IT-ADMINISTRATOR.DE

09/2010

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Messaging und Collaboration

VORSICHT: SCHLECHTER TONER

ZIEHT IHNEN DAS GELD AUS DER TASCHE!

Undichte Tonerkartuschen, unbrauchbare Ausdrucke und häufige Ausfälle treiben Ihre Druckkosten unerwartet in die Höhe.
Original HP Toner sind optimal auf HP LaserJets abgestimmt und liefern hervorragende Qualität – Tag für Tag, Seite für Seite.

HIT **PRINT**
INTELLIGENTLY

Vermeiden Sie versteckte Druckkosten!
Entscheiden Sie sich für Original HP Toner!
Weitere Informationen finden Sie unter:
www.hp.com/de/toner

EDITORIAL

Einfach mal abschalten

Liebe Leser,

sanft branden die Wellen am hellen Sandstrand an. Die Mittagssonne sticht vom blauen Himmel herunter, im Hintergrund ziehen Jetskis ihre Bahnen durchs Wasser. Ein wenig gelangweilt schaut Elvira B. ihrem Mann Holger unter dem orangefarbenen Sonnenschirm zu, wie er bereits zum dritten Mal an diesem Tag seine E-Mails abruft – Smartphone und moderne Datennetze machen es möglich. "Und, was gibt's neues in der Arbeit?", fragt sie. "Ach, ein Kollege wollte die Zugriffsrechte in der Buchhaltung ändern und war sich nicht sicher", antwortet Holger, vertieft in seine Antwortmail.

Abschalten kann er als IT-Verantwortlicher auch im Urlaub nicht wirklich. Ständig droht das Smartphone die verdiente Ruhe zu stören. Kommt Ihnen diese Szene vielleicht bekannt vor? Leider wurde es in der modernen Arbeitswelt immer mehr Usus, Mitarbeiter auch im Urlaub, am Wochenende oder mitten in der Nacht erreichen zu wollen. Früher hieß diese Erreichbarkeit "Bereitschaft", war bezahlt und planbar. Heute wird sie schlicht erwartet. Auch die Angst davor, entbehrlich sein zu können, treibt immer mehr Arbeitnehmer in die Erreichbarkeitsfalle.

Dass es auch anders geht, bewies zuletzt die Deutsche Telekom. Sie ordnete mit der Richtlinie "Umgang mit mobilen Arbeitsmitteln außerhalb der Arbeitszeit" offiziell an, dass ihre Mitarbeiter nach Arbeitsschluss auch tatsächlich ihre dienstlichen mobilen Begleiter mit gutem Gewissen abschalten. So soll künftig der nächste Morgen oder der kommende Montag für die Antwortmail ausreichen. Vorbildlich. Denn ist ein Mitarbeiter in seiner Freizeit unentbehrlich und muss ständig erreichbar sein, läuft etwas in der Unternehmensplanung schief. Durch vernünftige Übergaben und Vertretungsregeln sollten sich auch zwei Wochen überbrücken lassen, ohne dass das große Chaos ausbricht. Wie Sie trotzdem für den Fall der Fälle den sicheren Zugriff auf Exchange einrichten, erfahren Sie ab Seite 50.

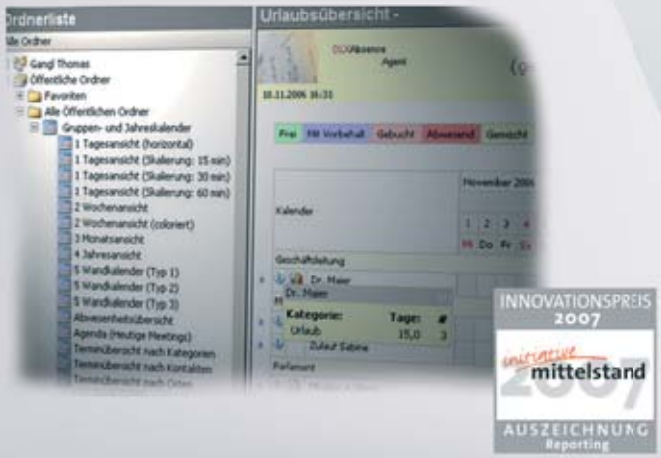
Zurück im Hotel kämpft Holger B. inzwischen mit IT-Problemen ganz anderer Art: Sand hat sich in der Tastatur seines Smartphones festgesetzt und blockiert hartnäckig drei der Tasten. Schade nur, dass es sein Privates ist.

Viel Spaß beim Lesen unserer September-Ausgabe und dem gelegentlichen Abschalten, Ihr

Daniel Richey
Stellv. Chefredakteur

Wer liefert Ihnen das fehlende Puzzleteil zu Outlook© und Exchange©?

Gruppenkalender
Terminmanagement



Mobiler Zugriff
auch für Öffentliche Ordner

Unternehmensweite
Signaturen & Disclaimer

Individualentwicklung
Vertrauen in Erfahrung

www.gangl.de

Ihr Partner für praxisorientierte Outlook© und Exchange© Lösungen!

Ihre Ansprüche sind unser Ansporn!

✉ info@gangl.de ☎ +49 7173 9290 53

INHALT

IT-Administrator – Ausgabe September 2010

Messaging und Collaboration

Einkaufsführer: Systeme zur E-Mailarchivierung

Die Archivierung von E-Mails stellt für viele Unternehmen nach wie vor eine große Herausforderung dar. Angesichts stetig steigender Datenvolumina und der immer größeren Anzahl geschäftlich verschickter Nachrichten werden an die Archivierungslösungen zusehens höhere Ansprüche gestellt. So stehen IT-Verantwortliche vor der wichtigen Aufgabe, diese Datenmengen langfristig sinnvoll und auch rechtssicher zu verwalten und zu organisieren. Auf welche Aspekte Sie beim Thema E-Mailarchivierung achten sollten, zeigt unser Einkaufsführer.

Seite 34

Desktop-Verteilung mit dem Microsoft Desktop Optimization Pack (4)

In unserer Workshopserie zum Microsoft Desktop Optimization Pack (MDOP) stellen wir Ihnen in der letzten Folge das Microsoft System Center Desktop Error Monitoring (SCDEM) vor. Das Werkzeug hilft bei der Fehlersuche, wenn sich auf den Arbeitsstationen Abstürze des Betriebssystems oder von Anwendungen ereignen. So lassen sich selbst dann zentral die Probleme einzelner Computer und der darauf laufenden Applikationen erfassen, wenn Anwender durch einen Neustart in Eigenregie versuchen, die Schwierigkeiten zu lösen. Dann ist das Symptom zwar momentan aus der Welt, aber die Ursache des Problems bleibt im Verborgenen und kann jederzeit wieder zu einem Fehler führen. Wir bringen Ihnen in unserem Workshop näher, wie Ihnen SCDEM bei der Datensammlung und dem Finden von Fehlerursachen hilft.

Seite 57

Themenübersicht

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

In vielen Unternehmen ist das Intranet genauso wichtig wie der externe Webauftritt. Der Software-Hersteller Bitrix bietet Administratoren hierfür mit dem **Bitrix Intranet Portal** eine intuitiv zu bedienende Lösung für den Aufbau und die Pflege des Intranets. Der Clou dabei: Mit der **Extranet Edition** erstellen Sie nicht nur das eigene Intranet, sondern machen dieses auch noch gezielt für Geschäftspartner wie Lieferanten oder wichtige Kunden zugänglich. Diese können so mit den internen Mitarbeitern zusammenarbeiten und sich über den Status aktueller Projekte informieren.

Gemeinsam mit Bitrix verlost IT-Administrator insgesamt **15 Lizenzen** der Bitrix Intranet Portal – Extranet Edition. Diese sind gültig für jeweils ein Jahr und 25 User. **Wert pro Lizenz: 1.759 Euro**. Für die Teilnahme an der Verlosung müssen Sie lediglich die Frage beantworten, aus welchem Land Bitrix ursprünglich stammt. Kleiner Tipp: Das Entwicklungszentrum von Bitrix in Kaliningrad liegt dort. Senden Sie Ihre Antwort bis 30. September 2010 per E-Mail an **redaktion@it-administrator.de** mit dem Betreff **Bitrix**. Viel Glück! *(dr)*

