IT-ADMINISTRATOR.DE

12/2010

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Wi-Fi, VoIP und WLAN-Management

X. Neu definiert.

Bislang war die Sache ganz einfach: Wer mehr Rechenleistung braucht, z. B. für neue, speicherintensive Anwendungen, der muss eben mehr Server kaufen. Das Problem dabei: Mit der Zahl der Server wächst eher die Ineffizienz als die Leistung. Die meisten Server laufen heute nur mit 10 % ihrer Kapazität.[1] Zum Glück haben die Entwickler von IBM dieses Problem gelöst. Die 5. Generation der Enterprise X-Architektur verfügt über leistungsstarke Intel® Xeon® 7500-Prozessoren. Vor allem aber kann man erstmals Speicher unabhängig vom Prozessor nachrüsten. Das Resultat: IBM eX5-Systeme können 6-mal mehr Speicher ansprechen als aktuelle x86-Server. Sie können damit rund 50 % Lizenzgebühren und bis zu 97 % der Speicherkosten sparen.[2]

Smarte Unternehmen brauchen intelligente Software, Systeme und Services. Also: Machen wir den Planeten ein bisschen smarter. Wie, erfahren Sie unter ibm.com/systems/de/ex5

IBM®

intel Xeon® inside™

Leistungsstark.
Intelligent.

[1]Die McKinsey-Studie finden Sie hier: http://www.datacenterknowledge.com/archives/2009/04/15/mckinsey-data-centers-cheaper-than-cloud/ [2]Vergleich eines IBM System x3850 X5 + MAX5 mit 96 DIMMs x 16 GB für insgesamt 1,5 TB Speicher gegenüber einem IBM System x3850 M2 mit 32 DIMMs x 8 GB = 256 GB. Vergleich von Lizenzgebühren auf Prozessorbasis für aktuelle Prozessorsysteme der Generation 4 mit 64 DIMMs gegenüber dem IBM System x3690 + MAX5. Bei Verwendung der IBM eXFlash-Technologie wäre es für einen Kunden nicht mehr erforderlich, zwei Einstiegsserver und 80 JBODs zur Unterstützung einer Datenbankumgebung mit 240.000 IOPs zu kaufen, was einer Einsparung von 97 % bei Server- und Speicher-Anschaffungskosten entspricht.

EDITORIAL

Langsamstarter

Liebe Leser,

"Never Change a Running System!" lautet eine Adminweisheit. Und solange keine triftigen Gründe dagegen sprechen, ist dieses Vorgehen durchaus berechtigt. Auch IPv4 lässt sich als ein solches System mit vertrauten Begriffen wie Network Address Translation, internen und externen IP-Adressen und mehr oder weniger einfachen Subnetzen bezeichnen.

Doch das soll sich dank des Nachfolgers IPv6 bald ändern – mal wieder! Oft schon wurde der Durchbruch des neuen Internet-Protokolls vorhergesagt, ohne dass daraufhin etwas Nennenswertes passiert ist. Immerhin: Aktuelle Betriebssysteme wie Windows Server 2008 oder Windows Vista und 7 glänzen inzwischen mit IPv6-Unterstützung und auch die meiste Hardware spricht das neue Protokoll. Da brauchen wir uns wohl nicht mehr zu fürchten, wenn im Frühjahr 2011 endgültig die letzten IPv4-Adressen über den großen Ladentisch der IANA gehen sollen. Der triftige Grund für einen Wechsel scheint gekommen.

Dabei bietet IPv6 sogar noch weitere Vorteile. So entfällt etwa die Notwendigkeit, private Adressen über NAT in öffentliche umzusetzen und umgekehrt. Damit können sich Geräte flexibel mit ihrer eigenen IP-Adresse ins Internet und untereinander verbinden. Es ist jedoch – Sie ahnen es – nicht alles Gold, was glänzt. Im zweiten Teil unserer Workshopserie ab Seite 47 zeigen wir auf, welche Tücken unter IPv6 etwa in Tunnelnetzen lauern und wie die Duplicate Address Detection für Probleme sorgen kann. Doch so sehr unsere Beitragsserie auch die Unwegsamkeiten von IPv6 hervorhebt, überwiegen die Vorteile klar – besonders dann, wenn die Tücken von vornherein bekannt und damit vermeidbar sind. Drücken wir also dem Neuen im Netzwerk die Daumen fürs nächste Jahr.

Übrigens: IPv6 ist nicht die einzige Neuerung, die der IT-Welt ins Haus steht. IT-Administrator macht nämlich Schluss mit überlangen Hyperlinks im Heft. Künftig steht Ihnen für jeden Link ein Kürzel, der sogenannte Link-Code, zur Verfügung. Mit diesem gelangen Sie über unsere Webseite bequem auf die jeweiligen Zielseiten – egal wie lang der eigentliche Link dahinter ist.

Das gesamte Team des IT-Administrator wünscht Ihnen ein frohes und besinnliches Weihnachtsfest und einen guten Start in ein erfolgreiches und gesundes neues Jahr!

Ihr

Daniel Richey
Stellv. Chefredakteur

IDEAL INDUSTRIES NETWORKS

IDEAL

LanXPLORER PRO

Inline-Netzwerktester

AUTOTEST
AUTO
Testen auf Knopfdruck

Verdrahtungsplan
auf Pinebene

Netzwerkplan
Aktive Geräte abbilden und speichern, später überprüfen

PoE und PoE+
Spannungserkennung und Last-Tests

VoIP
Qualitätsparameter überwachen

Inline-Messungen
Leistungsdaten aktiver Geräte prüfen

Loopback-Device
Gegenstelle für aktive Tester bis inkl. Layer 3

- **Robustes, kompaktes Design**
- **Hochauflösender, farbiger Touchscreen**
- **Intuitive Bedienung**
- **Austauschbare, handelsübliche SFP-Module**
- **Keine Kalibrierung erforderlich**

IT – Troubleshooting einfach gemacht

Einsetzbar in Multimedianetzen: Kupfer, LWL + WLAN

Vielfältiges Funktionsspektrum

☎ +49-(0)89-996860

✉ germanysales@idealnwd.com

www.lanxplorer.de

INHALT

IT-Administrator – Ausgabe Dezember 2010

Wi-Fi, VoIP und WLAN-Management

Einkaufsführer: Voice over WLAN-Umgebungen

Mobilität und damit einhergehend die drahtlose Kommunikation innerhalb eines Unternehmens werden immer wichtiger. Dazu zählt neben der Datenmobilität auch die Beweglichkeit in Bezug auf die Sprachkommunikation. Diese lässt sich unter anderem durch VoIP über WLAN erreichen. Welche Aspekte Sie für den Aufbau einer solchen Umgebung beachten müssen, zeigt Ihnen unser Einkaufsführer.

Seite 36

Lösungsansätze gegen Netzwerkengpässe

Multimedia-Anwendungen benötigen einen unterbrechungsfreien, verlustarmen und verzögerungsarmen Transport der Datenströme. Diese Dienste stellen definierte Anforderungen, die in klassischen Datennetzen nicht ohne weiteres realisierbar sind. Daher ist die Übertragung von Informationen mit einer definierten Dienstgüte der zentrale Punkt bei der Entwicklung besserer Datennetze.

Seite 44

Neu im IT-Administrator: Link-Codes

Unsere neuen Link-Codes ersparen Ihnen mühsame Tipparbeit bei langen URLs

Logdaten-Verwaltung in einem Gerät

LogLogic bringt die **SIEM LX820 (Security Information und Event Management- und Daten-Management-Appliance)** auf den Markt. Das Gerät basiert auf der **LogLogic 5-Plattform** und kann bis zu 5.000 Messages je Sekunde (MPS) verarbeiten. Dabei unterstützt die Appliance mit einer Höheneinheit standardmäßig über 340 Systeme und Gerätetypen. LogLogic 5 bietet eine Rundumsicht auf die gesamten IT-Aktivitäten durch eine zentralisierte Strukturierung der IT-Daten. Durch die "Log Label"-Funktionalität können laut Hersteller zudem beliebige weitere Geräte und Anwendungen integriert werden. Es soll den Unternehmen so ermöglichen, eine sichere und effiziente IT-Infrastruktur mit verbesserter Transparenz und Kontrolle zu betreiben. Drei GBit-Ethernet-Anschlüsse sowie ein serieller Port sorgen für die Anbindung der Appliance an das Netzwerk. Die Speicherkapazität beträgt zwei mal 500 GByte im RAID 1-Verbund. Die LX820 ist ab sofort verfügbar und startet mit einem Listenpreis von 25.000 US-Dollar. *(dr)*

LogLogic: www.loglogic.com/lx820/

VMs mit Netz und doppeltem Boden

Veeam bietet seine Software **Backup & Replication für VMware** in **Version 5** an. Die Software erlaubt das **Sichern und Wiederherstellen** von virtuellen Maschinen unter **VMware ESX(i)**. Mit der Technologie namens vPower kann Backup & Replication v5 eine VM direkt aus der komprimierten und dedupplizierten Backup-Datei heraus starten. Dies kann entweder innerhalb einer Produktionsumgebung oder in einer isolierten virtuellen Laborumgebung im normalen Backup-Speicher geschehen. Dadurch ist es nun möglich, eine VM direkt aus der Backup-Datei wiederherzustellen oder einzelne Objekte wie E-Mails oder Datenbankeinträge aus virtualisierten Anwendungen zu retten. Außerdem prüft Version 5 dank SureBackup Recovery Verification automatisch die Wiederherstellbarkeit eines jeden Backups, ohne weitere Hardware oder den Einsatz zusätzlichen IT-Personals. Mit vPower können Unternehmen zudem ihre Investitionen in Backup-Speicher besser ausschöpfen: Die "On-Demand-Sandbox" in Veeam Backup & Replication v5 erlaubt eine Nutzung der Speicherkapazitäten zum Beispiel für Troubleshooting, Testumgebungen oder die Entwicklung und Qualitätssicherung. Veeam Backup & Replication v5 ist ab sofort verfügbar. Die europäischen Listenpreise beginnen bei 790 Euro pro Socket für die Enterprise Edition. Kunden, die zum 30. Juni 2010 eine gültige Wartungslizenz besaßen, können kostenlos zur Enterprise Edition upgraden. *(dr)*

Veeam: www.veeam.com/vmware-esx-backup.html

Nachwuchs in der NAS-Familie

Mit der Produktserie **ReadyNAS Pro** fügt **Netgear** seinem Angebot an **NAS-Speichern** einen weiteren Baustein hinzu. Die Geräte sind in unterschiedlichen Konfigurationen mit zwei, vier oder sechs Laufwerkseinschüben erhältlich und stellen die RAID-Modi 0, 1, 5 und 6 zur Verfügung. Maximal ist mit der Verwendung von 2 TByte-SATA-Festplatten eine Kapazität von 12 TByte möglich. Der Austausch einzelner Magnetspeicher im laufenden Betrieb stellt gemäß Hersteller keine Probleme dar. Zwei redundante GBit-Ethernet-Ports sollen die Ausfallsicherheit des Systems garantieren. Das Gehäuse bietet darüber hinaus drei USB 2.0-Ports für die Anbindung externer Festplatten, Drucker oder USVs. Die Storage-Server sind für die Verwendung unter vSphere und Hyper-V zertifiziert und kompatibel zu zahlreichen Backup-Lösungen. Laut Netgear können bis zu 200 Anwender auf das Speichersystem zugreifen, Active Directory wird unterstützt. Zudem meldet das ReadyNAS Pro dem Administrator mit Hilfe der integrierten Monitoring-Funktion außergewöhnliche Situationen wie Festplattenausfälle über E-Mail-Alarme. Außerdem ist das Gerät mit einem automatischen VPN-Service für einen sicheren Fernzugriff ausgestattet.

Einmal in die entsprechende Schiene geschraubt, lassen sich Festplatten bei den ReadyNAS Pro-Geräten auch im laufenden Betrieb austauschen

Die Preise beginnen für das 2-Bay-Modell mit zwei 1 TByte-Platten bei rund 630 Euro und enden bei knapp 4.100 Euro für die Variante mit sechs 2 TByte-Magnetspeichern. Im Preis enthalten ist bei jedem Modell eine Einjahreslizenz für ein Online-Backup mit maximal 100 GByte. *(ln)*

Netgear:
www.netgear.de/Unternehmen/Netzwerkspeicher/

Schutz fürs neue Jahr

Kaspersky Lab stellt neue und aktualisierte Produkte der **Unternehmens-Lösung Kaspersky Open Space Security** vor. **Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition** beispielsweise schützt Daten auf Servern mit Windows-Betriebssystemen von Microsoft (einschließlich x64-Versionen) vor Schadprogrammen. Viren-Scans werden laut Hersteller fünf- bis siebenmal so schnell durchgeführt wie in der Vorgängerversion. Das Produkt ist unter anderem kompatibel mit Windows Server 2008 R2 und Virtualisierungs-Systemen von VMware. Die Softare schützt außerdem Microsoft-Terminalserver sowie Citrix-XenApp-Server (früher Presentation Server). Eine weitere Version mit EMC-Celerra-Unterstützung wird ebenfalls erhältlich sein. **Kaspersky Security 8.0 für Microsoft Exchange Server 2007/2010** soll mit der vierten Generation der Anti-Spam-Engine von Kaspersky Lab besonders gute Malware- und Spam-Erkennung bieten. Dabei würde

Kaspersky Lab macht seine Unternehmensprodukte mit Version 8.0 fit für das neue Jahr

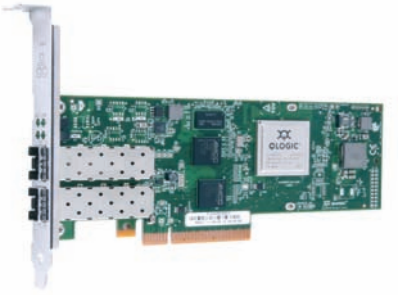
bei unerwünschten E-Mails eine Erkennungsrate von 99 Prozent erreicht bei minimalen False-Positives. Daneben bietet Kaspersky die **Anti-Virus-Version 8.0 für Linux File Server, für Lotus Domino, für Microsoft ISA Server und Forefront TMG Standard Edition, für Linux- und Mac-Rechner sowie für Smartphones** an. Das Kaspersky Open Space Security 5+1 Base Pack für einen File-Server und fünf Workstations kostet beispielsweise 209 Euro. *(dr)*

Kaspersky Lab: www.kaspersky.com/de/business_products/

Einer für alle

QLogic baut mit der neuen **Produktserie 8200** sein Angebot an **Converged Network-Adaptern** (CNA) mit einer **Übertragungsgeschwindigkeit von 10 GBit/s** aus. Die Lösung vereint verschiedene Karten auf einem Adapter und ermöglicht es erstmals, die Daten- und Speicherprotokolle FCoE, iSCSI und TCP/IP zur selben Zeit auf der gleichen Hardware zu verarbeiten. Durch die Bearbeitung der Informationsströme direkt auf dem Netzwerkadapter nimmt dieser nur rund neun Prozent der Server-CPU in Anspruch. Die dadurch freigesetzte Bandbreite soll besonders **in virtualisierten Umgebungen für eine deutlich erhöhte Performance** sorgen. Ein in die Komponente integrierter Layer 2 Ethernet-Switch ermöglicht zudem, dass virtuelle Maschinen direkt und somit unabhängig vom Hypervisor, vom Betriebssystem, vom Protokoll oder Switch miteinander kommunizieren. Mit Hilfe der Technologie "VMflex" lässt sich außerdem jeder physikalische 10 GbE-Port in bis zu vier virtuelle Ports aufteilen und diesen die von den einzelnen VM-Anwendungen geforderte Bandbreite zuweisen. Alle im konvergenten Netzwerk eingesetzten Produkte einschließlich sämtlicher unterstützter Protokolle lassen sich über die ebenfalls neue Konfigurationssoftware "QConverged-Console" zentral über den Webbrowser verwalten. Je nach Modell und Portausstattung sind die neuen CNAs zu Preisen ab 1.300 Euro erhältlich. *(ln)*

QLogic: www.qlogic.com/Products/adapters/



Die Converged Network-Adapter aus QLogics 8200er- Serie verarbeiten die Protokolle FCoE, iSCSI und TCP/IP auf einer Hardware

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

Itelio bietet die Software **Docusnap** in Version 5.1 an. Damit ist es nun möglich, Abhängigkeiten zwischen Servern zu hinterlegen und graphisch darzustellen. Jeder Bericht in Docusnap lässt sich zudem über eine Zeitplanung vom Docusnap-Server ausführen. Die Ergebnisse werden im Dateisystem abgelegt oder per E-Mail versandt. Die Rollenberechtigungen wurden auf Objekte beziehungsweise Erweiterungen ausgedehnt, so ist es etwa möglich ein bestimmtes Passwort nur für eine Rolle sichtbar zu machen. Der Basispreis liegt bei 200 Euro für bis zu 24 Systeme. *(dr)*

www.docusnap.de

Red Hat erweitert mit Version 6.0 den Funktionsumfang des Betriebssystems **Red Hat Enterprise Linux** (RHEL). Die neue Version bietet unter anderem eine optimierte KVM-Virtualisierung mit besserer Skalierbarkeit und einer durchgängigen Applikationsnutzung in virtuellen und physischen Umgebungen. Daneben bietet RHEL 6 eine umfassende IPv6-Unterstützung und ein überarbeitetes Power-Management. Das Dateisystem EXT4 soll nun größere Dateien unterstützen und verkürzte Reparaturzeiten ermöglichen. Das Open Source-Betriebssystem ist ab sofort erhältlich und kostet für ein 2-Sockel-Server und Premium-Support 1.039 Euro pro Jahr. *(dr)*

www.redhat.de

Der neue **Cloud Service 3.0** von **Zscaler** erlaubt seinen Anwendern nun auch eine Single-Sign-on-Authentifizierung an dessen gehosteten Web- und E-Mail-Security Service. Möglich macht dies das standardisierte Schnittstellenprotokoll SAML (Security Assertion Markup Language). So kann zum Beispiel ein im Active Directory angemeldeter Anwender ohne erneute Eingabe von Benutzername und Passwort vom Zscaler-Dienst authentifiziert werden. Die entsprechenden Policies für die von ihm aufgerufenen Webseiten werden dann automatisch angewendet. *(dr)*

www.zscaler.com

Quantum hat die Datenmanagement-Software **StorNext** mit einer neuen Funktion zur Migration von bisherigen Archivplattformen auf StorNext ausgestattet. Das Archive Conversion Utility (ACU) soll eine bessere Steuerung der Migration von Archiven anderer Hersteller ermöglichen und den Aufwand dabei deutlich reduzieren. Laut Hersteller können Nutzer mit Hilfe der ACU-Funktionalität innerhalb von Stunden nach Beginn der Datenmigration auf Terabytes oder Petabytes archivierter Daten auf Tape zugreifen. Das Werkzeug bietet in der ersten Version Support für Oracle/SUN SAM-FS- sowie QFS-Softwareplattformen und kostet 20.000 US-Dollar. *(ln)*

www.quantum.com

Kostenlos, aber mächtig

Spiceworks präsentiert mit **Version 5.0** das neueste Release seiner gleichnamigen **kostenlosen Software zum Netzwerk-Management**. Neu ist unter anderem die Verwaltungsoberfläche "People View", die es Administratoren ermöglicht, **anwenderbasiert Rechner und Cloud-Dienste zu überwachen, zu verwalten und bereitzustellen**. IT-Verantwortliche haben damit die Möglichkeit, E-Maildienste, die Helpdesk-Tickethistorie oder kürzlich angeforderte Anschaffungen jedes einzelnen Benutzers mit Hilfe einer zentralen Oberfläche zu verwalten. Durch die Integration von Microsoft Active Directory erlaubt die Funktion das automatische Anlegen von Profilen und Benutzerkonten. Außerdem neu ist das Feature, Konfigurationen von Netzwerkgeräten wie etwa Switches und Router zu scannen, zu sichern, zu vergleichen und wiederherzustellen. Dabei aktualisiert die Software die Scans in regelmäßigen Abständen oder wenn neue Geräte zum Netzwerk hinzugefügt werden. Außerdem erfolgt bei Änderungen der Netzwerkkonfigurationen automatisch eine Benachrichtigung. Eine weitere Funktion stellt außerdem eine ferngesteuerte Wiederherstellung von Einstellungen auf Netzwerkgeräten mit Hilfe des integrierten TFTP-Servers bereit. Für IT-Dienstleister interessant dürfte auch die neue Möglichkeit sein, zentralisierte Helpdesk- und anpassbare Kundenportale zur Verfügung zu stellen. Dies soll die Verwaltung mehrerer Kundendienstanfragen in einer einzigen Konsole vereinen. Die jüngste Version des kostenlosen, durch Werbeeinblendungen finanzierten Werkzeugs steht ab sofort zum Download bereit. *(ln)*

Spiceworks: www.spiceworks.com

Modulares Datenmanagement

CommVault stellt mit **Simpana 9** eine neue Version seiner **Software-Suite zum Datenmanagement** vor. Je nach Bedarf besteht die Lösung unter anderem aus Modulen zum **Backup und zur Archivierung, zur Replikation** oder stellt globale Suchfunktionen bereit. Neu ist unter anderem eine **verbesserte Unterstützung von virtuellen Maschinen** (VM). So will der Hersteller auch in heterogenen Umgebungen die Absicherung einer großen Zahl von VMs ermöglichen und greift dabei auf die SnapProtect-Technologie zurück. Die Snapshots werden hierbei direkt auf dem Storage-Array abgelegt, so dass bei einer Wiederherstellung der Daten kaum Last auf den Produktivservern anfällt. Darüber hinaus soll die Software die Verwaltung virtualisierter Umgebungen vereinfachen – eine zentrale Konsole informiert über die Ressourcennutzung und die Speicherauslastung virtueller und physikalischer Infrastrukturen. Geschraubt hat CommVault ferner an der integrierten Deduplizierungsfunktion. Neben der Entfernung redundanter Daten auf dem Backup-Ziel erfolgt nun bereits Client-seitig eine Eliminierung doppelter Informationen. Auf diese Weise verringert sich schon vor dem Transport der Daten deren Volumen; der Hersteller spricht von einer Reduzierung des Backup-Fensters von bis zu 30 Prozent. Was das Tiering von Informationen betrifft, sollen automatische Policies den Bedarf an manuellen Eingriffen minimieren, egal, ob Unternehmen die Daten vor Ort ablegen oder in die Cloud auslagern. Die Lizenzierung erfolgt nach der Anzahl der Server. Das Einstiegspaket mit fünf Servern inklusive Backup- und Deduplizierungsfunktionen schlägt mit 4.050 Euro zu Buche. *(ln)*

CommVault: www.commvault.com/simpana.html

Dedupe für den Mittelstand

Mit der Storage-Appliance **ETERNUS CS800 S2** erweitert **Fujitsu** sein Portfolio an **Speicherlösungen mit integrierter Deduplizierung** um ein Einstiegsmodell für mittelständische Unternehmen. Das Gerät setzt zur Datensicherung auf Festplatten und will mittels der eingebauten Deduplizierung die Kapazitätsanforderungen für das Backup um bis zu 90 Prozent verringern. Auch für die Replikation zwischen unterschiedlichen Standorten sieht der Hersteller die Komponente geeignet und will dabei den Bedarf an Netzwerkbandbreite um den Faktor 20 senken. Das Modell verfügt in der Minimalkonfiguration über eine Kapazität von 4 TByte, lässt sich aber bis 160 TByte ausbauen. Anschluss ans Netzwerk findet die NAS-Appliance je nach Variante über mindestens 5 GBit-Ethernet-Ports. Die größeren Modelle unterstützen zur direkten Erstellung von Bändern Symantecs OpenStorage-API sowie Path-to-Tape und lassen sich zu diesem Zweck mit zwei 8 GBit-FC-Anschlüssen aufrüsten. Maximal stellt das Speicher-Element über NFS beziehungsweise CIFS bis zu 128 Netzwerk-Freigaben bereit. Je nach Skalierung misst ETERNUS CS800 S2 mindestens zwei Höheneinheiten und verbraucht 600 Watt Energie. Die neue Produktreihe ist ab sofort erhältlich und kostet je nach Ausstattung knapp 10.000 Euro. *(ln)*

Fujitsu: http://de.fujitsu.com/products/storage/

Fujitsu richtet sich mit ETERNUS CS800 S2 vor allem an mittelständische Unternehmen und verspricht verringerte Backup-Zeiten durch Deduplizierung

Datenfilter auf allen Kanälen

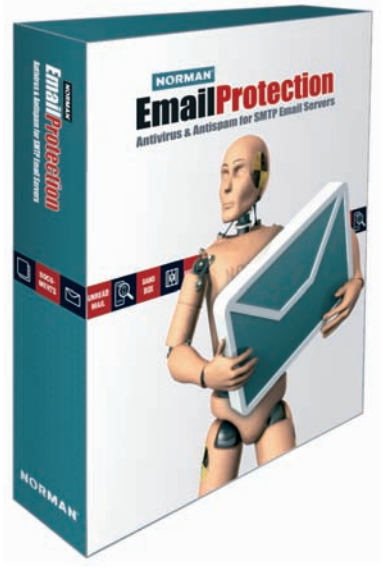
DeviceLock bietet **Version 7** der gleichnamigen Software DeviceLock an. Das neue Release vereint wichtige Funktionen zur **Inhaltsfilterung** und **Überwachung der Netzwerkkommunikation**. Zusätzlich zur Zugriffskontrolle für Schnittstellen und Peripheriegeräte besteht DeviceLock 7.0 aus zwei neuen, getrennt lizenzierten Komponenten: ContentLock, dem Modul zur Überwachung und Filterung von Inhalten und NetworkLock, dem Modul zur Kommunikationskontrolle im Netzwerk. ContentLock erkennt mehr als 80 Dateiformate sowie Datentypen und extrahiert und filtert die Daten, die auf Wechsellaufwerke und Plug&Play-Speichergeräte kopiert werden. Dasselbe geschieht mit Daten, die über andere Ein- und Ausgabekanäle der Computer übertragen werden. NetworkLock ergänzt das Paket um Port-unabhängige Netzwerkprotokollierung, Applikationserfassung und -filterung, Meldungs- und Sitzungswiederherstellung mit Datei-, Daten- und Parameterextraktion sowie Ereignisprotokollierung und Datenspiegelung. Durch die Integration von ContentLock und NetworkLock unterstützt DeviceLock 7.0 Inhaltsüberwachung und -filterung gängiger Netzwerkprotokolle und Anwendungen wie SMTP, HTTP/S, Instant Messenger, S/FTP oder Telnet. DeviceLock 7.0 unterstützt zudem BitLocker To Go, die in Windows 7 integrierte Datenverschlüsselung für Wechseldatenträger. Anwender der Version 6.4.1 können kostenlos upgraden. Bei 100 bis 249 Rechner kostet die Suite 72 Euro – jeweils 18 Euro für DeviceLock und NetworkLock sowie 36 Euro für ContentLock. *(dr)*

DeviceLock: www.devicelock.de

Mehr Sichtbarkeit im Netzwerk

SonicWALL bringt **SonicOS 5.8** für die Produktlinien der **Next Generation Firewalls** auf den Markt. Das neue Release bietet einen erweiterten Funktionsumfang für die intelligente **Applikationsüberwachung und -kontrolle**. Die Software umfasst ein Tool für die Analyse und Visualisierung, so dass sich IT-Verantwortliche alle Anwendungen sowie den damit entstehenden Datenverkehr grafisch darstellen lassen können. Mit SonicOS 5.8 erkennen Administratoren, welche Ressourcen für Anwendungen oder Benutzer aktuell zur Verfügung stehen beziehungsweise zur Verfügung gestellt werden müssen. Auf Basis dieser in Echtzeit bereitstehenden Informationen ist es nun möglich, die jeweilige benötigte beziehungsweise gewünschte Bandbreite für diese Anwendungen zu definieren und zu vergeben. Zudem sehen IT-Verantwortliche, welche unerwünschten Anwendungen Mitarbeiter nutzen und können den Start dieser Applikationen blockieren. Daneben bietet Sonic-OS 5.8 Verbesserungen bezüglich der Sicherheit und des Schutzes vor Malware. So nutzt SonicWALL das eigene Netzwerk Global Response Intelligent Defense (GRID), das in Echtzeit Millionen von Datenpunkten analysieren und Malware und Bedrohungen erkennen soll. Ab sofort ist Version 5.8 auf dem Markt. Das Visualisierungstool ist ein kostenfreier Bestandteil von Sonic-OS 5.8 und verfügbar für die Produktlinien TZ und NSA der aktuellen fünften Generation. Die Application-Firewall ist Bestandteil der kostenpflichtigen GAV/IPS-Subscription. Der Preis für ein Jahr beginnt bei 235 Euro für das Modell TZ 210 und geht bis rund 10.000 Euro für die NSA8500. *(dr)*

SonicWALL: www.sonicwall.de



Soll dank Echtzeitdaten noch besser vor E-Mail-Gefahren schützen: Norman Email Protection 5.0

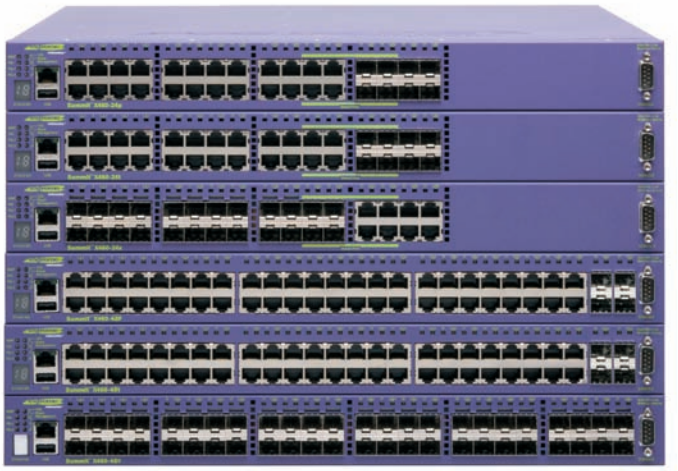
E-Mailschutz dank Echtzeitdaten

Norman stellt die **E-Mail-Management-Lösung Norman Email Protection** mit neuen Funktionen vor. **NEP 5.0** bietet ein weiterentwickeltes Sender Reputation-System, das die E-Mail-Reputation in Echtzeit analysiert. Die Server des Reputation-Systems werden alle fünf Minuten aktualisiert und reagieren damit unmittelbar auf Veränderungen der Absender-Reputation. Ebenfalls neu ist die Möglichkeit, den Quarantäne-Report zum Durchsehen an eine andere Person weiterzugeben. Für den Zugriff ist der Berechtigungsnachweis des Account-Inhabers nicht notwendig. Als Add-on schützt die Komponente "Policy Management" Unternehmen vor Datenverlusten und Datendiebstahl per E-Mail. Die Anwenderunternehmen können mit der Funktion die Einhaltung von Richtlinien zu Inhalten von E-Mails überwachen. NEP 5.0 bindet Microsoft Exchange 2010 vollständig ein und übernimmt die automatischen Whitelists "Adress Book Contacts" aus Microsoft Exchange 2007/2010 und "Safe Senders" aus Microsoft Exchange 2010 in die Scan-Engine. Lotus Domino und alle weiteren Server, die mit dem SMTP-Standard arbeiten, werden ebenfalls unterstützt. Ab sofort ist die neue Version zu haben. Der Spamschutz plus Virenschutz für bis zu 25 Mailboxen mit einer Laufzeit von zwei Jahren kostet 960 Euro, mit Policy Management 1.440 Euro. *(dr)*

Norman: www.norman.com/products/email_protection/de

Vielseitige GBit-Switches

Extreme Networks stellt mit der Serie **Summit-X460** drei **GBit-Ethernet-Switches** mit fester Konfiguration vor. Die Switches gibt es mit Optionen für **28, 48 und 52 Ports** sowie Kupfer, Glasfaser und Power-over-Ethernet (PoE). Neben Standard-PoE-Geräten (802.3af) werden auch PoE-Plus-kompatible Geräte (802.3at) mit bis zu 30 Watt Leistungsaufnahme an allen Ports unterstützt. Die redundanten Netzteile können dabei die Last untereinander verteilen und PoE-Plus-Ports Priorität erhalten. Zudem können IT-Verantwortliche bis zu acht Switches in einem virtuellen Chassis zusammenfassen. Dabei lassen sich die Geräte entweder über das SummitStack-Modul mit 40 GBit/s, über das neue SummitStack-V80-Modul mit 80 GBit/s oder über 10-GBit-Ethernet mit dem neuen SummitStack-V und dem 10-GBit-Ethernet-Modul XGM3-2sf untereinander verbinden. Sämtliche X460-Switches basieren auf dem hochverfügbaren Betriebssystem ExtremeXOS, das einen durchgehenden Betrieb, einfache Administration und operationale Effizienz ermöglichen soll. Die Switches sind zudem mit speziellen Funktionen für den Einsatz als Top-of-Rack-Switches in Rechenzentren ausgestattet. Hierzu zählen eine Luftführung zur Kühlung von vorne oder der Seite nach hinten. Zudem unterstützen die Geräte für den Übergang zu virtualisierten Netzwerken und der Cloud die "Direct Attach"-Switching-Architektur für Rechenzentren. Diese lagert die Switching-Funktionen von Hypervisoren auf die physikalischen Switches aus. Ab rund 4.500 US-Dollar sind die Geräte erhältlich. *(dr)*



Die Switches der Summit-X460-Reihe bilden bei Bedarf den Übergang zur Cloud

Extreme Networks: www.extremenetworks.com

Sicherer Zugang via VDSL

LANCOM Systems erweitert sein **VPN-Router-Portfolio** um den **VDSL-Router 1681V**. Das Gerät erlaubt die nahtlose Integration von Außenstellen, Partnerfirmen oder die Anbindung mobiler Nutzer über **IPSec-VPN**. Der Router bietet neben dem integrierten VDSL-Modem vier frei konfigurierbare Ports für LAN und WAN (für Zwei-Kanal-Load-Balancing und Backup-Verbindungen mit zusätzlichen ADSL-, SDSL-, UMTS- oder Kabel-Modems), DMZ, VLAN, Monitoring sowie eine ISDN-Schnittstelle für Remote Control, LANcapi und Dynamic VPN. Fünf VPN-Kanäle inklusive Hardwarebeschleunigung sind serienmäßig verfügbar, eine Zusatzoption stockt diese auf 25 Kanäle auf. Außerdem bietet der Router bis zu acht virtuelle IP-Netze und ermöglicht damit eine flexible Mehrfachnutzung des LANs und der WAN-Schnittstelle. Das Gerät verfügt daneben über einen USB-Port, der wahlweise als Printserver oder zur Absicherung der VDSL-Verbindung über UMTS Verwendung finden kann. Als UMTS-Modem dient ein handelsüblicher USB-Stick, die Umschaltung auf die Mobilfunkverbindung erfolgt automatisch bei Ausfall der Hauptverbindung. Die integrierte Firewall mit Stateful Inspection, Intrusion Detection und Denial-of-Service Protection soll das Netzwerk vor Attacken aus dem Internet schützen. Die mitgelieferten Management-Tools bieten neben der Fernwartung ganzer Installationen und komfortablen Setup-Assistenten auch eine vollständige Echtzeitüberwachung und Protokollierung. Backup- und High-Availability-Funktionen sollen den unterbrechungsfreien 24-Stunden-Betrieb garantieren. Der LANCOM 1681V ist ab sofort für 599 Euro erhältlich. *(dr)*

Der Router 1681V von LANCOM verbindet über VDSL und UMTS

LANCOM Systems: www.lancom-systems.de

Das Netzwerk im Blick – immer und überall

PRTG to Go: mobiles Network Monitoring mittels iPhone, iPad, Blackberry & Co.

Monitoring für die Hosentasche: Viele Administratoren kennen das Problem, dass sie gerade unterwegs sind und ausgerechnet dann im Unternehmen ein schwerwiegender Netzwerkfehler auftritt. Paessler hat genau für diese Situation Lösungen für ein mobiles Monitoring entwickelt. Grundlage ist die Netzwerküberwachungslösung PRTG Network Monitor der Paessler AG. Verschiedene Benutzeroberflächen ermöglichen den Zugriff über mobile Geräte wie iPhone oder iPad, Blackberry, Android oder Windows Mobile. So haben Administratoren alle Informationen zum Zustand ihrer IT-Infrastruktur jederzeit und überall im Blick.

Ein funktionierendes Netzwerk ist die Grundlage für einen reibungslosen Geschäftsbetrieb. Denn Ausfälle von Mailservern, Webshops, ERP-Systemen etc. bzw. Leistungseinbrüche verursachen oft enorme Schäden. Die Verantwortung für das einwandfreie Funktionieren der IT-Infrastruktur liegt in der Regel beim Administrator, und zwar rund um die Uhr und unabhängig von seinem Aufenthaltsort. Aus diesem Grund ist es unerlässlich, permanent über den Zustand des Netzwerks informiert zu sein bzw. bei Problemen umgehend alarmiert zu werden.

PRTG Network Monitor ist eine umfassende Monitoring-Lösung, die Netzwerke aller Art und Größe kontinuierlich überwacht, die gesammelten Daten auswertet und übersichtlich darstellt. Im Bedarfsfall alarmiert das System den Verantwortlichen über unterschiedliche Kanäle. Neben einer auf Ajax basierenden Web-Oberfläche verfügt PRTG über ein zweites, reduziertes „Mini-HTML-Interface". Dieses ist speziell für kleine Bildschirme und Anbindungen mit geringer Bandbreite konzipiert, um einen einfachen und schnellen Zugang zum PRTG-Server zu gewährleisten. Es liefert übersichtliche Sensor-Listen, Tabellen und Graphen mit Echtzeitinformationen. Der Administrator ist so jederzeit über den Status seines Netzwerks auf dem Laufenden.

Mobiler Monitoring-Assistent iPRTG

Neben dem „Mini-HTML-Interface" bietet Paessler mit iPRTG eine App für mobile Apple-Geräte wie iPhone, iPod oder iPad an. Die Anwendung ist für die Bedienung über Touchscreen optimiert und bietet komfortable Features wie beispielsweise das automatische Anmelden am PRTG Server. Mit der aktuellen Version 2.1 lässt sich iPRTG jetzt auch mit dem iPhone 4, dem iPod Touch oder dem iPad optimal nutzen.

Ob iPRTG oder „Mini-HTML" – mit PRTG profitieren Administratoren von einer höheren Mobilität bei maximaler Sicherheit. Der Stressfaktor wird erheblich gesenkt, wenn sie orts- und zeitunabhängig über den Status ihres Netzwerks up to date sind und wissen, dass sie im Notfall zuverlässig alarmiert werden (beispielsweise über SMS, E-Mail etc.) und rechtzeitig eingreifen können.

iPRTG Netzwerk-Monitoring via iPhone oder iPad

Im Überblick – iPRTG zeigt die folgenden Informationen an:

- **Statusleiste:** Der aktuelle Status aller Sensoren steht immer ganz oben (z.B. wie viele Sensoren sich im Status „Fehler", „OK", „Pause" usw. befinden).
- **Startseite (Home):** Zeigt die Favoriten-Sensoren und deren aktuellen Status an.
- **Geräte:** Stellt den „Gerätebaum" mit Gruppen und Geräten dar.
- **Sensoren:** Zeigt verschiedene Sensorlisten aus der individuellen PRTG-Konfiguration an (schnellster/langsamster Ping, höchste/niedrigste Bandbreite und viele andere).
- **Alarme:** Listet alle Sensoren, die sich in einem Alarm-Status befinden („Ungewöhnlich", „Warnung", „Fehler").
- **Maps:** User können eine Map einfach durch Tippen auswählen und anzeigen.

Die Vollversion von iPRTG kann ab sofort im iTunes App Store zu einem Preis von 15,99 Euro bezogen werden. Wer iPRTG bereits nutzt, kann kostenfrei auf die aktuelle Version 2.1 upgraden. Weitere Informationen zu iPRTG und ein Video stehen unter http://www.de.paessler.com/iPRTG zur Verfügung.

PAESSLER®

Paessler AG
Burgschmietstraße 10
D-90419 Nürnberg
Tel.: +49 (911) 7 39 90 30
Fax: +49 (911) 7 39 90 31

E-Mail: info@paessler.com
URL: www.de.paessler.com
Ansprechpartner:
Dorte Winkler

SNW Europe, 26. und 27. Oktober, Frankfurt am Main

Blick in die Zukunft

von Lars Nitsch

Kurz und knackig – unter diesem Stichwort lassen sich die beiden Veranstaltungstage der Storage Networking World (SNW) in Frankfurt einordnen. Auch wenn das Stelldichein der Speicher-Branche auf zwei Tage eingedampft wurde, bot sich den Besuchern genügend Gelegenheit, neben den großen Themen wie Cloud Computing in Theorie und Praxis ins Detail zu gehen und sich etwa mit den technischen Spezifikationen neuer SSD-Generationen auseinanderzusetzen. IT-Administrator war vor Ort und hat sich über Neuigkeiten, Schlagworte und Insider-Wissen schlau gemacht.

Das Motto der Storage-Messe lautete in diesem Jahr "The Power of 3" – darauf anspielend, dass die SNIA (Storage Networking Industry Association) neben der klassischen SNW Europe auch die beiden Kongresse "Datacenter Technologies" und "Virtualization World" unter das Dach des Frankfurter Congress Centers gebracht hatte. Die meisten der insgesamt fast 1.650 Aussteller und Besucher begrüßten zwar den Virtualisierungs-Schwerpunkt, konnten mit der Hinzunahme des recht weiten Begriffs des Rechenzentrums aber oft nicht allzu viel anfangen. Die SNW ist und bleibt für das Gros der Gäste der klassische Treffpunkt der Speicher-Branche, sollte laut Meinung der Teilnehmer ihre Wurzeln nicht vergessen und sich nicht unnötig verwässern lassen.

Am Konzept hatte sich trotz der inhaltlichen Erweiterung nichts geändert: In der Ausstellungs-Halle konnten sich Storage-Verantwortliche über neue Produkte informieren sowie Geschäftskontakte knüpfen und pflegen, während in nahezu 150 technischen Sessions sämtliche Bereiche der Speicher-Bereitstellung zur Sprache kamen. Erfreulich war hierbei, dass durch das breite Angebot die meisten Vorträge zwar gut besucht, nicht aber heillos überfüllt waren, wie dies in den vergangenen Jahren ab und an der Fall war.

Quelle: Angel Business Communications

Cloud Computing in aller Munde

Viel diskutiert wurde wie erwartet die Datenwolke. Bemerkenswert hierbei war, dass sich bei der Abwägung des Nutzens von Cloud Computing weder Fachbesucher noch Hersteller auf eine gemeinsame Einschätzung einigen konnten. Von "in der jetzigen Form ist die Cloud unbrauchbar", dem klassischen "alter Wein in neuen Schläuchen" über "Cloud Computing ist kein Thema für den Mittelstand" bis hin zu "die gezielte Auslagerung von Daten wird sich auch in Deutschland bald durchsetzen" war ein weites Spektrum an O-Tönen zu vernehmen. Insgesamt lässt sich jedoch festhalten, dass die Zahl der Fundamental-Skeptiker abnimmt, die Cloud Computing als reines Buzzword und hohlen Marketing-Sprech verurteilen.

Gründe für eine ernsthafte Beschäftigung mit dem Thema sind zum einen die verstärkte Existenz von deutschen Cloud-Anbietern oder zumindest im Inland stehenden Rechenzentren. Rechtliche Unwägbarkeiten sollten durch diesen lokalen Faktor und die zu erwartende stärkere Reglementierung zumindest mittelfristig in den Hintergrund geraten. Zum

anderen sehen viele Storage-Verantwortliche und -Hersteller Daten in der Cloud nicht mehr nur als Entweder/Oder-Szenario an. Durch den Einsatz hybrider Cloud-Umgebungen und effizientes Daten-Management gerät die selektive Auslagerung von Daten mehr und mehr in den Fokus. Sensible Informationen bleiben auf diese Weise in Unternehmenshand, während die Masse an Daten, etwa im Bereich E-Mailkommunikation und Datenbanken, von den flexiblen Möglichkeiten der Cloud profitiert.

Deduplizierung und Data Tiering ab Werk

Vom Hype zur handfesten Funktion hat sich die Deduplizierung entwickelt. Während Deduplizierungs-Features noch bis vor kurzem meist als eigene Software von Drittherstellern den Weg ins Rechenzentrum fanden, bieten fast alle Hardware-Hersteller mittlerweile eigene Lösungen an, die bereits ab Werk in die Systeme integriert und meist ohne nennenswerten Aufpreis zu haben sind. Auch hier findet sich wieder eine Verzahnung zum Thema Cloud Computing – durch die signifikante Reduktion der übertragenen Datenmenge lassen sich selbst große Backup-Sätze schnell und unkompliziert über WAN an einen anderen Standort replizieren. Generell scheint der Trend mehr und mehr zu All-in-One-Strukturen zu gehen, in denen ein Storage-Hersteller alle Funktionen anbietet, seien es nun Virtualisierungs-Features, Tools zum Daten-Management oder eben die angesprochene Deduplizierung.

Im Rahmen einer bestmöglichen Kapazitätsauslastung und vor allem einer schnellen Bereitstellung häufig genutzter Daten ist nach wie vor "Data Tiering" in aller Munde. Besonders an Fahrt gewinnt dieses Thema durch den zunehmenden Einsatz von Solid State Disks (SSD). Auch wenn sich die Preise für Flash-basierte Datenträger, die für den Unternehmenseinsatz geeignet sind, noch lange nicht an herkömmliche Magnetspeicher angeglichen haben, kann die Verwendung von

Wer zwischen zwei Sessions einmal pausieren wollte, konnte sich die Zeit mit Surfen vertreiben

SSDs für "hot data" selbst für den Mittelstand durchaus schon eine Alternative sein. In diesem Zusammenhang erwarten viele Hersteller eine Änderung der physikalischen Zusammensetzung der weniger wichtigen Tiers. Wie genau das Resultat dieser Umschichtung aussehen wird, darüber gibt es jedoch auseinandergehende Meinungen – während einige das komplette Verschwinden von SAS-Laufwerken prognostizieren (die wirklich wichtigen Daten finden auf SSDs Platz, für den Rest reicht SATA), sehen andere das Aussterben der weniger leistungsfähigen SATA-Speicher (SAS wird immer günstiger und bedarf deshalb keiner noch billigeren Alternative).

Die Zukunft: SSDs mit 8 TByte

Was die kleinste logische Einheit der Storage-Infrastruktur, den Datenträger, betrifft, gestalten sich die Aussichten generell spannend. IBM etwa geht davon aus, dass magnetische Festplatten schon bald nur noch im 2,5 Zoll-Format produziert würden – selbst die großen Hersteller könnten es sich nicht auf Dauer leisten, sämtliche Magnetspeicher in zwei unterschiedlichen Formfaktoren herzustellen. Noch aufregender stellt sich ein Blick in die Zukunft der SSDs dar: Zum einen dürfte schon bald auch bei Flash-Speichern für den Unternehmenseinsatz der Umstieg auf Multi-Level-Cell-Speicherzellen (MLC) vollzogen sein. Verbesserte Produktionsverfahren und ausgereiftere Technologien sorgen dann für noch mehr Kapazität bei abnehmenden Fehlerraten. Zum anderen soll die PCM-Technologie (Phase Change Memory) nahezu revolutionäre Folgen haben: Durch den Einsatz sogenannter Chalkogenide und Wärme, um zwischen amorphen und kristallinen Zuständen zu wechseln, werden in Zukunft deutlich höhere Dichte-Grade möglich. SSD-Speicher im HD-Format mit 4 oder sogar 8 TByte rücken so in den Bereich des Möglichen.

Selbst wenn derartiges im Moment noch Zukunftsmusik ist – wer wollte, konnte sich auf der SNW sowohl in technischen Details verlieren als auch das große Ganze ins Auge fassen. Die gesunde Mischung aus Informationsmöglichkeiten direkt beim Hersteller und produktneutralen Vorträgen und Hands-on-Workshops war für die meisten Teilnehmer der Hauptanreiz für den Besuch der Fachmesse. Termin und Ort für nächstes Jahr stehen übrigens schon fest: Am 2. und 3. November 2011 wird die Storage-Gemeinde wieder nach Frankfurt pilgern.

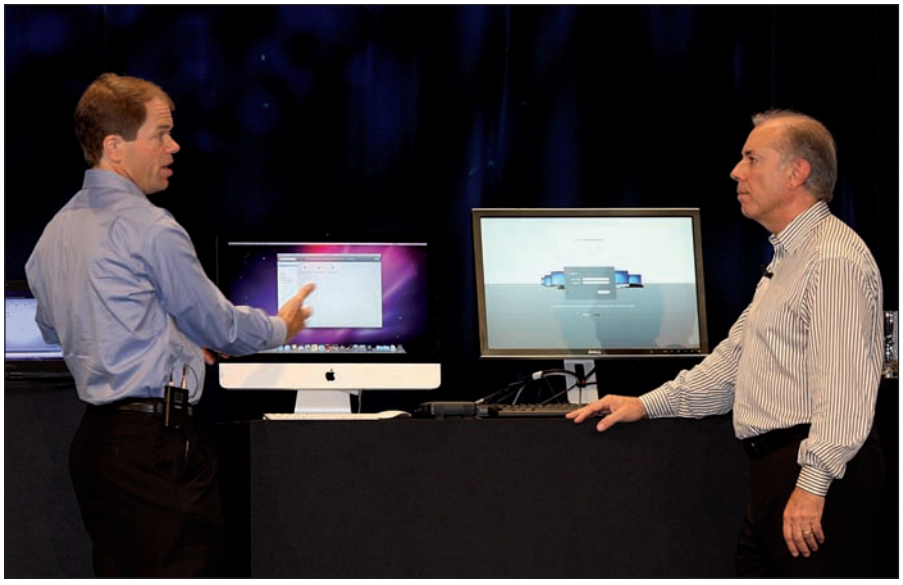
Citrix Synergy, 6. bis 8. Oktober 2010, Berlin

Europa-Premiere

von Christian Knermann

Anfang Oktober fand im Estrel Convention Center in Berlin die Citrix Synergy 2010 statt. Die weltweite Kundenveranstaltung des Herstellers – bislang auf die USA beschränkt – bekam damit erstmalig einen Ableger in Europa und war mit mehr als 3.000 Besuchern aus über 50 Ländern ausgebucht. IT-Administrator war für Sie vor Ort.

