen, reicht aber für die Übermittlung einer Präsentation oder eines Treiberpakets. Sollen mehrere Dateien auf einmal freigegeben werden, so empfiehlt es sich, diese in eine Datei zu packen, da es nicht vorgesehen ist, ganze Ordner freizugeben. An sich sind derartige Freigaben nichts Besonderes. Ansprechend und einfach ist aber die Art, in der das geschieht – nämlich per E-Mail. So ver-

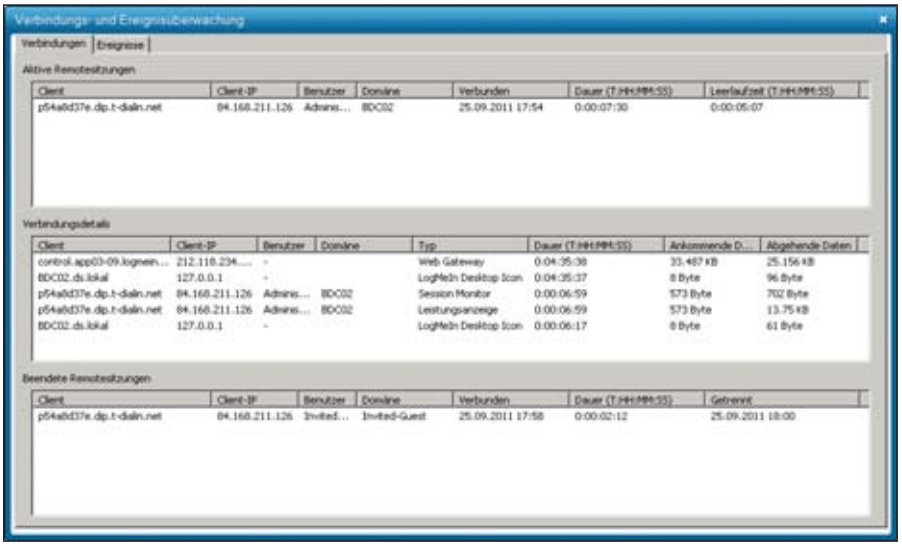


Bild 3: Der Agent bietet eine genaue Übersicht über die aktiven sowie die beendeten Remotesitzungen samt der Verbindungsdetails

schickt der Benutzer eine Einladung entweder über einen Mailserver von LogMeIn oder über einen eigenen Server.

Für den zweiten Fall generiert der Agent einen Link, den der Anwender in seine E-Mail kopieren muss. Bei Nutzung der integrierten Mailfunktion gibt er nur die Ziel-Mailadresse ein und gegebenenfalls einen Anschreiben-Text. Der Gast klickt einfach auf den Link in der erhaltenen Mail, um zur Datei- oder Desktopfreigabe zu gelangen. Die Datei kann sofort heruntergeladen werden, bei der Desktopfreigabe muss der Hostanwender den Zugriff noch bestätigen. Da sich auf Gastseite alles im Browser abspielt, ist dort außer einem ActiveX Add-On nichts zu installieren. Diese Funktion empfanden wir im Test als komfortabel gelöst. Der aktive Remotezugriff auf die Desktopfreigabe eines Hosts wird für den Anwender am Rechner unübersehbar durch einen halbtransparenten Hinweis signalisiert. Durch einen Klick auf die darin enthaltene "Schließen"-Schaltfläche kann er die Verbindung jederzeit beenden, sollten ihm die Aktionen des Remotebenutzers missfallen.

Gut gefallen hat uns, dass bei beiden Freigabearten zwingend eine Dauer anzugeben ist, in der der Gast die Einladung annehmen muss. Dadurch besteht nicht die Gefahr, dass die Freigaben unbegrenzt lange nutzbar bleiben und womöglich in Vergessenheit geraten. Bei der Dateifreigabe kann der Anwender vorgeben, wie oft die Datei heruntergeladen werden darf. Auf den Registerblättern für die Einrichtung der beiden Freigaben befindet sich jeweils eine Übersicht über die letzten zehn Einladungen mit Verfallsdatum und die Information, ob die Einladung noch aktiv ist und wie oft sie benutzt wurde. Abgelaufene Einladungen werden in rot dargestellt, so dass sich leicht erkennen lässt, ob noch etwas aktiv ist.

Zusätzlich zu diesen Daten liefert auch das Registerblatt "Überblick" Informationen darüber, wie viele Einladungen aktuell aktiv sind und ob ein Remotebenutzer angemeldet ist. Beim Anklicken einer Einladung werden weitere Details angezeigt wie auch der dazugehörige Link, so dass es möglich ist, für bestehende Freigaben nochmals Einladungen zu verschicken. Bei der Dateifreigabe ist angegeben, ob und wie oft die Datei schon heruntergeladen wurde. Über das Register "Optionen" sind die zuvor erwähnten Einstellungen erreichbar und darüber hinaus lässt sich hier eine detaillierte Verbindungs- und Ereignisüberwachung aufrufen. Übersichtlich wird angezeigt, welche Remotesitzungen gerade aktiv sind und welche beendet wurden. Auslesen lassen sich die Verbindungsdetails mit IP-Adressen, Dauer und ankommenden sowie abgehenden Datenmengen.

Komfortables Internet-Portal für den Remote-Zugriff

Neben der beschriebenen Datei- und Desktopfreigabe zu einem beliebigen Gast beherrscht LogMeIn Pro auch einen Remotezugriff von einem zentralen Web-Portal auf mehrere Systeme. Diese Vorgehensweise deckt den Bedarf für eine zentrale Administration oder einen zentralen Helpdesk ab. Mit der beschriebenen Registrierung wird ein Portalzugriff bei LogMeIn angelegt. Alle Systeme, die über den zugehörigen Benutzeraccount mit dem Agenten bestückt werden, erscheinen auf diesem Portal und lassen sich dort für einen Remotezugriff anwählen. Dabei stehen für den Direkteinstieg neben dem Hauptpunkt "Fernsteuerung" noch die Optionen "Hauptmenü", "Dashboard", "Datei-Manager" und "Updates" zur Verfügung.

Erforderlich ist in jedem Fall zunächst eine reguläre Anmeldung entweder mit einem lokalen oder Domänenbenutzer. Der Remotebenutzer muss also die passenden Credentials kennen. Damit gelangt er auf eine Administrationskonsole für das System, die über seitliche Reiter verschiedene Optionen anbietet wie "Dashboard", "Fernsteuerung", "Dateimanager", "Dialog", "Computerverwaltung", "Computereinstellungen", "Geplante Tasks und Meldungen", "Leistungsinformationen" sowie "Einstellungen".

Zu beachten ist, dass sich die Rechte in der Konsole nach den Vorgaben in der Benutzerzugriffssteuerung von LogMeIn Pro richten. Standardmäßig haben Administratoren auf dem Host die vollen Rechte, andere Benutzer gar keine. Wird dies geändert, dann überschreiben diese Angaben die über das Active Directory vergebenen Rechte. In der Praxis bedeutet dies beispielsweise, dass ein Benutzer, der auf das Dateisystem eines Servers über das Active Directory keine oder nur eingeschränkte Zugriffsrechte hat, trotzdem über den Dateimanager von LogMeIn Pro in vollem Umfang agieren kann, wenn dies in der Zugriffssteuerung entsprechend

Systemvoraussetzungen

Windows 7, Vista, XP oder Server 2003, 2008 (alle einschließlich 64 Bit), Windows 2000 (32 Bit) sowie Mac OS 10.4 bis 10.7 auf Power-PC und Intel-basiert.

eingetragen wurde. Für den Desktopzugriff ist das unproblematisch, da hier eine zusätzliche Anmeldung auf dem System erforderlich ist. Gut ist, dass LogMeIn Pro anbietet, die Credentials der Konsolenanmeldung weiterzureichen. Damit entfällt eine erneute Eingabe. In der Praxis dürfte es auch die Regel sein, dass Konsolen- und Fernsteueranmeldung identisch sind.

Realisiert wird die Fernsteuerung als RDP-Zugriff, der Remotebenutzer schaltet sich also nicht auf den Desktop eines eventuell vor Ort arbeitenden Benutzers auf, sondern er bekommt einen eigenen. Zu beachten ist dabei die Eigentümlichkeit von Remote Desktop, dass ein Nutzer eventuell eine Sitzung übernimmt, wenn diese bereits von anderer Stelle mit gleichem Account gestartet wurde. Hinsichtlich der Fernbedienungsfunktionen gibt es einige besondere Features zu nennen. So wird Audio mit transferiert, so dass sich Ausgaben am Ferncomputer auf das Administrationssystem übertragen lassen. Auch ein Ausdruck von Ferndateien auf einem lokalen Drucker ist möglich. Schlussendlich wird Wake-on-LAN unterstützt, um einen Ferncomputer bei Bedarf auch aufwecken zu können.

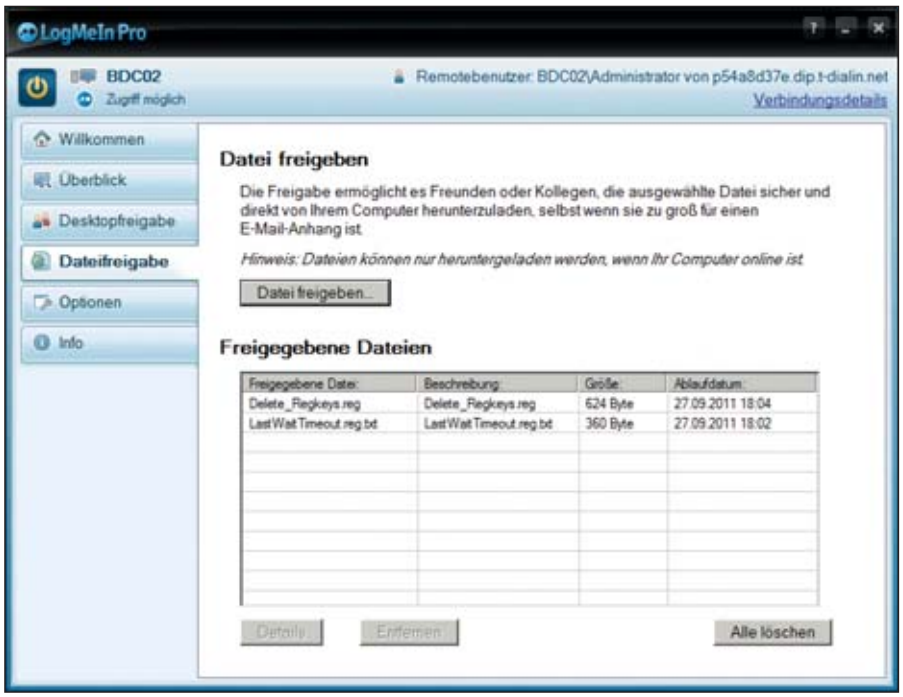


Bild 4: Alle eingerichteten Dateifreigaben werden mit Größe und Ablaufdatum übersichtlich in einer Tabelle aufgelistet

Direkt auf der Konsole kann der Administrator für jedes System die Windows Updates steuern. Ähnlich wie in der Windows-eigenen Routine werden anstehende Updates angezeigt, es lässt sich nach Updates suchen und die Installationsweise anpassen. Für die Kontrolle und das Ausführen von Updates ist es damit nicht notwendig, sich auf ein System aufschalten zu müssen.

Um den Zugriff auf das Web-Portal noch sicherer zu gestalten, gibt es die Möglichkeit, mit zusätzlichen Sicherheitscodes ähnlich der PIN beim Internet-Banking zu arbeiten. Ein Administrator kann hierzu Listen erzeugen, die achtstellige Einmal-Sicherheitscodes enthalten, oder er nutzt die Mail-Funktion, die bei jeder Anmeldung einen Code zusendet. Dies setzt allerdings normalerweise ein Smartphone oder ähnliches voraus, um die Codes jederzeit und überall empfangen zu können.

Bei der Verschlüsselung arbeitet LogMeIn Pro mit AES 256 Bit und Zertifikaten mit 2.048 Bit RSA-Schlüssel. Für eine eingehende Sicherheitsbetrachtung stellt der Anbieter ein Whitepaper [1] bereit, das die Arbeitsweise beim Verbindungsaufbau recht gut beschreibt. Für allgemeine Sicherheit sorgt auch die detaillierte Kontoüberwachung, die bei allen möglichen Ereignissen eine E-Mail an eine Adresse, normalerweise den Account des LogMeIn-Kontos, verschickt. So können beispielsweise sich häufende E-Mails wegen

fehlgeschlagener Anmeldungen auf einen Eindringversuch hindeuten.

Umfassende Überwachung und Verwaltung inbegriffen

Neben der Fernsteuerung und dem Dateimanager beinhaltet LogMeIn diverse Monitoring- und Verwaltungsfunktionen, die den großen Vorteil haben, dass sie hier in einer GUI zusammengefasst sind, während ein Administrator direkt am System an vielen Stellen nachschauen müsste. Außerdem ist der Zugriff so schneller und flüssiger.

Das Dashboard liefert auf einen Blick die wichtigsten Systeminformationen und die letzten Ereignisse, weiterhin eine Prozessliste, den Netzwerkverkehr, eine Laufwerksbelegung und noch einiges mehr. Beim Anklicken einer Rubrik werden dazu weitere Detailinformationen angezeigt, die dann auch unter den Reitern "Computerverwaltung" und "Leistungsinformationen" zu finden sind. Es wäre zu umfangreich, alle hier gebotenen Funktionen im Detail aufzulisten, aber ein Blick darauf zeigte uns schnell, dass sich typische administrative Tätigkeiten am System wie die Verwaltung lokaler Benutzer oder das Editieren der Registry bereits hier erledigen lassen, was eine zeitaufwändige Aufschaltung auf das System erspart. Bei den Leistungsinformationen liefert LogMeIn Pro nicht nur typische Daten wie die CPU- oder Hauptspeicherlast, sondern auch die geöffneten TCP/IP-Ports, geöffnete Registrierungsschlüssel und geladene DLLs sowie Gerätetreiber.

Mehrwert durch weitere Tools

Die Verwaltungskonsole von LogMeIn Pro ist durchaus dazu geeignet, die Übersicht über mehrere Computer zu behalten. Unserer Einschätzung nach sollte das für bis zu 50 Systeme recht gut funktionieren. Wächst die Anzahl aber deutlich darüber hinaus, wird es zunehmend schwerer, die Übersicht zu behalten. Dann bietet es sich an, zusätzlich LogMeIn Central zu verwenden. Die Software erlaubt eine Gruppierung von Systemen, beinhaltet eine Software-Verteilung, übernimmt das Ausrollen von Windows-Updates für viele Systeme gleichzeitig, enthält eine zusätzliche eigene Benutzerverwaltung, eine erweiterte Berichtserstattung und eine Verwaltung von Warnmeldungen. Bei einem kurzen Blick auf LogMeIn Central haben wir den Eindruck gewonnen, dass sich damit auch einige hundert Systeme verwalten lassen müssten.

Angesichts der Vielfalt an Funktionen, die LogMeIn Pro bietet, ist es wichtig, den Einsatz der Software als Administrator zu überwachen, damit die Sicherheitsinfrastruktur nicht umgangen wird. Für diesen Zweck stellt LogMeIn unter der Bezeichnung "Zugriffssteuerungstools für Systemadministratoren" kostenlos Vorlagen für Active Directory-Gruppenrichtlinien zur Kontrolle von LogMeIn bereit.

Fazit

Insgesamt macht der Agent von LogMeIn Pro einen sehr übersichtlichen Eindruck. Darüber hinaus hat er im Test durch eine intuitive Bedienung überzeugt, die das Lesen des Handbuchs erst einmal überflüssig machte. Nur bei der Konfiguration der Einstellungen sollte sich der Administrator vorher eingehender mit den Möglichkeiten befassen. Neben dem Zugriff auf Windows-Systeme gibt es auch einen Agenten für Mac OS. So deckt das Werkzeug verschiedene Fernsteuerungsszenarien via Internet ab, wie den Zugriff auf viele Clients von einer zentralen Konsole aus und die Freigabe des Desktops oder einzelner Dateien von einem Client aus an eine beliebige Gegenstelle im Internet. Damit eignet sich das Tool sowohl für die zentrale Verwaltung und als Helpdesk für die eigenen Systeme beziehungsweise Anwender als auch als Hilfsmittel für eigene Mitarbeiter, wiederum Kunden zu helfen oder neuen Interessenten etwas via Fernzugriff zu präsentieren.

Neben den Funktionen zur Fernsteuerung und Dateiübertragung hilft LogMeIn Pro auch bei der Verwaltung von Systemen durch einen schnellen Zugriff auf deren Systemeinstellungen und die Computerverwaltung. Ein weiteres Feature ist die Verwaltung der Windows Updates. Sehr einfach lässt sich kontrollieren, ob die entfernten Systeme auf aktuellem Stand sind, wobei bei Bedarf ein Updateprozess initiiert werden kann.

Letztendlich haben wir den Eindruck gewonnen, dass hier eine umfassende Funktionalität geboten wird. Gut gefallen hat uns auch die Möglichkeit, LogMeIn Pro bei Bedarf mit weiteren Produkten zu kombinieren. Vor allem die Kombination mit LogMeIn Central erscheint uns in größeren Umgebungen ab etwa 50 Systemen sehr sinnvoll. *(dr)*

[1] LogMeIn-Whitepaper zu Sicherheit
C1T11

Link-Codes

Produkt
Software zur Fernsteuerung und -wartung über das Internet.

Hersteller
LogMeIn
www.logmein.com

Preis
LogMeIn Pro gibt es im Monats- und Jahresabo. Im Jahresabo kostet eine Lizenz 53 Euro, 10 Lizenzen kosten 339 Euro. Für größere Mengen gelten Staffelpreise.

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

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

Internet-Portal	8
Fernzugriffsfunktionen	9
Monitoring	7
Systemverwaltung	7
Sicherheitsmechanismen	8

Dieses Produkt eignet sich

optimal für Firmen mit mehreren Außenstellen oder vielen Mitarbeitern, die überwiegend im Home Office arbeiten oder ständig unterwegs sind. Hier kann LogMeIn Pro die Fernwartung übernehmen und dem Helpdesk als Support-Plattform dienen.

bedingt in Umgebungen, in denen alle Netzbereiche über das Internet via VPN-Tunnel miteinander verbunden sind. Hier können in der Regel Windows-Bordmittel für die Fernwartung verwendet werden.

nicht für Unternehmen, die keine Fernsteuerung außerhalb ihres Intranets benötigen. Weiterhin gibt es keine Unterstützung für Linux.

LogMeIn Pro 4.1

Kompetentes Schnupperabo sucht neugierige Administratoren

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

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

Damit Sie sich Zeit, Nerven und Kosten sparen.

Teamwork in Bestform. Überzeugen Sie sich selbst!

6 Monate lesen

3 Monate bezahlen

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

Im Test: AppSense Application Manager 8.3

Schlüssel zum Programmstart

von Jürgen Heyer

Einheitliche Desktops an Thin und Fat Clients sowie im VDI- und Terminalserver-Umfeld helfen durch einfacheren Support und weniger Pflegeaufwand bei der Kostenreduzierung. Dies hat allerdings oft zur Folge, dass viele Anwender aus Gründen der Vereinfachung mehr Rechte und Zugriff auf Applikationen erhalten als eigentlich notwendig. Eine zusätzliche Kontrollebene zieht hier der Application Manager von AppSense ein. Dieser versorgt jeden Anwender mit individuellen Berechtigungen auf die von ihm wirklich benötigten Programme und Inhalte. Wir haben unter anderem getestet, wie sich das Werkzeug in Bezug auf einfache Bedienbarkeit schlägt.

Der Application Manager ist Bestandteil der AppSense Management Suite, die weiterhin noch aus den Modulen Performance Manager und Environment Manager besteht. AppSense will mit dem Paket komplexe Benutzerumgebungen über verschiedene Verteilmechanismen und unterschiedliche Plattformen hinweg konsistent bereitstellen. Die Module sind je nach Bedarf weitgehend unabhängig voneinander einsetzbar. Der von uns getestete Application Manager übernimmt das Anwendungsmanagement, also die individuelle Kontrolle der Programmnutzung seitens der Anwender durch die Steuerung der Ausführungsrechte. Dies umfasst insgesamt fünf Stufen: Prüfung der Besitzrechte (Trusted Ownership Checking), rollenbasierter Applikationszugriff, erweiterte Netzwerkzugriffskontrolle (Advanced Network Access Control / ANAC), Management der Benutzerrechte und Lizenz-Konformität bei Terminalservern und VDI. Die Software ist laut Hersteller in Umgebungen zwischen 350 und 160.000 Benutzern im Einsatz.

Umfassendes Installationspaket

Das bei AppSense heruntergeladene Paket zur Installation der Suite ist rund 960 MByte groß und enthält bereits fast alle Zusätze, die für die Einrichtung notwendig sind, etwa sämtliche Quellen für das Setup von SQL 2005 Express sowie einige weitere Pakete von Microsoft. Als Voraussetzungen gefordert werden der IIS und BITS.

Das Setup beinhaltet nur wenige Abfragen wie den Lizenzschlüssel und die Wahl zwischen einer lokalen und einer Enterprise-Installation. Auch lassen sich für die beiden hier nicht näher betrachteten Module Environment und Performance Manager noch optionale Komponenten aufspielen. Unerwartet war für uns, dass nicht danach gefragt wurde, welche der Module der Suite zu installieren sind. Es wird vielmehr alles eingerichtet und nur die Lizenz entscheidet letztendlich über die mögliche Nutzung. Laut AppSense gibt es aber neben der Suite auch getrennte Installationspakete, die nur die einzelnen Module enthalten.

Stellt das Setup nun fest, dass eine der nötigen Voraussetzungen fehlt, so stoppt die Routine für eine Nachinstallation. Erst dann geht es weiter. Nach Abschluss der Basis-Installation muss der Administrator auf die nun fertig eingerichtete Webseite des AppSense Management Centers springen, denn dort stehen alle für die weitere Einrichtung notwendigen Konsolen, Agenten und die Dokumentation als Installations-Sourcen bereit. Interessanterweise ist auch die Dokumentation als MSI-Datei verpackt und muss erst an gewünschter Stelle installiert werden. Sie besteht aus einigen PDF-Files und einer browserbasierten Hilfe.

Pro Modul eine eigene Konsole

AppSense hat die Funktionen der einzelnen Module auf eigene Konsolen verteilt, hinzu kommt noch eine zentrale Management-Konsole, die in jedem Fall benötigt wird. Zur Nutzung des Application Manager mussten wir uns also mit zwei Konsolen beschäftigen.

Vom Prinzip her dienen die Konsolen der drei Module dazu, die eigentlichen Regeln und Einstellungen zu konfigurieren. Die Resultate lassen sich dann entweder als Konfigurationspakete im MSI-Format in einem beliebigen Verzeichnis speichern, im Paketspeicher des Management Servers ablegen oder lokal auf dem gerade genutzten System sofort aktivieren.

Standard ist die Ablage im Paketspeicher, damit die Pakete in der zentralen Management-Konsole sichtbar werden und

Systemvoraussetzungen

Server: Windows 2003 (R2) / 2008 (R2), 32 und 64 Bit, deutsch und englisch

Konsole und Agent: Windows XP SP2 / Vista / 7, Server 2003 (R2) / 2008 (R2)

Unterstützte Technologien: Citrix XenApp (Presentation Server) bis Version 6.0, Citrix XenDesktop bis Version 5.0, VMware View Version 4.5 und 4.6, Microsoft App-V Version 4.5 und 4.6

von dort aus ihren Weg auf die Clients finden. Die Möglichkeit, ein Paket lokal zu aktivieren, hat den Vorteil, dass sich die Einstellungen erfreulich einfach austesten lassen, wenn der Administrator nur einen Client mit den entsprechenden installierten Konsolen bereithält. Die Ablage als MSI-Paket gibt dem IT-Verantwortlichen zudem die Möglichkeit, den Inhalt an anderer Stelle wieder zu importieren oder ohne den Verteilungsprozess des Management Servers direkt auf einem Client zu installieren. Denkbar ist hier auch das Ausrollen mit einer anderen, bereits im Einsatz befindlichen Softwareverteilung. Letztendlich sind die Konfiguration der Pakete und deren Verteilung völlig getrennte Prozesse.

Die Verbindung zu den Clients erfolgt über Agenten, wobei es wiederum pro Modul eigene Agenten gibt, außerdem einen allgemeinen Client Communication Agent (CCA) quasi als Basis-Agent für die Verteilung. Es sind demnach bei voller Nutzung der Suite vier Agenten parallel aktiv, wobei sich das in der Praxis nicht als hinderlich erweist, da sich die Agenten recht komfortabel über die Management-Konsole verteilen und überwachen lassen.

Ausfallsicherheit und Load Balancing als Bordmittel

Um den gesamten Dienst ausfallsicher zu gestalten, hat AppSense entsprechende Möglichkeiten integriert. So lassen sich mehrere Server für ein Failover parallel installieren. Diese werden in der Management-Konsole in eine Liste eingetragen, die an die Agenten übermittelt wird. Bei Nichtverfügbarkeit eines Servers wird der Nächste in der Liste angesprochen. Um darüber hinaus eine Lastverteilung zu ermöglichen, unterstützt die Suite den Network Load Balancing-Cluster von Windows Server 2003/2008. Ein Dokument beschreibt detailliert die notwendigen Schritte zur Einrichtung.

Für den Test konfigurierten wir in einer Domäne einen Management Server sowie diverse dedizierte Clients und einen Terminalserver. Außerdem installierten wir auf einem Client die beiden für die Administration benötigten Konsolen.

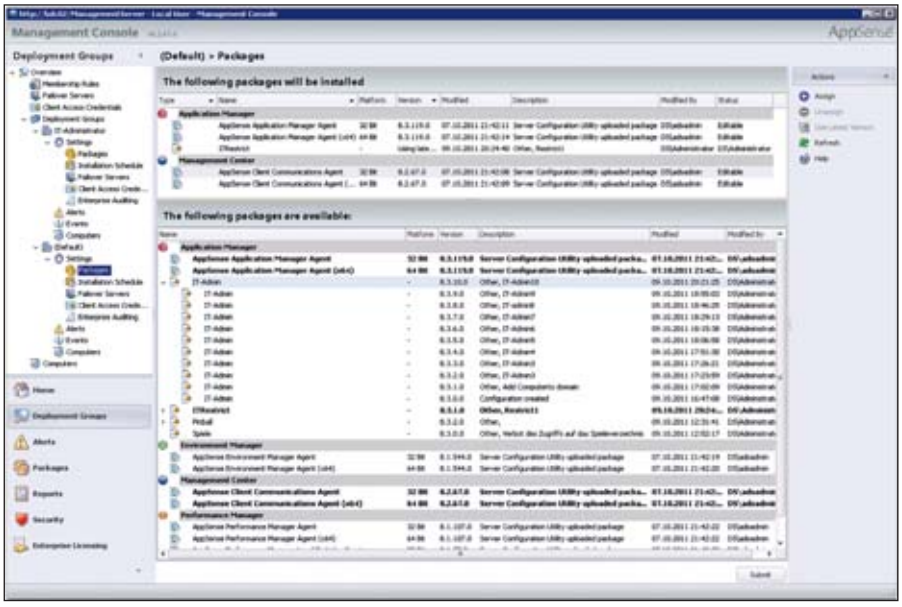


Bild 1: Die Konfigurationspakete im Paketspeicher verwaltet der Administrator über eine separate Management-Konsole. Die automatische Versionspflege hilft dabei, auch bei vielen Paketen die Übersicht zu behalten.

Integrierte Versionsverwaltung

Die Konsole des Application Manager dient dazu, Konfigurationspakete zu schnüren, die dann über die Management-Konsole den Verteilergruppen zugewiesen werden. Bei dieser Arbeit ist zu beachten, dass sich später im Management Server jeder Verteilergruppe und damit jedem Client nur ein Konfigurationspaket zuordnen lässt. Alle gewünschten Einstellungen sind also in einem Paket umzusetzen. Von Vorteil ist dabei die konsequente Versionsvergabe bei Verwendung des Paketspeichers des Management Server. So wird bei der Weiterentwicklung eines Pakets jede Variante mit einer aufsteigenden Versionsnummer versehen. Vergibt der Administrator beim Speichern einen neuen Namen, entsteht dadurch ein neues, unabhängiges Paket, das dann wieder weiterentwickelt werden kann.

Beim Speichern eines Pakets hat der Nutzer die Möglichkeit, einen Grund für die Änderung aus einer Liste zu wählen und ein Beschreibungsfeld zu füllen. Von dieser Möglichkeit sollte er intensiv Gebrauch machen, um die verschiedenen Versionen eines Pakets sowie gegebenenfalls die Unterschiede zwischen den Paketen auch später noch erkennen zu können.

Damit ein Konfigurationspaket, das sich noch in der Entwicklung befindet, nicht von einem anderen Administrator parallel geändert werden kann, ist es solange gesperrt, bis es der Ersteller freigibt. In der Management-Konsole ist genau zu sehen, welches Paket von wem modifiziert wurde und wer es gegebenenfalls gesperrt hat. Hier sollten sich mehrere Administratoren hinsichtlich einer einheitlichen Vorgehensweise absprechen.

Feine Stellschrauben für Benutzerrechte

Wie eingangs erwähnt, greift der Application Manager auf fünf unterschiedliche Arten in die Rechtevergabe ein. Die effiziente Nutzung aller Möglichkeiten erfordert eine umfassende Einarbeitung und eine Portion Erfahrung. Beeindruckend ist, dass der Manager die Benutzerrechte nicht nur beschränken, sondern auch gezielt erweitern kann, um dadurch letztendlich den Umfang der Standardrechte zu reduzieren. Im Normalfall sollte ein Anwender nirgendwo mit Administratorrechten arbeiten, auch nicht auf seinem Arbeitsplatz. Ziel ist es aber, den Anwender trotzdem stets mit den Rechten zu versehen, die er für die aktuelle Tätigkeit benötigt. Das können durchaus Administratorrechte für bestimmte Arbeitsschritte sein. Der Application Manager vermeidet aber, dass ein Anwender generell lokale Administratorrechte bekommt, nur weil er diese für ein oder zwei Aktivitäten benötigt.

Die erste Stufe, genannt "Trusted Ownership Checking", geht davon aus, dass die Clients, egal ob physikalisch, als VDI oder

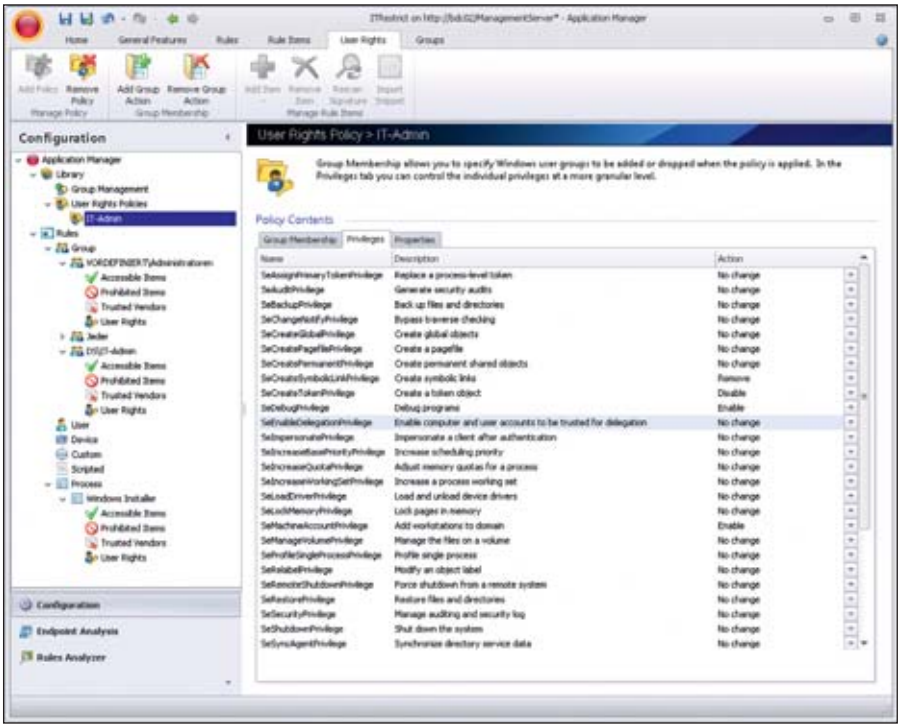


Bild 2: Der Application Manager erlaubt mit Hilfe einer weiteren Konsole die gezielte Manipulation von Benutzerprivilegien auf einem sehr granularen Niveau

als Desktop, auf einem Terminalserver von einem zentralen Account aus eingerichtet und gepflegt werden. Dieses Konto ist dann auch der Besitzer der ausführbaren Dateien. Sobald nun ein Anwender versucht, eine aus dem Internet heruntergeladene oder per USB-Stick mitgebrachte Software zu installieren, ist er der Besitzer. Es reicht auch, eine Datei auf dem Client umzukopieren, um den Besitzer zu ändern.

Indem nun die bekannten und berechtigten Besitzer im Manager erfasst werden, kann die Software anschließend bei jedem Programmaufruf daraufhin prüfen und den Start verweigern, wenn das Besitzerrecht nicht passt. Dies wirkt übrigens nicht nur bei unlizenzierter oder unerwünschter Software, die der Anwender bewusst installiert, sondern auch bei Spyware, Hacker-Tools, Trojanern und Viren. Das Einrichten dieses Mechanismus ist erfreulich einfach, da nur die berechtigten Accounts zu erfassen und die Funktion zu aktivieren ist. Im Test mit einem XP-Client fiel uns hier allerdings ein Problem in Verbindung mit Windows Updates auf, das anfangs zu unerklärlichen Meldungen hinsichtlich fehlender Berechtigungen führte. Ist bei einem XP-Client Windows Update aktiviert, so wird bei aktualisierten Dateien der aktuell angemeldete Benutzer als Besitzer eingetragen. Der ist aber nicht zwingend beim Application Manager als Trusted Owner hinterlegt. Bei neueren Windows-Versionen tritt dieser Fehler nicht mehr auf, da dort die Besitzrechte in Verbindung mit dem Updateprozess anders vergeben werden.

Alarm bei Umgebungswechsel

Ebenso wie sich die Besitzrechte in einem Konfigurationspaket global prüfen lassen, gibt es noch weitere globale Filterfunktionen. So kann der Nutzer Dateien anhand ihrer Endung von jeglicher Prüfung ausnehmen oder die Prüfung auf bestimmte Dateitypen beschränken. Weiterhin kann die Software eine Applikation beenden, wenn sich die Voraussetzungen plötzlich geändert haben. Eine Änderung kann durch Einspielen neuer Regeln verursacht werden, aber beispielsweise auch dadurch, dass ein Anwender eine laufende Terminalsitzung auf ein anderes Gerät übernimmt, auf dem das Ausführen der Applikation nicht erlaubt ist, oder sich die IP-Adresse des Gerätes ändert. Der Anwender erhält eine Warnung und bekommt eventuell noch eine Karenzzeit zum Speichern offener Dateien oder gegebenenfalls zum Wechsel zurück auf den vorherigen Zustand.

Während alle bisher beschriebenen Optionen global auf eine Konfiguration wirken, sind alle weiteren Regeln mit einer Filterung nach AD-Gruppen, Anwendern, Endgeräten oder Prozessen verbunden. Dabei lässt sich je Filterbereich eine Sicherheitsstufe festlegen, die vorgibt, mit welchen Konsequenzen die Regeln umgesetzt werden. Entweder kommt es prinzipiell zu einer Befolgung der Regeln oder der Anwender kann sich bei benutzerbezogenen Regeln selbst zur Applikationsnutzung berechtigen und so Ausnahmen schaffen. Ferner ist es möglich nur ein Auditing durchzuführen. Auf Wunsch lassen sich auch alle Applikationen erlauben – die Regel ist damit ohne Wirkung. Sinnvoll erscheint uns die Anwendung dieser stufenweisen Verschärfung beispielsweise bei der Einführung neuer Regeln. Immerhin besteht die Gefahr, dass falsche oder zu strenge Regeln die Anwender bei der Arbeit behindern. Durch einen Einstieg mit einem Auditing kann der Administrator erst einmal beobachten, wo die Regel greifen würde.

Kommen wir nun zur zweiten Stufe, dem "rollenbasierten Applikationszugriff". Hier lässt sich der Zugriff für Anwender, Anwendergruppen und Endgeräte auf Applikationen gezielt über Verbots- und Erlaubnislisten sowie anhand von Signaturen steuern. Die Listen können wiederum einzelne ausführbare Dateien, aber auch Ordner, Laufwerke und Signaturdateien enthalten. In Verbindung mit den Erlaubnislisten lässt sich über eine Zeitangabe zusätzlich eine zeitliche Beschränkung hinterlegen.

IP-basierte Überwachung der Wege

Die dritte, mit der Version 8 neu hinzugekommene Stufe "Advanced Network Access Control (ANAC)" ermöglicht eine Kontrolle durch Überwachung des IP-Verkehrs auf Benutzerebene oder auf Benutzer- und Prozessebene. Hierzu werden entsprechende Regeln für erlaubte oder verbotene IP-Adressen, Adressbereiche, Hostnamen und Dateifreigaben hinterlegt. In der Praxis lässt sich das so konfigurieren, dass ein Anwender beispielsweise von seinen normalen Arbeitsplatz aus auf einem Terminalserver bestimmte Applikationen aufrufen kann, aber nicht über sein Notebook über einen WLAN-HotSpot, wo die Lokation

nicht klar ist und die Gefahr besteht, dass ihm jemand über die Schulter schaut. Auch Double-Hop-Szenarien lassen sich überwachen, so dass ein Anwender von einem Terminalserver nur auf bestimmte andere weiterspringen kann.

In Verbindung mit der Prozesskontrolle wiederum lässt sich so beispielsweise verhindern, dass ein Anwender für den Mailzugriff statt Outlook einen anderen E-Mailclient verwendet. Über eine dedizierte Portkontrolle ist es weiterhin möglich, den Datenverkehr über definierte Protokolle wie HTTP, FTP oder RDP zu beschränken.

Die vierte Steuermöglichkeit besteht darin, dass Benutzerrechte gezielt für einzelne Aktionen verändert werden. Dazu sind zuerst eine oder mehrere Policies anzulegen, die beschreiben, wie sich die Rechte verändern. Beispielsweise kann für eine Aktion die Mitgliedschaft in einer AD-Gruppe hinzugefügt oder verworfen werden. Weiterhin lassen sich Systemprivilegien individuell erlauben oder verweigern. Anschließend kann der Administrator diese Regelsätze einzelnen Dateien oder ganzen Ordnern sowie Signaturen zuweisen.

Nicht zuletzt kann eine Regel auch das Recht für den Zugriff auf Objekte in der Systemsteuerung sowie auf Management Snapins verändern, also entweder erweitern oder sperren. Beeinflussen lassen sich weiterhin Web-Installationen, damit die Anwender dort angebotene Werkzeuge selbst einrichten können oder eben dies verboten wird. So genannte "Snippets" helfen dabei, immer wieder benötigte Einstellungen zu speichern. Für häufig genutzte Tools wie Adobe Reader, Flash und Quicktime werden passende Snippets bereits mitgeliefert, was eine einheitliche Konfiguration erleichtert und die Einrichtung deutlich beschleunigt.

Granulare Admin-Rechte auf Zeit

Eine Besonderheit ist noch die mit Version 8.3 hinzugekommene Self-Elevation. Ist ein Benutzer dazu berechtigt, kann er für einen Programmaufruf eine Ausführung als lokaler Administrator selbst veranlassen. Dieses Recht lässt sich wieder auf bestimmte Applikationen beschränken oder es sind bestimmte Programme ausgeschlossen. Auch kann der Anwender aufgefordert werden, vorher eine Begründung einzugeben.

Bei der Manipulation der Benutzerrechte nutzt der Application Manager übrigens nicht die Funktion "Run as ..", um die Aktion einfach unter einem anderen Benutzer laufen zu lassen, sondern es wird gezielt das Benutzerzertifikat ausgetauscht. Neu in Version 8.3 ist, dass das Werkzeug berücksichtigt, dass trotz der erweiterten Applikationsrechte bei normalen Dialogen wie "Datei öffnen" nur die normalen Benutzerrechte wirken und ein Anwender nicht aufgrund der Manipulation beispielsweise auf Dateien zugreifen kann, auf die er normalerweise kein Recht hat. AppSense nennt dies "Secure Dialogs".

Mit der fünften Stufe gibt der Application Manager einem Unternehmen die Möglichkeit an die Hand, trotz Nutzung einer Desktop-Farm für systemgebundene Lizenzen von Microsoft sicherzustellen, dass eine Applikation nur auf bestimmten Systemen ausführbar ist. Hierzu werden in einer geräteabhängigen Regel genau die eingetragen, für die eine bestimmte Applikation freigegeben ist. Das Verfahren ist von Microsoft zertifiziert, die Nutzung muss aber dort angemeldet werden. Zu beachten ist allerdings, dass sich die Kontrolle ausschließlich auf diese spezielle Thematik beschränkt und eine generelle Lizenzüberwachung nicht implementiert ist.