Bitrix: www.bitrix.de

Zu gewinnen: Bitrix Intranet Portal für 1.759 Euro

Leise All-in-one-Druckmaschinen

Samsung erweitert sein Portfolio an **Multifunktionsdruckern** um drei Geräte. Das Modell **CLX-3185** ist ein 3-in-1-System für Drucken, Kopieren und Scannen. Die 4-in-1-Modelle **CLX-3185FN** und **CLX-3185FW** verfügen zusätzlich über eine Fax-Funktion und sind mit einem automatischen Dokumenteinzug für bis zu 15 Vorlagen ausgestattet. Die Drucker lassen sich, je nach Modell, über USB 2.0, kabelgebundenes Ethernet oder WLAN anbinden. Mit Abmessungen von 416 x 378 x 344,2 Millimetern (CLX-3185FN und CLX-3185FW) sind die neuen Drucker zudem die laut Anbieter weltweit kleinsten Farblaser-Multifunktionsgeräte. Sie geben bis zu 16 Schwarzweiß- oder vier Farbseiten pro Minute aus, bei einer effektiven Auflösung von 2.400 x 600 dpi. Das Wireless-Modell CLX-3185FW soll durch einfachen Knopfdruck auf die WPS-Taste (WiFi Protected Set-up) innerhalb von maximal zwei Minuten in der Wireless-Umgebung betriebsbereit sein. Die WLAN-Verbindung wird dabei automatisch konfiguriert und geschützt. An Speicher stehen den Geräten 256 MByte (128 MByte bei CLX-3185) zur Verfügung. Durch die sogenannte NO-NOIS-Technologie liegt der Geräuschpegel bei unter 46 dB(A) beim Farbdruck und unter 48 dB(A) beim Schwarz-Weißdruck. Die neuen Farblaser-Multifunktionsgeräte sind ab sofort erhältlich. Die Preise liegen bei 318 Euro für Modell CLX-3185, rund 400 Euro für den CLX-3185FN und 461 Euro für den CLX-3185FW. *(dr)*

Samsung: www.samsung.de

Die neuen Multifunktionsdrucker von Samsung sollen besonders leise arbeiten

Durchblick in der virtuellen Landschaft

Ipswitch stellt **WhatsUp Gold WhatsVirtual 2.0** vor. Die Software setzt auf dem vSphere API von VMware auf und bietet aktuelle Informationen über die **Verfügbarkeit und die Performance in virtuellen Infrastrukturen** auf Basis von VMware. Version 2.0 der Monitoring-Lösung unterstützt nun VMware vCenter, vMotion, High Availability und virtuelle Cluster. Im Bereich vCenter übernimmt WhatsVirtual das Discovery, das Monitoring und die Kontrolle aller virtuellen Ressourcen durch VMware vCenter. Zudem überwacht die Lösung vMotion Live-Migrationen von VMs zwischen physischen Servern. Dadurch sollen Anwender jederzeit eine vollständige und präzise Abbildung der Zuordnung zu physischen Servern sowie historische Informationen, Reports und Warnmeldungen erhalten. Außerdem ermöglicht Version 2.0 die Überwachung und Verfolgung von VMs, die nach Hardware- oder Betriebssystemausfällen automatisch neu gestartet oder auf andere physische Server migriert werden. Das Discovery, Mapping, Monitoring und Management von ESXi-Hosts und deren virtuellen Maschinen können dabei über eine gemeinsame Konsole erfolgen. WhatsVirtual 2.0 ist ab sofort zu einem Einstiegspreis von rund 1.260 Euro für 25 Devices verfügbar. Für den Einsatz von WhatsVirtual ist WhatsUp Gold v14.2 erforderlich. *(dr)*

Ipswitch: http://de.whatsupgold.com/products/whatsup-gold-plugins/whatsvirtual/

Netzwerk-Aufseher physikalisch und virtuell

BalaBit IT Security stellt **Version 3.0** der **Shell Control Box** (SCB) vor. Die Appliance dient der **Kontrolle und Nachverfolgung von administrativen Zugriffen** im Netzwerk. Die neue Version läuft auf einer leistungsfähigeren Hardware mit Intel-Xeon-5600-Prozessoren, bis zu 24 GByte Hauptspeicher sowie Speicherkapazitäten zwischen 1 und 10 TByte. Je nach Anforderung sind verschiedene Modelle der Shell Control Box 3.0 mit unterschiedlicher Ausstattung erhältlich. Für den Einsatz von zwei Appliances im Cluster-Verbund hat der Hersteller zudem die Hochverfügbarkeitsfunktionen erweitert. So kann eine SCB beispielsweise naheliegende Router überwachen und jetzt auch bei Ausfall einer externen Netzwerkstrecke auf das Ersatzgerät umschalten. Ab Version 3.0 gibt es die Shell Control Box zudem als virtuelle Appliance für VMWare ESX-Systeme. Unternehmen erhalten damit die Möglichkeit, die Shell Control Box auf ihrer bestehenden IT-Hardwareinfrastruktur einzusetzen. Weiterhin hat BalaBit die Unterstützung der Protokolle um VMware View erweitert und bei RDP, SCP und SFTP weiter ausgebaut. Die Preise für die SCB richten sich nach der Anzahl der kontrollierten Hosts und beginnen bei 5.900 Euro. *(dr)*

BalaBit IT Security: www.balabit.com/network-security/scb/

Die Shell Control Box 3.0 von BalaBit ist nun auch als virtuelle Appliance erhältlich

Kompakter Speicherriese

Overland Storage präsentiert den **SnapServer N2000** – einen **konsolidierten Block- und Dateispeicherserver** in 2U-Bauhöhe, der auf bis zu **144 TByte** skalierbar ist. Der Server bietet eine konsolidierte Speicherarchitektur, über die Unternehmen simultan Block- und Dateidaten über Windows-, UNIX/Linux- und Mac OS-Plattformen hinweg speichern und abrufen können, sowie virtuelle Server, Datenbanken, E-Mail- und Back-up-Anwendungen. An Funktionen beinhaltet das Modell unter anderem die Datenreplikation, eine Snapshot-Funktion für Datei- und iSCSI-Volumes, die Möglichkeit, mehrere SnapServer-Geräte über eine Konsole zu verwalten, sowie die Unterstützung für SAS- und SATA-Laufwerke. Basierend auf dem GuardianOS-Betriebssystem stellt das Storage-Gerät Assistenten bereit, die die Nutzer durch die Installation und Erstellung von Speichervolumes führen sollen. Zudem verfügt der N2000 über eine webbasierte Managementkonsole für die Systemadministration. Der SnapServer N2000 ist ab sofort in unterschiedlichen Konfigurationen erhältlich, die bei rund 4.000 Euro starten. *(dr)*

Overland Storage: www.overlandstorage.com/products/network-attached-storage/snapserver-n2000.aspx

Overland Storage bietet mit dem SnapServer N2000 einen auf 144 TByte skalierbaren Speicherserver an

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

Parallels stellt Version 4.0 der Virtualisierungslösung **Parallels Server for Mac** vor. Zu den Neuerungen gehören der Support von Snow Leopard Server als Host und Gast sowie von Windows Server 2008 R2 und Windows 7 als Gäste. Version 4.0 unterstützt zudem Apples Clusterdateisystem Xsan, virtuelle Netzwerke (VLANs), die Ermittlung des Ressourcenverbrauchs für das Accounting, vollständige und inkrementelle Backups, die Migration und Umwandlung von virtuellen Maschinen sowie die Express-Installation von Windows- und Linux-Gastsystemen. Für 1.499 Euro ist Parallels Server for Mac zu haben. *(dr)*

www.parallels.de

Die **baramundi software AG** bringt ihre **Management Suite** in **Version 8.2** heraus. Im Bereich der Softwareautomatisierung steht Nutzern das neue Modul "baramundi Automate" zur Verfügung. Es beinhaltet das "Automation Studio" zum Erstellen von Skripten für Administrationsaufgaben oder zur Oberflächenautomatisierung sowie den "Application Wizard" zum Anlegen von automatischen Installationen für die meisten Setup-Verfahren. Die neue Version ist ab sofort auf dem Markt und kostet bei 500 Clients 49,70 Euro pro Rechner. *(dr)*

www.baramundi.de

PNY Technologies bietet die zweite Generation seiner Solid State-Festplatten an: die **SSD Optima 2,5 Zoll SATA II/USB 2.0**. Basierend auf einem MLC-Speicher (Multi Level Cell), erreichen die SSDs laut Hersteller Lese- und Schreibgeschwindigkeiten von bis zu 235 MByte/s beziehungsweise 150 MByte/s. Sie verfügen dabei über einen JMicron-Controller, der unter Windows 7 die Trim-Funktion steuert und so eine bessere Verteilung der Daten im Speicherbereich gewährleisten soll. Für rund 234 Euro ist beispielsweise die 128 GByte-Variante erhältlich. *(dr)*

www.pny-europe.com

GFI Software hat seine Lösung für Remote Monitoring und Remote Management, **MAX RemoteManagement**, um eine Komponente für die Fernwartung erweitert. MAX RemoteManagement ist ein Managed Service, der es Dienstleistern ermöglicht, die Server, Desktops, Netzwerke und Software ihrer Kunden kontinuierlich zu überwachen. Die Integration von Take Control in das RemoteManagement-Dashboard ermöglicht Dienstleistern nun, sich bei Problemen direkt in das entsprechende System einzuloggen und Fehler zu beheben. *(dr)*

www.gfisoftware.de

Server mit ruhigem Schlaf

Fujitsu bietet mit dem **PRIMERGY TX100 S2** einen neuen, energieeffizienten Einstiegsserver an. Das Modell richtet sich an kleinere und mittlere Unternehmen, die IT-Aufgaben wie Drucken im Netzwerk, zentrale Datenspeicherung oder Bereitstellung von Gruppenlaufwerken zentralisieren möchten. Der Server verfügt über ein sogenanntes 0-Watt-Feature. Anders als bei herkömmlichen Servern, die selbst, wenn sie ausgeschaltet sind, noch Reststrom beziehen, verbraucht der TX100 S2 im inaktiven Zustand keinerlei Strom mehr. Dabei ist er laut Hersteller so konzipiert, dass er sich problemlos regelmäßig abschalten und wieder booten lässt. Jedes System der PRIMERGY-Reihe sei für rund 5.000 Ein- und Ausschaltvorgänge getestet. Wartungsarbeiten und Updates kann der Administrator auch außerhalb der Arbeitszeiten in einem vorkonfigurierten Zeitfenster vornehmen, zu dem der Server sich dann automatisch einschaltet. Zur Verfügung stehen dabei bis zu vier 320 GByte SATA- oder 146 GByte SAS-Festplatten. Zudem bietet der Server bis zu 16 GByte RAM und einen Intel Core 2 Duo-Prozessor. Der Preis für den Server beginnt bei 700 Euro. *(dr)*