Nach einem ersten Block von parallelen Sitzungen stand zunächst die zweistündige Keynote auf dem Programm, in deren Verlauf Citrix President Mark B. Templeton die Themen Virtual Meetings, Virtual Desktops und Virtual Datacenters fokussierte. Mit der nächsten Generation der Online-Produkte aus der GoTo-Meeting-Familie sollen Web- und Videokonferenzen zusammenwachsen. Eine Erweiterung names HDfaces wird dabei Video-Kommunkation mit einer Auflösung von bis zu 720 Pixeln ermöglichen, was mit Citrix-Mitarbeitern in den USA als Gegenstelle eindrucksvoll demonstriert wurde. HDfaces befindet sich derzeit im Beta-Test und soll Anfang 2011 ohne Aufpreis als Teil von GoToMeeting verfügbar werden.



Citrix-Präsident Mark B. Templeton (rechts) bei der Demonstration des neuen Citrix Receiver

Interessant wurde es anschließend im Bereich zur Desktop-Virtualisierung. Hier kündigte Templeton mit XenDesktop 5 bereits die nächste Hauptversion an. Diese stellt er unter das Motto "From wow to how". Nachdem viele Kunden sich von den Funktionen der bisherigen Versionen begeistert gezeigt hätten, stünden sie nun vor der Frage, wie diese im Unternehmen implementiert werden könnten. Die Antwort soll das neue XenDesktop 5 liefern und die Bereitstellung virtueller Desktops wesentlich vereinfachen. Eine wichtige Rolle spielt dabei der neue Desktop Director. Mit dieser webbasierten Konsole lassen sich im operativen Betrieb die laufenden Desktops überwachen und innerhalb weniger Minuten neue Desktop-Instanzen erzeugen.

Templeton kam daraufhin zum XenClient, dem wenige Tage zuvor veröffentlichten Client-Hypervisor. Er kündigte an, dass neben Dell- und HP-Notebooks zukünftig auch Lenovo-Geräte ab Werk mit dem XenClient bestellt werden können. Nach einer Demonstration des XenClient folgte die Überleitung zum dritten Baustein, dem virtuellen Rechenzentrum. Hier soll das Feature Pack 1 für den XenServer 5.6 weitere Verbesserungen im Hinblick auf die Storage-Anbindung bringen und die Basis sowohl für virtuelle Desktops als auch für Cloud-Angebote liefern. Den Abschluss bildete ein Ausblick auf den kommenden Citrix Receiver für das iPad iOS 4.2. Dieser wird Verbesserungen bei der Touch-Bedienung von Windows-Applikationen mit sich bringen und zudem Multi-Tasking unterstützen, so dass die Verbindung zu veröffentlichten Anwendungen bestehen bleibt, auch wenn der Receiver im Hintergrund läuft.

Über die angekündigten Neuerungen wie auch die bestehenden Produkte konnten sich die Besucher im Laufe der nächsten Tage in über 60 Breakout-Sessions detaillierter informieren. Parallel dazu liefen die "Learning Labs" – drei- bis vierstündige Schulungen, in denen Citrix-Techniker den Umgang mit den verschiedenen Lösungen vermittelten. Die nächste europäische Citrix Synergy wird im Oktober 2011 in Barcelona stattfinden. *(dr)*

LANCOM

. . . connecting your business

Made
in
Germany

Das beste WLAN aller Zeiten!

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

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

Ob im kleinen Netz mit wenigen Access Points, im Controller-basierten WLAN mit Tausenden von Geräten, für den Hotspot-Betrieb oder im Freien: 802.11n WLAN von LANCOM sorgt überall für ungekannte Leistungsfähigkeit – auf Wunsch sogar ganz dezent ohne sichtbare Antennen.

Kundenstimmen unter: www.lancom.de/referenzen

INNOVATIONSPREIS-IT
KATEGORIESIEGER
2009
initiative mittelstand
STORAGE/NETZWERKE

LANCOM OAP-310agn

LANCOM
Systems

www.lancom.de

Im Test: Fluke AirCheck Wi-Fi Tester

Handlicher Wellenreiter

von Jürgen Heyer

Bei der WLAN-Nutzung in Unternehmensnetzen ist es überaus wichtig, die Installation regelmäßig hinsichtlich Verfügbarkeit, Sicherheit, tatsächlicher Nutzung und Störungen zu überprüfen. Für eine komfortable und einfache Analyse hat Fluke Networks einen neuen, kompakten Handheld-Tester entwickelt, um schnell und unkompliziert umfassende WLAN-Informationen zu ermitteln. IT-Administrator ging mit diesem Gerät zum "Wellenreiten" und hat sich dessen Leistungen im Test genauer angesehen.

Viele Unternehmen setzen bei der internen Vernetzung zunehmend auf WLAN. Dies ist vor allem in Außenstellen beliebt, lassen sich doch so die beträchtlichen Kosten für eine aufwändige Festverkabelung sparen. Eine passende Netzabdeckung ist bei der Einrichtung eines oder mehrerer WLANs ebenso wichtig wie die Vermeidung von Störungen, damit den Mitarbeitern allerorts eine ausreichende Performance zur Verfügung steht. So muss der Administrator beispielsweise bei einer engmaschigen Abdeckung vermeiden, dass mehrere Access Points (APs) mit gleicher SSID, deren Sendebereiche sich womöglich ein wenig überlappen, den gleichen Kanal nutzen.

Wichtig ist zudem die konsequente Umsetzung der Sicherheitseinstellungen, damit sich keine Unternehmensdaten ungewollt verflüchtigen oder unerwünschte Hacker auf drahtlosem Weg in das Firmennetz eindringen. Dass professionelle WLAN-APs neuester Technologie alle möglichen Sicherheitsfeatures besitzen, ist heutzutage durchwegs Standard, wichtig ist aber auch deren Nutzung beziehungsweise Aktivierung. Neben der sorgfältigen Konfiguration ist daher eine abschließende unabhängige Kontrolle von außen, also aus Client-Sicht, auf jeden Fall zu empfehlen.

Prinzipiell ist es möglich, die genannten Aspekte mittels eines WLAN-fähigen Notebooks und entsprechender Scansoftware zu überprüfen – letzten Endes aber ist diese Vorgehensweise ziemlich umständlich. Weitaus mehr Komfort verspricht der Einsatz eines speziellen Messgerätes wie des AirCheck Wi-Fi Testers von Fluke Networks. Insgesamt bietet der Hersteller mehrere Lösungen zur WLAN-Analyse an, wobei das hier getestete Gerät in erster Linie für eine schnelle Analyse und einen möglichst mobilen Einsatz gedacht ist.

Betriebsbereit in wenigen Sekunden

Der AirCheck Wi-Fi-Tester ist in der Tat ein sehr handliches Gerät mit robustem Gehäuse, das in der von Fluke Networks bekannten, gelb-orangen Signalfarbe gehalten ist. Es wird standardmäßig mit einer Tragetasche ausgeliefert, in der das Netzgerät und sonstiges Zubehör (CDs, USB-Kabel, Kurzanleitung) Platz finden. Vor der ersten Inbetriebnahme ist es wichtig, den Akku über mehrere Stunden hinweg zu laden. Die Betriebsdauer einer Ladung ist mit fünf Stunden angegeben und ermöglicht damit auch längere Analysen. Optional ist eine automatische Abschaltung nach zehn Minuten Inaktivität einstellbar. Besonders positiv fällt die sehr schnelle Einsatzbereitschaft auf, denn rund drei Sekunden nach dem Einschalten beginnt der Tester mit dem Scan der WLAN-Kanäle. Spätestens dann dürfte die erfreulich helle und sehr gut lesbare LCD-Anzeige in der Auflösung 320 x 240 Punkte auffallen. Die Bedienung erfolgt über insgesamt elf Tasten. Fünf Tasten bilden eine Cursorsteuerung mit Auswahl. Zwei Tasten werden variabel genutzt, wobei die aktuell gültige Belegung stets im Display ersichtlich ist. Insgesamt halten wir die Steuerung für sehr intuitiv, und es bereitete von Anfang an keinerlei Probleme, den Tester sicher und zielstrebig zu bedienen.

Nach dem Einschalten stehen die vier Rubriken "Netzwerke", "Access Points", "Kanäle" und "Tools" zur Verfügung. Bei der ersten Verwendung benötigt der Nutzer zuerst den Tools-Bereich, um einige Konfigurationseinstellungen vorzunehmen. Dazu zählen etwa die Auswahl der Sprache sowie die Länderangabe, da länderabhängig einige Kanäle nicht genutzt werden dürfen, was die Anzeigelegende auch berücksichtigt. Anzumerken ist hier,

dass der Tester immer alle Kanäle scannt, so dass offensichtlich wird, wenn ein AP falsch eingestellt ist und einen nicht zugelassenen Kanal nutzt.

Bild 1: Leicht verständliche, farbige Icons ermöglichen eine komprimierte Anzeige aller wichtigen Informationen

Darüber hinaus kann der Benutzer unter anderem vorgeben, welche Bänder (2,4 oder 5 GHz) er aktivieren möchte. Außerdem sollte er Datum und Uhrzeit richtig setzen, damit dies bei Aufzeichnungen korrekt dokumentiert wird. Hinsichtlich der Visualisierung lassen sich eigene Werte für die farbliche Darstellung (rot, gelb, grün) der Schwellwerte Signalstärke, Störungsgrad und S/N-Verhältnis vorgeben. Weiterhin hat der Administrator Zugriff auf einen internen Dateisystembereich, um Profile zu laden und zu speichern sowie Dateien wie Sitzungsaufzeichnungen umzubenennen oder zu löschen. Abschließend hat Fluke im Tools-Bereich eine in der Regel weniger benötigte Client-Prüfung implementiert, die nicht nach APs sucht, sondern nach WLAN-Clients in der Umgebung. Der Tester zeigt dann die MAC-Adressen der gefundenen Geräte an, außerdem die Feldstärke und den genutzten Kanal.

Übersichtliche Rubriken

Während die Tools-Rubrik in erster Linie den Zugriff auf die individuellen Einstellungen gewährt, dienen die übrigen drei Rubriken der WLAN-Analyse aus verschiedenen Blickrichtungen.

WLANs und APs auf einen Blick

So listet der Tester in der ersten Ansicht der Rubrik Netzwerke alle gefundenen WLAN-Netze auf. Gut ist die komprimierte Listenübersicht, die bereits erste Informationen wie SSID, Feldstärke, Anzahl der gefundenen Access Points für jedes WLAN, mögliche Betriebsvarianten (802.11a, b, g oder n) und die aktive Verschlüsselung liefert. Fluke Networks nutzt dabei das farbige Display konsequent, um möglichst viele Informationen zu vermitteln. Beispielsweise ist das Verschlüsselungssymbol bei einer WEP-Verschlüsselung orange und bei einem WPA-Verfahren grün, bei einem offenen Netz ist das symbolisierte Schloss offen und zudem rot dargestellt. Vorteilhaft ist weiterhin, dass der Tester einmal gefundene Netze, die beispielsweise aufgrund schwankender Bandbreite nicht permanent erreichbar sind, solange in der Übersicht behält, bis der Bediener diese per Knopfdruck bereinigt. Nicht erreichbare Netze werden dabei ausgegraut dargestellt. In der Listenansicht ist über eine der beiden variabel belegbaren Tasten eine Legende aufrufbar, die alle Spalten und alle möglichen Symbole kurz beschreibt. Dies erspart dem Anwender den Blick in die Bedienungsanleitung.

Möchte der Gerätenutzer mehr über ein WLAN erfahren, wählt er dieses aus und kommt so in die Übersicht der dazugehörigen Access Points. Klickt er nun einen AP an, so erhält er zu diesem die Detaileinstellungen aufgelistet: aktuelle Signalstärke, Rauschen und Signal-/Rauschabstand, genutzter Kanal, MAC-Adresse und daraus ermittelter Hersteller, SSID, BSSID, Verschlüsselungsart und -typ wie WEP, WPA, WPA2, AES und TKIP sowie eine eventuelle Landeseinstellung. Die Angaben zur Signalstärke und zu Störungen werden dabei ständig aktualisiert. Gerade für die Verwendung an Orten, an denen viele APs sichtbar sind, ist im AirCheck Tester eine sehr sinnvolle Ordnungsfunktion implementiert. So kann der Anwender jedem AP eine Autorisierung zuweisen wie "Autorisiertes Gerät", "Nachbargerät", "Gastgerät" und "Markiertes Gerät", was jeweils durch ein eigenes Icon symbolisiert

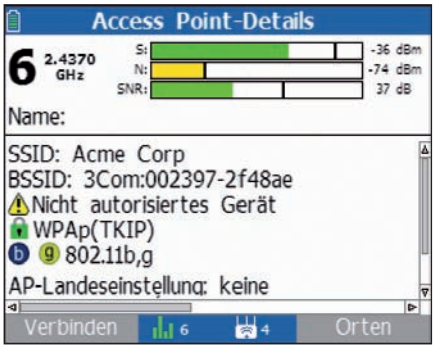


Bild 2: Zu jedem AP liefert der Tester detaillierte Informationen hinsichtlich Verschlüsselung und aktueller Signalqualität

wird. Am Anfang führt das System jeden neu gefundenen AP als "Nicht autorisiertes Gerät", so dass sich auf diese Weise leicht feststellen lässt, wenn sich an einem Ort die Situation ändert und neue APs auftauchen.

Engpässen und Signalrichtungen auf der Spur

Falls den Administrator zu einem AP die Auslastung des genutzten Kanals interessiert, so kann er sich auch diese anzeigen lassen. AirCheck gibt dann an, wie viele APs aktuell den Kanal nutzen und stellt die Auslastung in Prozent als ständig aktualisierte grafische Darstellung über 60 Sekunden dar. Außerdem unterscheidet das Gerät zwischen Signal und Rauschen. Sehr gut lässt sich beobachten, wie beispielsweise bei einer Kopieraktion über das WLAN die Last sprunghaft ansteigt. Engpässe, beispielsweise durch eine kontinuierlich hohe Last bei 80 Prozent und mehr, lassen sich auf diese Weise gut aufdecken.

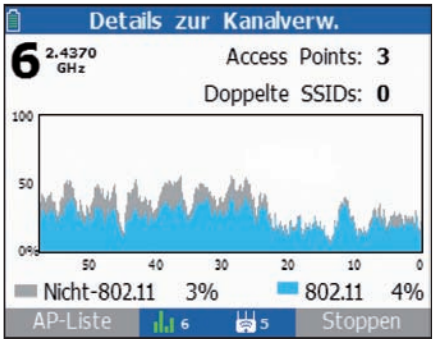


Bild 3: Neben einem Gesamtüberblick lässt sich die Kanalverwendung auch im zeitlichen Verlauf (Zeitfenster fest 1 Minute) verfolgen

Bild 4: Bei einem Verbindungstest meldet sich der Tester wie ein Client bei einem AP an und führt dann diverse Ping-Prüfungen durch

Steigt der Benutzer über die Rubrik Access Points ein, so listet der Tester eben diese auf, unabhängig davon, zu welchen WLANs sie gehören, gibt aber neben dem Namen auch die SSID an. Die Ansicht der Detailinformationen ist verständlicherweise identisch zu derjenigen beim Einstieg über die Rubrik Netzwerke. Nicht erreichbar ist die Ansicht der Kanalauslastung, stattdessen gibt es eine Ortungsfunktion, um die Richtung zu einem AP festzustellen. Die Anzeige der Signalstärke erfolgt optisch und wird zudem akustisch umgesetzt, ähnlich wie bei einem Geigerzähler. Wer des Öfteren APs auf diese Weise ausfindig machen muss, für den bietet Fluke Networks optional eine spezielle Richtantenne an, die sich an die Unterseite des Testers anschließen lässt. Diese Antenne stand uns allerdings nicht zur Verfügung. Ortungsversuche mit der internen Antenne lieferten im Test beim Drehen um die eigene Achse nur eine grobe Richtung – mit der zusätzlichen Antenne dürfte eine deutlich genauere Ortung möglich sein.

Störende Kanäle aufspüren

Sehr interessant für die Analyse von Störungen und für die optimale Verteilung sowie Konfiguration mehrerer APs in einem örtlich begrenzten Bereich erweist sich die Rubrik Kanäle. Hierbei scannt der Tester kontinuierlich alle WLAN-Kanäle im 2,4- und 5-GHz-Band und zeigt an, wie viele Access Points die Kanäle nutzen, sowie, wie hoch Auslastung und Störanteil sind. Über eine Beschriftung der Kanäle in schwarz und rot erkennt der Administrator zudem, welche Kanäle entsprechend der eingestellten Länderkennung überhaupt genutzt werden dürfen. Bei der Auswahl eines Kanals erscheint die schon beschriebene Ansicht über die Auslastung der letzten 60 Sekunden. Weiterhin kann der Bediener zu jedem Kanal die AP-Liste aufrufen und so weiter zu den AP-Details gelangen.

Letztendlich sind viele Ansichten im Tester auf verschiedenen, intuitiven Wegen erreichbar. Für eine spätere Auswertung kann der Anwender Sitzungen abspeichern und mit der weiter unten beschriebenen Software AirCheck Manager öffnen. Eine Sitzung wird standardmäßig unter einem fortlaufenden Namen gespeichert. Für eine bessere spätere Zuordnung lässt sich dieser aber auch individuell festlegen. Ebenfalls implementiert ist eine Verbindungsprüfung, wozu der Tester versucht, sich wie ein Client bei einem AP anzumelden. Dies ist allerdings bei geschützten WLANs nur dann möglich, wenn die Anmeldedaten wie nachfolgend beschrieben im genutzten Profil hinterlegt sind. Eine Eingabe von Authentifizierungsinformationen direkt am Tester ist nicht vorgesehen.

Verwaltung nur über PC-Software

Ein wichtiger Bestandteil des AirCheck Testers ist die mitgelieferte Software Network AirCheck Manager. Die Verbindung für die Kommunikation erfolgt per USB, wobei der Tester nicht benutzbar ist, sobald diese hergestellt wurde. Der interne Speicher des Testers ist als Wechselmedium sichtbar, so dass sich aufgezeichnete Sitzungen leicht übertragen lassen. Die Software greift wahlweise direkt auf den Speicherbereich des Testers zu oder lädt Sitzungs- und Profildateien vom PC. Zweck der Lösung ist das Definieren von Profilen sowie das Auswerten aufgezeichneter Sitzungen. Außerdem lassen sich damit Firmware-Updates einspielen.

Profile per USB

Mit dem im AirCheck Manager eingebetteten Profil Manager kann der Administrator bestehende Profildateien zwischen dem PC und dem Tester kopieren oder verschieben sowie neue Profile anlegen. Ein Profil enthält unter anderem die Informationen zu einem, aber auch mehreren WLANs. Am besten legt der Administrator für unterschiedliche Lokationen eigene Profile an. Dazu trägt er die eingerichteten Netze mit SSID, der IP-Konfiguration (DHCP oder fes-

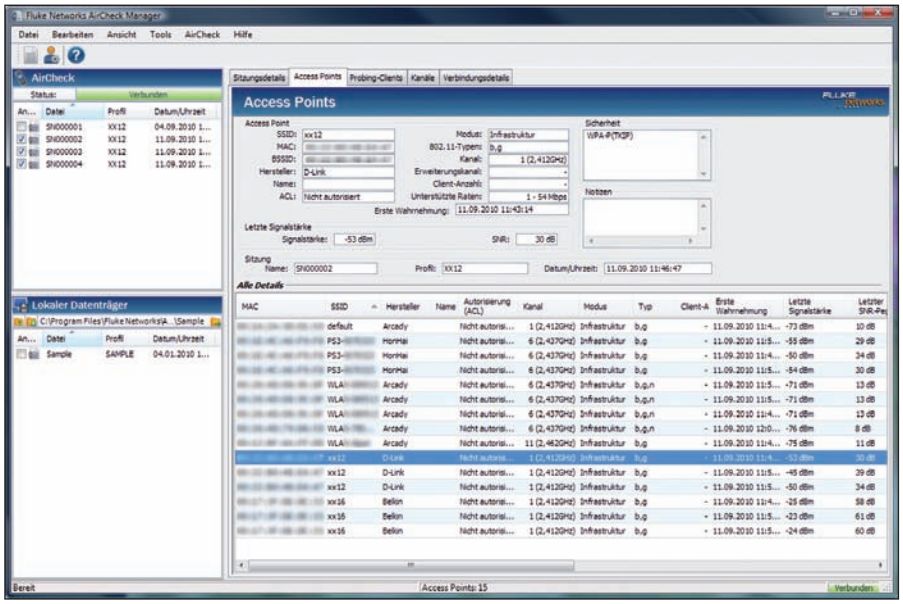


Bild 5: Mit dem AirCheck Manager lassen sich mehrere Sitzungen zugleich öffnen und so die Resultate gut vergleichen

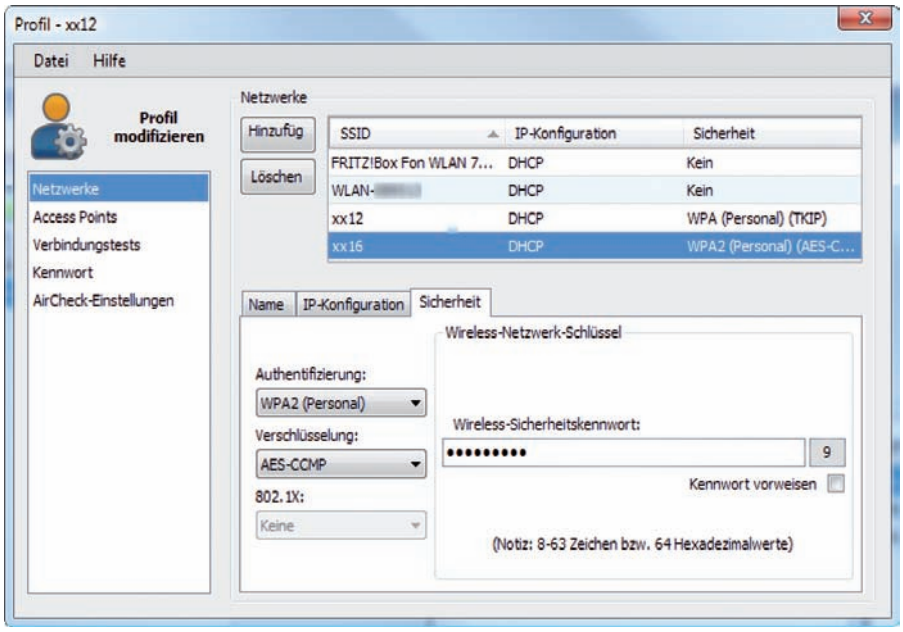


Bild 6: Anmeldeinformationen für Verbindungstests können nur über Profile mit dem AirCheck Tester genutzt werden

te IP-Adresse) sowie den Sicherheitsdaten (Authentifizierung, Verschlüsselung und Schlüssel) ein. Weiterhin kann er APs mit BSSID, Name und Autorisierungsstatus hinterlegen. Für einen individuellen Verbindungstest lassen sich neben den Standardzielen wie Gateway, DHCP- und DNS-Server noch eigene Hostnamen oder IP-Adressen angeben. Zu beachten ist aber, dass diese Tests immer gleich durchgeführt werden, egal, mit welchem der eingetragenen WLANs eine Verbindung zustande kommt. Bezogen auf fest vorgegebene individuelle IP-Adressen wird der Test dann nicht immer zu sinnvollen Resultaten führen. Besser ist es daher, für den Test einzelner WLANs jeweils individuelle Profile zu nutzen.

Als Letztes lassen sich in einem Profil die Einstellungen des Testers (Länderkennung, Schwellwerte, aktivierte Frequenzbänder) vorgeben. Mittels Kennwort ist es schließlich möglich, Profile vor Veränderungen zu schützen. Insgesamt sind die Profile eine gute Möglichkeit, einen AirCheck Tester für den Einsatz an verschiedenen Orten schnell optimal einzustellen. Außerdem lassen sich die Einstellungen damit zügig übertragen oder duplizieren, wenn ein Unternehmen mehrere dieser Geräte einsetzt. Wird das aktive Profil auf einem Tester geändert, so fragt dieser nach dem Abziehen der USB-Verbindung, ob nun das aktualisierte Profil geladen werden soll.

Insgesamt hat uns das Verfahren mit den Profilen überzeugt. Allerdings vermissten wir die Möglichkeit, Profile ohne die PC-Software im Tester ändern oder zumindest für einen Anschaltversuch entsprechende Authentifizierungsinformationen eingeben zu können.

Messergebnisse nicht als Verlauf

Nachdem wir für den Test ein Profil mit den Authentifizierungsinformationen für zwei von uns betriebenen APs angelegt und aktiviert hatten, führten wir einige Anschaltversuche durch und konnten dabei gut verfolgen, wie der Tester umfassende Informationen zum Ablauf des Verbindungsaufbaus inklusive eines kompletten Verbindungsprotokolls lieferte. Problemstellen lassen sich so genau ermitteln.

Bezüglich der Analyse von Sitzungen speichert der Tester stets die Eckdaten, aber keine Verlaufswerte über die Zeit, wie sie bei der Kanalverwendung oder der Verbindungsreichweite in den Diagrammen angezeigt werden. Die Management-Software kann eine oder mehrere Sitzungen gleichzeitig anzeigen. Letzteres hilft enorm beim Finden von Unterschieden. Das Programm liefert grundlegende Detaildaten zum verwendeten Testgerät, weiterhin eine Liste der APs mit entsprechenden Informationen, eine Liste der gefundenen Clients, eine Kanalübersicht mit mittlerer Auslastung und letztem Messwert, Rauschanteilen, Anzahl der APs pro Kanal und gegebenenfalls doppelte SSIDs. Sollte während der Sitzung ein Verbindungstest mit einem oder mehreren APs stattgefunden haben, so kann der Administrator die Verbindungsschritte und auch Ping-Ergebnisse sowie das Verbindungsprotokoll herauslesen.

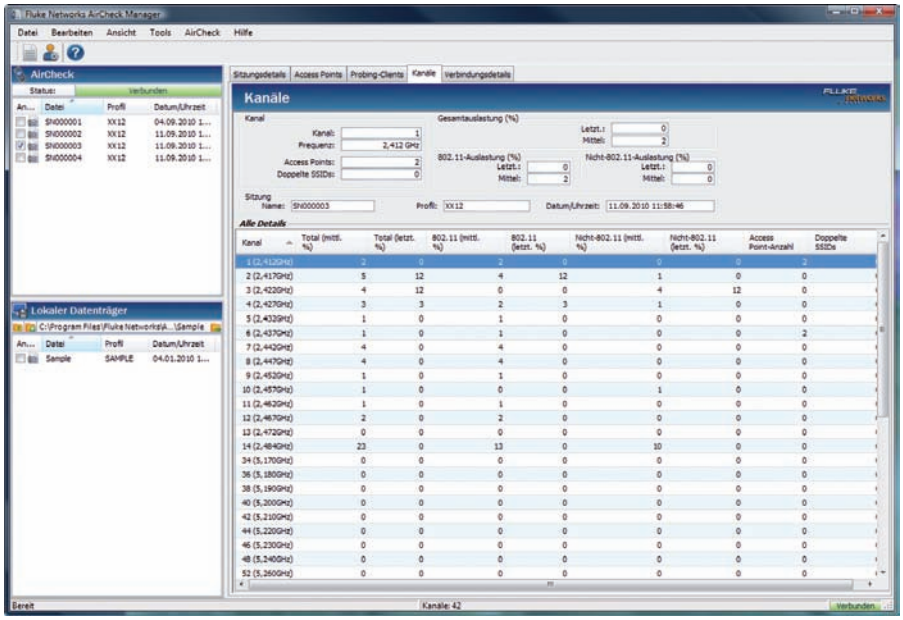


Bild 7: Ein Sitzungsprotokoll enthält Detailangaben zu allen Frequenzkanälen, es werden aber keine zeitlichen Verläufe aufgezeichnet

Insgesamt liefert der Tester umfangreiche Informationen, wobei zu beachten ist, dass die Aufzeichnung von Langzeitanalysen nicht vorgesehen ist. Das Gerät liefert zwar Mittelwerte und zuletzt ermittelte Messwerte, aber keine Verlaufsinformationen (wie beispielsweise die Kanalbelegung über mehrere Stunden). Wer die bereits erwähnte automatische Abschaltung zur Schonung der Akkukapazität nutzt, sollte berücksichtigen, dass bei einer Abschaltung alle Daten der Sitzung verloren gehen, sofern nicht schon vorher etwas gespeichert wurde. Soll also eine spätere Auswertung stattfinden, muss der Nutzer die automatische Abschaltung deaktivieren.

Durchschnittliche Empfindlichkeit

Um die Empfindlichkeit des AirCheck Wi-Fi Testers abschätzen zu können, begaben wir uns mit dem Gerät und zwei Notebooks auf WLAN-Suche, wobei wir auf Letzteren den WLAN-Scanner Vistumbler installierten. Dann suchten wir an mehreren Orten über eine längere Zeit nach vorhandenen WLANs und verglichen die Resultate. Dabei konnten wir feststellen, dass der AirCheck Wi-Fi Tester mit der internen Antenne eine vergleichbare Empfindlichkeit besitzt. Eines der beiden Notebooks fing sogar meist ein oder zwei schwache WLANs mehr ein. Unter praktischen Gesichtspunkten erscheint uns diese vergleichbare Empfindlichkeit durchaus vernünftig, denn nur so lässt sich eine Aussage darüber treffen, ob an einem Punkt die Signalstärke ausreicht, um beispielsweise ein Notebook zu verbinden. Andernfalls würde der Tester eine zu große Netzabdeckung vorgaukeln, die sich in der Praxis dann gar nicht nutzen liesse.

Fazit

Der Fluke AirCheck Wi-Fi Tester erweist sich als einfach zu bedienendes, schnelles Prüfwerkzeug für 802.11a/b/g/n-Netzwerke. Das Gerät analysiert die Netzabdeckung, zeigt Überlastungen von Funkkanälen auf, erkennt HF-Störungen, macht falsche oder uneinheitliche Sicherheitseinstellungen sichtbar und hilft auch bei Client-Problemen. Durch seine robuste Bauweise und eine Akkulaufzeit von fünf Stunden eignet sich der Tester ideal für den mobilen Betrieb. Sehr positiv hervorzuheben sind die schnelle Einsatzbereitschaft innerhalb von wenigen Sekunden sowie die intuitive Bedienbarkeit.

Durch die Möglichkeit, unterschiedliche Profile zu laden, lässt sich der Tester sehr gut an unterschiedlichen Orten einsetzen und dahingehend vorbereiten, dass sich Veränderungen im WLAN-Umfeld wie beispielsweise neue Access Points gut aufdecken lassen. Für Unternehmen, die bei ihrer Vernetzung auf WLAN-Technik setzen, bietet der AirCheck Wi-Fi Tester wertvolle Unterstützung, um die Umgebung mit sicheren Einstellungen aufzubauen und Störungen zu vermeiden. Gut ist, dass sich Sitzungen für eine spätere Auswertung aufzeichnen lassen. Nicht geeignet ist der Tester allerdings für komplexe Langzeitanalysen, da er zwar Mittel- und Schlusswerte speichert, aber keine Verlaufsdaten. *(ln)*

Produkt
Mobiles Testgerät für drahtlose Netzwerke.

Hersteller
Fluke Networks
www.flukenetworks.com

Preis
1.195 Euro

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

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

Bedienung	10
Robustheit des Gehäuses	9
Funktionsumfang des Geräts	8
Funktionsumfang der Software	7
Dokumentation	8

Dieses Produkt eignet sich

optimal für die häufige, schnelle und mobile Analyse größerer WLAN-Installationen.

bedingt für den Einsatz in eher kleinen WLANs. Hier sollten Preis und Nutzen genau gegeneinander abgewogen werden.

nicht für die Aufzeichnung von Langzeitanalysen mit zeitlicher Darstellung von Verfügbarkeiten oder Signalstärken.

Fluke Networks AirCheck Wi-Fi Tester

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

Im Test: Nextragen Trafficlyser TraceSim VoIP

Einfach gute Sprache

von Mathias Hein

VoIP-Messungen, die die QoS-Parameter im Netzwerk überprüfen, bilden die Grundlage für das Gelingen eines VoIP-Projekts. Um die VoIP-Fähigkeit eines oder mehrerer Unternehmensnetzwerke festzustellen, müssen nicht zuerst die geplanten VoIP/UC-Komponenten (Telefone, Server, Gateways) angeschafft und installiert werden. Vielmehr übernehmen VoIP-Simulatoren beziehungsweise -Analysatoren die Aufgabe, hunderte von Anwendern und deren Telefonverhalten nachzubilden und Schritt für Schritt in das Netzwerk einzuspielen. Nextragen bietet mit Trafficlyser TraceSim VoIP ein Simulationswerkzeug zur Evaluierung der Sprachqualität für Voice over IP. IT-Administrator hat die Software hinsichtlich der Messungen der VoIP-Readiness und des laufenden Betriebs getestet.

Die VoIP- und Unified Communication-Technologien stellen besondere Anforderungen an Netzinfrastrukturen. Daher bildet eine umfassende und qualitative Aussage (Messung), ob und welche Teile des vorhandenen Netzwerks VoIP-fähig sind, die Basis für den Umbau der Dienste und der Netze. Dabei liegt das Augenmerk besonders auf folgenden Eigenschaften: Gesprächsqualität, Minimierung der Verzögerungen und die Sicherstellung der Zuverlässigkeit. Bereits kleine Fehler bei der Netzkonfiguration können zu erheblichen Qualitätseinbußen bei den VoIP-Verbindungen führen.

Trafficlyser TraceSim VoIP (TTSV) von Nextragen ist ein Softwaretool zur Simulation von VoIP-Gesprächen und zur Langzeitanalyse der Sprachqualität. Die Testdaten werden an einem beliebigen Netzknoten eingespeist und zu einer oder mehreren Gegenstellen (TraceSim VoIP-Clients) geschickt. Für eine VoIP-Simulation ist es wichtig, dass realistische VoIP-Szenarien nachgebildet werden. Daher muss für die Tauglichkeitsprüfung das Messsystem mehrere parallele VoIP-Verbindungen simulieren, um die Priorisierungsmechanismen der IT-Infrastruktur unter Last zu testen. Eine solche VoIP-Simulation kann auch zur Überprüfung der mit dem Carrier für die Verbindung zwischen mehreren Standorten vereinbarten Service Level Agreements (SLAs) genutzt werden. Dabei lokalisieren die übermittelten Testdaten aktiv Fehler und Probleme in den einzelnen Netzsegmenten. Für die Auswertungen der simulierten VoIP-Verbindungen nutzt der TTSV das E-Modell gemäß ITU Rec. G.107 und den PESQ-Algorithmus gemäß ITU Rec. P.862. Bei der Simulation der VoIP-Verbindungen werden zwischen dem zentralen Messsystem TTSV und der kostenlosen Gegenstelle Trafficlyser TraceSim VoIP-Client eine oder mehrere VoIP-Verbindungen übermittelt.

Problemlose Installation

TTSV ist fester Bestandteil der Trafficlyser VoIP Test-Suite. Die Installationssoftware lässt sich nach der erfolgreichen Registrierung und den entsprechenden Freischaltungen im Support-Bereich auf der Homepage des Herstellers herunterladen. Das Setup der aktuellen Version 1.0.12 hat eine Größe von 116 MByte. Der Betrieb des Softwareprodukts erfordert einen lizenzierten USB-Dongle. Diesen Dongle erhält der IT-Verantwortliche nach dem Kauf der Software, er dient der Lizenzverwaltung. Die Nextragen-Software lässt sich prinzipiell auf einer unbegrenzten Anzahl von Rechnern installieren, jedoch nur mit eingestecktem Dongle aktivieren. Dies hat den Vorteil, dass die Analyse-Software auf den Laptops von mehreren Technikern installiert sein kann. Bei Bedarf bekommt der jeweilige Techniker den Dongle für seine Messung ausgehändigt und kann sofort arbeiten. Einzig der TTSV-Client und das Reportingtool lassen sich ohne Dongle ausführen.

Zum Test des Softwarepakets nutzten wir zwei Rechner mit jeweils einem Intel DualCore mit 2,67 GHz und 4 GByte RAM. Ein Messsystem arbeitete mit dem Betriebssystem Windows 7 und auf dem zweiten Rechner wurde Windows XP installiert. Auf beiden Testsystemen ließ sich das gleiche Setup problemlos installieren und die Software startete sofort nach dem Einstecken des USB-Dongles.

Gut dokumentierte Verwaltungskonsole

Nach dem Start der Software erkennt der Nutzer in der Bildschirmmitte eine Reihe von Steuerelementen, die ohne tiefere VoIP-Kenntnisse auf den ersten Blick erschreckend kompliziert wirken. Doch das mitgelieferte Handbuch gibt hier die notwendigen Antworten. Der Startbildschirm zeigt im oberen Drittel eine leere Tabelle, die später die gemessenen VoIP-Verbindungen auflistet. Das untere Drittel enthält

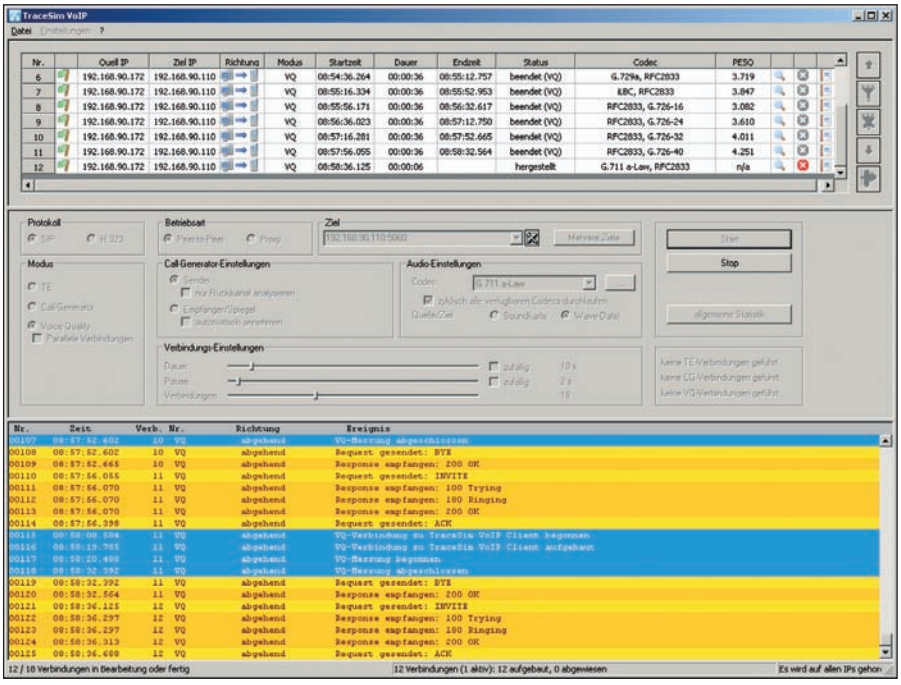


Bild 1: Der Hauptbildschirm von Trafficlyser TraceSim VoIP teilt sich in drei Bereiche

eine Aufstellung, in der das Signalling der Verbindungen angezeigt wird. Zusätzlich legt das Werkzeug hier diverse Logs ab, wenn bestimmte Zustände während einer Messung auftreten.

Im mittleren Drittel des Fensters finden sich Steuerelemente zur Konfiguration der Messung. Hier wählt der Benutzer die Art der Messung und deren Ausführung aus. Typische Einstellungen, wie beispielsweise die Wahl des Codecs oder die Wahl der Signalisierung, werden hier festgelegt. Zwischen zwei Endpunkten wird anschließend eine echte VoIP-Verbindung generiert. Hierzu musste im Test quasi als Messgegenstelle auf einem zweiten Rechner der TTSV-Client installiert und gestartet werden. Alternativ lässt sich auch die von Nextragen entwickelte Hardware-Sonde "NTG|Small" für diese Aufgabe nutzen.

Um den kostenlosen TTSV-Client (Windows oder Linux) in Betrieb zu nehmen, mussten wir drei Konfigurationen vornehmen: Über die Einstellungsoption öffnet sich das Dialog-Fenster für die Grundkonfiguration. Hier verstecken sich die Details für die SIP- beziehungsweise H.323-Konfigurationen. Der Nutzer bestimmt damit, welches Signalisierungsprotokoll er für den Test benutzen möchte. Zur Aktivierung der Client-Software musste lediglich der Haken zum Aktivieren des SIP-Profils und die IP-Adresse gesetzt werden. Nach der Bestätigung der aktuellen Einstellungen arbeitet der VoIP-Client im SIP Peer-to-Peer Modus.

Erste Messung vorbereiten und anstoßen

Für die erste Messung mit TTSV trugen wir die IP-Adresse des VoIP-Clients im Feld "Ziel" ein. Nach Betätigen des Startknopfs füllten sich automatisch die bisher leeren Tabellen. Im unteren Drittel des Bildschirms wird eine Signalisierungstabelle dargestellt. Auf Basis dieser Informationen erkennt der Nutzer, dass das SIP-Signalling funktioniert und die notwendigen SIP-Nachrichten für einen erfolgreichen Verbindungsaufbau übermittelt werden. Das obere Drittel des Bildschirms enthält eine Verbindungsliste mit den zu den generierten Verbindungen zugehörigen Informationen. Während der Messung wird der Status der Verbindungen aktualisiert und dargestellt, welche Verbindung noch aktiv ist oder bereits beendet wurde. Die Spalte "Dauer" zeigt an, wie lange das Gespräch bereits aktiv war und wird im Sekundentakt aktualisiert. Die letzten drei Spalten der Tabelle liefern weitere Schaltflächen für Aktionen zu jeder Verbindung. Mit dem "X" können die Verbindungen beendet werden und mit "Block" wird ein detaillierter Report für die jeweilige Verbindung angefertigt.

Der Klick auf die Lupe öffnete das Detailfenster zu den jeweiligen Verbindungen. Dem Benutzer werden hier alle VoIP-spezifischen Merkmale angezeigt. Dabei wird die Verbindung in zwei RTP-Sessions (Hin- und Rückrichtung) unterteilt und die jeweiligen VoIP-Parameter – beispielsweise Minimal-, Maximal- und Durchschnittswerte des Jitters, der Paketverluste, der Verzögerung – gegenübergestellt. Ebenfalls werden die Qualitätskennwerte wie R-Faktor und MOS-Wert angezeigt. Anhand dieser Parameter erkennt der Nutzer auf einen Blick, wie das Messsystem die getesteten Verbindungen bewertet. Der MOS-Wert beschreibt dabei die Qualität der Verbindung. Bei schlechten MOS-Werten geben die anderen Parameter genaue Auskunft über die vorhandenen Fehler.

Die Netzwerkeinstellungen ermöglichen die Anpassung der VoIP-Konfiguration an die für den Betrieb im vorhandenen Netz notwendigen IP-Umgebungen. Wird ein durch eine Network Address Translation (NAT) notwendiger STUN-Server benötigt, dann muss der Administrator diesen entsprechend der SIP-Richtlinien vor dem Test im TTSV eintragen. Ähnliches gilt für die zu nutzende Priorisierung im Netz; hier erleichtert der integrierte DiffServ-Wizard dem unerfahrenen Nutzer die korrekte Einstellung der DiffServ Code Points.

Ebenfalls müssen die SIP- beziehungsweise H.323-Einstellungen entsprechend der Nutzungsvariante an die VoIP-Konfiguration der vorhandenen TK-Anlage angepasst werden. TraceSim VoIP kann sich wie ein reguläres VoIP-Endgerät im Zusammenspiel mit einer TK-Anlage verhalten, sich am TK-System registrieren und die bereits vorhandene TK-Infra-

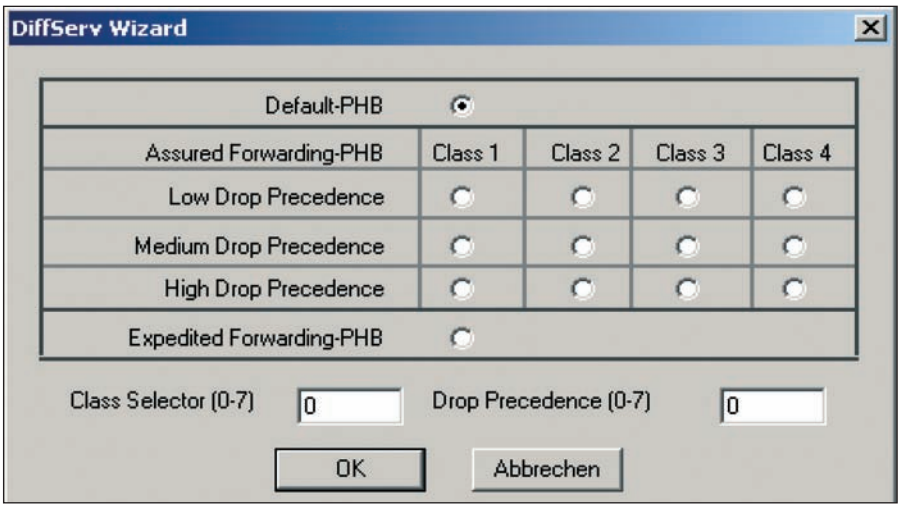


Bild 2: Der DiffServ Wizard soll die Einstellung der DiffServ Code Points erleichtern

struktur nutzen. Bei der Konfiguration der SIP-/H.323-Einstellung ermöglicht die Software das Anlegen von mehreren Profilen. So lassen sich unterschiedliche Konfigurationen definieren, die beim Test aktiviert werden. Dies erspart bei der Überprüfung von mehreren TK-Anlagen oder mehreren SIP-Accounts viel Zeit. In unseren Tests konzentrierten wir uns auf reine Peer-To-Peer Verbindungen.

Unter den Benachrichtigungseinstellungen verbirgt sich ein Einstellungsfenster zum Konfigurieren der Alarme. Werden mit TTSV automatisierte Messungen durchgeführt, lassen sich in diesem Fenster die Schwellenwerte für die MOS/PESQ-Werte definieren. Nach dem Über- beziehungsweise Unterschreiten des Schwellenwerts wurde in unserem Test eine E-Mail an die hinterlegte Adresse geschickt und dadurch der Alarm signalisiert. Weitere Konfigurationsoptionen sind:

- Codec-Einstellungen
- Größe des Jitterbuffers
- DTMF-Einstellungen
- Sprache
- Kundendaten für den Report

Drei Methoden für aktives Messen

Die Grundidee von TTSV ist simpel: Ein Simulator generiert zwischen einem und mehreren Punkten im Netzwerk reale VoIP-Gespräche und überprüft diese. Dabei muss sowohl die Anzahl der gleichzeitigen Gespräche variiert als auch zu unterschiedlichen Tages- und Wochenzeiten gemessen werden. Um in konvergenten Netzen die Sprachqualität richtig zu messen, ist es notwendig alle Netzsegmente zu erfassen. Nur so ist eine durchgängige Qualitätsaussage von Ende-zu-Ende möglich. Das Nextragen-System stellt hierzu mehrere Messmethoden zur Verfügung:

- Im TE-Modus wird ein Telefonanschluss eines VoIP-Anbieters simuliert und dieser in Verbindung mit dem VoIP-Netz des Providers getestet. Dabei wird eine entsprechende Testrufnummer des VoIP-Anbieters angerufen.
- Der Call Generator-Modus testet automatisch mehrere Verbindungen mit einstellbarer Dauer und belastet das angeschlossene VoIP-Netzwerk.
- Der VQ-Modus überprüft die VoIP-Verbindungen auf die VoIP-Leistungsfähigkeit des Netzes sowohl im Peer-to-Peer- als auch im Proxy-Verfahren.

Die Besonderheit des VQ-Modus steckt in den Messungen paralleler Verbindungen. Die Verbindungen werden treppenförmig aufgebaut, so dass jede neue Verbindung eine zusätzlich Last über das Netzwerk generiert. Die dadurch generierten Messwerte zeigen an, ab welcher Anzahl von aktiven VoIP-Verbindungen die Qualität einbricht.

Im VQ-Modus werden die PESQ-Werte zusätzlich in der Verbindungsliste angezeigt. Bei einer PESQ-Messung fließen Referenzsignale vom Messgerät an den TTSV-Client und vom Client an das Messgerät. Dadurch ermittelt das Messsystem präzise die Übertragungsfehler auf der Strecke. Von der Verbindungsliste lässt sich in die "Wave"-Ansicht wechseln und beide Signalrichtungen (gesendetes Referenzsignal und empfangenes Signal) darstellen. Legten wir im Test die beiden Signale übereinander, erkannten wir leicht die aufgetretenen Veränderungen. So ließ sich einfach erkennen, wenn das Signal zum Beispiel gedämpft wurde, da das empfangene Signal dann eine kleinere Amplitude aufwies. Das kurzzeitige Ausbleiben von Signalen verdeutlicht Paketverluste.

Auswertung der gesammelten Informationen

Nach unseren Messungen konnten wir die Messergebnisse in der Verbindungslis-

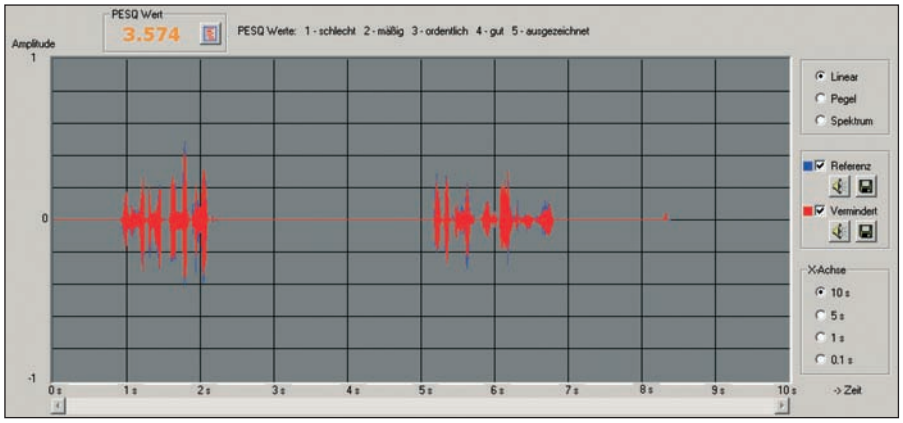


Bild 3: Die Wave-Anzeige von Trafficlyser TraceSim VoIP gibt Auskunft über Signal-Dämpfungen

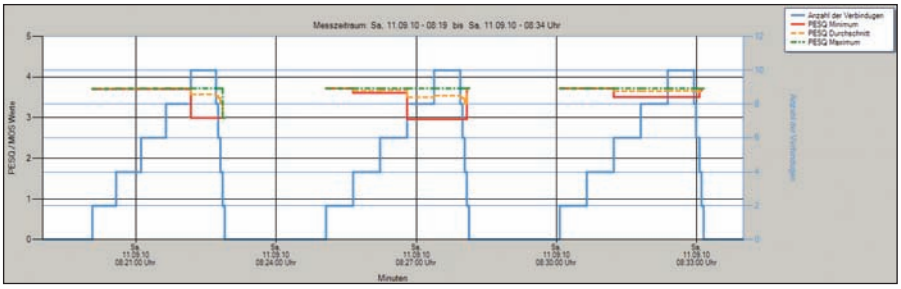


Bild 4: Der PESQ-Graph des Trafficlyser Reportingtools

te oder über die Details der Verbindungen begutachten. Der Benutzer erkennt anhand der ermittelten Werte sofort, wenn Verbindungen Probleme aufweisen. Die MOS-/PESQ-Werte liefern dabei die Zusammenfassung der Qualitätswerte der jeweiligen Verbindung.