Ein wichtiger Aspekt beim Einsatz des Application Manager ist ein Auditing, um relevante Ereignisse wie Fehler, Selbstautorisierungen und unterbundene Zugriffe zu erfassen. Die Meldungen lassen sich in verschiedene Log-Dateien leiten, zudem ist eine Anonymisierung möglich. Auf Wunsch erfolgt ein Export in das XML- oder CSV-Format, um sie dann mit anderen Tools auszuwerten.

Neben den beschriebenen Kontrollmechanismen beinhaltet der Application Manager auch eine Endpunktanalyse. Zu beachten ist, dass hierfür DCOM erlaubt sein muss. Dann liefert ein Scan-Durchlauf alle ausführbaren Prozesse. Zudem ist es möglich, alle Applikationsaufrufe zu protokollieren, wobei Letzteres weniger als Langzeitanalyse gedacht ist, sondern vielmehr hilft, einzelne Aktionen aufzuzeichnen, um deren Ablauf und eventuelle Abhängigkeiten (Welcher Prozess ruft welche weiteren mit auf? Welche DLLs werden mit geladen?) zu erkennen. Nicht mit protokolliert werden Zeiten. Dennoch ist darauf zu achten, dass derartige Analysen nicht die Persönlichkeitsrechte der Mitarbeiter in Hin-

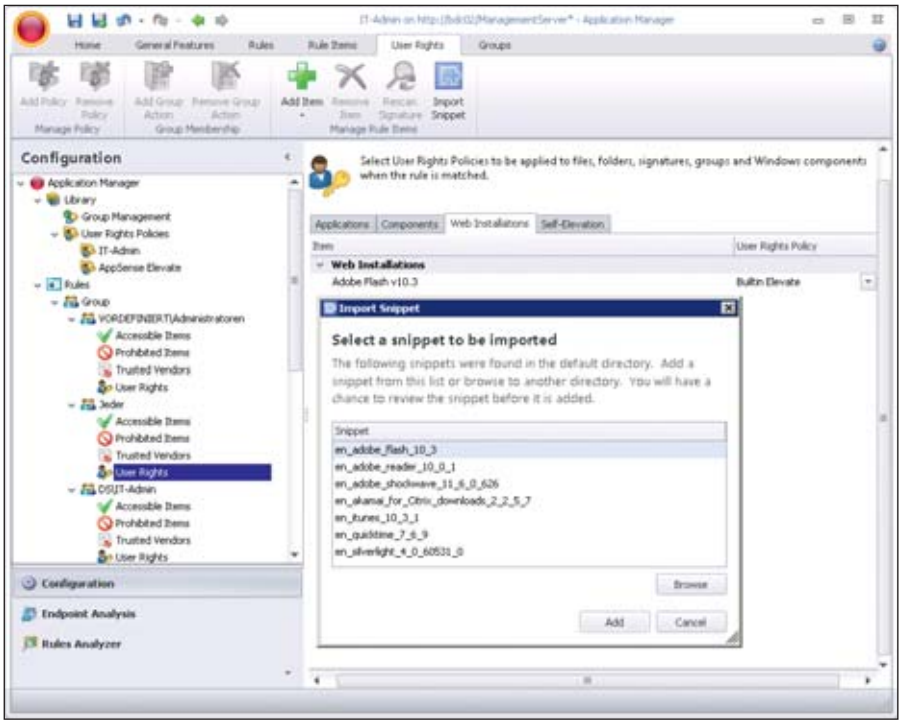


Bild 3: Vorbereitete Snippets erleichtern dem Administrator die Einrichtung häufig benötigter Benutzerrechte für typische Installationen

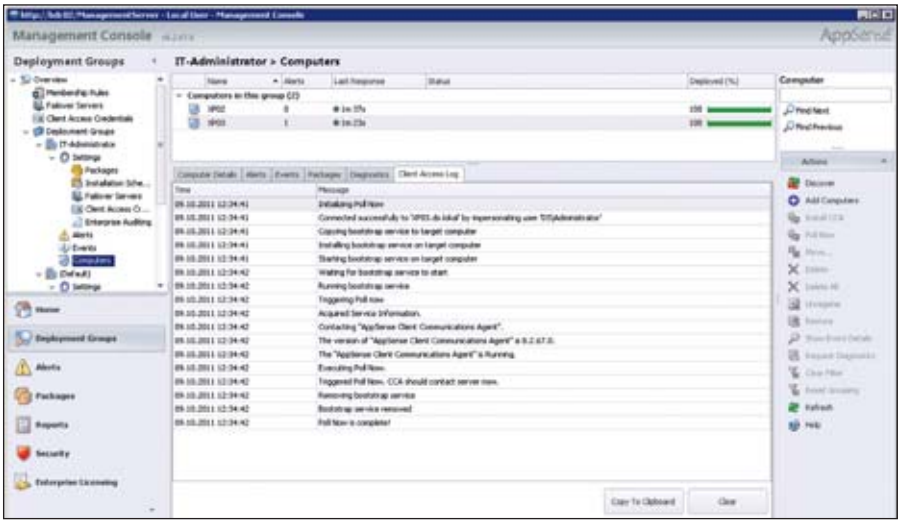


Bild 4: Die verwalteten Clients sind in mehreren Verteilergruppen zu finden. Der Verteil-Status wird dabei übersichtlich dargestellt.

blick auf unzulässige Beobachtungen verletzen. Die Regelanalyse letztendlich liefert eine Übersicht der geblockten Prozesse.

Komfortable Verteilung via Management-Konsole

Innerhalb der für die Verteilung der erstellten Regeln zuständigen Management-Konsole kann der Nutzer mehrere Gruppen anlegen, sofern sich die Konfigurationsvorgaben für unterschiedliche Clients unterscheiden. Dies dürfte zum Beispiel beim Betrieb an mehreren Standorten durchaus der Fall sein. Über ein Regelwerk wird anhand des NetBIOS-Namens sowie der Container- oder Gruppenzugehörigkeit im Active Directory festgelegt, in welche Gruppe ein neu erfasster Client einsortiert wird. Pro Verteilergruppe legt der Administrator fest, welche Pakete zu installieren sind, nach welchen Regeln Agenten und Konfigurationen ausgerollt werden sollen (gar nicht, sofort bei Verfügbarkeit, bei Client-Start oder regelmäßig in bestimmten Abständen), welche Failover-Server in Frage kommen, welche Credentials für die Installation des CCA-Agenten gelten und ob ein Auditing erfolgen soll. Die Auflistung der Clients erfolgt übersichtlich inklusive Verteil-Status in Form einer Balkenanzeige. So lässt sich genau herauslesen, welcher Client die aktuelle Konfiguration besitzt.

Alarme und Events werden nach Verteilergruppen getrennt sowie pro Client angezeigt. Für jeden Client kann der Administrator weiterhin die wichtigsten Eigenschaften (Betriebssystem, CPU, RAM, Plattenkapazität) sowie die installierten AppSense-Pakete auslesen und eine Diagnose beauftragen.

Fazit

Auf verschiedene, gut umgesetzte Arten steuert AppSense Application Manager die Verwaltung der Benutzerrechte in Bezug auf die auf einem System installierten Applikationen. So lässt sich sehr wirkungsvoll vermeiden, dass Anwender selbst installierte Applikationen nutzen können. Im Test konnten wir uns davon überzeugen, dass es erfreulich einfach ist, in einheitlichen Umgebungen via VDI oder Terminalserver die einzelnen Benutzer für unterschiedliche Applikationen zu berechtigen. Komplexere Konfigurationen sind notwendig, wenn es darum geht, die Benutzerrechte für bestimmte Aktionen gezielt zu verändern. Gefallen hat uns, dass das Programm die Rechte nicht nur beschränken, sondern auch erweitern kann. Dadurch sollte es in den meisten Fällen möglich sein, die Basisrechte der Anwender herunterzusetzen und im Gegenzug gezielt für bestimmte Aktivitäten auszubauen.

Gut ist ferner die Möglichkeit, die Zugriffsrechte auf Applikationen vom genutzten Endgerät und von der Lokation im Netzwerk abhängig zu machen. Dadurch lässt sich unterbinden, dass beispielsweise aus unsicheren Bereichen auf sensible Daten zugegriffen wird. Als etwas umständlich hingegen empfanden wir es, dass sich die Bedienung auf mindestens zwei Konsolen verteilt. Wer noch weitere Module der Suite nutzt, hat sogar noch mehr Konsolen zu bedienen.

Um alle Möglichkeiten des Application Manager nutzen zu können, halten wir eine umfassende Einarbeitung für sehr empfehlenswert, wobei der Hersteller Schulungen anbietet und zertifizierte Partner bei der Einführung unterstützen. Für einen Test im eigenen Unternehmen stellt AppSense Trial-Versionen mit 21 Tagen Laufzeit zur Verfügung. Diese lassen sich aber nicht einfach herunterladen, sondern müssen erst angefordert werden. *(ln)*

Produkt

Software zur Steuerung des Anwenderzugriffs auf installierte Programme und zur granularen Rechtevergabe.

Hersteller

AppSense
www.appsense.com

Preis

AppSense Application Manager kostet pro Lizenz 36 Euro (für Named User) zuzüglich Subskription und Support. Für größere Abnahmemengen gibt es Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Agentenmanagement	8
Applikationsmanagement	8
Anwendungsverfügbarkeit	9
Reporting und Auditing	8
Lizenzverwaltung	6

Dieses Produkt eignet sich

optimal für größere Unternehmen mit einigen hundert oder mehreren tausend Benutzern in einer komplexen Umgebung mit virtuellen Desktops und zentraler Applikationsbereitstellung.

bedingt in kleineren Umgebungen, wenn spezielle Sicherheitsanforderungen verlangt werden, die genau definierte Desktops voraussetzen. Hier ist der im Vergleich hohe Administrationsaufwand zu berücksichtigen.

nicht für Umgebungen, die nicht auf Windows setzen.

AppSense Application Manager 8.3

DEUTSCHE UNTERNEHMERBÖRSE

Ein Partner von Handelsblatt

NACHFOLGE IN GEFAHR?

Mit einem Inserat auf DUB.de erreichen Sie bis zu 1,2 Millionen potenzielle Nachfolger – **einfach, sicher und schnell**.

Service für „IT-Administrator"-Leser

DUB ZUM SONDERPREIS: Schalten Sie einfach Ihr Drei-Monats-Verkaufsangebot auf DUB.de zum Preis von zwei Monaten. Sie sparen 59 Euro. Es fallen keine weiteren Kosten an.

UND SO GEHT'S: Schreiben Sie eine E-Mail mit dem Betreff „IT-Administrator" an kai.mueller@dub.de oder rufen Sie an unter 040/46 88 32-661. Sie erhalten dann umgehend Ihre Zugangsdaten. So können Sie DUB.de ausprobieren und sparen.

WWW.DUB.DE

Im Kurztest: PocketCould Remote Desktop Pro

Mobiler Remotezugriff

von Sandro Lucifora

Statt mit dem Notebook lässt sich mit der App PocketCould Remote Desktop Pro von Wyse auch mit Android-Geräten von überall auf den Windows- und Mac-Desktop zugreifen. PocketCould Remote unterstützt neben RDP auch Verbindungen zu VNC-Systemen und VMware View. Unser Kurztest untersucht, wie gut und komfortabel dieses Vorhaben funktioniert.

Die Installation von PocketCould Remote (PCR) erfolgt über den Android Market. Neben der von uns getesteten Pro-Version steht auch die kostenlose Variante mit eingeschränktem Funktionsumfang zur Verfügung. Getestet haben wir unter Android 2.2.1. PCR soll laut Hersteller ab Android 2.1 lauffähig sein und für Tablets mit Android 3.0 ein angepasstes User Interface erhalten haben. Nach der Installation und dem Start begrüßte uns ein Setup-Wizard, der uns nach dem Login zu unserem Google-Account fragte. Über das Google-Konto kann die App im Zusammenspiel mit der gleichnamigen Windows- beziehungsweise Mac-Anwendung Verbindungsdaten austauschen. Alternativ ließ sich eine RDP-, VNC- und VMware View-Verbindung auch manuell einrichten.

Bei Inbetriebnahme auf mögliche Sicherheitsrisiken achten

Zunächst installierten wir die Windows-Anwendung von Wyse auf einem Windows 7-Desktop und einem Windows 2008 Server. Das Setup richtet den Remote Desktop ein, konfiguriert die Firewall am Computer, NLA (Network Location Awareness), die Benutzerrechte, das Windows-Kennwort (sofern noch nicht vorhanden) und richtet die Verbindung zum Austausch mit der Android-App über das Google-Konto ein. Nach einem kurzen Moment zeigte ein Icon im Tray, dass die Software aktiv ist. Über die Oberfläche konnten wir zusätzlich noch festlegen, auf welche Verzeichnisse die Mobile-App zugreifen darf. Was wir vermissten, war die Option, den Namen des Computers zur Identifizierung in der PocketCloud individuell festzulegen.

Zurück auf dem Smartphone erschien eine Liste der bei PocketCloud registrierten Remote-Computer. Durch das Auswählen eines Eintrages stellte PocketCould die Remote-Verbindung her. Alternativ führten wir auch eine RDP-Verbindung über die manuelle Konfiguration durch. Neben der IP-Adresse beziehungsweise der URL konnten wir optional direkt den Benutzernamen und das Anmeldekennwort sowie die Domäne hinterlegen, so dass sich die Software nach der Verbindung am System einloggen konnte. Das macht vor allem bei einem Smartphone Sinn, das durch seine Tastatur nicht gerade zum Eintragen komplexer Kennwörter einlädt, birgt jedoch auch ein Sicherheitsrisiko, falls das Smartphone verloren wird.

Komfortabler Remote-Support

Die Remote-Verbindung läuft über WLAN und UMTS flüssig. Ausgeklügelt ist die Bedienung: Neben einer virtuellen Tastatur blendet der Hersteller auch die Sondertasten Strg, Windows, Alt und Tab ein. Über einen Button sendet der Nutzer Strg+Alt+Entf an den Remote-Rechner. Die Funktionstasten sowie der komplette Block mit Richtungspfeilen, Seite hoch und runter et cetera lassen sich ebenso darstellen. Bei Wyse steuert der Anwender zudem eine angezeigte Maus. Um die Maus herum befindet sich ein Kranz, über den wir Funktionen wie linke und rechte Maustaste, Tastatur, Sondertasten und so weiter komfortabel aufrufen konnten.

Während des Betriebs fiel auf, dass sich die automatische Skalierung der Anzeige nicht an die Ausrichtung des Smartphones anpasst. So bleibt die Anzeige der Auflösung in dem Format – vertikal oder horizontal –, das zum Verbindungsaufbau gewählt war.

Fazit

Die clevere Bedienung von PocketCloud sowie der Austausch der Verbindungsdaten über das kostenlose Desktop-Tool machen das Plus zu anderen Remote-Lösungen aus. Dennoch gibt es Stellen, an denen der Hersteller nacharbeiten muss. *(jp)*

Produkt

App für Android-Smartphones zur Fernwartung von Windows- und Mac-Rechnern. Lauffähig ab Android 2.1. Geeignet für Smartphone und Tablet. Berechtigungen: Uneingeschränkter Internetzugriff, Inhalt des USB-Speichers und der SD-Karte ändern/löschen, WLAN-Status anzeigen und Netzwerkstatus anzeigen

Hersteller

Wyse Technology Inc.
www.wyse.de

Preis

Circa 11 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Umsetzung	6
Handhabung	9
Aufwand der Konfiguration	8
Zuverlässigkeit	7
Kosten/Nutzen	6

PocketCloud Remote Desktop Pro 1.2.265

User Environment Management für virtuelle Applikationen

Virtuell verzahnt

Quelle: 123RF

von Falko Gräfe

Werkzeuge zur Applikationsvirtualisierung schließen typischerweise Funktionen ein, um benutzerspezifische Konfigurationen sauber von den Applikationskomponenten zu trennen. Benutzerspezifische Einstellungen liegen in der Regel in Formaten vor, die ein einfaches dynamisches Transferieren zwischen unterschiedlichen Maschinen und Betriebssystemen ermöglichen. Dieser Artikel stellt die Frage, ob User Virtualization-Lösungen wie RES, AppSense, FlexProfiles oder Citrix Profile Management diese Konfigurationen überhaupt verwalten können und wann es sinnvoll sein kann, Benutzer- und Anwendungsvirtualisierung zu kombinieren.

Das Konzept der Applikationsvirtualisierung – geprägt durch die Entkopplung von Anwendungen vom Betriebssystem und die Isolation einzelner Anwendungen voneinander – hat sich in den letzten Jahren als Standardtechnologie etablieren können. Für Software unter dem Sammelbegriff "User Environment Management" (UEM) ist zurzeit ein hohes Engagement der Anbieter zu beobachten, Kunden unter dem Aspekt der "Heterogenen Desktops" für diesen Bereich von Windows-Systemen zu sensibilisieren.

Unabhängig von der Ausprägung der Applikationsvirtualisierung (AppVirt) und unabhängig von der letztlich untersuchten UEM-Lösung erscheint die Klärung grundsätzlicher Fragen für diesen Technologie-Mix geboten:

- Lassen sich UEM-Werkzeuge überhaupt mit der Applikationsvirtualisierung kombinieren – oder werden hier durch Isolation und Umleitung Schranken gesetzt?
- Ist es sinnvoll, UEM-Software zusammen mit der Applikationsvirtualisierung einzusetzen, oder ist ein Konzept bereits als Teilfunktion des anderen Konzeptes realisiert?
- Welche Vor- und Nachteile ergeben sich beim gemeinsamen Einsatz beider Konzepte?

Um es auf den Punkt zu bringen: Applikations-Virtualisierung und User Environment Management – macht das überhaupt Sinn?

Konfigurations-Management in AppVirt-Werkzeugen

Eine vollständige Betrachtung des Konzeptes der Applikationsvirtualisierung in Bezug auf die Speicherung und Wiederherstellung von Benutzerkonfigurationen ist nicht sinnvoll, da sich die technischen Realisierungen der Einzelprodukte voneinander unterscheiden (so wie unter dem Begriff Applikationsvirtualisierung unterschiedliche Lösungsansätze zu finden sind). Für eine Vereinfachung werden wir uns auf die drei wichtigsten Produkte Citrix (Application) Streaming, Microsoft App-V und VMware Thinapp beschränken. Einen Einblick in diese drei – und weitere – AppVirt-Tools geben umfangreiche Whitepaper [1, 2] im Internet.

Allen drei Lösungen ist gemein, dass sie Konfigurationsänderungen, die vom Benutzer vorgenommen werden, separat vom ursprünglichen virtuellen Paket außerhalb der virtuellen Umgebung ablegen. Der externe Ablageort dieser Konfigurationsänderungen ist verallgemeinernd das Benutzerprofil des Anwenders, wobei es einige Unterschiede gibt: Citrix Streaming speichert benutzerspezifische Dateien im Dateisystem unter *AppData* und benutzerspezifische Registry-Änderungen in der lokalen Registry in HKCU. Die einzelnen Pakete werden durch einen Ordner beziehungsweise einen Key mit der Paket-GUID unterschieden. App-V fasst alle Dateien und die Registry zu einer Container-Datei zusammen (die PKG-Datei) und legt sie in *AppData* ab. Die einzelnen Ordnernamen setzen sich aus einer Kombination aus Primärverzeichnis-Kurzversion und Paket-GUID zusammen. VMware ThinApp schließlich speichert benutzerspezifische Dateien im Dateisystem unter *AppData*. Dort liegt auch eine Datei, die die Registry repräsentiert. Zur Unterscheidung wird der Paketname verwendet.

Alle drei Lösungen legen die Änderungen, die ein Anwender während der Nutzung der Applikation durchführt, außerhalb der virtuellen Umgebung ab – standardmäßig an den Stellen, die vom Betriebssystem für das Speichern von Benutzerkonfigurationen vorgesehen sind. Werden servergespeicherte Profile (Roaming Profiles) verwendet, wandern diese Einstellungen zusammen mit dem Anwender von Rechner zu Rechner. Die AppVirt-Produkte erlauben es auch, den Ablageort für die Benutzerkonfigu-

rationen zum Beispiel auf eine Netzwerkfreigabe umzulegen (Ordnerumleitung), so dass diese Daten nicht als Bestandteil des Benutzerprofils ge- und entladen werden müssen.

Lösungen für das Einstellungsmanagement

Am Markt existiert eine recht hohe Anzahl etablierter Produkte, die die Verwaltung von Benutzereinstellungen vereinfachen sollen. Begriffe wie "User (State) Virtualization", "User Profile Management" oder "User Environment Management" werden zur Klassifikation der Lösungen verwendet. Der Begriff "User Environment Management" scheint sich als Sammelbegriff durchzusetzen und wird hier im Weiteren vor allem in seiner Abkürzung UEM verwendet werden.

Ohne hier auf Details einzugehen, bieten viele dieser Produkte einen Mix aus unterschiedlichen, aber verwandten Funktionen wie zum Beispiel:

- Anpassen der Benutzerumgebung zur Anmeldezeit (Verbinden von Laufwerken oder Druckern)
- Speichern und Wiederherstellen von Betriebssystem-Konfigurationen
- Speichern und Wiederherstellen von applikationsspezifischen Einstellungen
- Durchsetzen von Sicherheitsrichtlinien
- Steuern der Benutzer-Umgebung (Erzeugen des Startmenüs oder von Desktop-Verknüpfungen)
- Nutzung von Benutzereinstellungen über Betriebssystem-Grenzen hinweg (v1/v2-Profile, Desktop/Server-Profile, x86/x64-Profile)
- Schnellere An- und Abmeldezeit

Einige Produkte konzentrieren sich auf eine Auswahl dieser Funktionen, andere Lösungen bieten Features an, die über die hier genannten hinausgehen. Im Fokus dieses Artikels sollen diejenigen Funktionen stehen, die Einfluss auf die Applikationskonfiguration haben. Die relevanten Funktionen sollen gewährleisten, dass zum Beispiel eine Office-Applikation in unterschiedlichen Umgebungen (lokal/remote, V1/V2-Profile, x86/x64, Desktop-OS/Server-OS) stets identisch konfiguriert ist. Dies soll garantieren, dass Konfigurationsänderungen

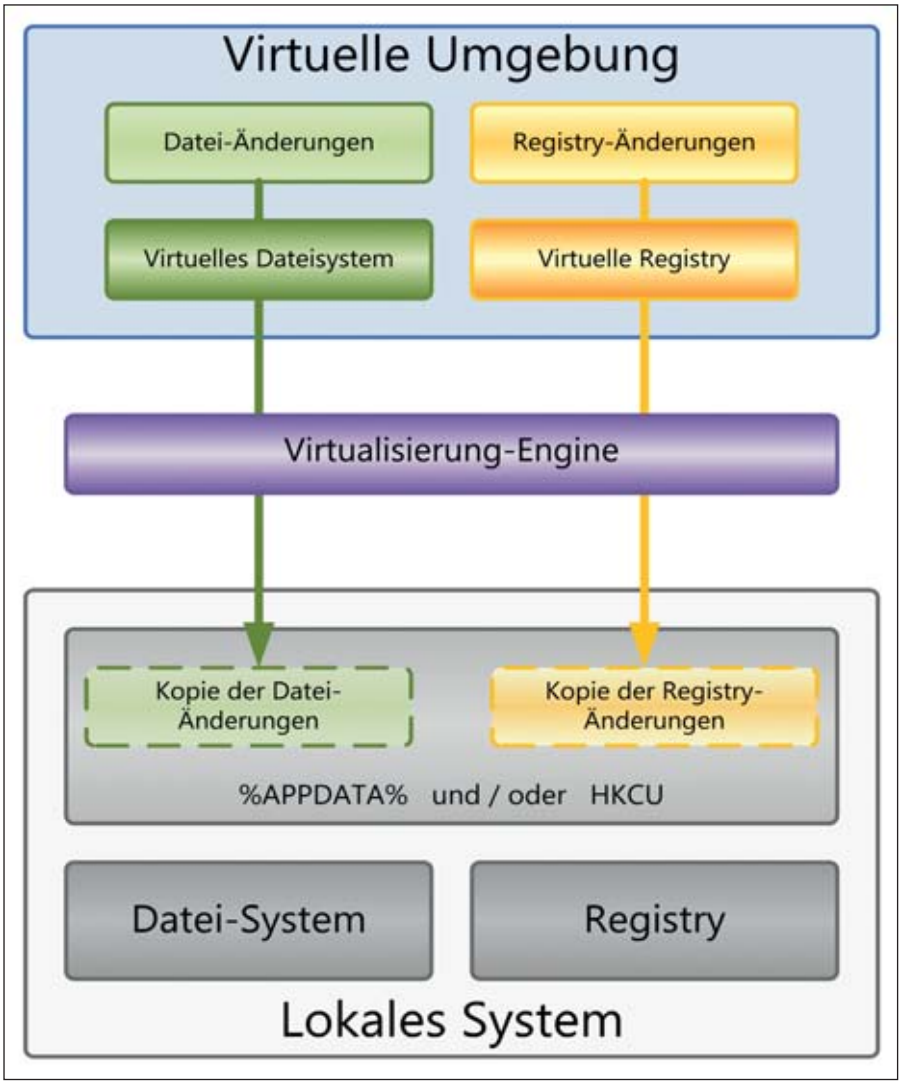


Bild 1: Konfigurationsänderungen virtueller Applikationen werden beim Beenden lokal in proprietäre Bereiche des Benutzerprofils geschrieben

innerhalb einer Session oder Umgebung ebenso in andere Umgebungen übertragen werden. Die grundsätzlichen Produktansätze – wenn auch teilweise mit abweichenden Begriffen vermarktet – lassen sich wie folgt klassifizieren.

Profil-Streaming, Profil-Virtualisierung

Hier analysiert die Software – durch Filtertreiber oder API-Hooks – permanent die Lese- und Schreiboperationen der Applikation. Werden Dateien oder Registry-Operationen identifiziert, die der Applikationskonfiguration zuzuordnen sind, werden diese Operationen unterbrochen und die Ressource von der Lösung zur Profilvirtualisierungs zur Verfügung gestellt. Das Profile Streaming-Produkt unterbricht also eine Anforderung und bedient sie zum Beispiel aus einer Datenbank oder von einem Dateiserver. Die Applikationskonfigurations-Daten werden dabei nicht wirklich in die Windows-Sitzung des Anwenders kopiert, sind also etwa nicht in der Registry unter HKCU zu finden. Typische Vertreter dieser Gattung sind AppSense Environment Manager, RES Workspace Manager oder triCerat Simplify Profiles/PAT.

Klassisches Profil-Management

Produkte, die wir hier etwas salopp als klassisches Profilmanagement bezeichnen wollen, sind dadurch charakterisiert, dass die Konfigurationsdaten lokal in die Benutzersitzung hineinkopiert werden. Das Wegschreiben besteht darin, lokale Dateien und Registry-Werte zu sammeln und an eine zentrale Stelle zu kopieren. Im Laufe der Sitzung ist also beispielsweise die Office-Konfiguration durch alle Applikationen und das Betriebssystem unter "HKCU \ Software \[…]"

sicht- und veränderbar. Immidio Flex Profiles und Citrix Profile Management gehören zu dieser Kategorie.

Layering Technologien

Für virtuelle Maschinen – oder konkreter, deren Festplatten – erfreuen sich sogenannte Layering-Technologien zunehmender Aufmerksamkeit. Die Grundidee ist, dass eine oder mehrere Differenz-Disks "über" eine Basis-Disk gelegt werden und somit eine virtuelle Platte entsteht, die dann etwa Applikationen oder Benutzerkonfigurationen verteilen, aber auch aufnehmen und speichern kann. Layering-Technologien sollen an dieser Stelle jedoch unberücksichtigt bleiben, da sie das Speichern von Applikationskonfigurationen eher als Nebeneffekt mitbringen und heute eher noch ein Nischenkonzept repräsentieren. Vertreter sind hier Unidesk und MokaFive. Citrix ist durch die Übernahme von RingCube in diese Runde eingestiegen.

Benutzereinstellungen und die Kunst des Fischens

Es stellt sich zunächst die Frage, ob eine Integration oder Interaktion zwischen Applikationsvirtualisierung und Konfigurationsmanagement technisch überhaupt möglich ist. Schließlich sind hier unterschiedliche Schichten des "Technology Stack" recht eng miteinander zu verzahnen – und die Applikationsvirtualisierung zeichnet sich durch ein hohes Maß der Abschottung (vor anderen Applikationen, Diensten und dem Basis-Betriebssystem) aus. Grundsätzlich haben die UEM-Lösungen drei Ansatzpunkte, um die Konfigurations-Daten von virtuellen Applikationen zu sichern und natürlich auch wiederherzustellen.

Schleppnetz-Fischerei

Die einfachste Methode, eine rudimentäre Verwaltung der Applikationskonfigurations-Daten vorzunehmen, besteht für die UEM-Produkte im Ignorieren der Applikationsvirtualisierung: Es werden einfach alle Daten des klassischen Profils verwaltet, da die AppVirt-Lösungen hier ja selbständig die Applikationskonfigurations-Daten ablegen (die PKG-Dateien von App-V, die Citrix-Streaming-Ordner in HKCU und AppData oder das Sandbox-Verzeichnis in ThinApp). In diesem Fall würde die UEM-Lösung faktisch nicht die eigentliche Applikation, sondern nur die Ausführungs-Umgebung (AppVirt-Software) verwalten. Die Applikation, zum Beispiel Office oder Notes, ist für die UEM-Lösung unsichtbar. Diesen Ansatz kann sich jede UEM-Lösung zu Nutze machen, da die zu verwaltenden Daten ja im lokalen Betriebssystem sichtbar sind. Ein echtes Management ist dies natürlich nicht.

Wie bei der Schleppnetz-Fischerei wird durch die UEM-Lösung einfach alles eingesammelt, was nicht durch die Maschen rutscht. In diesem Fall ist ein Mehrwert aus Sicht der Applikationsvirtualisierung nur begrenzt gegeben – schon durch die integrierten Windows-Mechanismen zur Profilverwaltung lässt sich ein vergleichbares Ergebnis erzielen. Diesen Ansatz betrachten wir deshalb im Folgenden nicht weiter.

Köder und Haken

Der zweite Ansatz besteht darin, der UEM-Software expliziten Zugang zur virtuellen Applikationsumgebung zu gewähren. Das UEM-Werkzeug wirft also Haken und Köder in die isolierte Anwendungsumgebung und muss das Ergebnis aktiv wieder einholen. Dabei wird ausgenutzt, dass Prozesse, die aus der virtuellen Applikationsumgebung heraus gestartet werden, in der Regel auch innerhalb dieser virtuellen Umgebung laufen. Die UEM-Komponente könnte also die Applikations-Konfigurationsdaten deswegen verwalten, weil sie dazu eingeladen wurde.

Technisch lässt sich das in der Regel durch Start- und Endskripte der virtuellen Applikationspakete realisieren. Bei diesem Ansatz ist ein echtes Management der Applikationskonfigurations-Daten möglich. Das UEM-Pro-

Bild 2: User State Virtualization und Application Virtualization sind zwei eigenständige Komponenten im Schichtenmodell der Desktop-Bereitstellung

dukt muss es allerdings erlauben, skriptgesteuert gestartet zu werden. Außerdem ist der Aufwand, in alle bestehenden und zukünftigen AppVirt-Pakete diese Skriptaufrufe einzubauen, nicht zu unterschätzen.

Tauchgang

Der dritte Ansatz basiert darauf, dass die UEM-Lösung dazu in der Lage ist, die Isolations-Techniken der AppVirt-Lösungen zu durchschauen und darauf Einfluss zu nehmen. Es ist technisch möglich, Ressourcenanfragen der Applikationen oberhalb der AppVirt-Schicht abzufangen und zu manipulieren. Die UEM-Software taucht also in die isolierte Umgebung ein und beobachtet – ohne Lichtbrechungen und störende Reflexionen – das Verhalten der virtuellen Applikation. Technisch können Produkte wie Microsofts Process Monitor (wenngleich kein UEM-Produkt) in App-V-Umgebungen hineinschauen und Ressourcen-Anfragen der Applikation innerhalb der virtuellen Umgebung nach außen berichten. Auch der Environment Manager von AppSense erkennt Ressourcenaufrufe, bevor sie von einzelnen AppVirt-Umgebungen identifiziert und beantwortet werden.

Bezüglich Implementationsaufwand und Ergebnis ist dieser Ansatz der attraktivste: Das UEM-Werkzeug wird ganz regulär in der Benutzersitzung ausgeführt und verwaltet lokal installierte und virtuelle Applikationen gleichermaßen. Weder auf Seiten der Applikationsvirtualisierung noch auf Seiten des Einstellungsmanagements sind besondere Maßnahmen zu ergreifen. Ein hohes Risiko für die UEM-Anbieter besteht aber in der hohen Spezialisierung: Ändern sich grundlegende Implementierungs-Eigenschaften der AppVirt-Lösung, können diese Änderungen zur Folge haben, dass die UEM-Software zu spät in den Ressourcenanforderungs-Prozess eingreifen und dann eben keine Konfigurationsdaten mehr identifizieren kann. Die verbleibende Möglichkeit wäre dann nur noch (wie im ersten Ansatz), dass Daten außen durch die AppVirt-Komponenten in den AppVirt User Cache geschrieben werden.

UEM-Lösungen können also – wenn auch mit unterschiedlicher Integrationsstärke – potentiell die Einstellungen virtueller Applikationen verwalten.

Vorteile der Applikationsvirtualisierung für die Benutzerkonfiguration

Aus Sicht der klassischen Profilverwaltung ergeben sich schon durch den Einsatz der Applikationsvirtualisierung alleine Vorteile, auch wenn diese eher ein Nebenprodukt der Applikationsvirtualisierung sind:

- Benutzerkonfigurationen werden pro Applikation gespeichert: Bei Konfigurationsproblemen muss nicht das gesamte Profil gelöscht werden. Dieses Zurücksetzen ist teilweise auch durch Anwender beherrschbar.
- Benutzerkonfigurationen werden an verwaltbaren Orten gespeichert: Sie liegen nicht über mehrere Verzeichnisse, Dateien oder mehrere Stellen in der Registry verstreut. Der Ablageort kann relativ flexibel gewählt werden.
- Teilweise sind obligatorische (mandatory) Profile möglich: Legt die AppVirt-Lösung die Applikationskonfigurationen nur im (umgeleiteten) Dateisystem ab, könnte das Windows-Profil schreibgeschützt konfiguriert werden.
- Plattform- und Architektur-Wechsel sind möglich: In der Regel mappen die AppVirt-Lösungen Benutzerkonfigurationen an die richtige Stelle und ermöglichen damit eine geringere Abhängigkeit von Profil-Generation (v1/v2), Sprache oder Architektur (x86/x64). Dieser Wechsel kann auch mehrfach und in unterschiedliche Richtungen erfolgen.
- Reduzierung des "Last Write Wins"-Problems: Applikationseinstellungen werden nicht am Block im Abmeldeprozess, sondern jeweils beim Beenden einer virtuellen Applikation zurückgeschrieben. Da die zurückgeschriebenen Daten pro Applikation getrennt sind, betrifft die Last Write Wins-Problematik nicht alle Einstellungen einer Session, sondern maximal noch individuelle Applikationen. Je nach Kombination aus UEM- und AppVirt-Lösung kann das User Environment Management darüber hinaus speziell für virtuelle Applikationen einige deutliche Vorteile bringen.

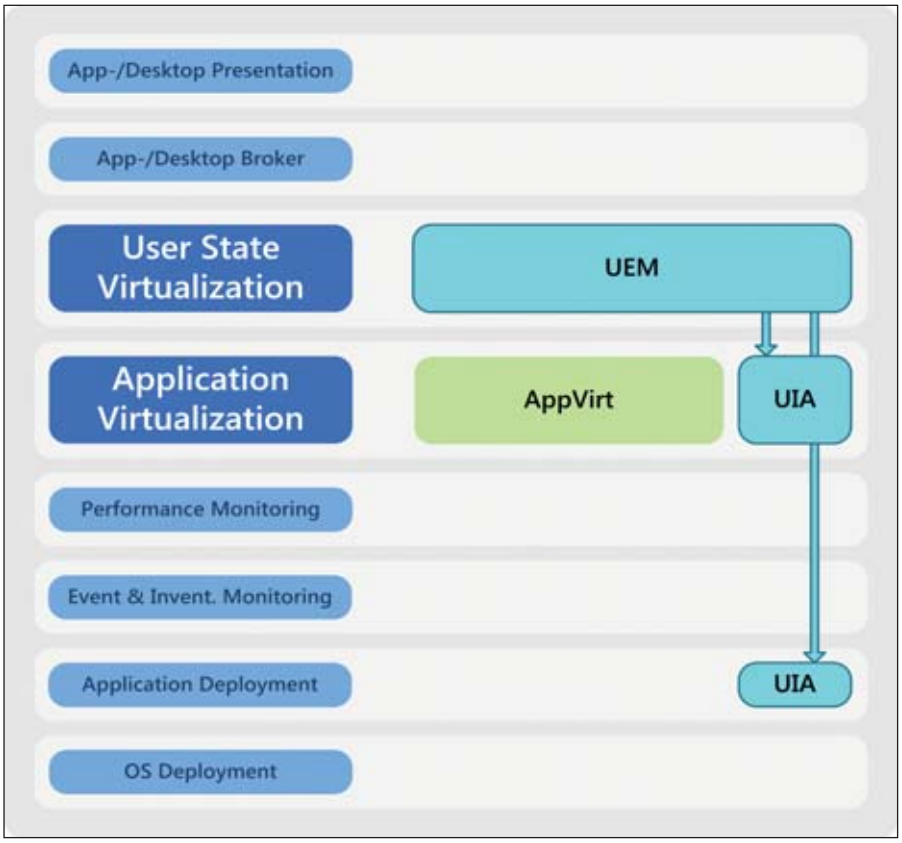


Bild 3: Die Funktion "User Installed Applications" (UIA) des User Environment Management führt eine funktionale Überschneidung mit den Schichten "Applikationsvirtualisierung" und "Applikationsbereitstellung" ein.

Benutzereinstellungen und Updates virtueller Applikationen

Werden neue Versionen von zu virtualisierenden Applikationen eingeführt, können zwei grundsätzliche Taktiken verfolgt werden:

- Das bestehende Paket wird aktualisiert
- Die neue Anwendungsversion wird komplett neu virtualisiert (paketiert)

Das Aktualisieren eines Paketes ist aus Konfigurations-Sicht der einfachere Weg: Da sich die ID des Pakete nicht ändert, werden die alten Konfigurationen weiterhin mit dem neuen Paketinhalt assoziiert. Die Konfigurationen bleiben erhalten. Allerdings führt ein wiederholtes Aktualisieren der Pakete nicht unbedingt zu einem stabilen Paket. Spätestens bei Major Release-Wechseln der Applikation wird gerne neu virtualisiert.

Dieses Neu-Virtualisieren erzeugt zwar saubere Pakete, aber die Verbindung des neuen Paketes zu den alten Einstellungen über die Paket-ID ist zerstört. Eine Migration der Alt-Einstellungen in das neue Paket ist recht kompliziert (bei XenApp Streaming oder ThinApp) oder faktisch gar nicht realisierbar (wie bei App-V).

UEM-Lösungen können hier einen erheblichen Mehrwert bieten, insbesondere, wenn das Laden der Applikationseinstellungen über die Technologien Filtertreiber oder Hook nutzbar ist. Die neue Version der Applikation kann sofort auf die alten Einstellungen zurückgreifen. Ist nur die Einladungs-Methode (das Heben der UEM-Lösung in die virtuelle Umgebung) möglich, lassen sich Einstellungen recht komfortabel weiter nutzen– nur ist der Konfigurationsaufwand eben deutlich höher.

Weitere UEM-Einsatzgebiete

Werden innerhalb der Organisation bestimmte Applikationen sowohl virtualisiert als auch klassisch installiert genutzt, kann ein UEM-Produkt eine wichtige Komponente zur Sicherstellung einer konsistenten Benutzerumgebung darstellen. Nur mit Hilfe des User Environment Managements ist es möglich, Applikationseinstellungen zwischen lokalen Applikationen und virtuellen Applikationen austauschbar zu machen. Je nach Integrationsfähigkeit der UEM-Software mit den AppVirt-Tools wäre es gegebenenfalls sogar möglich, Applikationskonfigurationen zwischen unterschiedlichen Applikationsvirtualisierungs-Lösungen (zum Beispiel ThinApp auf dem Desktop, App-V auf dem RDS-Server) auszutauschen.

Viele UEM-Lösungen erlauben zudem, bestimmte Voreinstellungen in die Benutzerkonfiguration zu injizieren und damit bestimmte Einstellungen der Anwender zu überschreiben. Diese Voreinstellungen lassen sich abhängig von der aktuelle Ausführungsumgebung (Online/Offline, Büro/ HomeOffice) anwenden. Dadurch sind virtuelle Applikationen flexibler in unterschiedlichen Umgebungen einsetzbar.

Eine (einfachere) Sonderform des Mischbetriebes sind Migrations-Szenarien, in denen bisher klassisch installierte Applikationen in Zukunft virtualisiert bereitgestellt werden sollen. Auch ein Wechsel des Werkzeugs zur Applikationsvirtualisierungs wird – unter dem Aspekt des Erhaltens der Applikationskonfigurationen – durch den Einsatz einer UEM-Software deutlich vereinfacht.