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

Flexible Stromzufuhr im Netz

Netgear präsentiert ein neues Modell der **ProSafe Smart** Switch-Familie: Der 8-Port GBit PoE Smart Switch **GS110TP** soll eine hohe Netzwerkperformance bieten und die Stromversorgung dynamisch regeln. Der Power-over-Ethernet-fähige Switch beliefert PoE-fähige Geräte mit Daten und Strom an allen acht 10/100/1000 MBit-Anschlüssen. Das Modell kann dabei die Energieversorgung priorisieren, so dass spezifische Ports den benötigten Strom auch dann garantiert erhalten, wenn der gesamte Energiebedarf das zur Verfügung stehende Limit übersteigt. Basierend auf der tatsächlich benötigten Energie des angeschlossenen Netzwerkgeräts weist der Smart-Switch den PoE-Ports den benötigten Strom dynamisch zu. Zusätzlich bietet der Switch zwei Small Form-factor Pluggable (SFP) Fiber-Anschlüsse für optionale Glasfaseranbindungen. An Sicherheitsfeatures bietet der Switch eine 802.1x-Authentifizierung, RADIUS sowie einen ACL (Access Control Lists)-Filter, um Datenverkehr bestimmter MAC- oder IP-Adressen zu erlauben oder zu unterbinden. Advanced QoS soll für ein optimales, zuverlässiges und flexibles Bandbreitenmanagement sorgen, während der Switch SNMP v1, 2c und v3 unterstützt. Die allgemeine Administration der Schaltstation erfolgt über das webbasierte "New Smart Control Center". Für rund 318 Euro ist das Gerät erhältlich. *(dr)*

Netgear: www.netgear.de

Der Smart Switch GS110TP von Netgear soll für die passende Stromzufuhr sorgen

Barracuda-Portfolio künftig auch virtuell

Barracuda Networks bietet sein gesamtes Lösungsportfolio für IT-Sicherheit sowie Netzwerk- und Storage-Lösungen künftig auch in virtualisierter Form an. Ab sofort erhältlich sind die **Barracuda Spam & Virus Firewall Vx** und das **Barracuda SSL VPN Vx**. Die **virtuellen Appliances** lassen sich dabei auch hochverfügbar nutzen und sind skalierbar. Steigen die Anforderungen, lässt sich die Kapazität erhöhen, ohne dass laut Hersteller Hard- oder Software ausgetauscht werden müssen. Die Virtual Appliances bieten Kunden die gleichen Plug-and-Play-Features wie die physischen Appliances und sollen sich auf beliebiger Hardware implementieren oder in vorhandene virtuelle Frameworks integrieren lassen. Die Virtual Appliances unterstützen aktuell die VMware ESX/ESXi-Plattform. Für die kommenden Monate kündigt der Hersteller die Unterstützung weiterer Plattformen an. Interessenten können sich sowohl die Barracuda Spam & Virus Firewall Vx als auch das Barracuda SSL VPN Vx als 30-Tage-Testversion kostenlos von der Herstellerseite herunterladen. *(dr)*

Barracuda Networks: www.barracuda.com/virtualization

IT-Administrator-Workshop "Windows 7" am 21. September 2010 in Karlsruhe

Gefährliche Klippen umschiffen

von John Pardey

ITANet Workshop-Partner: matrix42

Die Umstellung auf Windows 7 wird von den IT-Verantwortlichen in den Unternehmen aus verschiedenen Gründen ins Auge gefasst. Auf der einen Seite bietet der neue Microsoft-Client im Zusammenspiel mit dem Server 2008 R2 eine ganze Reihe von Features, die die Produktivität und Effizienz der IT steigern können, andererseits ist das "Auslassen" dieser Client-Generation vor dem Hintergrund des auslaufenden XP-Supports für viele Unternehmen keine Option. Letztendlich sind die Gründe für einen Umstieg nicht von Belang. Wenn es für die IT-Verantwortlichen und Administratoren darum geht, die Migration zu planen und durchzuführen, warten auf alle die gleichen Aufgaben und Herausforderungen. Unser Workshop soll helfen, die Klippen dieses Projekts zu umschiffen und Migration und Rollout möglichst reibungslos abzuwickeln.

Vor der tatsächlichen Umstellung der Endanwender auf Windows 7 steht natürlich eine gründliche Vorbereitung und Planung. Doch auch wenn sich schon jetzt herauskristallisiert hat, dass Windows 7 deutlich einfacher zu handhaben ist als sein wenig geliebter Vorgänger Vista, wissen die Dozenten unseres Workshops doch von einigen Hürden auf dem Weg zum Windows 7-Netzwerk zu berichten.

Migration bedarf genauer Planung

So müssen sich die IT-Abteilungen Aufgaben wie etwa der Profilmigration stellen. Auch eine genaue Untersuchung der Applikationen auf ihre Windows 7-Tauglichkeit ist unumgänglich und verbunden mit der Frage, wie mit nicht-kompatiblen Anwendungen verfahren wird. Hier bietet die Virtualisierung einige mögliche Vorgehensweisen, aber auch eine Strategie mit einem Windows XP/7-Parallelbetrieb ist denkbar.

Und da von XP kein direktes Upgrade auf Windows 7 möglich ist, stellt sich zudem die Frage, wie die Benutzerprofile zu migrieren sind – zu all diesen Themen geben unsere Workshopexperten den Teilnehmern wertvolle Tipps und Hinweise zur Umsetzung.

Der Rollout von Windows 7

Ist die Planung abgeschlossen und alle Kompatibilitätsfragen sind geklärt, geht es daran, Windows 7 im Unternehmen zu verteilen. Dabei wendet sich unser Workshop zunächst der Frage zu, wie Windows 7 für die automatische Softwareverteilung vorbereitet werden muss. Nachdem der Client derart präpariert worden ist, steht dann die tatsächliche Verteilung an und die Frage, wie sich beispielsweise die virtuellen Festplatten, die Windows 7 bietet, dabei nutzen lassen. Und natürlich ist so ein Rollout kaum ohne Tool-Unterstützung zu realisieren, weshalb wir im Workshop beispielhaft die Rollout-Unterstützung durch das MS Systems Center betrachten.

Somit will unser Workshopnachmittag helfen, den Umstieg auf Windows 7 so einfach wie möglich zu gestalten, indem er den Teilnehmern geeignete Vorgehensweisen vermittelt und zudem mögliche Werkzeuge des Rollouts untersucht. Wir freuen uns auf jeden Fall, Sie in Karlsruhe zu begrüßen.

ITANet
Die System und Netzwerk User Group

Die Agenda des Workshops

13.00 Uhr: Begrüßung

13.05 Uhr: Herausforderungen der Windows 7-Migration
- Hardwareauswahl
- Anwendungen portieren
- Parallelbetrieb mit Windows XP
- Migration der Benutzerprofile

Dozenten: Thorsten Christoffers und Thomas Wegener, Berater, sepago GmbH, Köln

14.30 Uhr: Kaffeepause

14.45 Uhr: Lösungen für die Windows 7-Migration: Empirum Client Life Cycle Management

Dozent: Roland Schäfer, matrix 42 AG

15.30 Uhr: Rollout von Windows 7
- Vorbereitung der Verteilung
- Automatische Installation
- Virtuelle Festplatten nutzen
- Unterstützung durch MS System Center

Dozenten: Thorsten Christoffers und Thomas Wegener, Berater, sepago GmbH, Köln

17.30 Uhr: Ende des Workshops

Ort: Der Blaue Reiter Designhotel, Amalienbadstr. 16, 76227 Karlsruhe

Teilnahmegebühren: Für IT-Administrator Abonnenten kostenlos.