Die von TTSV gesammelten Daten lassen sich entweder exportieren oder mit dem mitgelieferten Reportingtool bearbeiten. Das Reportingtool stellt diverse Graphen, Listen und Statistikfunktionen zur Verfügung. Die Graphen zeigen den Qualitätsverlauf der Verbindung in Kombination mit der Anzahl an parallelen Gesprächen an. Dadurch wird ermittelt, ab welcher Menge an Gesprächen die Verbindungen an Sprachqualität verlieren. Die Statistikfunktionen stellen die gemessenen Werte (Minimal-, Maximal- und Durchschnittswerte) der Sprachqualität dar. Dadurch erhält der Anwender einen schnellen Überblick über die gesamte Messung. Zur Vereinfachung der Auswertung von mehreren Messreihen stellt das Reportingtool die entsprechenden Filterfunktionen zur Verfügung. Hier lässt sich beispielsweise nach bestimmten IP-Adressen oder Verbindungen mit bestimmten MOS-Werten filtern.

Die Verbindungsliste liefert einen Überblick über die durchgeführten Messungen. Die Details zu jeder Verbindung liefern die ermittelten Messwerte. Wird beispielsweise eine Verbindung mit schlechten MOS-Werten gefunden, kann mit einem Doppelklick in die entsprechenden Verbindungsdetails gewechselt werden. Zusätzlich zu den Auswertungen ist es möglich, mit dem Reportingtool einen Report zur Messung anzufertigen und die gesammelten Daten als PDF-Dokument zu archivieren. Die individuelle Anpassung der Reportinhalte erleichtert die Handhabung der vielen Details.

Automatisieren der Messprozesse

Ein Highlight von TTSV steckt in den automatisierten Messungen. Alle Programmeinstellungen und getroffenen Messeinstellungen lassen sich als Messkonfiguration abspeichern. Hinter dem Menüpunkt "Jobs planen" verbirgt sich ein Dialog, der die gespeicherten Konfigurationen zu bestimmten Zeiten ausführt. Im Test wählten wir zuerst die gespeicherte Messkonfiguration aus und wurden anschließend nach einem Ordner gefragt, in dem die Messergebnisse gespeichert werden sollen. Im nächsten Schritt legten wir fest, zu welchen Zeitpunkten die Messkonfiguration aktiviert und die betreffende Messung durchgeführt werden soll.

Nach einem Ablauf der vorkonfigurierten Messreihe befanden sich im Messordner die Messergebnisse der einzelnen Testläufe. Diese bestanden aus einer Messdatei und mehreren Wave-Dateien (Sprachinformationen der Verbindungen). Mit Hilfe des Reportingtools konnten wir den gesamten Ordner laden und die VoIP-Strecken bewerten.

Fazit

Mit Trafficlyser TraceSim VoIP steht dem Administrator eine Softwarelösung zur Verfügung, die nach einer gewissen Einarbeitungsphase in Kombination mit dem notwendigen VoIP-Wissen ein optimales und preiswertes Werkzeug zur Evaluierung der VoIP-Qualität bietet. Auch ein VoIP-Readiness-Check ist mit diesem Tool problemlos möglich. Durch die integrierte Möglichkeit der automatisierten Messungen ist die Software auch für eine Langzeitüberwachung geeignet. *(jp)*

Produkt
Software zur Messung der Übertragungsqualität von VoIP.

Hersteller
Nextragen GmbH
www.nextragen.de

Preis
Trafficlyser TraceSim: Bis zu 300 parallele VoIP-Verbindungen für 3.000 Euro pro Server-Lizenz, VoIP-Clients kostenlos.

Trafficlyser TraceSim mit PESQ-Lizenz: Bis zu 300 parallele VoIP-Verbindungen für 4.800 Euro pro Server-Lizenz, VoIP-Clients kostenlos.

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

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

Installation	9
Bedienung	8
VoIP-Analyse	10
Reports	9
Dokumentation	8

Dieses Produkt eignet sich

optimal für die Überprüfung von Netzwerken auf VoIP-/UC-Fähigkeit und trägt dazu bei, Fehler im Netzwerk und der QoS-Konfiguration zu orten und deren Ursachen zu beheben. Zusätzlich lässt sich durch das Langzeit-Monitoring auch der gesamte VoIP/UC-Betrieb dokumentieren.

bedingt in kleineren VoIP-Infrastrukturen; hier sollten IT-Verantwortliche Preis und Nutzen abwägen.

nicht in Unternehmen, die keine VoIP-Anlage betreiben und dies auch nicht planen.

Nextragen Trafficlyser TraceSim VoIP

Im Test: sepago Profile Migrator 1.0

Profilumzüge in drei Schritten

von Jürgen Heyer

Betriebssystem-Migrationen stoßen meist auf wenig Akzeptanz, wenn die Anwender dabei ihre gewohnte Arbeitsumgebung verlieren. Vor allem beim Wechsel von Windows XP und 2003 auf Windows 7und 2008 Server ist die Übernahme bestehender Roaming Profiles nicht möglich, da Microsoft mit diesen Versionen das Profilformat geändert hat. Abhilfe verspricht der Profile Migrator von sepago – ein leicht zu bedienender Profilkonverter, der eine Migration in nur drei Schritten ermöglichen soll. IT-Administrator hat das Werkzeug einmal ausprobiert.

Sobald sich in größeren Unternehmen die Benutzer häufig an wechselnden Arbeitsplätzen anmelden, setzen die Administratoren in der Regel auf Roaming Profiles, damit jedem Anwender überall die gleiche Arbeitsumgebung zur Verfügung steht. Auch im Terminalserver-Umfeld sind die Profile nutzbar und der Anwender bekommt stets seinen Desktop, auch wenn er in einer Terminalserver-Farm wie üblich je nach Lastverteilung immer wieder mit einem anderen Server verbunden wird. Bis einschließlich Windows XP und Windows 2003 Server war es kein Problem, bei einem Betriebssystemwechsel bestehende Profile weiter zu nutzen, da es sich um so genannte V1-Profile (Version 1) handelte. Mit der neuen Windows-Generation hat Microsoft das Profilformat jedoch grundlegend geändert und die V2-Profile (Version 2) eingeführt. Beide Profil-Varianten sind nicht kompatibel und Microsoft hat keinen automatischen Migrationspfad vorgesehen.

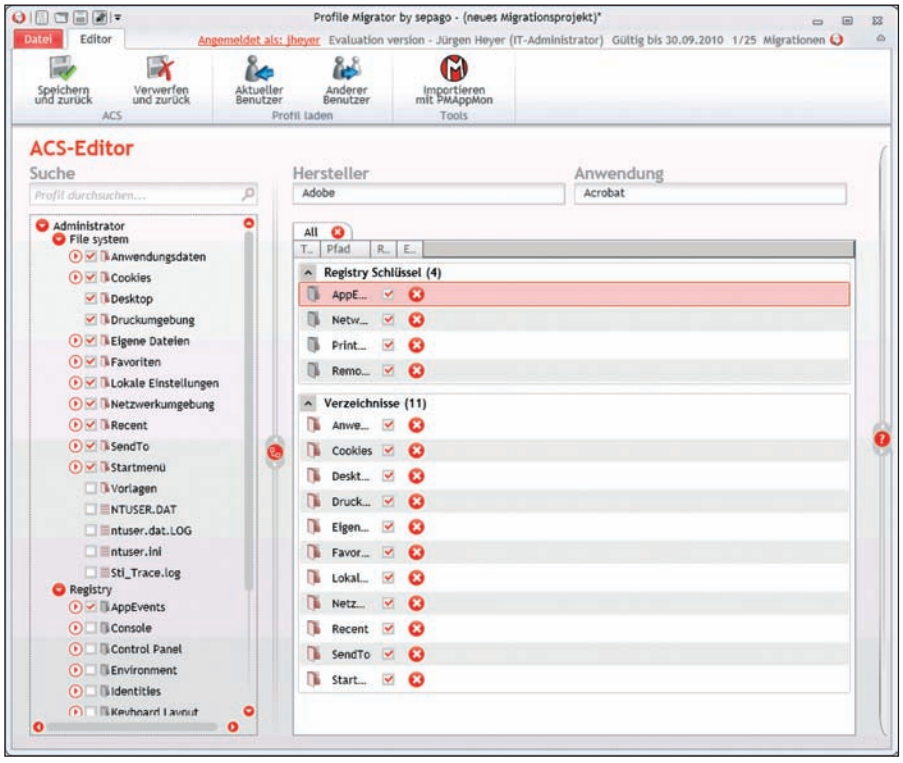


Bild 1: Der ACS-Editor bietet einen genauen Überblick über die bei einer Profilmigration notwendigen Anpassungen und ermöglicht eigene Änderungen

Für Unternehmen, die auf Terminalserver etwa in Verbindung mit Thin Clients setzen, hat der Verlust der Profile für die Anwender enorme Auswirkungen. Nicht nur das Desktop-Design ist hier hinterlegt, sondern auch sehr viele individuelle Programmeinstellungen der genutzten Software. Allein Microsoft Office verfügt über mehrere hundert Einstellungen und aus eigener Erfahrung dürften die meisten Administratoren wissen, wie mühevoll es ist, beispielsweise Outlook nach einer Umstellung wieder in den gewohnten Zustand zu konfigurieren. Die Folgen sind offensichtlich, denn wenn in einem größeren Unternehmen alle Anwender ihre Benutzereinstellungen erneut einrichten müssen, erfordert dies schnell einige hundert oder gar mehrere tausend Arbeitsstunden inklusive einer enormen Belastung des Helpdesks. Vor diesem Hintergrund hat die Kölner sepago GmbH den Profile Migrator entwickelt, um solche Profilmigrationen zu automatisieren. Die Referenzliste auf der Website belegt, dass dieses Tool bereits von diversen großen Unternehmen für die Portierung der Benutzereinstellungen genutzt wird.

Variabler Installationsort

Für den Test stand uns die Version 1.0.0.1654 des Profile Migrator zur Verfügung. Mangels Handbuch waren wir anfangs etwas unsicher, was den optimalen Installationsort anbelangte. Eine Nachfrage beim Hersteller ergab jedoch, dass dieser variabel gewählt werden kann. Voraussetzung ist letztendlich, dass Microsoft Active Directory genutzt wird und der Quell- ebenso wie der Zielserver zu dieser Domäne gehören. Gleiches gilt, wenn es sich um eine Terminalserver-Farm, gegebenenfalls mit Thin Clients, handelt. Der Fokus von Profile Migrator liegt eindeutig auf der Migration von Server-basierten Roaming Profiles. Es ist zwar auch eine Migration einzelner lokaler Profile denkbar, jedoch dürfte dies eher unüblich sein. Zudem bietet Microsoft für derartige Migrationen mit "User state migration tool" (USMT) und "Easy transfer" zwei eigene Tools an. Beide laufen ausschließlich auf Fat Clients mit lokal existierenden Profilen und sind somit eher für Privatanwender interessant. Roaming Profiles von zentral verwalteten Systemen wie Terminalservern lassen sich damit nicht migrieren.

Der Profile Migrator lässt sich letztendlich auf einem beliebigen Server oder auch Arbeitsplatz in der Domäne installieren, er muss nur lesenden Zugriff auf das Verzeichnis haben, in dem die Profile liegen. Auf das Verzeichnis, in dem die neuen Profile abgelegt werden sollen, benötigt das Tool Vollzugriff sowie das Benutzerrecht "Übernehmen des Besitzes von Dateien und Objekten". Die Installation gestaltet sich überaus einfach und bis auf den Installationspfad mussten wir keine weiteren Informationen angeben. Den erhaltenen Lizenzschlüssel trugen wir beim ersten Start ein. Wichtig ist zudem noch eine Registrierung bei sepago, um einen Online-Zugriff auf die so genannte ACS-Datenbank zu erhalten. ACS steht für "Application Configuration Set". ACS-Dateien enthalten für verschiedenste Programme die Information, wie die Benutzereinstellungen funktionieren und welche Daten für eine Migration zu erfassen sind. Die ACS-Datenbank wird von sepago ständig erweitert, so dass nach und nach für immer mehr Programme fertige ACS-Dateien verfügbar sein sollten. Abgesehen davon ist es auch möglich, eigene ACS-Dateien beispielsweise für selbst erstellte Software zu generieren. Die Vorgehensweise dafür ist weiter unten beschrieben.

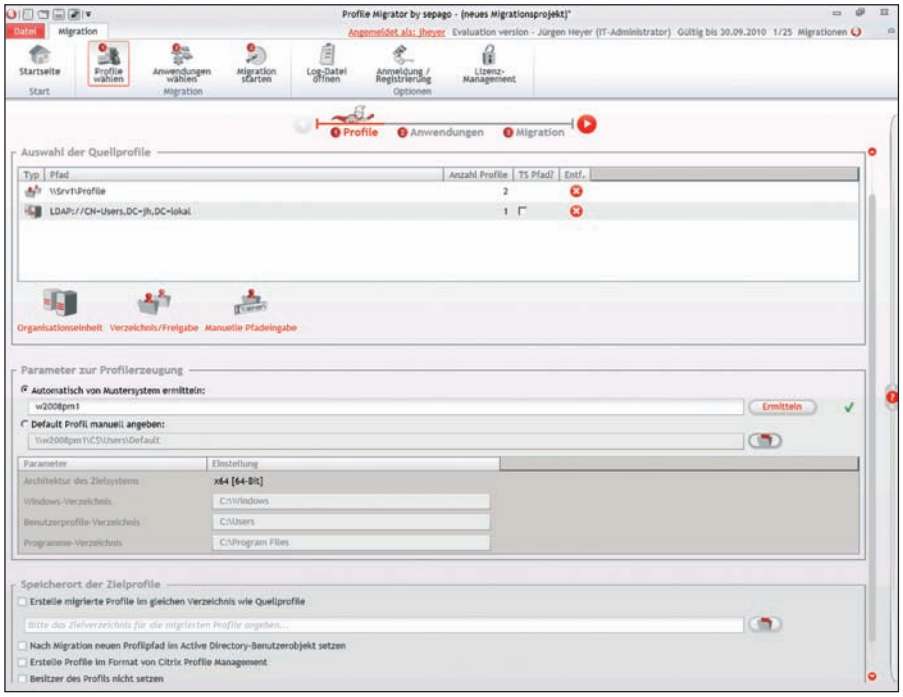


Bild 2: Der erste Migrationsschritt fragt alle Angaben zu den Quell- und Zielprofilen ab, um so den Migrationsweg festzuschreiben

Um den Profile Migrator zu testen, haben wir als Quellsystem einen Windows-2003-Server als Terminalserver eingerichtet und auf diesem Office 2003 installiert. Weiterhin legten wir in der Domäne einige Benutzer an, die an einer zentralen Stelle gespeicherte Profile benutzten. Als Zielsystem wählten wir zwei Windows 2008-Server, einen ebenfalls mit installiertem Office 2003 und einen mit Office 2010. Der Hintergrund dafür ist, dass der Profile Migrator nicht nur V1-Profile in das V2-Format migriert, sondern zusätzlich auch die Einstellungen für den Umstieg auf andere Programmversionen anpassen kann, also wie von uns gewünscht von Office 2003 auf Office 2010. Entscheidend ist nur, dass entsprechende ACS-Dateien existieren.

Migration in drei Schritten

Der Profile Migrator besteht aus einer Startseite, die die Benutzerprofil-Migration in drei übersichtliche Schritte teilt, so dass sich das Tool erfreulich intuitiv bedienen lässt. Positiv ist, dass sich für jeden der drei Schritte auf der rechten Seite eine breite Hilfe-Spalte mit umfangreichen Beschreibungen einblenden lässt, so dass ein zusätzliches Handbuch über weite Strecken nicht erforderlich ist. Außerdem erscheint beim Überstreichen eines Eingabefeldes oder einer Option eine Popup-Hilfe, die zusätzlich beschreibt, was sich dahinter verbirgt.

Systemvoraussetzungen und Lizenzen

Windows Active Directory-Domäne mit servergespeicherten Profilen/Roaming Profiles, Clients und Server ab Windows XP beziehungsweise 2003. Die Lizenzierung des Profile Migrator erfolgt auf Basis der Named User, wobei hier auf Vertrauensbasis mit dem Kunden abgerechnet wird. Eine Migration bricht bei Überschreitung der lizenzierten Nutzer nicht ab. Müssen pro Anwender mehrere Profile migriert werden, so ist dies mit einer Lizenz abgedeckt. Auf einen Lizenzserver oder Ähnliches hat sepago bewusst verzichtet.

1. Schritt: Quellprofile festlegen

Der erste Schritt beschäftigt sich mit der Lokation der Quell- und Zielprofile sowie grundlegenden Einstellungen für eine Migration. So wählt der Administrator zuerst die Quellprofile aus und hat hierzu drei Möglichkeiten. Einmal kann er im AD eine Organisationseinheit mit Benutzern auswählen. Alle Profile der Benutzerobjekte, bei denen ein Profilpfad angegeben ist, werden migriert. Statt des normalen Profilpfades lässt sich auch der Terminalserver-Pfad auswerten. Weiterhin kann er ein Verzeichnis beziehungsweise eine Freigabe angeben, wobei dann alle darin sowie in Unterverzeichnissen enthaltenen Profile ausgewählt werden. Als dritte Variante lässt sich ein Pfad oder eine Freigabe manuell eingeben, wobei nach dem Eintippen der ersten Zeichen eine Browserfunktion hilft. Gut ist, dass sich die drei Varianten auch kombinieren lassen, da alle Angaben in eine Liste geschrieben werden, die dann abgearbeitet wird.

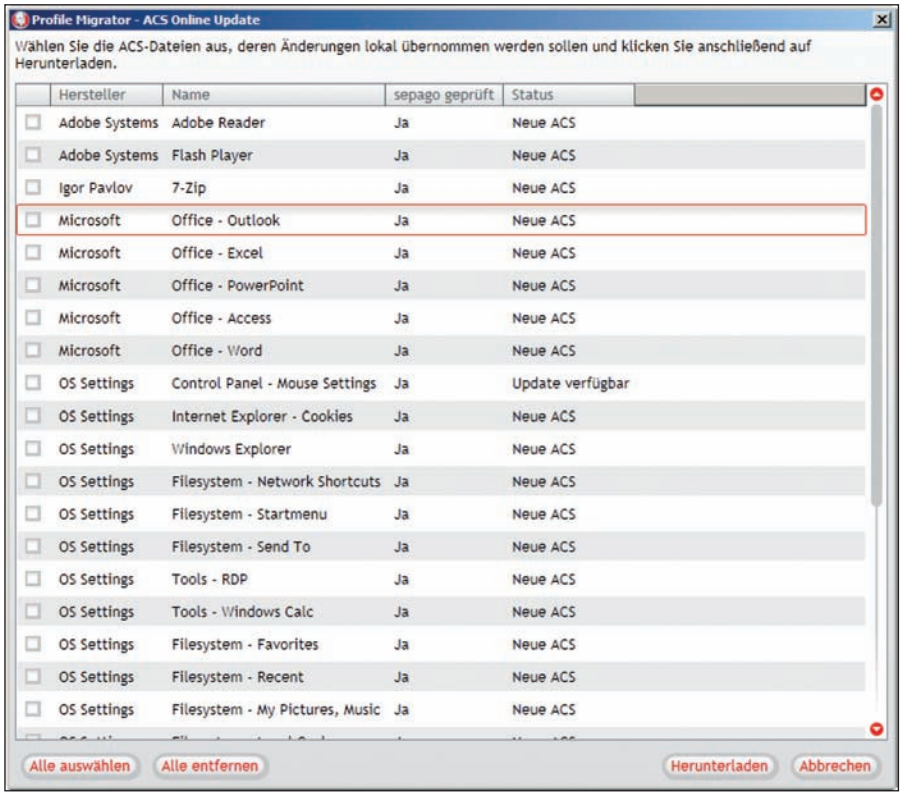


Bild 3: sepago liefert für eine zunehmende Anzahl an Anwendungen vorbereitete ACS-Dateien, die die Migration inklusive eines Versionsumstiegs deutlich vereinfachen

Für die Profilerzeugung ist entweder ein Musterprofil oder der Zielserver anzugeben. Der Profile Migrator ermittelt daraus wichtige Parameter wie die Architektur des Zielsystems sowie die Verzeichnisse für Windows, die Programme und die Profilablage.

Zuletzt ist der Speicherort für die Profile mit einigen Optionen anzugeben. Eine Speicherung in das Quellverzeichnis ist möglich und auch realistisch, wenn durchwegs V1- in V2-Profile konvertiert werden, da bei einem V2-Profil zur Unterscheidung der Name des Benutzerverzeichnisses um das Kürzel V2 erweitert wird. Bei einem anderen Zielverzeichnis ändert der Profile Migrator auf Wunsch auch die entsprechende Pfadangabe im AD und erstellt bei Bedarf die Profile im Format für das Citrix Profile Management.

Sollten in einem Zielverzeichnis für einige Benutzer entsprechende Profile bereits existieren, so kann der Administrator vorgeben, ob diese übersprungen, umbenannt oder überschrieben werden sollen. Beim Überschreiben geht der Profile Migrator einen sicheren Weg, indem er das vorhandene Profil erst umbenennt, dann das neue erzeugt und zuletzt das umbenannte löscht. Schlägt die Erstellung des neuen Profils fehl, wird das alte wieder zurückbenannt. Die Option, vorhandene Profile zu überspringen, gibt dem Administrator übrigens die Möglichkeit, eine anstehende Umstellung in mehreren Schritten durchzuführen. Er muss dann nicht peinlich darauf achten, bereits migrierte Anwender nicht mehr auszuwählen, sondern kann sich auf die Prüfung durch den Profile Migrator verlassen.

2. Schritt: Übernahme der Einstellungen

Im zweiten Schritt legt der Administrator fest, welche Einstellungen migriert werden sollen. Bezüglich der Übernahme von Anwendungseinstellungen ist es unbedingt erforderlich, sich wie oben beschrieben bei sepago zu registrieren, sonst stehen nur drei Einträge wohl mehr zu Demonstrationszwecken zur Auswahl (Winzip, Mozilla Firefox, Windows-Mauseinstellungen). Nach der Registrierung und Anmeldung bei sepago besteht Zugriff auf weitere Betriebssystem-bezogene Profilinhalte. Diese sind in 18 Rubriken (unter anderem Netzwerk-Mappings, Mauseinstellungen, Desktop, Startmenü und Favoriten) unterteilt, so dass je nach Bedarf auch nur Teile übernommen werden können. Weitere ACS-Dateien beinhalten die Migrationsanweisungen für die MS Office-Produkte Excel, Powerpoint, Access und Outlook, dann 7-Zip, Adobe Flash Player und abschließend noch zwei weniger bekannte Applikationen. Im Laufe des Tests konnten wir feststellen, dass einzelne ACS-Dateien aktualisiert wurden. Außerdem wurden die Informationen für die Migration von Microsoft Word bereitgestellt.

Bezüglich des insgesamt noch nicht so umfangreichen Angebots an ACS-Dateien ist anzumerken, dass teilweise überaus komplexe Einstellungen einzuarbeiten sind. So besitzt Outlook rund 300 Parameter und es werden die Versionen 2003, 2007 und 2010 unterstützt, deren Profilinhalte wiederum unterschiedlich aufgebaut sind. Das zeigt schon, wie umfangreich der Inhalt der

ACS-Dateien sein kann. Auch ist sepago bestrebt, die bereitgestellten Dateien vor der Veröffentlichung eingehenden Überprüfungen zu unterziehen. Wie auch schon während unseres Tests sollen nach und nach kontinuierlich neue ACS-Dateien entwickelt und bereitgestellt werden.

In den Profile Migrator ist ein Editor für ACS-Dateien integriert, der es ermöglicht, die einzelnen Anweisungen einzusehen und auch Änderungen vorzunehmen, was natürlich entsprechende Detailkenntnisse voraussetzt. Der Editor ist recht übersichtlich aufgebaut und untergliedert die Einstellungen in Registry-Werte, Registry-Schlüssel sowie Vorgaben zu Dateien und Verzeichnissen.

Neben der Nutzung der vorbereiteten ACS-Dateien hat der Administrator, wie eingangs schon erwähnt, die Möglichkeit, eigene ACS-Dateien zu erzeugen. Eine wertvolle Hilfe hierzu ist der so genannte PMAppMon, der quasi mitschneidet, worauf eine Applikation beim Start zugreift. Es ist naheliegend, dass beim Starten überwiegend auf diejenigen Bereiche im Benutzerprofil zugegriffen wird, die Programm-relevante Einstellungen enthalten. Um den PMAppMon nutzen zu können, sind jedoch einige Voraussetzungen zu berücksichtigen. So lässt sich das Tool unter Windows XP und 2003 Server nur im so genannten Analysemodus verwenden. Dazu sind Log-Dateien mit dem Process Monitor von Sysinternals zu erstellen, aus denen der PMAppMon dann die relevanten Informationen extrahiert und daraus eine ACS-Datei erzeugt.

Ab Windows Vista und Server 2008 ist der PMAppMon direkt nutzbar. Dazu muss allerdings vorher das Windows Performance Toolkit (WPT) installiert werden, das im Windows 7 SDK enthalten ist. Durch das Mitschneiden mit PMAppMon kann der Administrator recht gut erkennen, wo die Zugriffe erfolgen und die entsprechend aufgelisteten Bereiche in die Profilmigration mit aufnehmen. Diese Information wird nun als ACS-Datei gespeichert, so dass der Administrator diese Daten jederzeit wieder verwenden kann. Im Gegensatz zu den von sepago entwickelten ACS-Dateien, die auch eine Konvertierung beim Wechsel einer Programmversion ermöglichen, eignen sich selbsterstellte ACS-Dateien in erster Linie für die Portierung der Profileinstellungen ohne gleichzeitigen Versionswechsel. Um so etwas zu realisieren, müssten die ACS-Dateien mit dem beschriebenen Editor manuell nachbearbeitet werden.

3. Schritt: Migration

Sind schließlich die zu migrierenden Einstellungen festgelegt, kann der Administrator im dritten und letzten Schritt die eigentliche Migration starten. Bei Bedarf bietet sich noch ein Pre-Check an, der eine lange Prüfliste abarbeitet und nach dem Ampelsystem für die einzelnen Punkte ein OK, eine Warnung oder einen Alarm liefert. Werden Alarme gefunden, lässt sich die Migration nicht ausführen. Im Labor haben

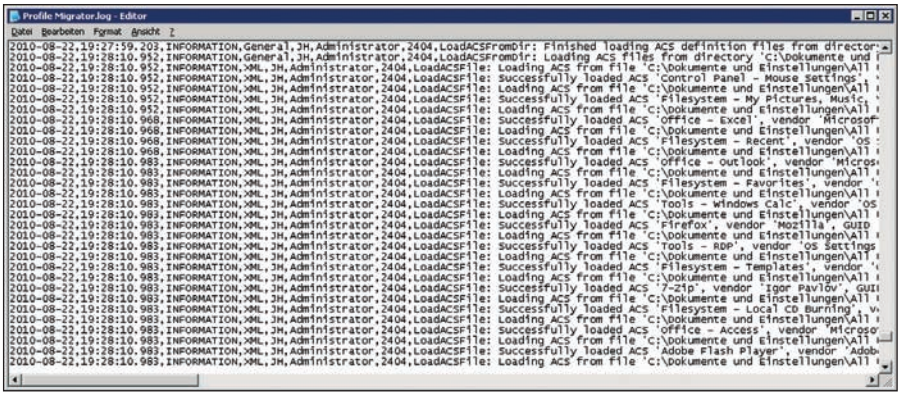


Bild 4: In einer umfangreichen Log-Datei listet der Profile Migrator für eine spätere Kontrolle alle durchgeführten Aktionen auf

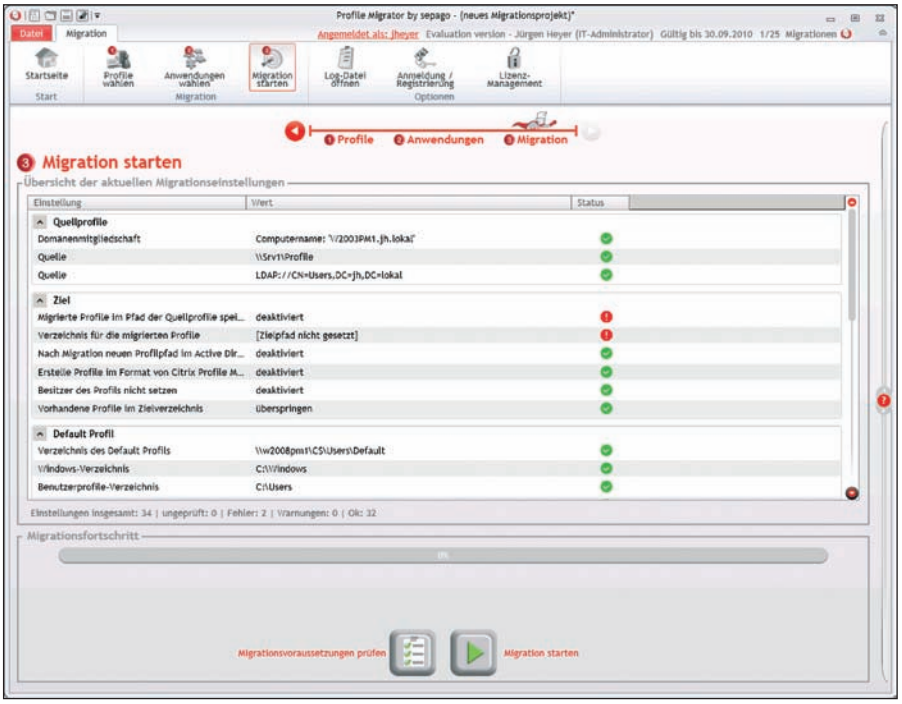


Bild 5: Ein Pre-Check nach dem Ampelsystem prüft vor einer Migration alle Vorgaben und warnt oder alarmiert bei fehlenden oder falschen Angaben

wir testweise verschiedene Migrationen zwischen unserem Windows 2003- und den beiden Windows 2008-Servern durchgeführt. Dabei leistete der Profile Migrator im Test durchwegs gute Arbeit und der Vorteil wurde offensichtlich, sobald wir uns als Benutzer am neuen System anmeldeten.Vor der Migration gezielt durchgeführte Einstellungen beispielsweise unter Outlook wurden korrekt übernommen. Sehr komfortabel gelingt die Migration vor allem bei den Programmen, für die sepago fertige ACS-Dateien bereitstellt. Müssen diese über den PMAppMon selbst erstellt werden, ist der Aufwand deutlich höher.

Fazit

Der Hauptfokus von Profile Migrator richtet sich darauf, innerhalb von großen Terminalserver-Umgebungen beim Umstieg von Windows XP/2003 Server auf Windows Vista/7/2008 Server die Benutzereinstellungen vom bisherigen V1-Profilformat auf das neue V2-Format zu migrieren. Damit lassen sich Umstellungen realisieren, ohne dass die Anwender auf ihre gewohnte Desktopumgebung verzichten müssen. Darüber hinaus eignet sich der Profile Migrator auch für die Umstellung vom älteren Office 2003 auf die neueren Versionen 2007 und 2010. Über vorbereitete ACS-Dateien liefert der Hersteller die dazu notwendigen Konvertierungsinformationen. Momentan ist dieses Angebot allerdings noch recht beschränkt, es wird jedoch ständig erweitert.

Das Tool ist sehr übersichtlich aufgebaut und unterteilt eine Migration in drei logisch sinnvolle Schritte. Recht informativ ist zudem die integrierte Hilfe, die ein Handbuch fast überflüssig macht. Eine Einarbeitung sollte sehr schnell gelingen, nur entsprechendes Wissen zu den servergespeicherten Profilen ist notwendig. Das sollte aber in der Regel vorhanden sein, wenn viele Terminalserver zu betreuen sind. Nichtsdestotrotz vermissten wir eine kurze Bedienungsanleitung, die zumindest die Installationsvoraussetzungen sowie die beste Reihenfolge der notwendigen Installationsschritte und die prinzipielle Arbeitsweise beschreibt. Dies lässt sich nicht auf Anhieb der integrierten Hilfe entnehmen. Auch die Besonderheiten zur Nutzung des PMAppMon erschließen sich nicht sofort aufgrund der knappen Hinweise beim Start des Tools. Diese Informationen haben wir nach und nach bei sepago erfragt, sie gehören aber unserer Meinung nach in eine begleitende Dokumentation.

Bleibt festzuhalten, dass, je größer das Unternehmen ist und je mehr Anwender umzustellen sind, sich aus unserer Sicht die Anschaffung dieses Werkzeugs lohnt. *(dr)*

Produkt

Programm zur Profilkonvertierung zwischen den Microsoft-Formaten V1 und V2 sowie beim Versionswechsel von Applikationen.

Hersteller

sepago
www.sepago.de

Preis

Profile Migrator kostet bis 499 Lizenzen (Named User) je 15 Euro, bei größeren Abnahmemengen gibt es Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation	9
Bedienung	8
OS-Migration	9
Applikations-Migration	8
Dokumentation und Hilfe	7

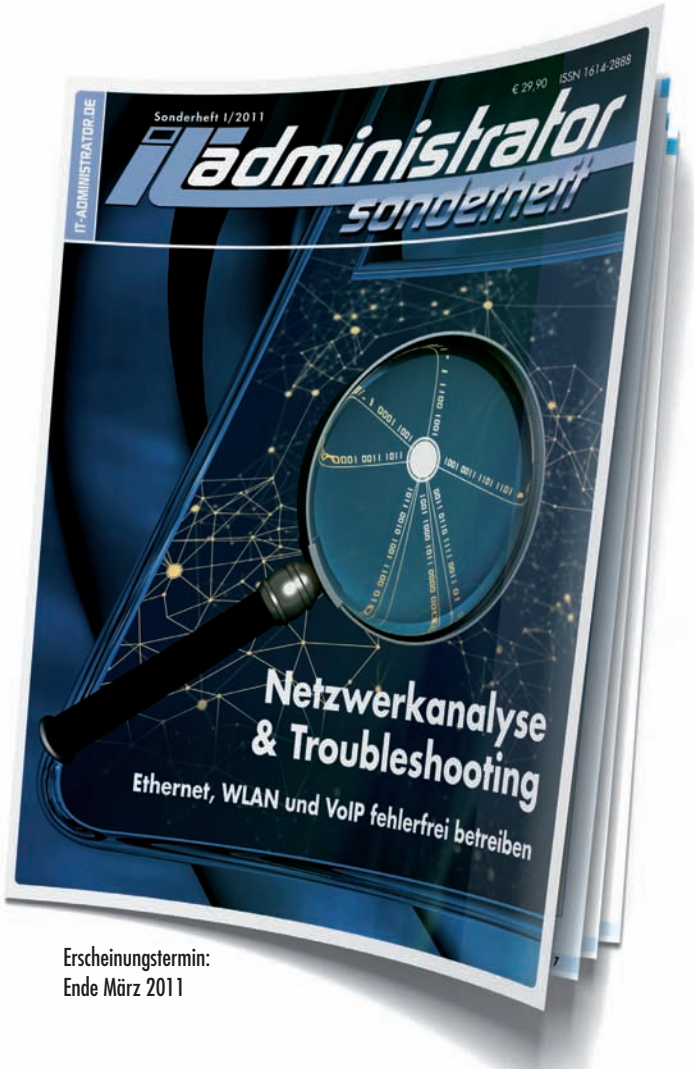
Dieses Produkt eignet sich

optimal für große Terminalserver-Umgebungen sowie bei servergespeicherten Profilen zur Migration vom V1- in das V2-Format.

bedingt für kleinere Umgebungen oder wenn überwiegend lokale Profile genutzt werden. Dann sind Kosten und Aufwandsersparnis genau abzuwägen.

nicht, wenn bereits ein anderes Werkzeug zum Desktop-Management eingesetzt wird.

sepago Profile Migrator 1.0



Erscheinungstermin:
Ende März 2011

Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft I/2011 für € 24,90. Nichtabonnenten zahlen € 29,90. 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/

iadministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 1210

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

Im Test: Secunia Corporate Software Inspector 4.0

Ein Inspektor für alle Fälle

von Thomas Gronenwald

Viele Unternehmen nutzen zum Patchmanagement die WSUS-Dienste zum Verteilen der monatlich veröffentlichten Microsoft-Sicherheitsupdates. Allerdings wird hierbei immer noch allzu oft auf die regelmäßige Aktualisierung von 3rd-Party-Software im Unternehmen verzichtet – so sind veraltete Adobe Reader-, Flash- oder Java-Versionen keine Ausnahmen, sondern eher die Regel. Vor dem Hintergrund der seit 2007 um fast 400 Prozent gestiegenen Anzahl an Sicherheitslücken in Drittanbietersoftware entsteht so ein erhebliches Risiko für die IT-Sicherheit in diesen Unternehmen. Der Corporate Software Inspector 4.0 vom dänischen Hersteller Secunia erlaubt es, diese Sicherheitslücken zu erkennen, zu bewerten und zu beheben. In unserem Test musste das Werkzeug seine Fähigkeiten unter Beweis stellen.

Neu ist hierbei die Integration des Corporate Software Inspector 4.0 (CSI) in die Microsoft-Lösungen WSUS und System Center Configuration Manager (SCCM). Diese Synergie erlaubt es, nun mehr als 13.000 Applikationen, Plug-Ins und Erweiterungen im Unternehmensnetz zentral zu überwachen und mit geeigneten Sicherheitsupdates zu versorgen. Dabei benutzt CSI die gleiche Technik wie beim kostenlosen Personal Software Inspektor (PSI) von Secunia, um festzustellen, welche Software in welcher Version auf einem System installiert ist und ob eventuell neuere Versionen vorhanden sind.

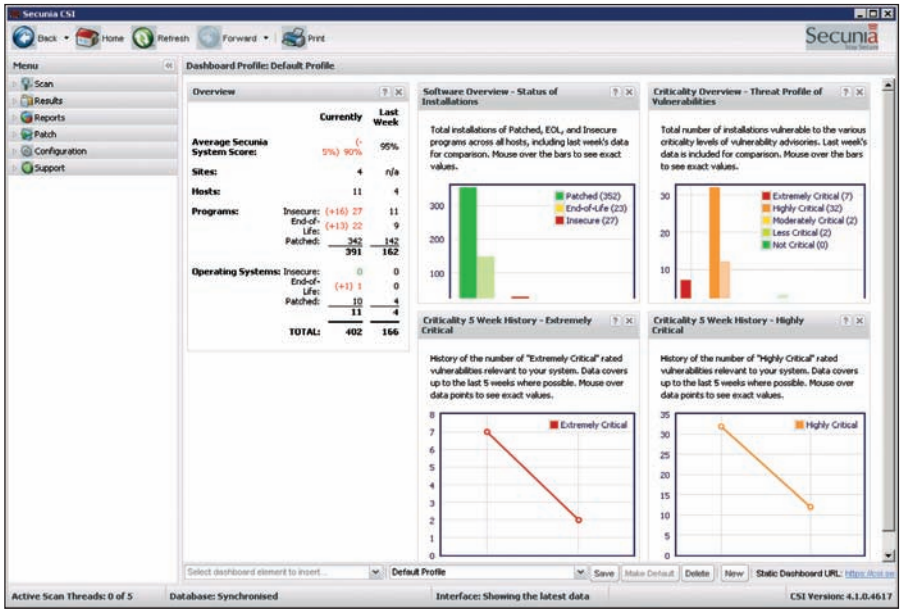


Bild 1: Die Oberfläche von CSI 4.0 wirkt aufgeräumt und bietet schnellen Zugriff auf wichtige Funktionen

Bis dato mussten für ein flächendeckendes Patch-Management von Windows-Umgebungen zahlreiche Tools eingesetzt werden. Dies führte jedoch in aller Regel dazu, dass nur halbherzig gepatcht wurde. Nun ermöglicht Secunia, das Patch-Management von Drittanbietersoftware auch über die Microsoft-Mechanismen bereitzustellen. Kombiniert wird dies weiterhin durch die bereits aus den Vorgängerversionen bekannten und hoch geschätzten Programmfunktionalitäten. Verschiedene Sicherheitsberichte aller eingesetzten Anwendungen sowie potenzielle Gefährdungen lassen sich über die überarbeitete Programmoberfläche abrufen. So behalten Administratoren und Sicherheitsverantwortliche stets den Überblick über Anwendungen, Betriebssysteme und Service Packs in ihrem Unternehmen und können so schnell und zuverlässig auf neue Sicherheitsrisiken reagieren.

Systemvoraussetzungen und Installation

Die Installation der CSI-Konsole in der aktuellen Version 4.1.0.4617 stellt einen Administrator vor nicht allzu große Probleme und ist innerhalb von wenigen Minuten abgeschlossen. Wichtig ist lediglich, dass das Setup mit administrativen Berechtigungen ausgeführt wird. Außerdem ist es notwendig, das Service Pack1 für das Microsoft .NET Framework 2.0 (ab Windows Server 2008 enthalten) sowie das Microsoft Visual C++ 2008 SP1 zu installieren.

Die Konsole ist dabei sowohl auf einem administrativen Client oder auch direkt auf

Bild 2: Die unterschiedlichen Scan-Methoden lassen sich leicht konfigurieren

dem WSUS-Server installierbar. In unserem Test diente ein Windows Server 2008 R2 mit bereits konfiguriertem WSUS-Server als Basis für die Integration von CSI.

Für die reibungslose Bereitstellung von selbsterstellten Update-Pakten müssen lediglich kleinere Anpassungen innerhalb der bestehenden Domäne vorgenommen werden. Damit die Microsoft-Lösungen die Verteilung von Drittanbietersoftware erlaubt, sind hierfür entsprechende Gruppenrichtlinien zu erstellen. Diese sind dann zum einen für die Verteilung der benötigten Zertifikate als auch für das Bereitstellen der Patches verantwortlich. Diese Konfiguration kann dabei entweder über den mitgelieferten Assistenten oder selbständig durchgeführt werden.

Betrieb für mobile Nutzer und im Unternehmensnetz

CSI unterscheidet zwischen einem "agent-based"- (Installation eines Agenten notwendig) und einem "agent-less"-Modus (keine Installation notwendig). Hierbei erfolgt der Zugriff, wie der Name schon sagt, entweder über einen Agent oder über eine direkte Remoteabfrage des Clients über das Netzwerk. Mit der "agent-based"-Methode erhält der Administrator zudem zwei weitere Möglichkeiten, seine Umgebung anforderungsgerecht zu überwachen. Bei der Installation kann zwischen dem "Single Host Mode" und dem "Network Appliance Mode" unterschieden werden.

Der Single Host Mode ist dabei speziell für Unternehmens-Notebooks entwickelt worden. Aufgrund der Tatsache, dass diese immer öfter nicht direkt mit dem Netzwerk des Unternehmens verbunden sind, ist ein geplanter Scan oft nicht möglich. Dieser Modus erlaubt es, dass, sobald eine Internetverbindung besteht, ein Abgleich der installierten Programme mit der Secunia-Datenbank vorgenommen werden kann. Die Ergebnisse werden dann an die CSI-Konsole übermittelt – so behalten Administratoren auch stets ihre mobilen Geräte im Auge.

Der Network Appliance Mode hingegen ist für Administratoren gedacht, die mehr als einen Standort und dementsprechend mehrere IP-Netze betreuen. Hierbei ist es möglich, an jedem Standort einen CSI-Agenten im sogenannten "Network Appliance Mode" zu betreiben und zeitgesteuerte Scans durchzuführen – vergleichbar mit einem Relay- oder Antivirenserver. Die Ergebnisse werden von den einzelnen Agenten dann im Anschluss zur eigentlichen CSI-Konsole gesendet und können zentral ausgewertet werden.

Neu in der aktuellsten Version ist außerdem, dass Systeme, die mit dem Personal Software Inspector (PSI) ausgestattet sind, sich ebenso in den CSI einbinden lassen. Hierfür ist lediglich ein festzulegender Code auf der Client-Seite notwendig. Dieser wird dann im Anschluss in das hierfür vorgesehene Feld innerhalb der Konsole eingetragen.

Arbeit mit dem CSI Dashboard

Das Dashboard des CSI wartet mit einer frei anpassbaren Oberfläche auf. Diese erlaubte es uns mittels verschiedener Elemente, unsere eigene Oberfläche per Drag & Drop zu konfigurieren. Angefangen von einem generellen Sicherheitsstatus der Umgebung bis hin zu einzelnen Installationen und Gefährdungen lässt sich alles für den ersten Blick in der Konsole konfigurieren. Sehr gut ist ebenso die mitgelieferte Funktion der Historie, die einen chronologischen Überblick über den Sicherheitsstatus liefert und so schnell Änderungen innerhalb der Umgebung aufzeigt.

CSI unterstützt mehrere Scan-Methoden und liefert so für verschiedene Einsatzzwecke die passenden Wege. Der Scanprozess ruft dabei die spezifischen Metadaten der einzelnen Applikationen ab, primär .EXE-, .DLL- und .OCX-

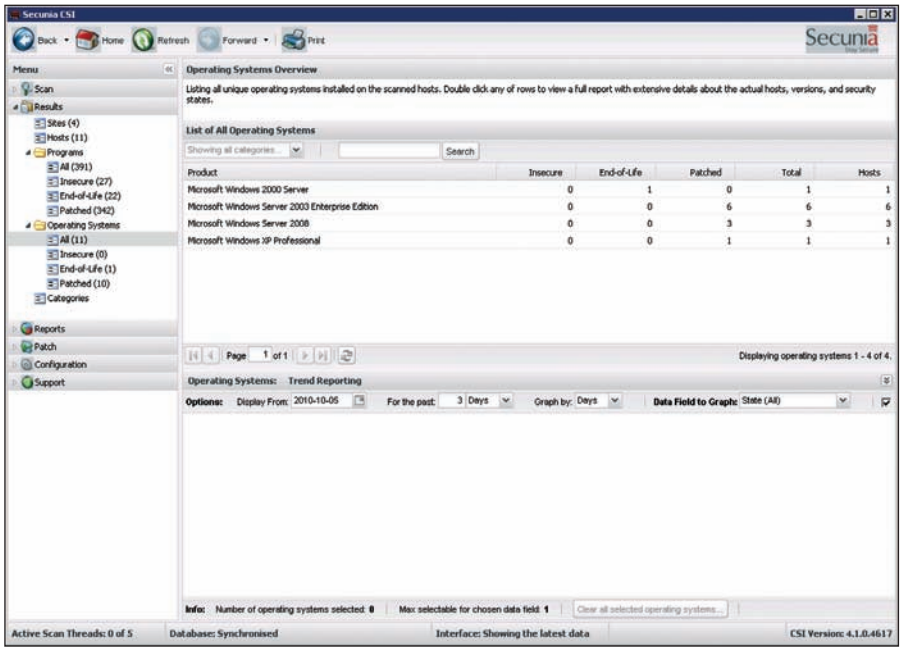


Bild 3: Die Ergebnisse eines ersten Scans

Dateien, und erstellt eine vollständige Inventarisierung der installierten Software. Diese Ergebnisse werden dann mit der "Secunia Secure Data Processing Cloud" (DPRC) und den hinterlegten Dateisignaturen abgeglichen. In einem weiteren Schritt werden dann die Secunia Advisory- und Vulnerability-Datenbanken abgefragt und den jeweiligen Sicherheitslücken und Programmen zugeordnet. Als Ergebnis daraus erhält der Administrator eine präzise Inventarisierung aller installierten Applikationen, deren Versionen und dem genauen Sicherheitsstatus mit Hinweisen auf die bereits veröffentlichten Security Advisories.

Innerhalb der CSI-Konsole stehen dafür mehrere Scantypen zur Verfügung. Zum einen ist es über einen "Quick Scan" möglich, einen einzelnen Client durch Eingabe der IP-Adresse oder des DNS-Namens abzufragen. Zum anderen besteht auch die Möglichkeit, Gruppen anzulegen. Diese wiederum können dann manuell geprüft oder mit einem geplanten Scan auf Sicherheitslücken getestet werden.

Unter dem Menüpunkt "Results" erhält der Administrator einen schnellen Überblick über alle Systeme und kann dort direkt einsehen, welche Programme installiert sind. Zudem erhält er hier einen direkten Überblick über Informationen und Sicherheitslücken.

Umfassendes Reporting

Der Menüpunkt "Reports" bietet dem IT-Verantwortlichen ein umfangreiches Werkzeug, mit dem sich die eingesetzten Betriebssysteme, Service Packs und Anwendungen sinnvoll betrachten und entsprechend den bekannten Risiken bewerten lassen. Dabei unterscheidet CSI zwischen den drei Kategorien:

- Insecure: Unsicher, es bestehen Sicherheitslücken
- End-of-Life (EoL): Produktlebenszyklus beendet, es besteht kein Support mehr
- Patched: Keine bekannten Sicherheitslücken vorhanden

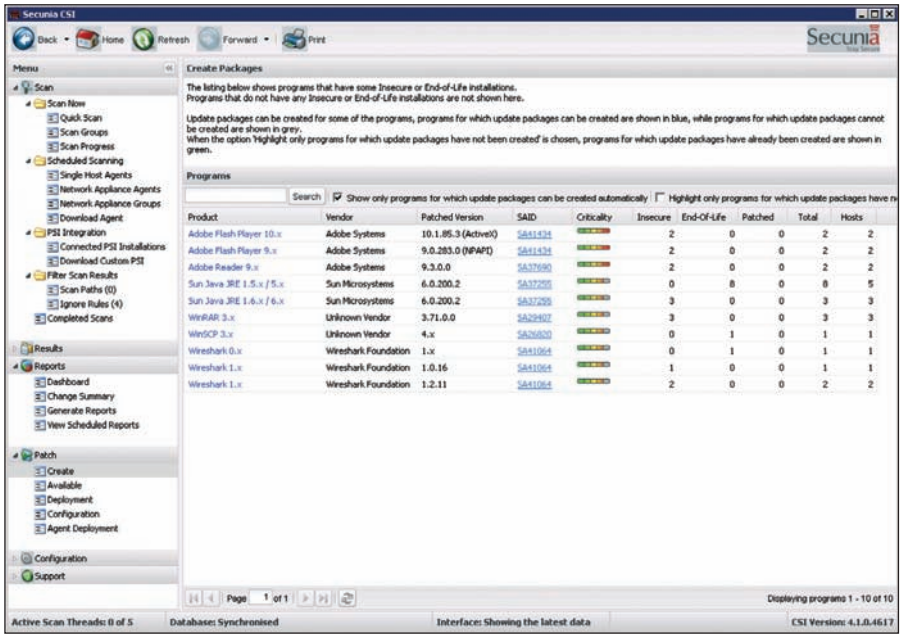


Bild 4: CSI findet notwendige Patches und erlaubt auch, diese gleich zur Verteilung zu paketieren

Für Programme, die aus verschiedenen Gründen nicht aktualisiert werden können, erstellten wir mittels eines Assistenten eine Ausnahmeregel. Damit erreichten wir, dass diese nicht wiederkehrend geprüft werden. Aus sicherheitstechnischer Sicht sollte dies jedoch nur sehr vorsichtig genutzt werden, denn ansonsten droht ein trügerisches Gefühl der Sicherheit. Daher sollten diese Programme auch regelmäßig betrachtet werden.