Die Tücken liegen im Detail

Einige der am Anfang verwendeten Formulierungen lassen bereits darauf schließen: Nicht jedes UEM-Werkzeug ist mit jeder AppVirt-Lösung beliebig integrierbar: Einige UEM-Produkte bieten eine hervorragende Integration mit bestimmten AppVirt-Tools, stehen anderen Lösungen aber blind gegenüber. Eine fundierte Aufstellung der Möglichkeiten würde – aufgrund der hohen Anzahl der UEM-Komponenten und der auch nicht unerheblichen Anzahl von AppVirt-Produkten – den Rahmen dieses Artikels sprengen. Eine derartige Matrix hätte – angesichts der rapiden Innovationszyklen einiger UEM-Produkte – auch nur eine begrenzte Halbwertszeit.

Wenn Sie vor der Entscheidung zur Einführung einer UEM- oder auch AppVirt-Lösung stehen, sollte die Integration beider nicht zwangsweise im Mittelpunkt

der Überlegungen stehen. Grundsätzlich bieten UEM-Werkzeuge eine Vielzahl an Funktionen und können somit eine hohe Zahl unterschiedlicher Anforderungen bedienen. Diese Anforderungen müssen natürlich priorisiert und bewertet werden. Ist eine Integration mit einem AppVirt-Produkt geplant, ist diese Integration auch ein Bewertungspunkt. Eine hohe Priorität sollte die AppVirt-Integration in der UEM-Bewertung aber nur erhalten, wenn gemeinsamer Zugriff von klassisch installierten und virtuellen Applikationen auf die Applikationskonfigurationen gewünscht ist. Gibt es keine Überschneidung der beiden Bereitstellungsmethoden, können die Funktionsunterstützungen für die AppVirt-Lösung relativ gering bewertet werden – wie eben erläutert, bieten die AppVirt-Werkzeuge in sich schon einige Vorteile aus Sicht der Applikationskonfiguration.

Aus strategischer Sicht ist die Festlegung auf einen UEM-Anbieter heute mit einem recht hohen Risiko verbunden. Selbst die Anbieter weit verbreiteter Lösungen wie AppSense oder RES sind noch nicht zu groß, um marginalisiert oder von anderen IT-Konzernen akquiriert zu werden. Für Anbieter mit geringeren Marktanteilen oder höheren Produktspezialisierungen gilt das natürlich nicht weniger. Egal, welche Lösung gewählt wird: Zumindest aus der (sehr fokussierten) Sicht des Applikationskonfigurations-Managements sollten die Lösungen immer in der Lage sein, Einstellungen bei Bedarf in das normale Benutzerprofil zu exportieren. Damit ist sichergestellt, dass auch bei Marktaustritt, Akquisition oder Integration in andere Lösungen immer ein Ausweg existiert.

Die Zukunft bringt mehr Layering

Während die technische Entwicklung im Bereich der Applikationsvirtualisierung zurzeit relativ stabil ist, also durch die Hersteller keine revolutionären Neuentwicklungen angekündigt wurden, entwickeln sich die Funktionen der Benutzerkonfigurations-Lösungen noch recht dynamisch. Die wichtigsten UEM-Hersteller bieten für die nächsten Versionen fast durchgehend Funktionen an, die in den Vorgängerversionen der Produkte nicht oder nur rudimentär implementiert waren.

Da die in diesem Artikel nicht besprochenen Layering-Technologien (Unidesk, Moka5, teilweise RingCube) auch aus Sicht des Applikationskonfigurations-Managements einigen Mehrwert bieten, entwickeln einige UEM-Anbieter Technologien, um Teilfunktionen des Layerings umzusetzen. Ein aktuell sehr intensiv diskutierter Ansatz sind "User Installed Applications" (UIA): Anwender installieren ihre Applikationen innerhalb einer Sitzung selber, diese Installation wird aber von der UEM-Lösung als Benutzerkonfiguration interpretiert und verwaltet. Das Installationsergebnis wird also nicht lokal auf der Maschine integriert, sondern als Bestandteil der Benutzerkonfiguration bei Bedarf geladen (natürlich mit der notwendigen Integration in das OS, wie Desktop-Shortcuts oder Dateityp-Zuordnungen).

Meldet sich der Benutzer ab, sind seine "User Installed Applications" verschwunden – und natürlich (je nach Implementierung) auch zur Laufzeit in Mehrbenutzersystemen nicht in anderen Sessions sichtbar. In den aktuellen (oder angekündigten) Implementierungen von User Installed Apps werden die Applikationen in einer Schicht bereitgestellt – die User Installed Applications sind also durchaus (teilweise) vom Betriebssystem separiert, aber nicht untereinander isoliert. In dieser aktuellen Implementierung handelt sich also (noch?) nicht um Lösungen zur Applikationsvirtualisierung. Die bisher recht klar umrissenen Grenzen zwischen den einzelnen Schichten des Technology Stack verschwimmen also zunehmend.

Fazit

Die technologischen Funktionen der Lösungen zur Anwendungsvirtualisierung, Applikationskonfigurationen granular zu speichern, lassen eine Integration mit Konfigurationsmanagement-Werkzeugen auf den ersten Blick nicht unbedingt als notwendig erscheinen: AppVirt-Software bietet einige Vorteile, die auch durch UEM erreicht werden sollen. Sollen virtuelle Applikationen aber oft aktualisiert werden, ist der Einsatz von UEM-Produkten fast zwingend. Auch wenn bestimmte Applikationen – je nach Desktop-Modell – parallel klassisch installiert und virtualisiert genutzt werden, führt kaum ein Weg an UEM vorbei. In diesem Fall sind aufgrund der Isolationseigenschaften virtueller Applikationen die Integrationsmöglichkeiten genau zu bewerten.

Natürlich bieten UEM-Lösungen in ihrer Produktvielfalt eine ganze Reihe von Mehrwertfunktionen, die für sich alleine den Einsatz des User Environment Management rechtfertigen. Die Integration mit der Applikationsvirtualisierung ist hier oft nur ein Aspekt der Produktbewertung. Riskant sind die hohe Herstellersegmentierung und die Funktionsvielfalt der UEM-Tools. Während sich bei der Applikationsvirtualisierung einige sehr wenige Hersteller und ein technologischer Ansatz scheinbar durchgesetzt haben, gibt es diese klare Bereinigung im Bereich von UEM noch nicht – vielmehr etablieren sich andere technologische Konzepte wie das Layering, die UEM-Teilfunktionen enthalten.

Spannend ist darüber hinaus, ob und wie UEM-Anbieter ihre Lösungen mit zukünftigen Generationen der Applikationsvirtualisierung integrieren können. Änderungen am Applikationsvirtualisierungs-Layer können dazu führen, dass Hooks oder Filtertreiber der UEM-Lösung "blind" werden. Sehr interessant ist die Entwicklung einiger UEM-Anbieter, durch User Installed Applications technologisch in Teilbereiche der Applikationsvirtualisierung vorzustoßen – und zwar mit Vorteilen, die die reine Applikationsvirtualisierung aktuell nur selten bieten kann. *(ln)*

Falko Gräfe ist als Senior Consultant und Trainer bei Login Consultants Germany GmbH mit den Schwerpunkten Anwendungs- und Desktop-Virtualisierung beschäftigt. Er ist MVP für App-V.

[1] Whitepaper "User Environment Management Smackdown" C1P01

[2] Whitepaper "Application Virtualization Smackdown" C1P02

Link-Codes

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 0112

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: pixelio.de

OpenVPN im Praxiseinsatz

Der sichere Weg nach Hause

von Dr. Holger Reibold

Mit Hilfe von virtuellen privaten Netzen, kurz VPN, lässt sich eine sichere Kommunikation über das Internet realisieren. Sie sind häufig bereits seit Jahren fester Bestandteil der Kommunikationsinfrastruktur von Unternehmen. Neben einer Vielzahl kommerzieller und zum Teil auch proprietärer VPN-Produkte hat sich OpenVPN – die SSL-VPN-Lösung aus dem Open Source-Lager – inzwischen einen festen Platz erarbeitet. Doch in der Praxis muss so manche Hürde genommen werden, insbesondere beim Umgang mit dynamischen IP-Adressen, NAT und Proxy-Servern, wie Ihnen dieser Workshop zeigt.

Während die meisten kommerziellen VPN-Produkte auf dem IPsec-Standard basieren, liegen die Vorzüge von OpenVPN in anderen Bereichen – bei gleichwertigem Sicherheitsniveau übrigens. So sind die Konfiguration und die Administration des VPN-Servers und der Clients in der Regel wesentlich einfacher. Ein weiterer Pluspunkt: OpenVPN kann problemlos über Firewalls, NAT-Gateways und Proxy-Server kommunizieren. Und OpenVPN steht als Server und als Client für alle relevanten Betriebssysteme (Windows, Linux, Mac OS X, BSD und Solaris) zur Verfügung.

Gerade erfahrene Administratoren schätzen OpenVPN als zuverlässiges und robustes System, um gesicherte Verbindungen zwischen Rechnern und Netzen über das Internet herzustellen. Ein weiterer Punkt spricht für den Einsatz von OpenVPN – gerade in Zeiten knapper Kassen: Für den Einsatz von OpenVPN fallen keine Lizenzgebühren an.

Die Betriebsmodi von OpenVPN

OpenVPN unterstützt verschiedene Betriebsmodi. Sofern in der OpenVPN-Konfigurationsdatei nicht anders definiert, nutzt die Sicherheitsumgebung standardmäßig den Point-to-Point-Modus. Es empfiehlt sich, den Betriebsmodus explizit in der Konfigurationsdatei aufzuführen, da die Konfigurationsdatei so leichter verständlich und auch für Dritte einfach zu interpretieren ist. Der sogenannte Point-to-Point Modus verlangt für jeden Tunnelendpunkt eine eigene Konfigurationsdatei und verwendet exklusiv einen eigenen TCP- oder UDP-Port. In der Praxis ist es daher nur sinnvoll, den Point-to-Point-Modus zu verwenden, wenn Ihr VPN lediglich aus zwei Teilnehmern besteht. In der Konfigurationsdatei aktivieren Sie mit der folgenden Direktive den Peer-to-Peer-Modus: *mode p2p*.

In der Praxis kommen allerdings eher typische Remote Access-Szenarien zum Einsatz, bei denen sich mehrere Benutzer über einen zentralen Server in ein Netzwerk einwählen. Hier sprechen wir daher auch vom Server-Modus. Bei dieser Variante werden alle eingehenden Verbindungen von einem einzigen Serverprozess verwaltet. Dabei muss in der Firewall auch nur ein Port geöffnet werden. Da sich die Beschränkung auf eine einzelne Konfigurationsdatei beschränkt, vereinfachen sich die Administration und Wartung natürlich erheblich. Um den Server-Modus in der OpenVPN-Konfigurationsdatei zu aktivieren, verwenden Sie die Direktive *mode server*.

Zum Server-Modus hat OpenVPN auch das passende Gegenstück zu bieten: den Client-Modus. Wie beim Server- und P2P-Modus erfolgt die Client-Definition in der OpenVPN-Konfigurationsdatei. Hierfür wird das Schlüsselwort *client* verwendet. Der Client-Modus von OpenVPN erlaubt es, mehrere Clients mit einer spezifischen Client-Konfiguration zu versehen. Somit kann der Server beispielsweise den Clients beliebige IP-Adressen zuweisen oder die Routing-Tabelle auf dem Betriebssystem des Clients manipulieren. Prinzipiell können Sie ein- und dieselbe Konfigurationsdatei für eine große Anzahl an Clients verwenden. Abhängig von der gewählten Authentifizierungsmethode – static Key-Mode oder SSL/TLS-Mode mit Zertifikaten – sollten Sie allerdings für jeden Benutzer ein eigenes Zertifikat mit individuellem Common Name (CN) nutzen. Es ist zwar auch prinzipiell möglich, dass sich mehrere Benutzer ein Zertifikat teilen. Doch das bringt ein anderes Problem: Bei jedem Ausscheiden eines Teilnehmers muss das Zertifikat auch bei allen anderen Clients geändert werden.

Für das Verbinden von Netzwerken gibt es zwei verschiedene Prinzipien: Routing und Bridging. Jeder dieser Ansätze bietet

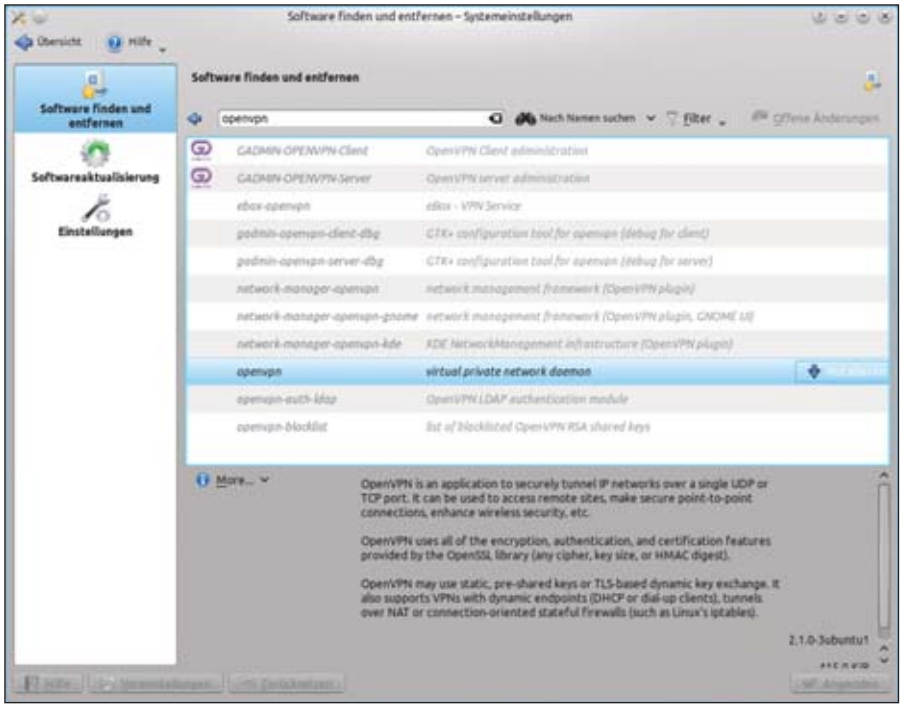


Bild 1: Mithilfe eines Paketmanagers ist OpenVPN schnell und zuverlässig installiert

spezifische Vor- und Nachteile. In der Regel ist der Routing- dem Bridging-Modus vorzuziehen, da dieser eine bessere Skalierbarkeit gewährleistet. Je größer die Anzahl der Teilnehmer am VPN ist, um so eher ist das Routing-Prinzip geeignet.

OpenVPN in Betrieb nehmen

Schauen wir uns als Nächstes an, wie Sie OpenVPN in Betrieb nehmen. Die Sicherheitslösung steht als Source-Code-Paket für Unix-Betriebssysteme wie BSD, Mac OS X, Solaris und Linux sowie für Windows-Betriebssysteme zum Download [1] bereit. Besonders einfach ist die Installation des entsprechenden Pakets mithilfe des Paketmanagers Ihrer Distribution. Die aktuelle Version ist OpenVPN 2.2.1. Unter Windows ist die Installation ebenfalls sehr einfach durchzuführen: Starten Sie einfach das Installationsprogramm und folgen Sie den wenigen Anweisungen am Bildschirm.

Die eigentliche Konfiguration von OpenVPN erfolgt bei allen Betriebssystemen über die Konfigurationsdateien. Das Schöne dabei: Sie können eine unter Linux erstellte OpenVPN-Konfigurationsdatei prinzipiell auch unter Windows verwenden. Sie müssen nur darauf achten, dass Windows und Linux unterschiedliche Zeichen für das Zeilenende verwenden.

Nachdem Sie OpenVPN installiert haben, können Sie mit einem ersten Verbindungsaufbau die OpenVPN-Funktionalität testen. Dazu erzeugen Sie zunächst einen statischen Key, dann die Server- und schließlich die Client-Konfigurationsdatei. Exemplarisch beschreiben wir die Verwendung von Linux als Server- und Windows als Client-Plattform. Wenn Sie OpenVPN aus den Quellen übersetzt und den beschriebenen Kryptografietest durchgeführt haben, besitzen Sie bereits einen Static-Key namens "test.key". Um einen neuen Key zu erzeugen, verwenden Sie folgenden Befehl:

```
openvpn –genkey
  –secret
  myopenvpn.key
```

Die Schlüsseldatei wird im aktuellen Verzeichnis abgelegt. Kopieren Sie diese auf einen geeigneten Datenträger, damit Sie sie auf Ihren (Windows)-Client übertragen können. Als Nächstes erstellen Sie die sehr einfache Konfiguration für Ihren VPN-Server und den VPN-Client. Auf dem (Linux-)Server starten Sie Ihren bevorzugten Editor und hinterlegen dort folgenden Code:

```
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret myopenvpn.key
```

Speichern Sie die Datei als *server.conf* ab. In der Konfiguration sind folgende Einstellungen hinterlegt:

- Als Schnittstelle wird ein TUN-Device verwendet.
- Dem TUN-Device wird auf dem Server die IP-Adresse 10.8.0.1 zugewiesen.
- Als Schlüssel kommt die Datei *myopenvpn.key* zum Einsatz.

Auf dem Windows-Client legen Sie folgende Konfiguration an:

```
remote {IP-Adresse des Servers}
dev tun
ifconfig 10.8.0.2 10.8.0.1
C:\\Programme\\OpenVPN\\secret
  test.key
```

Beachten Sie, dass Sie bei der Pfadangabe für den Key einen doppelten Backslash verwenden müssen. Sichern Sie die Datei als *client.ovpn* im Verzeichnis *C:\Programme\OpenVPN\config*. Starten Sie als Nächstes die OpenVPN-Installation auf dem Server und geben Sie die Server-Konfigurationsdatei als Parameter an: *openvpn server.cfg*. Anschließend gibt OpenVPN nach dem erfolgreichen Start eine Statusmeldung aus.

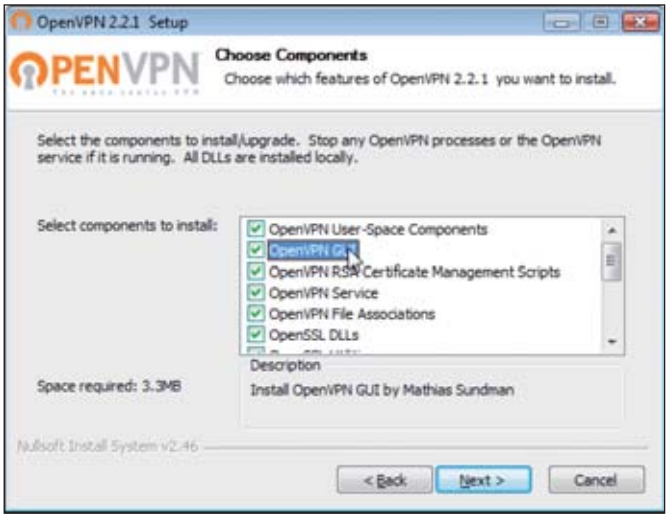


Bild 2: Das Windows-Setup bietet Ihnen die Auswahl der verschiedenen OpenVPN-Komponenten an

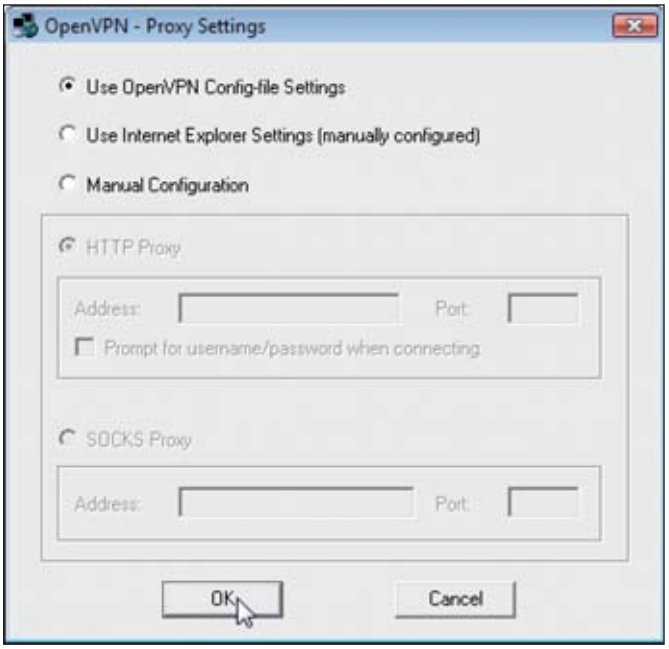


Bild 3: OpenVPN unter Windows: Über das System-Tray-Icon greifen Sie auf die OpenVPN-GUI zu, die auch die Konfiguration eines Proxy Servers erlaubt

Der nächste Schritt dient dem Herstellen einer VPN-Verbindung vom Windows-PC zum Server. Dazu klicken Sie mit der rechten Maustaste auf das OpenVPN-Icon im Windows-System-Tray und führen den Befehl *Connect* aus. Der Client öffnet das Log-Fenster, in dem der aktuelle Status der Verbindung angezeigt wird. Kommt die Verbindung zustande, so erhält die TUN-Schnittstelle die IP-Adresse 10.8.0.2 zugewiesen. Nach dem erfolgreichen Verbindungsaufbau sollten Sie vom Client aus die IP-Adresse des TUN-Interfaces des Servers anpingen können – und umgekehrt: *ping -c 3 10.8.0.1*.

Sollte sich im config-Verzeichnis nur eine ovpn-Datei befinden, stellt OpenVPN-GUI automatisch eine Verbindung mit dieser Konfiguration her. Sollten Sie allerdings mehrere ovpn-Dateien in diesem Verzeichnis abgelegt haben, stellt Ihnen die OpenVPN-GUI diese zur Auswahl.

Konfiguration der Sicherheitsumgebung

Ihre OpenVPN-Umgebung legt die Konfigurationsdatei und die Schlüssel beziehungsweise die Zertifikate unter Linux standardmäßig im Verzeichnis */etc/openvpn* ab, unter Windows in *C:\Programme\ OpenVPN\config*. Haben Sie mithilfe von Easy-RSA bereits ein Zertifikat für Ihren Server generiert und das easy-rsa-Verzeichnis nach */etc/openvpn* kopiert, so finden Sie im Verzeichnis */etc/openvpn/easy-rsa/2.0/keys* sämtliche Zertifikate, die Datei mit den Diffie-Hellman-Parametern sowie die Zertifikatsrückzugsliste (*crl.pem*). Um den OpenVPN-Server verwenden zu können, benötigen Sie die Dateien *ca.crt*, *ca.key*, *crl.pem*, *dh2048.pem*, *server.crt*, *server.csr* und *server.key*. Kopieren Sie diese ebenfalls nach */etc/openvpn*.

Die oben vorgestellte, einfache Konfigurationsdatei taugt lediglich für einen ersten Testlauf. Wenn Sie OpenVPN produktiv einsetzen, wird die Konfiguration naturgemäß aufwendiger. Legen Sie mit einem Editor Ihrer Wahl im Verzeichnis */etc/openvpn* die Serverkonfigurationsdatei *server.conf* an (siehe Kasten "Serverkonfigurationsdatei").

Werfen wir einen detaillierten Bick auf die Konfigurationsdatei: Mit den Direktiven "mode server", "proto udp" und "dev tun" bestimmen Sie, dass es sich um einen OpenVPN-Server handelt, der den Standardport 1194/UDP verwendet und als virtuelle Schnittstelle für das VPN ein TUN-Device bereitstellt. Alternativ könnten Sie auch ein gebridgtes VPN aufsetzen, das eine TAP-Device-Schnittstelle verwendet.

Die Direktive "management 127.0.0.1 44000" aktiviert das OpenVPN-Management-Interface so, dass es lediglich vom Server aus ansprechbar ist. Mit den folgenden Konfigurationseinträgen "ca ca.crt", "cert server.crt" und "key server.key" geben Sie die Bezeichnungen der zu verwendenden Zertifikate für die CA und Schlüssel an.

Danach finden Sie den Eintrag "crl-verify crl.pem". Damit sorgen Sie dafür, dass der OpenVPN-Server mithilfe der Datei *crl.pem* zurückgezogene Zertifikate identifizieren kann. Der Parameter "dh dh2048.pem" gibt die Datei an, in der die Diffie-Hellman-Parameter hinterlegt sind, "server 10.5.5.0 255.255.255.0" bestimmt, dass OpenVPN mit dem virtuellen Netzwerk "10.5.5.0/24" arbeitet und IP-Adressen aus diesem Netzwerk an die Clients vergibt. Dem OpenVPN-Server wird im-

Integration von OpenVPN in IPCop

Bereits für IPCop Version 1.4 gab es das Add-on Zerina, das die Firewall-Umgebung um OpenVPN erweiterte. In IPCop 2.0, das im September 2011 freigegeben wurde, ist das VPN-Modul integriert. IPCop stellt Ihnen über das VPN-Menü mehrere VPN-spezifische Funktionen zur Verfügung. Hier finden Sie auch die OpenVPN-Integration. Vor dem Start und dem Einsatz des OpenVPN-Servers müssen Sie über das Menü "VPN / CA" die Zertifizierungsstelle erstellen. Anschließend können Sie sich mit dem Befehl "VPN / OpenVPN" an die Einstellungen des Tunnelsystems machen. Die globalen Einstellungen zeigen Ihnen in der ersten Zeile an, ob der OpenVPN-Server gestartet oder angehalten ist. Aktivieren Sie das Kontrollkästchen "OpenVPN auf ROT", um OpenVPN für die roten Schnittstellen nutzbar zu machen. Tragen Sie außerdem unter "Lokaler VPN-Hostname/IP" den vollqualifizierten Domänennamen oder die öffentliche IP-Adresse der roten Schnittstelle ein. Wenn Sie einen dynamischen DNS-Service nutzen, geben Sie hier Ihren dynamischen DNS-Namen ein. In den erweiterten OpenVPN-Einstellungen können Sie verschiedene DHCP-Einstellungen, Push-Routen und Logfile-Optionen vornehmen.

Serverkonfigurationsdatei

```
# Basiskonfigurationsdatei für den OpenVPN-Server
mode server
proto udp
dev tun
management 127.0.0.1 44000
ca ca.crt
cert server.crt
key server.key
crl-verify crl.pem
dh dh2048.pem
server 10.5.5.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
```

mer die erste IP-Adresse aus dem hier angegebenen Netz zugewiesen.

Der Eintrag "ifconfig-pool-persist ipp.txt" sorgt dafür, dass OpenVPN in der Datei *ipp.txt* festhält, welchem Client welche IP-Adresse zugewiesen wurde. So können Sie sicherstellen, dass der betroffene Client nach einem Verbindungsabbruch stets wieder die gleiche IP-Adresse erhält. Beim Parameter "keepalive 10 120" handelt es sich um eine sogenannte Helper-Direktive. Die Konfiguration "comp-lzo" sorgt dafür, dass die übertragenen Daten mit dem LZO-Verfahren komprimiert werden.

Mit den beiden Konfigurationen "user nobody" und "group nogroup" entziehen Sie dem OpenVPN-Prozess aus Sicherheitsgründen nach dem Start des Daemons die Root-Rechte wieder. Beachten Sie dabei, dass dies nur beim Einsatz unter Linux funktioniert. Sie müssen außerdem sicherstellen, dass der User "nobody" und die Gruppe "nogroup" auf Ihrem System existieren. Die nächsten Einstellungen stellen sicher, dass bei einem womöglich erforderlichen Neustart des Tunnels die Schlüsseldatei nicht neu eingelesen (persist-key), das virtuelle Netzwerk-Interface nicht geschlossen und wieder geöffnet wird (persist-tun).

Mit dem Parameter "status openvpn-status.log" ist sichergestellt, dass der Zustand des OpenVPN-Servers in die Datei *openvpn-status.log* geschrieben wird. Die Protokolldatei wird automatisch erzeugt und im Verzeichnis */etc/openvpn* abgelegt. Mit dem letzten Parameter (verb 3) bestimmen Sie schließlich die Geschwätzigkeit, also wie detailliert die Logmeldungen des OpenVPN-Daemons ausfallen.

Automatischer Start

Wenn Sie OpenVPN als festen Service in Ihre Infrastruktur integrieren, so werden Sie den Server natürlich nicht bei jedem Systemstart manuell hochfahren wollen. Wenn Sie OpenVPN unter Linux ausführen, lässt sich das recht einfach mit den Init-Skripts realisieren.

Der VPN-Server legt bereits bei der Installation ein Init-Skript mit der Bezeichnung *openvpn* ins Verzeichnis */etc/init.d*. Das Skript startet nach einem Neustart den OpenVPN als Daemon. Der wiederum sucht im Verzeichnis */etc/openvpn* nach Konfigurationsdateien mit der Dateierweiterung "conf" und startet für jede gefundene Konfigurationsdatei je einen eigenen OpenVPN-Daemon.

Abhängig von dem von Ihnen verwendeten Betriebssystem müssen Sie dafür sorgen, dass der Start von OpenVPN im gewünschten Runlevel auch tatsächlich erfolgt. Wenn Sie Debian oder Ubuntu verwenden, erledigt das folgender Befehl:

```
root@rechner:/etc/openvpn# update-
  rc.d openvpn defaults
 Adding system startup for
  /etc/init.d/openvpn ...
   /etc/rc0.d/K20openvpn ->
  ../init.d/openvpn
   /etc/rc1.d/K20openvpn ->
  ../init.d/openvpn
   /etc/rc6.d/K20openvpn ->
  ../init.d/openvpn
   /etc/rc2.d/S20openvpn ->
  ../init.d/openvpn
   /etc/rc3.d/S20openvpn ->
  ../init.d/openvpn
   /etc/rc4.d/S20openvpn ->
  ../init.d/openvpn
   /etc/rc5.d/S20openvpn ->
  ../init.d/openvpn
```

Mit dem Kommando */etc/init.d/openvpn start* prüfen Sie, ob der Daemon alle benötigten Dateien für den automatischen Start gefunden hat. Ist das der Fall, wird folgende Erfolgsmeldung ausgegeben: * *server (OK)*. Sollten Sie die Meldung * *server (FAILED)* erhalten, verrät ein Blick in die Protokolldatei */var/log/syslog* beziehungsweise */var/log/messages*, woran die Ausführung scheitert.

Kann OpenVPN alle benötigten Dateien einlesen, steuern Sie den OpenVPN-Daemon mit den Befehlen:

```
/etc/init.d/openvpn {start|stop|
  reload|restart|force-reload|
  cond-restart}
```

Beim nächsten Systemstart sollte OpenVPN nun automatisch mit Ihrer Serverkonfiguration starten. Das können Sie mit einem Blick in die Prozessliste des Servers prüfen:

```
root@rechner# ps wax | grep openvpn
5440 ?        Ss     0:00 /usr/
  local/sbin/openvpn –writepid
  /var/run/openvpn.server.pid
  –daemon ovpn-server –cd
  /etc/openvpn –config
  /etc/openvpn/server.conf
```

WLAN absichern

Eine der häufigsten Anforderungen an eine VPN-Umgebung ist die Absicherung von WLAN-Verbindungen für mobile Clients. Exemplarisch sei die Konfiguration bei folgendem Einsatzszenario illustriert: Der OpenVPN-Server auf Linux-Basis verfügt über zwei Netzwerkschnittstellen bei aktiviertem IP-Forwarding. Der eine Adapter sorgt für die Ethernet-Anbindung, der andere für die

```
# Konfigurationsdatei fuer den OpenVPN Server
   (WLAN)
mode server
proto udp
dev tun
management 127.0.0.1 44000
ca ca.crt
cert server.crt
key server.key
crl-verify crl.pem
dh dh2048.pem
server 10.5.5.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Konfigurationsdatei für den OpenVPN-Server (WLAN)