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

Workshop "Windows 7" am 21. September 2010 in Karlsruhe

1&1 – DER PERFEKTE PARTNER FÜR WEBSITES

*

SOFTWARE INKLUSIVE

BEI DEN 1&1 WEBHOSTING PAKETEN DER NÄCHSTEN SEITE!*

NetObjects Fusion® ist eine umfangreiche Webdesign-Applikation, mit der sich auch anspruchsvolle Online-Anwendungen erstellen lassen, ohne eine einzige Zeile HTML-Code selbst schreiben zu müssen. Die exklusive 1&1 Edition enthält darüber hinaus mobile Templates für eine optimierte Anzeige der Website auf mobilen Endgeräten.

Adobe® Dreamweaver® CS4 ist die „Premium"-Lösung zur Realisierung hochwertiger Websites. In Kombination mit Adobe Device Central – exklusiv für 1&1 – kann man den generierten HTML-Code sowie Flash-Applikationen für mobile Endgeräte und Übertragungsparameter bequem in einem Emulator testen.

MEMBER OF united internet

PROFESSIONELLE WEBDESIGNER

GO MOBILE

Immer mehr Menschen nutzen BlackBerry, iPhone oder andere Smartphones, um im Internet zu surfen. Darum wird es immer wichtiger, dass Websites auch für die Ansicht auf mobilen Endgeräten optimiert sind. Bei 1&1 gibt's jetzt die Software dafür inklusive!*

- ✓ **Professionelles Webdesign – optimiert für mobile Endgeräte**
- ✓ **Hochwertige Software inklusive***
- ✓ **Mit exklusiven Templates für 1&1**

1&1

Jetzt informieren und bestellen:

0 26 02 / 96 91
0800 / 100 668

www.1und1.info

* NetObjects Fusion 1&1 Edition oder Adobe Dreamweaver CS4 inklusive z.B. bei 1&1 Homepage Professional, 6 Monate für 6,99 €/Monat, danach 14,99 €/Monat. Einmalige Einrichtungsgebühr 14,90 €. 12 Monate Mindestvertragslaufzeit. Software wird im 1&1 Kundenbereich zum Download bereitgestellt. Preise inkl. MwSt.

Im Vergleichstest: Messaging- und Groupware-Server

Fünf gegen Goliath

von Thomas Bär und Sandro Lucifora

Quelle: El Gaucho, Fotolia.com

Der Standard im Messaging-Umfeld ist zweifellos Microsoft Exchange. Doch in diesem großen Markt sind die Anforderungen der Anwender sehr unterschiedlich in Bezug auf Sicherheit, Administration oder auch den Preis. So stellen sich die fünf in unserem Vergleichstest untersuchten Messaging- und Groupware-Systeme dem Platzhirsch. Dabei nahm unser Expertenteam die Herausforderer IceWarp, Kerio Connect, MDaemon, Collax/Zarafa und Ipswitch IMAIL hinsichtlich zentraler Features wie Administration, Zugriff durch normale und mobile Benutzer und Sicherheit unter die Lupe.

Soll im Unternehmen tatsächlich Exchange abgelöst werden, dann ist aus Sicht des Budgetverantwortlichen sicher das Preis-Leistungs-Verhältnis ein entscheidendes Kriterium. Doch gerade bei E-Mail- und Groupwaresystemen kommt der Akzeptanz durch die Nutzer – Anwender, aber auch Administratoren – eine entscheidende Bedeutung zu. Für Anwender ist das E-Mailfrontend eines der wichtigsten Mittel der täglichen Arbeit und Features oder eine Bedienbarkeit, die zu deutlich hinter dem "Outlook-Standard" zurückbleiben, dürften Probleme bereiten. Daher haben wir diesen Aspekten in unserem Test besonderes Augenmerk gewidmet, dabei aber einen weiteren Teilbereich – die Sicherheit – nicht aus den Augen gelassen. Den kompletten Überblick über die Leistungsfähigkeit der fünf Systeme im Vergleich zu Exchange finden Sie in unserer abschließenden Tabelle.

IceWarp Server 10.1.1

Unser erster Testkandidat ist der IceWarp Server 10.1.1 vom gleichnamigen Hersteller aus Prag. Den einstigen Namen "Merak Mailserver" hat der Hersteller aus Marketinggründen abgelegt. In der Positionierung gegenüber dem Microsoft Exchange Server verweist der Hersteller darauf, dass seine Lösung insgesamt kostengünstiger und ressourcenschonender ist. Bis zur Version 9.x im Jahre 2009 war IceWarp in erster Linie auf die Grundfunktionen ausgerichtet: SMTP-Dienst, Anti-Spam oder Anti-Virus. Somit waren die primären Kunden kleinere und mittlere Unternehmen, die eine reine Mail-Lösung für den Firmeneinsatz suchten, beziehungsweise KMUs und größere Unternehmen, die den IceWarp als SMTP-Relay/Gateway einsetzen. Erst in der jüngsten Version wird der Fokus verstärkt auf Collaboration gesetzt.

Die komplette Produktdokumentation der Software selbst ist aktuell ausschließlich in englischer Sprache verfügbar, eine Übersetzung ins Deutsche ist laut Informationen des Herstellers jedoch angedacht. Die Oberflächen der Software, sowohl für den Anwender als auch den Administrator, lassen sich aber auf Deutsch einstellen.

Einfache Installation

Die Installation des Servers ist sehr einfach. Die vom Hersteller angekündigten 30 Minuten für die Installation des Servers sind in keinem Fall übertrieben. Nach dem knapp über 100 MByte großen Download wird der Einrichtungsvorgang von einem Assistenten begleitet. Das Installationspaket ist sowohl für die reguläre Installation als auch für die 30-Tage-Testversion geeignet. Eine Demoinstallation kann so durch die Aktivierung mit einem Lizenzschlüssel schnell zu einer Produktivinstallation werden.

Ohne die Eingabe einiger persönlicher Daten wie Name und E-Mailadresse lässt sich der IceWarp Server 10 leider nicht in Betrieb nehmen. Im nächsten Dialogfeld legt der Administrator den Installationstyp als "Standard" oder "Erweitert" fest. Die Standard-Variante wird laut diesem Dialogfenster für eine Installation mit "weniger als 500 Knoten" empfohlen. Größere In-

Systemvoraussetzungen

Typischer 32 Bit-Windows-PC/Server, ab Windows NT/98 – auf x64-Windows als 32 Bit-Task lauffähig; x86-Linux-Distributionen, Red Hat Enterprise Linux 4, 5 oder CentOS (eine betriebssystemunabhängige PHP5-Umgebung wird mitgeliefert). Die Linux-Variante erscheint stets einige Zeit verzögert zur Windows-Version.

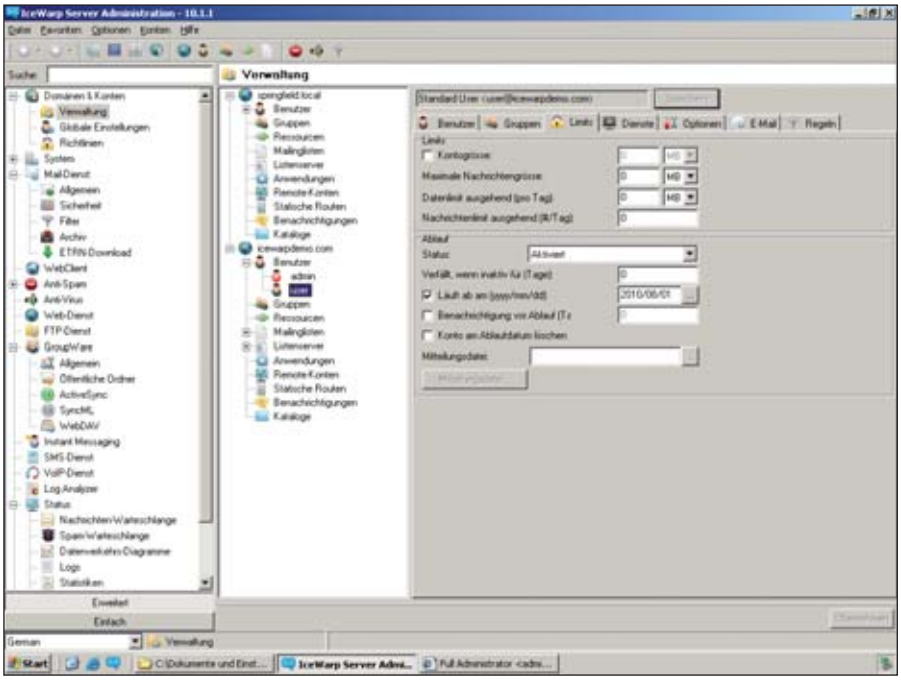


Bild 1: Die Administrationsoberfläche des IceWarp-Servers bietet alles, was für die Administration notwendig ist: von der Benutzeranlage, LDAP-Sync, Backup bis hin zur Logfile-Analyse

stallationen vom Typ "Erweitert" benötigen eine externe Datenbanksoftware, ansonsten kommt SQLite als Basis zum Einsatz. Die direkte Erklärung beider Installationstypen im Dialogfenster ist zwar löblich, doch bleibt die Frage, warum hier im Zusammenhang mit Mailservern von Knoten anstatt Mailboxen die Rede ist. Die Installation selbst ist nach der Eingabe einiger Eckdaten in wenigen Minuten erledigt. Unter "Addons" findet sich eine Demo-Konfiguration, die sich hervorragend als Anschauungsobjekt für die eigene Parametrierung eignet. Im Anschluss an die Einrichtung wird ein Ordner mit den Verknüpfungen zu Administration und Clients heruntergeladen; die Ordner zu WebAdmin und WebClient werden voreingeblendet.