Darüber hinaus bietet CSI die Möglichkeit, täglich per E-Mail über den aktuellen Status benachrichtigt zu werden. Diese Mitteilungen liefern auch Veränderungen im sogenannten Change Summary. Dieses erkennt, ob neue Software installiert wurde und informiert darüber hinaus über deren eventuelle Risiken.

Außerdem erlaubte es uns CSI, verschiedene Report-Groups zu definieren. Hiermit erhalten IT-Abteilungen die Möglichkeit, mehrere Systemverantwortliche zu definieren, die wiederum angepasste, auf Ihre Systeme ausgelegte Reports per E-Mail erhalten. Ferner ließen sich verschiedene Reports automatisch generieren und per E-Mail zustellen. Hier boten sich uns vier Berichtstypen an:

- Executive Summary Report: Sicherheitsbericht über alle Systeme (geeignet für IT-Sicherheitsverantwortliche und IT-Leiter)
- Administrative Report: Sicherheitsbericht über alle Systeme des Verantwortungsbereiches (geeignet für verschiedene Administratoren, zum Beispiel: Server- und Clientadministratoren)
- Host-Level-Report: Sicherheitsbericht über bestimmte ausgewählte Clients (geeignet für als hochkritisch eingestufte Systeme)
- Program-Level-Report: Sicherheitsbericht über bestimmte ausgewählte Programme (geeignet für Applikationsverantwortliche, Softwareentwickler)

Patches finden und verteilen

Die größte Neuerung in CSI bildet der Punkt "Patch". Hierüber lassen sich die Microsoft-Mechanismen für die Verteilung von Updatepaketen nutzen. Dafür werden die innerhalb der Scans gefundenen Schwachstellen mit der Secunia-Datenbank verglichen und im Anschluss angezeigt, ob für diese Applikationen eine Paketierung möglich ist. CSI bietet dabei zur Unterstützung einen direkten Downloadlink zur benötigten Herstellerseite an – daher ist auch kein

langes Suchen nach der aktuellsten Version mehr notwendig.

Die innerhalb der CSI-Konsole implementierte Paketierungsfunktion erstellt aus dem heruntergeladenen Programmupdate ein geeignetes, WSUS-kompatibles Paket und stellt es für die Verteilung innerhalb von CSI bereit. Die Bereitstellung kann dann über die im WSUS konfigurierten Computergruppen freigegeben werden. Die Bereitstellung der zuvor mit CSI paketierten Updates erfolgt im Anschluss dann über den bekannten Windows-Update-Dienst.

Fazit

Secunia bietet mit dem Corporate Software Inspector 4.0 ein bisher nicht dagewesenes Werkzeug, mit dem der IT-Administrator seine IT-Infrastruktur zu jederzeit bezüglich existierender Sicherheitslücken überwachen und auch patchen kann. Durch die umfangreichen Sicherheitsberichte, die zusätzlich innerhalb der Lösung bereitgestellt werden, ist stets eine Einschätzung der Sicherheitsanfälligkeiten möglich.

Durch die Symbiose aus einer bereits bestehenden Patch Management-Lösung und der CSI-Komponente erhöht das Werkzeug das Sicherheitsniveau signifikant. Dabei bietet Secunia für fast alle Infrastrukturarten, egal ob klein oder Mittelstand, die geeigneten Scans, Agenten (agent-less und agent-based), Methoden (Appliance-Mode) und Lizenzmodelle an.

Als wir während unseres Tests einen kleineren Fehler innerhalb der Oberfläche feststellten, wurde dieser übrigens – nach kurzem E-Mailkontakt mit Secunia und der zuständigen Entwicklungsabteilung – innerhalb von weniger als zwei Stunden behoben. Vorbildlich, wie wir finden. *(jp)*

Thomas Gronenwald ist Security-Berater bei der adMERITia GmbH in Langenfeld und Blog-Autor (blog.port389.de).

Produkt

Software zum Finden und Patchen von Sicherheitslücken.

Hersteller

Secunia
www.secunia.com

Preis

Secunia bietet derzeit vier Lizenz- und Preismodelle an:

Secunia CSI Small Business, Standard Support
Microsoft WSUS-Integration mit weniger als 100 Clients: 2.000 Euro.

Secunia CSI, Standard Support
Microsoft WSUS-Integration mit weniger als 400 Clients: 6.000 Euro.

Secunia CSI Professional, Premium Support
Microsoft SCCM- und Microsoft WSUS-Integration mit weniger als 1.000 Clients: 12.000 Euro.

Secunia CSI Enterprise, Enterprise Support
Microsoft SCCM- und Microsoft WSUS-Integration mit mehr als 1.000 Clients: 24.000 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation und Konfiguration	9
Funktionsumfang	8
Reports	10
Patchmanagement (Drittanbieter)	7
Sicherheitsscan	9

Dieses Produkt eignet sich

optimal für Unternehmen, die überwiegend Microsoft-basierte Betriebssysteme und Anwendungen betreiben und zudem bereits eine Microsoft Patch-Management-Lösung einsetzen.

bedingt für mittelständische und große Unternehmen, die andere Bereitstellungsmechanismen nutzen und darüber hinaus keine geeigneten Microsoft Patch-Management-Lösungen einsetzen.

nicht für Unternehmen, die zum größten Teil Linux-basierte Betriebssysteme und Applikationen einsetzen.

Secunia Corporate Software Inspector 4.0

Einkaufsführer: Voice over WLAN-Umgebungen

Sprache ganz ungebunden

von Hans-Dieter Wahl

Mobilität und damit einhergehend die drahtlose Kommunikation innerhalb eines Unternehmens werden immer wichtiger. Dazu zählt neben der Datenmobilität auch die Beweglichkeit in Bezug auf die Sprachkommunikation. Diese lässt sich unter anderem durch VoIP über WLAN erreichen. Welche Aspekte Sie für den Aufbau einer solchen Umgebung beachten müssen, zeigt Ihnen dieser Einkaufsführer.

Im Zusammenhang mit der mobilen Kommunikation im Unternehmen wird oft das Schlagwort "One Number Reach" verwendet. Dieser Begriff beschreibt nichts anderes, als dass ein Teilnehmer sowohl an seinem Arbeitsplatz als auch unterwegs im Unternehmen sowie außerhalb unter einer Rufnummer erreichbar sein soll. Um die Forderung der Mobilität im Unternehmen zu realisieren, ist eine Komponente für die Telefonanlage des Unternehmens nötig, um diese mit drahtlosen Telefonen zu erweitern. Technisch umgesetzt wird drahtlose Telefonie im Unternehmen häufig durch DECT-Systeme. Dieser Standard ist etabliert, hat aber den Nachteil, dass ein eigenes unabhängiges DECT-Funknetz im Unternehmen aufgebaut werden muss. Viele Unternehmen haben aber bereits eine WLAN-Infrastruktur, um Ihre mobilen Datengeräte, wie Notebooks, PDAs, Wireless Barcode Scanner und vieles mehr, anzubinden. In Verbindung mit einer Voice over IP-fähigen Telefonanlage lässt sich die WLAN-Infrastruktur daher hervorragend für Voice over WLAN nutzen.

Besonders wichtig: Das WLAN-Netz muss absolut lückenlos im Unternehmen verfügbar sein, dazu zählen auch Nebenräume, Treppenhäuser, Garagen und ähnliche Bereiche – schließlich möchten die Mitarbeiter überall telefonisch erreichbar sein. Dazu sollten Sie die WLAN-Infrastruktur und die WLAN-Ausleuchtung von einem Fachmann überprüfen lassen. Sicherlich muss in fast allen Fällen die Anzahl der Access Points erhöht werden, um die notwendige Funkabdeckung zu erreichen. Nähere technische Informationen hierzu finden Sie unter anderem im kommenden Sonderheft I/2011 sowie im "VoIP Praxisleitfaden" [1].

Auswahl der Hardware

Wenden wir uns nun den Auswahlkriterien für VoWLAN-Telefone zu, die Sie berücksichtigen sollten. Auf die ergonomischen und ästhetischen Gesichtspunkte, über deren Wichtigkeit je nach Unternehmenseinsatz individuell entschieden werden muss, soll hier nur stichpunktartig eingegangen werden. Hierzu zählen natürlich Dinge wie die Größe und Lesbarkeit des Displays, aber auch die Robustheit und Lebensdauer des Gerätes. In manchen Unternehmen wird auch das Gerätedesign entscheidend sein. Um die Benutzbarkeit der Telefone je nach Einsatz zu erhöhen, sollte ein Blick auf die Liste der angebotenen Zubehörteile nicht fehlen. Manche Hersteller bieten hier neben größeren Akkus und Headsets auch drehbare Gürtelbefestigungen an, bei denen das Telefondisplay ohne Abnehmen des Gerätes vom Gürtel abgelesen werden kann. Ein weiteres wichtiges Zubehör sind Rack-Ladeeinrichtungen. Diese Einrichtung dient nicht nur als zentrale Aufladestation für die Akkus, sondern lässt etwa einen Schichtleiter im Betrieb bei Bedarf erkennen, welcher Mitarbeiter gerade an- beziehungsweise abwesend ist. Einige Telefone können darüber hinaus das Einstecken in die Ladeschale auswerten und beispielsweise im Falle der Abwesenheit eine automatische Rufweiterschaltung aktivieren.

Darüber hinaus gibt es eine Reihe allgemeiner technischer Geräteeigenschaften, auf die Sie achten sollten. An erster Stelle ist hier die Batterielaufzeit des Gerätes zu nennen. Wir unterscheiden zwischen der Sprechzeit und der Stand-by Zeit. Gute Geräte erreichen Sprechzeiten von acht Stunden und Stand-by Zeiten von bis zu 40 Stunden oder mehr. Dies sind erstmals Zeiten, die einen professionellen Einsatz im beruflichen Umfeld ermöglichen. Im direkten Vergleich mit aktuellen DECT-Endgeräten schneidet WLAN allerdings noch immer schlechter ab, was an den technischen Anforderungen der WLAN-Technologie liegt. Trotzdem werden die oben angegebenen Werte durch die konsequente Anwendung von Stromsparmechanismen erreicht, die im WLAN-Standard vorgesehen sind. Besonders zu erwähnen ist das Verfahren U-APSD (Unscheduled Automatic Power Save Delivery). Dabei schaltet der WLAN-Client (VoWLAN-Telefon) während eines aktiven Gespräches immer dann, wenn gerade kein Datenpaket über die WLAN-Funkverbindung geschickt werden muss, seine WLAN-Hardware in den Stromsparmodus. Dabei ist besonders wichtig,

Bild 1: Access Points mit abgesetzter MIMO-Antenne lassen sich im Unternehmen unauffällig unterbringen

dass auch der Access Point dieses Verfahren unterstützt, denn dieser muss alle Datenpakete, die an das Telefon geschickt werden, während der Power Down-Phase zwischenspeichern.

Zentrales Management und Telefonbuch

Als weitere Systemeigenschaft sollten Sie berücksichtigen, in welcher Art und Weise sich die Geräte konfigurieren und verwalten lassen. Für Unternehmen mit einer großen Anzahl mobiler Telefone ist dabei wichtig, dass der Hersteller des VoWLAN-Telefons zentrale Managementsysteme anbietet, mit denen sich die Konfiguration und die Softwarestände der Geräte zentral verwalten lassen. Zu den dezentralen Methoden hingegen zählen die Konfiguration über die Bedienoberfläche am Telefon selbst, eine eventuelle Webbrowser-Konfiguration oder die Konfiguration über Programmieradapter und PC-gestützter Software. Bei den letztgenannten Verfahren ist darauf zu achten, dass die Software für die gängigen Betriebssysteme verfügbar ist und welche Kosten eventuell für Software und Programmieradapter aufgewendet werden müssen.

Mobile Endgeräte bieten heute Telefon-Komfortfunktionalitäten, auch wenn es hier aufgrund der beschränkten Anzahl von Tasten einige Einschränkungen gibt. Funktionen wie Halten, Makeln, Rückfrage und Anruferliste mit Zeitstempeln sind bei fast jedem Telefon Standard. Dies gilt auch für Merkmale wie Mehrsprachenfähigkeit, Freisprechen und Lauthören. Wichtiger noch ist es zu beachten, wie der Anbieter des VoWLAN-Telefons das Telefonbuch realisiert hat. Handelt es sich nur um ein lokales Telefonbuch, stellt sich für kleinere und mittlere Unternehmen die Frage, ob dieses nur lokal oder auch zentral verwaltet werden kann. Größere Unternehmen dürften auf ein zentrales LDAP-basiertes Systemtelefonbuch kaum verzichten können.

WLAN-Standards und -Telefonie

Jetzt stellt sich noch die Frage nach dem WLAN-Standard, den das Telefon unterstützt. Ein VoWLAN-Telefon benötigt zwar nur rund 80 KBit/s Bandbreite für ein Telefongespräch, dennoch sollte das Telefon mindestens 802.11g (54 MBit/s) unterstützen. Einige ältere Modelle unterstützen lediglich 802.11b (11 MBit/s) – das genügt zwar für Telefonate, doch bremst bereits ein einziges WLAN-Gerät, das nach dem alten 802.11b-Standard arbeitet, das gesamte Netz auf 11 MBit/s herunter und schränkt damit die Mitbenutzung der WLAN-Infrastruktur durch andere Endgeräte wie Notebooks mit höherem Bandbreitenbedarf stark ein.

Anders sieht es mit der Interoperabilität zwischen dem neuen 802.11n-Standard und der gleichzeitigen Verwendung von 802.11g-Geräten im gleichen Netz aus. Der neue n-Standard leistet bis zu 300 MBit/s und erlaubt Interoperabililtät zu 802.11g-Geräten, ohne den Datendurchsatz anderer im WLAN befindlicher 802.11n-Geräte zu reduzieren. Derzeit sind bereits erste VoWLAN-Telefone am Markt oder befinden sich in der Markteinführung, die auch 802.11n unterstützen. Diese Geräte haben aus Stromspargründen nur eine sogenannte 1x1 Mimo-Technik und erlauben bis zu 75 MBit/s Datendurchsatz – damit lässt sich gegenüber den 802.11g-Geräten eine etwas größere Anzahl von gleichzeitigen Gesprächen führen. Ein echtes Kaufargument für 802.11n-Telefone ist dies aber nicht. Wählen Sie daher Telefone aus, die mindestens 802.11g (54 MBit/s) unterstützen. Einige moderne VoWLAN-Telefone unterstützen neben dem Betrieb in 2,4 GHz-Netzen auch den Betrieb in 5 GHz-Netzen. Bei 5 GHz ist die Ausbreitungscharakteristik deutlich schlechter als bei 2,4 GHz, dadurch müssen für ein 5 GHz VoWLAN-Netz deutlich mehr Access Points als für ein 2,4 GHz-Netz gesetzt werden. So dürfte sich VoIP im 5 GHz-WLAN nicht durchsetzen, da die Wirtschaftlichkeit leidet.

WLAN und die Sicherheit

SRTP (Secure Real-Time Transport Protocol) nach RFC 3711 und andere Ende-zu-Ende-Verschlüsselungstechnologien finden sich bei VoWLAN-Telefonen im Gegensatz zu kabelgebundenen VoIP-Telefonen nicht. Eine sichere Verschlüsselung der Funkschnittstelle ist daher unabdingbar. Dass die WEP-basierte Verschlüsselung nicht sicher ist, hat sich inzwischen weitgehend herumgesprochen, dennoch sind in unteren Preisklassen gelegentlich derartige Geräte vorzufinden. Ein modernes VoWLAN-Telefon muss WPA2-PSK und WPA2-Enterprise (802.1x) unterstützen. In der Regel sollte die Verwendung von WPA2-PSK (WiFi Protected Access 2 mit Pre-Shared-Key) genügen. Der Vorteil bei WPA2-PSK ist, dass keine weitere Infrastruktur nötig ist, demgegenüber steht ein höherer Bearbeitungsaufwand bei einem eventuell notwendigen Tausch der Pre-Shared-Keys in den Endgeräten und Access Points. Zur Vermeidung dieses Aufwands machen größere Unternehmen daher gern von WPA2-Enterprise (802.1x) Gebrauch, auch wenn dieser Standard einige Nachteile beim Seamless Roaming mitbringt.

Seamless Roaming mit Tücken

Seamless Roaming sorgt dafür, dass das VoWLAN-Telefon sich auch während eines Telefongespräches von einer Funkzelle in die nächste bewegen kann, ohne dass das Gespräch abreißt und es zu Gesprächsunterbrechungen oder Störgeräuschen kommt. Dazu muss das Telefon bereits frühzeitig im Hintergrund nach einem neuen stärkeren Access Point suchen. Um die Suche nur auf die relevanten Funkkanäle zu begrenzen, verwenden die meisten VoWLAN-Telefone einen sogenannten Channel Plan, in dem der Administrator vorgibt, welche Funkkanäle (beispielsweise 1, 6 und 11) gescannt werden sollen. Nachdem sich dann das VoWLAN-Telefon mit einem neuen Access Point verbunden hat, muss die Sicherheit wiederhergestellt werden. Dies geschieht zwar automatisch, aber je nach verwendetem Sicherheitsstandard müssen einige Meldungen hin- und hergeschickt werden, um die Verbindung endgültig wiederherzustellen – dies kostet wiederum wertvolle Zeit.

Beim Wiederherstellen der Security ist besonders das Interworking zwischen Access Point und VoWLAN Telefon wichtig. Gut abgestimmte Implementierungen realisieren bei WPA2-PSK Verschlüsselung Roamingzeiten von unter 40 ms. Leider gibt es bei den meisten Geräten keine verlässlichen Angaben in den Datenblättern über die erreichbaren Roamingzeiten sowie über die verwendeten Verfahren.

Protokolle und Codecs

Die heute üblichen IP-TK-Anlagen verwenden zur Verbindungssteuerung SIP (Session Initiation Protocol) nach RFC3261. Protokolle nach ITU H.323 spielen kaum noch eine Rolle. Daher genügt es in fast allen Fällen, wenn ein VoWLAN-Telefon SIP unterstützt. Der Bandbreitenbedarf für ein Telefongespräch, das nach G.711 unkomprimiert übertragen wird, beträgt etwa 80 KBit/s. Die Übertragung als unkomprimiertes Signal hat den Vorteil, dass es zu keinen Qualitätseinschränkungen kommt. Aus diesem Grund arbeiten alle IP-TK-Anlagen vorzugsweise mit G.711. Da im WLAN und auch im LAN genügend Bandbreite zur Verfügung steht, spricht also nichts gegen eine unkomprimierte Übertragung. Die Sprachcodecs, die eine Datenkompression realisieren, wie beispielsweise G.729, G.723.1, G.726, werden also für ein VoWLAN-Telefon, das an einer IP-TK-Anlage angeschlossen wird, nicht benötigt. Im Gegensatz dazu gewinnt der hochqualitative Breitband-Codec G.722 im VoIP-Umfeld immer mehr an Bedeutung. Dieser Trend wird sich fortsetzen, wenn, wie bereits angekündigt, einige namhafte SIP-Provider diesen Standard unterstützen.

Einige VoWLAN-Geräte bieten Zusatzfunktionen wie Messaging, mit der beispielsweise in einem Krankenhaus Notfallteams kurzfristig zusammengerufen werden können oder mit deren Hilfe ein Ausfall einer Maschine direkt auf das Mobilteil des Technikers signalisiert werden kann. Einige Telefone haben darüber hinaus auch Alarmtasten und Push-to-Talk-Funktionen. Diese Funktionen können je nach Art des Unternehmens unterschiedlich eingesetzt werden und helfen dabei, Abläufe zu optimieren oder ersetzen andere Rufsysteme.

Eine IP-TK Anlage mit VoWLAN-Telefonen besteht aus mindestens drei Kom-

Auswahlkriterien VoWLAN-Telefone

Funktionen	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Gesprächszeit ohne Akkuwechsel	sehr wichtig	sehr wichtig	sehr wichtig
Stand-by Zeit ohne Akkuwechsel	sehr wichtig	sehr wichtig	sehr wichtig
Ergonomie (Größe und Lesbarkeit des Displays)	wichtig	wichtig	wichtig
Standard-Funktionen wie Makeln, Rückfrage, Halten	wichtig	wichtig	wichtig
Zentrale Konfiguration für alle VoWLAN-Telefone im Netz	weniger wichtig	wichtig	sehr wichtig
Zentrales Telefonbuch	weniger wichtig	wichtig	wichtig
WLAN-Standard 802.11n (> 54 MBit/s)	weniger wichtig	weniger wichtig	weniger wichtig
WLAN-Sicherheitsstandards WPA2-PSK	sehr wichtig	sehr wichtig	sehr wichtig
WLAN-Sicherheitsstandards 802.1x	weniger wichtig	wichtig	wichtig
QoS / WMM 802.11e	sehr wichtig	sehr wichtig	sehr wichtig
SIP nach RFC3261	sehr wichtig	sehr wichtig	sehr wichtig
Sprachcodecs G.711 (64 KBit/s)	sehr wichtig	sehr wichtig	sehr wichtig
Kompatibilität zu anderen Herstellern	wichtig	wichtig	wichtig

ponenten, der IP-TK Anlage, den Wireless Access Points und den VoWLAN-Telefonen. Alle drei Komponenten arbeiten nach entsprechenden Standards und gewährleisten schon dadurch eine gewisse Kompatibilität. Die Tücken liegen aber hier oftmals im Detail, da die Parameter aller drei Komponenten sorgfältig aufeinander abgestimmt werden müssen. Die Hersteller der meisten VoWLAN-Telefone zertifizieren regelmäßig Drittanbieter-Komponenten und geben entsprechende Beispielkonfigurationen heraus. Wenn für eine vorhandene Infrastruktur keine solche Zertifizierung vorliegt, sollte ein Fachmann hinzugezogen werden, der die Geräte aufeinander abstimmt.

Der Einsatz von Smart-Phones als VoWLAN Telefon

Viele moderne Smart-Phones bieten WLAN und VoIP an und sind durchaus kompatibel mit einer vorhandenen IP-TK-Anlage und einer WLAN-Infrastruktur. Jedoch haben manche Geräte erhebliche Schwachstellen in Bezug auf das lückenlose Roaming zwischen den Access Points. Ebenso werden oft nur kurze Akkulaufzeiten erreicht, weil entsprechende Stromsparmechanismen nicht oder nur unzureichend implementiert sind. In kleinen Unternehmen mit nur wenigen Büros ist oftmals nur ein Access Point vorhanden, dort spielt das Roaming keine Rolle und ein Smart-Phone kann durchaus als Ersatz für ein professionelles VoWLAN-Telefon herangezogen werden.

Fazit

VoWLAN ermöglicht es, die vorhandene WLAN-Infrastruktur für das Telefonieren mitzubenutzen. Wenn ein professioneller Einsatz in einem mittleren oder größeren Unternehmen geplant ist, sollte jedoch ein Dienstleister oder Hersteller, der entsprechende Services anbietet, hinzugezogen werden, um die Funkausleuchtung zu optimieren und die VoWLAN-Telefone optimal den vorhandenen Gegebenheiten anzupassen. Die Auswahl des richtigen Telefons ist sehr wichtig – jedoch ist das Interworking mit den weiteren Komponenten wie der Telefonanlage und dem drahtlosen Netz mindestens genauso bedeutend. In kleinen oder sehr kleinen Unternehmen kann bereits ein einfaches VoWLAN-Telefon oder sogar ein Smart-Phone verwendet werden, denn hier spielen Roaming und andere Einschränkungen möglicherweise nur eine untergeordnete Rolle. *(dr)*

Dipl.-Ing. Hans-Dieter Wahl ist Produktmanager bei Funkwerk Enterprise Communications GmbH in Nürnberg.

Literatur

[1] VoIP Praxisleitfaden
Dr. Jörg Fischer, ISBN-10: 3-446-41188-7

Sicherheit für das WLAN

Abhörsicher

von Thomas Hümmler

In einem nicht ausreichend gesicherten WLAN gibt es einfache Möglichkeiten, das Funknetz aufzuspüren und über ungesicherte Zugänge einzudringen. In diesem Workshop erfahren Sie, wie Angreifer vorgehen und was Sie als Administrator unternehmen sollten und sogar müssen, um sich vor unberechtigten Zugriffen zu schützen. Dabei zeigen wir, wie sich WLANs mit den Linux-Standardtools Kismet und Aircrack-ng auf Schwachstellen prüfen lassen. Sie erfahren dabei, wie sich mit Kismet WLAN-Aktivitäten aufzeichnen lassen und wie Aircrack-ng Passwörter entschlüsselt.

Von Kismet spricht ein Muslim, wenn er das Schicksal meint. Kismet ist aber auch der Name eines Sniffers, mit dem sich Funknetzwerke aufspüren lassen. Das Programm läuft unter Linux und Mac OS, in der Bezeichnung Kiswin auch als Client unter Windows. In Verbindung mit dem Programm GPSDrive kann Kismet WLAN-Zugangspunkte kartographisch erfassen. Mit Schicksal hat das allerdings nichts mehr zu tun. Diese Methode ist als Wardriving bekannt, wobei "War" nicht für Krieg steht, sondern als Akronym für "Wireless Access Revolution". Wardriver kennzeichnen offene Hot Spots, so dass andere diese als Internetzugänge nutzen können.

Wardriver bewegen sich in Deutschland in einer rechtlichen Grauzone. Denn die Nutzung eines offenen, privaten WLANs kann als unerlaubtes Abhören einer Funkanlage gewertet werden; das ist nach dem Telekommunikationsgesetz verboten. Allerdings lehnte zuletzt in diesem Jahr das Amtsgericht Wuppertal (Aktenzeichen 20 Ds-10 Js 1977/08-282/08) die Eröffnung eines Hauptverfahrens ab, weil die Strafbarkeit des Angeschuldigten nicht ersichtlich war. Der Beschuldigte hatte zweimal einen offenen Access Point als Internetzugang genutzt, allerdings keine Daten ausgespäht. Auch der Umstand, dass der Täter billigend eine finanzielle Schädigung des WLAN-Besitzers in Kauf genommen hatte (der eventuell keine Flatrate hatte), war für ein Verfahren nicht ausreichend.

Der Zugang zu offenen und WEP-verschlüsselten Access Points ist banal. Bösewichte benötigen nur ein Notebook mit WLAN-Karte und entsprechende, überall erhältliche Freeware-Tools. Was sich in dem Wuppertaler Urteil eher wie die Spielerei eines Schülers liest, könnte ebenso auch von Angreifern mit wirtschaftlichen Interessen kommen, die das WLAN nicht zum Surfen nutzen, sondern interne Daten ausspähen und an die Konkurrenz weitergeben.

Wer nicht sichert, haftet

Schon aus diesem Grund ist es wichtig, das eigene WLAN abzusichern. Einen weiteren Grund liefert ein Urteil des Bun-

```
Datei  Bearbeiten  Ansicht  Terminal  Hilfe
    Last       : "Mon Oct 11 09:13:34 2010"
    Min Loc: Lat 90.000000 Lon 180.000000 Alt 0.000000 Spd 0.000000
    Max Loc: Lat -90.000000 Lon -180.000000 Alt 0.000000 Spd 0.000000

Network 30: "<no ssid>" BSSID: "00:0F:B5:C9:B0:3C"
    Type       : infrastructure
    Carrier    : 802.11b
    Info       : "None"
    Channel    : 11
    Encryption : "None"
    Maxrate    : 22.0
    LLC        : 1
    Data       : 0
    Crypt      : 0
    Weak       : 0
    Dupe IV    : 0
    Total      : 1
    First      : "Mon Oct 11 09:03:02 2010"
    Last       : "Mon Oct 11 09:03:02 2010"
    Min Loc: Lat 90.000000 Lon 180.000000 Alt 0.000000 Spd 0.000000
    Max Loc: Lat -90.000000 Lon -180.000000 Alt 0.000000 Spd 0.000000

Network 31: "FRITZ!Box WLAN 3170" BSSID: "00:24:FE:A1:31:91"
    Type       : infrastructure
    Carrier    : 802.11b
    Info       : "None"
    Channel    : 01
    Encryption : "WEP TKIP WPA PSK AES-CCM "
    Maxrate    : 11.0
    LLC        : 280
    Data       : 0
```

Bild 1: Mancher denkt fälschlicherweise, ohne ESSID würde ein Funknetz nicht entdeckt werden; dass die Mac-Adresse hinter BSSID zur Identifikation bereits reicht, ist kein allgemeines Wissen

desgerichtshofs (Aktenzeichen: I ZR 121/08) in Bezug auf WLAN und Störerhaftung vom Mai diesen Jahres. Hierin kommt der BGH zu dem Schluss, dass die "Prüfpflicht mit der Folge der Störerhaftung verletzt ist, wenn die gebotenen Sicherungsmaßnahmen unterbleiben". Oder anders: Wer sein WLAN nicht vernünftig absichert, haftet im Rahmen der Störerhaftung für Folgeschäden mit. Als abgesichert gilt ein Router, in dem die zum Kaufzeitpunkt marktüblichen Sicherungen ihrem Zweck entsprechend wirksam eingesetzt werden.

Was aber heißt marktüblich? Spätestens seit dem Jahr 2003 ist der als sicher geltende WPA-Standard verbreitet und marktüblich. WLAN-Router dieses Baujahrs und jünger müssten somit mindestens diese Verschlüsselung nutzen. Wer keine oder nur die unsichere WEP-Verschlüsselung einsetzt, wäre damit ein Fall für die Störerhaftung.

Kismet als passiver Schnüffler

Kismet [1] ist ein sogenannter passiver Sniffer. Das Programm liest also nur die Daten mit, die zwischen Access Point und angeschlossenen Geräten verschickt werden. Das funktioniert, indem die WLAN-Karte des Empfängers in den Monitormodus geschaltet wird. So erlaubt es, selbst sogenannte versteckte WLAN-Kennungen zu finden. Kismet unterstützt sogar Plug-Ins, mit denen beispielsweise DECT ausspioniert oder ein WEP-geschütztes WLAN geknackt werden kann. Mit sogenannten Dronen kann der Benutzer Kismet in ein verteiltes Intrusion Detection System verwandeln. Damit löst das System verschiedene Alarme, basierend auf "Fingerabdrücken" und Trends bestimmter Angreifer, aus. So protokolliert es unter anderem Netstumbler-Anfragen, aber auch SSID-Brute-Force-Angriffe mit dem Perl-Programm Wellenreiter. Weitere Fähigkeiten des frei zugänglichen Sniffers:

- Sniffing von Funknetzen der Typen 802.11b, 802.11g, 802.11a, 802.11n
- Multi-Card-Unterstützung und Channel-Hopping
- Runtime-WEP-Decoding
- Versteckte SSIDs entdecken

Unter Ubuntu ist das Tool schnell installiert: Ein *apt-get install kismet* genügt, anschließend müssen Sie nur noch zwei Zeilen in der Konfigurationsdatei */etc/kismet/kismet.conf* anpassen. Die Zeile "suiduser=your_name_here" sollte den Namen des Kismet-Nutzers enthalten; allerdings müssen Sie Kismet als Root starten, normale Nutzer werden in der Standardeinstellung nicht akzeptiert. Des Weiteren muss die Zeile "source=none,none,addme" unbedingt angepasst werden. Hier tragen Sie den Wireless-Treiber ein (etwa "ath5k"), die Schnittstelle (zum Beispiel "wlan0") und einen beliebigen Namen für diese Quelle, so dass die Zeile anschließend beispielsweise lautet:

```
source=ath5k,wlan0,wlan
```

Welche Treiber verfügbar sind, steht unter Ubuntu oder Debian in der Datei */usr/share/doc/kismet/README.gz*. Den Rest der Konfiguration können Sie unverändert lassen. Nun starten Sie mit *kismet* den Sniffer. Das Programm listet alle gefundenen WLAN-Netze auf und schreibt die Daten in seine Log-Dateien unter */var/log/kismet*; die Liste der Netze steht in der Datei */var/log/kismet/Kismet-{DATUM}-{Nr}.network*. Unsere zwei Kilometer kurze Wardriving-Testfahrt zeigte Erschreckendes: Von 123 gefundenen Netzen sind 18 nur mit WEP verschlüsselt und sechs WLAN-Access Points überhaupt nicht – somit wäre jeder fünfte Betreiber ein Fall für die Störerhaftung.

Sichere Passwörter mit Aircrack-ng

Das zweite Tool, das in jeder Linux-Standarddistribution mitgeliefert wird, ist Aircrack-ng [2]. Aircrack-ng kann WEP- und WPA-PSK-Passwörter knacken, wenn genügend Datenpakete zur Verfügung stehen. Dazu nutzt es verschiedene Kryptoattacken: Der Standardangriff ist die sogenannte PTW-Methode (nach Andrej Pyshkin, Erik Tews und Ralf-Philipp Weinmann von der TU Darmstadt), mit der ein WEP-Schlüssel in weniger als einer Minute entschlüsselt wird [3]. Ein weiterer ist der FMS-Angriff, der von Scott Fluhrer von Cisco Systems sowie Itsik Mantin und Adi Shamir vom israelischen Weizmann-Institut bereits 2001 beschrieben wurde [4]; damit kann ein WEP-Schlüssel aus vier bis sechs Millionen Datenpaketen entschlüsselt werden. Dieser Algorithmus wurde von einem Hacker namens KoreK verbessert, sodass für einen 104-Bit-Schlüssel 500.000 bis zwei Millionen Datenpakete ausreichen. Auch

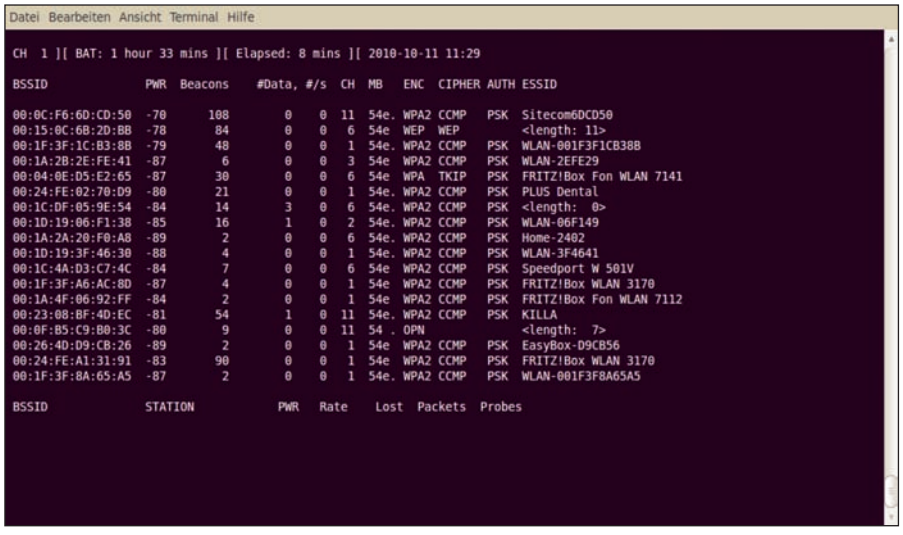


Bild 2: Airdump-ng speichert die Datenpakete der erreichbaren WLAN-Netze. Die Spalte "ENC" zeigt einem Angreifer, wie die Netze verschlüsselt sind: WEP ist schnell zu knacken, OPN steht für "Open", also komplett ohne Passwort.

Bild 3: Wenn es der WLAN-Router erlaubt, nur bestimmte MAC-Adressen zuzulassen, können Sie die WLAN-Nutzung auf diese Geräte einschränken

Angriffe auf WPA- und WPA2-Schlüssel kann Aircrack-ng ausführen; dazu nutzt es die Wörterbuchmethode.

Voraussetzung für das Dekodieren von WLAN-Passwörtern ist eine genügend große Zahl an Datenpaketen, die im WLAN kursieren. Diese werden mit dem Befehl

```
airodump-ng -w DATEI wlan0
```

in die Datei *DATEI* gespeichert. Das Kommando funktioniert allerdings nur, wenn sonst kein Dienst wie wpa-supplicant oder avahi-daemon auf die WLAN-Schnittstelle zugreift. Ob das das Fall ist, zeigt der Befehl *airmon-ng start wlan0*. Die angezeigten Prozesse sollten Sie vorher beenden.

Anschließend wird der Datenpakete-Dump durchgeführt. Danach suchen Sie mit dem Befehl *aircrack-ng DATEI.cap* das WLAN aus, dessen Passwort Sie entschlüsseln möchten. Wer zu viele WLANs im Umkreis hat, kann den airodump-ng-Befehl mit der Option "-d BSSID" auf die MAC-Adresse des eigenen WLANs einschränken und nur Datenpakete von dort sichten. Es muss allerdings schon einiges an Daten hin- und hergeschickt werden, damit aircrack-ng das Passwort entschlüsseln kann. Ist der WLAN-Router eine Fritzbox, kann der Parameter "-h" dienlich sein: Er sorgt dafür, dass der numerische Schlüssel der Fritzbox schneller gefunden wird. Mit "-K" verwenden Sie die KoreK- an Stelle der PTW-Methode. Um WPA-Passwörter mit einer Länge von acht bis 63 Zeichen zu knacken, benötigen Sie die Option "-w" sowie eine Wortliste. Links zu Wortlisten finden Sie in der Dokumentation auf der Aircrack-ng-Homepage.

Das WLAN absichern

Da das Ausspüren von WLANs mit Standardtools wie Kismet und Aircrack-ng äußerst simpel ist, sollten Sie die Sicherheit Ihres WLANs unbedingt an heutige Standards anpassen. Dazu gehört als Verschlüsselungsverfahren WPA oder WPA2, die beide als sicher gelten. Allerdings müssen Sie darauf achten, dass auch die Passwörter entsprechend sicher gewählt sind. Das heißt: Vermeiden Sie Wörter aus Wörterbüchern oder einer der Listen, die in den Aircrack-ng-FAQ genannt sind.

Lassen Sie die Finger von Clients, die selbst nur nach dem WEP-Standard verschlüsseln können. Der Router muss in dem Fall nämlich auf diese Verschlüsselungsmethode zurückgreifen. Das wiederum macht es einem Angreifer leicht, Passwörter auszuspionieren und Zugang zum WLAN zu bekommen.

Wenn der WLAN-Router erlaubt, den Zugang auf eine feste Anzahl von Geräten einzuschränken, kann das eine zusätzliche Sicherheitsmaßnahme sein. Dann werden nur Geräte mit tatsächlich vorhandenen MAC-Adressen im WLAN-Netz zugelassen, weitere lassen sich bei Bedarf per Hand nachtragen.

Ein weiterer Sicherheitsaspekt: Reduzieren Sie die Sendeleistung im WLAN, falls der Router Änderungen zulässt. Damit verringern Sie die Reichweite des WLANs im günstigsten Fall soweit, dass nicht über das Firmengebäude oder -gelände hinaus gefunkt wird. Allerdings sollten Sie auch in Betracht ziehen, dass Angreifer mit entsprechenden Antennen auch schwächer sendende WLAN-Netze empfangen.

Es bringt rein gar nichts, dem Funknetz keinen Namen zu geben. Der Effekt ist der, dass keine sogenannte ESSID übertragen wird. Das schert einen Angreifer aber nicht. Denn die BSSID mit der MAC-Adresse wird immer in die Gegend gefunkt – und für einen Angriff ist die sogar noch eindeutiger. Verwenden Sie stattdessen einen zufälligen Namen, den Sie zwar zuordnen können, nicht jedoch Angreifer von außen. *(jp)*

Sichere WLAN-Nutzung für Handelsreisende

Wer öffentliche und halböffentliche Hot Spots für die Verbindung ins Internet nutzt, sollte besonders achtsam sein. Das WLAN-Passwort erhält beispielsweise in einem Hotel jeder Gast an der Rezeption, der Angreifer genauso wie der harmlose Außendienstler. Deshalb sollten Sie gerade bei Firmennotebooks einige Dinge beachten: E-Mails sollten grundsätzlich verschlüsselt verschickt werden und die Notebook-eigene Firewall sollte so eingestellt sein, dass nur Standardports ausgehend (etwa 80 für den Internetzugang) offen sind. Sicherer wird eine Verbindung über ein virtuelles privates Netz oder auch, indem statt eines WLANs eine direkte UMTS-Verbindung zum Einsatz kommt.

Link-Codes

[1] Kismet
ABP61

[2] Aircrack-ng
ABP62

[3] Unsicherheit des WEP-Schlüssels
ABP63

[4] WEP-Schlüssel aus Datenpaketen entschlüsseln
ABP64

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

Quelle: Bernard Breton – Fotolia.com

Lösungsansätze gegen Netzwerkengpässe

Mittel gegen Paketstau

von Mathias Hein

Multimedia-Anwendungen benötigen einen unterbrechungsfreien, verlustarmen und verzögerungsarmen Transport der Datenströme. Diese Dienste stellen definierte Anforderungen, die in klassischen Datennetzen nicht ohne weiteres realisierbar sind. Daher ist die Übertragung von Informationen mit einer definierten Dienstgüte der zentrale Punkt bei der Entwicklung besserer Datennetze.

Jeder Mechanismus zur Sicherung der Dienstgüte bei VoIP muss sich an der Übertragungsqualität der Sprachnetze messen lassen. Jede Multimedia-Anwendung erwartet von einem Netzwerk bestimmte Eigenschaften. Erforderlich sind dabei Kenntnisse über diejenigen Parameter, die die Qualität einer Übertragung bestimmen. Die Verarbeitungsprozesse in aktiven Komponenten, wie Gateways, Switches und Router, sind die Quelle der meisten Beeinflussungen, daher müssen Quality of Service- (QoS) Mechanismen die spezifischen Parameter (effektive Bandbreite, Verzögerung, Paketverluste und Jitter) im Netzwerk garantieren.

Überdimensionierung ist nur die halbe Lösung

Die zu erwartenden Kosten der Netzwerkkomponenten haben sich in den vergangenen Jahren stark zum Vorteil der Nutzer nach unten entwickelt. Hier wirkt sich indirekt auch das aus der Computertechnik bekannte Mooresche Gesetz (Verdoppelung der Leistungsfähigkeit von Chips in 18 Monaten) vorteilhaft auf die Netzwerkkomponenten aus. Ethernet Netzwerke, die im Core-Bereich mit einem Mehrfachen von 10 GBit/s-Ethernet ausgerüstet sind, sind keine Seltenheit mehr. Der Preisverfall der Ethernet-Technik macht es möglich. Daher besteht heute in der Überdimensionierung des Netzes die einfachste Möglichkeit, für ausreichende Bandbreite zu sorgen. Die Übertragungsgeschwindigkeiten aller Medien (elektrische oder optische Leitungen, Funkstrecken) und die Verarbeitungsgeschwindigkeit der angrenzenden Netzknoten (Switches, Router) muss bei diesem Lösungsansatz stark überdimensioniert werden. Dies bietet den Vorteil, dass eine Verringerung der Wartezeiten in den Paket-Vermittlungsknoten erreicht wird. Grundlage einer Überdimensionierung der Netze ist die Homogenität der Netzkomponenten. Eine bewusste Beschränkung auf eine möglichst einheitliche Ausstattung der Netzwerkkomponenten ist ein wichtiger Schlüssel, um eine leistungsfähige und qualitätsgesicherte Prozessorganisation zu erreichen.

Bei Überdimensionierung sind in den Teilnetzen keine zusätzlichen administrativen Maßnahmen nötig. Dies gewährleistet eine unverändert einfache Wartung und Fehlersuche und vermeidet Abhängigkeiten von herstellerspezifischen Sonderlösungen. Diese Methode ist immer anwendbar und erfordert keine Veränderung der bisher verwendeten Funktionsprinzipien wie Übermittlungsprotokolle oder Algorithmen in den Vermittlungsknoten. In der Praxis erreichen Sie durch die Überdimensionierung des Netzes allerdings nur kurzfristig Ihr Ziel. Moderne Applikationen erfordern immer höhere Bandbreiten und neue Anwendungen – beispielsweise Videokonferenzen und andere Videodienste – fressen die verfügbaren Bandbreiten kontinuierlich auf. Schließlich schafft Verfügbarkeit auch neue Möglichkeiten.

Darüber hinaus sind selbst in einem lokalen Netzwerk die Zeitpunkte und Orte des Verkehrs nur schwer abschätzbar. Auch kommt es in Netzen, deren mittlere Bandbreitenausnutzung aller Links auf 50 Prozent dimensioniert ist, nach wie vor in gewissen Hochlastfällen zu Verstopfungen, die zu erhöhten Verzögerungen, Verzögerungsschwankungen und Paketverlusten führen. Bei diesem Lösungsansatz ist unbedingt ein kontinuierliches Monitoring der verfügbaren Bandbreite erforderlich. Auf Basis der entsprechenden Kennzahlen wird bestimmt, ob die Bandbreitenansprüche erfüllt werden oder ob Handlungsbedarf besteht. Darüber hinaus ist ein laufendes Monitoring der Bandbreite hilfreich, um schleichende Degeneration der verfügbaren Netzressourcen frühzeitig zu erfassen und aktiv entsprechende Maßnahmen einleiten zu können.

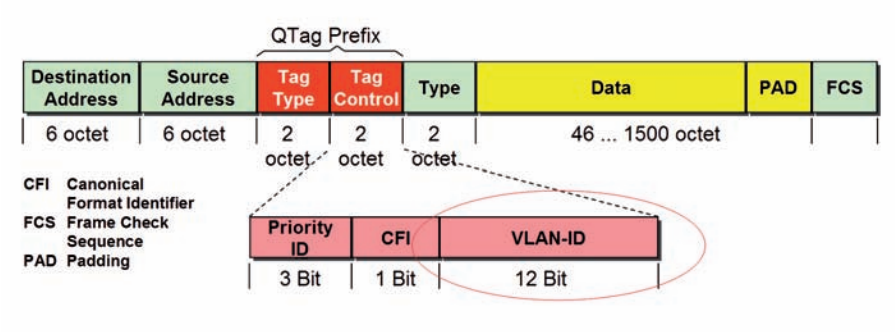


Bild 1: Ein Tagged-Frame mit Infos zur Priorisierung

Die richtige Menge Netzwerk

Beim "Rightsizing" wird im Falle vermeintlich knapper Ressourcen versucht, die Knappheit selbst zu beseitigen, anstatt eine Verwaltung der zu geringen Ressourcen mittels Priorisierung, Scheduling oder Bandbreiten-Reservierung zu realisieren. Die Trends bei den technischen Möglichkeiten sowie der Wirtschaftlichkeit von Netzwerkkomponenten begünstigen das Rightsizing. Es unterscheidet sich von Overprovisioning dadurch, dass versucht wird die Überlasten im Netzwerk auf extreme Fälle zu limitieren. In diesen Netzen wird eine gewisse Zusatzkapazität über den üblichen Datenverkehr (Datenspitzen) zur Verfügung gestellt. In der Praxis gleicht dieser Ansatz der bei der klassischen Telefonie verwendeten Erlang-Berechnung für die höchste Auslastung.

Beim Rightsizing geht es nicht ausschließlich um die Bandbreite. Die Vermeidung von Überlasten minimiert die Paketverluste und den Jitter. Grundlage des Rightsizings ist eine optimierte Netzarchitektur, welche die Anzahl der Hops auf ein Minimum reduziert und Engpässe vermeidet. Das Rightsizing wird hauptsächlich in kleineren und mittleren Unternehmensnetzen mit GBit-Ethernet genutzt. Einen ähnlichen Ansatz verfolgen viele Service Provider in ihren kommerziellen Backbones: Da die mittlere Auslastung dieser Backbones in der Regel bei zehn bis 15 Prozent liegt, werden Überlastungen in Spitzenzeiten umgangen. Werden jedoch Sprach- und Videoanwendungen im Netzwerk eingesetzt, konkurrieren diese Datenströme um die gleiche Bandbreite und führen schnell zu einer weiteren Überlastung in den Netzsegmenten.

Priorisierung im Netz

Der Begriff "Quality of Service" (QoS) beschreibt in der TCP/IP-Welt die Güte eines Kommunikationsdienstes aus der Sicht der Anwender. Dabei wird verglichen, wie stark die Güte des Dienstes mit dessen Anforderungen übereinstimmt. QoS bezeichnet allgemein die Dienstgüte von Übertragungskanälen. Durch Quality of Service werden aktiv bestimmte Parameter beeinflusst, die für das Management der Network Service Quality verantwortlich sind. QoS ist somit kein zusätzliches Feature, das sich an eine Netzinfrastruktur wie ein Add-on anflanschen lässt. QoS ist vielmehr das Resultat einer Vielzahl von aufeinander abgestimmten Maßnahmen, die im grundsätzlichen Design einer Netzinfrastruktur verankert sein müssen. Die QoS-bezogene Priorisierung wird durch die Sicherung der Dienstgüte gemäß IEEE 802.1p realisiert. Der Standard 802.1p beschreibt Methoden für die Bereitstellung der Dienstgüte auf der Schicht 2. IEEE 802.1p und IEEE 802.1Q definieren eine Erweiterung des MAC-Headers. Diese Erweiterung wird als Tag und die Frames mit dieser Erweiterung als Tagged-Frames bezeichnet. Die Unterscheidung der Pakete und der entsprechenden Zuordnung zu den Queues kann durch die Identifizierung der Prioritäten eines Paketes oder Frames erreicht werden. Der IEEE 802.1p-Standard empfiehlt die User-Priority und deren Umwandlung (Mappen) zu den Verkehrsklassen (Traffic-Classes) und damit zu den vorhandenen Queues.