```
# Konfigurationsdatei fuer den OpenVPN-Client
   (WLAN)
client
dev tun
proto udp
comp-lzo
remote 192.168.120.253
route 192.168.1.0 255.255.255.0 10.5.5.5
redirect-gateway
ca ca.crt
cert tzn.crt
key tzn.key
ns-cert-type server
verb 3
```

Konfigurationsdatei für den Client (WLAN)

OpenVPN mit Android

Um die Kommunikation eines Android-Smartphones mithilfe von OpenVPN abzusichern, muss der OpenVPN-Client auf dem Smartphone installiert werden. Für Android-Geräte gibt es im Android Market verschiedene Apps. Um OpenVPN zu installieren, verwenden Sie am besten den OpenVPN Installer von Sascha Volkenandt. Das Installationsprogramm prüft verschiedene Systemvoraussetzungen und gibt gegebenenfalls die entsprechenden Hinweise aus, welche Komponenten vor der OpenVPN-Einrichtung installiert werden müssen. Anschließend bietet sich der Download von OpenVPN GUI an. Auch diese App finden Sie im Android Market. Sie ermöglicht das Starten und Stoppen von OpenVPN-Verbindungen.

Verbindung zum WLAN-Access-Point. Der Access Point selbst arbeitet als Bridge und das WLAN verwendet ein eigenes privates IP-Netz.

In der Regel ist das Ziel, die Kommunikation aller WLAN-Clients mithilfe von OpenVPN abzusichern. Dazu benötigen Sie zunächst die entsprechenden Zertifikate und Keys. Sind diese erzeugt und auf die beteiligten Systeme verteilt, können Sie sich an das Erstellen der Konfigurationsdateien für den Server und Ihre WLAN-Clients machen. Dazu führen Sie zunächst OpenVPN auf dem Server aus: *openvpn server.conf*. Dann starten Sie OpenVPN mit *openvpn client.conf* auf den Clients.

In den Protokolldateien können Sie gegebenenfalls prüfen, ob die Verbindung zustande gekommen ist. Das Standard-Gateway des Clients und die Route ins LAN zeigen nun nicht mehr auf die WLAN-IP-Adresse des OpenVPN-Servers, sondern auf den Tunnelendpunkt des Clients. Die gesamte Kommunikation in das LAN und ins Internet wird vollständig über OpenVPN verschlüsselt. Das lässt sich recht einfach mit einem Netzwerksniffer prüfen. Wenn Sie die VPN-Verbindung beenden, werden die Routen in Richtung LAN und Internet wieder auf die WLAN-Schnittstelle umgestellt und der Datenverkehr wird wieder unverschlüsselt übermittelt. In den Kästen "Konfigurationsdatei für den OpenVPN-Server (WLAN)" und "Konfigurationsdatei für den Client (WLAN)" finden Sie zwei Musterkonfigurationsdateien, die Ihnen als Grundlage für die Umsetzung in Ihrer Infrastruktur dienen.

Dynamische IP-Adresse an beiden Endpunkten

OpenVPN unterscheidet sich in einem Punkt von vielen anderen VPN-Lösungen: Die freie Umgebung kann hervorragend mit dynamischen IP-Adressen umgehen. Das gilt für Clients und Server – sogar gleichzeitig. Die Integration erfolgt mithilfe eines dynamischen DNS-Dienstes wie *DynDNS.com*. Bei den meisten DSL-Routern ist heute bereits ein DynDNS-Client für die Nutzung eines solchen Dienstes integriert. Sie müssen daher lediglich auf der Website des jeweiligen Anbieters einen Account anlegen. Beim Anlegen bestimmen Sie die Zugangsdaten sowie einen oder mehrere Hostnamen unter einem der vom DynDNS-Anbieter angebotenen Domainnamen.

Wenn Sie OpenVPN auf einem Linux-System betreiben, können Sie statt des DynDNS-Clients im Router zu ddclient [2] greifen. Das Perl-Skript ist einfach zu konfigurieren und läuft als Daemon im Hintergrund. Wenn Sie einen Windows-Server bevorzugen, greifen Sie zum kostenlosen DynDNS-Updater [3]. Immer dann, wenn Ihnen durch Ihren Provider eine IP-Adresse zugewiesen wird, übermittelt der DynDNS-Client die neue IP-Adresse an die DNS-Server. Erfolgt die Trennung während einer bestehenden Verbindung zum Server, ist sie in der Regel für kurze Zeit nicht benutzbar.

Wird die neue IP-Adresse vom DynDNS-Client zum DynDNS-Provider und von dort zu den DNS-Servern im Internet rasch übertragen, können Sie in der Regel die bestehende Verbindung weiter verwenden. Dafür sorgt der Parameter "keepalive 10 120" in der Serverkonfiguration. Mit dieser Einstellung prüft der Server alle zehn Sekunden, ob die Verbindung zum Client noch steht. Ist der Client 120 Sekunden lang nicht erreichbar, wird die Verbindung getrennt und anschließend neu initiiert.

Umgang mit NAT

Da Sie Ihren OpenVPN-Server mit großer Wahrscheinlichkeit hinter einem NAT-Gerät, also beispielsweise hinter einem DSL-Router betreiben, nutzt dieser den bekannten privaten Adressraum, der in RFC 1918 definiert ist. Da diese Adressen nicht ins Internet geroutet werden, sind sie auch nicht direkt erreichbar. Damit Sie aber dennoch Ihren lokalen OpenVPN-Server unter seiner privaten IP-Adresse aus dem Internet ansprechen können, muss das vorgelagerte NAT-Device die Port-Weiterleitung unterstützen. Erfüllt Ihre Infrastruktur diese Voraussetzungen, ist ein Ansprechen des VPN-Servers in der Regel problemlos möglich, auch, weil OpenVPN mit nur einem Port auskommt.

Wenn Sie den OpenVPN-Server in einer Standardkonfiguration betreiben, müssen Sie im NAT-Device lediglich folgende Portweiterleitung anlegen:

- Protokoll: UDP
- Public Port: 1194
- Private IP: IP-Adresse des OpenVPN-Servers
- Private Port: 1194

Alle von außen eingehenden Datenpakete auf Port 1194/UDP werden dann vom Router an den OpenVPN-Server im LAN weitergereicht.

Fazit

Mit OpenVPN steht Ihnen eine vorzügliche VPN-Lösung zur Verfügung, die auch professionellen Ansprüchen genügt. In der Praxis verhält sich OpenVPN sehr stabil und bietet für alle typischen Einsatzszenarien die passenden Einstellungen. Sollten Probleme oder Fragen auftauchen, steht Ihnen eine sehr aktive Community mit Rat und Tat zur Seite. *(jp)*

Link-Codes

[1] OpenVPN: Download und Forum
C1P51

[2] ddclient
C1P52

[3] DynDNS-Updater
C1P53

Fast Lane

Fast Lane, die Spezialisten für:

Training & Consulting rund um sichere IT-Infrastrukturen

Content Security • Endpoint Security • Firewalls • Security Management • VoIP Security • Virtual Private Networks • Wireless Security

Security-Trainings, z.B.:

IP Security Fundamentals (IPSF)		
28.03.2012 Düsseldorf	02.05.2012 Hamburg	04.06. 2012 Stuttgart
Anti-Hacking Workshop (HACK)		
05.03.2012 Hamburg	02.04.2012 Düsseldorf	23.04. 2012 München
Voice Anti-Hacking Workshop (VHACK)		
28.03.2012 Berlin	06.06.2012 Hamburg	25.07.2012 Frankfurt
WLAN Anti-Hacking Workshop (WHACK)		
01.02.2012 Düsseldorf	02.04.2012 Berlin	13.06.2012 Hamburg
Malware Inside (MWI)		
26.03.2012 Berlin	04.06.2012 Hamburg	23.07.2012 Frankfurt
IT-Forensik (ITF)		
16.04.2012 Berlin	11.06.2012 Hamburg	06.08.2012 Frankfurt
Check Point CCSA & CCSE Power Workshop (CPPW)		
06.02.2012 Frankfurt	27.02.2012 Düsseldorf	19.03.2012 Hamburg
Securing Your Web with Cisco IronPort S-Series (SYW)		
09.02. 2012 Berlin	23.02.2012 Hamburg	15.03.2012 München
Securing Your Email with Cisco IronPort C-Series (SYEPW)		
06.02.2012 Berlin	20.02.2012 Hamburg	12.03.2012 München

Implementing Cisco IOS Network Security (IINS)		
13.02.2012 München	05.03.2012 Düsseldorf	12.03.2012 Berlin
Securing Networks with Cisco Routers & Switches (SECURE)		
06.02.2012 Hamburg	12.03.2012 Düsseldorf	19.03.2012 Leipzig
Deploying Cisco ASA Firewall Features (FIREWALL)		
06.02.2012 Stuttgart	13.02.2012 Hamburg	27.02.2012 München
Deploying Cisco ASA VPN Solutions (VPN)		
13.02.2012 Stuttgart	20.02.2012 Hamburg	05.03.2012 München
Implementing Cisco Intrusion Prevention System (IPS)		
06.02.2012 Berlin	20.02.2012 Stuttgart	27.02.2012 Hamburg
Introduction to 802.1X Operations for Cisco Security Professionals (802.1X)		
01.02.2012 Hamburg	07.03.2012 München	02.04.2012 Frankfurt
Implementing Cisco Identity Service Engine Secure Solutions (ISE)		
27.02.2012 Hamburg	26.03.2012 Frankfurt	16.04.2012 Stuttgart
Implementing Cisco Security MARS (MARS)		
14.02.2012 Frankfurt	27.03.2012 Stuttgart	10.04.2012 Düsseldorf
Advanced IPSec (AIPSEC)		
27.02.2012 Hamburg	19.03.2012 Frankfurt	23.04.2012 Stuttgart

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

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

NetApp Partner Award 2011

Cisco Partner Learning Specialized

NetApp Authorized Learning Partner

vmware PARTNER AUTHORIZED TRAINING CENTER

Symantec. Authorized Education Delivery Partner

Sicherheitsvorfälle im Active Directory erkennen (2)

Überwachung leicht gemacht

Quelle: Regisser - Fotolia.com

von Thomas Gronenwald

Wie im ersten Teil unserer Workshop-Serie dargestellt, sollten Server- und Clientsysteme überwacht werden, um die Systemsicherheit und Systemintegrität aufrechtzuerhalten. Nur so decken Sie mögliche Sicherheitslücken, Verstöße gegen die geltenden Sicherheitsrichtlinien oder gar Angriffe durch Außen- und Innentäter auf und können Gegenmaßnahmen einleiten. Im zweiten und abschließenden Teil unserer Workshopserie gehen wir auf die erweiterten Überwachungsrichtlinien in Windows Server 2008 R2 sowie die Überwachung via PowerShell ein.

Die Active Directory Domain Services (AD DS) unter Windows Server 2008 R2 bieten neben den standardmäßig bereits unter Windows Server 2003 verfügbaren neun Überwachungsrichtlinien nun weitere 53 sogenannte Unterkategorien, die innerhalb der erweiterten Überwachungsrichtlinien unter "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Erweiterte Überwachungsrichtlinienkonfiguration" zu finden sind. Neben den bereits unter Windows Server 2003 verfügbaren Kategorien kamen die folgenden Überwachungsrichtlinienkategorien hinzu:

- Kontoanmeldung
- Kontenverwaltung
- Detaillierte Überwachung
- DS-Zugriff
- Anmelden/Abmelden
- Objektzugriff
- Richtlinienänderung
- Berechtigungen
- System
- Globale Objektzugriffsüberwachung

Mit Hilfe dieser neuen Einstellungen lässt sich das Verhalten der zu überwachenden Ereignisse besser und präziser steuern. Einträge, die ohne oder nur von geringer Bedeutung sind, lösen Sie einfach aus der Überwachung heraus, damit diese das Event Log nicht mehr mit unnötigen Informationen füllen. Dabei verwenden Sie die erweiterten Überwachungseinstellungen anstelle der neun grundlegenden Überwachungseinstellungen unter "Lokale Richtlinien / Überwachungsrichtlinie". Genauer gesagt sollten Sie diese auch anstelle der neun standardmäßig vorhandenen Richtlinien verwenden – eine Kombination beider Richtlinienarten ist nicht empfehlenswert.

Die passende Protokollierung

Sie sollten sich vorab Gedanken über geeignete Methoden der zentralen Sicherung von Protokolldateien machen. Neben vielen kommerziellen Lösungen bietet Microsoft in der aktuellsten Version auch die Möglichkeit, Protokolleinträge an einen zentralen Log-Server weiterzuleiten. Ebenso ist es je nach Größe der zu überwachenden IT-Infrastruktur ratsam, geeignete Mechanismen zur Alarmierung zu integrieren. Auch hier bietet Microsoft diverse Lösungen an. Von den kostenpflichtigen System Center-Lösungen über selbst erstellte PowerShell-Skripte, mit denen sich das Event Log übrigens hervorragend verwalten lässt, bis hinzu kostenlosen Lösungen wie beispielsweise Nagios.

Neben den bereits angedeuteten Voraussetzungen für eine funktionierende Überwachung spielt die Systemzeit der einzelnen Server- und Computersysteme eine existenzielle Rolle bei der Systemüberwachung und der Auswertung protokollierter Sicherheits-Logs. Insbesondere, wenn mehrere Systeme, die voneinander abhängig sind, überwacht werden, sollte die Systemzeit auf allen Systemen einheitlich und synchron sein. Überprüfen und überwachen Sie daher die Synchronisierung der Uhrzeit genau und konfigurieren Sie diese nach den Hersteller-Best Practices – nur so lässt sich im Ernstfall eine valide Aussage über einen Sicherheitsvorfall treffen.

Standard versus erweiterte Überwachungsrichtlinien

Wie bereits erwähnt, können Sie in Windows Server 2008 R2 und Windows

Datenschutz beachten

Wichtig ist es, bevor Sie geeignete Überwachungsrichtlinien definieren und testen, den Datenschutzbeauftragten und den Personal- oder Betriebsrat frühzeitig in die Planung der Überwachungsmaßnahmen einzubeziehen – so ersparen Sie sich in der Regel unnötigen Aufwand. Denn bei einer Überwachung erfassen Sie zumeist auch personenbezogene Daten, um im Falle einer Sicherheitsverletzung den Verursacher zuverlässig feststellen zu können. Dies wiederum muss natürlich datenschutzrechtlich betrachtet und innerhalb von Datenschutz- und Sicherheitsrichtlinien fest verankert werden.

7 auch durch die erweiterten Überwachungsrichtlinien das Clientverhalten auf dem Computer gezielter überwachen, um Angriffe schneller zu identifizieren. Ein gutes Beispiel hierfür ist die Richtlinieneinstellung für Anmeldeereignisse. Hier gab es in Windows Server 2003 unter "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Lokale Richtlinien / Überwachungsrichtlinie" lediglich die Option "Anmeldeereignisse überwachen". Innerhalb der erweiterten Überwachungsrichtlinien unter "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Erweiterte Überwachungsrichtlinienkonfiguration / Systemüberwachungsrichtlinien" hingegen stehen in der Kategorie "An-/Abmeldung" nun insgesamt neun unterschiedliche Optionen zur Auswahl. Auf diese Weise können Sie wichtige Aspekte der An- und Abmeldung, die Sie nachvollziehen möchten, präziser steuern. Eine Auswertung ist außerdem auch mit weniger Aufwand verbunden, da schlichtweg weniger Einträge generiert werden.

Konflikte vermeiden

Um im Betrieb Problemen vorzubeugen, gilt es einige Punkte in Bezug auf die erweiterte Überwachung zu berücksichtigen. Verwenden Sie sowohl die grundlegenden neun Überwachungsrichtlinieneinstellungen unter "Lokale Richtlinien / Überwachungsrichtlinie" als auch die erweiterten Einstellungen unter "Erweiterte Überwachungsrichtlinienkonfiguration", kann dies nämlich zu unerwarteten Ergebnissen führen. Kombinieren Sie daher die beiden Komponenten mit Überwachungsrichtlinieneinstellungen nicht miteinander.

Verwenden Sie die Einstellungen unter "Erweiterte Überwachungsrichtlinienkonfiguration", sollten Sie die Richtlinieneinstellung "Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen (Windows Vista oder höher), um Kategorieeinstellungen der Überwachungsrichtlinie außer Kraft zu setzen" unter "Lokale Richtlinien / Sicherheitsoptionen" nutzen. Damit verhindern Sie Konflikte zwischen ähnlichen Einstellungen, indem die grundlegenden Sicherheitsüberwachungen ignoriert werden.

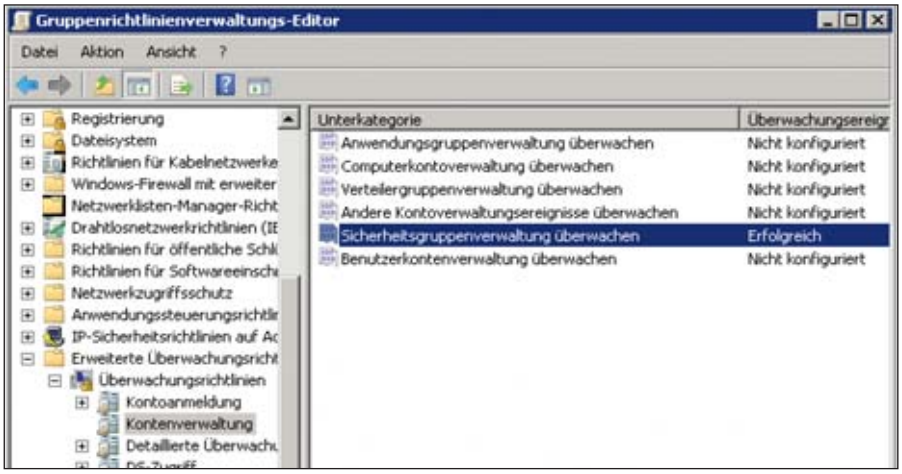


Bild 1: Über den Gruppenrichtlinienverwaltungs-Editor aktivieren Sie die Sicherheitsgruppenverwaltung, um die Ergebnisse Ihrer Änderungen zu sehen

Beispiel: Änderungen von administrativen Gruppen

Eine der elementaren Aufgaben bei der Überwachung von sicherheitskritischen Ereignissen ist es, die Veränderungen von administrativen Gruppen zu überwachen. Mithilfe der erweiterten Überwachungsrichtlinie "Sicherheitsgruppenverwaltung überwachen" können Sie genau diese Ereignisse überwachen, die durch Änderungen an Sicherheitsgruppen generiert wurden. Dazu zählen beispielsweise folgende Ereignisse:

- Erstellen, Ändern oder Löschen einer Sicherheitsgruppe
- Hinzufügen eines Mitglieds zu einer Sicherheitsgruppe
- oder Entfernen eines Mitglieds aus einer Sicherheitsgruppe
- Ändern des Gruppentyps

Um Änderungen an sicherheitsaktivierten Gruppen zu überwachen, muss dies an zwei Stellen konfiguriert werden. Zum einen ist die Aktivierung der Gruppenrichtlinie auf das betreffende Computerkonto (in unserem Fall der Domain Controller) mit der jeweiligen Überwachungsrichtlinie erforderlich und zum anderen die Aktivierung der Überwachung auf dem entsprechenden Objekt (SACL). In unserem Fall die Gruppe "gr_dhcp_adm".

Protokollierung sicherstellen

Die System Access Control List (SACL) für das jeweilige Objekt ist dann bedeutsam (zwingend notwendig), wenn es darum geht, zu bestimmen, ob eine Zugriffsüberprüfung stattfindet. Ist innerhalb der SACL eines Objektes kein Zugriffssteuerungseintrag (Access Control Entry, ACE) vorhanden, der die Protokollierung von Attributänderungen erforderlich macht, werden auch dann keine Überwachungsereignisse protokolliert, wenn die Unterkategorie "Kontenverwaltung" aktiviert ist. Ist beispielsweise in einer SACL, die den Zugriff zum Schreiben von Eigenschaften auf ein Gruppenobjekt überwacht, kein ACE vorhanden, werden bei Änderungen innerhalb der Mitgliedschaften keine Überwachungsereignisse generiert – das gilt auch bei aktivierter Unterkategorie "Kontenverwaltung".

Erstellen der Gruppenrichtlinie

Um Änderungen innerhalb der Mitgliedschaften des Active Directory zu überwachen, erstellen wir im ersten Schritt eine neue Gruppenrichtlinie. Die Nutzung der bereits standardmäßig erstellten Gruppenrichtlinien (Default Domain Policy oder Default Domain Controller Policy) empfiehlt sich in der Praxis in der Regel nicht. Über die Gruppenrichtlinienverwaltungs-Konsole erstellen wir nun ein neues Gruppenrichtlinien-Objekt. Wir bearbeiten die Richtlinie und wechseln in "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Erweiterte Überwachungsrichtlinienkonfiguration / Kontoverwaltung". Aktivieren Sie nun die Unterkategorie "Sicherheitsgruppenverwaltung überwachen" für erfolgreiche Änderungen. Danach aktualisieren Sie die Gruppenrichtlinien auf Ihrem Domain Controller mittels *gpupdate /force*. Mit dem Befehlszeilenkommando *audit-*

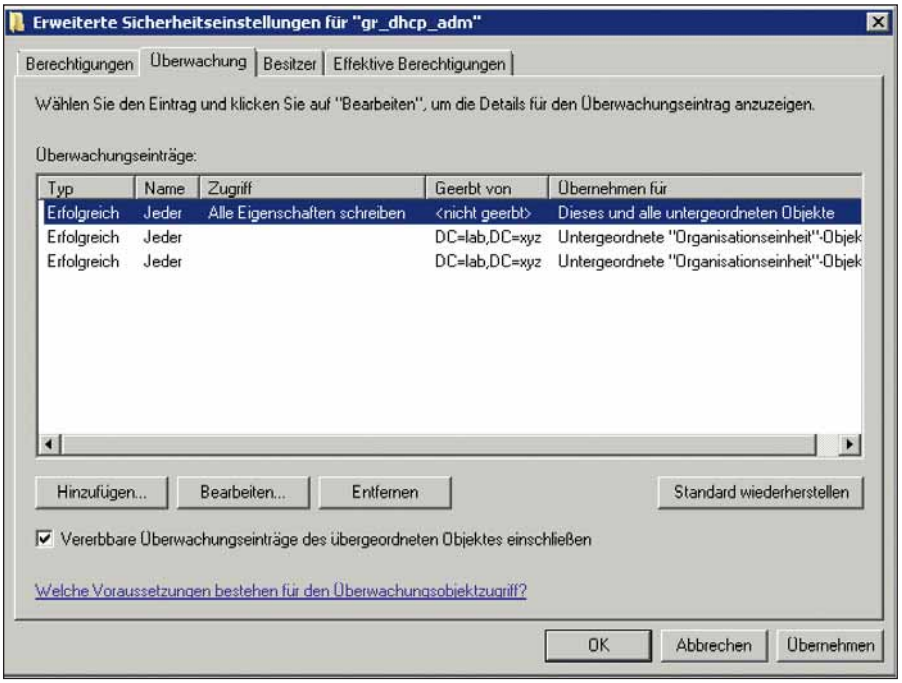


Bild 2: Taucht in den erweiterten Sicherheitseinstellungen für "gr_dchp_adm" die Meldung "Erfolgreich" auf, haben Ihre Änderungen gegriffen

*pol.exe /get /category:** prüfen Sie anschließend, ob die Unterkategorie erfolgreich angewendet wird. Hier sollten Sie in der Sicherheitsgruppenverwaltung den Eintrag "Erfolg" vorfinden. Um nun die SACL für die administrative Gruppe zu konfigurieren, wechseln Sie in die erweiterte Ansicht in der Verwaltungskonsole "Active Directory Benutzer und -Computer" und wählen Sie die Eigenschaften der Gruppe "gr_dhcp_adm". Hier navigieren Sie zum Reiter "Sicherheit" und dort in den Menüpunkt "Erweitert". Unter dem Reiter "Überwachung" fügen wir den Benutzer "Jeder" hinzu und wählen unter erfolgreichem Zugriff die Berechtigung "Alle Eigenschaften schreiben". Hiermit werden alle Änderungen am Objekt protokolliert.

Zur Überprüfung der Funktionalität fügen Sie der Gruppe einen Benutzer hinzu und kontrollieren Sie das Ereignisprotokoll. Hier sollte nun ein Eintrag mit der EventID "4737" vorhanden sein. Im gleichen Atemzug löschen Sie den Benutzer wieder aus der Gruppe. Auch in diesem Fall sollte eine EventID, diesmal die Nummer "4729", generiert werden. Im nachfolgenden Eventlog-Auszug erkennen Sie genau, welcher Benutzer wann zu welcher Gruppe durch wen hinzugefügt wurde:

```
Ein Mitglied einer sicherheitsaktivier-
  ten globalen Gruppe wurde entfernt.

Antragsteller:
  Sicherheits-ID: LAB\Administrator
  Kontoname: Administrator
  Kontodomäne: LAB
  Anmelde-ID: 0xeafb0c
Mitglied:
  Sicherheits-ID: LAB\Administrator
  Kontoname:
  CN=Administrator,CN=Users,DC=lab,
  DC=xyz
Gruppe:
  Sicherheits-ID:
  LAB\gr_dhcp_adm
  Gruppenname:   gr_dhcp_adm
  Gruppendomäne: LAB
```

Ereignisüberwachung via PowerShell

Wie bereits beschrieben, können Sie mithilfe des PowerShell-Cmdlets "Get-WinEvent" Ereignisse aus den Ereignisproto-

Wichtige Sicherheitsereignisse auf Domain Controllern

Event ID	Kategorie	Beschreibung
4771	Audit account logon events	Wird durch einen fehlerhaften Anmeldeversuch auf einem Domain Controller mit einem Domänenbenutzer über Kerberos protokolliert. Vermehrte oder unregelmäßige fehlerhafte Anmeldungen können auf einen Sicherheitsvorfall hindeuten. Genaue Hinweise liefern die innerhalb des Events aufgeführten Kerberos Codes (siehe Tabelle "Kerberos Fehlercodes").
4768	Audit account logon events	Beschreibt einen weiteren Typ einer fehlerhaften Authentifizierung über Kerberos (siehe Tabelle "Kerberos Fehlercodes").
4776	Audit account logon events	Deutet auf einem Domain Controller auf einen fehlerhaften Anmeldeversuch über NTLM mit einem Domänenbenutzer hin (siehe Tabelle "NTLM Fehlercodes").
4738	Audit account management	Protokolliert eine Änderung an einem spezifischen Benutzer-Account. Dies kann eine Reset-Password-Anfrage oder eine Aktivierung eines gesperrten Accounts sein.
4728, 4732, 4756	Audit account management	Alle drei Events beschreiben das Hinzufügen eines Benutzers zu einer spezifischen Gruppe (Lokale, Globale und Universelle).
4720	Audit account management	Ein neuer Benutzer wurde angelegt.
4740	Audit account management	Ein Benutzer wurde nach mehrmaligen, fehlerhaften Anmeldeversuchen gesperrt.
1102	Audit system events	Ein spezifischer Benutzer hat das Security Event Log gelöscht.

kollen abrufen und filtern. Dies umfasst sowohl die klassischen Protokolle wie das System-, Anwendungs- und das Sicherheitsprotokoll als auch die Ereignisprotokolle, die von der in Windows Vista eingeführten Windows-Ereignisprotokolltechnologie generiert werden. Hierdurch lassen sich beispielsweise Reports generieren. Durch eine automatisierte und tägliche Ausführung lesen Sie so sicherheitsrelevante Informationen aus und archivieren diese. Ohne zusätzliche Parameter rufen Sie mit dem Befehl "Get-WinEvent" alle Ereignisse aus allen Ereignisprotokollen auf dem Computer ab. Der folgende Befehl zeigt unter Windows Server 2008 R2 alle verfügbaren Eventlogs:

```
Get-WinEvent -listlog *
```

Mithilfe des folgenden Befehls zeigen Sie die letzten fünf Sicherheitsereignisse innerhalb des Security-Logs an:

```
Get-WinEvent Security -MaxEvents 5
```

Durch folgenden Befehl filtern Sie durch eine Kombination von mehreren Befehlen einerseits die Events des Security-Logs und andererseits die darin enthaltene ID "4771":

```
Get-WinEvent Security | where-object
  {$_.Id -eq "4771"}
```

Beachten Sie, dass "Get-WinEvent" mindestens Windows Vista und Windows Server 2008 R2 erfordert. Zudem wird das Microsoft .NET Framework 3.5 oder eine höhere Version benötigt.

Eigene PowerShell-Berichte

Mithilfe der PowerShell lassen sich so schnell auf die eigenen Bedürfnisse angepasste Sicherheitsberichte erstellen. Der nachfolgende Auszug aus einem PowerShell-Skript soll dies verdeutlichen:

```
# -- Members removed from Global
  Groups --
$MyReport += Get-CustomHeader "1"
  "Members removed from Global
  Groups on domaincontroller
  $domaincontroller"
$MyReport += Get-HTMLTable ($event-
  log | Where-Object {$_.EventID -eq
  "633" -or $_.EventID -eq "4729"} |
  select TimeGenerated,Message  )
$MyReport += Get-CustomHeaderClose
```

So erstellen Sie mithilfe der PowerShell eigene HTML-Berichte, die Sie dann auch per Taskplaner an die verantwortlichen Administratoren schicken können. Innerhalb der Gruppe "gr_dhcp_adm" sehen Sie den hinzugefügten und anschließend gelöschten Benutzer.

Hilfreiche Event IDs

Um Sicherheitsvorfälle mithilfe der Ereignisprotokolle zu erkennen, ist es äußerst wichtig zu wissen, welche Event IDs Rückschlüsse auf einen Sicherheitsvorfall zulassen. In der Tabelle "Wichtige Sicherheitsereignisse auf Domain Controllern" finden Sie eine Aufstellung von sicherheitsrelevanten Events, die protokolliert und ausgewertet werden sollten.

Diese Aufstellung kann Ihnen als Grundlage für ein Security-Monitoring dienen. Je nachdem, welche Ereignisse Sie protokollieren und auswerten wollen, ist diese entsprechend zu ergänzen. Durch die in der Tabelle "NTLM-Fehlercodes" aufgeführten Codes haben Sie die Möglichkeit, die genaue Ursache für den fehlerhaften Anmeldeversuch über NTLM zu definieren.

NTLM-Fehlercodes

Fehlercode (Dezimal)	Fehlercode (Hex)	Beschreibung
3221225572	C0000064	Benutzername existiert nicht
3221225578	C000006A	Unbekannter Benutzername oder ungültiges Kennwort
3221226036	C0000234	Benutzeraccount ist gesperrt
3221225586	C0000072	Benutzeraccount ist deaktiviert
3221225583	C000006F	Anmeldezeit-Beschränkung
3221225584	C0000070	Computer-Beschränkung
3221225875	C0000193	Benutzeraccount ist abgelaufen
3221225585	C0000071	Das Passwort ist abgelaufen
3221226020	C0000224	Der Benutzer muss sein Passwort bei der nächsten Anmeldung ändern

Kerberos-Fehlercodes

Fehler Code	Begründung
6	Der Benutzername existiert nicht
12	Computer-Beschränkung; Anmeldezeit-Beschränkung
18	Benutzer deaktiviert, abgelaufen oder gesperrt
23	Das Benutzerpassword ist abgelaufen
24	Authentifizierung fehlgeschlagen; falsches Password
32	Ticket abgelaufen
37	Die Zeit zwischen Workstation und Domain Controller ist zu weit auseinander

Durch die Kerberos-Fehlercodes wird die genaue Ursache für die fehlgeschlagene Authentifizierung über Kerberos sichtbar. Weitere Kerberos Codes finden Sie unter [1].

Fazit

Mithilfe der erweiterten Überwachungsrichtlinien erhält der Administrator nun ein umfangreiches Richtlinienwerk. Kombiniert mit einem funktionierenden Mechanismus zum Alerting lassen sich nahezu alle Ereignisse überwachen und so einem vermeintlichen Angriff durch Außen- und Innentäter geeignete Gegenmaßnahmen entgegensetzen. *(dr)*

[1] Kerberos-Fehlercodes
C1P61

Link-Codes

Microsoft Small Business Server 2011 Essentials einrichten und verwalten

Klein, aber fein

von Christian Knermann

Mit dem Windows Small Business Server 2011 Essentials hat Microsoft ein Angebot für Unternehmen mit bis zu 25 Mitarbeitern geschnürt. Dieser neueste Spross der Windows-Familie schließt die Lücke zwischen Windows Home Server 2011 und dem Small Business Server 2011 Standard. An Funktionen muss der IT-Verantwortliche dabei gerade für kleinere Umgebungen keine Abstriche machen. IT-Administrator stellt die Möglichkeiten und Grenzen des Server-Betriebssystems vor.

Um den SBS 2011 Essentials in den Windows-Stammbaum einzuordnen, beginnen wir bei seinem Vorfahren: Bereits der Windows Server 2003 hatte einen kleinen Bruder namens Windows Home Server oder kurz WHS, der sich hauptsächlich als Medienzentrale und NAS-Lösung für Heimanwender empfahl. Aufgrund des sehr einfach zu bedienenden und vollständigen Client-Backups hatte dieses System auch für Einzelunternehmer und sehr kleine Büros mit wenigen Windows-Clients durchaus seine Reize [1]. Gleiches gilt für den Nachfolger WHS 2011, der auf dem Windows Server 2008 R2 basiert und entsprechend ausschließlich als 64 Bit-Version vorliegt.

Die Vorteile des Vorgängers sind auch dem WHS 2011 zu eigen, namentlich die einfache Einrichtung und das ebenso einfache Backup der Clients. Allerdings bleiben auch die Nachteile des WHS v1 erhalten. Das System unterstützt maximal zehn Nutzer und bietet keine zentrale Benutzerverwaltung. Server und Clients finden nur im Verbund einer Arbeitsgruppe zueinander. Dies bedeutet in der Praxis, dass auf dem Server und allen Clients pro Benutzer identische Anmeldeinformationen zu pflegen sind. Dass dies für Administratoren im Unternehmensumfeld keine Option ist, hat offensichtlich auch Microsoft erkannt und als engen Verwandten des WHS 2011 den Small Business Server 2011 Essentials entwickelt. Dieser erbt die Vorteile des WHS 2011 und bringt zusätzlich ein Active Directory für bis zu 25 Benutzer mit. Dessen Komplexität bleibt zunächst weitestgehend verborgen.

Installation ohne viele Rückfragen

SBS 2011 Essentials stellt während der Erstinstallation und der späteren Konfiguration wesentlich weniger Fragen als Windows Server 2008 R2. Zu Beginn überprüft das System die Hardware-Anforderungen. Die Installation lässt sich nur fortsetzen, wenn die Setup-Routine mindestens einen mit 1,3 GHz getakteten 64 Bit-Prozessor, eine 160 GByte große Festplatte sowie 2 GByte RAM vorfindet. Insbesondere im Hinblick auf CPU und Hauptspeicher geben sich die Essentials damit deutlich genügsamer als die nächst größere Windows-Variante, der SBS 2011 Standard. Warum die Standard-Edition 40 GByte Festplattenplatz weniger fordert als die Essentials, bleibt das Geheimnis von Microsoft. Erfüllt die Hardware die Voraussetzungen, können Sie im nächsten Schritt die Festplatte zur Installation auswählen. Daraufhin legt das Setup erst einmal selbsttätig los, installiert das Betriebssystem und richtet die Hardware ein. Je nach Leistungsfähigkeit des Zielsystems können Sie sich für 30 bis 60 Minuten anderen Dingen zuwenden. Anschließend geht es weiter mit der Auswahl der Regions- und Sprachoptionen und der Eingabe des Lizenzschlüssels.

Erst der nächste Dialogschritt verdeutlicht einen Unterschied zwischen WHS und SBS: Fragt der Home Server an dieser Stelle nur nach dem Servernamen, möchte der SBS zusätzlich den Firmennamen und den Namen der internen Domäne wissen. Dies wird begleitet von dem dringenden Hinweis, dass sich die Informationen nachträglich nicht mehr ändern lassen – sie werden

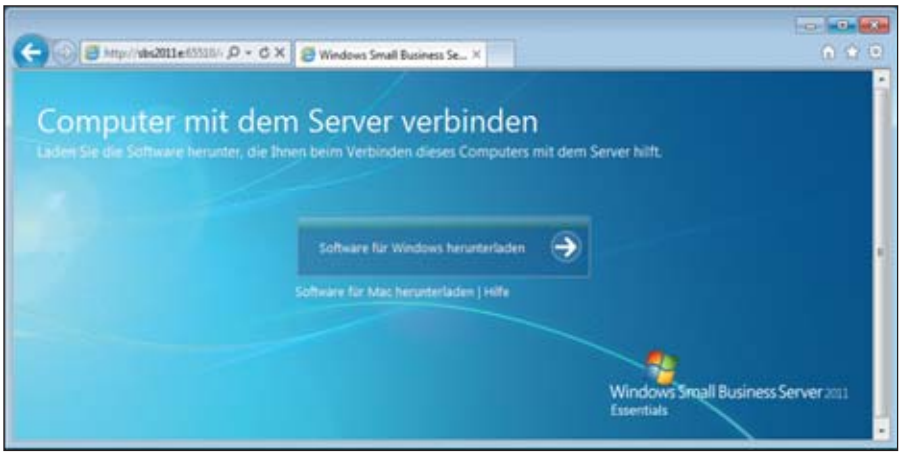


Bild 1: Den Client-Connector bietet der Server zum Download an

zur Einrichtung der Active Directory-Dienste und des AD-integrierten DNS verwendet. Als Domäne geben wir in unserem Beispiel "SMALLBUSINESS" und als Servernamen "SBS2011E" ein. Aus dem NetBIOS-Namen leitet das Setup automatisch den vollqualifizierten internen Domänennamen "smallbusiness.local" ab. Im weiteren Verlauf haben Sie die Gelegenheit, Namen und Passwörter für das Administratorkonto und einen ersten Benutzer festzulegen. Anschließend können Sie einstellen, ob und wie der Server auf dem neuesten Stand gehalten werden soll. Da "Empfohlene Einstellungen" auch beinhaltet, Informationen zur Nutzung und zu Fehlern an Microsoft zu übertragen, entscheiden wir uns für "Nur Updates installieren". Damit ist die Konfiguration bereits abgeschlossen und der Server nimmt seinen Betrieb auf. Dabei versorgt er sich vom DHCP-Server – sofern vorhanden – automatisch mit einer IP-Adresse. Hier empfiehlt es sich, diese Adresse statisch zuzuordnen.

Ohne weiter Hand an den Server zu legen, können Sie nun direkt Client-Computer einrichten. Beginnen Sie beispielsweise mit einem Client unter Windows 7 Enterprise, auf dem Sie im Browser den Link *http://sbs2011e/connect* aufrufen. Vom Server laden Sie nun den "Windows Small Business Server 2011 Connector" herunter und installieren diesen (siehe Bild 1). Das Setup prüft, ob das .NET-Framework 4.0 vorhanden ist und installiert es bei Bedarf. Anschließend geben Sie Namen und Kennwort eines Benutzers auf dem Server ein. Bemerkenswert ist an dieser Stelle, dass es sich dabei nicht um einen Server-Administrator handeln muss, ein normaler Benutzer reicht. Daraufhin bietet der Installer an, den lokalen Benutzer, unter dem Sie die Installation ausführen, mit all seinen Daten und Einstellungen in einen Netzwerk-Benutzer zu konvertieren. Wir nehmen für unseren Workshop dieses Angebot an, was einen Neustart notwendig macht. Der Connector kümmert sich nun vollautomatisch darum, dass der Client-Computer Mitglied der Domäne SMALLBUSINESS wird. Nach dem Reboot können Sie sich als Domänen-Benutzer an dem Client anmelden. Auf dem Desktop begrüßt Sie das "Launchpad", mit dem der Benutzer manuell eine Sicherung des Clients starten, den Remotewebzugriff sowie die für ihn freigegebenen Ordner und das "Dashboard" aufrufen kann (siehe Bild 2). Letzteres verlangt nach einem Administratorkonto und erlaubt die weitere Konfiguration des Servers.

Bild 2: Launchpad und Dashboard ermöglichen Zugriff und Administration des Servers

Dashboard aus der Ferne

Beim Dashboard handelt es sich nicht um eine Client-seitige Anwendung, sondern um eine Remote App. Das Dashboard startet auf dem Server und wird per RDP zum Client übertragen. Auf der Seite "Start" finden sich sämtliche weiteren Schritte zur Basiskonfiguration des Servers. Unter "Benutzer" können Sie die Kennwortrichtlinie steuern, vorhandene Konten verwalten und weitere Benutzer anlegen (siehe Bild 3). Der entsprechende Dialog erwartet lediglich Vornamen, Nachnamen, Kontonamen und das Passwort. Die Zugriffsebenen beschränken sich auf die Optionen "Standardbenutzer" oder "Administrator". Im nächsten Schritt setzen Sie die Zugriffsrechte des neuen Benutzers auf bereits vorhandene Freigaben. Zur Auswahl stehen hier lediglich "Lesen / Schreiben", "Schreibgeschützt" oder "Kein Zugriff".

Im Bereich "Computer und Sicherung" nehmen Sie globale Einstellungen für das Backup vor. Dies betrifft das Zeitfenster für Sicherungen sowie die Anzahl an täglich, wöchentlich und monatlich aufbewahrten Sicherungen. Standardmäßig werden die Clients komplett gesichert. Über die Aufgabe "Sicherung für den Computer anpassen" nehmen Sie pro Client abweichende Einstellungen vor und wählen einzelne Ordner aus. Innerhalb des Zeitfensters werden sämtliche Windows-Clients gesichert. Bei Bedarf starten abgeschaltete Clients zu diesem Zweck automatisch, sofern Sie die entsprechende Option bei der Installation des Connectors aktiviert haben. Der Server überwacht den Zustand der Clients und gibt Warnungen aus, falls diese nicht gesichert wurden oder ein aktueller Virenschutz fehlt. Das gilt gleichermaßen für den Server selbst, der ebenfalls gesichert werden sollte. Um die Sicherung zu konfigurieren, müssen Sie per USB, Firewire oder eSATA eine entsprechend große externe Platte verbinden.

Unter "Serverordner und Festplatten" verwalten Sie den Speicherplatz. Auf der Registerkarte "Serverordner" erzeugen Sie neue Freigaben und legen bei Bedarf pro Benutzer individuell die Zugriffsrechte fest. Sollte der Platz knapp werden, können Sie einzelne Ordner auf eine andere Festplatte verschieben. Ein beliebtes Feature des WHS v1, der "Drive Extender" mit der Ordnerduplizierung, fehlt leider. Mit dieser Funktion ermöglichte Microsoft im früheren WHS, vorhandene Partitionen im laufenden Betrieb auf neue Festplatten zu erweitern und pro Freigabe festzulegen, ob Schreibzugriffe im Hintergrund auf zwei Festplatten repliziert werden sollen. Der Vorteil gegenüber einem RAID bestand darin, dass nur die Daten doppelt abgelegt wurden, für die dies explizit gewünscht war. Im WHS und SBS 2011 ist diese Funktion leider nicht erhalten geblieben. Das Add-in "Drive Bender" [2] möchte diese Lücke schließen. Alternativ bleibt zur Erhöhung der Datensicherheit nur, die konventionellen

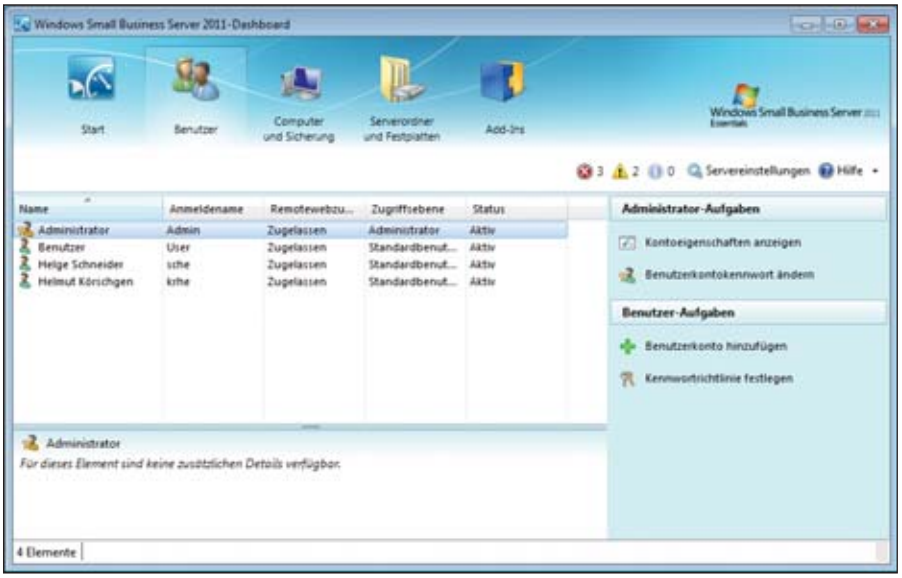


Bild 3: Benutzer und Clients werden im Dashboard verwaltet

Methoden zu nutzen, entweder die Software-RAID-Funktionen des Betriebssystems oder ein Hardware-RAID.

Nachdem wir uns mit dem Dashboard vertraut gemacht haben, fügen wir dem Server weitere Clients hinzu. Als zweites Beispiel dient uns Windows 7 Home. Dass die Home Edition nicht Mitglied einer Domäne werden kann, vermag auch der SBS 2011 Connector nicht zu ändern und so läuft das Setup des Connectors analog zu dem des Home Servers ab. Während der Installation sind hierbei die Anmeldeinformationen eines Server-Administrators erforderlich. Der Client bleibt in seiner Arbeitsgruppe und der lokale Account bleibt lokal. Wie beim WHS auch müssen Sie in diesem Fall manuell dafür sorgen, dass auf dem Server ein gleichnamiger Account mit identischem Passwort vorhanden ist. Dann lässt der SBS den jeweiligen Benutzer auch ohne erneute Authentisierung auf das Launchpad und die freigegebenen Ordner zugreifen. Andernfalls wird eine zusätzliche Anmeldung nötig. Um von der Vorteilen der AD-Domäne voll zu profitieren, empfehlen sich entsprechend die professionellen Windows-Editionen als Client.

Lückenhafte Integration von Mac-Rechnern

Microsoft gibt an, dass WHS und SBS 2011 Essentials Mac OS ab Version 10.5 unterstützen. Dies haben wir mit einer Installation von Mac OS 10.6.8 getestet. Auch für den Mac steht unter *http://{servername}/connect* ein Connector zum Download bereit. Dessen Fähigkeiten bleiben allerdings hinter dem Windows-Pendant zurück. So ist das Setup nicht in der Lage, den Mac so zu konfigurieren, dass er gegen das Active Directory authentisiert. Am Launchpad wird ein zweiter Logon fällig.

Wer von der zentralen Benutzerverwaltung profitieren möchte, muss entsprechend manuell tätig werden. Dass auch Mac OS grundsätzlich mit einem AD spricht, haben wir bereits gezeigt [5]. Die Option findet sich ab Mac OS 10.6 allerdings nicht mehr bei den Dienstprogrammen, sondern unter */System / Library / CoreServices / Verzeichnisdienste.app*. Der Mac Connector beinhaltet weiterhin keinen Link zum Dashboard. Falls Sie dieses nutzen möchten, müssen Sie einen RDP-Client installieren und direkt auf den Desktop des Servers zugreifen. Auch bei der Datensicherung ist der Connector keine große Hilfe. Der Link "Backup" ruft lediglich die Konfiguration von Apples eigenem Tool "Time Machine" auf. Die Volume-Auswahl von Time Machine bleibt jedoch leer, da Freigaben des Windows-Servers nicht als geeigneter Ort für Time Machine-Backups erkannt werden. Abhilfe schafft hier ein beherzter Griff ins Getriebe [6]. Das Add-in "Orbital Backup Configuration" [7] verspricht, die nötige Konfiguration automatisch zu erledigen. Version 1.0.0.1 ließ sich allerdings auf unserem deutschen SBS 2011 Essentials nicht erfolgreich in Betrieb nehmen. Die entsprechende Option erschien nicht im Lauchpad auf dem Mac. Damit bietet der Connector derzeit für Mac-Clients einen eher geringen Nutzen, zumal das jüngste Mac OS 10.7 noch nicht unterstützt wird. So bleibt nur zu hoffen, dass Microsoft hier nachbessert.

Restore mit Windows-Clients

Für Windows-Clients funktioniert die Datensicherung dagegen tadellos. Um einzelne Objekte wiederherzustellen, starten wir das Dashboard auf einem Client und wählen im Bereich "Computer und Sicherung" den Client aus. Im folgenden Dialog wählen wir die gewünschte Sicherung, die daraufhin geöffnet wird, so dass wir einzelne Ordner und Dateien extrahieren können. Soll ein Client komplett wiederhergestellt werden, bringt der SBS dazu eine passende Boot-CD mit, von der ein minimales Windows-System startet, das per USB gegebenenfalls noch mit passenden Treibern für Netzwerk oder Massenspeicher bestückt werden muss. Anschließend wählen Sie den Client und die gewünschte Sicherung aus. Dann stellen Sie den kompletten Client oder einzelne Partitionen wieder her.

Blick unter die Haube

Alle bislang vorgestellten Schritte erfolgen über das Dashboard. Neulinge etwa können somit grundlegende Aufgaben bewältigen, ohne überhaupt wissen zu müssen, dass unter der Haube ein vollwertiges Active Directory seinen Dienst tut. Dessen Möglichkeiten stehen Ihnen aber dennoch offen. Melden Sie sich als Administrator per RDP oder lokal am Desktop des Ser-

Add-ins

Add-ins wie das zuvor genannte "Drive Bender" tragen die Dateiendung .wssx. Führen Sie eine solche Datei auf einem Windows-Client aus, wird die Erweiterung auf dem mit dem Client verbundenen Server installiert. Ein beliebtes Add-in ist beispielsweise "Lights-Out For Windows Home Server 2011" [3]. Add-ins für den WHS funktionieren in der Regel auch auf dem SBS und so finden Sie nach der Installation dieses Add-ins auch auf Ihrem SBS ein zusätzliches Icon im Dashboard vor, das es ermöglicht, den Server nach einem definierbaren Zeitplan herauf- und herunterzufahren (siehe Bild 4). Ein gut sortiertes Verzeichnis von weiteren Add-ins für die verschiedensten Zwecke findet sich unter [4].

Bild 4: "Lights-Out" fährt den Server zeitgesteuert herauf und herunter

vers an, finden Sie neben dem Dashboard die gewohnten Administrationswerkzeuge. Alternativ installieren Sie auf einem Client-Computer die Remoteserver-Verwaltungstools für Windows 7 [8]. Damit stehen Ihnen dann beispielsweise die Konsolen "Active Directory- Benutzer und -Computer" sowie die "Gruppenrichtlinienverwaltung" zur Verfügung.

Sie haben nun die Möglichkeit, Organisationseinheiten für Ihre Benutzer und Client-PCs zu erstellen, Objekte dorthin zu verschieben und schließlich mittels Gruppenrichtlinienobjekten beliebige Einstellungen zu definieren. Über den Server-Manager lassen sich zudem weitere Rollen und Features hinzufügen – alles wie auf einem "großen" Windows Server 2008 R2.

Notwendige Hardware

Wie auch der WHS v1 ist der WHS 2011 als OEM-Produkt positioniert. Eher dünn gesät zeigt sich bislang das Angebot an vorgefertigten Lösungen für den WHS 2011. So hat Acer die Produkte RevoCenter RC100 mit Intel Atom D410 und RC101 mit Intel Atom D510 angekündigt. Der britische Hersteller Tranquil PC hat mit dem "Leo HS4" und dem "Home Server SQA-5H" bereits zwei Geräte im Angebot. All diesen Modellen ist aber gemeinsam, dass sie nur mit dem WHS 2011 ausgeliefert werden. Zudem hat Microsoft für entsprechende OEM-Hardware zur Auflage gemacht, dass diese im Bundle mit dem WHS nur ohne Grafikanschluss vertrieben werden darf. Wer also auf einer solchen Hardware den Small Business Server installieren möchte, muss über den in der Regel vorhandenen Diagnose-Port eine Grafikkarte nachrüsten oder unbeaufsichtigt installieren [9]. Alternativ sind bereits auf den Bedarf von KMUs ausgerichtete Systeme mit dem SBS 2011 Essentials am Markt verfügbar, beispielsweise der HP ProLiant MicroServer oder zwei Modelle aus Lenovos ThinkServer-Reihe.

Sind vorkonfektionierte Systeme nicht das Richtige, bleibt natürlich noch die Option, auf beliebiger anderweitiger Hardware zu installieren. Eine Systembuilder-Version von WHS 2011 ist bereits für unter 40 Euro im Handel zu finden, die Preise für den SBS 2011 Essentials beginnen bei 300 Euro. Erwähnenswert ist hierbei noch, dass im Basispreis die Lizenzen für den Zugriff auf den Server, die Client Access Licenses (CAL), für die jeweils maximale Anzahl an Benutzern bereits inbegriffen sind. Der SBS 2011 Standard beinhaltet nur fünf CALs, weitere CALs im Fünfer-Pack kosten extra. Der Preisunterschied und die höheren Hardware-Anforderungen ergeben sich daraus, dass die Standard-Edition des SBS einige zusätzliche Dienste beinhaltet, insbesondere Exchange Server 2010 sowie SharePoint Foundation 2010. Anstelle lokal installierter Groupware-Funktionen setzt Microsoft bei den Essentials dagegen voll auf die Cloud und das hauseigene Angebot "Office 365".

Die Integration mit den entsprechenden Online-Diensten ist allerdings noch nicht abgeschlossen. Das Dashboard des Servers verweist lediglich darauf, dass ein passendes Add-in bald verfügbar sein wird und führt weiter auf einen TechNet Blog-Beitrag [10]. Dieser stellt das kommende "Office 365 Integration Module" vor, das lokale Benutzeraccounts auf dem Server mit Office 365-Benutzern verknüpfen soll. Da das Modul bis Redaktionsschluss noch nicht verfügbar war, konnten wir uns von der Funktionalität nicht überzeugen. Auch ohne die Integration ist die Nutzung zwar bereits jetzt möglich, dann sind aber pro Benutzer manuell zwei Konten zu pflegen, das lokale und der Office 365-Benutzer. Letzterer schlägt mit 5,25 Euro pro Benutzer pro Monat zu Buche.

Fazit

Auch ohne die Integration mit Office 365 stellen WHS 2011 und SBS 2011 Essentials bereits jetzt interessante Lösungen für kleine Unternehmen dar und bieten den derzeit günstigsten Einstieg in die Windows-Welt. Insbesondere das vollständige Backup der Client-Computer ragt dabei heraus und ist in dieser Form bei den größeren Windows Servern nicht zu finden. Die zentrale Benutzerverwaltung spricht für den SBS 2011, solange maximal 25 Benutzer zu betreuen sind. Wer dagegen absehen kann, dass sein Unternehmen in naher Zukunft darüber hinaus wächst, sollte sich eher mit dem SBS 2011 Standard beschäftigen. *(dr)*

[1] "Zu Hause ist es doch am schönsten – Im Test: Fujitsu Scaleo Home Server 2205" in IT-Administrator 12/2009
[2] Add-In "Drive Bender" C1P92
[3] Lights-Out For Windows Home Server 2011 C1P93
[4] Weitere Add-ins für WHS 2011 C1P94
[5] "Der Apfel im Windows-Netz - Mac OS X 10.5 in Windows-Netzen einsetzen" in IT-Administrator 8/2008
[6] Backups mit Time Machine ermöglichen C1P96
[7] Add-in "Orbital Backup Configuration" C1P97
[8] Remoteserver-Verwaltungstools für Windows 7 C1P98
[9] TechNet-Eintrag zur Installation mit Antwortdatei C1P99
[10] TechNet-Eintrag zum Office 365 Integration Module C1P90

Link-Codes


Quelle: 123RF

Office 365 im Unternehmen einsetzen

Flugbegleiter durch die Cloud

von Ulf B. Simon-Weidner

Seit Mitte 2010 bietet Microsoft eine Online-Variante seiner Office- und Collaboration-Lösungen. In diesem Artikel beleuchten wir, was genau hinter diesem Angebot steckt und wo dessen Vor- und Nachteile liegen. Außerdem gehen wird darauf ein, wie eine mögliche Strategie beim Gang in die Wolke aussehen kann. So müssen sich Unternehmen etwa entscheiden, ob sie die komplette Kommunikations- und Office-Umgebung auslagern oder ob sie weiterhin eigene Server betreiben.

Cloud-Computing ist in aller Munde und hat nicht nur Administratoren im Unternehmen erreicht – auch Verbraucher können sich vor entsprechenden Angeboten mittlerweile kaum retten. Ob Smartphone-Hersteller, Internet-Provider, Webspace-Hoster oder Notebook-Hersteller, alle haben die unterschiedlichsten Web-Dienste im Angebot. Microsoft hat es relativ frühzeitig in die Cloud getrieben. Die bisherige Microsoft Business Productivity Online Suite (BPOS) wurde derweil von Office 365 abgelöst und ermöglicht Unternehmen und Selbstständigen, Kommunikations- und Collaboration-Lösungen online zu nutzen. Exchange für E-Mail, Kontakte und Kalenderfunktionalitäten, SharePoint für eine Webplattform, Lync für Instant Messaging sowie Online-Konferenzen und -Meetings – all diese Angebote werden im Abonnement bezogen und mit einem Fixpreis pro Benutzer und Monat bezahlt.

Angebote für alle Unternehmensgrößen

Office 365 gibt es für zwei Anwendergruppen: Der Plan P1 [1] richtet sich an Selbstständige und kleinere Unternehmen. Er enthält E-Mail, Kontakte und Kalender mit 25 GByte großen Postfächern und eine Archivierungsfunktion. Desweiteren kann mit den Office-Webapplikationen Word, Excel, Powerpoint und OneNote aus dem Webbrowser heraus gearbeitet werden. Sollte der Nutzer eine reguläre Office-Lizenz besitzen, lassen sich die Desktop-Anwendungen auch in das Cloud-Angebot integrieren. Zusätzlich steht SharePoint für Webseiten und zur Dokumentenverwaltung zur Verfügung. Lync, der Nachfolger des Office Communication Servers (OCS), bietet in einer Online-Version Instant Messaging, Online-Chats und -Meetings sowie Audio- und Videogespräche. Zudem ist es möglich, den Desktop oder Präsentationen freizugeben. Zusätzlich ist mit Microsoft Forefront eine Anti-Spam- und Antivirenlösung integriert. Der Plan P1 unterstützt bis zu 25 Anwender, bietet Online-Support und kostet monatlich 5,25 Euro pro Nutzer.

Die Pläne E1 bis E4 [2] orientieren sich an den Anforderungen mittelständischer und großer Unternehmen. Hier sind 9 bis 25,50 Euro pro Benutzer und Monat fällig. Zusätzlich zu den bereits erwähnten Optionen bieten sie erweiterte, unterneh-

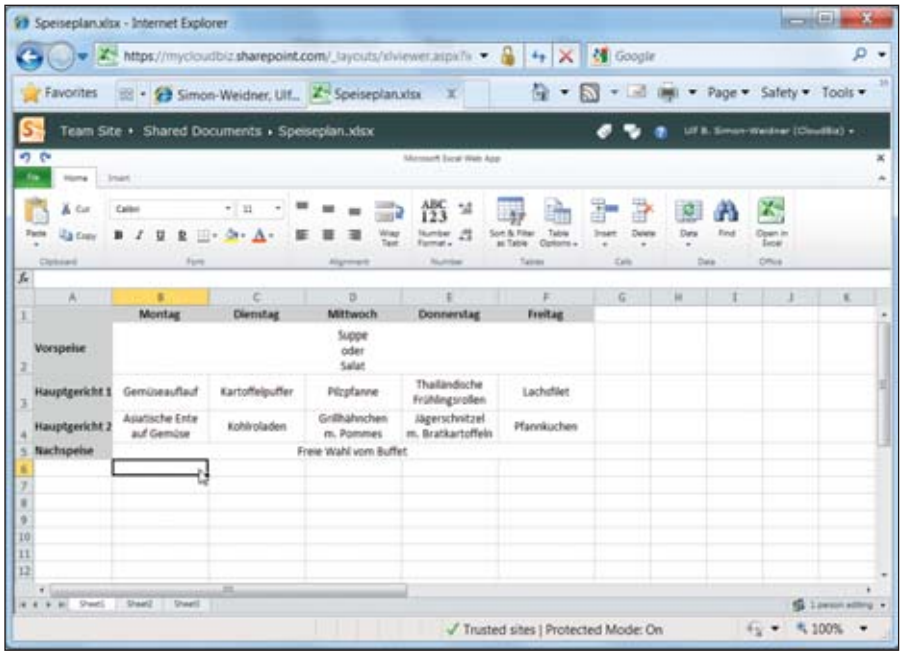


Bild 1: Excel im Webbrowser – fast so umfangreich wie die Desktop-Anwendung

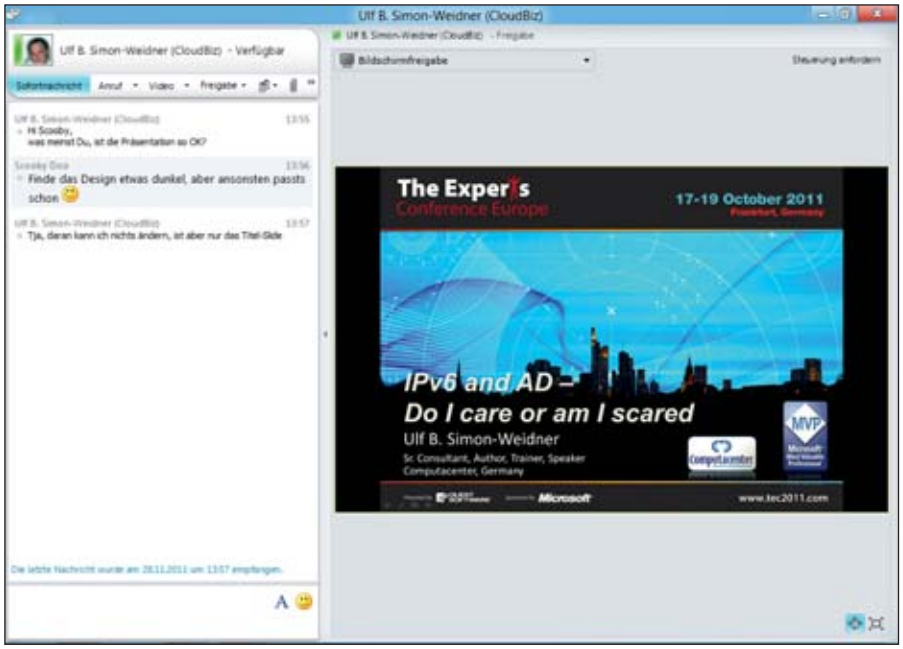


Bild 2: Mit Lync gestaltet sich das gemeinsame Arbeiten einfacher, ob per Chat, Dokumentfreigabe oder Audio/Video-Telefonie

mensorientierte Administrationsmöglichkeiten, eine Active Directory-Integration und 24x7-Unterstützung. Zusätzlich verfügt das Unternehmen über lizenzierte Rechte, um im Unternehmensnetzwerk lokal auf Exchange, SharePoint und Lync zuzugreifen, so dass eine Hybrid-Lösung möglich ist. Während E1 im Gegensatz zu P1 keine Webversionen der Office-Anwendungen bietet, sind diese ab E2 für 14,25 Euro voll vorhanden. Bei E3 ist für 22,75 Euro dann sogar eine Lizenz für die Office-Applikationen auf dem Desktop des Anwenders mit dabei. Zusätzlich lassen sich ab dieser Version auch kompliziertere Formulare in SharePoint abbilden, Daten über Visio-Services darstellen und einfache Access-Datenbanken per SharePoint im Web veröffentlichen.

Lync und Exchange bieten zudem erweiterte Archivierungsmöglichkeiten und die Integration von Voice-Mailboxen. Hier ist zu erwähnen, dass in Deutschland aufgrund gesetzlicher Bestimmungen derzeit nicht der gleiche Funktionsumfang bei Lync zur Verfügung steht wie in anderen Ländern. Dies betrifft zum Beispiel die Möglichkeit, Online-Meetings abzuhalten (in Deutschland auf 1:1-Meetings begrenzt) sowie die in E4 enthaltene Option, mit Lync eine komplette Unternehmenstelefonanlage zu ergänzen oder sogar vollständig zu ersetzen. Diese Einschränkungen in Deutschland gelten pro Anwender, das heißt in internationalen Unternehmen kommen die Limits nur für deutsche Anwender zum Tragen, während die meisten europäischen Nachbarn diesen Beschränkungen nicht unterliegen [3].

Alle Daten sind in der Cloud gesichert und redundant abgelegt und lassen sich im Notfall laut Microsoft wiederherstellen, ohne dass sich der Kunde groß darum Gedanken machen oder zusätzliche Softwarelizenzen für die Datensicherung erwerben muss. Microsoft garantiert eine Verfügbarkeit von 99,9 Prozent. Sollte dieser Wert nicht eingehalten werden, ist fest definiert, bei welchen Verfügbarkeiten welcher Betrag zurückerstattet wird.

Arbeiten in der Cloud

Exchange findet sich in den meisten Unternehmen als Lösung zur Integration von E-Mail, Kontakten, Kalendern und vor allem zur Zusammenarbeit. Auch SharePoint ist mittlerweile vielen Administratoren und Unternehmen geläufig. Während es sich mit diesen Mitteln als einzelner Anwender schon sehr bequem arbeiten lässt, trumpft Office 365 primär mit der Zusammenarbeit von vielen Anwendern auf. Mit Hilfe von Lync kann der Anwender nicht nur schnell mit dem Kollegen chatten, es unterstützt ferner den Windows Live Messenger. Dies äußert sich dann so, dass bei E-Mails angezeigt wird, ob der Adressat gerade online verfügbar, offline oder in einem Meeting ist. Direkt aus der Mail heraus lässt sich dann eine Konversation per Instant Messaging, ein Telefonat oder eine Videokonferenz starten.

Das Gleiche gilt für SharePoint. Lädt ein Anwender ein Dokument hoch oder wird er in einer Liste erwähnt, ist direkt neben dem Namen immer dessen Statussymbol zu sehen – auch hier lassen sich direkt Gespräche initiieren. Die Integration hört hier noch nicht auf: An Office-Dokumenten ist das gemeinsame Arbeiten möglich. Wenn zum Beispiel ein SharePoint-Dokument in Word geöffnet wird und ein anderer Anwender möchte das gleiche Dokument bearbeiten, sehen beide Anwender in der Statusleiste, wie viele Anwender gerade mit der Datei beschäftigt sind. Per Mausklick kann sich der Anwender dann die Namen anzeigen lassen und eine direkte Konversation starten. Zusätzlich sperrt Word im Dokument einzelne Absätze mit dem Vermerk, dass ein anderer Nutzer gerade an diesem arbeitet und führt die Dokumentänderungen aller Anwender automatisch zusammen. Diese Funktionalität erstreckt sich auch auf Excel, Powerpoint und OneNote.

Neben der hohen Integration der Anwendungen steht die Office 365-Umgebung natürlich jederzeit an jedem Ort zur Verfügung. Während der Administrator bei den lokalen Versionen von Exchange und SharePoint erst darüber nachdenken muss, wie er zum Beispiel Outlook Web Access (OWA), den Vollzugriff auf Outlook per RPC über HTTPS, oder ActiveSync für Mobilgeräte sicher veröffentlicht oder wie bei SharePoint der Zugriff vom Internet auf das Intranet eingerichtet wird, kümmert sich im Fall von Office 365 Microsoft um all diese Szenarien und eine möglichst sichere Veröffentlichung. Damit ist der Zugriff von jedem System aus über die Administrationsoberfläche nur wenige Mausklicks nach dem Einrichten von Office 365 möglich.

Cloud-Strategien erfolgreich integrieren

Betrachten wir zunächst die Sicherheit in der Cloud: Hier muss sich ein Unternehmen überlegen, vor welchen Angriffen es sich schützen möchte beziehungs-

weise muss. Zunächst einmal ist davon auszugehen, dass Microsoft um ein höchstmögliches Maß an Sicherheit bemüht ist, da Cloud-Kunden abgeschreckt werden oder verloren gehen könnten, wenn es hier zu Angriffen kommt. Auch die Autonomität von Daten gegenüber anderen Office 365-Kunden sollte gewährleistet sein. Allerdings ist hier zu berücksichtigen, dass Microsoft als US-Unternehmen dem Patriot Act untersteht und im Zweifelsfall bei Terror-Verdacht den amerikanischen Behörden Zugriff auf sämtliche Daten gewährleisten muss. Dieser Fall dürfte eher unwahrscheinlich sein, trotzdem sollten Unternehmen für Anwendungsfälle höchster Vertraulichkeit zusätzliche Maßnahmen oder eine eigene Infrastruktur verwenden.

Natürlich gibt es die Möglichkeit, E-Mails zu verschlüsseln – dann haben nur Sender und Empfänger Zugriff auf die Daten. Und mittlerweile lässt sich sogar der Rights Management Server in Office 365 integrieren, so dass sich eine Möglichkeit bietet, sowohl Office-Dokumente als auch E-Mails mit einem zusätzlichen Schutz über SharePoint oder Exchange in der Cloud abzulegen. Die Diskussionen über Sicherheit in der Cloud sind beliebig komplex, hängen von den jeweiligen Anforderungen des Unternehmens ab und davon, wovor die Daten geschützt werden müssen und inwieweit das Sicherheitsbedürfnis noch pragmatisch zu verwalten ist. Dies ist jedoch ein Thema, das sowohl On- wie auch Off-Premise gilt.

Reibungslose Komplett-Migration in die Wolke

Es gibt unterschiedliche Migrationswege (Deployment-Modelle) in die Cloud. Betrachten wir zunächst die Möglichkeiten für Unternehmen, die komplett in die Cloud umziehen wollen. Hierfür existieren unterschiedliche Migrationsmethoden. Für Unternehmen, die bisher ihre Mails mit Exchange 2003 oder höher verwalten und bis zu 1.000 Benutzerkonten haben, gibt es die Cut-Over-Migration: Der von Microsoft zur Verfügung gestellte Migrationsdienst liest die globale Adressliste aus und richtet alle Benutzer und Verteilergruppen in der Cloud ein. Danach benutzt er Outlook Anywhere oder OWA, um die Mails aus den Mailboxen initial in die Cloud zu synchronisieren. Wenn dies erfolgt ist, läuft die Synchronisation alle 24 Stunden, um die Unterschiede anzupassen. Haben alle Mailboxen einen konsistenten Stand, kommt es zu einer Meldung an den Administrator, damit dieser den Mail-Fluss mittels DNS-Eintrag direkt in die Cloud lenken und die Benutzer umstellen kann.

Für größere Unternehmen bietet Microsoft in den Enterprise-Plänen E1 bis E4 die "Staged Migration" (stufenweise Migration) an. Hierbei kann der Administrator per CSV-Datei bestimmte Konten definieren, die in die Cloud geschoben werden sollen. So ist es etwa möglich, zum Beispiel abteilungsweise oder nach Standorten vorzugehen. Bei der Staged Migration ist zunächst ein Tool zu installieren, das die Benutzerkonten und Verteiler vom lokalen Active Directory in die Cloud synchronisiert (DirSync). Dann kommen CSV-Liste und Migrationsservice zum Einsatz und synchronisieren genauso wie bei der Cut-Over-Migration die im CSV angegebenen Mailboxen in die Cloud. Daher greift auch diese Methode nur dann, wenn bisher mindestens Exchange 2003 genutzt wurde.

Für Unternehmen, die andere Mailsysteme als Exchange nutzen und in die Office 365-Cloud migrieren wollen, kommt die IMAP-Migration in Frage. Das bisherige Mailsystem muss, wie der Name schon sagt, IMAP unterstützen. Hierbei werden zunächst die Konten – bevorzugt mittels einer CSV-Datei – in der Cloud angelegt. Bei der nun folgenden Migration gibt der Administrator dann den IMAP-Server an und übermittelt eine CSV-Datei, die dem Migrationsassistenten mitteilt, wie der Name und das verschlüsselte Passwort für jeden Benutzer lauten. Wie bei den anderen Migrationen lässt sich weiter mit dem bisherigen Mailsystem arbeiten, bis alle Daten umgezogen sind.

All diese Migrationsmethoden gehen davon aus, dass alle Mailboxen in die Cloud migriert werden. Natürlich können einzelne Mailsysteme auch On-Premise bleiben, allerdings muss sich der IT-Verantwortliche dann mit unterschiedlichen Domänennamen in den E-Mailadressen behelfen, wenn es zu einem E-Mailaustausch zwischen der Cloud und der On-Premise-Lösung kommen soll.

Hybride Szenarien verschaffen Flexibilität

Wenn mittelfristig geplant ist, Mailboxen in der gleichen Maildomäne On-Premise und in der Cloud zu haben, kommt ein Hybrid-Szenario in Frage, das auch "Reiche Koexistenz" genannt wird. Dies ist ein sehr komplexes Szenario, das aber volle Integration bietet und in dem sich etwa Anwendungen, die ein lokales Ex-

Cloud-Terminologien

Standorte der Cloud

On-Premise: Die für die Cloud benötigte Hardware steht im Netzwerk / Rechenzentrum des Nutzers.

Off-Premise: Die für die Cloud benötigte Hardware befindet sich außer Reichweite des Nutzers.

Service Modelle

Software as a Service (SaaS): Der Nutzer verwendet die Anwendung des Anbieters, hat aber keine Kontrolle über die Infrastruktur oder globale Einstellungen.

Platform as a Service (PaaS): Der Nutzer kann in der Cloud-Infrastruktur eigene oder zugekaufte Anwendungen laufen lassen. Er hat keine Kontrolle über die Infrastruktur, jedoch über die Anwendungseinstellungen und gegebenenfalls über die Konfigurationseinstellungen der Umgebung für die Anwendung.

Infrastructure as a Service (IaaS): Der Konsument kann CPU-Last, Speicher, Netzwerk und andere fundamentale Ressourcen nutzen und beliebige Software bis hin zu Betriebssystemen laufen lassen. Er hat keine Kontrolle über die Cloud-Infrastruktur, jedoch über das Betriebssystem. Möglicherweise ist auch eine limitierte Kontrolle über Netzwerkkomponenten wie Firewalls vorhanden.

Deployment-Modelle

Private Cloud: Dedizierte Cloud für ein Unternehmen, kann vom Nutzer selbst oder von einem Dienstleister verwaltet werden. Ist sowohl On- als auch Off-Premise möglich.

Community Cloud: Hier teilen sich verschiedene Organisationen mit gemeinsamen Interesse die Cloud. Auch hier ist unerheblich, wer die Infrastruktur verwaltet oder ob die Hardware On- oder Off-Premise steht.

Public Cloud: Hier wird die Cloud der breiten Öffentlichkeit oder vielen Unternehmen zur Verfügung gestellt und von einer Firma verwaltet, die derartige Outsourcing-Services verkauft.

Hybrid Cloud: Eine Verknüpfung verschiedener Cloud-Modelle, die mit Hilfe standardisierter oder proprietärer Technologien verbunden werden.

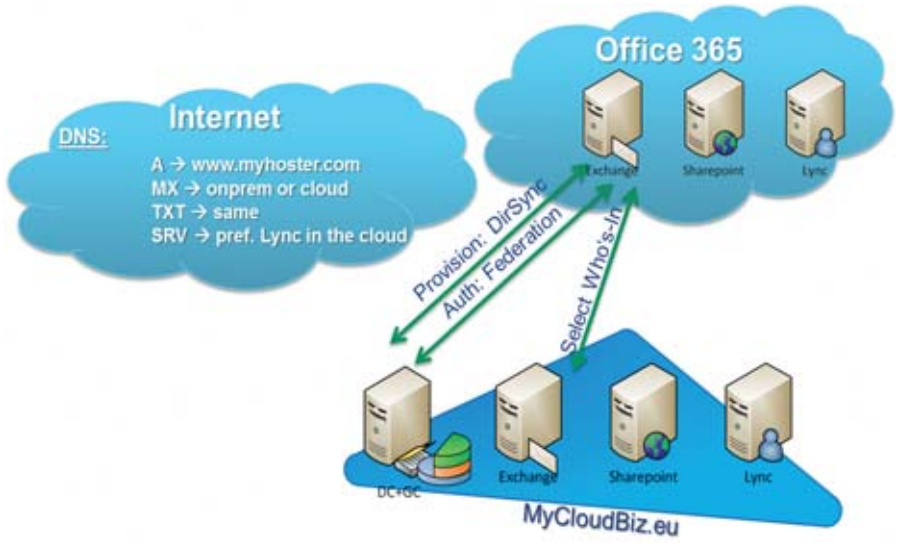


Bild 3: Bei der "Reichen Koexistenz" kann der Administrator Postfächer zwischen dem eigenen Rechenzentrum und der Cloud beliebig hin- und herschieben

change benötigen, weiterhin betreiben lassen. Bei dieser Migrationsmethode wird das Directory Services Synchronisationstool (DirSync) eingesetzt, das Office 365 zur Verfügung stellt. Hierbei handelt es sich um eine eingeschränkte und angepasste Version des Forefront Identity Managers (FIM). Dieser synchronisiert alle Benutzerkonten und Verteilergruppen in die Cloud. Ausnahmen sind standardmäßig zwar nicht erlaubt, allerdings bedeutet die Synchronisation nicht, dass alle Mailboxen zwangsweise in die Cloud müssen.

Beim Einrichten von DirSync muss sich der Administrator vielmehr entscheiden, ob eine Ein- oder Zwei-Wege-Synchronisation stattfinden soll. Bei der Einbahnstraßen-Variante werden nur die On-Premise-Accounts in die Cloud gelegt. Wenn dann vor Ort Änderungen stattfinden, werden diese in der Cloud aktualisiert, nicht aber anders herum. Die Einweg-Synchronisation ist daher weniger bei einem Hybrid-Szenario, sondern eher bei einer Staged Migration denkbar. Die Zwei-Wege-Synchronisation hingegen stellt sicher, dass die Benutzerkonten und Verteilergruppen in beiden Richtungen stets auf aktuellem Stand sind. Somit wird ein Konto, das in der Cloud geändert wird, auch im lokalen Active Directory des Unternehmens angepasst. Für hybride Szenarien, wo meist langfristig geplant ist, On- und Off-Premise-Mailboxen parallel zu verwalten, ist dies sehr sinnvoll.