Client- und Anwenderfunktionen

Obwohl erst mit der Version 10 die Groupware-Funktionen eingefügt wurden, bedient IceWarp doch bereits alle Anforderungen einer modernen Kommunikationsumgebung. Öffentliche Adressbücher, Kalender, Aufgaben, Notizen, Ordner und Journale gehören ebenso zu den Funktionen wie das Abonnieren von Öffentlichen Ordnern, Gruppen-Konten oder Benutzer-Konten von Kollegen. Eine nahtlose Integration in Microsoft Outlook ist dank eines speziellen Outlook Connectors gewährleistet. In den IceWarp-Server ist ein WebDAV-Modul für den Zugriff auf öffentliche Ordner integriert. Die Synchronisation zu mobilen Geräten oder PIM-Applikationen wird über die Standard-Protokolle SyncML und CalDAV realisiert. Über vCard, vCal oder vFreeBusy – ebenfalls Standardverfahren – ist ein Austausch von Kontakt- und Kalenderfunktionen auch zu externen Systemen möglich.

Der Webclient von IceWarp lehnt sich bei den Grundfunktionen am Standard an, geht jedoch im Detail bei vielen Funktionen weiter: Farbliche Hinterlegung von Terminen im Kalender, Steuerung von Spam-Einstellungen, das Führen der Black- und White-List – je nach Einstellungen des Administratoren können Benutzer dies selbst festlegen. Sofern ein Anwender je mit einem typischen Webmail-Client gearbeitet hat, wird er sich intuitiv bei IceWarp zurechtfinden. Kalenderfunktionen, beispielsweise das Freischalten für Kollegen und Mitarbeiter oder Zugriffsregelungen, sind mit IceWarp kein Problem. Neben dem Webmailer bietet IceWarp zudem einen eigenen Desktop-Client als Ersatz für Microsoft Outlook an.

Durch die Integration des optionalen IceWarp SMS-Servers wird die Weiterleitung von wichtigen Nachrichten, Benachrichtigungen oder der Versand von Massen-SMS ermöglicht. Berechtigte Benutzer können SMS direkt über Webmail oder jeden Mailclient durch Eingabe einer speziellen Syntax versenden. Antwortet der

Migration von Exchange

IceWarp bietet für die Migration von Exchange ein Migrations-Tool als öffentliche Beta-Version an. Mithilfe dieses Programms können Konten, Ordnerhierarchien, Nachrichten, Kalender, Aufgaben, Notizen und Kontakte zu IceWarp migriert werden. Anhänge an Kontakten und Aufgaben, Erinnerungen und öffentliche Ordner indes lassen sich aktuell nicht migrieren.

MDaemon wird mit einem Migrationstool ausgeliefert, mit dem sich Benutzer, Mailboxen, öffentliche Ordner und Einstellungen aus Microsoft Exchange extrahieren und in MDaemon importieren lassen. Die vorhandene Hardware kann dabei weiterverwendet werden, da MDaemon im Gegensatz zu Microsoft Exchange 2007/2010 nicht zwingend auf eine x64-Umgebung angewiesen ist.

Die Umstellung der Daten von Exchange zu **Kerio Connect 7** wird durch einen bedienerfreundlichen Assistenten unterstützt, der ebenfalls kostenlos erhältlich ist. Ab Exchange 5.5 bis zu Exchange 2007 werden neben den Benutzerkonten und Verteilerlisten auch alle Ordner und Unterordner, inklusive Ordneroptionen, Kalender, Kontakte, Notizen, Aufgaben und Öffentliche Ordner, übertragen.

Zarafa bietet die Datenübernahme mittels PST-Datei an. Um nicht auf jedem Client das Benutzerkonto als PST zu exportieren, bietet sich das Microsoft-Tool Exmerge (Exchange Mailbox Merge) an. Damit kann der Server-Administrator Daten aus Postfächern in eine PST-Datei extrahieren. Auf der Gegenseite kommt das Zarafa Migration Tool zum Einsatz. Hiermit werden die im PST-File befindlichen Daten auf den Groupware-Server übertragen. Im Test übertrugen wir fünf Postfächer auf diese Weise und konnten keine Probleme feststellen.

Zur automatischen Übernahme der Daten von Exchange zu **IMAIL** steht kein direkter Weg und kein Tool zur Verfügung. Anwender können die Daten über Outlook, im Zuge der Einrichtung des Workgroup-Client, aus der bestehenden PST-Datei zum IMAIL-Server übernehmen. Jedoch bleiben dabei Einstellungen wie die Abwesenheits-Nachricht und Regeln auf der Strecke.

Empfänger per SMS auf die Nachricht, wird diese vom Mailclient interpretiert und wieder auf die sendende E-Mailadresse weitergeleitet. In kleineren Umgebungen werden per Kabel angebundene GSM-Modems oder Handys unterstützt. Als Unternehmenslösung empfiehlt sich die Anbindung mehrerer solcher GSM-Modems oder aber die Anbindung eines SMS-Gateways. Eine SIP-Server-Integration erlaubt den Verbindungsaufbau via VoIP-Server aus dem Webmail-Client oder Microsoft Outlook. Desweiteren bietet der Hersteller eine integrierte Instant-Messaging-Lösung für den Firmeneinsatz auf Basis von XMPP (Extensible Messaging and Presence Protocol), besser bekannt als Jabber.

Hersteller

IceWarp / i-TEC Innovative Technologies GmbH
www.icewarp.de

Preis

Die Preisgestaltung ist abhängig von den gewählten Modulen. In der kleinsten Ausbaustufe (ohne zusätzliche Module) mit zehn Client-Zugriffslizenzen liegt der Preis bei rund 245 Euro. Inklusive aller Features (SMS, Webmailer, IM et cetera) kostet die Software 409 Euro für zehn Benutzer, 1.519 Euro für 50 Benutzer, 5.475 Euro für 250 Benutzer und rund 20.000 Euro für 1.000 Benutzer.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Systemanforderung	8
Flexibilität	9
Funktionsumfang Webmailer	8
Collaboration	9
Preis/Leistung	8
Gesamtwertung	**8,6**

IceWarp Server 10

Ob es dem Administrator nun gefällt oder nicht: Die Benutzer werden mobiler und Daten müssen jederzeit verfügbar sein. Die Synchronisation in Echtzeit, bei IceWarp das sogenannte "PUSH" mit ActiveSync, unterstützt den Trend zu mehr Mobilität. Die Nutzung von E-Mail, Kalendern, Kontakten und Aufgaben ist überall und jederzeit mit beliebigen Mailclients und jedem aktuellen mobilen Endgerät wie iPhone, Windows Mobile, Blackberry oder Android möglich. Der Webmailer erlaubt zudem eine funktionell reduzierte Darstellung speziell für Kleinstcomputer oder Smartphones.

Intuitive Administration

IceWarp bietet eine traditionelle Management-Software mit zwei Baumstrukturen für alle Objekte. Auch ohne einen Blick in die Anleitung findet sich ein versierter Admin sofort zurecht. Alle Einstellungen werden pro Domäne vorgenommen, somit kann der IceWarp-Server für unterschiedliche Adressräume unterschiedlich konfiguriert werden. Neben der eigenen Benutzerverwaltung, die sich auf die wichtigsten Informationen zu einem Benutzer beschränkt, verfügt der IceWarp zudem über eine Synchronisation mit einem Verzeichnisdienst.

Der IceWarp-Server liefert auf den ersten Blick alles, was für eine ordentliche Administration benötigt wird. In der Menüstruktur finden sich ein Log-Analyzer, der Status der Nachrichtenschlange, Statistiken und der Zugriff auf die Spam-Schlange. Leider sind die Auswertemöglichkeiten eingeschränkt, beispielsweise existiert im Datenverkehrs-Diagramm keine Möglichkeit, sich die Uhrzeiten genauer anzuschauen – ein 30 Minuten-Raster ist stets vorgegeben. Durch einen Export der Log-Dateien ist eine Auswertung mit zusätzlicher Software jedoch möglich.

Sicherheit

Was die Sicherheitsfunktionen angeht, so ist der IceWarp mit einem eingebauten Virenschutz und einer Anti-Spam-Funktion auf Basis des SpamAssassin gut gerüstet. Die Einstellungsmöglichkeiten lassen keine Wünsche offen und selbst Gimmicks wie "EICAR-Test-Virus senden" sind eingebaut – wer schon einmal versucht hat, den EICAR zu Testzwecken zu versenden, weiß, welchen Aufwand das machen kann, bis die Workstation dies überhaupt einmal zulässt.