Beim IP-Protokoll (Schicht 3) erfolgt die Datenübermittlung ungesichert und verbindungslos. Zusätzliche Funktionen wie beispielsweise Fehlererkennung, Überwachung der Reihenfolge, Flusskontrolle und Sicherung der Übertragung werden durch die Protokolle höherer Schichten realisiert. Zur Realisierung einer skalierbaren QoS-Lösung mit unterschiedlichen Dienstklassen wurden von der IETF die Differentiated Services (DiffServe, RFC 2474 und 2475) entwickelt. Die Eigenschaften von DiffServe sind:

- Die Zuweisung von Ressourcen ist gebunden an die durch DiffServe definierten Serviceklassen.
- Jedes Paket enthält innerhalb des IP-Headers Informationen über die benötigte Verkehrsklasse.
- Die Markierung der eingehenden Pakete erfolgt an der Netzgrenze durch die Edge-Router.
- Die Markierung eines Paketes entscheidet über die Weiterbehandlung und das Weiterleiten von Paketen innerhalb der Switche und Router. Daraus folgt, dass jeder Switch und jeder Router innerhalb der Domäne in der Lage sein muss, die Werte innerhalb des DSCP-Feldes zu interpretieren.

DiffServe verwendet dazu das IPv4 DiffServe (DS)-Feld. Dieses besteht aus einem sechs Bit langem Differentiated Service Codepoint (DSCP)-Feld für 64 mögliche QoS-Klassen. DiffServe benötigt keine Signalisierung und Zustandsspeicherung in den Netzelementen, da jedes einzelne Paket individuell nach seiner Dienstklasse von den Netzelementen behandelt wird. Stattdessen definiert DiffServe eine kleine Anzahl von Regeln für Qualitätsklassen (Per Hop Behaviours – PHBs), die von den Routern durch geeignete Maßnahmen unterstützt werden müssen.

Der Sender setzt über die Service-Primitives der Applikation das DS-Feld im IP-Header. Im Edge-Router erfolgt die Klassifizierung, indem bei jedem Paket das DS-Feld ausgewertet beziehungsweise durch ein vom Administrator vorgegebenes DSCP-Feld ersetzt wird. Dieser "Stempel" definiert die weitere Behandlung des IP-Pakets innerhalb der betreffenden DiffServe-Domäne. Die Core-Router sind nur für das Routing der DiffServe-Pakete anhand der sechs DSCP-Bits zuständig und schließen anhand des DSCP-Stempels auf die Behandlung des Pakets. Bei DiffServe beschränkt sich daher die Intelligenz auf den Edge, während Core-Router lediglich das DiffServe-Feld auswerten müssen. Außerdem darf der hochpriorisierte Verkehr nur einen Bruchteil des gesamten IP-Verkehrs ausmachen. Daher ist eine Zugangskontrolle (Admission Control) unumgänglich, die den priorisierten Verkehr limitiert.

Die Vorteile von DiffServe liegen in der guten Skalierbarkeit für große Netze und in der Interoperabilität mit MPLS. Darüber hinaus erlaubt der DiffServe-Ansatz lediglich eine relative Bevorzugung gegenüber anderen Dienstklassen und sobald der Verkehr einer Dienstklasse zu hoch ist, verhält sich DiffServe wie der normale Best Effort-Transport. Daher ist es wichtig, für hochpriorisierten Verkehr parallel dazu für genügend Bandbreite zu sorgen. Obwohl die Dienstklassen (PHBs) definiert sind, gibt es keine Festlegungen für die einzelnen Werte und jede Domain kann die PHBs unterschiedlich behandeln.

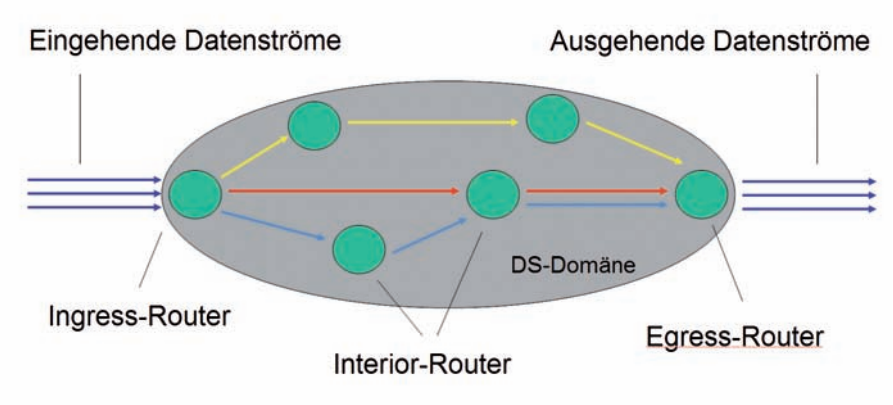


Bild 2: Ein DiffServe-Netzwerk, in dem die Pakete individuell behandelt werden

Die Prozessorganisation ist besonders im WAN-Umfeld (Ende-zu-Ende-Bereitstellung) der DiffServe-Definitionen besonders wichtig. Da mehrere Beteiligte mit diesem Prozess zu tun haben, ist eine formalisierte Ausgestaltung von Handlungsabläufen unabdingbar. Ohne eine Prozessorganisation muss ständig mit der Gefahr gerechnet werden, dass durch unangemessene oder falsche Maßnahmen die QoS einer Netzinfrastruktur empfindlich leidet.

Fazit

Die Bandbreitenmanagementverfahren sorgen für eine Verbesserung der Sprachqualität bei der Übermittlung von VoIP/Video-Strömen. Keine QoS-Lösung bietet das Allheilmittel für jedes Netzwerkproblem. Aus diesem Grund ist es wichtig, einige Schritte beim Design des Netzwerks zu beachten. Eine ausreichend dimensionierte Bandbreite im Netzwerk trägt zur Reduzierung der Verzögerungen bei und vermindert Paketverluste. Dennoch kann es in einigen Teilen des Netzes (speziell im WAN) aus Kostengründen oder aufgrund mangelnder Verfügbarkeit zu Bandbreitenengpässen kommen.

Die DiffServe-Mechanismen erweisen sich in der Praxis als kostengünstig, verwaltbar und reichen auch für den WAN-Einsatz völlig aus. Einer Sättigung beziehungsweise Überlast einer oder mehrerer Verbindungen im Übertragungsweg muss mit entsprechenden Queuing-Verfahren begegnet werden. Dadurch wird gewährleistet, dass die hochpriorisierten Verkehrsströme auch bei Überlastung der Transportressourcen übermittelt werden. Qualität schließlich lässt sich nur durch Qualitätssicherung erreichen. Dies beinhaltet die Kontrolle der geplanten Qualität mit geeigneten Messinstrumenten. *(dr)*

Stolperfallen bei der Umstellung auf IPv6 (2)

Neues Protokoll, neue Probleme

von Christian Rusch und Alexander von Gernler

Nach wie vor hat sich das neue Internet-Protokoll IPv6 noch nicht durchgesetzt. Nur zögerlich trauen sich Provider und Unternehmen an die Umstellung. Nicht ganz ohne Grund, denn neben den Vorteilen des größeren Adressraums und flexibleren IP-Adressen birgt IPv6 auch einige Stolperfallen. Im zweiten Teil unserer Workshopserie lesen Sie, wie sich Anwendungsprotokolle an IPv6 anpassen müssen und welche Tücken bei der Namensauflösung lauern.

Beginnen wollen wir den zweiten Teil unserer Workshopserie mit Anwendungsprotokollen und ihrer Kompatibilität zu IPv6. Praktisch alle Protokolle, die beim Datenaustausch über IP-Adressen kommunizieren, nutzen feste Felder, in die die betreffenden IP-Adressen hineingeschrieben werden. Diese Art der Adressierung wird als in-band bezeichnet. Als diese Protokolle entworfen wurden, war IPv6 noch kein Thema, daher wurde meist auch nicht über die 32 Bit breiten IPv4-Adressen hinaus gedacht. Es ist jetzt aber unmöglich, die 128 Bit breiten IPv6-Adressen dort unterzubringen, was eine v6-Fähigkeit dieser Protokolle ohne spezielle Änderungen von vornherein verhindert. In solchen Fällen muss dann entweder auf ein anderes Protokoll ausgewichen, das bestehende Protokoll erweitert oder eine neue, IPv6-fähige Version des Protokolls spezifiziert werden. Bei den meisten Protokollen ist dies bereits passiert, teilweise hinkt aber noch deren Implementierung auf verschiedenen Plattformen hinterher. Betroffen hiervon waren unter anderem:

- SMB: Das Server Message Protocol
- BGP, RIP, OSPF: Von Internet-Providern verwendete Routing-Protokolle
- RPC: Der unter anderem vom Dateisystem NFS verwendete Remote Procedure Call

Hier wurden jeweils neuere Versionen des Protokolls spezifiziert, und es existieren schon auf vielen Plattformen Implementierungen der Protokolle. Andere Protokolle konnten hingegen mit neuen Befehlen oder geeigneten Protokollerweiterungen an IPv6 angepasst werden. Hierzu zählen:

- File Transfer Protocol (FTP)
- Session Initiation Protocol für Internet-Telefonie (SIP)
- Domain Name System (DNS)

Es gibt jedoch auch eine Entwarnung für die meisten anderen Protokolle: Viele sind nur dafür gedacht, reine Datenströme zu transportieren, wofür sie nicht im Protokoll selbst nochmals über die ohnehin schon erfolgte Adressierung kommunizieren müssen. Andere Protokolle reden zwar über Adressen, verwenden dafür aber keine Felder mit fester, auf 32 Bit beschränkter Länge. Derartige Protokolle sind sozusagen out-of-the-box IPv6-fähig. Dazu zählen beispielsweise HTTP, SMTP, NTP und SSH.

Probleme mit der String-Repräsentation

Daneben stellt die Anwendungsebene noch eine Schwierigkeit dar: Überall, wo Netzwerkadressen von ihrer 32 oder 128 Bit-Darstellung in ein menschenlesbares Format konvertiert werden, muss von der maschineninternen Darstellung in eine sogenannte String-Repräsentation der Adresse umgerechnet werden. Kommt zu der Adresse noch die Spezifikation eines TCP- oder UDP-Ports hinzu, wird es endgültig kompliziert. Es werden übrigens nicht nur reine Adressen selbst in Konfigurationsdateien oder Eingabemasken verwaltet, sondern auch komplexere Konstrukte wie Netzwerk-ACLs etwa für Programme wie den Squid WWW-Cache.

Traditionell wird eine IPv4-Adresse in ihrer String-Repräsentation als eine Gruppe von vier Dezimalzahlen notiert, die jeweils Werte von 0 bis 255 einnehmen können und voneinander durch Punkte getrennt sind. Eventuelle Port-Angaben werden bei IPv4 mittels eines Doppelpunktes an die IP-Adresse angehängt, also etwa 192.168.200.1:80 für den HTTP-Port eines Rechners mit der IP-Adresse 192.168.200.1. IPv6-Adressen dagegen werden in Hex-Darstellung notiert, wobei jeweils nach zwei Byte mit einem Doppelpunkt abgetrennt wird. Soll hier noch ein Port angegeben werden, entsteht die Situation, dass der Doppelpunkt nun mit zwei verschiedenen Bedeutungen verwendet wird. Um diese Klippe zu umschiffen, besagt RFC 3986, dass eine IPv6-Adresse in eckigen Klammern angegeben werden kann und der Port außerhalb der Klammern angehängt wird, so dass die Trennung nun wieder eindeutig ist, also [2001:db8:dead:beef::1]:80. Doch ist diese Darstellung nicht in allen Software-Lösungen einheitlich, da das RFC eher spät aufkam und bereits vorher Entwickler ihre eigene Darstellung entworfen und in ihrer Software umgesetzt haben.

Die Mischung beider Formate bei einem IPv4- und IPv6-fähigen Dienst ist nicht nur für die Benutzer verwirrend, sondern auch für die Software-Entwickler. Bedenken Sie die Vielzahl an Eingabefeldern für IP-Adressen, ACLs und Ähnliches in der unglaublichen Menge an freier und kommerzieller Software, so fällt es schwer zu glauben, dass alle diese Eingabebehandlungen auf Anhieb korrekt programmiert wurden. Darüber hinaus kennt IPv6 scoped link-local Adressen, bei denen auch noch der Name des Interfaces (von System zu System verschieden) angegeben werden kann. Diese sehen dann etwa so aus: fe80::216:d3ff:fe21:97e0%pppoe0. Ein Validator bei der Eingabe müsste auch noch die angehängten Namen der Schnittstellen auf Gültigkeit prüfen. Bis auch hier eine Konsolidierung durch das Alter der Software und eine entsprechend große Benutzerbasis eintritt, wird auch in diesem Fall noch mit einigen Überraschungen zu rechnen sein. Im besten Fall handelt es sich dann um nicht funktionierende Features einer Software - und im schlimmsten Fall um den nächsten Exploit.

Neue Konzepte des Netz-Designs

IPv6 bringt eine Menge neuer Konzepte mit, die von den Benutzern erst nach und nach verstanden und erlernt werden müssen. So gibt es nicht nur private und öffentliche IP-Adressen wie unter IPv4, sondern mehrere, teils feiner abgestufte, teils nie dagewesene andere Klassen von IPs wie zum Beispiel Global, Link-Local, Unique-Local, Anycast und Multicast. Grundsätzlich sind sowohl die öffentlichen IPv4-Adressen mit den Global Unicast IPv6-Adressen als auch die nach RFC 1918 als privat deklarierten IPv4-Bereiche mit den Local-Adressklassen von IPv6 vergleichbar. Doch bedeutet das noch lange nicht, dass sich daraus die selbe Netztopologie wie vorher ergibt, also etwa private IP-Adressen im internen Netz, NAT und Proxys zur Umsetzung nach außen und in öffentliche Adressen im Internet. Ein Rechner in der IPv6-Welt bekommt je nach seiner Rolle verschiedene IPv6-Adressen gleichzeitig zugewiesen. Es können zudem pro Netzsegment mehrere gültige Router existieren, die alle jeweils eine Anbindung nach draußen anbieten. Je nach Ziel wird sich der IPv6-Host dann den günstigsten Router mit der größten Übereinstimmung mit dem Präfix des Ziels aussuchen. In der IPv4-Welt gibt es in kleineren Netzen meist lediglich den einen Default-Router. Doch es ist weder üblich, einer Workstation mehr als eine IPv4-Adresse gleichzeitig zuzuweisen, noch mehrere Router in einem Subnetz gleichzeitig im Einsatz zu haben, ohne auf den Clients noch ein dynamisches Routing zu verwenden.

Durch diese wenigen Beispiele sollte klar werden, dass IPv6 aufgrund seiner höheren Komplexität viel mehr Möglichkeiten zur Gestaltung von Netzen bietet. Unglücklicherweise geht dieser Vorzug einher mit den neuen Möglichkeiten, sich mit falschen Entwürfen ordentlich ins Bein zu schießen. IPv6 verlangt eine neue Denkweise, und nichts wird einen davor bewahren, sich irgendwann einmal darauf einlassen zu müssen.

Tücken neuer Features: DAD

Die Socket-API, die praktisch alle Programmierer von Netzwerkdiensten benutzen, sieht sich durch IPv6 mit neuen Fehlerfällen konfrontiert, auf die existierende Software meist nicht vorbereitet ist. Ein Beispiel: IPv6 bringt bereits einen eingebauten Mechanismus namens Duplicate Address Detection (DAD) mit, der die noch von IPv4 bekannten Adresskollisionen vermeiden soll.

Hierbei wird vor dem Aktivieren einer IPv6-Adresse auf einem Netzwerkinterface zunächst auf dem lokalen Netzwerksegment geprüft, ob die Netzwerkadresse nicht schon verwendet wird. Ist dies der Fall, wird die neue Adresse nicht aktiv geschaltet und sie taucht nicht doppelt im Netzwerksegment auf. Allerdings benötigt die Überprüfung selbst eine wenn auch minimale Zeit. Nun kann der Fehler in der Software-Entwicklung auftauchen, dass ein Rechner so schnell bootet, dass die Duplicate Address Detection noch nicht abgeschlossen ist, aber schon der erste Netzwerkdienst hochfährt. Dies ist meist kein großes Problem, denn fast alle Netzwerkdienste binden sich auf "*", lauschen also auf allen momentan aktiven Netzwerkadressen des Systems, ohne diese näher zu spezifizieren. Will sich jedoch ein Dienst auf eine einzelne IPv6-Adresse binden, so schlägt dies fehl, weil die Duplicate Address Detection noch nicht abgeschlossen ist. Ein solcher Effekt wäre unter IPv4 nicht möglich gewesen, da im IPv4-Fall jede Adresse an einem Interface sofort aktiv wird, sobald sie gesetzt ist. Dafür ist hier auch das unfreiwillige Erzeugen von Adress-Duplikaten einfacher. Dass eine Adresse auf einer Schnittstelle konfiguriert ist, heißt bei IPv6 noch nicht, dass sie auch benutzt werden kann. Es gibt im Gegensatz zu IPv4 eine Anzahl von Zuständen, in denen normalerweise problemlose Funktionen wie bind() fehlschlagen. Situationen wie diese können jetzt unter IPv6 auftreten und müssen beim Entwickeln von Software berücksichtigt werden.

IPv6 und DNS

DNS ist für den Übergang von IPv4 zu IPv6 praktisch und unerlässlich. Jedoch steckt der Teufel im Detail der verschiedenen Implementierungen von Resolvern – also den Mechanismen, die sich in Betriebssystem- oder Basisbibliotheken um die zentral wichtige Namensauflösung kümmern – sowie von Nameservern und Software, die Resolver oder Nameserver benutzen. So wird deutlich, dass eine Benutzung von IPv6 ohne die Abstraktion durch Domain-Namen praktisch nicht möglich wäre: Keinem Menschen ist zuzumuten, sehr lange und mit Doppelpunkten getrennte Hex-Kombinationen wie etwa 2001:db8:8fda:12c3:b45:789:11a:2 einzugeben, wenn er sich mit einem Rechner verbinden möchte. Schon unter IPv4 fällt es oft schwer, sich die nur 32 Bit

langen Zahlen zu merken. Doch sind die Resolver je nach Betriebssystem leicht unterschiedlich implementiert und verhalten sich deshalb auch unterschiedlich. Manche liefern beispielsweise immer zuerst den AAAA-Record, also eine IPv6-Adresse des angefragten Ziels, zurück, auch wenn mehrere IPv4- und IPv6-Adressen existieren. Andere entscheiden zufällig, welche der vielen Adressen sie zuerst liefern, und wieder andere Resolver liefern immer eine IPv4-Adresse zurück. Der konkrete Ablauf einer Namensanfrage ist im Bild unten dargestellt: Zuerst stellt eine Anwendung eine Namensanfrage, indem sie einen entsprechenden Aufruf der zuständigen Bibliotheksroutine (hier in der sogenannten Libc) absetzt (1). Die Systembibliothek setzt dies in eine Folge von Aufrufen an den Kernel um (2), die das Verschicken eines Netzwerkpaketes nach sich ziehen (3). Trifft die Antwort ein (4), so kann sie von der Bibliothek mittels eines Systemaufrufes abgeholt (5) und an die Anwendung weitergegeben (6) werden.

Tunnelnetze machen Probleme

Die Dual-Stack-Implementierung von IPv6 neben IPv4 ist zwar extrem günstig für die sanfte Migration zum neuen Protokoll, kann aber auch Grund für Komplikationen sein. Betrachten wir zum Beispiel den Fall eines Nutzers, der sich aus der misslichen Lage befreien möchte, dass sein Provider nur IPv4 per DSL anbietet. Dieser Benutzer registriert sich bei einem freien Tunnelprovider wie etwa Hexago oder sixxs.net für IPv6 und lässt sich ein IPv6-Netz nach Hause tunneln. Das Setup dürfte gut funktionieren, solange der Tunnel steht und echte IPv6-Connectivity zu Hosts besteht, die per IPv6 erreichbar sind. Allerdings geht der Traffic für IPv4 jetzt einen ganz anderen Weg ins Internet als der für IPv6. Dadurch können merkwürdige Effekte auftreten, je nachdem, welche Adresse gerade für einen entfernten Server benutzt wird, der sowohl per IPv4 als auch per IPv6 erreichbar ist.

Noch interessanter wird es, wenn der Tunnel kurz wegbricht oder nur eingeschränkt funktioniert, so dass zwar noch Pakete durch den Tunnel geschickt werden, diese aber auf der anderen Seite verworfen werden. In diesem Fall wird das Betriebssystem auch weiterhin versuchen, entfernte Server per IPv6 zu erreichen, mit dem Resultat, dass keine Verbindung dorthin aufgebaut werden kann, obwohl per IPv4 noch weiter problemlos Konnektivität besteht. Darüber hinaus stellen Tunnelnetze konkrete Sicherheitsprobleme dar: Bisher konnte sich ein Anwender hinter seiner DSL-Box in Sicherheit wiegen, war doch seine interne Netzinfrastruktur für das Internet dank Network Address Translation (NAT) nicht sichtbar. Plötzlich aber ist durch die IPv6-Konnektivität das gesamte Heimnetz schutzlos im Internet sichtbar und jeder Rechner, ob mit aktueller Software, Firewall und Virenscanner versehen oder nicht, weltweit erreichbar. Zwar ist dieses Problem bei einem herkömmlichen IPv4-VPN ähnlich, für die volle Ausbeutbarkeit der Situation mussten aber weltweit gültige (also nicht-private) IPv4-Adressen geroutet werden. Diese stehen bei IPv6 in enormem Umfang für jeden zur Verfügung, so dass die Gefahr an dieser Stelle realer ist als noch mit IPv4-VPNs.

Ein politisches Problem haben Tunnelnetze auch noch: Ihre zunehmende Verbreitung nimmt den Druck von den Providern, endlich native IPv6-Connectivity bereitzustellen. Immerhin können diese bei weiteren Nachfragen bequem darauf verweisen, dass diejenigen Personen, die IPv6 wollen, es sich ja längst auch ohne ihre Mithilfe besorgen können. Auch hier existieren allerdings Gegenmeinungen, die behaupten, die zunehmende Existenz von Tunnels beweise den echten Bedarf an IPv6-Adressen und baue eher Druck auf die Provider auf. Tunnel machen auch die Fehlersuche extrem schwierig und sollten daher in Zukunft vermieden und durch echtes Peering ersetzt werden.

Lesen Sie im dritten Teil unserer Serie, welche Sicherheitslücken und Fehler in praktisch jeder IPv6-Software lauern. *(dr)*

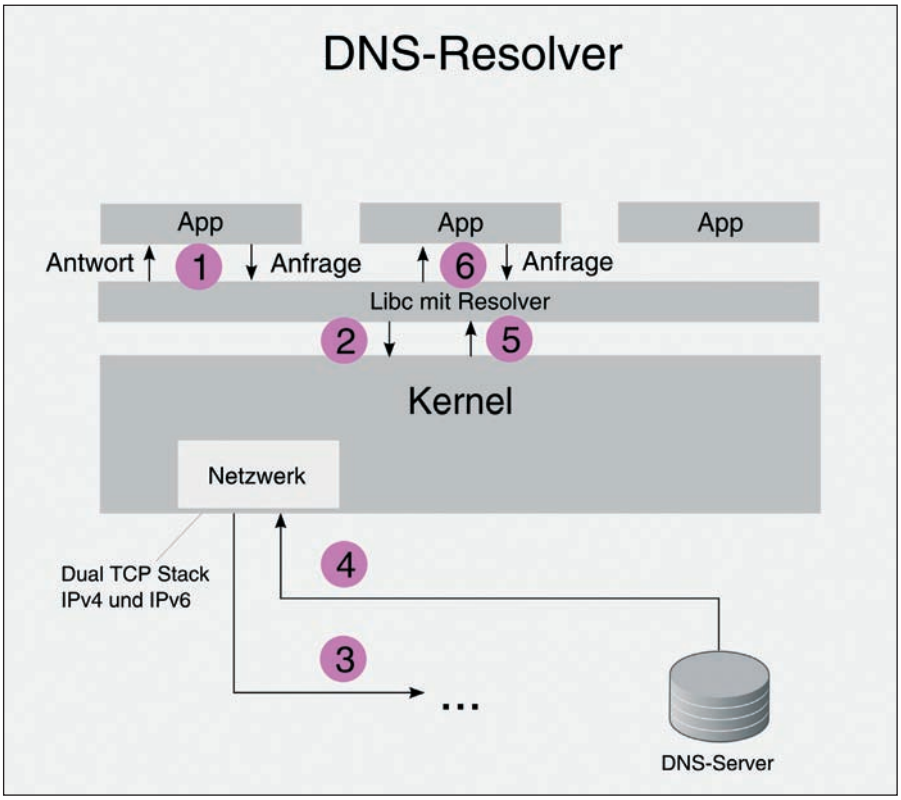


Bild 1: Der typische Ablauf von Namensauflösungen mit dem DNS-Resolver

Drucken im Netzwerk (3)

Druckerhelfer

von Thomas Bär

Der dritte und abschließende Teil der Serie rund um das Thema Drucken im Netzwerk widmet sich Programmen, die es Ihnen einfacher machen sollen, Ihre Drucker zu verwalten und anzusteuern. Die Bordmittel der Betriebssysteme bieten eine insgesamt solide und robuste Grundlage für das Ausdrucken von Dokumenten. In komplexeren Umgebungen jedoch wird die Verwaltung mit diesen Standardmitteln mitunter so schwierig, dass Zusatzlösungen ein wahrer Segen sein können. Wir stellen vier dieser praktischen Werkzeuge vor und erklären Ihnen die wichtigsten Handgriffe.

Oft sind es in erster Linie die beiden Bereiche Druckerzuordnung und Treiberbereitstellung, die das Drucken insbesondere in Terminalserver-Umgebungen so schwierig machen. Sofern genügend Know-how im Unternehmen verfügbar ist und es nicht an der Zeit mangelt, eigene Konzepte mit Skripten abzubilden, so ist über das Anmeldeskript eine genaue Druckerzuordnung möglich. Komfortabel sind diese selbstgestrickten Programme leider in den seltensten Fällen. Anstelle viel Zeit mit der Erstellung eigener Skripte zu verbringen, ist möglicherweise eine der hier vorgestellten Speziallösungen die bessere Wahl. Microsoft Windows bietet in Terminalserver-Umgebungen eine automatisch aktivierte Druckstromkompression. Die Programme von Drittherstellern gehen über diese Basisfunktionen hinaus und erlauben sogar eine verlustbehaftete Reduktion von grafischen Inhalten.

Drucker-Steuerung ohne Anmeldeskript

Das zu Quest Software gehörende Unternehmen ScriptLogic bietet eine Vielzahl verschiedener Produkte für das Management von professionellen IT-Umgebungen an. In erster Linie ist "Desktop Authority" [1] ein Programm zur gezielten Bereitstellung von Desktop-Umgebungen. Es regelt zum Beispiel, welche Programme auf dem Desktop angezeigt werden und welche Befehle ein Anwender ausführen darf und welche nicht. Auch das Ausbringen von MSI-Paketen möglichst ohne manuelles Zutun auf einer größeren Zahl von Computern nach verschiedenen Regelwerken gehört zu den Kernbereichen des Werkzeugs.

In Bezug auf die Bereitstellung von Druckern bietet sich eine Funktion aus dem Umfang von Desktop Authority besonders an: Die typischen Login-Skripte der Windows-Umgebung werden durch die Software ersetzt. Für die Durchführung von Konfigurationsanpassungen steht Ihnen eine grafische Oberfläche zur Verfügung, in der Sie die Regelwerke lediglich zusammenklicken müssen. Mit den bekannten booleschen Logik-Parametern wie "OR", "NOR" oder "AND" und einer Vielzahl weiterer Werte aus Windows ist eine sehr feine Steuerung der Druckzuordnung möglich.

Zur Auswahl stehen beispielsweise Gruppenzugehörigkeit, OUs aus dem Active Directory, IP-Adressen, Benutzernamen oder Client-Namen. Die auf dem Server festgelegten Regeln werden im Anmeldeskript von der Software dynamisch ausgewertet und auf die aktuelle Anmeldesituation angewendet. Desktop Authority ermöglicht zudem eine sehr einfache Unterscheidung zwischen den unterschiedlichen Client-Betriebssystemen und der Festlegung von Einstellungen in Terminalserver-Umgebungen. Auf welche Betriebssysteme oder Endgeräte eine Konfigurationseinstellung angewendet werden soll oder nicht, wählen Sie durch Checkboxen aus. Steht beispielsweise ein älterer DIN A3-Farblaserdrucker nicht für Windows Vista oder Windows 7-Computer zur Verfügung, da es keinen geeigneten Treiber gibt, so entfernen Sie einfach diese beiden Betriebssysteme aus der Zuordnung.

Neben den Druckereinstellungen erlaubt das Ersetzen des Anmeldeskripts mit Desktop Authority die Zuordnung von Laufwerken, die gezielte Anpassung der Registry, das Erstellen von Verknüpfungen, Browser-Anpassungen oder die Modifikation von Einstellungen für Microsoft Office oder Outlook. Das gezielte Setzen von Optionen für Outlook oder die au-

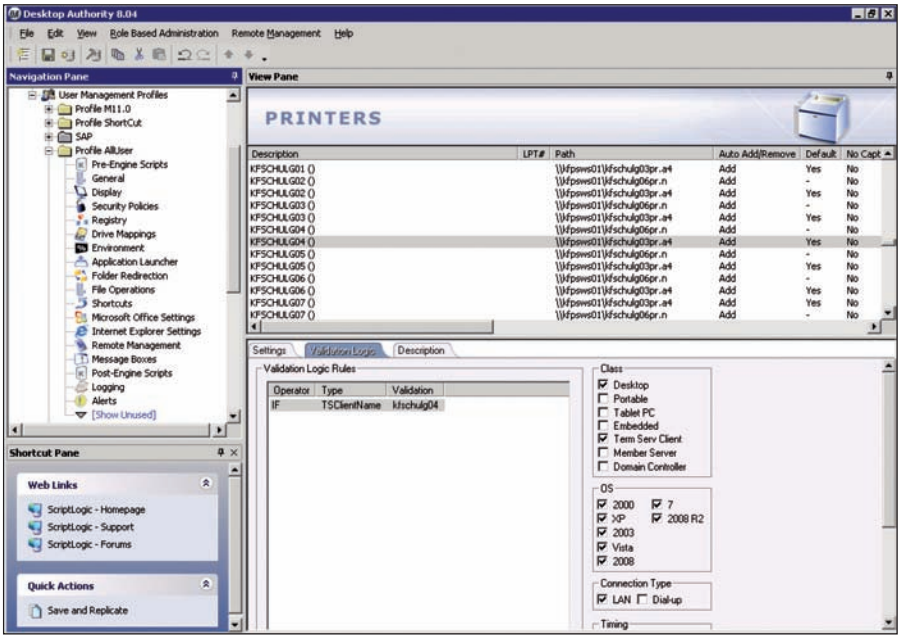


Bild 1: ScriptLogics Desktop Authority erlaubt die Zuweisung von Druckern über verschiedene Parameter. Die Oberfläche von Desktop Authority lässt sich deutlich einfacher bedienen, als eine große Zahl an Anmeldeskripten anzupassen.

tomatisierte Bereitstellung von Signaturen setzt bei Desktop Authority keine genaueren Kenntnisse der Registry von Windows voraus. Die Einstellungen sind mit für sich selbst sprechenden Texten versehen, was die Bearbeitung einfach macht.

Drucken für Terminal Server

Während Desktop Authority in erster Linie das Management rund um den Desktop und die damit verbundenen Konfigurationseinstellungen vereinfacht, ist die ThinPrint AG ein Spezialist für das Drucken in verteilten Netzwerkumgebungen. Das Hauptprodukt des aus Deutschland stammenden Softwarehauses ist die Drucklösung ThinPrint .print [2]. Neben der Vereinfachung der Druckertreiberbereitstellung über die sogenannte Driver Free Printing-Technologie bietet das System eine Druckdatenkomprimierung, verbindungsorientierte Bandbreitenkontrolle, SSL-Verschlüsselung der Druckdaten und ein Tracking Service zur Analyse der Druckkosten. Die ThinPrint Client-Komponenten sind nicht nur unter Microsoft Windows nutzbar. Eine große Zahl von Herstellern hat die Software in Thin Clients, Terminals, Printerboxen und Netzwerkdrucker integriert.

Eines der wichtigsten Argumente für den Einsatz von Lösungen wie .print ist die Druckdatenkomprimierung, die je nach Datentyp mit verschiedenen Kompressions-Algorithmen eine verlustfreie Reduktion ermöglicht. Die maximale Komprimierungsrate liegt, in Abhängigkeit von den Druckdaten, bei PCL- und PostScript-Druckertreibern bei bis zu 95 Prozent. Neben der verlustfreien Kompression bietet die Software die Möglichkeit, vor dem eigentlichen Druckauftrag auf dem Bildinhalt auch verlustbehaftete JPEG-Komprimierungen durchzuführen.

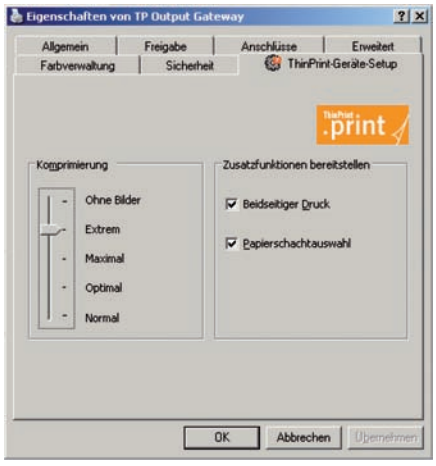


Bild 2: ThinPrint stellt Programme her, die unter anderem die Größe des Druckstroms reduzieren

Soll ein Ausdruck einfach nur zügig bearbeitet werden, lässt sich der Bildinhalt mit einem Klick komplett aus dem Druckdokument entfernen. Beide Verfahren zusammen können einen deutlichen Geschwindigkeitszuwachs beim Ausdruck bewirken – vor allem dann, wenn zwischen den Kommunikationspartnern eine leistungsschwache Netzwerkverbindung besteht – je nach Konfiguration und Kompressionsgrad aber zur Lasten der Ausdrucksqualität. Die verbindungsorientierte Bandbreitenkontrolle des Tools lässt sich einsetzen, um nur eine gewisse Bandbreite für die Übertragung von Druckdaten freizugeben und so ausreichende Kapazitäten für andere Anwendungen vorzuhalten.

Mit einem einheitlichen Drucktreiber, der als "Driver Free Printing Technology" patentierten Methode, will ThinPrint auch dem Administrator das Leben einfacher machen, da für unterschiedliche Druckertypen nur eine einzige Treibersoftware zum Einsatz kommt. Spezielle Fähigkeiten der einzelnen Drucker, wie Farbdruck, Ansteuerung unterschiedlicher Papierfächer oder der Duplex-Druck, bietet der Output Gateway-Treiber ebenfalls an. Auf Wunsch können Sie vor dem eigentlichen Ausdruck eine Druckvorschau aktivieren, so dass der Nutzer auf dem Client noch letzte Einstellungen vornehmen kann, die durch den Einheitstreiber nicht abgedeckt werden.

Je nach Einsatz-Szenario bieten sich mit ThinPrint verschiedene Möglichkeiten, um den Druckvorgang zu optimieren. Findet sich an einem Standort beispielsweise lediglich ein Printserver mit verschiedenen Druckern, so empfiehlt sich der Einsatz der .print Desktop Engine auf den verschiedenen Windows-Clients. Der Druck auf dem Printserver erfolgt so mit Bandbreitenanpassung und Kompression. Ist für einen Printserver keine ThinPrint-Client-Software verfügbar, beispielsweise bei einfacheren Printerboxen, so können Sie dieses Gerät per LPD ansprechen. Bei der LPD-Variante geht zwar die Kompression

verloren, die Bandbreitensteuerung für die Druckaufträge bleibt aber erhalten.

In einer Terminalserver-Umgebung mit Microsoft Windows mit und ohne Citrix-Erweiterung wird auf dem Terminal-Server eine entsprechende Server-Komponente installiert, die den Druckstrom dann komprimiert aus der Terminal-Sitzung heraus an den lokalen Rechner schickt, auf dem ein .print-Client installiert ist. Besonders hier ist die Bandbreiteneinstellung von Bedeutung, wenn die Terminalsitzungen über schwächere WAN-Verbindungen aufgebaut werden. Die Installation von unterschiedlichsten Druckertreibern entfällt durch das treiberlose System auch hier komplett. Alle Benutzer erhalten in den Druckerdialogen die gleichen Optionen. Kommen Heimarbeitsplätze mit den verschiedensten Consumer-Druckern mit ins Spiel, so ist diese Funktionalität besonders elegant.

Die Zuweisung von Druckern (Mapping), entweder eine Baustelle für das Scripten oder ein in der Praxis leicht zum Wildwuchs werdendes Thema, lässt sich mit einer Funktion namens .print AutoConnect vereinfachen. Mit Hilfe von Joker-Zeichen weisen Sie Templates für Druckobjekte zu, ohne dass dabei Druckertreiber automatisch geladen werden müssen. Verschiedenste Drucker lassen sich mit Druckerklassen zu Druckergruppen oder -standorten zusammenfassen. Durch die Zuweisung von Bandbreiten können Sie im Zusammenspiel mit der allgemeinen Priorität von Druckaufträgen dafür sorgen, dass einzelne Clients besonders schnell in den Genuss eines Druckauftrags kommen, während andere Plätze eher langsamer abgearbeitet werden.

Schneller drucken

Die aus den USA stammenden Produkte triCerat ScrewDrivers 4 und Simplify Suite [3] haben sich ebenfalls der Optimierung der Druckerzuordnung, der Reduktion des Datenvolumens im Druckdatenstrom und der Einführung eines einheitlichen Druckertreibers verschrieben. Während ScrewDrivers über das Terminalserverprotokoll arbeitet und als reinrassige Lösung auf beiden Seiten ein Windows-Betriebssystem erfordert, unterstützt die in der Simplify Suite eingebettete Drucklösung Simplify Printing jedwede Client-Technologie. Der Transport der Druckdaten erfolgt dabei vom Terminalserver zu einem Windows-Druckserver und – anders als bei ScrewDrivers – nicht über das Terminalserverprotokoll, sondern über eine dedizierte TCP/IP-Verbindung. Ähnlich wie ThinPrint hebt auch dieser Hersteller die Notwendigkeit zur Installation von herstellerspezifischen Druckertreibern auf den Terminalservern auf.

triCerat ScrewDrivers unterstützt alle Arten von Druckern, egal ob sich um USB- oder Netzwerkdrucker handelt. Multifunktionsdrucker können Sie mit den spezifischen Einstellungen wie Farbdruck, Auflösungen und Fähigkeiten ebenfalls ansteuern. Diese weitreichende Unterstützung erreicht das Tool durch das Ansprechen der Originaltreiber, die auf dem Client-Computer installiert sind. Die Funktionen werden in den Druckereinstellungsdialogen des Werkzeugs dann adaptiert dargestellt. So ist ein Ausdruck auf jedem verfügbaren Client-Drucker auch aus einer Terminalsitzung möglich, ohne dass Sie als Administrator die Umgebung dafür vorbereiten müssen. Die vom Benutzer gewohnten lokalen Druckernamen werden in der Sitzung angezeigt, was die Verwechselungsgefahr reduziert.

Neben der Vereinfachung der Druckerbereitstellung in Terminalserverumgebungen bietet die Software eine Verbesserung der Druckgeschwindigkeit und erlaubt eine Reduktion der Bandbreite für den Druckauftrag durch Kompression und Streaming. Die Entwickler des Anbieters haben dafür ein eigenes Kommunikationsprotokoll geschrieben, das dem bekannten Microsoft Windows EMF-Format (Enhanced Metafile Format) in einigen Funktionen überlegen ist. EMF, ursprünglich Mitte der 1990er Jah-

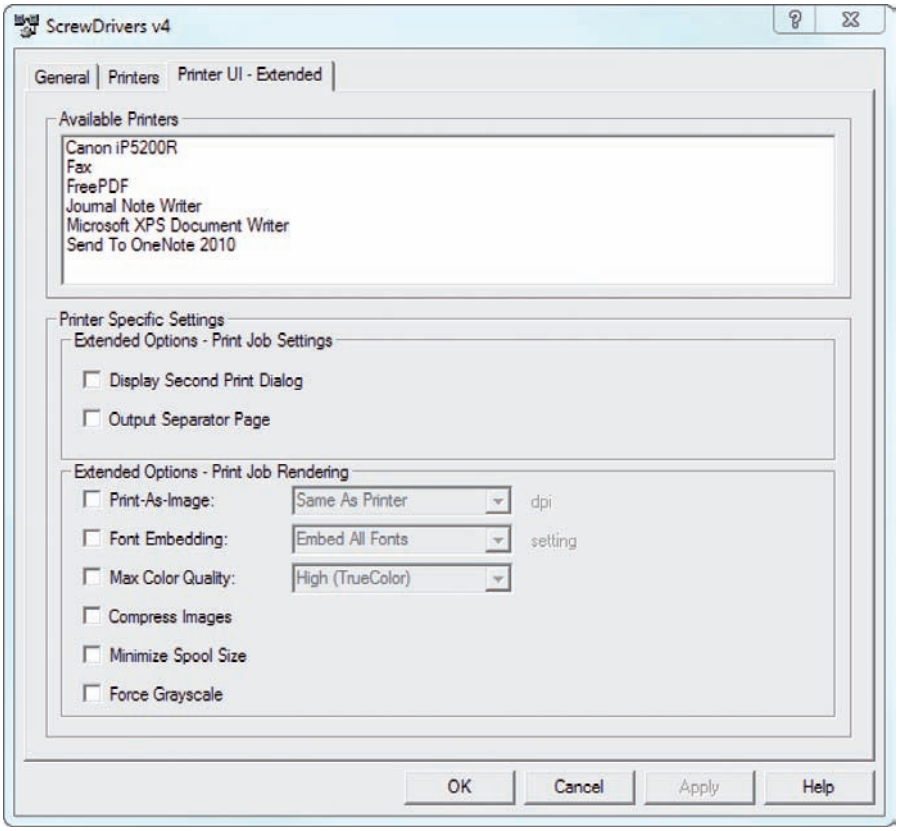


Bild 3: ScrewDrivers von triCerat bietet verschiedene Möglichkeiten, Einfluss auf den Ausdruck und dessen Qualität zu nehmen

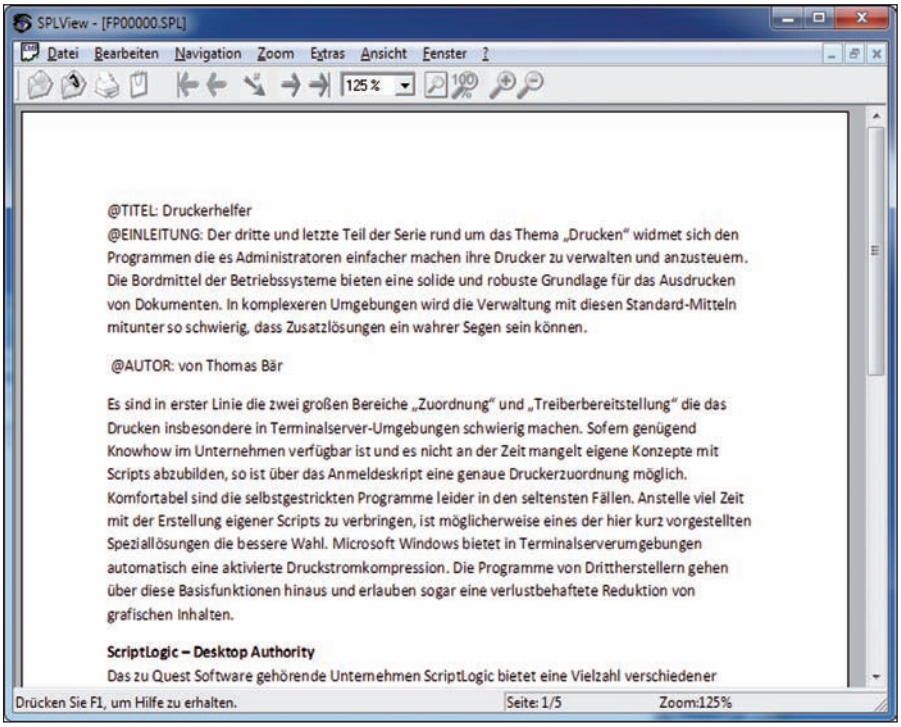


Bild 4: Die Freeware SPLViewer ermöglicht es, Dokumente in der Druckerwarteschlange direkt zu betrachten

re zur Anzeige und zum Ausdruck von Informationen entwickelt worden, ist in erster Linie eine Spooler-Datei im GDI-Umfeld. Jede neue Windowsversion verfügt über eine im Detail verbesserte und aktualisierte Version von EMF. Infolgedessen kann es zwischen den verschiedenen Windowsversionen zu geringen Unterschieden beim Ausdruck kommen.

triCerat nennt die eigene Entwicklung, die anstelle von EMF zum Einsatz kommt, das "triCerat Metafile Format" (TMF). TMF wurde speziell für das Drucken im Terminalserverumfeld entwickelt und berücksichtigt die Kompression der Druckdaten bereits auf dieser Protokollebene. Schriftarten, die am Client-Computer nicht verfügbar sind, bettet die Software bei Bedarf automatisch in den Druckjob ein. Druckaufträge lassen sich in den Formaten PDF, TMF oder BMP auf den Server oder den Client-Computer exportieren. Trotz des Funktionsumfangs ist die Client-Software nicht einmal 2 MByte groß.

Der Wegfall der individuellen Treiberinstallation im Terminalserverumfeld ist besonders mit Blick auf die jüngsten Entwicklungen im Bereich Virtual Desktop Infrastructure (VDI) bedeutsam. Virtuelle Desktops und deren Applikationen, die möglicherweise auf verschiedensten Servern in der Cloud gehostet werden, müssen nach wie vor Ausdrucke produzieren können. Der Benutzer erwartet zu Recht, dass sich der am Zugriffsgerät angeschlossene Drucker aus der Sitzung ansprechen lässt. In VDI-Konzepten unterstützt triCerat als Host/Server-Komponente die Betriebssysteme Windows 2000, XP, Vista und 7 – außer bei Windows 2000 sowohl die x86- als auch die x64-Variante.

Feinsteuerung des Drucks

Im Vergleich zu den bereits vorgestellten Produkten stellt sich PrintMulti [4] etwas anders dar. Das Tool ist ein eigenständiger Print-Prozessor, der es ermöglicht, einen Druckauftrag auf mehreren Druckern gleichzeitig auszugeben. Für jeden der erzeugten Druckaufträge können Sie dabei unterschiedliche Einstellungen vornehmen. Die jüngste Version erlaubt es sogar, den zu wählenden Druckernamen anhand der Seitenzahl, des Titels, des Benutzers oder des Seitenformats automatisch festzulegen. Mit den Scripting-Möglichkeiten auf Druckausgaben ist beispielsweise die automatische Archivierung von Ausdrucken in PDF-Dateien realisierbar. Die Einstellung der Software steuern Sie dabei ausschließlich über INI-Dateien. Auf der Homepage des Herstellers findet sich ein überaus lesenswerter Satz: "PrintMulti ist nicht für den unbedarften Anwender gedacht, sondern richtet sich an Administratoren mit Kenntnissen im Druckbereich."

Leider ist es unter Microsoft Windows nicht so einfach möglich, die Dateien, die in der Druckerwarteschlange auf den Ausdruck warten, direkt zu betrachten. Besonders, wenn verzweifelte Benutzer mehrfach auf den Druckbefehl klicken, sammelt sich eine große Anzahl von Druckaufträgen in der Warteschlange der Printservers. Es gibt nur eine indirekte Möglichkeit mit der Freeware SPLViewer, einen Blick in diese Dokumente zu werfen. Das schlanke Werkzeug verknüpft sich mit der Dateinamenerweiterung .SPL und ermöglicht so einen Blick in das Spooler-Verzeichnis unter *%windir%\system32\spool\printers*. SPLViewer bietet zwar die Möglichkeit, die Druckerwarteschlange direkt einzusehen und die dortigen Druckaufträge mit einem Doppelklick zu öffnen, doch schlägt diese Funktion unter Windows 7 x64 fehl. Die Druckereinstellungen von Windows lassen sich bei Bedarf so verändern, dass die Spool-Dateien nicht gelöscht werden. Somit können Sie auch nachträglich einen Blick in die bereits gedruckten Dokumente werfen. *(ln)*

[1] ScriptLogic Desktop Authority
ABP31

[2] ThinPrint .print
ABP32

[3] triCerat ScrewDrivers 4 / Simplify Suite
ABP33

[4] LVB Print PrintMulti / SPLViewer
ABP34

Link-Codes

Kerberos Ticket-Limit in Windows Server

Unbekannte Grenzen

von Matthias Wessner


Quelle: Pixelio.de

Seit Windows 2000 und der Einführung des Active Directory ist das Kerberos-Protokoll zusätzlich zum NT LAN Manager (NTLM) eingeführt worden. Kerberos ist sicherlich auch als wesentlich leistungsfähiger als der NTLM anzusehen, doch hat auch das Kerberos-Protokoll seine Grenzen, die aber nicht immer bekannt sind. Dieser Workshop zeigt anhand eines Beispiels aus dem echten Leben, wo das Protokoll an seine Limits stößt und wie Administratoren diese erkennen und umgehen.

In unserem Beispiel betrachten wir das Active Directory-Konzept in einem internationalen Konzern. Da Niederlassungen in unterschiedlichen Ländern aus administrativer Sicht getrennt werden sollen und auch immer wieder neue akquirierte Firmen integriert werden müssen, wurde im Konzern ein Active Directory (AD) in einem Multi-Domain-Modell konzipiert und umgesetzt.

Szenario

Ein Teil dieses Active Directory-Konzeptes ist das Gruppen-Design. Dabei wurde, wie auch im TechNet beschrieben [1], nach dem Konzept "AGLP" vorgegangen (Accounts in Global, Global in Local und Local erhält die Permissions). Das bedeutet, dass Berechtigungen wie zum Beispiel Datei- oder Druckerzugriffe in "Domänenlokale Gruppen" vergeben werden und Benutzer in "Domänenglobale Gruppen" zusammengefasst werden. Diese Domänenglobalen Gruppen werden dann in die Domänenlokalen Gruppen aufgenommen, um den Anwendern letztendlich die Rechte zuzuweisen. Der Vorteil dieser Konstellation ist, dass die Administration der Globalen Gruppen in den einzelnen Domänen stattfinden kann und sich damit die Aufgaben delegieren lassen. Universelle Gruppen wurden in dem Design nicht betrachtet, da eingangs noch ein Mixed Mode Active Directory im Einsatz war.