Der Reiz der "Reichen Koexistenz" liegt primär auf der Exchange-Seite: Die Exchange-Server des Unternehmens (On-Premise) werden mit den Exchange-Servern in der Cloud genauso wie innerhalb einer Organisation verbunden. Damit hat der Administrator volle Kontrolle über das Verschieben von Postfächern, indem er mittels des Mailbox Replication Services festlegt, ob ein Konto in der Cloud oder On-Premise liegt – exakt so, wie er es bei mehreren lokalen Exchange-Servern tun würde. Auch beim Mail-Routing ist er bei diesem Szenario flexibel, On-Premise und Off-Premise haben jeweils die gleichen E-Mailadressen und der Administrator hat die Wahl, ob Mails von extern primär in die Cloud gehen (und hier die Sicherheitsfeatures von Forefront nutzen) oder ob die Nachrichten zunächst in sein On-Premise-Exchange laufen. Die Mails dann entsprechend zwischen vor Ort und der Cloud zu routen, übernimmt Exchange.

Ein weiterer Vorteil ist, dass der Administrator nicht das Outlook der Anwender umkonfigurieren muss, da der Mailclient einen Serverwechsel innerhalb der gleichen Exchange-Organisation automatisch feststellt. Damit ist das hybride Szenario die flexibelste Methode, erfordert aber, Exchange im lokalen Netzwerk zu betreiben. Sogar Outlook Web Access lässt sich in diesem Szenario so einrichten, dass der Anwender immer nur eine URL benötigt und damit Zugriff auf sein Postfach erhält, egal ob sich dieses in der Cloud oder vor Ort befindet.

Kommt das Szenario der "Reichen Koexistenz" zum Einsatz, lassen sich damit zum einen besondere Postfächer, etwa die des Vorstands oder der Personalabteilung, lokal hosten. Zum anderen können lokale Applikationen (zum Beispiel Fax-Server) auf Exchange zurückgreifen und der Administrator hat zusätzlich die Möglichkeit, weitere Funktionen wie

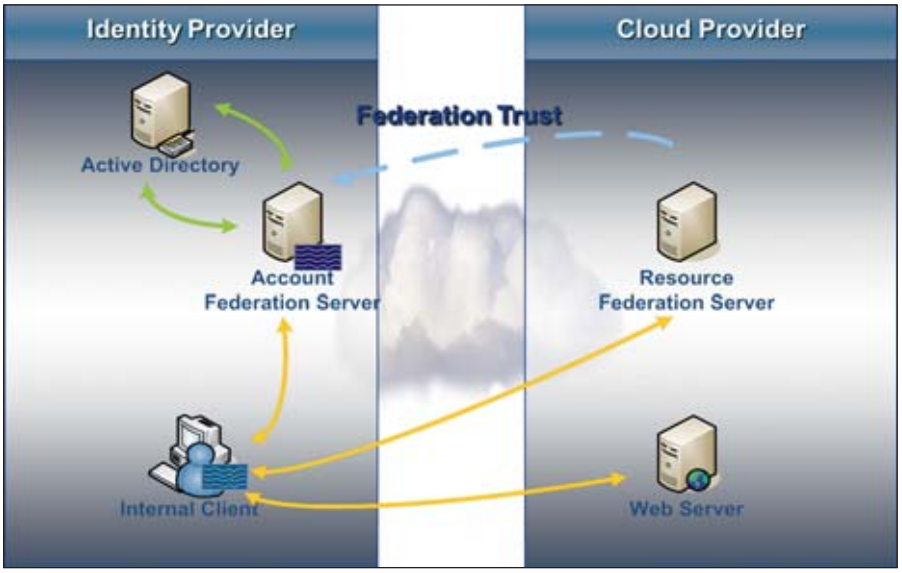


Bild 4: Der Federation Server ermöglicht Single-Sign-On an der Cloud über lokale Benutzerkonten des Unternehmens

Archivierung oder die Forefront-Mailfilter in der Cloud für die lokalen Postfächer zu verwenden.

Single-Sign-On für die Anwender

Ein weiteres Thema bei der erfolgreichen Integration von Cloud-Diensten im Unternehmen ist der Zugriff der Anwender auf ihre Mailbox beziehungsweise die Anmeldung vor der Nutzung weiterer Werkzeuge. Hier gibt es entweder die Methode, dass der Nutzer sein Passwort separat pflegt und sich an den entsprechenden Diensten mit diesen Cloud-Credentials anmeldet. Als komfortabler stellt sich eine Single-Sign-On-Variante dar, die vor allem in größeren Unternehmen empfehlenswert ist. Hierfür ist ebenfalls eine Directory-Synchronisation mittels DirSync notwendig. Zusätzlich kommt lokal ein Federation Server (Active Directory Federation Services, ADFS) zum Einsatz. Dieser wird für die Office 365-Cloud konfiguriert.

Wenn ein Anwender nun auf die Cloud-Dienste zugreifen möchte, egal ob er mit Word ein Dokument auf dem SharePoint-Server abspeichert, per Outlook auf sein Postfach zugreift oder mit Hilfe von Lync kommuniziert, wird er nicht mehr nach Benutzernamen und Passwort gefragt. Stattdessen verweist der Office 365-Server ihn auf den Federation Server. Dieser lokale Server überprüft, ob der Anwender bereits im Unternehmen angemeldet ist. Wenn nicht, wird er nach den Zugangsdaten für seinen Unternehmenslogin gefragt. Sobald der Benutzer dem Unternehmen gegenüber authentifiziert ist, erhält er einen Token und kommt wieder auf den Office 365-Server.

Idealerweise geschieht diese Authentifizierung ohne Benutzerinteraktion, außerdem bietet sie zusätzliche Sicherheit. Wenn ein Mitarbeiterkonto deaktiviert wird, kann der Nutzer auch auf Office 365 nicht mehr zugreifen. Ein zusätzlicher Nutzen: Das Passwort liegt nicht in der Cloud, denn der Anwender identifiziert sich gegenüber seinem Unternehmen und bekommt von dort ein signiertes Internet-Cookie, das ihn zum Zugriff auf Office 365 berechtigt. Ob dies über die Desktop-Versionen der Office-Anwendungen erfolgt oder über das Webportal von Office 365, ist weitestgehend egal.

Kommunikation über Unternehmensgrenzen hinweg

Bisher haben wir die Szenarien Exchange in der Wolke, die eventuell nötige Migration von Daten sowie die Verwaltung der Identitäten betrachtet. Was die Implementierung von Lync betrifft, gibt es nicht viele Varianten: Das Kommunikations-Werkzeug unterstützt kein hybrides Szenario im eigentlichen Sinne. Allerdings ist es theoretisch möglich, bei unterschiedlichen E-Mailadressen für On- und Off-Premise auch Lync On- und Off-Premise zu nutzen und miteinander kommunizieren zu lassen. Bei SharePoint hat der Administrator die Wahl, ob er alle SharePoint-Sites in der Cloud nutzen will oder nur lokal oder die eine Site in der Cloud und die andere vor Ort. Eine wirkliche Integration gibt es in diesem Fall nicht.

Lync kann der IT-Verantwortliche so einrichten, dass die Software die Communicator-Funktionalitäten (Instant Messaging, Online-/Offline-Status, Audio/Video-Anrufe mit Desktop-Sharing) im Verbund mit anderen Unternehmen nutzt. Hierfür muss sich der Administrator entscheiden, ob er die Kommunikation mit allen Unternehmen unterstützt (und gegebenenfalls einzelne blockt) oder ob er nur einzelne erlaubt. Das Gleiche gilt für die "Federation" mit Windows Live Messenger: Der Administrator kann bestimmen, dass die Kommunikation mit den "öffentlichen" Windows Live Messenger-Kontakten erlaubt sein soll. Hier funktionieren dann auch Instant Messages, Online-Offline sowie Audio/Video, allerdings keine Konferenzen oder Desktop Sharing.

Größenbeschränkungen und Integrationshürden

Office 365 bietet zwar eine Menge Möglichkeiten und ist in vielen Bereichen eine

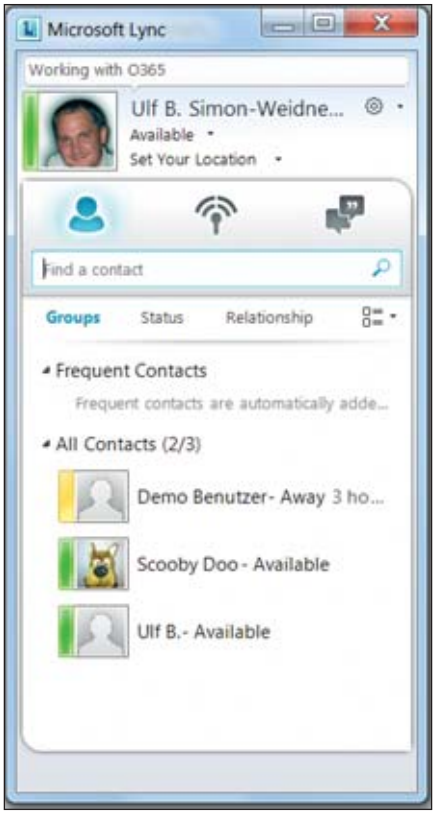


Bild 5: Lync kann auch mit Partnerunternehmen oder Windows Live-Konten kommunizieren, wenn der Administrator es erlaubt

runde Lösung, es gibt jedoch wie immer Punkte, die vor dem Einsatz diskutiert werden sollten. So zum Beispiel existieren einige Limits: Die 25 GByte Postfachgröße und 25 MByte pro Mail werden vielleicht für die meisten Unternehmen ausreichend sein. Aber es gibt etwa auch die Beschränkung, dass nur bis zu 10.000 Benutzer initial mit DirSync synchronisiert werden können. Dieses Limit lässt sich allerdings vom Support anheben, wenn das Unternehmen mehr Anwender in Office 365 bringt. Außerdem sind beim E-Mailversand für jedes Mailkonto nur Mails an 500 (bei P1) beziehungsweise 1.500 (bei den Enterprise-Plänen) individuelle Empfänger (externe E-Mailadressen oder in Office 365 integrierte Verteilerlisten) pro Tag zugelassen. Microsoft will so verhindern, dass die E-Mailserver von Office 365 als Spamserver missbraucht werden. Für Massenmails sollten daher entsprechende Dienste spezialisierter Dienstleister zum Einsatz kommen. Es gibt noch weitere, speziellere Limits, die unter URL [4] einsehbar sind.

Das Thema Sicherheit hatten wir bereits kurz betrachtet – bei der Verwendung von Online-Providern ist immer zu überlegen, welches Maß an Sicherheit im Unternehmen angebracht ist. Hier liegt Office 365 sicherlich nicht schlecht und auf jeden Fall deutlich über dem Extrem-Szenario einer Umgebung, in der sich der Administrator nicht fortbilden kann und in der für das Patchen und Aktualisieren keine Zeit bleibt. Office 365 wird immer aktuell gehalten und sämtlicher Netzwerkverkehr ist verschlüsselt. Auf der anderen Seite sind die Administratoren nicht persönlich bekannt und manche Sicherheitslösungen wie Festplattenverschlüsselung lassen sich nicht oder nur schwer integrieren.

Was die Administration betrifft, geschieht auf den ersten Blick sehr viel über das webbasierte Administrationsportal. Wenn eine Verzeichnisdienst-Synchronisation eingerichtet ist, kann der Administrator seine Standardkonsolen wie Active Directory-Benutzer und -Computer verwenden, um einen Teil der Verwaltung durchzuführen. Und auch die Exchange Verwaltungskonsole steht zum Einsatz bereit, um Exchange online zu managen. Zusätzlich kann der Administrator über die PowerShell Cmdlets für Office 365 viele Aufgaben über PowerShell-Skripte und -kommandos durchführen [5].

Für eine unternehmensintegrierte Office 365-Lösung ist zwar etwas Know-how der primär verwendeten Produkte sinnvoll, die eigentlichen Herausforderungen stellen sich jedoch an anderer Seite: Office 365 benötigt einiges an Hintergrundtechnologien. Zum Beispiel werden keine Domänenregistrierung und kein unternehmensspezifisches DNS angeboten. Dies muss das Unternehmen separat verwalten. Wenn E-Mailadressen zum Einsatz kommen sollen, die nicht nach dem Muster *Mailadresse@{Domäne}.onmicrosoft.com* aufgebaut sind, sind Einstellungen am öffentlichen DNS unausweichlich. So muss ein CNAME eingetragen werden, um Microsoft zu beweisen, dass der Name dem Unternehmen gehört und administrierbar ist.

Für Exchange sind die MX-Einträge anzupassen, für SharePoint wiederum bedarf es eines CNAME oder A-Eintrags. Um außerdem zu vermeiden, dass Unternehmen Mails nicht akzeptieren, ist ein TXT-Eintrag und für Lync sogar ein Service-Eintrag (SRV) vonnöten. All diese Feinjustierungen sind obligatorisch, nur um einen eigenen Domänennamen verwenden zu können. Für DirSync ist Directory-Know-how von Vorteil, es gibt sogar Szenarien, wo ein zusätzlicher Einsatz des Forefront Identity Managers sinnvoll ist (für Gesamtumgebungen mit mehreren Domänen, die ein Office 365 nutzen möchten). Für Single-Sign-On wiederum sollte sich der IT-Verantwortliche mit den Federation Services auseinandergesetzt haben, außerdem bedarf es an Zertifikaten, damit die Tokens signiert und sicher übertragen werden können.

Die Office 365-Onlinehilfe [6] bietet eine gute Unterstützung für die Einrichtung der benötigten Komponenten. Zusätzlich gibt es den Exchange Server Deployment Assistenten [7], der dem Administrator zur Seite steht, wenn es darum geht, seine Anforderungen zu definieren. Außerdem gibt es hier ein Dokument, das dem IT-Techniker bei der Einrichtung hilft. Trotzdem ist für die tägliche Arbeit und das Troubleshooting hilfreich, sich vor allem mit den im Hintergrund verwendeten Technologien auseinanderzusetzen.

Fazit

Office 365 bietet eine gute Rundum-Lösung für Unternehmen, die ihren Kommunikationsbackbone mit E-Mail, Terminverwaltung, Präsenz- und Sprachintegration, Dokumentenverwaltung, Intranet oder sogar Austauschplattform im Internet auf SharePoint und gemeinsames Arbeiten mit der Office Produktpalette in die Cloud legen wollen. Besonders durch die gut gelöste Integration der Anwendungen untereinander bis hin zum Desktop des Anwenders inklusive Single-Sign-On gestaltet sich das Arbeiten in der Cloud nahezu reibungslos. Nie außer Acht gelassen werden sollte hierbei, dass nicht die Download-, sondern die Upload-Geschwindigkeit der Netzwerkleitung ausschlaggebend für das Tempo der Migration ist.

Für die Integration in die Unternehmensinfrastruktur ist einiges an Know-how erforderlich. Dies betrifft nicht unbedingt die im Vordergrund stehenden Technologien, sondern auch Themen wie DNS, Verzeichnisdienste, Federation Services und Zertifikatsdienste. Insbesondere wenn mehr und mehr verschiedene Dienste aus unterschiedlichen Clouds genutzt werden, ist es wichtig, die Gesamtinfrastruktur im Überblick zu behalten. *(ln)*

Link-Codes

[1] Office 365 für Selbstständige und kleine Unternehmen
C1P11

[2] Office 365 für mittelständische und große Unternehmen
C1P12

[3] Informationen zu Lizenzbeschränkungen
C1P13

[4] Grenzen für Nachrichten, Postfach und Empfänger
C1P14

[5] Windows PowerShell für die Verwaltung von Office 365
C1P15

[6] Office 365-Onlinehilfe
C1P16

[7] Exchange Server Deployment Assistant
C1P17

Werkzeuge zum Aufbau eines internen Schulungsraums

Schöner lernen

von Thomas Bär

Klagen Anwender, dass sie über die Möglichkeiten von Applikationen nur unzureichend informiert sind oder keine Chance haben mit neuer Software zu üben, ist wohlmöglich eine Schulung der betreffenden Kollegen angebracht. Doch mit welchen Werkzeugen lässt sich eigentlich eine IT-Trainingsumgebung aufbauen? Um den Schulungserfolg zu gewährleisten, muss ein möglichst reales Abbild der Softwareumgebung der Benutzer dargestellt werden, um diese praxisnah zu schulen. Richtet sich die Maßnahme an einen größeren Personenkreis ist der Aufbau eines Schulungsraums sinnvoll. Dieser Beitrag stellt Werkzeuge vor, die Administratoren bei dieser Aufgabe unterstützen.

Eines sollte der technisch aufrüstende Trainingsleiter zunächst bedenken: Insbesondere die Fernwartungs- und Überwachungsfunktion ist bei Trainingsteilnehmern nicht unbedingt beliebt. Während es Teilnehmer gibt, die mit der Überwachung ihrer Bildschirminhalte überhaupt kein Problem haben, so gibt es andere Teilnehmer, die vor lauter Nervosität nicht mehr dem Unterrichtsstoff folgen. Hier gilt es ein gutes Händchen zu beweisen und lieber einmal mehr durch die Reihen der Teilnehmer zu gehen, als nur vom Lehrer-PC aus zu überwachen. Eine hohe Qualität des Unterrichtsstoffs ist in jedem Fall der Garant dafür, dass die Gruppe vom Unterricht profitiert und dass der Kurs insgesamt Spaß macht. Bei schlechtem Unterrichtsmaterial hilft die beste IT-Ausstattung im Trainingsraum nichts.

Microsoft Windows Multipoint Server 2011

Der Microsoft Windows Multipoint Server 2011 (WMS 2011) [1] löst die erst Anfang 2010 vorgestellte erste Fassung von WMS bereits wieder ab. An den WMS 2010 wurden die Eingabegeräte direkt über USB 2.0 an den WMS-Server, Benutzerbildschirme entweder an Grafikkarten im WMS-PC oder über USB-Grafikkartenlösungen angeschlossen. Die Begrenzungen im Konzept für bis zu elf Benutzerstationen werden durch dessen Nachfolger weitgehend aufgehoben. Die zweite Generation, der Microsoft Windows Multipoint Server 2011, erlaubt zusätzlich zur USB-Verkabelung die Verwendung von Arbeitsplätzen über traditionelle Netzwerkverbindungen. Der Zugriff erfolgt, wie bei Microsoft üblich, über das eigene Remote Desktop Protocol (RDP). Somit sind grundsätzlich alle Zugriffsgeräte, die RDP verstehen, für die Zusammenarbeit mit dem WMS 2011 geeignet. Und das sind faktisch alle Thin Clients am Markt.

Microsoft positioniert den WMS 2011 speziell für Bildungseinrichtung oder Unternehmen, die IT-Schulungen anbieten. Der Multipoint Server basiert auf Microsoft Windows Server 2008 R2 in der x64-Edition und wird wie dieser direkt vom Datenträger installiert. Es ist somit weniger eine Applikation für den Schulungsraum als ein komplett darauf zugeschnittenes Betriebssystem. Die Systemanforderungen ergeben sich aus dem Windows Server 2008 R2-Unterbau. Dank der identischen Oberflächen von Windows 7 und dem Windows Server 2008 R2 garantiert WMS 2011 die Schulung in einer typischen Windows-Umgebung. In der Standard-Edition ist der Schulungsleiter in der Lage, mit dem Server bis zu zehn Teilnehmer gleichzeitig auf einem einzigen Server zu trainieren, die größere Premium-Edition erlaubt bis zu 20 Benutzern den gleichzeitigen Zugriff. Ein weiterer Vorteil der Premium-Variante ist die Möglichkeit, mit dem Server einen "Domain Join" durchzuführen – diese Funktion bleibt der kleineren Version vorenthalten. Üblicherweise verkauft ein Anbieter den WMS 2011 als OEM-Variante direkt mit der Hardware. Für jeden zugreifenden Benutzer wird eine spezielle WMS 2011 CAL benötigt.

Der WMS 2011 ist jedoch mehr als ein angepasster Windows Terminalserver, da die Verwaltungssoftware speziell für den Trainingsbetrieb angepasst ist. Zur Steue-

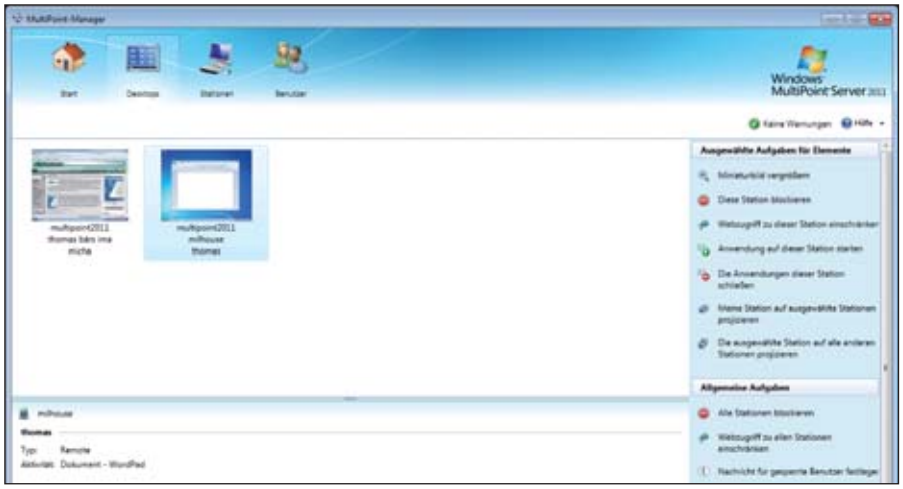


Bild 1: Der Windows MultiPoint Server von Microsoft ist eine spezielle Variante eines Terminalservers mit zusätzlicher Management-Oberfläche für das Trainings- und Schulungsumfeld

rung der Client-Systeme, Anlage von Benutzern und für die Überwachung der Desktops bietet die Software den Dialog "MultiPoint-Manager". Die Benutzeranlage ist für den Trainer sehr einfach – Anmeldenamen und vollständigen Namen eintragen, Passwort festlegen und in der Rechtesteuerung auswählen, ob es sich um einen "Standardbenutzer" oder um einen User mit "administrativen Rechten" handelt. Über den MultiPoint-Manager ist der Trainer mit einem einzigen Mausklick in der Lage, einzelne Client-PCs zu sperren, den Anwendern über die Schulter zu schauen oder den eigenen Desktop auf den Client-Bildschirmen zu präsentieren. Der Internet Explorer in den Client-Sessions ist in der Standardauslieferung freizügig konfiguriert – Schüler können somit alle Webseiten erreichen. Sobald die Webseiten-Einschränkung durch den Trainer aktiviert ist, erlaubt der WMS 2011 nur noch den Besuch der freigegebenen Seiten und deren Unterseiten. Das Surfen auf andere Ziele wird mit dem Hinweis "Navigation zu der Webseite wurde abgebrochen" unterbunden. Wird ein alternativer Browser, beispielsweise der Firefox, auf dem Server installiert, so greift die Webseiten-Einschränkung nicht – sie funktioniert nur mit dem IE. Microsoft OneNote ist laut Herstellerangaben auf das Zusammenspiel mit dem WMS 2011 angepasst, so dass mehrere Schulungsteilnehmer gleichzeitig an einem Dokument arbeiten können.

NComputing vSpace und L300

Die Zugriffsgeräte aus dem Hause NComputing [3] sehen auf den ersten Blick aus wie ganz gewöhnliche Thin Clients. Im Zusammenspiel mit der vom NComputing entwickelten vSpace-Software wird aus dem System eine Alternative, um Standard-PCs, Server oder virtuelle Computer wie kleine Terminalserver zu betreiben, jedoch nicht nur für den Schulungsraum, auch im Kiosk-Betrieb, Info- oder Anzeigeterminal über Internet-Cafes bis hin zum klassischen PC-Ersatz im Büro. Aber auch im Zusammenspiel mit dem bereits genannten Microsoft Windows Multipoint oder in Citrix VDI-Landschaften machen die Zugriffsgeräte ein gutes Bild.

Die zur eigenen vSpace-Software passenden Client-Zugriffsgeräte bietet der Hersteller in unterschiedlichen Ausbaustufen an. Die Zugriffsgeräte, da sie eigentlich keine reinrassigen Thin Clients sind, verwenden nicht die gewöhnlichen Terminal-Protokolle wie ICA oder RDP, sondern nutzen eine Eigenentwicklung von NComputing: das UXP (User eXtension Protocol). UXP überträgt alle Bildschirm-, Sound- und Schnittstelleninformationen über die Standard-Ethernet-Verbindungen. Eine zusätzliche Verkabelung ist nicht erforderlich. NComputing bietet drei unterschiedliche Varianten der nur wenigen Zentimeter großen Client-Systeme in der L-Serie an. Alle bieten den traditionellen VGA-Stecker zum Anschluss des Monitors, verfügen über ein externes Netzteil, haben keinen eingebauten Lüfter und sind somit komplett geräuschlos. Der Stromverbrauch liegt laut Herstellerangaben bei rund 5 Watt pro Gerät, sofern keine externen USB-Geräte angeschlossen sind. In Bezug auf Farbtiefe, Bildschirmauflösung und Anschlussmöglichkeiten bieten die Geräte alles, was Benutzer und Administratoren heutzutage erwarten.

Über einen Mikrofon-Anschluss verfügt lediglich das größere Modell, das L300. Dass ist jedoch nicht das einzige Leistungsmerkmal – Multimedia-Inhalte wie beispielsweise in Webseiten integrierte Videos oder bildschirmfüllende Filme werden in der Sitzung mit voller Geschwindigkeit dargestellt. Ein spezieller Chip im L300-Gerät – der Numo system-on-chip (SOC) – sorgt dafür. Das Geheimnis hinter dieser Beschleunigung ist das Zusammenspiel der vSpace-Software auf dem Hostsystem und dem Chip im Zugriffsgerät. Videoinhalte wie .avi- oder .wmv-Dateien transkodiert die vSpace-Engine und schickt diese als komprimierten Stream direkt an das Zugriffsgerät. Das L300 entschlüsselt die komprimierten Daten aus dem UXP-Protokoll und stellt diese in der vom Benutzer oder Programm geforderten Größe dar. Bedingung für eine problemlose und ruckelfreie Darstellung von Multimedia-Inhalten ist eine ausreichend dimensionierte Netzwerkanbindung. In einem Testszenario mit auf 10 MBit/s reduzierten Switches kam es erwartungsgemäß zu Aussetzern. Die Bedienung von Office-Programmen ist selbst bei 10 MBit/Half Duplex problemlos möglich.

Die Hardware-Voraussetzungen auf Seiten der PCs beziehungsweise Server hängen sehr stark vom geplanten Einsatzfeld ab. Um zirka 8-10 L300-Zugriffssysteme mit Standard-Büroprogrammen zu versorgen,

Lernplattform moodle

Geht es lediglich darum, Unterrichtsmaterial bereitzustellen und Kursteilnehmer sowie Kursinhalte zu verwalten, so ist möglicherweise eine gänzlich andere Plattform spannend. Das Lernsystem "moodle" [2] ist ein objektorientiertes Kursmanagementsystem und gleichzeitig eine Lernplattform auf Open Source-Basis. Die Software bietet die Möglichkeiten zur Unterstützung kooperativer Lehr- und Lernmethoden. Das in erster Linie auf PHP und MySQL aufsetzende System für Linux- und Windows-Rechner erfreut sich eines hohen Verbreitungsgrads und erlaubt, Kurse komplett über das Internet abzuwickeln. Selbst kleine virtuelle Maschinen, bei einem Hoster angemietet, eignen sich für den Betrieb von moodle im Internet.

empfiehlt der Hersteller eine aktuelle Core2-Maschine mit 3 GByte Hauptspeicher. Um Multimediainhalte auf derselben Anzahl von Clientsystemen darzustellen, sollte es ein Rechner der Core i7-Leistungsklasse sein. vSpace arbeitet auf allen 32/64-Bit Varianten von Microsoft Windows ab XP und unterstützt ebenfalls die eingangs erwähnte Microsoft Multipoint Server Edition. Die Unterstützung von Linux beschränkt sich auf Ubuntu 8.10 für die Zugriffsgeräte 130 und 230 beziehungsweise auf 8.04 LTS für die Geräte X350 und X550.

Interessierte können sich bei den Verkäufern von NComputing-Produkten eine vierzehntägige, kostenlose Teststellung zuschicken lassen. Test und Aufbau sind innerhalb weniger Minuten erledigt. Auf einem Windows-Computer sind die vSpace Desktop Virtualization Software zu installieren und die gewünschten Benutzer in die Gruppe der "Remotedesktopbenutzer" einzufügen. Die vSpace-Software muss der Administrator über ein Webinterface registrieren, da ansonsten keine Verbindung mit dem Zugriffsgerät möglich ist, und an das Zugriffsgerät Maus, Tastatur, Monitor und Netzwerk anschließen. Ein Zugriffsgerät vom Typ L300 benötigt rund eine Minute, bis es einsatzbereit ist, und findet die vSpace-Installationen im Netzwerk automatisch. Ein Doppelklick auf den Computernamen der vSpace-Installation und schon ist der Anmeldebildschirm von Windows sichtbar und nutzbar.

Etwas gewöhnungsbedürftig für den Administrator, der eine vSpace-Umgebung betreut, sind die Unterschiede im Vergleich zum Windows-Standard. Üblicherweise zeigt der Windows Task-Manager im Register "Benutzer" alle derzeit auf dem PC/Server verbundenen lokalen oder entfernten Sitzungen. Benutzer, die über vSpace angemeldet sind, fehlen in der Liste. Lediglich die vSpace-Konsole zeigt alle aktiven User-Sessions. Differenzierte Einstellungen und Berechtigungen nehmen Administratoren und Schulungsanbieter über die "Network UTMA/UTSA"-MMC vor. Das Menü der Konsole besteht aus fünf Menüpunkten, von denen einer auf die lokalen Windows/Benutzer-Einstellungen des Host-Systems verweist. Über die "Allgemeinen Einstellungen" legt der Administrator unter anderem fest, ob das Hintergrundbild von Windows angezeigt wird, welche Standardkompression für JPEG in der Sitzung verwendet wird oder wie viele Sitzungen auf einem PC/Server maximal zulässig sind. USB-Geräte können, sofern entsprechend aktiviert, über das Zugriffsgerät direkt in die Sitzung weitergeleitet werden – was insbesondere den Einsatz von Speichergeräten vereinfacht.

Im Menüpunkt "Sitzungen" zeigt die Software alle aktuellen Benutzersitzungen auf dem PC/Server an. Wie von der Microsoft-Terminalverwaltung bekannt, ist es dem IT-Profi möglich, einem Anwender über das "Spiegeln" des Desktops bei Problemen zu helfen und Kurzmeldungen in die Sitzungen zu senden. Dies ist jedoch eher eine Support-Möglichkeit denn eine Funktion für den Unterricht. vSpace eignet sich primär für die kostengünstigere Bereitstellung von Arbeitsplätzen. Preise ab 134 Euro pro Zugriffsgerät sind durchaus attraktiv. Das Microsoft-Lizenzrecht erfordert jedoch, was ein Blick in die Lizenzbedingungen zeigt, dass sowohl Windows-CAL als auch Terminalserver/Remotedienst-Zugriffslizenz beziehungsweise eine WMS 2011-CAL pro Zugriffsgerät erforderlich ist.

NetMan for Schools und die H+H Schulbox

Die H+H Software GmbH [4] bietet mit NetMan for Schools und der H+H Schulbox gleich zwei Produkte für das elektronische Klassenzimmer. Beide Windows-Lösungen ermöglichen eine klassische Unterrichts- und Anwendungssteuerung, bei der eine Lehrkraft den Schülern Anwendungen im Startmenü oder auf dem Windows-Desktop zur Benutzung freigeben und per Drag & Drop direkt für diese starten kann. Um dem Lehrer die Abwicklung einfacher zu machen, wird der Name des Schülers und optional sogar dessen Foto oder aktueller Bildschirminhalt auf dem Lehrer-PC angezeigt. Alle weiteren typischen Funktionen wie Spiegelung des Inhalts auf den Lehrer-Rechner und umgekehrt, Schwarzschalten aller Bildschirme, um die Aufmerksamkeit zu zentrieren, Gruppenbildung, Chat-Funktionen, Ordner/Laufwerks-Verwaltung, Steuerung von lokalen Laufwerken, Dateiaustausch und ein modernes Webfrontend bieten beide Programme.

Die H+H Software ist auf die Bedürfnisse von Bildungseinrichtungen zugeschnitten, in denen Kinder unterrichtet werden. Im Klassenarbeitsmodus kann der Lehrer Aufgaben verteilen und auch wieder einsammeln – der Hersteller versucht, sich ganz klar an der Terminologie der Schule zu orientieren. Weiter unterstützt die Software externe Filtertechniken für Webseiten wie Time 4 Kids oder Telco Tech. Globale Filtersets lassen sich vom Systembetreuer sehr leicht für die ganze Schule definieren. Eine Anpassung des Filters während des Unterrichts, quasi "on the fly", ist dem berechtigten Lehrer dennoch möglich.

Der primäre Unterschied ist, dass die H+H Schulbox lediglich im LAN-Umfeld eingesetzt werden kann. Das System kommt installiert und vorkonfiguriert als Hyper V- oder ESX-Image auf einer DVD und muss lediglich gestartet werden. Die H+H Schulbox wird von verschiedenen Resellern angeboten und ist für Grundschulen kostenlos, während der übliche Lizenzpreis bei rund 40 EUR liegt. Der typische Support über das Internet durch H+H-Mitarbeiter ist kostenfrei, zusätzliche Supportleistungen können auf Anhieb erworben werden.

NetMan for Schools, die größere Variante, nutzt alle erdenklichen Zugriffstechniken wie LAN, Remote Desktop, Terminal-Session, Virtual Desktop Infrastructure (VDI) und gestreamte Betriebssysteme, die sich selbst auf schwächeren Systemen wie Intel ATOM-getriebenen Thin Clients noch nutzen lassen. Die aktuelle Version 4.5 von NetMan for Schools bietet einen integrierten Multimonitor-Support. Beispielsweise kann so für den Lehrer auf dem regulären Monitor die Klassenraumsteuerung aktiv sein, während auf dem Smartboard Unterrichtsinhalte dargestellt werden. Selbst Apple iPads und Zero-Clients wurden, laut Informationen des Anbieters, in der aktuellen Version erfolgreich eingesetzt. Mit der neuen Version 5 kann 2012 gerechnet werden.

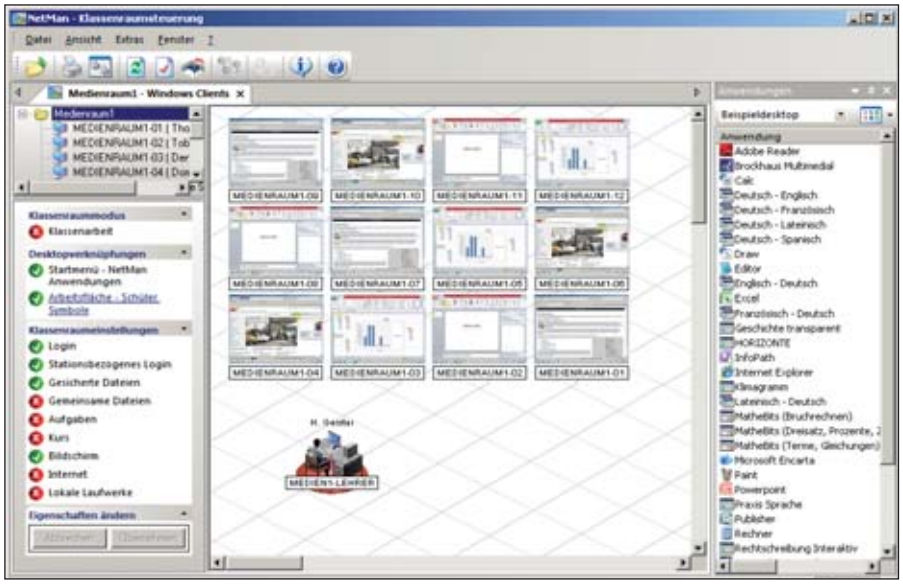


Bild 2: Die NetMan-Software ist speziell auf die Durchführung von digitalem Unterricht im Klassenzimmer optimiert

Klassenraum-Management mit NetOP School

NetOp School [5] ist wie die Software von H+H speziell auf die Anforderungen in Bildungseinrichtungen angepasst. Die Windows-Software verwaltet das Zusammenspiel von Trainer- und Teilnehmer-PCs in "interaktiven Klassenzimmern". In der kleinsten Ausprägung der Software wird lediglich ein Lehrer-PC eingerichtet – der Rechner, von dem aus der Unterricht geführt und vorbereitet wird. Studenten-PCs, die Installation für den Teilnehmer, schalten sich durch die Eingabe der "Klassenraumbezeichnung" oder über NetBIOS- beziehungsweise IP-Namen in den Unterricht auf. Mit Netop School können Lehrer die Aktivitäten der Schüler beaufsichtigen, das Surfen im Internet überwachen, den Bildschirminhalt jedes Computers zu den anderen Computern im Klassenraum übertragen und die Studenten-Computer fernsteuern.

Alle wichtigen Funktionen wie das Sperren von Bildschirm, Tastatur und Maus der Studenten-Computer, Anzeigen des Lehrer-Desktops auf den Studenten-Computern, Übertragen von Dateien zwischen dem Lehrer- und den Studenten-Computern, Überwachen der Studenten-Bildschirme, Unterbinden des Besuchs unerlaubter Websites im Internet, Übermitteln der Arbeit eines Schülers an die anderen Schüler, Unterstützen der Schüler durch Fernsteuerung der Student-Computer und das Chatten mit den Teilnehmern bietet NetOP School. Die Einrichtung der Software ist einfach und setzt kein tiefgreifendes IT-Know-how voraus. Es gibt lediglich zwei MSI-Pakete: Eines mit der Bezeichnung "Teacher", das andere mit der Bezeichnung "Student". Die Benutzeroberfläche der Software ist in faktisch allen europäischen Sprachen verfügbar und erklärt sich weitgehend von allein. Optisch spricht die Multifunktionsleiste im Stil der Microsoft Office 2007-Panes an. Anstelle Befehle in den Tiefen der Menüs zu suchen, sind diese thematisch sortiert in der Leiste angebracht.

Den Unterrichtsablauf kann der Trainer über die Funktion "Stundenplan" bereits im Vorfeld vorbereiten und speichern. Es gibt hierzu eine Reihe von Unterrichtsaktionen wie "Chatting", "Vorführen bestimmter Inhalte" oder das "Vorführen einer Media-Datei", die vorgeplant werden können. Eine äußerst spannende Funktion ist das Anlegen von "Tests" oder "Umfragen". Hierzu bietet die Software einen Assistenten und einen Demo-Test, beispielsweise die Möglichkeit "Bild-Zuordnungen" im Unterricht zu verwenden: Dies kann dann so gestaltet werden, dass beispielsweise die Namen der Planeten auf der rechten Bildschirmseite darauf warten vom Schüler per Drag & Drop an die richtige Stelle des grafisch dargestellten Sonnensystems gelegt zu werden. Insgesamt kennt Netop die Fragetypen Listenfelder, Aufsätze, Bild kennzeichnen, Bild

zuordnen, Texte zuordnen, Multiple Choice-Tests, Sortierung, Frage und Antwort und das Vervollständigen von Texten.

Eine Besonderheit von Netop ist die optional erhältliche Hardware – das so genannte "TeachPad". Das TeachPad ermöglicht Trainern die Steuerung von grundlegenden Funktionen der Klassenraum-Management-Software über nur fünf Tasten. Lehrkräfte können per Knopfdruck Schüler betreuen, Unterrichtsinhalte demonstrieren, Surfaktivitäten kontrollieren und Computerbildschirme sperren. In Bildungsstätten, in denen Terminal-Services eingesetzt werden, empfiehlt der Hersteller die Nutzung des "Netop Gateway". Das optionale Modul ermöglicht das Routing des Netop-Datenverkehrs über verschiedene Protokolle, beispielsweise http und UDP, und über verschiedene Server. Der Netop Class Server ist für Schulen konzipiert, in denen jeder Teilnehmer über einen Computer verfügt oder ein Großteil der Schüler mit Laptops arbeitet.

MasterSolution Protect – keine Änderungen bitte!

Eine kleine Software, MasterSolution Protect [6], eignet sich hervorragend für den Einsatz im IT-Trainingsraum. Mit MasterSolution Protect steuert der Systembetreuer mit wenigen Mausklicks den Zugriff auf Dateien und Ordner, Systemsteuerung, Desktopelemente, Anwendungen, Netzwerkressourcen, Drucker oder externe Speichermedien. Auch ohne die Integration in ein Active Directory und Nutzung von Gruppenrichtlinien ist dem Administrator mit Protect möglich Komponenten gezielt auszublenden oder den Zugriff zu verweigern.

Eine überaus spannende Funktion ist jedoch der aktive Schutz von Einstellungen auf dem Client-Rechner. Besonders in Schulungsräumen, in denen keine Überwachung durch IT-Personal gewährleistet ist, sind die Maschinen ansonsten oft "verkonfiguriert". Protect kann so eingestellt werden, dass alle Änderungen auf einer Festplatte beim Neustart rückgängig oder gezielt Änderungen in ausgewählten Ordnern gemacht werden.

Training in der Wolke

Einen gänzlich anderen Weg beschreitet der westfälische Anbieter Materna mit Sitz in Dortmund. "Training in a Cloud" [7] ist eine Cloud-Lösung für Anbieter von IT-Schulungen und -Weiterbildungen. Es basiert auf virtuellen Servern und Desktops und macht die manuelle Konfiguration der Schulungs-Umgebung nahezu überflüssig. Trainer rufen über ein Self-Service-Portal die einmal vorbereiteten Trainingsumgebungen ab und stellen diese über das System auf einer beliebigen Anzahl von Trainingsarbeitsplätzen bereit.

Mit Training in a Cloud laufen alle Arbeitsschritte für die Ausstattung der virtuellen Schulungsräume bis hin zur Einrichtung der Benutzerkonten für die Seminarteilnehmer im Idealfall automatisiert ab. Durch Einsatz von Technologien zur Desktop-Virtualisierung muss der Systemadministrator keine Schulungsumgebungen manuell auf den PCs installieren, da das System alle Konfigurationsaufgaben automatisiert durchführt. Die Aufträge für die Ausstattung der virtuellen Schulungsräume werden regelbasiert und in vom Trainer definierten Zyklen durchgeführt. Der Seminarplaner wiederum kann sich zusätzlich zum Management von Dozenten, Teilnehmern und Räumen auch direkt um das Bereitstellen der Trainingsumgebungen kümmern – alles aus einer zentralen Seminarverwaltungsoberfläche heraus und ohne den manuellen Eingriff durch IT-Experten.

Was ein wenig nach Science Fiction klingt, ist ein komplett ausgearbeitetes Projekt von Materna für die Produkte aus dem eigenen Hause und eine praktische Anwendung von VDI-Techniken. Dahinter verbergen sich verschiedene Software-Komponenten von Materna: DX-Union übernimmt das Erstellen der Desktop-Arbeitsplätze sowie der benötigten Benutzerkonten und administriert alle Ressourcen, die für eine automatisierte Bereitstellung physischer oder virtueller Desktops benötigt werden. DX-Union arbeitet hier mit den Virtualisierungstechnologien von Citrix und VMware zusammen. Eine von Materna entwickelte Automatisierungs-Engine realisiert das Provisioning der Desktops. Weitere Komponenten in diesem Konzept sind die Seminarverwaltungs-Software Orbis und das Schulungsteilnehmer-Frontend Caruso der Tochtergesellschaft Materna TMT, einem Spezialanbieter für Seminarverwaltungs-Software.

Die Lösung unterstützt den gesamten Geschäftsprozess von der Seminarplanung bis zur automatisierten Bereitstellung der IT-Trainings. Das Einrichten verschiedener Schulungsumgebungen ist laut Hersteller für den Seminaranbieter vollständig automatisierbar. Mit "Training in a Cloud" können Unternehmen, die nur über eingeschränkte Hardware-Kapazitäten verfügen, flexibel auf die Nachfrage nach Schulungen reagieren. So können Trainingsanbieter beispielsweise auch ausgefallene Schulungskonfigurationen anbieten, deren konventionelle Bereitstellung aus wirtschaftlichen Gründen bisher unattraktiv war. Weitere denkbare Einsatzgebiete wären die Inhouse-Schulungen beim Kunden und das Training in Hotel-Umgebungen, da lediglich Client-Systeme wie Notebooks für den Zugriff auf die VDI-Landschaft benötigt werden.

Fazit

Es gibt in Sachen Schulungsraum nicht immer die vollständig passende Variante. Aber die hier vorgestellten Tools erlauben gänzlich unterschiedliche Konzepte. Während sich manche Programme vorwiegend um die Gestalt des Unterrichts an sich kümmern, sind andere Lösungen eher für die Infrastruktur zuständig. Faktisch werden immer ein Arbeitsplatz und die gewünschten Programme benötigt, um die Schulungs-Maßnahme durchzuführen. *(jp)*

Link-Codes

[1] Microsoft Windows Multipoint Server 2011
C1P71

[2] Lernplattform moodle
C1P72

[3] NComputing Europe GmbH
C1P73

[4] H+H Software GmbH
C1P74

[5] Netop Solutions A/S
C1P75

[6] MasterSolution AG
C1P76

[7] MATERNA GmbH
C1P77

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

Innerhalb einer **Hyper-V-Installation** möchten wir im Unternehmen gerne **virtuelle Maschinen mit Linux als Betriebssystem** betreiben. Soviel ich weiß, stellt dies dank der sogenannten Integration Services von Microsoft keine große Herausforderung mehr dar. Trotzdem würde mich interessieren, **welche Linux-Distributionen** überhaupt für den virtualisierten Betrieb unter Hyper-V unterstützt werden, welche Treiber dazu nötig sind und wie sich diese am einfachsten aufspielen lassen. Können Sie mir hier weiterhelfen?

Die erforderlichen Treiber für Hyper-V sind ab Version 2.6.32 im Linux Kernel integriert. Der Source Code wurde der Linux Community übrigens von der Microsoft Open Source Community als GPL 2 zur Verfügung gestellt. Was die verschiedenen Distributionen betrifft, unterstützt Microsoft offiziell SUSE Linux Enterprise Server 10 SP4 und 11 SP1, Red Hat Enterprise Linux 5.2 bis 5.6, 6.0 und 6.1 sowie CentOS in den Versionen 5.2 bis 5.6 und 6.0. Dies bedeutet jedoch nicht zwangsweise, dass sich andere Distributionen nicht unter Hyper-V betreiben lassen. Ubuntu ist ein solches Beispiel: Microsoft unterstützt Ubuntu offiziell nicht, dennoch ist der Code für die Integration Services im Kernel integriert und demnach auch für virtuelle Maschinen unter Hyper-V verfügbar. Der Betrieb funktioniert in der Regel recht ordentlich, denn sind die Treiber bereits im Kernel enthalten, ist die Installation der Integration Services schnell durchgeführt. Generell gehen Sie bei der Virtualisierung einer Linux-Maschine folgendermaßen vor: Die Konfigurations-Datei bearbeiten Sie mit dem Kommando # *sudo gedit /etc/initramfs-tools/modules*. In einem Editor Ihrer Wahl müssen Sie nun folgende Einträge / Module bei "initframes" hinzufügen (die erste Code-Zeile dient allein zur Information):