Die Entwicklung der geplanten Version 11 geht weiterhin klar mehr in Richtung Groupware und Unified Communications. Mit der geplanten Integration eines Radius-Servers wird die Einsetzbarkeit in großen Unternehmen verbessert werden. Auch Clustering und Load-Balancing dürften erweitert werden.

Fazit

Der IceWarp Server ist ein insgesamt ausgereifter Mail- und Groupware-Server mit vielfältigen Einsatzmöglichkeiten. Besonders im Vergleich zu Microsoft Exchange sind sowohl Installation als auch Betrieb deutlich einfacher. Dank der geringeren Systemanforderungen ist zudem der Betrieb auf leistungsschwächerer Hardware möglich. Die vielen angebotenen Zusatzfeatures erlauben eine Leistungserweiterung in der Zukunft.

MDaemon Mailserver Pro V11

Der MDaemon Mailserver wird bereits seit 1997 am deutschen Markt vertrieben und hat aktuell die Version 11 erreicht. Die nächste anstehende Version – 12 – dürfte zum Erscheinungstermin dieser Ausgabe bereits fertiggestellt sein. Dank der beiden verfügbaren Varianten "Standard" und "Pro" werden nur die wirklich im Unternehmen benötigten Features bereitgestellt. Während die Standard-Version

Windows XP/Vista/2000/2003/2008 (inklusive x64-Varianten); Computer mit Pentium III 500 MHz (oder höher) Prozessor, 512 MByte RAM Arbeitsspeicher (1 GByte empfohlen); Festplattenkapazität 100 MByte zuzüglich Speicherplatz für E-Mails; Microsoft Internet Explorer 5.5 (oder höher).

Systemvoraussetzungen

1&1 – SOFTWARE UND SPAREN!

Bei 1&1 ist jetzt hochwertige Webdesign-Software inklusive – außerdem profitieren Sie im September von sensationellen Sparangeboten!

1&1 HOMEPAGE PERFECT

- 2 Domains (.de, .com, .net, .org, .biz, .info, .name, .at, .eu)
- NEU: 4 GB Webspace
- NEU: 5 MySQL-Datenbank
- SSI, PHP4, PHP5 inkl. Zend Framework, PHP6 (beta)
- NEU: 250 E-Mail Postfächer
- 250 Online-Office Accounts
- NEU: 4 FTP-Zugänge
- NEU: NetObjects Fusion® 1&1 Edition

6 Monate 50 % sparen!*

~~6,99 €/Monat~~

2,99 €/Monat*

50 % für 6 Monate, danach 6,99 €/Monat*

1&1 HOMEPAGE PROFESSIONAL

- NEU: 5 Domains (.de, .com, .net, .org, .biz, .info, .name, .at, .eu)
- 5 GB Webspace
- NEU: 10 MySQL-Datenbanken
- SSI, PHP4, PHP5 inkl. Zend Framework, PHP6 (beta)
- 500 E-Mail Postfächer
- 500 Online-Office Accounts
- 20 FTP-Zugänge
- NEU: NetObjects Fusion® 1&1 Edition oder Adobe® Dreamweaver® CS4

6 Monate 50 % sparen!*

~~14,99 €/Monat~~

6,99 €/Monat*

50 % für 6 Monate, danach 14,99 €/Monat*

1&1 HOMEPAGE PROFESSIONAL PLUS

- NEU: 12 Domains (.de, .com, .net, .org, .biz, .info, .name, .at, .eu)
- NEU: 10 GB Webspace
- NEU: 20 MySQL-Datenbanken
- SSI, PHP4, PHP5 inkl. Zend Framework, PHP6 (beta)
- 1.000 E-Mail Postfächer
- 1.000 Online-Office Accounts
- Shell-Zugang, CronJobs
- 50 FTP-Zugänge
- NEU: NetObjects Fusion® 1&1 Edition oder Adobe® Dreamweaver® CS4

6 Monate 50 % sparen!*

~~29,99 €/Monat~~

14,99 €/Monat*

50 % für 6 Monate, danach 29,99 €/Monat*

DOMAIN-ANGEBOTE:

.de, .eu, .com, .net, .org, .at

12 Monate für 0,– € danach ab 0,49 €/Monat*

0,– €/Monat*

1&1

MEMBER OF united internet

Jetzt informieren und bestellen:

0 26 02 / 96 91

0800 / 100 668

www.1und1.info

* 1&1 Homepage Perfect 6 Monate 2,99 €/Monat, danch 6,99 €/Monat, 1&1 Homepage Professional 6 Monate 6,99€/Monat, danach 14,99 €/Monat, 1&1 Homepage Professional Plus 6 Monate 14,99 €/Monat, danach 29,99 €/Monat. Einmalige Einrichtungsgebühr 14,90 € (9,60 € bei 1&1 Homepage Perfect).12 Monate Mindestvertragslaufzeit. Software wird im 1&1 Kundenbereich zum Download bereitgestellt. Preise inkl. MwSt.

.de, .eu, .com, .net, .org, .at Domain 12 Monate für 0,– €/Monat danach, .de 0,49 €/Monat, .eu, .com, .net, .org, 1,49 €/Monat, .at 1,99 €/Monat. Einmalige Einrichtungsgebühr 9,60 €. Preise inkl. MwSt.

eher Basisfunktionen bietet, sind in der Pro-Version Funktionen wie Integration des Blackberry Internet Services (BIS), Links auf Dateianlagen oder die Unterstützung für den Betrieb in verteilten Domänen, sprich mehrere Mailserver, die eine einzige Domäne abbilden, nutzbar. Im direkten Vergleich zum weit verbreiteten Microsoft Exchange weist der Hersteller darauf hin, dass sich MDaemon Mailserver deutlich einfacher installieren und administrieren lässt und gleichzeitig einen großen Funktionsumfang mit voller Groupware-Funktionalität zu einem geringeren Preis anbietet.

Installation mit Hürden

Der MDaemon besteht aus verschiedenen Modulen, die rund um den Mailserver das Gesamtsystem ergeben. Für jedes dieser Module ist ein passender Key erforderlich – auch für die 30 Tage-Testversion, die frei im Internet heruntergeladen werden kann.

Die Installation ist dank gut beschriebener Dialogfenster und einer ausgezeichneten Dokumentations- und Checkliste des Distributors einfach. Hier und da ist der Einrichtungsvorgang jedoch etwas holperig: Im ersten Dialogfenster wird nach der ersten Domain-Adresse und dem POP/IMAP-Server gefragt. Nach Eingabe dieser beiden Werte ist das erste Benutzerkonto anzulegen – jedoch ist ein Klick auf "Zurück", um in den vorherigen Dialog zu gelangen, nicht mehr möglich. Nach Eingabe des Benutzers ließ sich jedoch die Schaltfläche "Weiter" nicht mehr anklicken und nur durch einen Mausklick auf "X" wurde der Installationsvorgang abgebrochen. Beim erneuten Installationsvorgang fand der Installer die zuvor angelegten Daten und installierte in einem Rutsch durch. Nach der Basisinstallation bietet ein Dialogfenster das Herunterladen der beiden wichtigsten Zusatzmodule "SecurityPlus" und "Outlook-Connector" an.

Der Outlook-Connector besteht wiederum aus zwei Komponenten: dem Plug-In für Microsoft Outlook selbst und dem Connector für den Mailserver. Ein einheitlicher Installer für die große Version des MDaemon wäre möglicherweise die einfachere Lösung gewesen. Die Installation der zusätzlichen Module scheiterte auch zunächst daran, dass die Serverinstallation nicht erkannt wurde – erst nachdem der Server neugestartet worden war, ließen sich diese Module einrichten. Bei einem Programm, das seit nunmehr 13 Jahren am Markt ist, dürften solche "Schnitzer" eigentlich nicht mehr vorkommen.