Eine weitere Anforderung war das dedizierte Zuweisen von Berechtigungen auf Dateifreigaben. Das Konzept sieht vor, dass es pro Freigabe drei Lokale Gruppen gibt: eine für Lesen, eine für Schreiben und eine für Ändern. Soll ein Anwender alle drei Rechte bekommen, so muss er in allen drei Gruppen aufgenommen werden. Dieses passiert dann meistens wieder – je nach Anforderung – in der Bündelung in einer Globalen Gruppe.

Erste Störungen

Das Konzept ging gut auf, die Administration hatte sich eingespielt und die Gruppen-Erstellung war automatisiert. Doch eines Tages meldeten Anwender, dass sie Probleme mit dem Zugriff auf Ressourcen haben. Es häuften sich Support-Tickets bezüglich des Zugriffs auf Outlook Web Access. Anfangs nahm der Support selbstverständlich an, dass die Anwender ihr Kennwort nicht richtig eingegeben hatten. Dies wurde jedoch eingehend geprüft und konnte als Ursache für die Häufung ausgeschlossen werden. Da es nur wenige Anwender betraf und das OWA nur für das Home Office zum Einsatz kam, wurde der Fall erst mal als "Akte X"-Fall abgelegt.

Doch dann häuften sich die Probleme der Anwender: Immer wieder kam es zu dem Phänomen, dass sich ein Anwender nicht an der Outlook Web Access-Webseite anmelden konnte. Das Problem wurde daraufhin erneut analysiert. Es wurde zunächst kein sachlicher Zusammenhang bei den Benutzern festgestellt, sie kamen aus verschiedenen Standorten, ja sogar aus verschiedenen Domänen. Das Einzige, was die Anwender verband, war die Mitgliedschaft in vielen Gruppen. Parallel realisierte die IT-Abteilung ein neues Projekt, das den Zugriff über eine Webseite beinhaltete. Für die Autorisierung wurden wieder unterschiedliche Lokale Gruppen für die Berechtigungsverteilung gebildet, und in diese die Globalen Gruppen (mit den einzelnen Benutzerkonten) eingebunden.

Fehlersuche

Ein Teil der Anwender konnte aber nicht auf die Webseite zugreifen. Die Berechtigungen wurden doppelt geprüft, es ließ sich aber kein Unterschied zwischen funktionierenden und geblockten Anwendern finden. Um das Problem weiter einzukreisen, führten die Admins Netzwerk-Traces mit dem Microsoft Netzwerkmonitor durch und analysierten die Verbindung zwischen dem Client und dem Server. Die Netzwerk-Traces zeigten auf den ersten Blick

eigentlich nur, dass der Anwender nicht autorisiert ist, die Ressource anzufordern. Der einzige Anhaltspunkt war, dass es nur Benutzer traf, die Mitglied in vielen Gruppen waren. Dabei ist zu berücksichtigen, dass Gruppenmitgliedschaften rekursiv ermittelt werden. Ist ein Anwender zum Beispiel Mitglied in einer Globalen Gruppe, die wiederum Mitglied in drei (Domänen-) Lokalen Gruppen ist, so ist der Anwender insgesamt Mitglied von vier Gruppen. In einem Multidomänen-Modell zählen immer alle Globalen Gruppen aus allen Domänen, alle Universellen Gruppen und die Domänenlokalen Gruppen der Domäne, in der die Ressource liegt, auf die der Anwender zugreifen will. Durch das eingangs beschriebene AGLP-Modell wird der Anwender immer automatisch Mitglied von mindestens zwei Gruppen, wenn er eine Zugriffsberechtigung erhält.

Um die Vermutung zu bestätigen, dass das Problem an der Anzahl der Gruppenmitgliedschaften hängt, entfernten die Administratoren einen betroffenen Anwender aus verschiedenen Gruppen, so dass seine Gesamtgruppenzahl circa 50 Gruppen betrug. Und siehe da, der Zugriff auf die Website war wieder möglich. Mit der gewonnenen Erkenntnis wurden die Netzwerk-Traces erweitert und auch die Kommunikation mit den Active Directory-Servern einbezogen. Es fiel auf, dass bei Anwendern mit vielen Gruppen und entsprechenden Problemen der folgende Fehler auftrat, und zwar als Antwort auf die Kerberos-Anfrage an den Domänencontroller:

```
KerberosV5:KRB_ERROR  - KRB_ERR_
  RESPONSE_TOO_BIG
```

Dieser Fehler deutet darauf hin, dass der Inhalt des Kerberos-Tickets zu groß war. Damit gehen die Gruppenmitgliedschaften verloren beziehungsweise wird das Kerberos-Ticket an sich ungültig und ist somit nutzlos für die Autorisierung. Weitere Nachforschungen ergaben, dass die Kerberos-Ticketgröße per Default seit Windows 2003 SP2 auf 12.000 Byte beschränkt ist, dieser Wert sich aber über eine Registry-Änderung auf maximal 65.535 Byte erhöhen lässt. Dieser Eintrag muss möglichst auf allen Rechnern in einer Domäne gesetzt werden, damit das entsprechende Problem nicht auftritt.

Kerberos-Ticketgröße ermitteln

Die genaue Kalkulation der Ticketgröße ist nicht möglich, sondern immer von verschiedenen Faktoren abhängig. Es gibt aber eine Faustformel von Microsoft, mit der Sie einen Richtwert ermitteln. Dabei ist es wichtig, ob "SIDHistory" aktiviert ist oder nicht, denn jede zusätzliche (historische) SID, die an einer Gruppe hängt, benötigt zusätzlichen Speicherplatz. Jede Domain Local Group und Universal Group aus einer anderen Domäne benötigt 40 Bytes und jede Domain Global und Universal Group aus der eigenen Domäne 12 Bytes. Wird SIDHistory genutzt, dann zählt jede SID wie eine separate Gruppe (mit 12 oder 40 Bytes). Zusätzlich müssen Sie 1.200 Bytes für den Header des Tickets einkalkulieren. Ist "trusted for delegation" aktiviert, müssen Sie das Ergebnis verdoppeln.

Ist also ein Benutzer in 100 (Domänen) Lokalen Gruppen und in 200 (Domänen) Globalen Gruppen, ergibt sich eine Ticketgröße von etwa 7.600 Bytes (1.200 plus 40 Bytes mal 100 plus 12 Bytes mal 200). Wird jetzt noch für die 100 Lokalen Gruppen SIDHistory genutzt, sind wir schon bei einer Ticketgröße von 11.700 Bytes (1.200 plus 40 mal 100 mal 2 plus 12 mal 200), womit wir schon an der Grenze von 12.000 Bytes angelangt sind, die für Windows 2003 SP2 per Standard gilt.

Nun setzten die Administratoren die entsprechenden Werte und testeten das Szenario nach einem Neustart der entsprechenden Clients und Server. Das Fehlerbild war nun ein neues: Die Anwender erhielten die Meldung, dass ein "Bad Request" gestellt wurde und die Webseite wiederum nicht angezeigt werden kann. Jetzt durfte zwar das Kerberos-Ticket größer sein, nur der Webserver (Windows 2003 / IIS 6.0) konnte nicht mit dem großen Ticket umgehen. Eine Recherche ergab wiederum einen Optimierungsparameter für den Webserver, damit dieser auch mit großen Kerberos-Paketen umgehen kann. Dies sind die DWORD-Werte "MaxFieldLength" und "MaxRequestBytes" in dem Schlüssel "HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ http \ Parameters". Nach Anpassung des entsprechenden Registry-Wertes waren die Anwender in der Lage, die Webseite aufzurufen. Die Einstellungen wurden dann auch für die Outlook Web Access-Server durchgeführt, und auch die dort aufgetretenen Probleme waren damit gelöst.

Weiterführende Informationen

Da diese Begrenzungen des Protokolls der IT-Abteilung vorher nicht bekannt waren, stellten die Administratoren weitere Nachforschungen bezüglich des Kerberos-Ti-

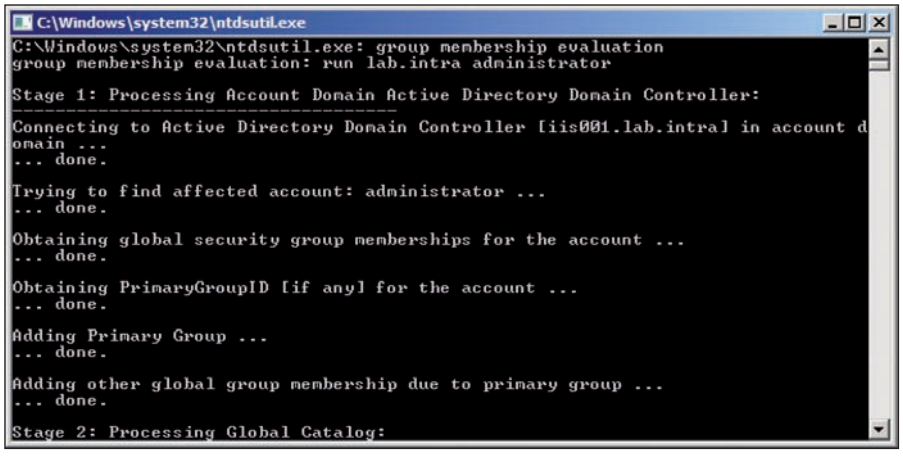


Bild 1: Analyse der Gruppenzugehörigkeiten mit NTDSUTIL

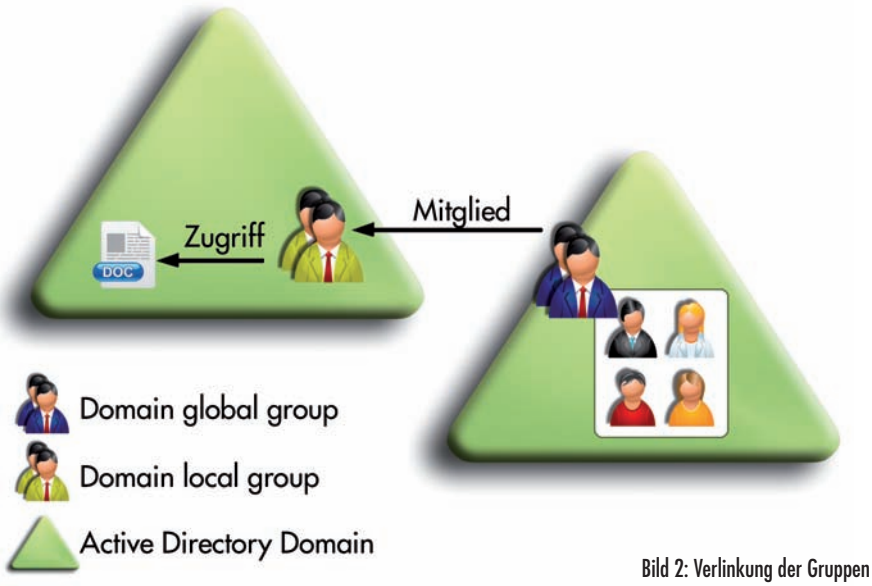


Bild 2: Verlinkung der Gruppen

ckets an. Und es gibt tatsächlich eine weitere Beschränkung: Ein Kerberos-Ticket kann maximal 1.023 Gruppen enthalten, wobei Microsoft empfiehlt, dass ein Anwender nicht Mitglied von mehr als 1.015 Gruppen sein sollte. Der Grund ist ganz einfach: Auch die Built In-Gruppen wie "Terminal Server Benutzer" oder "Interaktiv" zählen zu diesen Gruppen.

Die Überschreitung der Gruppenanzahl liefert glücklicherweise eine aussagekräftige Fehlermeldung bei der Anmeldung und im Eventlog. Microsoft stellt mit NTDSUTIL ein Programm bereit, mit dem Sie unter anderem die Gruppenmitgliedschaften analysieren. Sie sollten dieses Tool auf einem Domänencontroller ausführen, der auch Global Catalog Server ist. Nach Aufrufen von NTDSUTIL von der Kommandozeile gebe Sie *group membership evaluation* ein. Danach nutzen Sie *RUN {DOMAIN} {User}* (wobei dies die Domäne und der Benutzer ist, den Sie analysieren möchten), um eine Auflistung aller Gruppen, in denen der Anwender Mitglied ist – auch der Built In-Gruppen – zu erhalten.

Die Gefahr unbekannter Grenzen nimmt zu

Während Sie die maximale Kerberos-Ticketgröße durch Anpassen des Registry-Wertes relativ komfortabel erhöhen, stellt die Mitgliedschaft in 1.015 Gruppen eine feste, nicht erweiterbare Grenze dar. Auf den ersten Blick erscheint diese Anzahl an Gruppen zwar als ziemlich viel; bei Anwendung des AGLP-Prinzips halbiert sich dieser Wert aber zunächst auf nur etwa 500 Gruppen, da eine Ressourcen-Zuweisung ja immer über zwei Gruppen erfolgt.

Aufgrund des Paradigmenwechsels bei der Anwendungsbereitstellung wird das Thema Gruppenmitgliedschaft immer wichtiger. Anwendungen werden immer mehr den Benutzern zugewiesen und immer seltener den Arbeitsstationen. Insbesondere Technologien wie beispielsweise XenApp oder App-V werten die benutzerspezifische Anwendungszuordnung gegenüber der maschinenspezifischen Anwendungszuordnung deutlich auf. Auch "klassische" Softwaremanagement- und -verteillösungen rücken die Autorisierung anhand von Benutzergruppen stärker in den Vordergrund. Auch hier sieht das Modell vor, dass eine (Domänen) Lokale Gruppe das Recht auf die Anwendung erhält und die Anwender dann über die Mitgliedschaft einer Globalen Gruppe indirekt Mitglied der Lokalen Gruppe werden und damit auf die Anwendung (siehe Bild 3) zugreifen können. Durch diese anwenderzentrierte Applikationszuweisung erhöht sich die Anzahl der Gruppen, in denen ein Anwender Mitglied ist. Um dem Dilemma zu entkommen, wenn Sie das AGLP-Konzept nutzen und an die Grenzen des Kerberos-Tickets stoßen, bilden Sie separate Ressourcen-Domänen, in denen die Anwendungen berechtigt werden. Da Domänenlokale Gruppen nur in der jeweiligen Domäne gültig sind, werden die Domänenlokalen Gruppen aus anderen Domänen bei der Auswertung der Gruppenmitgliedschaften in einer Ressourcen-Domäne nicht mitgezählt, wodurch Sie einiges an Luft gewinnen – allerdings mit dem Nachteil, dass zusätzliche Lizenzen für die zusätzlichen Domänencontroller anfallen und sich die Komplexität der gesamten Infrastruktur erhöht.

Fazit

Das Kerberos Ticket-Problem erwischt Sie meist unverhofft. Da in einem solchen Fall bei Netzwerkanalysen häufig nicht die Active Directory-Anfragen ausgewertet werden, laufen erste Fehleranalysen ins Leere. Auf Basis der oben beschriebenen Modelle lässt sich aber sehr schnell ermitteln, ob die Ticketgröße das Problem verursacht. Zum Glück ist es dann sehr einfach, diese zu erhöhen, was sich auch nur geringfügig auf den Netzwerkverkehr auswirkt. Wir können gespannt sein, wann Microsoft die Einstellung auch gleich in die Standard-Gruppenrichtlinien aufnimmt, anstatt aufzuzeigen, wie Sie ein ADM-Template erstellen [2]. Die Anpassungen der Webservices oder anderer Dienste werden mittelfristig auch der Vergangenheit angehören, da aktuelle Programme entsprechend große Tickets akzeptieren sollten. Die Grenze der 1.015 Gruppen lässt sich aber nicht erweitern, sondern nur durch Design-Entscheidungen umgehen. *(jp)*

Matthias Wessner ist Principal Architect bei der Login Consultants Germany GmbH.

[1] Active Directory Groups
AAP21

[2] How to use Group Policy to add the MaxTokenSize registry entry to multiple computers
AAP22

Link-Codes

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2010!

180 Seiten Praxis-Know-how
rund um das Thema

Active Directory

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iladministrator
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/2010 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

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

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

Ich zahle ☐ per Bankeinzug

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 1210

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

Database Availability Groups unter Exchange 2010

Doppeltes Postfach

von Thomas Joos

Mit den neuen Database Availability Groups in Exchange Server 2010 können Administratoren Exchange-Datenbanken zwischen verschiedenen Servern synchron halten. Somit steht ein Weg zu erhöhter Verfügbarkeit bereit, der keinen Windows-Cluster benötigt. In diesem Workshop richten wir die Database Availability Groups ein, konfigurieren die Replikation und werfen einen Blick darauf, wie sich Postfachdatenbankkopien als produktive Datenbank einsetzen lassen.

Die Basis der Database Availability Groups (DAG) ist ähnlich zur lokalen Replikation (LCR) beziehungsweise der Cluster-Replikation (CCR) in Exchange Server 2007 angelegt. Notwendig ist dazu die Enterprise-Edition von Windows Server 2008 oder Windows Server 2008 R2, da die Funktion den Windows Clusterdienst nutzt. Sie müssen für den Einsatz von DAG aber keinen Cluster erstellen. Datenbankverfügbarkeitsgruppen sind auch mit der Standard Edition von Exchange Server 2010 möglich.

Funktionsweise der DAG

Die Replikation der Datenbanken zwischen den beteiligten Servern erfolgt über Transaktionsprotokolle. Administratoren können auch Nachlaufzeiten festlegen und Datenbanken erst nach gewisser Zeit durch Transaktionsprotokolle aktualisieren lassen. Jede DAG darf bis zu 16 Mitglieder haben. Die Standard-Edition von Exchange Server 2010 unterstützt bis zu fünf Postfachspeicher auf einem Server, die Enterprise-Edition bis zu 100, inklusive aller Postfachdatenbankkopien. Bei beiden Editionen dürfen die Datenbanken eine maximale Größe von 16 TByte erreichen. Fällt ein Server aus, können Sie leicht auf ein Replikat umschalten und die Anwender können weiterarbeiten.

Da in Exchange Server 2010 Datenbanken einen einmaligen Namen in der Organisation haben müssen, können Sie durch Postfachdatenbankkopien in einer DAG alle produktiven Datenbanken auf alle Postfachserver kopieren und bei Bedarf auch aktiv schalten. Bei einem Ausfall müssen Sie nicht mehr den kompletten Exchange-Server auf einen anderen Clusterknoten verschieben. DAGs sind sozusagen ein Exchange-RAID über mehrere Server hinweg.

Die Replikation erfolgt nicht über das Server Message Block-Protokoll (SMB), sondern über ein neues, spezielles Replikationsverfahren, bei dem Exchange 2010 einen festgelegten TCP-Port für den Datenaustausch verwendet. Aktive Transaktionsprotokolle der produktiven Exchange-Datenbank senden einen Datenstrom an die passiven Kopien. Der Datenstrom ist verschlüsselt und komprimiert. Exchange Server 2010 kann als Quelle für die Replikation der Daten die produktive Datenbank oder eine andere Postfachdatenbankkopie verwenden. Exchange nutzt für einen DAG-Cluster auch noch einen weiteren Server als Zeugen im Netzwerk, auf dem ein Verzeichnis liegt, das Daten des Clusters enthält. Microsoft empfiehlt dazu einen Hub-Transport-Server. Dieser Server, Zeugenserver genannt, ist nicht Bestandteil des Clusters, sondern logisch außerhalb angeordnet. Diese Freigabe trägt die Bezeichnung "File Share Witness" (Dateifreigabenzeuge) und dient der Absicherung des Datenflusses zwischen den Cluster-Knoten.

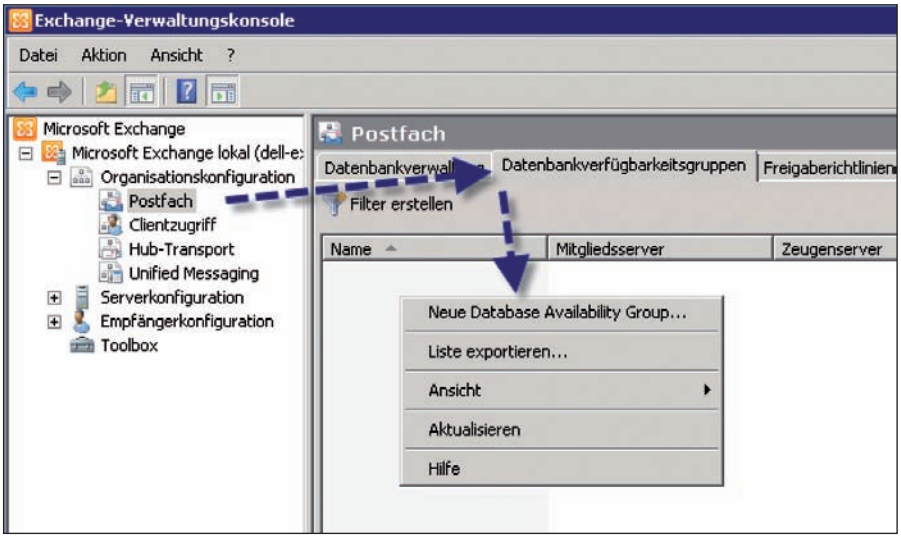


Bild 1: DAGs lassen sich in der Verwaltungskonsole einrichten

Hauptsächlich ist diese Erweiterung in Zwei-Knoten-Clustern notwendig. Beim Einsatz mehrerer Knoten ist ein Zeuge nicht immer notwendig, da der Ausfall eines Servers durch zwei Knoten abgefangen wird.

Erstellen und Verwalten von DAG in der Exchange-Verwaltungskonsole

In der Exchange-Verwaltungskonsole finden Sie die Steuerung der DAG über "Organisationskonfiguration / Postfach" auf der Registerkarte "Datenbankverfügbarkeitsgruppen". Setzen Sie im Unternehmen IPv6 ein, versucht der Assistent der DAG, auch eine IPv6-Adresse zuzuweisen.

Sie müssen für die DAG keinen Windows-Cluster erstellen oder die Server besonders ausrüsten. Auf allen Servern muss allerdings der gleiche Stand des Betriebssystems installiert sein. Der Zeugenserver für den DAG-Cluster muss allerdings nicht das identische Betriebssystem aufweisen. Sie können aber in einer DAG verschiedene Editionen von Exchange Server 2010 installieren, also die Standard Edition und die Enterprise Edition. Allerdings unterstützt Exchange Server 2007 keine DAG, daher können Sie keine Postfachserver mit Exchange Server 2007 in eine DAG aufnehmen.

Geben Sie bei der Erstellung den Namen für den Zeugenserver und das Verzeichnis nicht an, sucht der Assistent nach einem Hub-Transport-Server, auf dem die Postfachserverrolle nicht installiert ist. Der Assistent erstellt automatisch das Standardverzeichnis und die Freigabe auf diesem Hub-Transport-Server und verwendet den Server als Zeugenserver. Aktivieren Sie die Option "Zeugenserver" und geben einen Server an, können Sie die Option "Zeugenverzeichnis" deaktiviert lassen. In diesem Fall erstellt der Assistent das Standardverzeichnis auf dem angegebenen Zeugenserver. Auf dem Zeugenserver für einen DAG-Cluster muss nicht die Exchange Server 2010-Version installiert sein. In diesem Fall fügen Sie der lokalen Administratorgruppe auf dem Zeugenserver die universelle Exchange-Sicherheitsgruppe "Exchange Trusted Subsystem" manuell hinzu. Außerdem sollten Sie die Gruppe der Organisationsadministratoren in die lokale Administrator-Gruppe aufnehmen.

Den Namen der DAG legt der Assistent im Active Directory als Clusternetzwerkobjekt an. Nach dem Erstellen einer DAG verwendet diese zunächst DHCP zur Kommunikation, denn jede DAG benötigt eine eigene IP-Adresse. Mit dem Cmdlet "Set-DatabaseAvailabilityGroup" oder in den Eigenschaften der DAG in der Exchange-Verwaltungskonsole passen Sie die IP-Adresse an. Diese Einstellung ist aber erst nach der Installation von Service Pack 1 für Exchange Server 2010 verfügbar. Wollen Sie eine DAG nicht in der Exchange-Verwaltungskonsole, sondern der Exchange-Verwaltungsshell erstellen, verwenden Sie den Befehl

```
New-DatabaseAvailabilityGroup -Name
  {Name der DAG} -WitnessServer
  {Zeugenserver} -WitnessDirectory
  {Zeugenverzeichnis} -DatabaseAvai-
  labilityGroupIPAddresses {Liste
  der IP-Adressen, kommagetrennt}
```

DAG-Mitglieder hinzufügen und entfernen

Der nächste wichtige Schritt ist das Aufnehmen von Mitgliedern. Bei den Mitgliedern handelt es sich um Server mit der Postfachrolle in der Organisation, um die Datenbanken dieser Server über DAG zu replizieren. Jeder Server, der Mitglied der DAG ist, nimmt Exchange als Clusterknoten in den zu Grunde liegenden Windows-Cluster auf. In der Exchange-Verwaltungskonsole klicken Sie über "Organisationskonfiguration / Postfach" mit der rechten Maustaste auf die DAG auf der Registerkarte "Datenbankverfügbarkeitsgruppen". Wählen Sie über das Kontextmenü "Mitgliedschaft in Datenbankverfügbarkeitsgruppe verwalten" aus.

Auf der nächsten Seite können Sie einen oder mehrere Server zu der DAG hinzufügen. Klicken Sie dazu auf die Schaltfläche "Hinzufügen" und wählen Sie den Server aus, den Sie der DAG hinzugesellen wollen. Nur Datenbanken auf Postfachservern mit Exchange Server 2010, die Mitglied einer DAG sind, lassen sich durch die DAG absichern. Sie können über das gleiche Menü auch Server wieder aus der DAG entfernen. Neben der Exchange-Verwaltungskonsole können Sie auch Server in der Exchange-Verwaltungsshell zu einer DAG hinzufügen:

```
Add-DatabaseAvailbilityGroupServer
  -Identity {Name der DAG}
  -MailboxServer {Name des Servers}
```

Postfachdatenbankkopien für DAG einrichten

Eine DAG ist zunächst nur ein leeres Gerüst. Erst wenn Sie Server als Mitglieder aufnehmen und die Datenbanken dieser Postfachserver replizieren lassen, aktivieren Sie die Funktion. Exchange richtet aber keine automatische Replikation ein, wenn Sie einen Server in eine DAG aufnehmen. Sie müssen dazu selbst Postfachdatenbankkopien anlegen. Diese sind Replikate der produktiven Postfachdatenbanken auf den verschiedenen Mitgliedern der DAG. Sie können keine Kopien derselben Datenbank auf demselben Server erstellen. Alle Kopien einer Datenbank verwenden auf allen Servern denselben Pfad zu den Datenbankdateien.

Datenbankkopien erstellen Sie in der Exchange-Verwaltungskonsole oder mit dem Cmdlet "Add-MailboxDatabaseCopy" in der Exchange-Verwaltungsshell. Der Server muss Mitglied derselben DAG sein, eine Replikation zwischen verschiedenen DAGs ist nicht möglich. Bei der Erstellung einer Kopie geben Sie auch eine Zeitspanne in Minuten für die Wiedergabeverzögerung der Transaktionsprotokolle an. Verwenden Sie den Wert "0", deaktivieren Sie die Protokollwiedergabeverzögerung. Allerdings lassen sich Verzögerungen nur dann einstellen, wenn Sie die Kopie in der Exchange-Verwaltungsshell erstellen.

Die Aktivierungseinstellungsnummer dient als Entscheidungsgrundlage bei der Datenbankaktivierung. Erkennt Exchange im Fehlerfall, dass mehrere Datenbankkopien auf unterschiedlichen Servern dieselben Aktivierungskriterien erfüllen, verwendet Exchange bei einem Ausfall die Kopie mit der niedrigsten Aktivierungseinstellungsnummer. Die aktive Kopie der Postfachdatenbankkopie, also die produktive Datenbank, muss bereitgestellt (gemountet) sein, ansonsten lässt sich keine Kopie erstellen. Die Umlaufprotokollierung darf nicht aktiviert sein. Um eine Kopie zu schaffen, öffnen Sie die Exchange-Verwaltungskonsole und navigieren zu "Organisationskonfiguration / Postfach". Klicken Sie auf der Registerkarte "Datenbankverwaltung" mit der rechten Maustaste auf die Postfachdatenbank, von der Sie eine Kopie erstellen wollen, und klicken Sie dann auf "Neue Postfachdatenbankkopie hinzufügen".

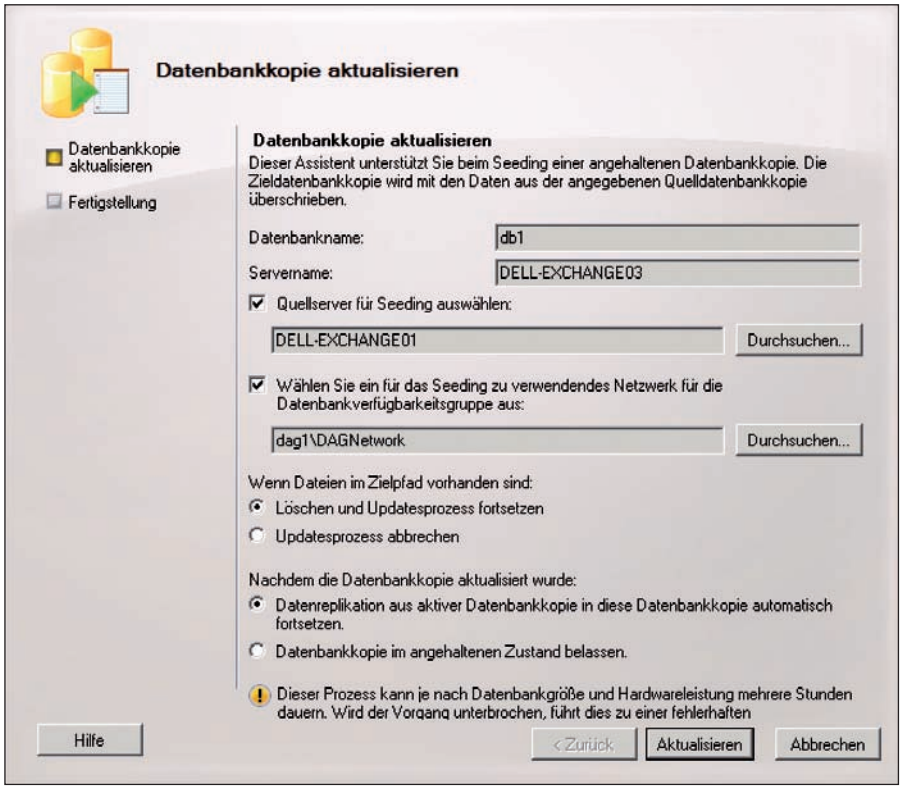


Bild 2: Nachdem die Replikation gestoppt ist, kann eine manuelle Aktualisierung der Postfachdatenbank erfolgen

Der Assistent zeigt nur die Postfachserver an, die Mitglied der gleichen DAG sind. Nach der Erstellung der Kopie sehen Sie deren Status auf der Registerkarte "Datenbankkopien" im unteren Bereich der Exchange-Verwaltungskonsole, wenn Sie die Datenbank markieren. Überprüfen Sie anschließend den Status der Kopien. Mit dem Cmdlet "Get-MailboxDatabaseCopyStatus" können Sie sich den Status der Replikation für die Datenbankkopie anzeigen lassen. Das Cmdlet "Test-ReplicationHealth" informiert Sie über den Status der Datenbankverfügbarkeitsgruppe und der Replikation. Wechseln Sie in der Exchange-Verwaltungsshell in das Scripts-Verzeichnis von Exchange Server 2010 (standardmäßig "C:\Program Files\Microsoft\Exchange Server\V14\Scripts"), können Sie durch Eingabe von *.\CheckDatabaseRedundancy.ps1* ebenfalls einen Test der Replikation durchführen. Wollen Sie eine Postfachdatenbankkopie löschen, klicken Sie diese mit der rechten Maustaste an und wählen Sie den Befehl "Entfernen" aus.

In der Exchange-Verwaltungsshell können Sie auch Verzögerungen konfigurieren, in denen die Daten der produktiven Datenbanken in die Postfachdatenbankkopien geschrieben werden. Das Cmdlet "Add-MailboxDatabaseCopy" verfügt über die beiden Optionen "ReplayLagTime" und "TruncationLagTime". ReplayLagtime legt fest, wie lange Exchange nach dem Kopieren der Transaktionsprotokolle auf dem Server mit der Postfachdatenbankkopie warten soll, bis die Transaktionsprotokolle in die Postfachdatenbankkopie übernommen werden (das Format dieser Option ist "Tage:Stunden:Minuten:Sekunden"). Der Standardwert ist "0", das heißt Ex-

change schreibt die Daten sofort in die Postfachdatenbankkopie. TruncationLagTime legt fest, wann Exchange die Transaktionsprotokolle löschen soll, die in die Datenbankkopie geschrieben sind. Alle Kopien einer Postfachdatenbank müssen sich auf jedem Server, der als Host für eine Kopie konfiguriert ist, im gleichen Pfad befinden. Um eine Postfachdatenbank in einer DAG zu verschieben, müssen Sie die Replikation für die Datenbank für alle Kopien deaktivieren. Es reicht nicht aus, die Replikation über das Kontextmenü der Kopie nur anzuhalten.

Anhalten oder Fortsetzen der Replikation

Sie können die Kopiervorgänge für die Replikation zeitweise deaktivieren. In diesem Fall bleibt die Konfiguration erhalten, aber Exchange kopiert keine Daten mehr von der produktiven Datenbank zur Datenbankkopie. Sie führen diese Vorgänge über das Kontextmenü der Datenbankkopie in der Exchange-Verwaltungskonsole durch. Wählen Sie im Kontextmenü die Option "Datenbankkopie anhalten" aus. Klicken Sie erneut mit der rechten Maustaste auf die Datenbankkopie, setzen Sie mit "Datenbankkopie fortsetzen" die Replikation fort.

Sie können eine Replikation auch manuell durchführen. Diesen Vorgang bezeichnet Microsoft als "Seeding". Eine manuelle Übertragung ist zum Beispiel sinnvoll, wenn Sie mit Eseutil eine Offlinedefragmentierung für eine Datenbank durchgeführt haben oder wenn Sie aus anderen Gründen sicherstellen wollen, dass die Postfachdatenbankkopie von der produktiven Datenbank aktualisiert wird. Verwenden Sie für diesen Vorgang das Cmdlet "Update-MailboxDatabaseCopy". Sie können auch den Assistenten zum Aktualisieren in der Exchange-Verwaltungskonsole verwenden, den Sie im Kontextmenü der Postfachdatenbankkopie finden. Eine weitere Möglichkeit sieht so aus, dass Sie die Bereitstellung der aktiven Datenbank aufheben und die Datenbankdatei auf den Postfachserver mit der Postfachdatenbankkopie kopieren.

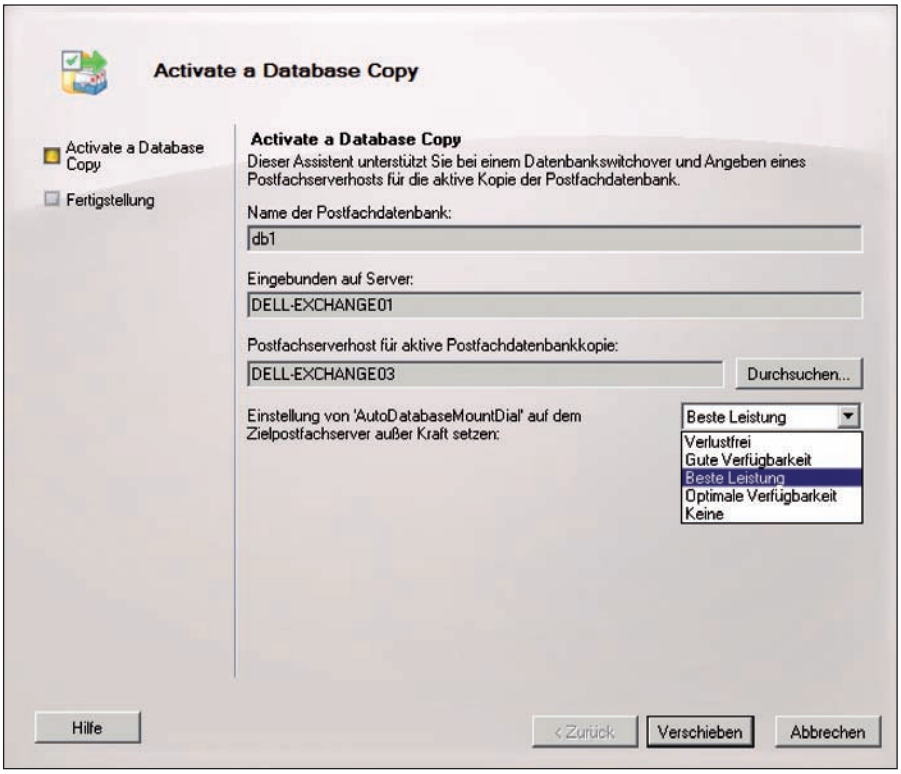


Bild 3: Aktivieren einer Postfachdatenbankkopie als produktive Datenbank

Damit Sie die Kopie einer Postfachdatenbank aktualisieren können, müssen Sie die Replikation zunächst anhalten. Diesen Befehl finden Sie im Kontextmenü der Postfachdatenbankkopie. Navigieren Sie in der Exchange-Verwaltungskonsole zu "Organisationskonfiguration / Postfach" und öffnen Sie die Registerkarte "Datenbankverwaltung". Klicken Sie mit der rechten Maustaste auf die Datenbankkopie, die Sie aktualisieren wollen, und wählen "Datenbankkopie aktualisieren" aus. Konfigurieren Sie auf der ersten Seite des Assistenten die notwendigen Optionen. Standardmäßig verwendet der Vorgang die produktive Datenbank als Quelle. Sie können aber auch eine passive Kopie der Datenbank für das Seeding verwenden.

Postfachdatenbankkopien als produktive Datenbank einsetzen

Beim Aktivieren einer Postfachdatenbankkopie legen Sie fest, dass eine der erstellten Postfachdatenbankkopien zur produktiven Datenbank wird und Anwender zukünftig mit dieser Datenbank arbeiten. Microsoft bezeichnet diesen Vorgang als "Switchover". Hierbei hebt Exchange die Bereitstellung der produktiven Datenbank auf und verwendet die Datenbankkopie auf dem Server mit der entsprechenden Postfachdatenbankkopie als neue produktive Datenbank. Die Datenbankkopie muss hierzu fehlerfrei und aktuell sein.

Navigieren Sie in der Exchange-Verwaltungskonsole zu "Organisationskonfiguration / Postfach" und öffnen Sie die Registerkarte "Datenbankverwaltung". Dort klicken Sie dann mit der rechten Maustaste auf die produktive Postfachdatenbank, von der Sie zukünftig eine Kopie als produktive Datenbank verwenden wollen. Klicken Sie dann auf "Aktive Postfachdatenbank verschieben" und wählen Sie im neuen Fenster den Server, der als Host für die produktive Datenbank verwendet werden soll. Nun legen Sie die gewünschte Einstellung für "AutoDatabaseMountDial" auf dem Server fest. Folgende Werte können Sie verwenden:

- Verlustfrei: Exchange stellt die Datenbank erst dann automatisch bereit, nachdem alle Transaktionsprotokolle in der neuen produktiven Datenbank eingeschrieben wurden.
- Beste Leistung: Exchange stellt die Datenbank sofort bereit – unabhängig von den Transaktionsprotokollen, die noch nicht in die passive Datenbankkopie geschrieben wurden.
- Gute Verfügbarkeit: Exchange stellt die Datenbank sofort automatisch bereit, wenn die Länge der Kopiewarteschlange kleiner oder gleich sechs ist. Dabei handelt es sich um die Anzahl der Transaktionsprotokolle, die Exchange noch replizieren muss. Ist die Länge der Kopiewarteschlange größer als sechs, stellt Exchange die Datenbank nicht automatisch bereit.
- Optimale Verfügbarkeit: Exchange stellt die Datenbank sofort automatisch bereit, wenn die Länge der Kopiewarteschlange kleiner oder gleich zwölf ist. Ist die Länge der Kopiewarteschlange größer als zwölf, stellt Exchange die Datenbank nicht automatisch bereit.
- Keine: Bei dieser Auswahl belässt der Assistent die Einstellung des Werts auf den Standard, der für die Datenbank bei der Erstellung gesetzt ist. Der Standardwert ist "Optimale Verfügbarkeit". Wenn Sie BestAvailability oder GoodAvailability angeben und nicht alle Protokolle von der aktiven Kopie auf die passive Kopie repliziert sind, kann es zum Verlust von Postfachdaten kommen.

Aktivieren einer Postfachdatenbankkopie als produktive Datenbank

Klicken Sie nun auf "Verschieben". Jetzt verwendet Exchange die bisherige Postfachdatenbankkopie als produktive Datenbank und die aktuelle produktive Datenbank als Postfachdatenbankkopie. Sie können diese Vorgänge auch in der Exchange-Verwaltungsshell anstoßen:

```
Move-ActiveMailboxDatabase {Name der
Datenbank} -ActivateOnServer {Server mit der Postfachkopie} -MountDialOverride:None (oder GoodAvailability, Lossless)
```

Sie können eine Postfachdatenbankkopie auch manuell aktivieren, wenn der Server mit der produktiven Datenbank in der DAG nicht mehr zur Verfügung steht. Klicken Sie einfach auf die entsprechende Postfachdatenbankkopie mit der rechten Maustaste und wählen Sie "Datenbankkopie aktivieren" aus. Anschließend wählen Sie auch hier aus, welche Einstellung Sie für AutoDatabaseMountDial auf dem Server verwenden wollen. Ist der ursprüngliche Server nicht verfügbar, können Sie auf diese Weise direkt einzelne Postfachdatenbankkopien aktivieren. Die Änderung des aktiven Servers ist für Benutzer vollkommen transparent. Es gehen keine Daten verloren. Unter Umständen müssen sich Anwender neu an OWA anmelden oder Outlook neu starten, um die Verbindung wieder herzustellen.

Die Aktivierung einer Postfachdatenbankkopie erfolgt automatisch, wenn eine Datenbank oder ein Postfachserver ausfällt. Datenbankkopien lassen sich aber auch für die Aktivierung so konfigurieren, dass Exchange diese nicht verwendet, sondern nur als Datensicherung einsetzt. Mit dem Befehl

```
Suspend-MailboxDatabaseCopy -Identity
{Postfachdatenbankkopie}
-ActivationOnly
```

verhindern Sie, dass Exchange die entsprechende Postfachdatenbankkopie im Falle eines Ausfalls der produktiven Datenbank aktiv schaltet. Mit dem Befehl

```
Resume-MailboxDatabaseCopy -Identity
{Postfachdatenbankkopie}
```

aktivieren Sie die Konfiguration wieder, so dass Exchange die Kopie als produktive Datenbank verwenden kann, wenn die aktuelle Produktionsdatenbank nicht mehr verfügbar ist.

Updates und Service Packs sollten Sie auf Mitgliedern von DAGs nicht automatisch installieren. Microsoft empfiehlt, die Installation von Updates und Service Packs auf Servern, die Mitglieder in einer DAG sind, in folgender Reihenfolge durchzuführen: Im ersten Schritt halten Sie die Replikation der Datenbank auf dem Server an, den Sie aktualisieren wollen. Verwenden Sie dazu die Exchange-Verwaltungskonsole oder die Exchange-Verwaltungsshell und geben Sie folgenden Befehl ein:

```
Get-MailboxDatabaseCopyStatus
-Server {Servername} |
Suspend-MailboxDatabaseCopy
```

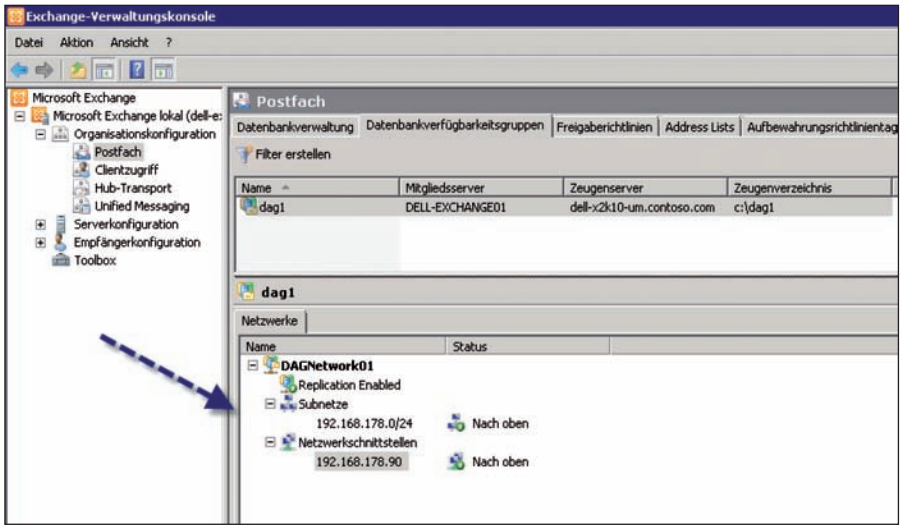


Bild 4: Verwalten der DAG-Netzwerke in der Exchange-Verwaltungskonsole

```
-ActivationOnly
-Confirm:$False -SuspendComment
"Installieren des Updates xyz"
```

In der Exchange-Verwaltungskonsole halten Sie die Replikation von Postfachdatenbankkopien an, wenn Sie mit der rechten Maustaste auf eine Datenbankkopie klicken und "Datenbank anhalten" auswählen. Auf den Servern, welche die produktive Datenbank bereitstellen, müssen Sie diesen Schritt nicht durchführen. Navigieren Sie anschließend in der Exchange-Verwaltungskonsole zu "Serverkonfiguration /Postfach" und wählen Sie den Server aus, auf dem Sie das Service Pack oder die Updates installieren wollen. Klicken Sie den Server mit der rechten Maustaste an und wählen Sie "Switchoverserver" aus. Verschieben Sie alle produktiven Datenbanken auf einen anderen Server in der DAG. Durch die beiden letzten Schritte ist sichergestellt, dass der Server, den Sie aktualisieren, weder eine produktive Datenbank bereitstellt, noch eine Aktualisierung der Postfachdatenbankkopien enthält. Installieren Sie anschließend die Aktualisierung auf dem Server. Nun setzen Sie die Replikation der Postfachdatenbankkopien auf dem Server fort und verschieben über "Serverwitchover" wieder die gewünschten produktiven Datenbanken auf den Server.

Grundsätzlich empfiehlt Microsoft, den Datenverkehr zur Replikation und die Verbindung der Anwender auf verschiedene Netzwerkkarten zu verteilen, die Sie während der Erstellung der DAG festlegen. Zur Erstellung eines DAG-Netzwerkes klicken Sie mit der rechten Maustaste auf die DAG und wählen "Neues Netzwerk für Datenbankverfügbarkeitsgruppen". Geben Sie im Fenster die entsprechenden Daten für das DAG-Netzwerk ein. Aktivieren Sie die Option "Replikation aktivieren", um dieses Netzwerk zur Replikation der Daten mit anderen Mitgliedern der DAG zu nutzen. Achten Sie aber darauf, dass in diesem Fall der Datenverkehr der Clients eingeschränkt ist und die Leistung einbrechen kann. Deaktivieren Sie diese Option, um dieses Netzwerk nicht für die Replikation der Daten zu verwenden, sondern nur für den Clientzugriff. Sie finden DAG-Netzwerke über "Organisationskonfiguration / Postfach" auf der Registerkarte "Datenbankverfügbarkeitsgruppen". Klicken Sie auf eine DAG, sehen Sie im unteren Bereich die verbundenen Netzwerke. Sie können auch die Reihenfolge der Netzwerke an dieser Stelle verändern, indem Sie diese mit den Schaltflächen nach oben oder nach unten schieben. Generell sollten Sie die Netzwerke, mit denen sich die Clients verbinden, ganz oben anordnen.

Komprimierung und Verschlüsselung für die Replikation steuern

Standardmäßig verwendet Exchange den Port 64327 zur Replikation der Daten zwischen den Servern. Sie können diesen Port aber beliebig anpassen. Mit dem Befehl

```
Get-DatabaseAvailabilityGroup
  {Name der Gruppe} -Status | fl
  ReplicationPort
```

sehen Sie den aktuell verwendeten Port. Um den Port anzupassen, verwenden Sie den Befehl

```
Set-DatabaseAvailabilityGroup
  {Name der DAG} -ReplicationPort
  {Portnummer}
```

Aktualisieren Sie anschließend eine Postfachdatenbankkopie, sehen Sie mit *Netstat -an |more*, dass Exchange jetzt diesen Port nutzt. Achten Sie bei der Änderung aber auch darauf, den neuen Port in der Windows-Firewall für die Kommunikation freizuschalten, ansonsten kann Exchange keine Daten mehr replizieren.

Exchange komprimiert die Daten vor einer Replikation zu den Kopieservern, wenn sich diese in verschiedenen Subnetzen befinden. Sie können sich den Status mit

```
Get-DatabaseAvailabilityGroup {Name
  der Gruppe} -Status | fl Network-
  Compression
```

anzeigen lassen. Die Einstellungen für die Komprimierung erfolgt immer für die ganze DAG, nicht für die einzelnen DAG-Netzwerke. Per Default ist die Einstellung auf "InterSubnetOnly" gesetzt. Das bedeutet, dass Exchange die Daten nur dann komprimiert, wenn diese über verschiedene Subnetze verteilt sind. Sie können folgende Werte verwenden:

- Disabled: Keine Komprimierung
- Enabled: Komprimierung bei allen Netzwerken, auch innerhalb des gleichen Subnetzes
- InterSubnetOnly: Komprimierung nur zwischen Subnetzen
- SeedOnly: Komprimierung nur beim manuellen Seeding

Wollen Sie die Komprimierung für alle Netzwerke einschalten, um dadurch die Belastung des Netzwerkes zu reduzieren, verwenden Sie den Befehl:

```
Set-DatabaseAvailabilityGroup
  {Name der DAG} -NetworkCompression
  Enabled
```

DAG nutzt die Kerberos-Authentifizierung zwischen den einzelnen Mitgliedern der DAG. Standardmäßig verschlüsselt Exchange die Daten vor einer Replikation zu den Kopieservern, wenn diese in verschiedenen Subnetzen positioniert sind. Sie können sich den Status mit

```
Get-DatabaseAvailabilityGroup
  {Name der Gruppe} -Status | fl
  NetworkEncryption
```

anzeigen lassen. Für die Verschlüsselung können Sie exakt die gleichen Werte eingeben wie bei der Komprimierung des Datenverkehrs. Über den Befehl

```
Set-DatabaseAvailabilityGroup
  {Name der DAG} -NetworkEncryption
  Enabled
```

schalten Siedie Verschlüsselung für alle Netzwerke ein, um dadurch die Sicherheit des Netzwerkes zu erhöhen. *(jp)*

Aktuelle IT-Anforderungen ändern das Netzdesign

Neuer Asphalt für die Datenautobahn

von Mathias Hein

Die besten Server und Storage-Komponenten der Welt sind ohne ein solides, gut geplantes Netzwerk wertlos. Doch durch neue Technologien, wie etwa Virtualisierung oder Voice over IP, ändern sich die Anforderungen an das Netzdesign. Das geänderte Netzwerkdesign betrifft alle Bereiche des LAN, des WAN und auch des SAN. Dieser Beitrag zeigt neue Protokolle und Technologien, die den Betrieb der Netzwerke für die Kommunikations- oder Virtualisierungsinfrastrukturen dramatisch ändern.