```
# Added for Hyper-V integration
hv_vmbus
hv_storvsc
hv_blkvsc
hv_netvsc
```

Danach aktivieren Sie mit dem Befehl # *sudo update-initramfs -u* die Module und führen mit *reboot* einen Neustart herbei. Für Red Hat und CentOS ab Version 6.x steht bereits eine neuere Version zur Verfügung, die Sie wie folgt installieren können: Mounten Sie dazu zunächst das ISO-Image *Linux IC v3.2.iso* der virtuellen Maschine. Die Installation selbst starten Sie dann mit folgendem Befehl:

```
# sudo mount /dev/cdrom /media/
# sudo /media/install.sh
# reboot
```

Erneut starten Sie mit **reboot** Linux neu durch. Mit **modinfo** überprüfen Sie sicherheitshalber, ob die erforderlichen Kernel-Module (hv_vmbus, hv_netvsc, hv_storvsc, hv_blkvsc und hv_utils) für Hyper-V geladen wurden. Noch eine Anmerkung zum Schluss für den Einsatz mit Hyper-V Failover Cluster: Linux-Gastsysteme, die Sie als High Available Virtual Machines (HAVM) konfigurieren, sollten Sie unbedingt mit einer statischen MAC-Adresse versehen. Da gewisse Linux-Versionen Probleme mit der dynamischen Zuweisung einer MAC-Adresse haben, verhindert dies, dass der Netzwerk-Zugriff nach einem Failover verloren geht. *(Michel Lüscher/ln)*

Server Talk

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

Nachdem wir auf einem Rechner mit **Windows Server 2003 SP1** mehrmals schnell hintereinander eine **externe USB-Festplatte** ab- und wieder angesteckt haben, funktioniert der entsprechende **USB-Port** nun plötzlich nicht mehr. Da der Anschluss zuvor tadellos funktioniert hat, schließen wir einen Hardware-Defekt aus. Was kann hier noch die Ursache sein?

Das von Ihnen beschriebene Problem ist sowohl unter Server 2003 als auch unter Windows XP bekannt. Aus irgendeinem Grund scheinen diese beiden Betriebssysteme Schwierigkeiten damit zu haben, wenn ein USB-Gerät mehrmals hintereinander entfernt und wieder angeschlossen wird. In so einem Fall wird der USB-Port deaktiviert und Sie müssen ihn manuell wieder aktivieren. Die einfachste Möglichkeit hierzu besteht über den Geräte-Manager, den Sie über das Startmenü und "Ausführen" mit dem Befehl *devmgmt.msc* starten. Klicken Sie hier mit rechts auf den Computer, so dass dieser markiert ist. Gehen Sie dann im Menü "Aktion" auf die Option "Nach geänderter Hardware suchen". Im besten Fall funktioniert der entsprechende USB-Port

schon nach diesem Scan-Durchlauf wieder. Ist dies nicht der Fall, probieren Sie es nach dem Suchdurchlauf doch noch einmal mit einem Neustart des Systems. Fruchtet auch dies nicht, bleibt nur, den USB-Controller neu zu installieren. Die dazu zunächst nötige Deinstallation funktioniert über den Gerätemanager. Navigieren Sie in der Auswahl-Liste zum Punkt "USB-Controller" und erweitern Sie diesen. Da leider keine Möglichkeit besteht, hier den richtigen Port zu identifizieren, müssen Sie über das Kontextmenü mit Hilfe des Befehls "Deinstallieren" alle hier aufgelisteten Controller kurzzeitig vom System werfen. Der nun durchzuführende Neustart sollte jedoch alle USB-Anschlüsse wieder aktivieren – auch denjenigen, der durch das mehrmalige An- und Abstecken von USB-Geräten seinen Dienst eingestellt hat. *(ln)*

Wir betreiben einen Windows **Server 2008 R2** als **Gastsystem unter VMware ESX**. Im Rahmen unserer Backup-Strategie wollen wir in regelmäßigen Zeitabständen eine **komplette Sicherung auf ein Netzlaufwerk** auf einem anderen Server anfertigen. Dieser **Kopiervorgang bricht jedoch ständig ab** mit der Fehlermeldung "Systemstatus: Der Vorgang wurde beendet. Detaillierter Fehler: Es steht nicht genug Speicherplatz auf dem Datenträger zur Verfügung". Auf dem Zielsystem ist mit einem halben TByte Kapazität jedoch mehr als genug Platz. Können Sie mir sagen, wie es zu dieser Problematik kommt?

Ihre Verwirrung hat damit zu tun, dass die von Ihnen beschriebene Fehlermeldung in einem Punkt leider nicht sehr präzise ist. Mit "dem Datenträger" ist nicht das Zielsystem gemeint, sondern die Ausgangsfestplatte. Deren Systempartition muss für das Erstellen von Schattenkopien eine gewisse Reserve vorweisen. Gerade bei virtuellen Servern fällt die eigentliche Systempartition jedoch äußerst knapp aus. Zudem ist zu beachten, dass die Systempartition meist in den Laufwerksbuchstaben C: und eine separate Partition ohne Laufwerksbuchstaben unterteilt ist, die die Bezeichnung "System-reserviert" trägt. Genau diese Teilpartition muss nun je nach ihrer Größe eine bestimmte freie Kapazität aufweisen – bei einer Partitionsgröße von bis zu 500 MByte etwa müssen mindestens 50 MByte frei sein. Die genauen Anforderungen lesen Sie auf der TechNet-Seite [Link-Code: C1PE4] nach. Wenn Ihre Systempartition diese Bedingungen nicht erfüllt, bleibt Ihnen also nur, die Systempartition zu vergrößern. Andernfalls ist es nicht möglich, Schattenkopien anzufertigen. *(ln)*

Linux

Neulich ist es uns passiert, dass ein Administrator versehentlich Dateien gelöscht hat, auf die er als regulärer Benutzer gar keinen Zugriff gehabt hätte. Mit einer **optisch anderen Darstellung des Login-Prompts** wäre für den Benutzer direkt sichtbar gewesen, dass er als Administrator und nicht als regulärer Benutzer angemeldet ist. Gibt es denn eine Möglichkeit, einen **root-Login auf einem Linux-Server** innerhalb einer SSH-Sitzung kenntlich zu machen?

Die Bash-Shell bietet die Möglichkeit, den Prompt, den ein Benutzer bei einem lokalen oder bei einem Netzwerk-Login sieht, individuell anzupassen. Wie dieser Prompt aussehen soll, ist in der Umgebungsvariablen PS1 hinterlegt. Mittels Escape-Zeichen besteht nun die Möglichkeit, den Prompt für den Benutzer root farblich anders zu gestalten – beispielsweise diesen in der Farbe Rot darzustellen. Dazu ist der folgende Eintrag in der Datei *~/.bashrc* im Heimatverzeichnis des Benutzers root auf dem Server notwendig:

```
export PS1="\[\033[1;31m\][\u@\h
  \w]\$ \[\033[0m\]"
```

Nach einem erneuten Login auf der entfernten Maschine leuchtet der Prompt für den Benutzer root nun in roter Farbe und ist damit deutlich von regulären Benutzer-Anmeldungen abgegrenzt. *(Thorsten Scherf/ln)*

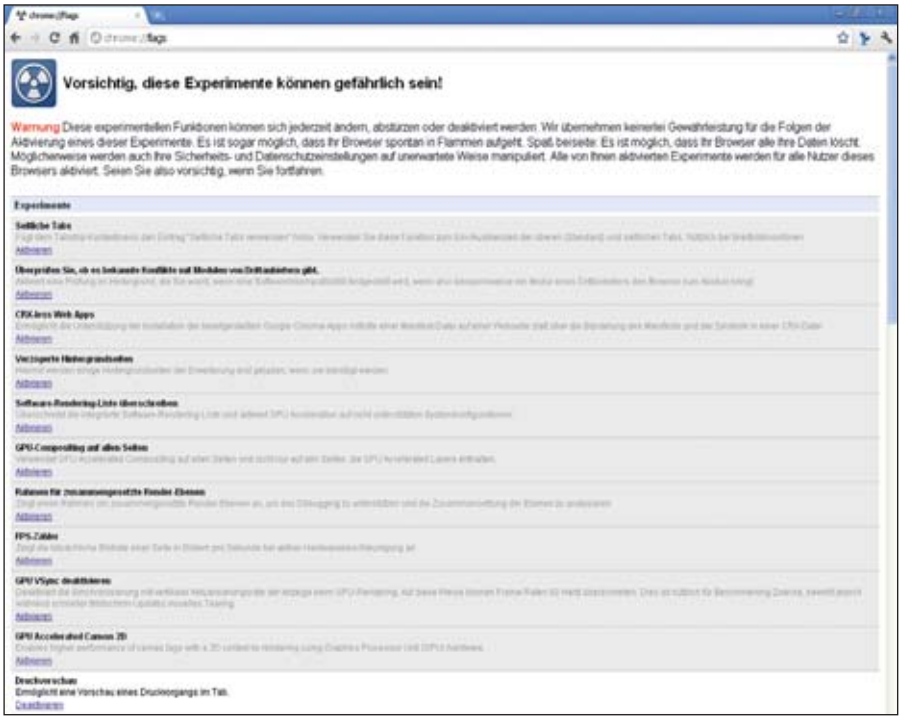
Citrix

Wir haben **Citrix VDI-in-a-Box 5.0** (ehemals Kaviza) im Einsatz. Hin und wieder erhalten wir die **Fehlermeldung "Could not find user"**. Wir sind eigentlich der Meinung, alles richtig konfiguriert zu haben. Haben Sie eine Idee, worauf die Fehlermeldung beruht und wie sich dieses Problem beheben lässt?

Vorausgesetzt, Sie haben VDI-in-a-Box korrekt mit dem Active Directory verbunden, hängt die Meldung sehr wahrscheinlich mit einer der folgenden Ursachen bei der Nutzer-Authentifizierung zusammen: Entweder gehört der Nutzer nicht zur "Sicherheitsgruppe" im Active Directory oder zu der in VDI-in-a-Box registrierten Gruppe. Außerdem muss sich der Nutzer in bestimmten Fällen mit dem User Principal Name (UPN)-Benutzerkonto (user@domain.com) einloggen und ordnungsgemäß authentifiziert werden. Loggen Sie sich also am besten zunächst ins Active Directory ein, um die Einstellungen des Nutzer-Accounts zu kontrollieren. Wählen Sie dazu unter "Eigenschaften/Properties" den Reiter "Account" aus und überprüfen Sie dort das Domain-Suffix. Dieser ist im rechten oberen Eingabefeld des Fensters zu finden. Ist der Adressbestandteil hier mit der unter dem Menüpunkt "Configure User Database" hinterlegten DNS-Domain identisch, so können sich Nutzer direkt mit ihrem Active Directory-Benutzernamen einloggen. Stimmen das angegebene Suffix und die DNS-Domain hingegen nicht miteinander überein, müssen Endanwender zur Anmeldung ihren vollen UPN-Kontonamen verwenden (zum Beispiel testupn@sv.demo-kaviza.com). Je nachdem, wie der Account im Active Directory angelegt wurde, sollten Sie versuchen, sich jeweils mit oder ohne UPN-Namen einzuloggen, um herauszufinden, ob der VDI-in-a-Box-Manager das betreffende Konto finden kann. Registrieren Sie den User dort testweise, um zu überprüfen, ob er sich erfolgreich individuell anlegen lässt. *(Citrix/ln)*

Google Chrome

Ich habe bisher hauptsächlich mit **Mozilla Firefox** als Webbrowser gearbeitet. Praktisch fand ich dabei, über die Eingabe von **"about:"-Befeh-**



Über die Eingabe von *chrome://flags* rufen Sie in Google Chrome experimentelle Funktionen wie eine praktische seitliche Tab-Leiste auf

len in der Adresszeile erweiterte Einstellungen vornehmen und diverse Systeminformationen sowie Statistiken auslesen zu können. Da ich in letzter Zeit vermehrt mit Google Chrome arbeite, würde mich interessieren, ob es derartige Befehle auch für diesen Browser gibt?

Wie Sie wahrscheinlich schon vermuten, hat auch Google seinen Internet-Browser mit versteckten Befehlen ausgestattet. In der aktuellen Version lassen sich diese Kommandos allerdings nicht mehr mit dem Prefix *about:* aufrufen. Stattdessen müssen Sie der gewünschten Funktion in der Adresszeile *chrome://* voranstellen. Die Eingabe von *chrome://about* listet zunächst einmal eine Übersicht über alle erweiterten Befehle auf, die Sie dann bequem über einen Link anklicken können. Mit den beiden Kommandos *chrome://cache* und *chrome://history* informieren Sie sich etwa sehr schnell über sämtliche im Cache abgelegten oder die besuchten Webseiten. *chrome://dns* bringt die zwischengespeicherten DNS-Einträge auf den Schirm. Mit *chrome://crashes/* lassen Sie sich nähere Informationen zu den letzten Abstürzen des Browsers anzeigen – allerdings muss dazu die Absturzberichtsfunktion aktiviert sein. Eine Vielzahl experimenteller Funktionen rufen Sie – laut Google ohne Gewähr – über die Eingabe von *chrome://flags* auf. Hier können Sie den Browser so einrichten, dass die Tabs seitlich und nicht waagrecht am oberen Bildschirmrand angezeigt werden. Auch die Möglichkeit einer Druckvorschau in einem extra Tab oder die Funktion, auf Knopfdruck zwischen mehreren Chrome-Profilen zu wechseln, könnte für einige Nutzer durchaus interessant sein. Wer genau wissen will, wie viel Arbeitsspeicher der Browser verbraucht, tipp teinfach *chrome://memory* ein. Dies ist besonders interessant, wenn Sie zusätzlich einen Konkurrenz-Browser geöffnet haben – dann werden die Werte nämlich verglichen. *(ln)*

Tools

Eine funktionierende und stets aktuelle **Inventarisierung** der IT-Assets des Unternehmens stellt schon für kleine Betriebe eine wichtig Basis für den störungsfreien Betrieb und auch die Kostenrechnung der IT dar. Doch oft bieten Inventarisierungswerkzeuge nur wenige Möglichkeiten, **direkte Aktionen auf einem oder einer Gruppe von Rechnern auszulösen**. Hier sind dann oft kostspiele System-Management-Suiten vonnöten.

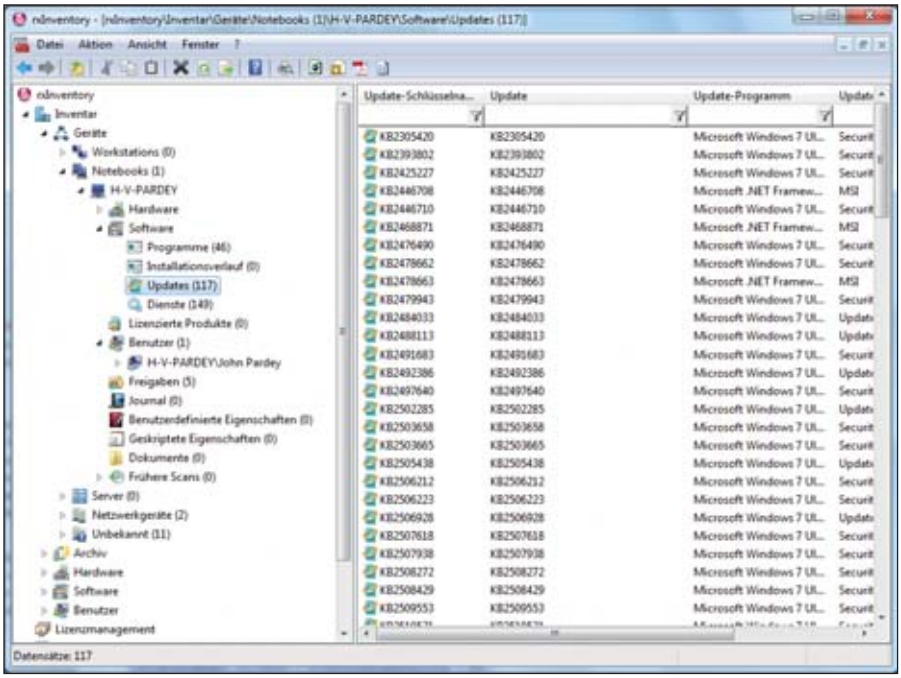
Mit der neuen Version 2.1 des **Advanced IP Scanner** bietet Hersteller Radmin nun einen kostenlosen **Netzwerkscanner**, der einerseits eine komplette oder individuell festgelegte Inventarisierung in Windeseile ermöglicht, andererseits dem Administrator **weitreichende Verwaltungsmöglichkeiten** auf Windows-Rechnern bietet. Mit Advanced IP Scanner 2.1 lassen sich hunderte von IP-Adressen gleichzeitig mit hoher Geschwindigkeit scannen. Die Software unterstützt das Scannen von HTTP, HTTPS, FTP und Ordnerfreigaben. Darüber hinaus lassen sich weiterführende Informationen über angeschlossene Geräte, beispielsweise Computernamen und MAC-Adressen, ermitteln. Über "Remote-PC-Shutdown" lassen sich einzelne Remote-Computer oder eine Gruppe von Computern mit Windows-Betriebssystem aus der Ferne herunterfahren. Dabei nutzt der IT-Verantwortliche die Standardzugriffsrechte oder er hinterlegt einen Anmeldenamen mit Kennwort zum Herunterfahren. Auf der anderen Seite unterstützt das Tool Wake-On-LAN und erlaubt so, Einzelplatzcomputer oder Gruppen von Remote-Computern hochzufahren (sofern die Netzwerkkarten Wake-on-LAN unterstützen). Advanced IP Scanner hat eine einfache, aber benutzerfreundliche Oberfläche. Zur Vereinfachung von Batchvorgängen lassen sich Gruppen zu scannender Computer in Favoritenlisten speichern. Beim Start lädt das Werkzeug automatisch die Favoriten und anschließend lässt sich auswählen, ob das gesamte Netzwerk oder nur die Computer der Favoritenliste gescannt werden sollen. Unterstützte Betriebssysteme sind Windows 2000/XP/2003/Vista/2008 und Windows 7 (32 und 64 Bit). *(jp)*

Link-Code:C1PE1

Wie schon bei unserem ersten Tool in diesem Monat erwähnt, stellt die **Inventarisierung** einen wichtigen Baustein des IT-Managements dar. Doch gerade sehr kleine Unternehmen scheuen entsprechende Investitionen und inventarisieren per Excel-Liste. Dabei stehen heutzutage kostenlose Werkzeuge zur Verfügung, die neben der reinen Inventarverwaltung beispielsweise auch das Lizenzmanagement abdecken.

Ein Vertreter dieser Klasse kostenloser Inventarisierungs-Tools ist **rxInventory**. Dieses Werkzeug ist bis zur Verwaltung von 20 Clients kostenlos und skaliert

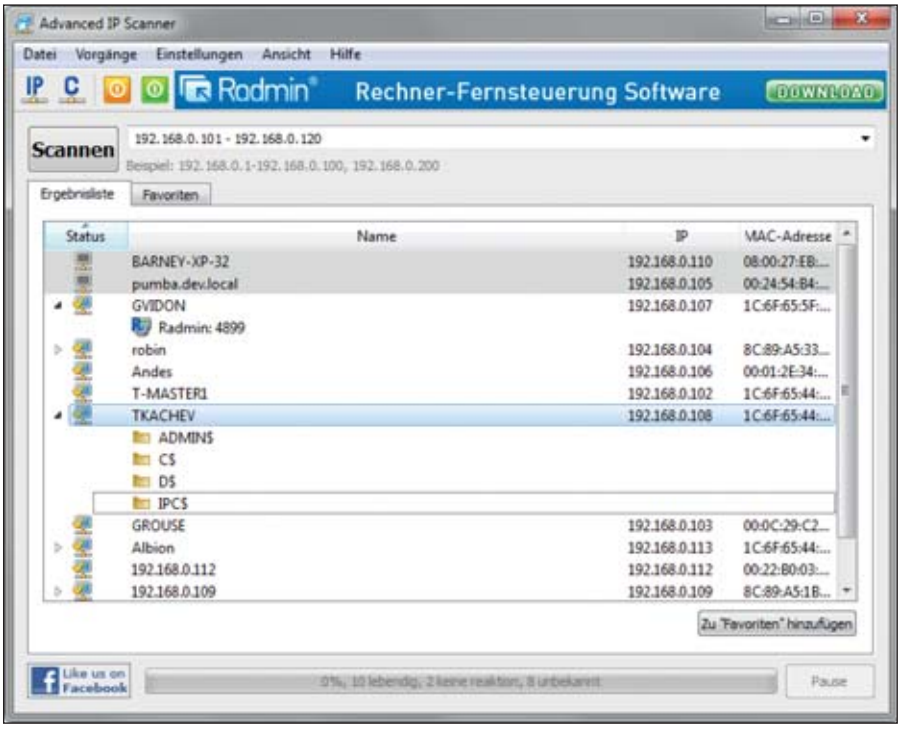
nach Herstellerangaben von kleinen Netzwerken bis zu Installationen mit einigen zehntausend Clients (hier dann selbstverständlich nur mit einer kostenpflichtigen Lizenz). Zur Datensammlung unterstützt rxInventory die wichtigsten SQL-Datenbanken (MS-JET beziehungsweise Microsoft Access, Microsoft SQL Server, Oracle Database, MySQL und PostgreSQL). Auch lassen sich die Daten jederzeit innerhalb der rxInventory-Konsole zwischen verschiedenen Datenbanktypen migrieren. Darüber hinaus bietet das Tool eine mächtige Oberfläche zum Entwurf von eigenen Abfragen. Dies ermöglicht Analysen über fast jeden Aspekt der Inventurdaten. Die Ergebnislisten lassen sich durch einfaches Cut & Paste in andere Programme übernehmen. Gleichzeitig stellt rxInventory eine stets aktuelle Auswertung zur Lizenzsituation im Unternehmen zur Verfügung. Innerhalb des integrierten Lizenzmanagements können ermittelte Programmpakete mittels definierbarer Regeln zu Produkten gruppiert werden. Lizenzinformationen über Zugänge, Abgänge, Kaufdatum, Gültigkeit und Preis werden anschließend als Lizenzpacks auf Produktebene zugeordnet. Die resultierende Reserve zeigt Über- und Unterlizenzierung zuverlässig an. Zusätzlich



Mit rxInventory ist es unter anderem möglich zu prüfen, ob der Zielrechner über alle notwendigen Updates verfügt

speichert das Tool alle Veränderungen an Hardware und Software. Selbst nach Jahren lässt sich feststellen, durch wen und wann eine Veränderung stattgefunden hat. Es ist nicht notwendig, Agenten auf den Clients zu installieren. rxInventory verwendet verschiedene Standardprotokolle, um Computer und andere Geräte im Netzwerk zu erfassen. Die Scans lassen sich zeitlich geplant und im Hintergrund durchführen. Auch Linux- und Mac OS X-Systeme erfassen Administratoren mit dem Inventarisierungswerkzeug. rxInventory meldet sich mit dem SSH-Protokoll an Linux- und Apple Mac-Rechnern an und ermittelt eine vollständige Übersicht über die Hardware und Software, indem es vorhandene Betriebssystembefehle absetzt. Für individuelle Anpassungen bringt rxInventory eine Visual Basic-ähnliche Skriptsprache zur Ermittlung von selbstdefinierten Registry-Werten und Dateiinformationen mit. Selbst beliebige WMI- und SNMP-Anfragen sind möglich und werden in den Ergebnissen als zusätzliche Geräteeigenschaften angezeigt. *(jp)*

Link-Code:C1PE3



Der Advanced IP Scanner in der neu veröffentlichten Version 2.1 erlaubt unter anderem den direkten Durchgriff auf Shares von Client-Computern

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

Die acht Gebote des Datenschutzes: Zugriffskontrolle (2)

Du sollst nicht begehren Deines Nächsten Server

von Giovanni Brugugnone

Bei einem genauen Blick in die Unternehmen kommen häufig eklatante Verstöße gegen den Datenschutz zu Tage. Im ersten Teil unserer Artikelserie haben wir uns mit den Anforderungen der Zutrittskontrolle befasst, die den physischen Zutritt zu Datenverarbeitungsanlagen regelt. Im zweiten Teil betrachten wir die Gebote der Zugriffskontrolle im Bereich Identifikation und Authentifizierung gegenüber EDV-Systemen.

Im Rahmen der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ist durch eine funktionierende Zugangskontrolle zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies verlangt das Bundesdatenschutzgesetz (BDSG) in Nr. 2 der Anlage zu § 9 Satz 1. Die Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, fällt hingegen in den Regelungsbereich der Zugriffskontrolle – Nr.3 der Anlage zu § 9 Satz 1 BDSG.

Das 2. Gebot: Zugangskontrolle für EDV-Systeme

Unbefugten ist der Zugang zu EDV-Systemen zu verwehren. Im Gegensatz zur Zutrittskontrolle geht es hier nicht um den physischen Zutritt zu, sondern um das Eindringen in beziehungsweise die Nutzung von EDV-Systemen durch unbefugte Personen. Hierbei ist im Rahmen der Authentifizierung zwischen "internen" und "externen" Mitarbeitern sowie dem Schutz der entsprechenden Zugänge zu unterscheiden.

IT-Dienstleister – offene Ports als Achillesferse

Grundsätzlich sollten Sie Remote-Zugänge zu Datenbanken äußerst restriktiv handhaben. Ist ein solcher Remote-Zugriff nicht zwingend notwendig, so ist dieser zu unterbinden. Oftmals mangelt es in Unternehmen auch an klaren Prozessen, wie sich Wartungsmitarbeiter von IT-Dienstleistern bei Remote-Zugriffen authentifizieren, welche Mindestverschlüsselung für bestehende Zugänge verwendet und wie durchgeführte Arbeiten protokolliert werden.

Soweit erforderlich, öffnen Sie Wartungszugänge und die entsprechenden Ports nur bei Bedarf sowie nach erfolgreicher Authentifizierung und schließen Sie diese nach Abschluss der Wartungsarbeiten wieder. Dadurch verhindern Sie, dass nach außen hin offene Verbindungen bestehen bleiben, die zwar nur zeitweise benötigt werden, aber dauerhaft ein erhebliches Sicherheitsrisiko für die IT darstellen. Für besonders sicherheitsrelevante Systeme können auch getrennte Netzbereiche oder sogar Stand-Alone-Systeme, also vom Netzwerk komplett losgelöste Systeme, sinnvoll sein.

Zudem ist in Zeiten steigender Industriespionage auch für mittelständische Betriebe die Nutzung von Intrusion Detection- und Prevention-Systemen sinnvoll, um verdächtige Netzwerkaktivitäten zu identifizieren und automatisch entsprechende Gegenmaßnahmen zu treffen. Dadurch werden nicht nur personenbezogene Daten, sondern auch die Unternehmensinterna geschützt.

Kombination aus Passwort und Token

Soweit Unternehmen erhöhte Sicherheitsanforderungen an Zugangskontrollen stellen, ist zu prüfen, ob Zugänge über eine klassische Authentifizierung mit Benutzername und Passwort (Merkmal: Wissen) genügen oder darüber hinaus nicht auch der Einsatz von Chipkarten oder Token (Merkmal: Besitz) sinnvoll ist. Denn eine solche Kombination der Merkmale Besitz und Wissen gewährleistet meist einen erhöhten Schutz für Zugänge. Hierbei sollten Sie beachten, dass die Ausgabe und der Entzug von Logins sowie Token dokumentiert und Regelungen zum Umgang mit Passwörtern und Zugangsmitteln (Chipkarte, Token) getroffen werden müssen.

Daneben sind soweit umsetzbar technische Passwortvorgaben einzuführen.

Hierzu zählen Passwortmindestlänge, Passwortkomplexität, Zwangswechsel für Passwörter nach beispielsweise 90 Tagen sowie eine Passworthistorie. Nähere Informationen hierzu liefert Punkt M 2.11 in den BSI IT-Grundschutz-Katalogen [1]. Weitere mögliche Maßnahmen sind

- Authentifizierung von Nutzern über Zertifikate
- Sperrung von Nutzerkonten nach dreimaliger Falscheingabe samt genutzter IP-Adresse (bei Wartungszugängen)
- Protokollierung von Zugriffen beziehungsweise Zugriffsversuchen und deren regelmäßige Auswertung
- Netzwerkseitig ist zu unterbinden, dass sich eine Benutzerkennung mehrmals im Netzwerk anmelden kann
- Nutzung von Antivirensoftware auf Clients und regelmäßige Aktualisierung
- Nutzung von Firewalls
- Bootschutz über externe Schnittstellen (CD/DVD-Laufwerke oder USB-Ports)
- Nutzung sicherer Übertragungstechniken (etwa IPSEC)

Bei der Zugangskontrolle ist neben der Einbindung der IT im Onboarding-Prozess insbesondere auch ein funktionierender Offboarding-Prozess erforderlich, um eine zeitnahe Deaktivierung externer Zugänge zu gewährleisten. Immer wieder finden sich in Unternehmen offene VPN-Zugänge ausgeschiedener Mitarbeiter, was ein erhebliches Sicherheitsrisiko darstellt. Auch seit Jahren ungenutzte, aber weiterhin aktive Wählzugänge sind in vielen Unternehmen in Vergessenheit geraten und deshalb ist auch an deren Sperrung zu denken. Grundsätzlich ist überdies empfehlenswert, ungenutzte Zugänge nach sechsmonatiger Inaktivität "präventiv" zu sperren.

Das 3. Gebot: Zugriffskontrolle durch Berechtigungskonzept

Im Gegensatz zur Zugangskontrolle, die nur zwischen befugten und unbefugten Personen unterscheidet, regelt die Zugriffskontrolle, dass grundsätzlich befugte Nutzer von EDV-Systemen nur auf Daten im Rahmen ihrer Befugnisse zugreifen können. Weiterhin soll hierdurch das unbefugte Lesen, Kopieren, Ändern oder Löschen personenbezogener Daten verhindert werden. Allgemeine Zielrichtung ist somit die Verhinderung unberechtigter Datenzugriffe. Hierzu sind sowohl technische als auch organisatorische Maßnahmen erforderlich.

Need-to-know-Prinzip und Vertreterregelung

Durch die Erstellung eines umfassenden Berechtigungskonzeptes legen Sie neben allgemeinen Zugriffsberechtigungen auch genau fest, wer bestimmte Daten lesen, ändern, löschen oder versenden darf. Hierzu prüfen Sie in einem ersten Schritt genau, welche Daten einzelne Mitarbeiter für ihre tägliche Arbeit benötigen. Im Anschluss erteilen Sie Zugriffsberechtigungen gemäß dem Need-to-know-Prinzip nur für diese Daten (siehe BSI IT-Grundschutz-Kataloge, Punkt M 2.8: Vergabe von Zugriffsrechten) [2]. Hierzu bietet es sich an, die jeweiligen Stellen- und Funktionsbeschreibungen heranzuziehen, um bereits frühzeitig die Berechtigungen auf einzelne Bereiche oder Abteilungen wie Controlling oder Personal zu beschränken. Sodann vergeben Sie innerhalb der jeweils vorhandenen Daten gemäß dem Need-to-know-Prinzip die Zugriffsberechtigungen. Keinesfalls dürfen hierbei Berechtigungen nur aufgrund einer gewissen Hierarchiestufe vergeben werden. Das auf dieser Grundlage erstellte Berechtigungskonzept sollte zusätzlich klare Vorgaben zur Vertreterregelung enthalten. In einem zweiten Schritt sind weitergehende Berechtigungen zu definieren und etwa zwischen Lese- und Schreibrechten zu unterscheiden. Insbesondere ist auch zu gewährleisten, dass Daten nicht unbefugt gelöscht werden können.

Regelung zur Rechtevergabe

Es sind Vorgaben zu Beantragung, Änderung und Entzug von Berechtigungen festzulegen. Eine Freischaltung quasi auf Zuruf, wie in vielen Unternehmen üblich, gilt es zu unterbinden. Darüber hinaus muss die zentrale Rechtevergabe samt Vertreterregelung in der IT-Abteilung angesiedelt und klar geregelt werden. Insbesondere bei Abteilungswechsel müssen Sie darauf achten, dass neben der Einrichtung "neuer" Berechtigungen auch die nicht mehr benötigten Berechtigungen entzogen werden, denn nicht selten verfügen übernommene Azubis über Zugriffsberechtigungen für beispielsweise eine Vielzahl von SAP-Modulen. Weitere mögliche Maßnahmen sind

- ein interner Prozess zur kontrollierten Vernichtung von Fehldrucken vertraulicher Dokumente etwa über sogenannte Datentonnen
- die mechanische Zerstörung entsorgter Festplatten samt Protokollierung des Zerstörungsvorgangs
- die Verschlüsselung von Laptop- und USB-Datenträgern. Der Zugriff auf ungeschützte Laptops oder mobile Speichermedien ist nicht kontrollierbar.
- die Sperrung externer Schnittstellen zur Verhinderung unautorisierter Zugriffe durch Booten des Rechners über USB-Stick und zur Verhinderung von Datenkopien (auch eine Maßnahme der Zugangskontrolle).
- Nutzung von Thin Clients, soweit keine vollwertigen Client-Rechner benötigt werden.

Fazit

Die gesetzlich geforderten technischen und organisatorischen Maßnahmen der Zugangs- und Zugriffskontrolle dienen – wie die übrigen TOMs – dem Schutz personenbezogener Daten. Für Unternehmen ergeben sich bei ordnungsgemäßer Umsetzung dieser Vorgaben indes neben dem Aspekt der Datenschutz-Compliance weitergehende Vorteile wie etwa der erhöhte Schutz unternehmenskritischer Informationen und des internen Know-hows. Somit kommen einzelne Maßnahmen der Datenschutz-Compliance nicht nur dem Schutz personenbezogener Daten zugute, sondern vielmehr wird hierdurch die gesamte Datensicherheit in Unternehmen erhöht und damit auch deren Wettbewerbsfähigkeit gesichert. *(dr)*

Giovanni Brugugnone ist Rechtsanwalt und Consultant Datenschutz und IT-Compliance bei der intersoft consulting services AG.

[1] BSI-Grundschutzkatalog zu Passwortkomplexität
C1W11

[2] BSI-Grundschutzkatalog zu Zugriffsrechten
C1W12

Link-Codes

Vorteile automatisierter Anwendungsvirtualisierung

Paketzusteller

von Steve Schmidt

Durch den Wandel vom PC zur Cloud gewinnt die Desktop-Virtualisierung zunehmend an Popularität. Die Verbreitung neuer und verschiedener Kundengeräte und der Bedarf der Anwender an Mobilität beschleunigen diese Entwicklung zusätzlich. Virtualisierte und voneinander getrennte Ressourcen (Betriebssystem, Anwendungen, Benutzerdaten und -einstellungen) bieten gegenüber dem Desktopmodell den Vorteil, dass alle Schichten unabhängig voneinander verwaltet und gegebenenfalls an den erforderlichen Stellen in Verbindung mit zahlreichen Technologien eingesetzt werden können.

Das Desktop Computing-Modell verändert sich zusehends durch die Bereitstellung neuer Betriebssysteme in Kombination mit Virtualisierungstechnologien. Die Anwendungsvirtualisierung ermöglicht eine schnellere Bereitstellung, besseren Support und mehr Flexibilität und reduziert den Aufwand beim Implementieren neuer Technologien. Organisationen stehen damit vor der Herausforderung, aus Hunderten oder Tausenden von Anwendungen mit unterschiedlichen Formaten Pakete erstellen zu müssen, die kompatibel sind mit herkömmlichen Desktops oder Desktopvirtualisierungstechnologien wie VDI und sessionbasierten Technologien, die Thin Clients, Tablets, Smartphones, nicht verwaltete Geräte oder Nicht-Windows-Geräte unterstützen. Zahlreiche IT-Abteilungen stellen inzwischen Windows 7 in der 64 Bit-Version sowie Webbrowser-Updates bereit, erstellen VDI-Infrastrukturen und optimieren ihre Sitzungsvirtualisierungs-Lösungen. Jede dieser Lösungen erfordert jedoch das Testen, Korrigieren und Optimieren von Anwendungen für jede Technologie.

Die Anwendungsvirtualisierung bietet einen Ansatz, der all diese Szenarien mit wenigen Einschränkungen ermöglicht. Sie bietet separate Tools zum Erstellen von Paketen, erfordert aber auch fundierte Applikationskenntnisse. Da vorhandene Anwendungen nicht in virtualisierter Form verfügbar sind, muss jede Anwendung einzeln in ein neues Format paketiert werden. Müssen die hierfür verantwortlichen Administratoren ein neues Tool erlernen, verringert dies die Produktivität entscheidend für die aktuelle Verwaltung eines Anwendungskatalogs. Schließlich sind Katalogveränderungen von 30 Prozent jährlich durchaus wahrscheinlich. Die Anwendungsvirtualisierung unterstützt zudem nicht alle Anwendungen. Daher ist zusätzliche Arbeit erforderlich, um Anwendungen herkömmlich zu paketieren, wenn diese nicht kompatibel sind.

Doch dank automatischer Anwendungsvirtualisierung können Unternehmen ihre aktuellen Ressourcen für die Anwendungspaketierung und ihre Vorarbeit nutzen, um die Paketierung mit nur einem Tool und in nur einem Prozess für jedes erforderliche Format wie Microsoft App-V, VMware Thin App und Citrix XenApp zu automatisieren. Die automatische Anwendungsvirtualisierung validiert kompatible Anwendungen und konvertiert diese Anwendungen gebündelt in virtuelle Anwendungspakete. Die weiteren Paketierungsarbeiten kann der IT-Administrator dann bei Anwendungen durchführen, die mit der Anwendungsvirtualisierung zwar kompatibel sind, aber zusätzlich konfiguriert werden müssen.

Der erste Schritt ist also die Repaketierung von Anwendungen in einem Standardformat (MSI). Als Nächstes werden die Anwendungen hinsichtlich ihrer Kompatibilität mit Betriebssystem und Webbrowser korrigiert und abschließend kompatible Anwendungen automatisch konvertiert. Während dieses Prozesses erhalten IT-Verantwortliche laufend Hinweise zur Fehlerbehebung für herkömmliche und virtuelle Anwendungen.

Schritte zur automatischen Anwendungsvirtualisierung

Die Automatisierung der Anwendungsvirtualisierung ist ein laufender IT-Prozess, der nicht mit der anfänglichen Konvertierung abgeschlossen ist. In einer Organisation, die 2.000 Anwendungen in ein Virtualisierungsformat konvertiert, werden durchschnittlich 600 Anwendungen jährlich aktualisiert. Zusätzlich kommt neue Software hinzu. Aufgrund der Menge neuer Programme sowie Updates für vorhandene Software kommen Organisationen heute kaum noch mit dem Paketieren von Anwendungen hinterher. Hinzu kommen noch IT-Projekte

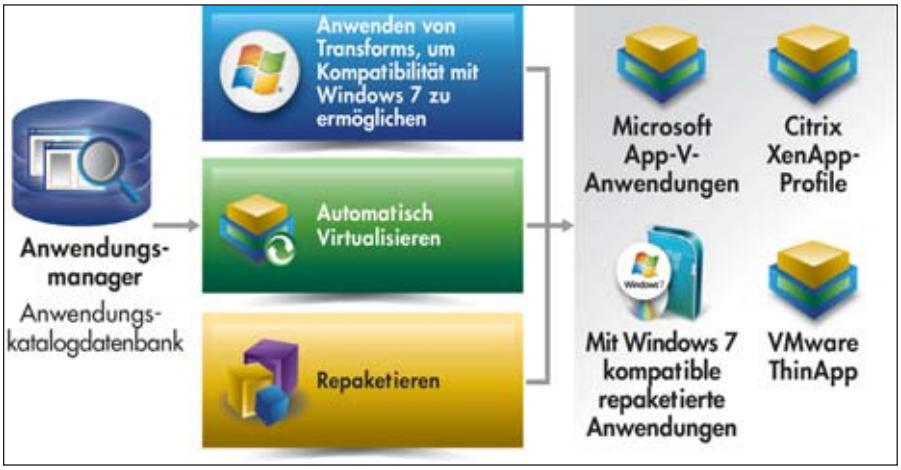


Bild 1: Der Anwendungsmanager ermöglicht es, Applikationen für virtuelle Desktop-Umgebungen vorzubereiten

und Initiativen, die neue Paketformate und Ausgabeendpunkte für Tests erfordern. Pakete müssen heutzutage auf herkömmlichen Desktops, virtuellen Desktops und sessionbasierten Lösungen (Remote-Desktop-Services und Citrix) funktionieren, um den Benutzerzugriff mit jedem Gerät zu unterstützen.

Im Fokus von Projekten zur Anwendungsvirtualisierung sollte der Wechsel vom reaktiven zum proaktiven Ansatz beim aktuellen Anwendungsmanagement stehen. Ziel der automatisierten Application Readiness ist es, aus Software jeglicher Quelle konsistente Pakete in verschiedenen Formaten zu erzeugen, um sie auf jedem Gerät bereitstellen zu können. Das gibt Administratoren mehr Flexibilität in Form von Software, die in einem für das nächste Projekt kompatiblen Format paketiert ist, da das Paketierungsteam die Dateien bereits erstellt und der Anwendungsbibliothek hinzugefügt hat. Für den Übergang einer Ad-hoc-Anwendungspaketierung zu einem wiederholbaren, konsistenten Prozess ist eine umfassendere Betrachtung des Prozesses erforderlich. Bild 2 zeigt die sechs Schritte, die zur Application Readiness führen.

1. Identifizieren

Im ersten Schritt gilt es, alle Anwendungen genau zu erfassen, die in der Organisation bereitgestellt sind, damit sich der Aufwand zur Fertigstellung des Projekts abschätzen lässt. Da die Vorteile der Anwendungsvirtualisierung mit der Anzahl an virtuellen Applikationen zunehmen, ist dies ein guter Zeitpunkt, um den aktuellen Anwendungsbestand zu erfassen und die Programme zu identifizieren, die nicht mehr verwendet werden. Außerdem erfolgt die Anwendungsvirtualisierung oft im Rahmen der Bereitstellung eines Betriebssystems, weshalb sich die gewonnenen Informationen für beide Zwecke verwenden lassen. Die meisten Anwendungen lassen sich virtualisieren, aber manche müssen auf herkömmliche Weise installiert werden. Daher ist es am besten, zunächst den genauen Bestand der Anwendungen zu kennen.

2. Optimieren

Im nächsten Schritt zur automatisierten Anwendungsvirtualisierung wird festgestellt, welche Anwendungen des Anwendungsbestands tatsächlich notwendig sind. Viele Organisationen verwenden seit Jahren dasselbe Betriebssystem und ihre Anwendungskataloge enthalten mehrere Versionen derselben Applikation, nicht verwendete Anwendungen und verschiedene Anwendungen, die nebeneinander installiert wurden und dieselben Aufgaben erfüllen. Durch die Konsolidierung dieser Anwendungen können Organisationen die Menge der Software reduzieren, die an das neue Betriebssystem angepasst und für die Anwendungsvirtualisierung konvertiert werden muss, und Kostenaufwand und Ausgaben für die Verwaltung doppelter und multipler Versionen derselben Software senken.

3. Kompatibilität bewerten

Die Optimierung der Anwendungen liefert eine Liste für die Konvertierung in Virtualisierungspakete, aber die Anwendungsvirtualisierung garantiert keine Kompatibilität zwischen Anwendung und Betriebssystem. Vor der Virtualisierung müssen Anwendungen nach wie vor auf Kompatibilität getestet werden. Normalerweise sind nur 30 bis 50 Prozent der Anwendungen, die auf Windows XP laufen, ohne vorherige Modifizierung mit Windows 7 kompatibel. Es ist schwierig und zeitaufwendig, jede Anwendung unter Windows 7 manuell zu installieren und alle Funktionen dieser Anwendung zu testen, um sicherzustellen, dass sie funktionieren. Viele Programme funktionieren unter Umständen beim ersten Test durch einen IT-Experten.

Wenn aber ein Unternehmensanwender diese Funktionen verwendet, kann es jedoch zu Kompatibilitätsproblemen kommen, die ein unvorhersehbares Anwendungsverhalten zur Folge haben können. Der kombinierte Einsatz von Kompatibilitätstools wie dem Application Compatibility Toolkit von Microsoft und AdminStudio Application Compatibility Pack von Flexera Software ermöglicht Organisationen die Identifikation von Anwendungen, die korrigiert werden müssen, um mit Windows 7 kompatibel zu sein, oder die nicht korrigierbar sind und ersetzt oder aktualisiert werden müssen.

Beim Start eines Anwendungsvirtualisierungsprojekts müssen IT-Verantwortliche also die Kompatibilität mit Windows 7 bewerten und erkennen, welche Anwendungen mit spezifischen Virtualisierungstechnologien kompatibel sind. Alle Virtualisierungslösungen beinhalten spezifische Angaben zu Inkompatibilitäten, die aber nur mit sehr umfangreichen Kenntnissen der Anwendungen ausgewertet werden können. Anwendungshersteller stellen möglicherweise Informationen zur Fehlerbehebung bei Anwendungen zur Verfügung, die mit dem bereitgestellten Paketierungstool nicht kompatibel sind. Diese Leitfäden bieten jedoch oft nur begrenzte Hilfe. Durch den Mangel an substanziellen Informationen wird der Paketierungsprozess der Anwendungen in ein virtualisiertes Format oft verzögert oder angehalten. Die automatisierte Virtualisierungstechnolo-

gie liefert hingegen Informationen darüber, welche Anwendungen nach der Virtualisierung laufen sowie Informationen zu bekannten Problemen und Anleitungen zur Anwendungskorrektur. Diese Informationen zur Fehlerbehebung können den zeitlichen Aufwand erheblich verringern, den Arbeitsaufwand für inkompatible Software beseitigen und helfen, bekannte Probleme schneller zu beheben.

4. Planen

Viele Organisationen verfügen bei der Planung und Budgetierung von Projekten nicht über ausreichende Informationen. Da Kompatibilitätstests und die Paketierung von Anwendungen kostenintensive und zeitaufwendige Komponenten eines Anwendungsvirtualisierungsprojekts darstellen, liefert eine detaillierte Übersicht der zu migrierenden Anwendungen und deren Application Readiness für anwendungsabhängige Projekte Informationen für die Budget- und Ressourcenzuweisung. Der Arbeitsaufwand der Phasen "Optimieren" und "Kompatibilität bewerten" liefert eine Liste rationalisierter Anwendungen und Details zu Kompatibilitätsproblemen, die behoben werden müssen. Mithilfe dieser Informationen können Administratoren den Umfang des Projekts realistisch einschätzen und den finanziellen und voraussichtlichen Zeitaufwand genau berechnen.

5. Fehler beheben und Paketierung

Anwendungen, die in der Phase "Kompatibilität bewerten" Probleme verursacht haben, müssen vor der Bereitstellung unter Windows 7 korrigiert oder ersetzt werden. Die manuelle Recherche oder Korrektur von Anwendungen liefert meist unterschiedliche Ergebnisse und erfordert dedizierte und hochqualifizierte Ressourcen. Die automatisierte Behebung von Kompatibilitätsproblemen sollte standardbasierte MSIs für die herkömmliche Bereitstellung erzeugen. Organisationen, die eine Anwendungsvirtualisierung im Rahmen einer Desktoptransformation durchführen, können virtualisierte Anwendungspakete aus korrigierten Installationen erstellen oder diese automatisch in eine spezifische Anwendungsvirtualisierungstechnologie konvertieren lassen wie etwa Microsoft App-V, VMware ThinApp und Citrix XenApp. All dies kann im Rahmen der Phase "Fehler beheben und Paketierung" bei Produkten wie AdminStudio von Flexera Software passieren. Dieses Produkt vereinfacht die Anwendungsvirtualisierung, indem es in einem einzigen Prozess ohne zusätzliche Tools sowohl herkömmliche (MSI) als auch virtualisierte Pakete erzeugt.

6. Bereitstellen

Bei der automatisierten Anwendungsvirtualisierung werden die erzeugten Pakete automatisch der elektronischen Softwarebereitstellung (ESD) hinzugefügt, ohne zusätzliche Kopien von Dateien und manuelle Übergaben. Eine automatisierte Lösung kann Pakete an praktisch jede Bereitstellungslösung übergeben, einschließlich Microsoft System Center Configuration Manager, LANDesk Management Suite, Novell Zenworks und andere. Dadurch hat der Administrator die Möglichkeit, einfach ein Paket aus dem Katalog auszuwählen und es auf den entsprechenden Zielgeräten bereitzustellen. Da die meisten manuellen Prozesse beseitigt wurden, um potenzielle Fehlerquellen zu beseitigen, kann der Bereitstellungsspezialist davon ausgehen, ein einheitliches und tragfähiges Paket geliefert zu haben.

Bild 2: Das Prozessmanagement umfasst die Schritte von der Identifizierung der Anwendungen hin zur Bereitstellung

Die letzte wichtige Komponente der automatisierten Anwendungsvirtualisierung ist die Erfassung der Tracking- und Trending-Informationen. Paketierungsabteilungen wissen nicht immer, wie viele Pakete in einem bestimmten Zeitraum erzeugt werden. Daher können sie die Ressourcen und den Aufwand, die erforderlich sind, um auf neue Technologien umzurüsten, die Application Readiness erfordern, nur ungenau einschätzen. Workflow-Verwaltung und Berichterstellung sind daher wichtige Komponenten eines vollständigen Application Readiness-Prozesses.

Fazit

Die automatisierte Anwendungsvirtualisierung bereitet Applikationen auf die Nutzung neuer Desktop-Technologien vor. Dieser Prozess ermöglicht, alle Anwendungsformate zu bearbeiten, entsprechend den Kompatibilitätsanforderungen zu korrigieren, für die Anwendungsvirtualisierung auszuwerten und konsistente Pakete in jedem erforderlichen Format von MSI bis hin zu Anwendungsvirtualisierungsformaten zu erzeugen. Durch die Automatisierung der Anwendungsvirtualisierung können Organisationen in einer benutzerzentrierten Lösung Bereitstellungsprojekte unter Windows 7 durchführen, VDI und Sitzungsvirtualisierung einsetzen und Anwendungen bereitstellen. Die Möglichkeit, Pakete für häufig verwendete Technologien zur Anwendungsbereitstellung zu veröffentlichen, kombiniert mit einer automatisierten Virtualisierungslösung, minimiert den Aufwand der IT-Abteilung und ermöglicht Paketierungsexperten, hochwertige Pakete für planbare Bereitstellungen zu erzeugen. *(dr)*

Steve Schmidt ist Vice President of Product Management bei Flexera Software.

Mobile Device Management

Herrscher im Geräte-Zoo

von Uwe Becker

Arbeitnehmer von heute verstehen moderne Informationstechnologien als wichtigen Teil ihres Arbeitsalltags. Wie seinerzeit E-Mails sind es nun Mobile Devices, die die Unternehmen auf den Kopf stellen. Um die Sicherheit von Kunden- und Firmendaten zu gewährleisten, müssen die IT-Abteilungen stets die Kontrolle über Einstellungen, Connectivity und über die Software aller im Unternehmen eingesetzten mobilen Endgeräte behalten. Dennoch kommen in vielen Unternehmen notwendige Management- und Sicherheitsinfrastrukturen immer noch nicht zum Einsatz. Dieser Beitrag liefert notwendiges Wissen um die sichere Verwendung von Smartphone und Co.

Quelle: pixelio.de

Die Anzahl und Vielfalt der internetfähigen Geräte in Unternehmen jeder Größenordnung steigt. Gleichzeitig hat das klassische Diensthandy ausgedient und wird zunehmend von den privaten Smartphones und Tablets der Mitarbeiter ersetzt. Klassische Smartphone-Anwendungen wie E-Mail, Kalenderfunktion und die Kontaktverwaltung sowie Zugriff auf CRM- und ERP-Systeme von unterwegs sind dabei erst der Anfang. Nach einer IDG-Untersuchung ziehen 39 Prozent der befragten Unternehmen bereits in Erwägung, funktionale Apps der nächsten Generation einzusetzen. Hierbei handelt es sich um die Nutzung von GPS, Kameras und sozialen Netzwerken, um das Tagesgeschäft der Mitarbeiter zu erleichtern.

Vielzahl an Geräten bereitet Kopfzerbrechen

Das Management und die Sicherheit der Daten auf diesen Geräten bereitet den IT-Abteilungen allerdings gehöriges Kopfzerbrechen. In der Vergangenheit wurden IT-Abteilungen solchen Problemen Herr, indem sie einfach die Anzahl der unterschiedlichen Plattformen limitierten. Diese Vorgehensweise ist allerdings nicht mehr umsetzbar, denn das Angebot an mobilen Endgeräten ist vielfältig. Selbst wenn ein Unternehmen die Strategie der Limitierung weiter verfolgen würde: Wie sollten die IT-Abteilungen die ständig zunehmende Anzahl an nicht zugelassenen, aber trotzdem genutzten Geräten sinnvoll managen? Warum sollte eine IT-Abteilung überhaupt den Mitarbeitern verbieten, ihr mobiles Endgerät zum Arbeiten zu nutzen und damit produktiv zu sein?

Das alte Argument, dass iPhones sich nicht als Business-Geräte eignen, ist längst überholt. Manche Anwendungen funktionieren besser auf der einen Geräteplattform als auf der anderen, was dazu führt, dass die Vielzahl an Kombinationsmöglichkeiten die optimale Lösung für alle denkbaren Aufgaben bereithält. Gerade die Vielzahl der Plattformen sorgt dafür, dass für jede Aufgabe auch das passende Tool zur Verfügung steht. Hier steckt der Teufel jedoch wie so oft im Detail. Denn jedes mobile Betriebssystem bietet höchst unterschiedliche Funktionalitäten in Bezug auf das Remote Management. Zwar werden Minimalfunktionen, wie zum Beispiel das Inventarmanagement, von allen mobilen Betriebssystemen unterstützt. Die am weitesten verbreiteten, Apples iOS sowie Android, verfolgen allerdings zwei völlig verschiedene Ansätze: Während Apple Fernzugriffsmöglichkeiten restriktiv handhabt und die Durchführung beispielsweise eines Remote Backups sehr stark reglementiert, sind die Möglichkeiten beim Mobile Device Management von Geräten mit Android-Betriebssystemen nahezu unbegrenzt.

Der Support muss stimmen

Welche Handlungsempfehlungen lassen sich hieraus nun für IT-Abteilungen ab-

leiten? Zunächst einmal die Einsicht, dass eine Einbindung unterschiedlicher Endgeräte nur über eine diversifizierte IT-Architektur funktioniert. Hier sind beispielsweise Virtualisierung sowie Cloud- und On-demand-Services geeignet, um die Belegschaftsstrukturen moderner Unternehmen abzubilden. Arbeiten im Home Office beziehungsweise von unterwegs gehört längst zum Alltag vieler Arbeitnehmer. Dementsprechend muss auch der Remote-Zugriff auf Firmennetze und -daten jederzeit und von überall sicher möglich sein.

Weiterhin ist es wichtig, dass mobile Endgeräte den gleichen Support erhalten wie der klassische PC oder Laptop. Aufgrund der hohen Komplexität muss hier ebenso eine Vielzahl an Parametern berücksichtigt werden, wie beispielsweise die Datensicherheit, das Datenmanagement und der Anwendungssupport. Mit den vielen unterschiedlichen Geräteplattformen, die mittlerweile in Unternehmen zum Einsatz kommen, sind Tools gefragt, die unterschiedliche Betriebssysteme wie Android, BlackBerry OS, Windows Mobile, iOS und Symbian managen. Typische Herausforderungen hierbei sind die Verwaltung der Anzahl und Einstellungen der unterschiedlichen Geräte, die Passwort- und Sicherheitseinstellungen, die Kontrolle der Connectivity sowie das Aufspielen neuer Software und Updates. Diese Herausforderungen lassen sich aus Unternehmenssicht am einfachsten durch mobile Endgeräte mit Symbian- und Windows Mobile-Betriebssystemen meistern, da beide eine vergleichsweise hohe Skalierung ermöglichen.

Sicherheitsrichtlinien unverzichtbar

Das meiste Kopfzerbrechen bereitet den IT-Verantwortlichen aber sicherlich das Sicherheitsmanagement. Mit durchschnittlich 8 GByte an Speicherkapazität lässt sich eine beachtliche Menge an Unternehmensdaten auf einem Smartphone speichern, die leicht durch einen Hackerangriff, manipulierte Software, einen Trojaner oder durch den physischen Verlust des Gerätes in die falschen Hände geraten könnte.

Parallel hierzu stellt sich die Frage der Durchführung von Backups und der Synchronisierung von Daten. Setzt ein Unternehmen Microsoft Exchange ein, wird auch die Synchronisierung durch dieses System verwaltet. Das mobile Endgerät empfängt in diesem Fall nur die Daten, ohne selber eine Anfrage an den zentralen Server zu stellen. Die Schwachstelle ist im Fall eines Manipulationsversuches auf Serverseite zu suchen und somit nicht ein proprietäres Problem der jeweiligen MDM-Lösung. Beim Thema Backup sieht es schon weitaus komplizierter aus, da nicht jedes Betriebssystem per se diese Funktion unterstützt. Android unterstützt diese Funktionalität beispielsweise von Haus aus nicht. Stattdessen kann man nur über Software eines Drittanbieters, die sowohl auf dem Client als auch auf dem Server installiert sein muss, diese wichtige Funktion in die jeweilige Mobile Device Management-Lösung implementieren.

Aber zurück zum Sicherheitsmanagement: Um hier auf mögliche Eventualitäten vorbereitet zu sein, ist es absolut notwendig, Sicherheitsrichtlinien zu etablieren. Diese müssen in jedem Fall drei Anforderungen erfüllen:

- Vertraulichkeit: Die Daten dürfen von keiner fremden Person eingesehen werden können.
- Integrität: Es muss sichergestellt sein, dass keine unautorisierten Veränderungen an den Einstellungen oder dem Datenbestand gemacht werden können.
- Verfügbarkeit: Die Daten müssen autorisierten Nutzern jederzeit zur Verfügung stehen.

Sicherheitstools müssen in der Lage sein, die ganze Bandbreite an Aufgaben, wie etwa Patch-Management, Vermeidung von Anwendungsfehlern, Abwehr von Virenangriffen sowie den nicht-autorisierten Gerätezugriff zu Firmennetzwerken, zu erfüllen. Zusätzlich müssen sie die Möglichkeit bieten, Geräte remote zu sperren oder zu löschen und vertrauliche Firmendaten zu verschlüsseln. Diese Tools sind in der Regel in ein zentrales Managementsystem implementiert und kontrollieren, installieren und konfigurieren Programme, Zertifikate und Einstellungen vollautomatisch über eine Software. Das Übertragungsspektrum reicht hierbei von sicheren VPN- oder APN-Verbindungen über Mobilfunk bis hin zu Network Access Control (NAC)-Lösungen. Auf dem Markt ist dementsprechend eine Vielzahl von Angeboten zu finden, die von Einzellösungen für bestimmte Aufgaben bis zu umfassenden Kombinationsmöglichkeiten reichen, die die Leistungsmerkmale mehrerer Technologien miteinander verbinden. Eine allgemeingültige Lösung existiert folglich nicht. Stattdessen hängt die Auswahl des jeweiligen Lösungspaketes davon ab, wie homogen beziehungsweise heterogen die IT-Architektur und die eingesetzten mobilen Endgeräte sind.

Automatisiertes Mobile Device Management

Der physische Zugriff auf alle mobilen Geräte, um Anwendungen zu implementieren oder Einstellungen zu ändern, ist in einem global agierenden Unternehmen rein vom Zeitaufwand her nicht möglich. Sich andererseits darauf zu verlassen, dass Mitarbeiter über den PC und USB-Anschluss Software aufspielen, ist ebenfalls nicht zu empfehlen, da dann die IT-Abteilung die Abläufe nicht unter Kontrolle hat.

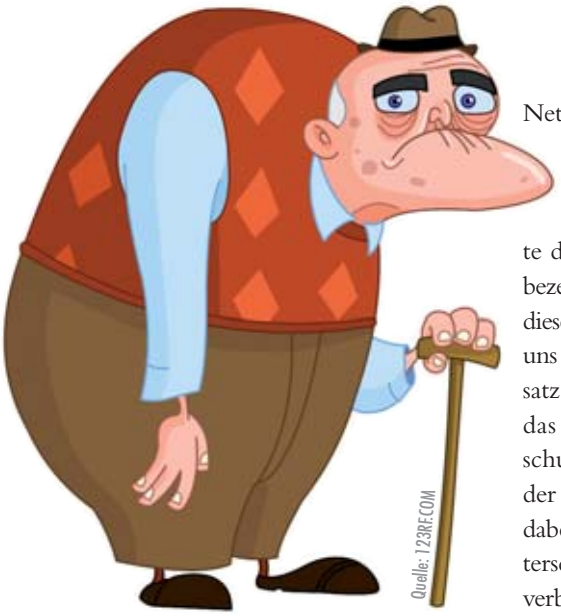
Als Alternative empfiehlt es sich hier, neue MDM-Tools zu verwenden, die automatisch die Gerätekonfiguration, den Support, die Administrierung und die Verwaltung der Sicherheitseinstellungen über das Mobilfunknetz durchführen. Dabei wird der ganze Gerätemanagementprozess, von der Software-Aktualisierung bis hin zum Ein- und Ausschalten bestimmter Funktionen, wie zum Beispiel der Kamera, durch das einfache Senden einer SMS gesteuert, ohne dass der User selbst einzugreifen braucht. Das Management eines mobilen Endgeräte-Pools bindet erhebliche finanzielle und personelle Ressourcen in Unternehmens-IT-Architekturen. Der Einsatz einer automatisierten Mobile Device Management-Lösung reduziert den Zeitaufwand und letztendlich Kosten beim Rollout und der Verwaltung mobiler Geräte. *(jp)*

Uwe Becker ist Head of Global Services Germany bei Orange Business Services.

Als Opa Admin war: Fuzzball

Und es werde … Netz!

von John Pardey



Unser heutiges Bild von Netzwerkkomponenten wie Routern ist zweifellos stark geprägt von einem Anbieter: Cisco. Aus aktuellen Netzwerken sind die Produkte dieser Firma nicht wegzudenken und leicht könnte der Schluss gezogen werden, Cisco hätte Router, Switches & Co praktisch im Alleingang erfunden und müsste sich heute nur noch mit einigen leidigen Konkurrenten herumschlagen, die aber im Prinzip nur die Produkte des Marktführers im weitesten Sinne kopieren.

Doch die Notwendigkeit, Netze zu verbinden, bestand schon weit früher als 1984, dem Gründungsjahr besagten Netzwerkausstatters. Sicher sehr bekannt ist der Vater aller Router, der Interface Message Processor, der schon 1969 als erster "Packet Router" seinen Dienst im ARPANET – dem Vorläufer des Internet unserer Tage – antrat.

Brücke zwischen Rechnerwelten

Doch dieser hatte eine vergleichsweise leichte Aufgabe, musste er doch nur die Kommunikation zwischen zwei Rechnern ermöglichen. Doch nur wenige Jahre später waren die Anforderungen rasant gestiegen, galt es mittlerweile doch, unterschiedliche Netze mit verschiedenen Protokollen zum Datenaustausch zu bewegen.

Und genau hier beginnt die Geschichte des Geräts, das als Urahn aller Router bezeichnet werden kann: der Fuzzball. Sechs dieser Geräte, deren technischen Details wir uns gleich noch zuwenden, waren im Einsatz, um das "NSF-net" zu ermöglichen, das die Netzwerke verschiedener Forschungseinrichtungen und Universitäten der USA verband. Der Fuzzball meisterte dabei die erwähnte Herausforderung, unterschiedlichste Protokolle miteinander zu verbinden. Dieses 56 KBit/s-Netz ermöglichte den Test der ersten Protokolle im Internet und hatte maßgeblichen Einfluss auf die Entstehung von TCP/IP.

Geburtshelfer des Internet

Der Fuzzball entstand auf der Basis des DEC LSI-11 Computers. Im eigentlichen Sinne beschreibt der Begriff Fuzzball nur die von David L. Mills auf dem LSI-11 entwickelte Software für die Kommunikation zwischen Netzwerken. Dabei umfasst Fuzzball eine Gruppe von Anwendungen inklusive eines Betriebssystems und einem Satz an Applikationen für den LSI-11. Dabei bleibt allerdings festzuhalten, dass Fuzzball keine einmalige Entwicklung war, die anschließend klaglos ihren Dienst im Netz verrichtete, sondern vielmehr über 17 Jahre (1971 bis 1988) hinweg als experimentelle Plattform für die Entwicklung von IT-Kommunikation diente. Zwar "entkamen", wie es Mills formulierte, einige Fuzzballs in "kommerzielle Umgebungen" (und wenn wir Quellen im Internet trauen dürfen, verrichten einige Fuzzballs noch heute ihren Dienst im Internet. Mills selbst fand 1990 den Letzten im aktiven Einsatz), doch eigentlich waren die Geräte nur als Zwischenstufe bei der Entwicklung von Routern gedacht.

Die Tragweite, die die Fuzzballs für unser heutiges Bild des Internet hatten, kann dabei nicht ausdrücklich genug betont werden. Die Geräte waren die erste Heimat von Prototypen unverzichtbarer Internet-Tools wie Telnet, FTP, DNS, EGP und SMTP. All diese wurden erstmals auf einem Fuzzball implementiert und getestet.

Noch ein vergessener IT-Pionier

Führen wir uns die Tragweite dessen vor Augen, was mit und auf dem Fuzzball in Sachen Internet entwickelt wurde, so müssen wir konstatieren, dass Dr. David L. Mills sich im gewissen Sinne in die Reihe vergessener Internet-Pioniere einreiht, von denen wir im Rahmen dieser Rubrik schon einige kennengelernt haben. Allerdings war Mills Zeit seines Lebens der Forschung verschrieben, so dass für ihn der kommerzielle Erfolg seiner Entwicklungen nicht unbedingt im Fokus stand. Doch sein Anteil an der IT, wie wir sie heute kennen (so ist er über Fuzzball hinaus auch noch der Erfinder des Network Time Protocol – NTP), ist so herausragend, dass er eigentlich in einem Atemzug mit Bill Gates und Steve Jobs genannt werden sollte. Dass dem nicht so ist, soll auch dieser Beitrag helfen, ein klein wenig zu ändern.

Der Fuzzball errichtete die ersten Brücken zwischen verschiedenen Netzwerken

Office 2010 Programmierung

Ebenso wie sich die Arbeit mit MS Office – insbesondere seit Version 2007 – weiterentwickelt hat, ist auch die zugehörige Programmierschnittstelle überarbeitet worden. Microsoft stellt die Visual Studio Tools für Office (VSTO) bereit, die auf .NET und Visual Studio aufsetzen. Für Entwickler gibt es aus diesem Segment nur wenig deutschsprachige Literatur. Der Autor Jan Tittel hat es sich zur Aufgabe gemacht diesen Fakt zu ändern. Natürlich beginnt die Publikation mit einer knappen, aber verständlichen Einführung in die Entwicklungsumgebung mit VSTO. Hingeben findet sich keine Einführung in die Programmierung mit .NET, sodass diesbezüglich Programmiervorkenntnisse vorausgesetzt werden oder auf entsprechende Sekundärliteratur zurückzugreifen ist.

Im weiteren Verlauf widmet sich das Buch der Praxis, wobei zuerst allgemeine Programmierkonzepte wie etwa das Erstellen von individuellen Menübänden, benutzerdefinierten Aufgabenbereichen, individuellen Kontextmenüs oder Forms-Dialogfeldern erläutert werden. In den Folgekapiteln geht der Autor auf die einzelnen Objektmodelle zu Outlook, Excel und Word ein. Dabei hat sich Tittel auf die Grundlagen als solide Basis für die Arbeit mit dem jeweiligen Objektmodell konzentriert. So können nach dem Studium dieser Kapitel Dokumente, Arbeitsblätter sowie Elemente von Outlook automatisiert eingesetzt werden. Auch in Bezug auf PowerPoint und Visio lässt der Autor den Leser nicht im Stich, wenngleich hier nur eine Grobübersicht gegeben wird. Für versierte Entwickler ist der Abschnitt zur Interaktion mit anderen Technologien relevant, bei dem das Zusammenspiel mit VBA oder OpenXML präsentiert wird.

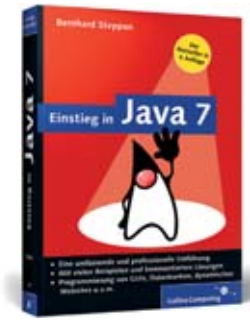
Fazit

Das Buch wendet sich an versierte Office-Anwender, die die neuen Möglichkeiten zur individuellen Lösungsgestaltung via VSTO nutzen möchten. Der Schwerpunkt liegt auf den Office-Flaggschiffen Word, Outlook und Excel. Für den Einsatz sind Grundkenntnisse von .NET von Vorteil, da sich das Buch primär mit den Office-Objektmodellen befasst und keine Einführung in die Programmiersprache gibt, so dass Kenntnisse von C# oder Visual Basic für das Verständnis Voraussetzung sind. Wer beabsichtigt in die Office-Programmierung einzusteigen, um seine Anwendungen individuell zu erweitern oder anzupassen, wird in diesem Buch fündig.

Frank Große

Autor	Jan Tittel
Verlag	Hanser
Preis	29,90 Euro
ISBN	978-3-446-42411-1
Bewertung *(max. 10 Punkte)*	**7**

Einstieg in Java 7, 4. Auflage



Insbesondere Web-Administratoren können nicht immer die Grenze zwischen reiner Administration und Softwarepflege ziehen. So werden sie bisweilen auch mit Quellcode konfrontiert. Für das Selbststudium im Fall von Java bietet sich das vorliegende Buch für Einsteiger an, das in drei große Teile gegliedert ist und die allgemeinen Grundlagen der Softwareentwicklung sowie eine Einführung zur Entwicklung von Java-Programmen bietet. Die Interaktion mit dem Leser findet durch Tutorien statt, bei denen der Leser entsprechende Übungsaufgaben zu absolvieren hat. Wer bereits Erfahrungen in klassischen oder objektorientierten Programmiersprachen sammeln konnte, der kann gleich mit dem Teil "Java im Detail" beginnen. Dort wird die Sprache und die Arbeit mit ihr vorgestellt.

Dem Autor ist es meist gelungen, sich auf das Wesentliche zu beschränken. An manchen Stellen sind die Ausführungen aber auch etwas zu knapp geraten. Im Praxisteil des Buches werden größere Projekte vorgestellt, bei denen für den Administrator primär Weboberflächen und Datenbanken von Interesse sind. In diesem Kontext soll der knappe Vergleich mit dem vor kurzem in der zehnten Auflage erschienenen Buch "Java ist auch eine Insel" von Christian Ullenboom aus dem gleichen Verlag gezogen werden. In akademischen Kreisen oft empfohlen, trifft die "Insel" dort wohl auch auf die entsprechende Zielgruppe, wo das Buch in Bezug auf die Praxistauglichkeit – besonders im Kontext von "quick and dirty" – Abstriche akzeptieren muss. Die Einführung in API gelingt Ullenboom ausgesprochen gut, ebenso die Nachschlagemöglichkeiten, nur die Übersichtlichkeit und Kompaktheit ist verloren gegangen.

Fazit

Die Konzeption dieses Einstiegsbuches ist keineswegs ausschließlich auf ein Stück-am-Stück-Lesen ausgerichtet. Der Leser lernt neben den Grundbegriffen und den wichtigsten Sprachelementen den Ansatz der objektorientierten Programmierung kennen. Im Buch finden sich rund hundert kleinere Beispielprogramme. Das bessere Verständnis für die Entwicklung einer Java-Anwendung entsteht aber durch die Präsentation von acht größeren – erfreulicherweise auch sorgfältig dokumentierten – Projekten verschiedener Couleur. Abgerundet wird der Inhalt durch jeweils ein knappes Kapitel über Java-Werkzeuge, Hardwaregrundlagen und ein Glossar. Java-Profis sollten zu fortgeschrittener Literatur greifen.

Frank Große

Autoren	Bernhard Steppan
Verlag	Galileo Computing
Preis	19,90 Euro
ISBN	978-3-8362-1662-3
Bewertung *(max. 10 Punkte)*	**8**

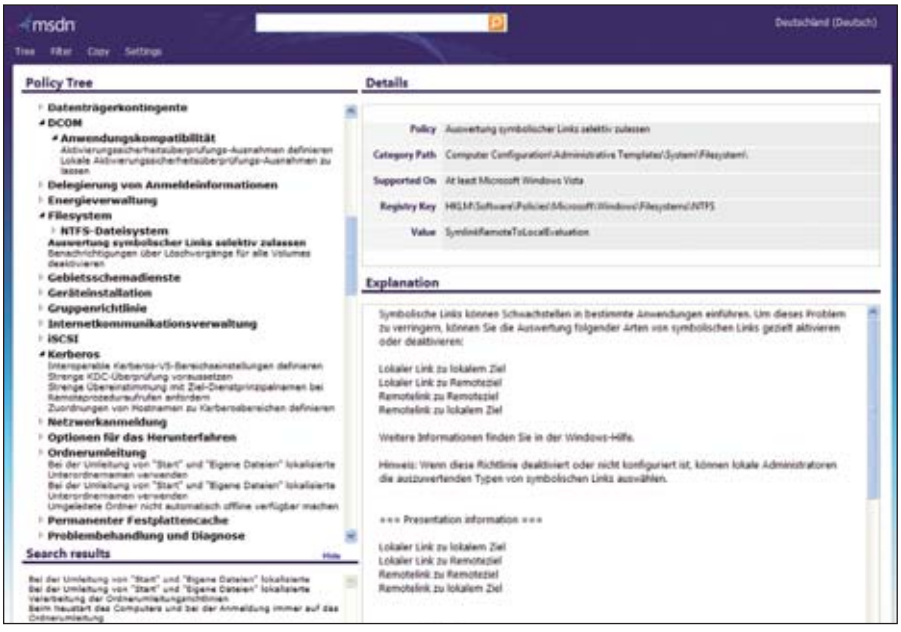
http://gps.cloudapp.net/

Gruppenrichtlinien-Kompendium

Gruppenrichtlinien sind in Windows-basierten Netzwerkumgebungen das Mittel der Wahl, wenn es darum geht, Einstellungen auf Rechnern zentral zu verwalten. Basierend auf dem Active Directory gibt es kaum einen Bereich, der sich nicht über die sogenannten Group Policy Objects – kurz GPO – verwalten lässt. Denn sie sind wohl das mächtigste Werkzeug, das einem Administrator an die Hand gegeben wird. Betrachten wir Gruppenrichtlinien dabei aus der Historie der Systemrichtlinien von Windows NT 4, sind diese beziehungsweise der Anteil der administrativen Vorlagen innerhalb der Group Policy Objects nichts anderes als Registryeinträge, die Administratoren zentral konfigurieren und dann an ein Ziel wie einen Benutzer oder Computer übergeben.

Mit Windows Server 2008 kamen dann noch einmal einige Neuerungen hinzu. Die zugrundeliegende Technik – die Vererbung und Hierarchie, die Filterung von Objekten, der Verwaltungs- und Anwendungsbereich der GPO, die Speicherorte, die Art der Erstellung – und ihre Werkzeuge sind mit dem Windows Server 2008 nahezu unverändert geblieben. Sie erlauben aber wesentlich mehr Funktionen und wurden unter der Haube verbessert, so dass sich am Ende Performance-Vorteile ergeben, ressourcenschonender gearbeitet werden kann und die Möglichkeiten der Administration erweitert wurden. Gut, wer hier als Admin nicht den Überblick verliert. Die Webseite http://gps.cloudapp.net des Microsoft Technical Evangelist Stephanus Schulte und Kollegen bietet einen umfassenden Überblick über die verfügbaren GPOs.

So finden Besucher auf der linken Seite den "Policy Tree" mit den jeweiligen Bereichen, die rund 7.000 GPOs betreffen – darunter etwa Desktop, Office, Freigaben, die Systemsteuerung oder Windows-Komponenten. Öffnen Nutzer nun einen der Oberpunkte, erhalten Sie die jeweilige Funktion, die mit einer Gruppenrichtlinie möglich ist, angezeigt. Nach einem Klick hierauf eröffnen sich den Besuchern die Details wie Category Path, unterstützte Betriebssysteme, zugehöriger Registry-Schlüssel und der Wert. Eine Beschreibung führt dem Admin in gut verständlichem Klartext vor Augen, was die jeweilige Richtlinie für Auswirkungen hat. Eine Volltextsuche erlaubt das einfache Auffinden von GPOs auch ohne den Policy Tree. Neben Englisch unterstützt die laufend aktualisierte Webseite dabei unter anderem auch Deutsch. Administratoren steht damit ein überaus umfassendes und dennoch übersichtlich und schlicht gehaltenes Kompendium zu Gruppenrichtlinien zur Verfügung. *(dr)*



Die Webseite gps.cloudapp.net gibt einen umfassenden Überblick zu Gruppenrichtlinien

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

Anforderungen an ein standardisiertes Thin Client-Management

Der Betrieb einer Thin Client-Umgebung fällt im Vergleich zum gemanagten Client/Server-Computing deutlich günstiger aus. Neue Entwicklungen im Bereich der Management-Werkzeuge weiten diese Vorzüge aus. In unserem Fachartikel im Web erfahren Sie unter anderem, wie sich heterogene Client-Umgebungen vereinheitlichen und standardisiert verwalten lassen, wie große Unternehmen das Thin Client-Management hochverfügbar machen und wie Sie pro Endgerät unterschiedliche Anwenderprofile anlegen und nutzen.
Link-Code: C1W51

Anwenderbericht: Dokumentation und Servicemanagement bei der QSC AG

Dokumentation und Servicemanagement gelten als unspektakuläre IT-Disziplinen. Nicht so beim Einsatz von Software aus der Open Source-Abteilung: Statt proprietärer Produkte von der Stange nutzt der Kölner Carrier QSC bei der Dokumentation seiner IT-Komponenten und der Bearbeitung von Support-Tickets freie Software. Lesen Sie in unserem Anwenderbericht, wie lange das Unternehmen mit der Implementierung des freien Systems beschäftigt war und wie der Einsatz der Configuration Management Database die Service-Qualität verbessert hat.
Link-Code: C1W52

Professionelles Management von mobilen Endgeräten

Die Zeiten, in denen sich Administratoren nur mit Windows als Client-OS befassen mussten, sind lange vorbei. Der Betrieb virtualisierter Desktops, die Überwachung mobiler Endgeräte oder das Management heterogener Umgebungen von iPhone über Android bis hin zu Blackberry – das sind die aktuellen Aufgabenstellungen. In unserem Online-Beitrag stellen wir die Frage, ob die Einbindung privater Geräte in das Firmennetzwerk kontrollierbar ist und zeigen, wie Administratoren mobile Devices mittels "Dynamic Workplace Management" effizient verwalten.
Link-Code: C1W53

Sicherheits-Vorteile einer konsolidierten Netzwerkinfrastruktur

Ein eigenes Netzwerk für fast jede IT-Aufgabe – viele Unternehmen sind von diesem Horrorszenario nicht weit entfernt. In einem derart heterogenen Netz muss auch der Kampf gegen Sicherheitsbedrohungen stets an mehreren Fronten ausgetragen werden. Die Konsolidierung der verschiedenen Netze bringt in Sachen Security gleich mehrere Vorteile. Im Beitrag auf unserer Webseite erklären wir, wie neben der reinen Malware-Abwehr gerade Aspekte wie Datenschutzrichtlinien, Archivierung und Datenintegrität von einem konsolidierten Netz profitieren.
Link-Code: C1W54

Besser informiert: Fachartikel auf der Website des IT-Administrator

»Ich habe mein Hobby zum Beruf gemacht«

David Hablützel (32) hat es nach einer Ausbildung bei den Schweizerischen Bundesbahnen (SBB) schnell in die IT verschlagen. In Schlatt, im Kanton Thurgau, machte er sich vor einigen Jahren mit seinem eigenen Unternehmen selbstständig. Der "HardwareShop Ernst" bietet seinen Kunden alle Dienstleistungen rund um die Planung, Implementierung und Wartung von IT-Komponenten und Lösungen, Netzwerken und Internet-Lösungen an.

Warum sind Sie IT-Administrator geworden?

Ich bin mit der IT aufgewachsen und habe mich bereits während der Schulzeit kontinuierlich mit Computern und Computerspielen beschäftigt. Das ging während meiner Berufszeit weiter und endet vorerst mit dem eigenen Geschäft, in dem ich mich auch wieder mit der IT befasse.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Ein wichtiger Ausgleich ist die Zeit mit meiner Familie.

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

Oft bleibt das nicht aus, da ich für meine Kunden den besten Service anbieten möchte. Damit einhergeht die ständige Erreichbarkeit, auch wenn die Probleme am Wochenende auftauchen. Wann immer es geht, nehme ich mir aber gerne die nötigen Auszeiten.

Wie stellen Sie sich die IT im Privatleben in zehn Jahren vor?

Die Technik wird noch mehr Bereiche unseres Lebens beeinflussen. Ich beneide meine Kinder um die Lösungen, mit denen sie in Berührung kommen werden. Ich könnte mir vorstellen, dass wir irgendwann ohne Bildschirme leben, mit Bildern direkt in die Brille oder ins Auge projiziert. Batterien werden mit den Schuhsohlen aufgeladen, Lautsprecher direkt im Ohr implantiert.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Derzeit arbeite ich am Ausbau meiner Dienstleistungen und der Erweiterung des Kundenstamms. Ich werde mit einer IT-gestützten Lösung einen noch besseren und schnelleren Service anbieten können – Kunden können dann auf unserer Webseite den Live Support wählen und direkt mit einem Techniker in Kontakt treten.

Welche Werkzeuge nutzen Sie für Ihr Client-Management?

Ich arbeite seltener als Administrator, setze dafür auf die Expertise meiner EDV-Partnerfirmen. Häufig kommt dabei die Software SiSoft Sandra 3B zum Einsatz.

Welche Aspekte Ihres Berufs machen Ihnen am meisten Spaß?

Spaß machen mir die Problembehebung und der Umgang mit Menschen. Mir gefällt es, Anwendern beim Umgang mit der IT zu helfen, ihnen bei Problemen zur Seite zu stehen. Der enge und vertrauensvolle Kontakt mit Kunden ist mir wichtig. Es gibt eigentlich nichts, was mir an meinem Beruf nicht gefällt. Das Analysieren der Computerprobleme ist eine geschenkte Leidenschaft.

Welches sind die nervigsten Client-Management-Aufgaben?

Die Beseitigung von Viren, Trojanern und anderen Problemen, die ein reibungsloses Arbeiten behindern, sind aufwändig und enden scheinbar nie.

Wo liegt Ihrer Meinung nach der größte Optimierungsbedarf beim Client-Management?

Die automatische Integration von Datensicherungssystemen ist bei vielen Infrastrukturen kaum oder nur unzureichend vorhanden. Da sollte jedes Unternehmen etwas ändern. Meine bevorzugte Managementsoftware dafür ist Acronis.

Wie denken Sie, arbeitet ein Administrator in zehn Jahren?

Der Arbeitsplatz wird sich verlagern. Der Administrator der Zukunft arbeitet überwiegend im Home Office oder mobil. Eine Anwesenheit vor Ort wird kaum noch erforderlich sein.

Welches IT-Problem ließ Sie in letzter Zeit verzweifeln?

Bei einem Kunden habe ich ein neues Computersystem installiert, auf das eine ältere CAD-Anwendung installiert werden musste. Das war mühsam.

Wenn Sie sich ein beliebiges Tool wünschen könnten, was würde dieses leisten?

Das wäre eine Art digitaler Zauberstab, der automatisch die Behebung aller Microsoft-Probleme übernimmt.

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

Der Beruf des Administrators ist für jeden etwas, der sich gerne mit Computern und der Technik auseinandersetzt. Wer gerne nach Fehlern und den passenden Lösungen sucht, anderen gerne bei Problemen zur Seite steht und helfen möchte, ist auf dieser Position genau richtig.

Welches ist der dümmste Anwenderfehler, der Ihnen untergekommen ist?

Es gibt keine dummen Anwenderfehler – nicht jeder kennt sich in dieser Materie aus. Klassiker sind jedoch USB-Stecker am COM- oder LAN-Port anschließen, Bildschirm auf den Kopf stellen, weil sich das Bild durch eine versehentlich genutzte Tastenkombination automatisch um 180 Grad gedreht hat, oder am Bildschirm mit Tipp-Ex einen Punkt streichen.

Das Interview führte Petra Adamik

Geburtstag: 20.04.1979
Admin seit: 12 Jahren
Hobbys: Computer, bügeln, Familienleben

David Hablützel, IT-Administrator

Ausbildung und Tätigkeit

- Ausbildung bei den Schweizerischen Bundesbahnen
- Danach bei verschiedenen IT-Unternehmen in der Administration und im Sicherheitsbereich
- Seit 2008 mit eigenem Unternehmen selbständig
- Heute Geschäftsinhaber, Geschäftsführer und Techniker sowie Administrator in Personalunion

Betreute Umgebung

- Arbeit mit Deltra Orgamax und SharePoint 2010
- Analyse und Lösung von IT-Problemen wie das Retten von Daten

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

Was haben Sie zu sagen?

Die Ausgabe 2/12 erscheint am 2. Februar 2012

Schwerpunktthema:

Monitoring

Im Test: WhatsUp Gold v15

Im Test: ManageEngine OpManager

Workshop: Log-Dateien auf Windows-Systemen auswerten

Systeme: Neues im Windows Server 8

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

Die Ausgabe im **März** richtet ihren Fokus auf das Thema **Netzwerkmanagement**. In unserer Test-Rubrik müssen unter anderem Network Ressource Manager v3.0 sowie Fluke Network Time Machine ihr Können unter Beweis stellen. In unserer Praxisrubrik erfahren Sie, wie Sie FreeRADIUS aufsetzen und einrichten.

Als Schwerpunkt im **April** geht es dann um das Thema **Backup & Verfügbarkeit**.

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, Uwe Becker, Giovanni Brugugnone, Falko Gräfe, Thomas Gronenwald, Frank Große, Jürgen Heyer, Christian Knermann, Sandro Lucifora, Dr. Holger Reibold, Steve Schmidt, Ulf B. Simon-Weidner

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

Es gilt die Anzeigenpreisliste Nr. 9 vom 01.01.2012
LAC/2011

Produktion / Anzeigendisposition
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

Vertriebsbetreuung
SI special interest Pressevertrieb GmbH,
www.specialinterest.com

Erscheinungsweise
monatlich

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

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

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

Diese Ausgabe enthält eine Teilbeilage der Firma ppedv sowie einen Einhefter zwischen Seite 34 und 35 mit Advertorials von den Firmen Iomega und Frontrange.

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

1&1 SERVER NEXT GENERATION

WELTNEUHEIT EXKLUSIV BEI 1&1:

2 x 16 CORE

AMD OPTERON™ PROZESSOR 6272

- **Sicher:** Modernste Rechenzentren, über 99,9 % Erreichbarkeit
- **Einfach:** Parallels® Plesk 10.4 unlimited enthalten
- **Flexibel:** Umfangreiche Betriebssystem- und Featureauswahl
- **Schnell:** Traffic Flatrate und über 275 GBit/s Anbindung
- **Fragen?** Kostenloser Support rund um die Uhr

Weitere 1&1 Server im Internet

DAS NEUE 1&1 DEDICATED SERVER PORTFOLIO:

NEU: 1&1 SERVER MIT INTEL-PROZESSOREN!

SERVER 4i

intel inside Xeon

- Intel® Xeon® E3-1220
- 4 Cores bis zu 3,4 GHz
- 12 GB ECC RAM
- 1.000 GB RAID 1 mit 2 x 1.000 SATA HDD

79,99 €/Monat*

AKTION: JETZT 3 MONATE SPARPREIS SICHERN!

SERVER XL 6

OPTERON PROCESSOR AMD

- AMD Hexa-Core Prozessor
- 6 Cores bis zu 3,3 GHz
- 16 GB ECC RAM
- 1.000 GB RAID 1 mit 2 x 1.000 SATA HDD

JETZT: 3 MONATE FÜR 0,– €*

~~99,99~~ **€/Monat***

EXKLUSIV BEI 1&1: DER WELTSCHNELLSTE HOSTING-SERVER!

SERVER XXL 32 CORE

OPTERON PROCESSOR AMD

- 2 x 16-Core AMD Opteron™ Prozessor 6272 („Interlagos")
- 2 x 16 Core bis zu 3,0 GHz
- 64 GB ECC RAM
- 2.400 GB RAID 6 mit 6 x 600 SAS HDD

499,99 €/Monat*

1&1

Internet made in Germany

Jetzt informieren und bestellen:

0 26 02 / 96 91

0800 / 100 668

www.1und1.info

* **Server 4i:** 79,99 €/Monat. **Server XL 6:** 3 Monate 0,– €/Monat, danach 99,99 €/Monat. **Server XXL 32 Core:** 499,99 €/Monat. Einmalige Einrichtungsgebühr 99,- € (entfällt bei Server 4i und Server XXL 32 Core). Mindestvertragslaufzeit 12 Monate. Preise inkl. MwSt.