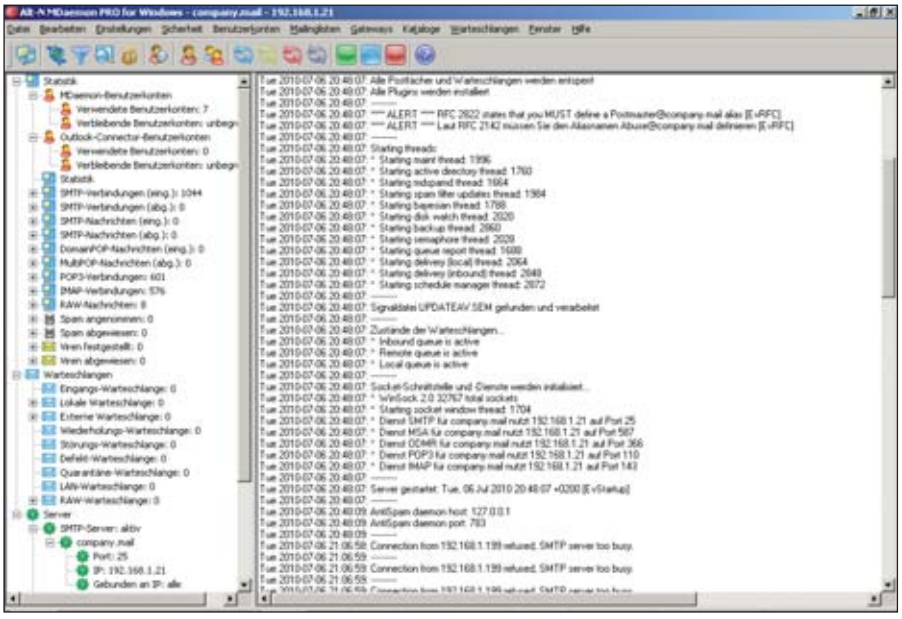


Bild 2: Auf den ersten Blick vielleicht unübersichtlich, erlaubt die Administrationsoberfläche des MDaemon Mailservers dennoch einen sehr schnellen Zugriff auf alle benötigten Funktionen oder Reports

Transparente Client- und Anwenderfunktionen

Alle wichtigen Funktionen, wie etwa die Anlage eines Benutzers, sind vollkommen selbsterklärend. Nach der Einrichtung der ersten E-Mailadresse und dem Testzugriff erlebten wir eine positive Überraschung: Der neue Benutzer erhält vom System eine Begrüßungs-E-Mail mit den wichtigsten Informationen zum Konto, inklusive Adresse des Webmail-Accounts. Der Webmailer selbst bietet verschiedene Designs, unterschiedliche Sprachen und ist, was Bedienung und Funktionsumfang betrifft, den gängigen Webmaildiensten ähnlich. Wird ein aktueller Browser eingesetzt, so sieht der so genannte "WorldClient" beinahe aus wie ein echtes Outlook – selbst Notizzettel lassen sich frei verschieben und bearbeiten.

Die Kalenderfunktion bei MDaemon entspricht der bekannten Darstellung. Die Freigabe von Ordnern für andere Benutzer oder das Öffnen solcher Ordner ist sehr einfach gelöst und erklärt sich ebenfalls von selbst. Selbiges gilt auch für gemeinsame Verteilerlisten oder Adressbücher. Verteilerlisten lassen sich sowohl vom Benutzer selbst erstellen als auch auf Serverebene vom Administrator konfigurieren. Äußerst pfiffig ist ein Leistungsmerkmal, das in der jüngsten Version überarbeitet wurde: Die Verlinkung von Dateianlagen. Diese Funktion nimmt die Dateianlagen aus E-Mails und speichert sie lokal auf dem MDaemon-Server. Statt der eigentlichen Dateianlage fügt MDaemon schlicht die URL zur Datei in die Nachricht ein. Somit wird die eigentliche Datei erst bei Bedarf tatsächlich bewegt, was sowohl auf der Server- als auch Client-Seite Bandbreite und Speicherplatz spart.

Mobile Clients

MDaemon unterstützt in der aktuellen Version Open Source SyncML-Clients auf Basis von Funambol Version 8.0. Gleichzeitig unterstützt MDaemon den BlackBerry

Internet Service (BIS). Nutzer des BIS können ihr E-Mail-Benutzerkonto in ihr BlackBerry-Smartphone integrieren und dadurch Push-Mail und verbesserte Verarbeitung von E-Mail-Nachrichten nutzen. Nachrichten, die der Anwender auf dem Endgerät verfasst, werden jetzt zur Zustellung an MDaemon übermittelt – nicht mehr über die BIS-Server. Für andere Geräte, wie zum Beispiel Smartphones, wird weiterhin IMAP4 für die E-Mails genutzt und SyncML für die anderen Daten (Kontakte, Kalender, Aufgaben und Notizen).

Administrative Funktionen

Nach dem zuvor beschriebenen, kurzen Durcheinander bei der Installation gibt ein Doppelklick auf das Programm-Icon den Blick auf die Administrations-Oberfläche frei. Zunächst einmal fühlt sich der Administrator von einer schier endlosen Aneinanderreihung von Einträgen in der Baumstruktur erschlagen. Auf der anderen Seite hat diese Form der Darstellung durchaus ihren Charme: Ein wildes Klicken in die endlosen Tiefen von Eigenschaften-Menüs, wie es von Exchange her bekannt ist, bleibt dem Administrator erspart. Er hat jedes Kommando und jede Einstellung sofort im Zugriff.

Und den Administratoren mangelt es beim MDaemon wahrlich nicht an Optionen und Stellschrauben, mit denen sich das System auf individuelle Wünsche anpassen lässt. Protokolle und Übersichten finden sich zu allen gebräuchlichen Einheiten. Im Vergleich zu Microsoft Exchange ist der zügige und einfache Zugriff auf die Warteschlangen ein echter Pluspunkt. Was und warum in einer Queue steckt, lässt sich sehr einfach und schnell herausfinden.

In der Voreinstellung sichert der Server automatisch um Mitternacht die Konfigurationsdateien im INI/DAT-Format in ein Backup-Verzeichnis. Die Nachrichten selbst werden als MSG-Dateien gespeichert und können ebenfalls durch einfaches Kopieren in das Postfachverzeichnis wiederhergestellt werden. Als Benutzerdatenbank verwendet MDaemon entweder eine lokale Datei mit Namen *USERLIST.DAT*, einen LDAP-Verzeichnisdienst oder eine beliebige über ODBC angebundene Datenbank. Im Zusammenspiel von Active Directory mit dem MDaemon kann dieser die eigenen Benutzerkonten automatisch anlegen, aktualisieren, löschen und sperren, wenn die zugehörigen Benutzerkonten im Active Directory geändert werden.

Eine Automatisierung des MDaemon über eine eigene API ist ebenfalls möglich. Der Server reagiert zudem auf eine Reihe von Dateien, die sehr vielseitig eingesetzt werden können – die sogenannten Signal- oder Semaphore-Dateien. MDaemon prüft das Unterverzeichnis "\APP\" regelmäßig auf das Vorhandensein solcher Elemente. Wird eine Datei erkannt, so werden die mit ihr verknüpften Aktionen ausgeführt und die Datei danach gelöscht. Hier-

Hersteller
Alt-N technologies
www.mdaemon.de
Deutschland-Distributor: EBERTLANG Distribution GmbH

Preis
In den Ausbaustufen 50 / 100 / 250 Clients kostet der MDaemon-Mailserver 750 / 1.003 / 1.235 Euro (alle Preise beinhalten ein Jahr Aktualisierungsgarantie). Der MDaemon Outlook Connector kostet zusätzlich 514 / 711 / 1.382 Euro. Weitere Module, wie beispielsweise MDaemon Security Plus oder das SMS-Gateway, sind optional und werden ebenfalls kostenpflichtig lizenziert. Eine im Leistungsumfang reduzierte Version für bis zu fünf Benutzer trägt den Namen MDaemon FREE und ist kostenlos.

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

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

Systemanforderung	9
Flexibilität	8
Funktionsumfang Webmailer	10
Collaboration	8
Preis/Leistung	9

Gesamtwertung	**8,8**

MDaemon Mailserver Pro V11

mit können Systemverwalter und Software-Entwickler MDaemon leicht steuern, ohne die Benutzeroberfläche zu bedienen.

Umfassende Sicherheit

In der Basisvariante des Servers ist ein Spam-Schutz mit den derzeit gebräuchlichen Methoden der Bekämpfung integriert: Black- und Whiteliste sowie ein selbstlernender Bayes'scher Filter. Mit diesen Mitteln lässt sich grundsätzlich auch ohne eine vorgelagerte Anti-Spam-Technik eine durchaus gute Spam-Filterung erreichen.

MDaemon bietet jedoch mehr – selbst die Auswertung von frei definierten "Honeypots", sprich E-Mailadressen, die eigentlich nie von "ordentlicher Post" erreicht werden können, gehört zum Repertoire. Für den Virenschutz setzt der Hersteller Alt-N auf die Integration einer Kaspersky AV-Engine, die hinlänglich bekannt sein dürfte.

Fazit

Von den Unzulänglichkeiten bei der Einrichtung einmal abgesehen, versieht der MDaemon einen ordentlichen Dienst. Die komplette Verwaltungsoberfläche wirkt ein wenig "old school", dafür bietet der Server sehr viele Steuerungsmechanismen. Wer sehr viel individuell einstellen und konfigurieren will oder muss, der wird am MDaemon ganz besondere Freude haben. Auf der Benutzerseite präsentiert sich das Webinterface modern und intuitiv und wird sicherlich problemlos angenommen werden.

Kerio Connect 7

Aus der Welt von Apple kommt Kerio Connect 7, vormals als Kerio MailServer bekannt geworden. Seit längerem auch als Windows- und Linux-Version verfügbar, hat die aktuelle Version eine technische und funktionale Runderneuerung erhalten. Bereits in der IT-Administrator-Ausgabe April 2009 testeten wir die Windows-Version des Vorgängers, weshalb wir uns im aktuellen Test auf die Linux-Variante fokussieren.