Alle Netzvarianten enthalten den so genannten Netzwerk-Kern (Core). Die Größe des Unternehmens bestimmt in der Regel die Größe und Kapazität des Netzwerkkerns. In den meisten Infrastrukturen unterscheidet sich der Datacenter Core vom Core des eigentlichen Netzwerks. Wenn wir von einem hypothetischen Netzwerk ausgehen, durch das ein paar hundert Nutzer in einem einzigen Gebäude mit einem Datencenter verbunden werden sollen, dann baut das Netzwerk auf folgender Struktur auf: ein oder mehrere große Switches im Core und mehrere Aggregation-Switches im Edge-Bereich.

Im Idealfall besteht der Kern aus zwei modularen Switching-Plattformen, die die Daten über 1 beziehungsweise 10 GBit-Glasfaser zu den Switches auf den Etagen transportieren. Die Core Switches befinden sich im gleichen Raum wie die Server- und Storage-Infrastrukturen. Eine Verbindung vom zentralen Switch mit zwei 1/10 GBit-Glasfaser-Links zum Etagenverteiler genügt zur Anbindung der meisten Geschäftsanwendungen. Werden höhere Bandbreitenanforderungen gestellt, lassen sich auch mehrere 10 GBit-Links ohne Probleme bündeln.

Neue Regeln für USV

Wird im Netzwerk VoIP eingesetzt, ist darauf zu achten, dass die Switches im Etagenverteiler über die Ethernet-Schnittstellen "Power over Ethernet" zur Verfügung stellen. Die Stromversorgung der VoIP-Endgeräte über den Etagen-Switch erfordert eine Absicherung gegen Stromausfall für die gesamte VoIP-Installation. Meist sind die USVs jedoch nicht in der Lage, die gesamte VoIP-Installation (bis hin zu den Etagen-Switches) mit Strom zu versorgen. Daher muss der Netzadministrator für die Telekommunikation ein eigenes Notstromkonzept entwickeln, um eine durchgängige Kommunikation (Notruf) auch bei Stromausfall gewährleisten zu können.

Die Überbrückungszeit liefert einen wichtigen Eckpunkt zur Berechnung der USV. Die Erfahrungen im VoIP-Umfeld zeigen, dass bei 70 bis 80 Prozent aller Arbeitsplätze etwa 30 Minuten ausreichen, um Vorgänge ordentlich zu beenden oder letzte Maßnahmen zu treffen, bevor die Kommunikationskanäle nicht mehr zur Verfügung stehen. Die restlichen 20 bis 30 Prozent entfallen auf Kommunikationsgeräte, die mindestens eine Stunde oder länger zur Verfügung stehen müssen. Bei der Dimensionierung einer USV für eine VoIP-Umgebung müssen alle aktiven Komponenten, die ein VoIP-Netz beeinflussen, mit in die Kalkulation einbezogen werden.

Redundanz für Switche

In jedem Netzwerkschrank auf der Etage beziehungsweise im Serverraum laufen mindestens zwei redundante Verbindungen auf. Installieren Sie in diesen Sammelpunkten mehr als einen Switch und binden jeden Switch unabhängig an den Core an, erhöht sich natürlich die Anzahl der notwendigen Verbindungen oder Glasfasern. Es lassen sich natürlich auch diese zusätzlichen Verbindungen einsparen, indem die Etagenanbindung über nur ein Verbindungspaar läuft. Die Anbindung läuft dadurch auf einem so genannten Aggregation-Switch auf. Dieser sorgt anschließend für die Anbindung der anderen Switches im Etagenverteiler.

Unabhängig von der physikalischen Struktur des Netzwerks müssen die Core-Switches auf jede mögliche Weise redundant ausgelegt werden: redundante Netzteile, redundante Verbindungen und redundante Routing-Protokolle. Im Idealfall verfügen die Geräte auch über redundante Controller-Module.

Die Core-Switches sind für das Packet Switching aller Daten innerhalb der Netzinfrastruktur verantwortlich. Aus diesem Grund müssen diese Geräte auf allen Ebenen die notwendigen Redundanzfunktionen bereitstellen. Daher sollte auf der Ebene 3 das HSRP (Hot Standby Routing Protocol) beziehungsweise VRRP (Virtual Routing Redundancy Protocol) für die erhöhte Verfügbarkeit sorgen. Beide Protokollmechanismen sorgen dafür, dass zwei Layer 3-Geräte (Router) wie ein Gerät wirken und gemeinsam eine einzige IP- und MAC-Adresse (als Default Gateway-Adresse) nutzen. Beim Ausfall des primären Routers übernimmt der Backup Router die Weitervermittlung des Datenverkehrs.

Mehr Bandbreite durch Shortest Path Bridging

Die heutigen Netzdesigns werden stark durch die aktuell verfügbaren Netzwerkstandards begrenzt. Bisher werden redundante Netzverbindungen zwar ermöglicht, deren Nutzung durch den Spanning Tree-Mechanismus jedoch rigoros unterbunden. Dies beseitigt Schleifen im Netz und die Eindeutigkeit der Wege im Netzwerk wird garantiert. Drei oder mehr Ethernet-Switches lassen sich dabei auf der logischen Ebene nicht zu einem Ring verknüpfen. Der Spanning Tree-Mechanismus deaktiviert einen Link und unterbricht die Schleife so lange, bis eine der aktiven Verbindungen nicht mehr arbeitet. Eine Verbindungsredundanz zwischen Switches wird zwar ermöglicht, aber ein Teil der theoretisch verfügbaren Bandbreite nicht genutzt.

Daher erfordern moderne Netzwerke zusätzlich Funktionen, die den parallelen Betrieb von Verbindungen im Ethernet ermöglichen. Um dies auch auf Layer 2 zu erreichen, werden gegenwärtig zwei Alternativen spezifiziert: Die IETF Standards Group schlägt dazu TRILL (Transparent Interconnection of Lots of Links) vor, während die IEEE Shortest-Path Bridging (IEEE 802.1aq) untersucht. In beiden Varianten geht es um eine Vernetzung zwischen Switches auf Layer 2 und die Nutzung paralleler Pfade zwischen Knoten. Das gewünschte Ergebnis von Layer 2 Multipathing ist eine höhere Bandbreite bei niedrigeren Latenzzeiten.

TRILL

TRILL wurde im RFC 5556 festgelegt und in Routing Bridges (RBridges) umgesetzt. RBridges terminieren das Spanning Tree-Protokoll und nutzen zur Kommunikation untereinander ein Link State-Protokoll. Über dieses Protokoll propagieren die RBridges die Konnektivität zueinander, so dass jede RBridge alle Verbindungen zu anderen RBridges kennt. Auf Basis dieser Informationen berechnen die RBridges die optimalen Pfade für die Übermittlung von Unicast-Paketen. Darüber hinaus wird ein Verteilbaum errechnet, der die eindeutige Weiterleitung von unbekannten Zieladressen, Broadcasts und Multicasts ermöglicht.

TRILL arbeitet auf Layer 2 und sorgt durch automatische Konfigurationsmechanismen für eine problemlose Integration in bestehende Netze. RBridges arbeiten vollkommen transparent für die höheren Schichten und alle parallelen Verbindungen zwischen RBridges wirken wie ein einziger logischer Link.

IEEE 802.1aq

Der 802.1aq-Standard spezifiziert das Shortest Path Bridging für Unicast- und Multicast-Frames und wandelt die klassischen Ethernet-Strukturen in logische Ethernet-Netzwerke um. 802.1aq arbeitet auf Layer 2 und sorgt durch automatische Konfigurationsmechanismen für eine problemlose Integration in bestehende Netze.

Das Shortest Path Bridging terminiert das Spanning Tree-Protokoll und nutzt stattdessen ein Link State-Protokoll zur Propagierung der Netzwerktopologie und logischen Netzwerk-Mitgliedschaften. Im Edge-Bereich werden die Pakete entweder in MAC-in-MAC (802.1ah) oder in Q-in-Q (802.1ad) Frames gekapselt und über die Netzwerkinfrastruktur über mehrere parallele Netzwerkpfade zu anderen Mitgliedern des logischen Netzwerks transportiert. Dieser Mechanismus unterstützt sowohl Unicasts als auch Multicasts und sorgt für das symmetrische Routing über parallele Verbindungen mit gleichen Kosten.

Neue Dynamik erschwert Fehlersuche

Bei beiden Verfahren wird der Verkehr zwischen den Netzwerkknoten immer über den oder die kürzesten Wege über-

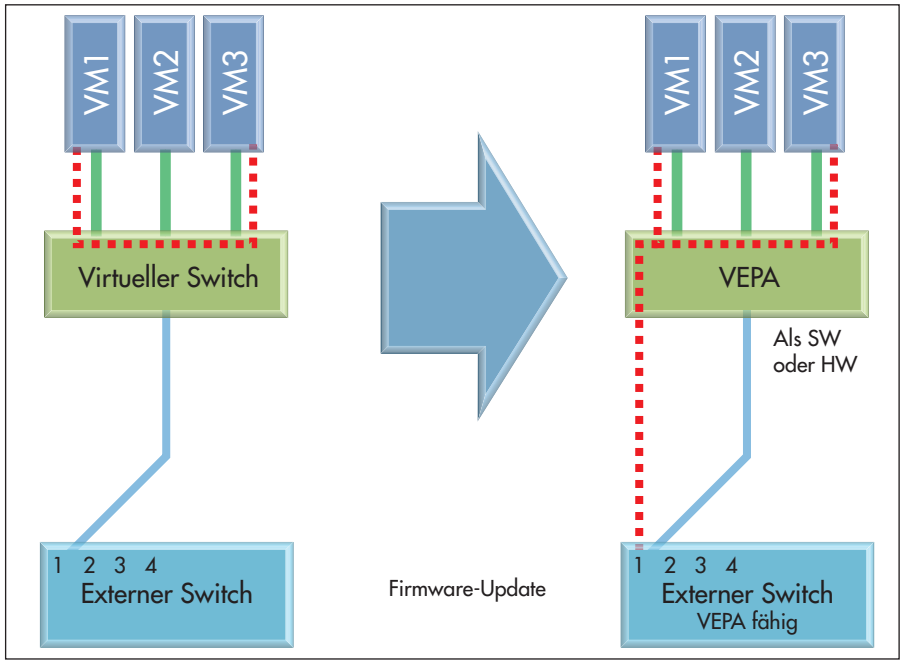


Bild 1: Hairpinning versetzt Switches in die Lage, Datenpakete in beide Richtungen zu senden

mittelt. Die bisher durch den Spanning Tree-Mechanismus brachliegenden Übertragungsressourcen werden genutzt und die Redundanz und Leistungsfähigkeit erhöht. Der Nachteil beider Shortest Path Mechanismen besteht darin, dass das Netz weitaus dynamischer reagiert, als wir es von den bisherigen Standards gewohnt sind. Die Netztopologie passt sich dynamisch an die Ereignisse an und ändert die Netzstrukturen nach Bedarf.

Das erschwert das Verkehrsmanagement und die Fehlersuche. Mit Hilfe von Netzwerk-Taps oder den Span-Ports in den Switches lassen sich jedoch die übermittelten Daten weiterhin mit Hilfe von Netzanalysatoren aufzeichnen. Dafür muss der Netzadministrator nicht wissen, ob sich die Netzwerkpfade dynamisch geändert haben und über welchen Datenpfad die betreffenden Datenflüsse gerade übermittelt werden. TRILL und auch 802.1aq befinden sich noch in der finalen Standardisierung und werden in einigen Produkten bereits als Pre-Standards unterstützt.

Neue Standards für die Virtualisierung

Im Rechenzentrum ist eine Integration der virtuellen Server und der Storage-Ressourcen erforderlich. Die explosionsartige Verbreitung von virtuellen Maschinen in Rechenzentren führt zu erheblichen Managementproblemen an den Schnittstellen zwischen den physischen Servern und den Netzkomponenten (Switches). Die IEEE 802.1Qbg- und 802.1Qbh-Spezifikationen verlagern viele Policies, Sicherheits- und Verwaltungsaufgaben von den virtuellen Switches auf den Network Interface Cards (NIC) und Blade-Servern hin zu den physikalischen Ethernet-Switches.

Die aktuellen Normentwürfe der IEEE führen das Virtual Ethernet Port Aggregation (VEPA) ein. Dabei handelt es sich um eine Erweiterung des physischen und virtuellen Switching zur Reduzierung der Verwaltungskomplexität der vielen im Rechenzentrum eingesetzten Switching-Elemente. Es erleichtert das Management für die Server- und Netzadministratoren und die Anzahl der zu verwaltenden Switching-Elemente und Element-Merkmale (Adresstabellen, Richtlinien für Sicherheits- und Service-Attribute und Konfigurationen) wird deutlich gesenkt.

Der Standard 802.1Qbg definiert das Edge Virtual Bridging: Ein physikalischer Server kann dabei über mehrere virtuelle Server verfügen und den Zugriff auf diese Ressourcen über das angeschlossene Bridged LAN bereitstellen. Fester Bestandteil von VEPA ist der so genannte Inter-VM Hairpinning-Mechanismus (manchmal auch Haarnadelmodus genannt). Bei virtuellen Rechnern müssen unter Umständen die Pakete an einen anderen virtuellen Rechner übermittelt werden. Sind beide virtuellen Rechner über den gleichen physikalischen beziehungsweise logischen Port zu erreichen, filtert der Eingangs-Port des angeschlossenen Switches diese Pakete aus und die Pakete werden nicht übermittelt. Es galt bisher: Ein über einen Switch-Port empfangenes Paket darf nicht mehr über diesen Port in Richtung des Empfängers übertragen werden. Mit Hilfe des Hairpining-Prozesses ist der Switch in der Lage, die betreffenden Pakete anschließend über den Empfangs/Ausgangs-Port zum virtuellen Zielrechner zurückzusenden.

Zusätzlich ist noch eine weitere Policy-Extension notwendig, um externe Switches in einer virtuellen Umgebung zu nutzen. Hier setzt 802.1Qbh an: Dieser Standard ermöglicht Edge Virtual Bridges die Replikation von Paketen über mehrere virtuelle Kanäle hinweg auf eine Gruppe von Remote-Ports. Dadurch lassen sich kaskadierte Ports für ein flexibles Netzdesign einrichten und die Bandbreite für Multicast-, Broadcast- und Unicast-Frames effizient nutzen.

Die durch 802.1Qbh erweiterten Port-Funktionen sorgen dafür, dass die Administratoren bei der Festlegung von Policys, ACLs, Filter, QoS und anderen Parameter den Switch frei festlegen können. So genannte Port-Extender agieren auf den Blade-Racks oder auf einzelnen Blades als Line-Card für den zugeordneten Switch. Dadurch wird das Management eines solchen Switch-Konstrukts erheblich vereinfacht und der externe Switch übernimmt alle Kontrollfunktionen.

VEPA verändert nicht das Ethernet-Paketformat, sondern nur das Weiterlei-

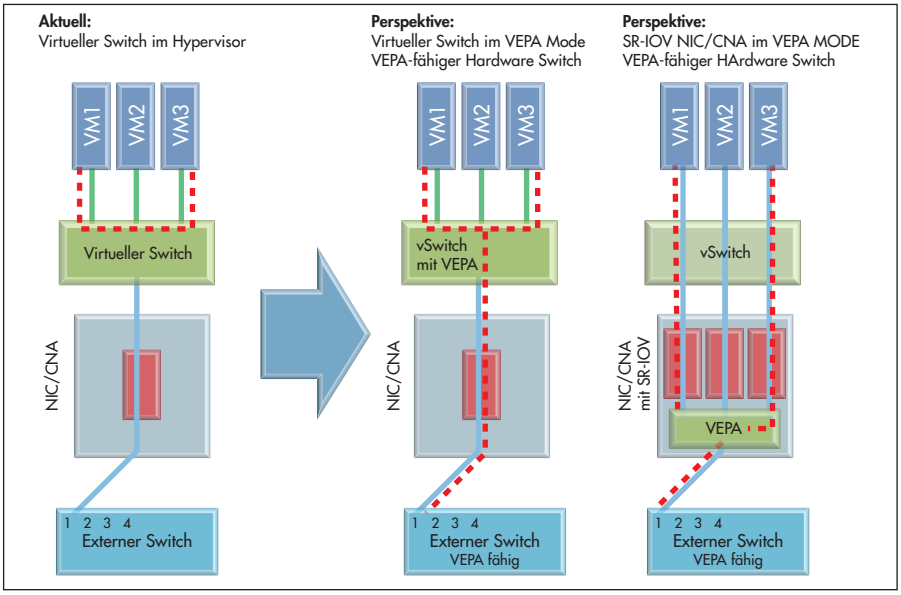


Bild 2: Die Weiterentwicklung von VEPA mit virtuellen Switches im VEPA-Modus

tungsverhalten von Switches. Der große Vorteil des Verfahrens besteht in der internationalen Standardisierung. Die zusätzliche Sicherheit hat keine Performancenachteile, da das gesamte Rechnersystem entlastet wird. Die vorhandene Hardware lässt sich weiter nutzen und Q-in-Q-fähige Switches in der Regel per Firmware-Update auf die VEPA-Fähigkeiten und den Hairpin-Modus hochrüsten. Außerdem lässt sich VEPA sowohl als Software (virtueller Switch) als auch als Hardware implementieren.

VEPA bietet auch eine klare Perspektive für weitere Entwicklungen, inklusive der Nutzung der Single Root I/O Virtualization (SR-IOV) Funktionalität in NICs und CNAs. Erst die SR-IOV ermöglicht es, einzelne virtuelle Maschinen direkt an einen virtuellen Netzwerk-Port zu mappen, der hardwareseitig durch einen SR-IOV-fähigen NIC oder CNA bereitgestellt wird. Damit wird der Hypervisor noch weitergehend von Switching-Aufgaben entlastet. Ein SR-IOV-fähiger NIC wird bis zu 128 dieser virtuellen Funktionen bereitstellen können.

Mehr Geschwindigkeit im Storage-Netzwerk

Nachdem der Netzwerkkern aufgebaut ist, folgt der Storage. Ein funktionierendes Storage-Netzwerk ist Voraussetzung für die Virtualisierung der Server. Inzwischen haben sich auch im Storage-Bereich unterschiedliche Technologien etabliert und es konkurrieren der Fibre Channel- und der iSCSI-Standard um die Gunst der Anwender. Fibre Channel liefert niedrigere Verzögerungszeiten als iSCSI. Fibre Channel erfordert spezielle FC-Switches und kostspielige FC-HBAs (Host Based Adapter) in jedem Server. iSCSI lässt sich dagegen auf standardmäßigen GBit-Ethernet-Komponenten realisieren.

Die Installation des Fibre Channels geschieht unabhängig vom Rest des Unternehmensnetzwerks und verfügt nur über eine Netzmanagementanbindung zum Hauptnetz. Dagegen werden für die Anbindung der iSCSI-Ressourcen die gleichen Ethernet-Switches des Unternehmensnetzes genutzt. Bei der parallelen Nutzung des Unternehmensnetzes als iSCSI-Speichernetzwerk sollte bei der Auswahl der Switches darauf geachtet werden, dass die Switches auch die Übermittlung von iSCSI-Datenverkehr garantieren. Bei einigen Switches sinkt die Performance bei der Übermittlung von iSCSI-Datenverkehr drastisch. Die Ursache liegt in der internen Struktur der Switches.

Fibre Channel

Fibre Channel basiert in der Regel auf dedizierten HBAs (Host Bus Adaptern) und Switches und unterstützt folgende Netzgeschwindigkeiten: 1, 2, 4, 8, 10 und 20 GBit/s. Da die 10 und 20 GBit/s-Geräte einen anderen Frame-Codierung Mechanismus verwenden und hauptsächlich im Bereich der Interswitch Links eingesetzt werden, wurde auf die Rückwärtskompatibilität verzichtet. Das Fibre Channel Protocol (FCP) wurde für die Übermittlung von Storage-Daten optimiert. Dies resultiert in einen geringeren Overhead und somit in geringen Verzögerungen. Das FCP stellt darüber hinaus einen integrierten Flusssteuerungsmechanismus zur Verfügung.

iSCSI

iSCSI baut auf dem TCP/IP-Protokoll auf und lässt sich auf bereits vorhandenen Netzkomponenten realisieren. Durch den zusätzlichen Overhead der SCSI-Befehle und der Kapselung im TCP/IP-Netzwerkprotokoll wird jedoch eine zusätzliche Verzögerung hervorgerufen. iSCSI belastet die CPU der Server stärker: Obwohl es Hardware-basierte iSCSI-HBAs gibt, nutzen die meisten iSCSI-Implementierungen diese nicht und lassen die Server-Prozessoren die Paketverarbeitung durchführen.

In Sachen Interface-Geschwindigkeit steht iSCSI Fibre Channel in nichts nach. Es können mehrere 1 GBit/s oder 10 GBit/s Ethernet-Links genutzt werden. Darüber hinaus profitiert iSCSI von der TCP/IP-Unterstützung, denn dadurch können die Storage-Daten über bestehende WAN-Verbindungen übermittelt werden.

Fiber Channel over IP

Fiber Channel over Internet Protocol (FCoIP) stellt eine Nischenlösung dar. Dabei werden die FCP Frames auf Basis von TCP/IP-Paketen übermittelt. Der Vorteil dieser Lösung besteht darin, dass das vorhandene TCP/IP-Netzwerk die FC-Daten übermittelt. Daher wird diese Lösung auch hauptsächlich zur Anbindung mehrerer Standorte für die SAN-to-SAN-Replikation und für Backup-Anwendungen über lange Strecken genutzt.

Fibre Channel over Ethernet

Der Standard Fibre Channel over Ethernet (FCoE) stellt das neueste Storage-Networking-Protokoll dar. Der FCoE-Standard nutzt die vorhandenen Ethernet-Netzwerke zur Anbindung der Storage-Komponenten. Im Gegensatz zum iSCSI werden die Daten nicht auf Basis von TCP/IP, sondern mit Hilfe eines eigenen Protokolls übermittelt. Auf der Server-Seite unterstützen die FCoE-Implementierungen 10 GBit/s schnelle Ethernet FCoE Converged Network Adapter (CNAs). Diese Geräte agieren sowohl als reiner Netzwerkadapter als auch als FCoE-HBA und entlasten die Server-CPU von unnötiger Protokollverarbeitung.

Fazit

Die neuen Anforderungen der Applikationen und der virtualisierten Server-Landschaften sorgen für dynamische Veränderungen der Netzstrukturen. Die hierfür notwendigen Standards stehen bereits in den Startlöchern oder wurden bereits in den Netzwerkkomponenten implementiert. Dadurch wird das Netzdesign nicht einfacher. Eine sorgfältige Planung garantiert, dass sich das Netzwerk dynamisch an die geänderten Anforderungen im Server- und im Storage-Bereich anpasst. *(jp)*

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.

Bei der **Migration von Windows Server 2003 auf Server 2008 R2** lassen sich **Server-gespeicherte Benutzerprofile** ja leider nicht mehr direkt weiterverwenden. Trotzdem würde mich interessieren, ob es Sinn macht, die anwendungsbezogenen Einstellungen irgendwie **manuell zu übernehmen** oder ob es hier zu viele Fallstricke gibt. Können Sie eine ideale Vorgehensweise oder geeignete Hilfsmittel empfehlen?

Wie Sie richtig bemerken, verwendet Microsoft in seinen Betriebssystemen ab Windows Vista ein anderes Format für Roaming Profiles. Bereits an dieser Stelle tun sich viele Hürden auf, etwa dadurch, dass V1-Profile (bis XP) sprachabhängig sind, V2-Profile (ab Vista) jedoch nur in englischer Sprache vorhanden sind – eine lokalisierte Anzeige erfolgt durch Konfigurationsdateien. Das ist jedoch nicht die einzige Schwierigkeit, schließlich findet beim Wechsel von Server 2003 auf 2008 R2 auch ein Umstieg von 32 Bit auf 64 Bit statt. Gerade die Speicherung der anwendungsbezogenen Einstellungen jedoch erfolgt teilweise in der Registry des Benutzers (HKCU). Wenn nun aber eine 32 Bit-Applikation im Bereich HKCU den Pfad zum eigenen Installationsverzeichnis speichert (zum Beispiel "C:\Programme\App1" oder "C:\Program Files\App1"), wird dieser auf einer x64 Plattform nicht gefunden. Der Grund dafür ist, dass der Pfad "C:\Program Files" auf einer x64-Plattform für 64 Bit-Programme vorbehalten ist (beziehungsweise die deutsche Variante "C:\Programme" nur als so genannte Verzeichnisverbindung, Junction, existiert). 32 Bit-Programme installiert das System gewöhnlich nach "C:\Program Files (x86)". Das Betriebssystem setzt zwar diesen Pfad für die 32 Bit-Applikationen transparent um, aber die hartkodierten Registry-Einträge werden dabei trotzdem falsch interpretiert. Das bedeutet, dass Sie die Einstellungen in HKCU bei einer Profilmigration für die Zielplattform auf die tatsächlich vorhandenen Verzeichnisse manuell umsetzen müssten. Alles in allem keine leichte Aufgabe, die Sie in größeren Umgebungen eigentlich nur durch Skripte lösen können. Sollte Ihnen zur Erstellung derartiger Helfer die Zeit fehlen, können Sie auf vorhandene Werkzeuge zurückgreifen – Quest bietet mit dem Migration Manager ein eher allgemeines Migrations-Tool an, die Firma sepago hat sich mit dem Profile Migrator auf die Umsetzung von Benutzerprofilen in nur wenigen Schritten spezialisiert. Mehr dazu finden Sie in unserem Test ab Seite 26. *(ln)*

Auch **Windows 7** verfügt über das Kontextmenü des Explorers über die **Funktion "Senden an"**, mit der sich Dateien per Mail, Fax oder Bluetooth direkt an einen Empfänger nach Wahl verschicken lassen. In älteren Windows-Versionen war es ja möglich, diesen **Eintrag um eigene Ordner zu ergänzen**, um beispielsweise Dokumente schnell in ein häufig genutztes Verzeichnis verschieben zu können. Lässt sich das Kontextmenü von Windows 7 ebenso um diese Funktion erweitern?

Selbstverständlich lässt sich das "Senden an"-Kontextmenü der jüngsten Windows-Variante um eigene Einträge ausbauen. Öffnen Sie dazu den Windows Explorer und geben Sie in der Adressleiste *shell:sendto* ein. Durch diesen Befehl kommen Sie direkt zu dem Verzeichnis, in dem alle möglichen Zielorte des "Send to"-Befehls hinterlegt sind. Hier legen Sie nun einfach eine Verknüpfung zu einem Ordner Ihrer Wahl an und schon erscheint dieses Ziel wie gewünscht nach einem Klick mit der rechten Maustaste unter der Option "Senden an". *(ln)*

Wenn ich im **Helpdesk** tätig bin, ist es manchmal recht schwierig, die Probleme von Anwendern zu lösen, die **temporär über keine Internetverbindung** verfügen, so dass ein Remote-Zugriff nicht möglich ist. Gerade die Systemumstände und die Aktivitäten des Users lassen sich in einem

Telefongespräch meist nur sehr umständlich herausfinden. Nun habe ich gehört, dass **Windows 7** über ein **eingebautes Tool zur Fehleraufzeichnung** verfügt. Wo finde ich das und wie funktioniert das Werkzeug?

Die Software, von der Sie sprechen, ist der "Problem Steps Recorder", der als Bordmittel in Windows 7 zu finden ist. Dieses Aufzeichnungsgerät kann der Anwender ganz einfach über die Eingabe von *psr* im Instant Search-Feld von Windows 7 starten. Der Problemrekorder nimmt dann alle Eingaben des Nutzers samt Bildschirmfotos der einzelnen Schritte auf. Weiterhin kann der Anwender auf Wunsch zusätzliche Kommentare hinterlegen. Nach Abschluss der Aufzeichnung wandelt das Werkzeug die Aufnahme in das Dateiformat MHTML um, so dass sich die Analyse einfach per Mail verschicken und systemunabhängig untersuchen lässt. Gerade was die Nachvollziehbarkeit immer wieder auftretender Probleme betrifft, kann das Programm eine sehr große Hilfe sein. *(ln)*

In den **Vorgängerversionen von Outlook 2010** konnte man sich über das **Kontextmenü die Eigenschaften einer E-Mail** und somit auch den **Header** anzeigen lassen. Bei der aktuellen Version finde ich diese Funktion aber nicht. Gibt es diese Option noch und wenn ja, wo kann ich sie aktivieren?

Um sich schnell den Header einer Nachricht anzeigen zu lassen, wählen Sie in Outlook oben links neben dem Office-Symbol das Dropdown-Menü aus und klicken dort auf "Weitere Befehle". Hier lässt sich die Symbolleiste für den Schnellzugriff anpassen. Bei den Optionen gehen Sie nun mit der Maus auf den Punkt "Befehle nicht im Menüband", um dann in der folgenden Liste die "Nachrichtenoptionen" hinzuzufügen. Ist dies getan, schließen Sie das Konfigurations-Menü wieder. Wenn Sie nun eine neue Mail markieren, kommen Sie über den neuen Link "Nachrichtenoptionen" wieder zu den Eigenschaften. Dort finden Sie im unteren Bereich dann zum Beispiel die Header-Informationen. *(sepago/ln)*

Sobald ein Nutzer in **Outlook 2007** eine **neue E-Mail** erstellt und damit beginnt, eine Adresse einzutippen, **schlägt der Mailclient bestimmte E-Mailadressen** vor. Da diese Mini-Datenbank ja anscheinend nichts mit den hinterlegten Kontakten zu tun hat, würde mich einmal interessieren, wo Outlook die entsprechenden Informationen ablegt und ob sich diese, ähnlich wie ein lokales PST-File, kopieren und somit sichern lassen.

Bis Outlook 2007 legt der Mailclient im "Verzeichnis Dokumente und Einstellungen \ {Benutzer} \ Anwendungsdaten \ Microsoft \ Outlook" eine Datei mit der Endung *.NK2 an. In dieser sind vom Nutzer häufig verwendete Mailadressen hinterlegt. Bei der Migration eines Outlook-Profils können Sie diese Datei einfach kopieren und auf dem neuen Rechner im gleichen Verzeichnis ablegen – die Funktion zur automatischen Vervollständigung von Name und E-Mailadresse funktioniert dann auch auf dem neuen PC. Zudem gibt es eine Reihe von Tools – etwa das kostenlose NK2View von Nirsoft –, die diese Datei auslesen können und einen Export der darin hinterlegten Informationen erlauben. Die NK2-Dateien gibt es in Outlook 2010 allerdings nicht mehr. Hier hat Microsoft die Daten zur Autovervollständigung im PST-File versteckt beziehungsweise legt sie im jeweiligen Exchange-Ordner ab – die Funktionen wandern so bei einer Migration automatisch mit dem Benutzer mit. In der Programmoberfläche haben die Redmonder die Funktionalität in den Ordner "Vorgeschlagene Kontakte" gepackt, den Sie in der Kontakte-Verwaltung finden. Outlook 2010 kann eine NK2-Datei von Outlook 2003 und Outlook 2007 aber ohne Probleme übernehmen, wenn Sie diese im oben beschriebenen Verzeichnis ablegen. Berücksichtigen Sie jedoch, dass der Ordner "Anwendungsdaten" standardmäßig versteckt ist und Sie die Ansicht erst entsprechend modifizieren müssen, um ihn zu sehen. *(ln)*

Linux

Ich möchte gerne zu Sicherungszwecken ein **Abbild meiner Festplatte auf einen entfernten Rechner** übertragen. Wie kann ich dies am einfachsten und schnellsten anstellen?

Mit Hilfe des sehr mächtigen Tools "netcat" (nc) lassen sich beliebige TCP- und UDP-Verbindungen zwischen einzelnen Rechnern aufbauen – deswegen wird es nicht selten das Schweizer-Taschenmesser im Netzwerkbereich genannt. Auf dem Rechner (Rechner A), auf den Sie das Festplatten-Image übertragen wollen, rufen Sie zunächst netcat im Listening-Mode auf einem beliebigen Port auf. Mittels einer Pipe schreibt die Kopierfunktion "dd" dann die empfangenen Daten in die angegebene Datei:

```
# nc -l 1234 | dd of=/tmp/sda.img
```

Auf dem Rechner, von dem Sie das Festplatten-Image erstellen und übertragen möchten, machen Sie ebenfalls mittels dd eine neue TCP-Verbindung zum entfernten Port 1234 auf. Die mittels dd erzeugten Sicherungsdaten senden Sie dann über diese TCP-Verbindung an den entfernten Port 1234:

```
# dd if=/dev/sda | nc {Rechner A}
  1234
```

Zu beachten ist hierbei, dass die Daten im Klartext durchs Netzwerk wandern. Sollte auf dem entfernten Rechner der SSH-Dienst laufen, so lösen Sie das Problem einfach mittels eines einfachen Kommandos auf dem sendenden Rechner:

```
# dd if=/dev/sda | ssh {Rechner A}
  dd of=/tmp/sda.img
```

(ln)

CITRIX

Wir verwenden im Unternehmen **Citrix XenServer**. Soweit ich weiß, geht dieser standardmäßig davon aus, dass eine **virtuelle CPU** einem Kern der virtuellen Maschine entspricht. Einige virtuelle Maschinen erlauben allerdings eine **höhere Zuweisung von Kernen**. Wie funktioniert dies genau beziehungsweise wie kann ich einer virtuellen Maschine eine festgelegte Anzahl an Kernen zuweisen?

Die von Ihnen gewünschte Funktionalität versteckt sich im Cores-Per-Socket-Parameter für virtuelle Maschinen. Vorweg sei jedoch gesagt, dass diese Option nur in der Advanced, Enterprise und Platinum-Edition von XenServer, nicht jedoch in der kostenlosen Version existiert. Finden Sie zunächst den Universally Unique Identifier (UUID) der virtuellen Maschine heraus, für die Sie den Parameter setzen wollen:

```
xe vm-list name-label={Name der VM}
```

Setzen Sie im Anschluss daran den Cores-per-Socket-Parameter:

```
xe vm-param-set platform:cores-per-
  socket=X uuid={UUID}
```

Anstelle von "X" fügen Sie "2" bei Dual Core- oder "4" bei Quad Core-Prozessoren ein. Um zum Beispiel eine CPU mit vier Kernen zu definieren, lautet das Kommando

```
xe vm-param-set platform:cores-per-
  socket=4 uuid={VM UUID}
```

Als Nächstes setzen Sie nun den Startup-Parameter der virtuellen CPU auf die gleiche Anzahl virtueller CPUs (Zahl der Kerne), die der virtuellen Maschine zugewiesen werden und setzen Sie den VCPU-Max-Parameter auf die Anzahl der insgesamt vorhandenen Kerne:

```
xe vm-param-set VCPUs-at-
  startup={Anzahl der VCPUs}
  uuid={UUID}
xe vm-param-set VCPUs-max={Maximale
  Anzahl der Prozessorkerne}
```

Für ein Dual-Quad-Core-System ist hier zum Beispiel "8" einzutragen. Die beim Start angezeigte Anzahl an CPUs entspricht der Zahl an Kernen, die der virtuellen Maschine zugesprochen werden. Wenn Ihr XenServer mit Dual Quad Core-CPUs ausgestattet ist und Sie *Cores-per-Socket=4* und *VCPUs-at-startup=8* eingestellt haben, sehen Sie acht CPUs im Performance-Reiter des Task Managers und zwei Prozessoren in den Systemeinstellungen der virtuellen Maschine. In diesem Fall nutzt die virtuelle Maschine alle acht Kerne der beiden Prozessoren. Auf ähnliche Weise gilt: Bei der Einstellung *VCPUs-at-startup=4* sehen Sie vier CPUs im Performance-Reiter des Task Managers, aber nur einen Prozessor bei den Systemeinstellungen. In diesem Fall nutzt die virtuelle Maschine nur vier Kerne und nur einen von zwei Prozessoren. Ist allerdings die Zahl bei *VCPUs-at-startup* größer als vier, kommt der zweite Prozessor zum Einsatz und auch in den Systemeinstellungen sind beide Prozessoren zu sehen. Die Beispiele zeigen, dass die Anzahl der Prozessoren, die die virtuelle Maschine nutzen kann, von der Anzahl der Kerne abhängt, die ihr zugewiesen wurden. *(Citrix/ln)*

Tools

Ein wichtiger Schritt auf dem Weg zu einer virtualisierten Infrastruktur ist das **Konvertieren physikalischer Maschinen zu virtualisierten Servern (P2V)**. Die eigentliche Konvertierung ist dabei in der Regel problemlos und lässt sich mit einer ganze Reihe von Tools durchführen. Doch sollte der Administrator auch die Vor- und Nachbereitung dieses Prozesses im Auge haben, wie es ihm ein kostenloses Tool von Quest erlaubt.

Das freie **vConverter SC** vereinfacht und beschleunigt P2V- und V2V-Konvertierungsprojekte, indem es viele Vor- und Nach-Konvertierungsaufgaben automatisiert, einschließlich der Möglichkeit des Konfigurierens von Source-Services und des Ausführens benutzerdefinierter Skripte auf der Ziel-VM. Mit einer vorgeplanten Umstellung ermöglicht das Werkzeug P2V-Konvertierungen, bei denen der Konvertierungsprozess getestet und dann Source- und Zielsysteme vor dem finalen Übergang synchronisiert werden, während das Source-System kontinuierlich weiterläuft. Zudem gewährleistet das Tool Datenkonsistenz in Source- und Zielsystemen durch die Verwendung einer Cold Clone Boot-CD zur Unterstützung transaktionaler Systeme wie Datenbank und E-Mailserver. Darüber hinaus gewährt vConverter SC der virtuellen Maschine direkten Zugriff auf ein LUN auf dem physischen Speichersystem. So lässt sich die zugrundeliegende SAN-Software für Schnappschüsse und Datenreplikation sowie zur Verbesserung von I/O nutzen. *(jp)*

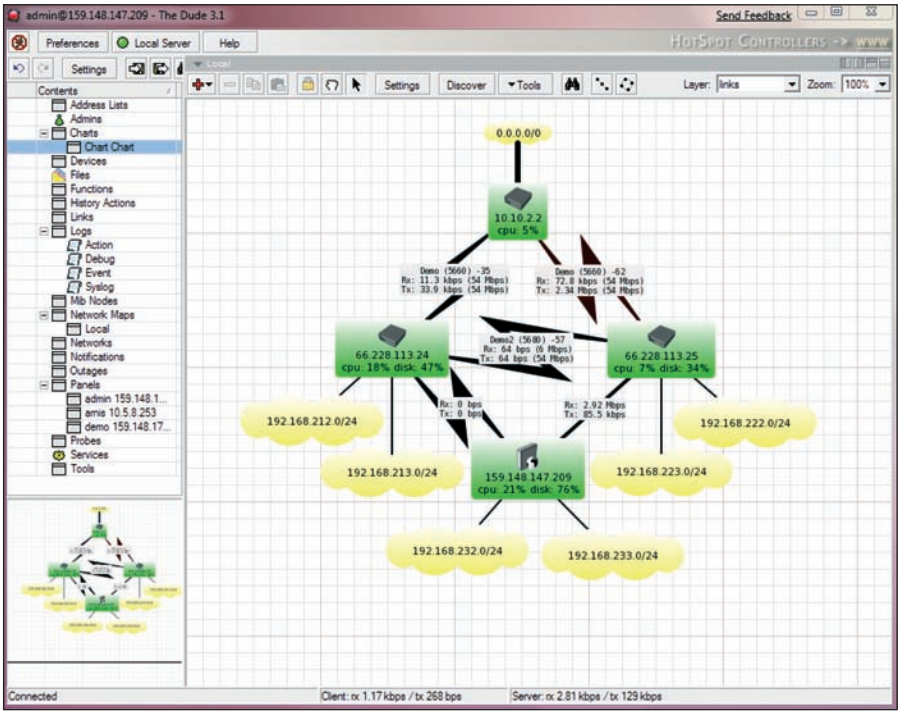
Quelle: http://ger.vizioncore.com/free/vconverter/features

Viele Systems-Management-Systeme überwachen Windows und die darauf installierten Dienste. Das **Management der**

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



The Dude schafft schnell Übersichtlichkeit im Netzwerk

Netzwerke, also der Switches, Router et cetera, die letztlich die Lebensadern der IT darstellen, erfolgt häufig nur in größeren Firmen. Das liegt eventuell daran, dass die Administratoren nicht die Zeit haben, sich intensiv mit SNMP auseinanderzusetzen, ist aber auch hohen Kosten für kommerzielle Lösungen geschuldet. Bei großen Firmen stellt sich die Frage weniger, da hier ein Netzwerkmanagement einfach dazu gehört. Kleinere Firmen scheuen den finanziellen Aufwand, der aber keiner sein muss, wie das folgende Werkzeug beweist.

Der kostenlose Netzwerkmonitor **The Dude** scannt ein Netzwerk automatisch und stellt alle Geräte als Symbole dar. Durch Verschieben der Elemente und Hinterlegen mit Plänen oder Karten entsteht eine grafische Dokumentation des Netzwerks. The Dude prüft laufend den Status der einmal gefundenen Server und stellt ihn den IT-Verantwortlichen übersichtlich dar. Soweit möglich werden per SNMP weitere Daten ausgelesen und einige Dienste ermittelt. Das Tool läuft auf Windows, kommt mit einer Installationsroutine und ist komplett per GUI administrierbar. Nach der Installation nimmt das Tool erst einmal alle Komponenten auf, die es im Netzwerk findet, ein klassisches Discovery also. Dabei ist es auch möglich, mehrere IP-Netzwerke anzugeben. Sind Router vorhanden, lässt sich die Funktion "recursive Hops" aktivieren. Das Layout der Karte, die das Werkzeug erstellt, ist auf IP-Netze und Router ausgelegt – The Dude erkennt nicht, an welchem Port welches Endgerät hängt. Aber selbst in größeren Netzwerken lässt sich so schnell ein Überblick gewinnen. Das Programm ist schnell auf einem PC installiert und nach sehr kurzer Zeit ist ein Netzwerk erfasst. Allerdings ist zumindest auf den Routern ein Lesezugriff per SNMP erforderlich. Details zu den Geräten liefert das Werkzeug, wenn diese selbst per SNMP erreichbar sind. *(jp)*

Quelle: www.mikrotik.com/thedude.php

Wer in der IT nach **Netzwerk- oder Systemmanagement mit Open Source-Software** fragt, erhält als Antwort typischerweise "Nagios". Das ist nicht verwunderlich, schließlich bietet Nagios dem Anwender viele Freiheiten und ist bereits in einer großen Anzahl von Installationen in Unternehmen unterschiedlicher Größe verbreitet. Aber es gibt noch eine Vielzahl weiterer Ansätze und Lösungen, um Netzwerke zu managen – vor allem wenn es um große Netze geht. Die Aufgabe, ein-, zwei- oder mehrere hundert Knoten zu managen (egal ob Netzwerkhardware oder Server), verlangt nach Automatisierung und der Möglichkeit, Daten über Performance, Status und Verfügbarkeit aus einer einzigen Konfigurationsbasis zu ermitteln.

Die kostenlose Management Suite "OpenNMS" nutzt wie The Dude SNMP zur Ermittlung der Leistung der Systeme und zur Erkennung von Ereignissen in den Systemen. Als Empfänger von SNMP-Nachrichten kann OpenNMS anhand der erhaltenen Informationen entscheiden, ob eine Eskalation notwendig ist oder nicht. Eine Integration mit Lösungen zum Konfigurationsmanagement verlangt nach einem datenbankgestütztem System. Außerdem ist in professionellen Umgebungen die Antwort auf die Frage entscheidend, wer über Probleme im Netz wann und wie informiert wird. All das bringt OpenNMS von Haus aus mit. Die komplett auf Java basierende Lösung lässt sich unabhängig vom Betriebssystem einsetzen und bietet eine stabile Plattform zum Management großer Netzwerke. Das Werkzeug stellt ein plattformübergreifendes Verfügbarkeits-, Performance- und Transaktions-Monitoring bereit, mit dem sich kleine als auch große IT-Infrastrukturen überwachen lassen. OpenNMS sammelt automatisch, ohne dass ein manueller Eingriff notwendig wäre, Daten von allen SNMP-basierten Komponenten und sammelt diese zentral in einer Datenbank. Hieraus können IT-Verantwortliche grafische Performance-Reports generieren. OpenNMS ist auf jeden Fall einen Blick wert, wenn Bedarf nach einem derartigen Werkzeug besteht. *(jp)*

Quelle: www.opennms.org

Neue WLAN-Technologien

Besser funken

von Christian Sauer

Viele kleine bis mittlere Unternehmen vertrauen noch nicht darauf, dass Wi-Fi die Art von Netzabdeckung und Zuverlässigkeit bieten kann, die für die Unterstützung verzögerungsanfälliger Anwendungen wie Sprach- und Multimediafunktionen erforderlich ist. Die meisten WLAN-Systeme ignorieren Störungen im Funkspektrum und bieten nicht die nötige Zuverlässigkeit, Reichweite und Leistung. Netzwerk- und IT-Administratoren haben deshalb weiterhin Schwierigkeiten, Benutzer in das Netzwerk zu bringen und die Verbindung aufrecht zu halten. Dieser Beitrag stellt neue Technologien vor, die diese Probleme beheben können und zudem kostengünstig sind.

Die zwei größten Wi-Fi-Probleme sind ungenügende Signalreichweite und unbeständige Leistung – und beide werden durch Funkstörungen verursacht. Funkstörungen können von nahezu jedem Gerät erzeugt werden, das elektromagnetische Signale abgibt: von kabellosen Telefonen über Bluetooth-Headsets bis hin zu Mikrowellen und sogar intelligenten Stromzählern. Was die meisten Unternehmen nicht realisieren, ist die Tatsache, dass die größte Wi-Fi-Störquelle das eigene WLAN-Netzwerk ist. Da IEEE 802.11n ein geteiltes Medium ist, das nicht lizenzierte Frequenzen (Spektrum) im 2,4 GHz- und 5 GHz-Bereich verwendet, kann jede Störung, jedes Hindernis oder jede Änderung an der Umgebung Probleme für alle Benutzer verursachen.

Funkstörungen führen zu Paketverlusten, die eine erneute Übertragung von Daten erfordern. Das verlangsamt den Durchsatz für die Benutzer, die auf einen bestimmten Wi-Fi-Access-Point (AP) zugreifen. Da Funkstörungen unregelmäßig sind und sich ständig ändern, müssen sich APs an Änderungen in der Umgebung anpassen können, indem sie erkennen, wo diese auftreten, und Wi-Fi-Übertragungen dann automatisch über saubere Pfade lenken. Aber dafür müssten die APs jederzeit wissen, was im Spektrum vor sich geht.

Herkömmliche 802.11-Wi-Fi-Systeme verringern bei Funkstörungen in der Regel die Datenrate, erhöhen die Übertragungsleistung und/oder wechseln zu einem anderen Funkkanal. Leider sind Leistungs- und Kanalanpassungen aufgrund von Vorschriften und Umgebungseinschränkungen nicht immer möglich, und eine geringere Datenrate verringert den Durchsatz und verstärkt Störungen für benachbarte Netzwerke. Deshalb können herkömmliche APs nicht mit diesen Änderungen umgehen und sind höchst ineffizient bei der Bereitstellung von Wi-Fi-Signalen an Clients. Die neue IEEE 802.11n-Technologie verstärkt dieses Problem durch den Einsatz vieler Rundstrahlantennen, die mehrere Wi-Fi-Datenströme gleichzeitig übertragen, um einen höheren Durchsatz zu erzielen.

Übliche Ansätze für die Lösung von Wi-Fi-Funkstörungen

Wie bereits kurz erwähnt, sind die folgenden drei Ansätze für die Lösung von Funkstörungen üblich:

- Verringerung der physischen Datenrate,
- Reduzierung der Übertragungsleistung des betroffenen Access Points oder
- ein Wechsel der Kanalzuordnung des Access Points.

Jeder dieser Ansätze ist in gewisser Hinsicht nützlich, aber keiner geht das grundlegende Problem an, direkt auf die Funkstörungen zu reagieren. Die meisten Wi-Fi-Access Points auf dem heutigen Markt verwenden Rundstrahl-Dipolantennen. Diese Antennen senden und empfangen Übertragungen gleichmäßig in beziehungsweise aus allen Richtungen. Da die Antennen in jeder Situation stets dasselbe übertragen und empfangen, haben sie bei einer Funkstörung nur eine einzige Reaktionsmöglichkeit. Sie müssen die physische Datenrate senken, bis die Paketverluste ein annehmbares Niveau erreichen.

Aber das Verringern der Datenrate eines APs kann die gewünschte Wirkung tatsächlich umkehren. Pakete sind jetzt länger unterwegs, wodurch die Wahrscheinlichkeit von Paketverlusten steigt, weil ihr Empfang länger dauert. Damit sind die Pakete wiederum anfälliger für zwischenzeitliche Funkstörungen. Diese Vorgehensweise ist äußerst ineffizient und führt

dazu, dass alle Benutzer, die diesen AP teilen, eine schlechtere Leistung erhalten.

Eine andere gängige Wi-Fi-Designmethode ist die Reduzierung der Übertragungsleistung eines AP, um die begrenzte Anzahl von Kanälen besser nutzen zu können. Das reduziert die Anzahl der Geräte, die einen AP gemeinsam benutzen, so dass sich die Leistung verbessern kann. Aber eine verringerte Übertragungsleistung kann auch die von den Clients empfangene Signalstärke reduzieren. Dies führt zu einer geringeren Datenrate und kleineren Wi-Fi-Zellen und damit möglicherweise zu Lücken in der Netzabdeckung. Diese Lücken müssen wiederum mit zusätzlichen Access Points geschlossen werden. Mehr APs bedeuten aber mehr Funkstörungen.

Kanalwechsel ziehen neue Probleme nach sich

Die meisten WLAN-Anbieter versuchen die Kunden davon zu überzeugen, dass der beste Ansatz für den Umgang mit Wi-Fi-Funkstörungen ein Kanalwechsel ist. Dabei wird automatisch ein anderer oder "sauberer" Kanal für den Access-Point ausgewählt, wenn die Funkstörungen stärker werden. Ein Kanalwechsel ist durchaus eine sinnvolle Methode, um gegen ständige Störungen in einer bestimmten Frequenz vorzugehen, aber häufig treten solche Störungen in unterschiedlichem Maße und unregelmäßig auf. Aufgrund der begrenzt zur Verfügung stehenden Kanäle verursacht dieses Vorgehen oft mehr Probleme als es löst. Innerhalb der 2,4 GHz-Frequenz, dem meist genutzten Wi-Fi-Band, stehen nur drei unabhängige Kanäle zur Verfügung. Selbst das 5 GHz-Band bietet nur vier sich nicht überlappende 40 MHz-weite Kanäle, wenn die Dynamic Frequency Selection (DFS) eliminiert wurde. Dies ist ein Mechanismus, der es nicht lizenzierten Geräten erlaubt, das Spektrum mit vorhandenen Radarsystemen zu verwenden.

Damit ein AP Kanäle wechseln kann, müssen die verbundenen Clients die Verbindung unterbrechen und dann erneut herstellen. Dies bedeutet, dass Sprach- und Videoanwendungen unterbrochen werden. Das Wechseln von Kanälen verursacht einen Dominoeffekt, da benachbarte APs ebenfalls ihre Kanäle wechseln, um Co-Channel-Interferenzen zu vermeiden. Eine Co-Channel-Interferenz wird verursacht, wenn Geräte einander stören, weil sie für die Übertragung und den Empfang von Wi-Fi-Signalen denselben Kanal oder dieselbe Funkfrequenz verwenden. Um Co-Channel-Interferenzen zu minimieren, versuchen Netzwerkmanager, eine Architektur für ihre Netzwerke und das begrenzte verfügbare Spektrum aufzubauen, in der sie APs weit genug auseinander platzieren können, damit diese einander nicht hören oder stören. Aber Wi-Fi-Signale lassen sich nicht stoppen und gehen über diese künstlichen Grenzen hinweg. Ein Kanalwechsel zieht außerdem nicht in Betracht, was das Beste für den Client ist. Bei diesem Ansatz werden Funkstörungen aus dem Blickwinkel des APs gesehen. Aber der Client profitiert nicht wirklich von einem Wechsel zu einem saubereren Kanal.

Gesucht: Stärkere Signale und weniger Funkstörungen

Eine typische Messmethode für die Vorhersage der Leistung von Wi-Fi-Systemen ist das Signal-Rausch-Verhältnis (Signal-to-Noise Ratio oder kurz SNR). Mit SNR wird der Unterschied zwischen der Stärke des Empfangssignals und der Stärke des Rauschens verglichen. Normalerweise führt ein höheres Signal-Rausch-Verhältnis zu weniger Bitfehlern und einem höheren Durchsatz. Aber wenn Funkstörungen auftreten, müssen sich Administratoren noch um einen anderen Wert kümmern: das Verhältnis der Signalleistung zur Störleistung (Signal-to-Interference plus Noise Ratio, SINR).

Mit SINR wird der Unterschied zwischen der Signalstärke und der Störstärke gemessen. Aufgrund der negativen Auswirkung von Funkstörungen auf den Benutzerdurchsatz ist der SINR-Wert ein wesentlich besserer Indikator für die Art von Leistung, die von einem Wi-Fi-System erwartet werden kann. Ein höherer SINR-Wert bedeutet höhere Datenraten und mehr Kapazität im Spektrum. Für einen höheren SINR-Wert müssen Wi-Fi-Systeme entweder die Signalstärke erhöhen oder die Störstärke verringern. Das Problem ist, dass die Signalstärke bei herkömmlichen Wi-Fi-Systemen nur erhöht werden kann, indem mehr Leistung hinzugefügt wird oder hochleistungsfähige Richtantennen an APs das Signal in eine Richtung verstärken, was jedoch die Reichweite auf einen kleineren Bereich beschränkt. Durch aktuelle Wi-Fi-Innovationen im Bereich der adaptiven Antennen-Arrays erhalten Netzwerkmanager jetzt die Möglichkeit, die Signalstärke- und Kanalvorteile einer Richtantenne zu nutzen, aber dennoch dieselbe Netzabdeckung mit weniger Access Points zu erzielen.

Abwehr von Funkstörungen mit intelligenteren Antennen

Die Lösung des Problems liegt in der Fähigkeit von Wi-Fi-Systemen, ein Signal direkt an einen Benutzer zu senden und dieses Signal zu überwachen, um sicherzustellen, dass es den höchstmöglichen Durchsatz liefert. Gleichzeitig leitet es dabei Wi-Fi-Übertragungen immer wieder neu über Signalpfade, die als sauber bekannt sind, ohne den Kanal zu wechseln. Neue Wi-Fi-Technologien, die Dynamic Beamforming mit kleineren intelligenten Antennen-Arrays (die als "Smart Wi-Fi" bezeichnet werden) vereinen, kommen dieser WLAN-Problemlösung am nächsten. Das dynamische, antennenbasierte Beamforming ist eine neue Technik, die entwickelt wurde, um die Form und Richtung der Funkenergie zu ändern, die vom AP ausgestrahlt wird. Dynamic Beamforming konzentriert Wi-Fi-Signale dort, wo sie benötigt werden, und "steuert" die Signale gleichzeitig um Funkstörungen herum, sobald diese auftreten.

Diese Systeme verwenden verschiedene Antennenmuster für jeden Client, die beim Auftreten von Problemen jeweils geändert werden. Wenn beispielsweise Funkstörungen auftreten, kann eine intelligente Antenne ein abgeschwächtes Signalmuster in die Richtung der Störung ausgeben und so den

SINR-Wert steigern und eine niedrigere Datenrate überflüssig machen. Das antennenbasierte Beamforming verwendet eine Reihe von Richtantennenelementen, um Tausende von Antennenmustern oder Pfaden zwischen dem AP und dem Client zu bilden. Die Funkenergie wird jetzt über den optimalen Pfad gestrahlt, der die höchste Datenrate und den geringsten Paketverlust sichert. Clientbestätigungen für die Standard-Wi-Fi-Medienzugriffskontrolle (MAC) werden überwacht, um die Signalstärke, den Durchsatz und die Paketfehlerrate eines ausgewählten Pfads festzulegen. Damit wird sichergestellt, dass der AP genau weiß, was der Client erwartet. Außerdem kann der AP jederzeit zu einem besseren Pfad wechseln, wenn eine Störung auftritt.

Intelligente Antennen-Arrays weisen Störungen außerdem aktiv ab. Da in einem Wi-Fi-Netz jeweils nur ein Benutzer sprechen kann, können Antennen, die nicht verwendet werden, Störungen ignorieren oder abwehren, die Wi-Fi-Übertragungen verhindern würden. Das führt in einigen Fällen zu einer deutlichen Steigerung der Signalstärke von bis zu 17 dB.

802.11n: Versprechen und Realität

Als deutliche Wi-Fi-Optimierung steigert IEEE 802.11n die Kapazität der Technologie von 54 auf 300 Mbit/s oder mehr. Das Problem ist, dass Benutzer diese Art von Leistung nie erleben, unabhängig davon, welchen Preis sie zahlen. Mit IEEE 802.11n werden mehrere Datenströme gleichzeitig über eine Reihe von Funkübertragungs- (TX) und Empfangsketten (RX) sowie Antennen übertragen, um den zusammengefassten Durchsatz einer bestimmten Verbindung zu steigern. Ein Strom ist eine Kette von Funkkomponenten, die Antennen gemeinsam verwenden. Jeder Strom wird gleichzeitig in der Funkdomäne übertragen. Dabei kommen Signalspiegelungs- oder "Multipath"-Funktionen zum Einsatz, um sicherzustellen, dass der Strom eindeutig empfangen wird. Dies wird als "Spatial Multiplexing" bezeichnet, bei dem mehrere Signale mit dem Bereich als Parameter codiert werden. Ein Empfänger decodiert die Signale über mehrere Antennen und bringt dabei jeden Strom in eine eindeutige Funkkette. Aber was geschieht, wenn die Übertragung oder der Empfang dieser (jetzt) mehreren Wi-Fi-Signale unterbrochen wird?

Ein häufig übersehener und wenig optimierter Aspekt kommerzieller IEEE 802.11n-Systeme ist die Kontrolle über die Funkfrequenzabweichung. Eine robuste, reaktionsfähige Funkschicht ist für die Leistung des Wireless-Netzwerks wichtig, insbesondere für ein Wi-Fi-Netz, das im offenen Spektrum betrieben wird. Ironischerweise berücksichtigen die meisten der auf IEEE 802.11n basierenden Systemprodukte diesen Aspekt nur, indem weitere Funkketten und Antennen integriert werden. Darüber hinaus kosten diese Geräte fast zwei- bis dreimal so viel wie ältere IEEE 802.11a/b/g-Geräte. Zwar wird erwartet, dass die IEEE 802.11n-Gerätepreise fallen, wenn bessere Chips zur Verfügung stehen, aber trotzdem sind diese Lösungen immer noch viel teurer als ihre früheren Gegenstücke. Was wirklich benötigt wird, ist eine Innovation, die über den Chip hinausgeht und die Leistung, Reichweite und Zuverlässigkeit deutlich verbessert. Auf diese Weise können alle Unternehmen von den Vorteilen profitieren, ohne einen hohen Preis zahlen zu müssen.

Dynamic Beamforming als Lösung

Beamforming – eine Option innerhalb des IEEE 802.11n-Standards – ist eine spezialisierte Methode der Funkübertragung, die entwickelt wurde, um die Reichweite und Leistung von Wi-Fi-Signalen zum Client zu steigern. Beamforming ist im IEEE 802.11n-Standard auf der Chipebene definiert, indem das Timing oder die "Phase" von Signalen während der Übertragung geändert wird. Typisches Beamforming ist zwar nützlich, berücksichtigt aber weder die explizite Kontrolle noch die Ausrichtung dieser Signale an einen bestimmten Client. Dynamisches, antennenbasiertes Beamforming, die aktuelle Innovation im Wi-Fi-Bereich, geht einen Schritt weiter und ändert oder steuert direkt die Form und Richtung von Signalen. Dabei werden Rückmeldungen von jedem Client verwendet, um jederzeit den schnellsten und saubersten Pfad zu bestimmen. Sender, die Dynamic Beamforming unterstützen, verwenden eine Reihe von Antennenelementen, um Antennenmuster oder Pfade zwischen dem AP und dem Client zu bilden. Der AP wählt jederzeit den besten Pfad aus. APs, die Beamforming unterstützen, lenken die ausgestrahlte Funkenergie direkt an ein empfangendes Wi-Fi-Clientgerät. Der Zweck ist eine Verbesserung des Signalempfangs im Client und daraus folgend ein höherer Durchsatz.

Mit diesem Ansatz werden Wi-Fi-Signale geformt und über ein leistungsstarkes "intelligentes" Richtantennen-Array an jeden Client geleitet. Richtantennenelemente im Array können einzeln ausgewählt oder kombiniert werden, um jede Paketübertragung zu optimieren. APs übertragen Wi-Fi-Signale nur bei Bedarf direkt an jeden Client und verwenden dabei den Signalpfad mit der höchsten Leistung, ohne dass Netzwerkadministratoren APs oder Antennen ausrichten müssen. Da jedes Wi-Fi-Signal ein konzentrierter "Funkstrahl" ist, wird die Reichweite bis um das Vierfache gesteigert, ohne Signale in Bereichen zu vergeuden, in denen sie nicht benötigt werden.

Fazit

Kombiniert mit IEEE 802.11n ermöglicht Dynamic Beamforming jetzt einen Grad der Zuverlässigkeit, der bisher nicht möglich war. Durch das Steuern jeder Übertragung über den Signalpfad mit der höchsten Qualität können Wi-Fi-Access Points mit Dynamic Beamforming Funkstörungen vermeiden, die Übertragungsgeschwindigkeit steigern und Übertragungsfehler minimieren. Das sorgt für eine deutliche Reduzierung der Anzahl der erforderlichen APs und für eine zuverlässige Abdeckung eines bestimmten Bereichs, was wiederum die Kosten erheblich senkt. *(jp)*

Christian Sauer ist Regional Sales Manager Central Europe bei Ruckus Wireless.

Bleiben Sie in Verbindung!

Folgen Sie uns auf Twitter

twitter.com/ita_blog

Werden Sie ein Fan auf Facebook

www.facebook.de/itanet

Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet

Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

Auf Facebook haben wir ein eigenes Profil. Neben ausgesuchten Informationen rund um das Magazin und Veranstaltungshinweisen finden Sie hier auch Gewinnspiele oder Wissenstests. Oder wollen Sie den IT-Administrator in 140 Zeichen täglich begleiten? Verfolgen Sie unser „Gezwitscher" über die interessantesten Neuigkeiten, besten Downloads und Tipps auf Twitter. Wenn Sie aber den direkten Austausch suchen, sind Sie in unserer Xing-Gruppe genau richtig. Lernen Sie dort Ihre Kollegen aus der IT und die Heftmacher des IT-Administrators persönlich kennen und nehmen Sie Einfluss auf Ihr Praxismagazin. Immer gut informiert bleiben Sie auch über unseren RSS-Feed.

Treten Sie unserer Community bei. Wir freuen uns auf Sie.

iTadministrator

Das Magazin für professionelle System- und Netzwerkadministration

SharePoint als Software-as-a-Service

Zusammenarbeit nach Maß

von Stephan Oetzel

Nicht selten arbeiten Mitarbeiter im Unternehmen mit externen Partnern zusammen, wollen aber Daten oder Dokumente nicht mehr per E-Mail austauschen – etwa um mangelnden Sicherheitseinstellungen aus dem Weg zu gehen. Kommt Microsoft SharePoint zum Einsatz, existieren für diesen Fall zwei Lösungen: den eigenen SharePoint-Server im Internet zu veröffentlichen oder SharePoint Online aus der Cloud zu nutzen. In diesem Beitrag wiegen wir beide Varianten anhand von Fallbeispielen gegeneinander ab und berücksichtigen dabei mögliche Strategien, mit denen Teams auch außerhalb des Unternehmens effizient zusammenarbeiten können.

Microsoft hat sich in den letzten Jahren vom reinen Software-Hersteller zum Service Provider weiterentwickelt und das Thema Software-as-a-Service (SaaS) stark forciert. Im Rahmen dieses Angebots stellt Microsoft verschiedene Dienste zur Verfügung. Die Microsoft Business Productivity Online Suite (BPOS) enthält verschiedene Bestandteile, die das Arbeiten mit Online Services gestatten: Neben der Möglichkeit, den eigenen internen E-Mailserver durch einen gehosteten Exchange Server abzulösen, lassen sich etwa auch Lösungen zum Web Conferencing nutzen. Ein gehosteter Office Communication Server ist ebenso bestellbar. Einer der wichtigsten Bestandteile des Cloud-Portfolios aber ist der gehostete SharePoint, mit dem Nutzer sehr zügig eine Collaboration Plattform aufbauen können.

Zugriff über Single-Sign-on oder Webinterface

Nachfolgend wollen wir verdeutlichen, was dieser gehostete SharePoint Server eigentlich leistet und wie der Zugriff genau funktioniert. Da die Beta-Version von SharePoint 2010 zum Zeitpunkt der Erstellung dieses Beitrags noch nicht freigegeben war, beziehen sich alle hier beschriebenen Szenarien auf die Version 2007, also die Standard-BPOS-Variante, bei der ein Unternehmen keinen dedizierten Server mietet, sondern zusammen mit anderen Kunden ein gemeinsames System nutzt.

Ist die grundlegende Einrichtung von BPOS abgeschlossen, steht dem Nutzer eine Single-Sign-On-Applikation (SSO) zur Verfügung, über die sich die verschiedenen Anwendungen starten lassen. Der SSO-Zugang ist allerdings nicht zwingend notwendig. Ebenso möglich ist der klassische Zugriff direkt auf die SharePoint-Site mittels Eingabe von Benutzername und Passwort. Nach erfolgreicher Anmeldung steht dem Nutzer eine SharePoint Server-Standardumgebung zur Verfügung. Die ersten Listen und Bibliotheken lassen sich gewohnt zügig erstellen. Auch weiteren Usern Zugriff zu gewähren, ist ohne Schwierigkeiten möglich.

Im nächsten Schritt folgt die Installation von Custom Web Parts. Dies funktioniert allerdings nicht mit der Version 2007, denn hier fehlt noch die Möglichkeit, eigene Entwicklungen auf einem gehosteten (und damit mehreren Kunden zur Verfügung gestellten) SharePoint Server bereitzustellen. Selbst auf einem dedizierten Microsoft-Server ist dies nur nach einer aufwändigen Zertifizierung der Software realisierbar. Auf den ersten Blick könnte nun fast der Eindruck entstehen, dass SharePoint als Bestandteil der BPOS-Suite kaum Sinn ergibt. Anhand einiger Fallbeispiele aus der Praxis wollen wir aber verdeutlichen, dass es einige nützliche Anwendungsgebiete für die gehostete SharePoint Lösung gibt.

Fallbeispiel 1: Expandierender Mittelstand

Beispiel Nummer eins ist ein fiktives Unternehmen, die Firma Möbel Meier. Sie hat sich auf den Import exklusiver Möbel aus Spanien und Italien spezialisiert. Zehn Mitarbeiter betreuen von der Zentrale aus die Kunden und fünf Außendienstler kaufen vor Ort die Möbel ein. Derzeit kommunizieren alle Beteiligten über verschiedene E-Mailadressen, eine zentralisierte IT ist nicht vorhanden. Das Geschäft floriert, die Kundenzahlen stei-

gen stetig an und parallel dazu das Kommunikationsvolumen. Der IT-affine Junior-Chef des Unternehmens erkennt die Problematik unkoordinierter und umständlicher Kommunikation durch die Mitarbeiter. Als dann sogar mehrfach Bestellungen verloren gehen, handelt er und fragt diverse Dienstleister an. Ein Dienstleister bietet die BPOS-Suite mit 15 Lizenzen an. Dieser Fall passt für das Unternehmen optimal, denn ohne den Zwang, eine eigene Serverlandschaft im Hause aufzubauen, deckt die Lösung die notwendigen Features ab:

- Zugriff auf einen zentralen Mailserver
- Gemeinsame Dokumentenablage von Bestellungen und Aufträgen im SharePoint
- Benachrichtigungen bei der Änderung von Dokumenten und dem Eingang von neuen Bestellungen
- Erstellen einer einfachen Übersicht über alle Bestellungen
- Einfache Zusammenarbeit mit den Einkäufern im Ausland
- Kurze Abstimmungswege zwischen Einkäufer und Kundendienst mittels Office Communications Server (OCS)

Im geschilderten Szenario ist BPOS die richtige Wahl. Ohne großen Aufwand lässt sich hier binnen weniger Tage eine Lösung erstellen, die die Produktivität der Firma sofort massiv steigert. Der finanzielle Aufwand für den Aufbau einer eigenen Umgebung wäre an dieser Stelle übermäßig hoch und nicht zu vertreten.

BPOS ermöglicht es, ein individuelles Paket aus folgenden Bestandteilen zu wählen:

- SharePoint Online
- Exchange Online
- Office Communications Online
- Office Live Meeting

Alternativ ist auch die Wahl zwischen zwei Suite-Produkten möglich:

- Microsoft Business Productivity Online Deskless Worker Suite (bestehend aus Exchange Online und SharePoint online)
- Microsoft Business Productivity Online Standard Suite (beinhaltet alle vier Bestandteile)

BPOS – SaaS nach dem Baukastenprinzip

Fallbeispiel 2: Dienstleister mit hohen Sicherheitsstandards

S3 – Schmidt Security Solutions entwickelt für Kunden in ganz Deutschland Sicherheitslösungen wie etwa Alarmanlagen. Die 300 Angestellten verteilen sich auf Büros in allen Bundesländern. Der Hauptsitz in München beheimatet das Rechenzentrum mit den Basis-Infrastrukturdiensten. Ein zweites Rechenzentrum in Nürnberg dient als Failover. Die derzeitige Lösung, bei der Dateien über Ordner-Freigaben ausgetauscht werden, ist sehr umständlich und erfordert die Einwahl per VPN. Als einzige Bedingung knüpft die Geschäftsleitung an die Einführung von SharePoint möglichst geringe Kosten.

Klein holt für das Projekt von einem IT-Dienstleister ein Angebot ein, in dem auch die gewünschte BPOS-Suite enthalten ist. Auf der Basis dieses Angebots präsentiert Klein vor der gesamten Geschäftsleitung sein Konzept für die gewünschten Projekträume. Doch die Präsentation führt nicht zum Erfolg, das Projekt wird eingefroren. Der IT-Leiter hatte nicht berücksichtigt, dass die bei jedem Projekt ausgetauschten Kundendaten als hochsensibel eingestuft werden. Da die Microsoft-Rechenzentren aber nicht in Deutschland lokalisiert sind, macht die Geschäftsleitung der S3 juristische Bedenken geltend. Die Rechtslage der Staaten, in denen die Rechenzentren arbeiten, unterscheide sich von der deutschen ganz erheblich.

Zudem verbieten die Datenschutz-Richtlinien der Firma S3 die Lagerung von Projektdaten außerhalb des Unternehmens. Klein hatte keine Informationen über die Qualität der auszutauschenden Daten eingeholt und muss nun das Konzept grundlegend überarbeiten. Für die Unternehmensberatung S3 ist BPOS daher keine Lösung: Die Lagerung der Daten auf fremden Trägern und auf Servern im Ausland ist nicht vereinbar mit den unternehmensinternen Richtlinien.

Bild 1: Microsoft stellt mit der Business Productivity Online Suite (BPOS) mehrere Applikationen über Single-Sign-On zur Verfügung

Fallbeispiel 3: Global Player mit internationalen Zulieferern

Die deutsche Firma Maschinenbau Müller AG exportiert über weltweite Niederlassungen ihre Maschinen zur Massenabfüllung von Bier und anderen Getränken. Die 2.000 Mitarbeiter arbeiten von den verschiedenen Standorten aus an gemeinsamen Projekten. Die Projektteams legen ihre Dateien auf verschiedenen Fileshares in diversen Lokationen ab. So kommt es häufiger vor, dass ganze Projektablagen nicht verfügbar sind und damit wichtige Informationen nicht abgerufen werden können.

Die IT-Abteilung der Maschinenbau Müller AG beklagt zudem die Situation hinsichtlich der Wartung und der Datensicherung – denn die Daten liegen nicht zentral auf einem Server, sondern weltweit verteilt. Ein gemeinsames Backup der Daten ist deshalb nicht möglich. Auch der Neustart von Servern für Wartungsarbeiten oder das Einspielen von Patches gestaltet sich schwierig. Die Server in China zum Beispiel werden zwar von Mitarbeitern vor Ort nicht benutzt, allerdings greifen Mitarbeiter von Europa und Nordamerika aus auf die in China gespeicherten Daten zu. IT-Leiter Wolfgang Weber steht vor einem weiteren Problem: die Anbindung von Zulieferern an die Pro-

jektdaten. Denn das Unternehmen hat sich in den letzten Jahren dahin entwickelt, Maschinen nur noch zusammenzusetzen, aber nicht mehr selbst zu bauen. Durch diese Konstellation ist es auf Projektebene unerlässlich, zusammen mit den Zulieferern mit denselben Daten zu arbeiten.

Weber erhält über seinen Software-Distributor den Hinweis auf BPOS und den darin enthaltenen SharePoint Online. SharePoint selbst wird im Unternehmen sogar schon produktiv eingesetzt: als BI-Lösung, um kaufmännische Informationen im Rahmen von technischen Projekten darzustellen. Maschinenbau Müller hat umfangreiche Sicherheitsmaßnahmen getroffen, um sich einerseits vor Angriffen aus dem Internet zu schützen, andererseits aber auch internen Datendiebstahl zu verhindern. Dadurch können Firmen-Externe nur unter großen Umständen auf Daten zugreifen, denn ein langwieriger und aufwändiger Genehmigungsprozess ist dafür erforderlich.

Deshalb plant Weber die Einführung von externen Projekträumen auf Basis von BPOS beziehungsweise SharePoint Online. Die Vorteile liegen für ihn und seine IT-Abteilung klar auf der Hand: Da die Projekträume hauptsächlich zum Austausch von Dateien, Terminen und Aufgaben dienen sollen, sind keine weiteren Funktionalitäten notwendig. Die Projektleiter können weiterhin auf dem internen SharePoint das Projektcontrolling durchführen und über den gehosteten SharePoint mit den Lieferanten und Mitarbeitern vor Ort zusammenarbeiten. Auch die Probleme Verfügbarkeit und Backup sind damit geklärt, da beides von Microsoft über das hochredundante Rechenzentrum sichergestellt wird.

SharePoint Online:
4,47 Euro/Monat pro User

Business Productivity Online Suite:
8,52 Euro/Monat pro User

Die Kosten für die BPOS-Dienste lassen sich über den Preiskalkulator [1] von Microsoft berechnen.

Kosten im Rahmen von Microsoft Online Services

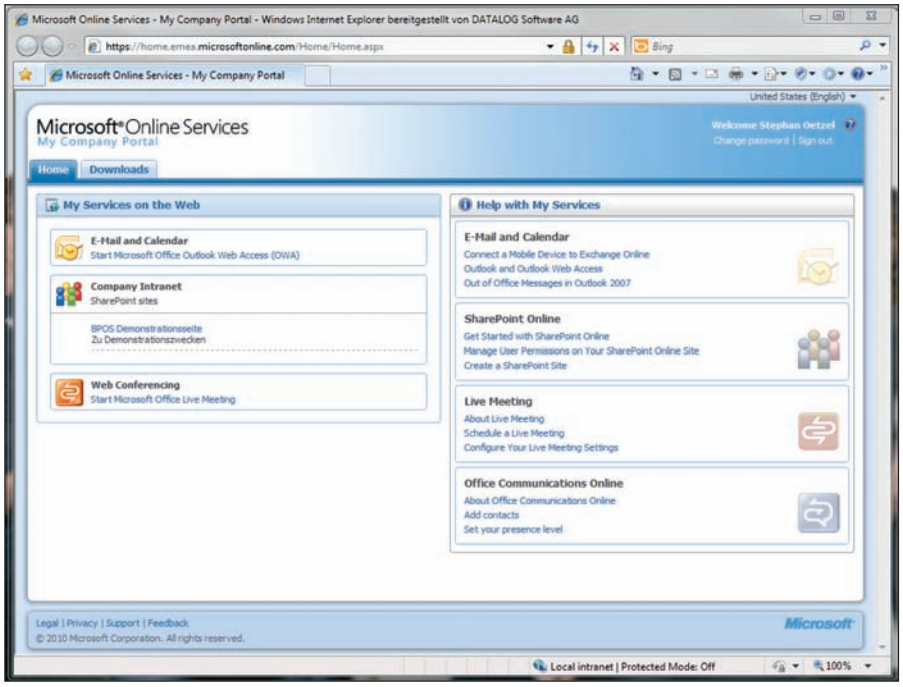


Bild 2: Das Company-Portal ist der zentrale Einstiegspunkt für den Zugriff auf die verschiedenen BPOS-Bestandteile

Kosten vergleichen

Vor der Einführung von SharePoint oder SharePoint Online sollten IT-Verantwortliche organisatorische und technische Voraussetzungen sowie etwaige Hindernisse bei der Einführung genau prüfen. Ebenfalls wichtig sind wirtschaftliche Überlegungen. Folgende Kosten sind hierbei genauer zu berücksichtigen:

- Basiskosten: Hierzu zählen die Kosten für den Server (Hardware oder virtuell), Kosten für die Energieversorgung und für die Klimatisierung
- Betriebskosten: Monatliche Wartungskosten (Personal), Kosten für Internetanbindung
- Software-Lizenzen: Betriebssystem, SharePoint Server und CALs, Backup-Software, Antiviren-Lösung, weitere Drittanbieter-Software

Genauen Anwendungsfall beachten

Aus den drei vorgestellten, völlig unterschiedlichen Praxisbeispielen geht klar hervor, dass ein grundsätzliches Urteil über SharePoint Online nur sehr schwierig zu fällen ist. Vielmehr kommt es – wie so oft – auf viele Details der jeweiligen Situation an. Wie sieht die vorhandene Infrastruktur aus? Wer soll auf die Daten zugreifen? Gibt es gesetzliche Vorgaben oder hausinterne Richtlinien, die gegen eine Auslagerung von Daten sprechen? Auch die Anzahl der künftigen Benutzer ist eine wichtige Kenngröße für die Entscheidung, ob "on-premise" oder "in the Cloud" die richtige Lösung ist. Was die Sicherheit betrifft, hat Microsoft die Online-Services nach SAS70 Type II, ISO 27001 und Cybertrust zertifizieren lassen. Ein eigenes Whitepaper [2] gibt darüber Aufschluss. Dieses klärt den Nutzer außerdem zu Themen wie Backup und Recovery oder Ausfallsicherheit auf. *(ln)*

Stephan Oetzel ist SharePoint-Berater bei der DATALOG Software AG in München.

[1] **Preiskalkulator für BPOS**
ABW11

[2] **Whitepaper zum Thema "Sicherheit der Microsoft Online Services"**
ABW12

Link-Codes

Exchange Server 2010

Das Buch "Exchange Server 2010 – Planung, Installation, Migration und Betrieb" hat sich die Aufgabe gestellt, alle jene Administratoren, die sich mit dem Messaging-Server auseinandersetzen müssen, zu befriedigen. Soviel Anspruch hat sein Gewicht und das Buch kommt mit über 1.300 Seiten Umfang nicht gerade kleinlich daher. Die typische (Erst)-Installation wird dabei Schritt für Schritt erarbeitet und sollte auch dem Exchange-Neuling keine Schwierigkeiten bereiten. Anschließend leitet der Autor den Leser zum essenziell wichtigen Kapitel "Nachrichtenfluss und Connectoren" weiter. Hier werden vorrangig die Themen E-Mail-Routing, Nachrichtentransport oder auch Warteschlangen behandelt. Das Kapitel Routing über mehrere AD-Standorte dokumentiert hauptsächlich Informationen zu den Themen AD-DNS und -Routing. Unerlässliche Themen wie Postfachdatenbanken, der Einsatz öffentlicher Ordner sowie die Arbeit mit Postfächern, Kontakten und Verteilergruppen, Archivierung sowie Clientanbindung werden vom Autor sehr ausführlich beschrieben.

Die nachfolgenden Kapitel bedienen die erfahrenen Administratoren und fortgeschrittenen Techniken, so die Einbindung des Forefront Threat Management Gateway 2010, Forefront Protection 2010, Edge-Tranport-Server und rollenbasierte Berechtigungen und Delegierung. Beim Abschnitt "Spamschutz und E-Mailsicherheit" wären weiterführende Anregungen jenseits des Microsoft-Horizonts wünschenswert gewesen. Die Aspekte der Datensicherung, Fehlerbehebung und Leistungsverbesserungen sowie Migration, Unified Messaging und Hochverfügbarkeit und Database Availability Groups schließen den anspruchsvollen Inhalt ab, bevor der Autor seine Beschreibungen für das Verbinden von Exchange-Organisationen und die Rechteverwaltung präsentiert. Die Erläuterungen sind zwischen zahlreichen Screenshots und Grafiken eingebettet.

Fazit: Der Einstieg in die Exchange-Welt dürfte aufgrund der zahlreich bebilderten Arbeitsanweisungen ebenso leicht fallen wie das Nachschlagen für erfahrene Administratoren. Alle Schwerpunkte für den Praxisbetrieb werden erläutert, wenngleich das ein oder andere Kapitel durch zu viele Randinformationen etwas aufgebläht wirkt. Die Neuerungen von Service Pack 1 sind ebenfalls verarbeitet sowie das Zusammenspiel mit dem Mail-Client Outlook 2010. Das Buch ist in erster Linie ein Praxisratgeber und hält sich selten in abstrakten Konzeptvorschlägen oder Planumgebungen auf. *Frank Große*

Autor:	Thomas Joos
Verlag:	Markt + Technik
Preis:	59,95 Euro
ISBN:	978-3-8272-4586-1
Bewertung:	★★★★☆

Praxishandbuch Speicherlösungen

Die Verwaltung und Konsistenz der stetig steigenden Datenmengen sollte bei IT-Verantwortlichen keine Fragen zur Daten(un)sicherheit offen lassen. Genau an diesem Punkt nimmt das erfahrene Autorentrio den Leser an die Hand. Dabei wird ein chronologisch-inhaltlicher Bogen vom typischen Ablauf der Implementierung, von der Bedarfsanalyse bis zur späteren Betriebsphase gespannt. Unabhängig davon, ob die neue Storage-Implementierung mit einem Consultant-Unternehmen oder in Eigenregie vollzogen werden soll: ein weitgehendes Verständnis und ein ausgefeiltes Konzept ist vonnöten. Den Grundriss dafür liefert der erste Teil des Buches, der über die Hälfte der Gesamtseitenzahl in Anspruch nimmt und sich den Themen Management und Assessment der Bedarfsanalyse widmet. Sowohl die denkbaren Betriebsmodelle wie auch die Auswahl der Speichersysteme und -komponenten werden umfangreich erörtert. Erfreulich, dass die Autoren zu technischen Erläuterungen den Praxisbezug herstellen (Thema Projektmanagement) und nicht nur mit Lehrbuchmerksätzen aufwarten. Weniger umfangreich werden der Ausschreibungsprozess und das Design sowie die Validierung der Speicherlösung beschrieben, wenngleich keine Fragen offenbleiben.

Im zweiten Teil wird die Inbetriebnahme an einem Beispielprojekt zur Implementierung eines Speichersystems mit Fibre Channel-SAN dargestellt. Dabei werden sowohl Anregungen für den Ablauf wie auch Empfehlungen aus Projektsicht gegeben. Der letzte Buchteil befasst sich mit den administrativen Aspekten der erfolgreich installierten Storage-Lösung.

Fazit: Knapp 350 informativ gefüllte Seiten hinterlassen einen beeindruckenden Inhalt. Das Autorentrio hat die anspruchsvolle Materie gut gebündelt und wird dem Anspruch eines Praxishandbuches weitestgehend gerecht. Die Ausrichtung abseits von Produktempfehlungen hinzu Best-Practices-Strategien weiß zu gefallen.

Frank Große

Autoren:	Roland Döllinger, Reinhard Legler, Duc Thanh
Verlag:	dpunkt-Verlag
Preis:	49,90 Euro
ISBN:	978-3-89864-588-1
Bewertung:	★★★★★

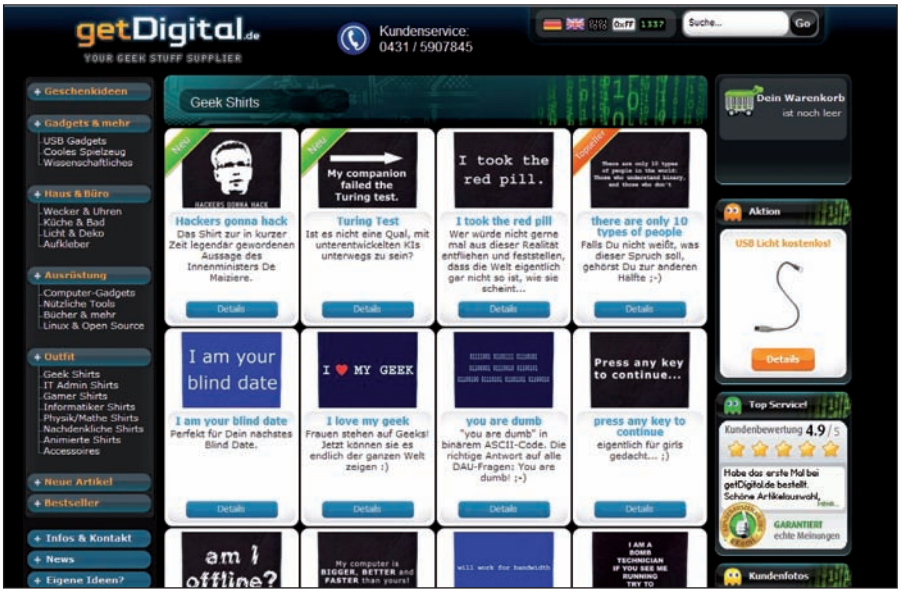
getdigital.de und digitalgeek.de

Weihnachtsgeschenke für Nerds

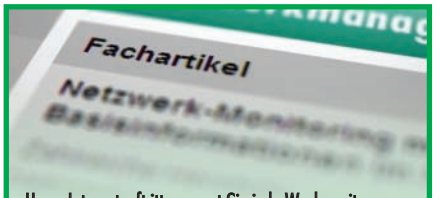
Weihnachten steht vor der Tür und damit auch wieder die Zeit für die passenden Geschenke. Doch was schenkt man einem IT-begeisterten Freund oder Kollegen, der im Prinzip schon alles hat? Nicht selten endet die Suche nach einem Präsent in überfüllten Geschäften und endlosen Schlangen an der Kasse, ohne wirklich das Richtige gefunden zu haben. Dabei gibt es online zahlreiche witzige Alternativen, besonders für IT-affine Menschen. Die beiden Portale getdigital.de und digitalgeek.de beispielsweise bieten zuhauf mehr oder weniger nutzlose, aber humorvolle Geschenke. Damit sorgen Sie garantiert für eine Überraschung und Aufmerksamkeit.

Wie wäre es zum Beispiel mit einem Retro-Telefonhörer mit USB-Anschluss oder einem USB-betriebenen Aktenvernichter? Letzterer frisst Dokumente mit einer Breite von bis zu 12 Zentimeter und bietet sogar einen Brieföffner. Dieser sollte jedoch im Betrieb nicht mit der Vernichtungsfunktion verwechselt werden. Natürlich gibt es auch sinnvollere Geschenke, wie etwa das solarbetriebene Ladegerät für Handys oder einen USB-Bleistiftanspitzer. Auch sehr nützlich und vor allem innovativ kommt die Laser-Tastatur für das Smartphone daher. Das Gadget projiziert die Tasten auf einer Fläche von 30 x 10,5 cm auf den Tisch und kommuniziert via Bluetooth mit dem Handy. Somit lassen sich Texteingaben bequemer und vor allem wesentlich schicker erledigen als auf der Originaltastatur. Kompatibel ist das Keyboard mit Windows Mobile, Palm OS, Blackberry, Mac OS und Linux. Bleibt schließlich noch der Klassiker zu nennen, die Geek-Bekleidung. Dies sind meist T-Shirts mit Sprüchen rund um die IT wie etwa "Realität ist da, wo der Pizzamann herkommt" oder "There's no place like 127.0.0.1".

All diese Geschenke eignen sich natürlich hauptsächlich für männliche Kollegen und Freunde, die sich etwa ab und an zur Gaming-Runde treffen. In der Damenwelt dürften derartige Nerd-Präsente wohl eher auf Unverständnis stoßen. Hier lohnt sich der traditionelle Gang in den Buchladen, die Parfümerie oder gar zum Juwelier – auch wenn es sicherlich Frauen gibt, die sich ebenfalls über ein nerdiges T-Shirt oder ein USB-Gadget zu Weihnachten freuen. *(dr)*



Über ein passendes Geek-Shirt freut sich der IT-Freak. Ob es beim anderen Geschlecht gut ankommt, sei dahingestellt.



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

WLAN als Grundlage für Fixed Mobile Convergence

Was die Kommunikation im Unternehmen angeht, stellen Anwender immer höhere Ansprüche an Zuverlässigkeit und Qualität. Dies betrifft in besonderem Maße die Übermittlung des gesprochenen Wortes. Fixed Mobile Convergence beschreibt das Zusammenwachsen von Fest- und Mobilfunknetzen und basiert im Wesentlichen auf Voice-over-WLAN. In unserem Online-Beitrag erklären wir, was Sie bei der Bereitstellung einer gleichbleibenden Servicequalität beachten müssen und wie die Voraussetzungen für ein nahtloses und einwandfreies Roaming aussehen.
www.it-administrator.de/themen/kommunikation/fachartikel/86966.html

High-End-Grafikarbeitsplätze auf virtuellen Desktops

Die Desktop Virtualisierung schreitet stetig voran und immer mehr Unternehmen entdecken das Potenzial dieser Technologie. Citrix bietet Kunden mit der Technologie "Multi GPU Pass-Through" die Möglichkeit, High-End-Grafikarbeitsplätze mit XenServer 5.6 zu virtualisieren. Mitarbeiter erhalten dann über XenDesktop Zugang zu diesen speziellen Arbeitsplätzen, die sich zum Beispiel für CAD/CAM-Anwendungen eignen. Unser Fachartikel im Web beschreibt den Einsatz und Nutzen dieser neuen Entwicklung.
www.it-administrator.de/themen/virtualisierung/fachartikel/86967.html

Bausteine zur Endpunkt-Sicherheit

Die Wahrung der Endpunkt-Sicherheit gestaltet sich heute wesentlich schwieriger und komplexer als noch vor zehn Jahren. So ist nicht nur die Häufigkeit von Angriffen gestiegen, auch sind die Attacken immer besser getarnt und komplexer denn je zuvor. Die Abwehr der Bedrohungen sollte daher idealerweise auf mehreren Ebenen erfolgen. Lesen Sie in unserem Online-Artikel, welche Mechanismen zum Endpunkt-Schutz Sie sich auf jeden Fall zu Nutze machen sollten und warum ein Schild gegen Malware allein nicht mehr ausreicht.
www.it-administrator.de/themen/sicherheit/fachartikel/86968.html

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

»Die IT unterstützt den internen Know-how-Transfer«

Peter Seiler (42) arbeitet bei der österreichischen FERRO-Montagetechnik in Wels, einem Unternehmen der FMT-Gruppe, als Leiter der IT. Mit seinem Team von drei Mitarbeitern sorgt er auch im administrativen Bereich dafür, dass an den fünf internationalen Unternehmensstandorten das IT-Netzwerk mit seinen zahlreichen unterschiedlichen Komponenten problemlos läuft.

Welche Ausbildung haben Sie gemacht?

Auf die kaufmännische Ausbildung an der Handelsakademie im oberösterreichischen Wels folgte eine firmeninterne Karriere. Dabei startete ich im Einkauf und war zwischenzeitlich auch für die Kostenrechnung verantwortlich. Mittlerweile bin ich ausschließlich für die IT zuständig, da dieser Bereich permanent gewachsen ist und die volle Aufmerksamkeit fordert.

Warum sind Sie IT-Administrator geworden?

Die Informationstechnik hat mich schon von jeher fasziniert. In diesem Unternehmensbereich stecken zahlreiche Möglichkeiten sowie das Potenzial, die Prozesse und Abläufe innerhalb des Unternehmens und seiner unterschiedlichen Bereiche zu optimieren.

Welche IT-Umgebung betreuen Sie aktuell?

Ich arbeite als Leiter der IT-Abteilung und bin im Rahmen meiner Aufgaben auch für die Administration mitverantwortlich. FERRO-Montagetechnik arbeitet an fünf Standorten in Österreich, Deutschland und Slowenien. Im Rahmen unseres Teams betreuen wir auch eine Vielzahl von Baustellen in aller Welt. Mehrere Hundert Anwender müssen in einer Microsoft-Umgebung administriert werden. Basis unseres Netzwerkes sind 20 Windows Server, die zum größten Teil virtualisiert sind. Eine Vielzahl unserer Hardware sind dabei mobile Endgeräte.

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

Eine reibungslos funktionierende IT ist das A & O für unseren Geschäftsalltag. Sie unterstützt uns dabei, Projekte termingerecht und transparent abzuwickeln. IT-intern setzen wir darauf, das Potenzial und Know-how der Mitarbeiter optimal auszuschöpfen. Darüber hinaus ist es uns auch extrem wichtig, dass die Mitarbeiter ihr Wissen und ihre Erfahrungen über die IT-Plattform kommunizieren und untereinander austauschen können.

Geburtstag:	05.11.1968
Familienstand:	verheiratet
Hobbys:	Laufen, Schifahren

Peter Seiler, IT-Administrator

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir haben eine Menge Projekte auf unserer Agenda. Dazu gehören unter anderem das Update und die Weiterentwicklung des Reporting für unsere Datenbank SQL Server 2008. Auch für unser ERP-System Microsoft Dynamics NAV steht ein Update an. Storage-Ausbau und -Optimierung sind weitere IT-Baustellen.

Was macht Ihnen an Ihrem Job am meisten Spaß?

Mein Aufgabengebiet hat nicht nur eine technische, sondern auch eine stark organisatorische Ausrichtung. Das macht mir sehr viel Spaß, denn dadurch lerne ich die Abläufe aller Abteilungen kennen und kann diese dann mit einem wissenden Auge unter Einsatz der IT optimieren.

Was war Ihr größter Erfolg als IT-Administrator?

Anfang Juni haben wir unser neues Firmengebäude in Wels bezogen. Mein IT-Team war intensiv in die Planung und Umsetzung der EDV- und Gebäudetechnik involviert. Heute arbeiten wir mit einer modernen Infrastruktur, die eine komplett neue Switching- und Firewall-Technologie von Cisco, eine neue Telefonanlage mit Computer-Telefon-Integration, ein elektronisches Zutrittssystem sowie ein gut gesichertes WLAN-System und viele kleinere technologische Highlights umfasst. Auf die maßgeschneiderte Konzeption sowie die Realisierung der Lösung im durchaus engen Zeitrahmen ohne große Probleme sind wir wirklich stolz.

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

Die immer stärker schwindenden Grenzen zwischen interner IT sowie der entsprechenden Datenhaltung und externen Dienstleistungen (Stichwort Cloud Computing, Outsourcing) so zu organisieren, dass diese für Anwender und Administratoren durchschaubar und vor allen Dingen anwendbar bleiben. Eine weitere Herausforderung ist und bleibt es, die Sicherheit und hier speziell die Datensicherheit so zu organisieren, dass diese den Managementvorgaben sowie gesetzlichen Regularien entspricht.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 1/11 erscheint am 10. Januar 2011

Schwerpunktthema:

Virtualisierung

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

Unsere Ausgabe im **Februar** befasst sich mit dem Schwerpunkt **Sicherheit von Unternehmensdaten**. In unserem Vergleichstest beweisen dabei unter anderem sechs Antivirus-Suiten für Unternehmen ihr Können. In den Workshops lesen Sie, wie die Benutzerauthentifizierung mittels PAM funktioniert.

Als Schwerpunkt im **März** folgt dann das Thema **Netzwerkmanagement**.

***Im Test:* XenClient Express 1.0**

***Im Test:* UC4 Automated Virtualization**

***Workshop:* KVM-basierte Umgebungen absichern**

***Know-how:* Backup virtueller Server**

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, Alexander von Gernler, Thomas Gronenwald, Frank Große, Mathias Hein, Jürgen Heyer, Thomas Hümmler, Thomas Joos, Christian Knermann, Stephan Oetzel, Christian Rusch, Christian Sauer, Hans-Dieter Wahl, Matthias Wessner

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

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

LAC/2008

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

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

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

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

Erscheinungsweise
monatlich

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

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

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

Internet
www.it-administrator.de

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

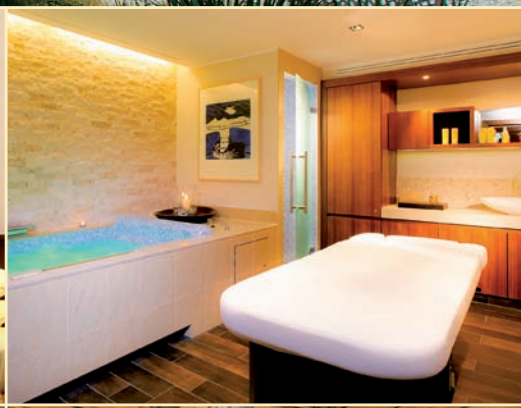
Bankverbindung für Abonnenten
Konto 174 966 462 bei der
Postbank Dortmund, BLZ 440 100 46
Kontoinhaber: Vertriebsunion Meynen

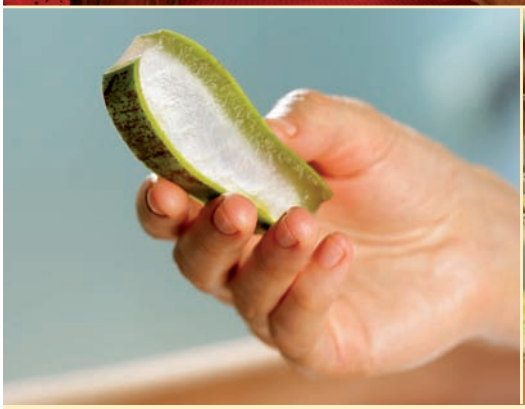
So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-10
Fax: 089/4445408-99
E-Mail: redaktion@it-administrator.de

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





Alpiner Rundum-Genuss in Murnau.
Tauchen Sie ein und besuchen Sie uns.

71 Zimmer und Suiten · Gourmetrestaurant Reiterzimmer (ein Michelin-Stern) · Hofmann's Restaurant · Sonnenterrasse · 6 Veranstaltungsräume bis 200 Personen · Yavanna Wellness & Spa · angegliederte Arztpraxis
Gästehaus Moosberg – traditionelles bayerisches Gästehaus

Ramsachstraße 8 · 82418 Murnau am Staffelsee
Tel. +49 (0) 88 41 / 491-0 · Fax +49 (0) 88 41 / 49 11 00
info@alpenhof-murnau.com · www.alpenhof-murnau.com

Alpenhof MURNAU

slh.com

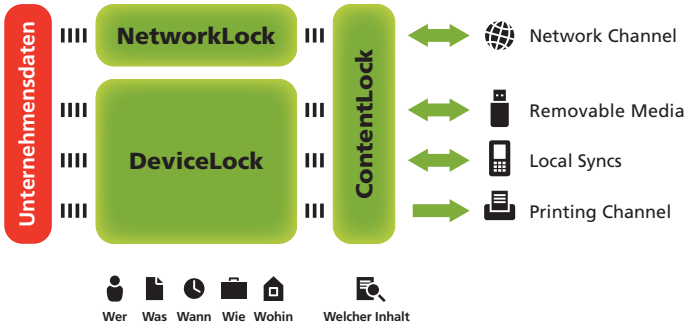
Bringt abends Arbeit mit nach Hause.

Und morgens Viren in die Firma.

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

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

Die Datenflusskontrolle der DeviceLock Endpoint DLP-Suite



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

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security