Kerio verzichtet auf ein eigenes Frontend und bedient sich als Client vorrangig Outlook ab Version 2003. Dass der Hersteller auf vorhandene Client-Lösungen zurückgreift, ist grundsätzlich zu begrüßen, da der Anwender so weiter mit seiner gewohnten Umgebung arbeiten kann. Als Client dient jede Software, die mit IMAP-Postfächern arbeitet – jedoch nur mit Outlook oder dem Web-Frontend ist der volle Groupware-Funktionsumfang, wie Kalender und Aufgaben, verfügbar und sinnvoll zu nutzen.

Zügige Installation

Kerio Connect 7 zeigt sich unter Windows als Ein-Klick-Installation schnell betriebsbereit. Für die einzelnen Linux-Distribu-

Intelligente Technologien für einen smarten Planeten

Es ist Zeit, intelligente Fragen zu stellen.

Was genau sagt ein Benchmark aus? In den letzten fünf Jahren belegte IBM DB2® Power Systems™ bei den drei wichtigsten Performance-Benchmarks der Industrie den ersten Platz länger als Oracle und Microsoft zusammen.[1] Aber sollten wir von unserer IT nicht mehr erwarten, als einfach nur Leistung zu liefern? Was wirklich zählt, ist kein theoretisches Leistungsmaß, sondern wie Unternehmen diese Leistung für sich nutzen können. Globe Telecom zum Beispiel nutzt eine Service Delivery Platform von IBM, um den Umsatz um 112 % zu steigern. EuResist verwendet ein integriertes Analysesystem, um die individuelle Wirkstoffkombination für HIV-Patienten vorherzusagen – mit einem Behandlungserfolg von 78 %. Und Dubai Gold & Commodities Exchange nutzt IBM Security Services, um eine Systemverfügbarkeit von mehr als 99,9 % zu erzielen. Das sind die Benchmarks, die auf einem smarten Planeten wirklich wichtig sind.

Smarte Unternehmen brauchen intelligente Software, Systeme und Services.
Machen wir den Planeten ein bisschen smarter. **ibm.com**/questions/de

Holen Sie sich die Antworten auf Ihre Fragen auf der
IBM SmarterSystems Tour2010:
Optimierung von Software, Hardware & Services.
In Deutschland am 23. September in Frankfurt
Anmeldung unter: **ibm.com**/de/events/systemstour

[1] Basis: Anzahl der Tage als Leistungsführer für die 3-Tier SD Benchmarks von TPC-C, TPC-H 10TB und SAP zwischen dem 1. Juni 2005 und dem 1. Juni 2010 ermittelt. Mehr Informationen finden Sie unter http://www.tpc.org und http://www.sap.com/solutions/benchmark. TPC, TPC-C und TPC-H sind Marken oder eingetragene Marken von TPC. IBM, das IBM Logo, ibm.com, das Blitzzeichen des Planeten, IBM DB2 sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Andere Namen von Firmen, Produkten und Dienstleistungen können Marken oder eingetragene Marken ihrer jeweiligen Inhaber sein. © 2010 IBM Corporation. Alle Rechte vorbehalten. O&M IBM CA 8/10a

tionen stehen angepasste Installationspakete zur Verfügung. Unter Novell open SUSE 11.1 mussten wir nur aus dem vorhandenen RPM-Paket installieren. Dabei wies die Routine zu Anfang auf die fehlende *libstdc++.so.5* hin, die wir mit dem compat-libstdc++-33 RPM-Paket nachträglich installierten. Für den Einsatz als virtueller Server unter VMware oder Parallels liefert der Hersteller auch fertige Appliances auf Basis von CentOS 5.3 aus. Während der Installation werden zur Grundeinrichtung die Hauptdomain für den E-Mailverkehr sowie die Anmeldedaten für den Administrator abgefragt. In der Vorgängerversion bemängelten wir, dass keine Lösung verfügbar war, um den Domain-Namen im Nachhinein zu ändern. Dies hat sich zwischenzeitlich geändert, so dass zum Beispiel der Wechsel von .de auf .com möglich ist. Dann muss jedoch die Anpassung von bereits vorhandenen E-Mailadressen und -Filtern manuell erfolgen.

Aufgeräumte Administration

Klar und logisch aufgebaut zeigt sich die Administration von Kerio Connect 7. Ein großer Nachteil von Exchange ist, dass der Administrator schon einiges an Fachwissen benötigt, um eine vernünftige Administration vornehmen zu können. Der Kerio Connect-Verwalter kommt mit gutem allgemeinem Administratoren-Wissen aus. Die Weboberfläche spiegelt optisch annähernd, in der Bedienbarkeit zu 100 Prozent, die Windows-Administrations-Konsole wider. Sauber strukturiert in die Bereiche "Konfiguration" und "Domäneneinstellungen" erhält der Betreiber unter den Punkten "Status" und "Protokolle" auch Echtzeitinformationen über das System. Die Benutzer werden wahlweise lokal angelegt oder aus einem Active Directory oder Novell eDirectory importiert. Die lokale Authentifizierung erfolgt über die interne Benutzerdatenbank oder gegen Linux PAM beziehungsweise Kerberos 5. Genauso einfach sind auch die Funktionen für das Anlegen von Gruppen, Domain- und E-Mail-Aliasen und weiterer Konfigurationen.

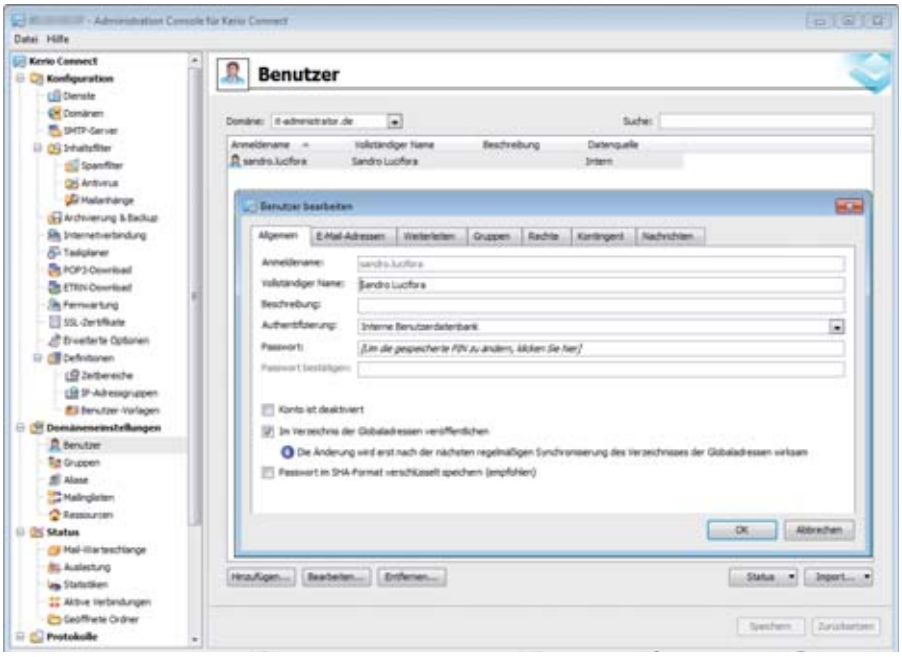


Bild 3: Die Kerio-Administrationskonsole kommt aufgeräumt und klar strukturiert daher

Der POP3-Download sammelt verschiedene POP3-Konten und verteilt sie auf dem System. Wenn zum Beispiel ein Wildcard-Konto abgerufen wird, verteilt Connect Nachrichten anhand der E-Mailadresse in der Kopfzeile an den internen Empfänger. Wer Kerio Connect als Mailserver einsetzen, ihn aber dennoch nicht ins Internet stellen möchte, kann ihn auch mit dem ETRN-Protokoll konfigurieren. Insgesamt benötigt die Software noch nicht mal einen Datenbank-Server, sondern verwaltet alle Informationen intern. Daraus ergibt sich, dass die klassische Zielgruppe des Produktes Firmen mit bis zu 150 Anwendern sind. Der Hersteller gibt bis zu 1.000 User als möglich an, was jedoch eher die Ausnahme sein dürfte.

Ausgefeilte Anwenderfunktionen

Hauptaufgabe des Servers ist die Zusammenarbeit in und von Gruppen. Hier steht Kerio Connect 7 dem Primus Microsoft Exchange in nichts nach und stellt neben E-Mail auch Kalender und Kontakte sowie das Journal, Notizen und Aufgaben zur Verfügung. Der Zugriff auf freigegebene als auch Öffentliche Ordner erfolgt gewohnt sicher und zuverlässig. Die für die Terminplanung unerlässliche frei/gebucht-Auskunft funktionierte im Test ebenso problemlos wie der Zugriff auf globale Adresslisten.

Der Umgang mit "Ressourcen", wie Räume und Geräte, stellt bei Kerio Connect einen eigenen Funktionspunkt dar und ist um einiges komfortabler gelöst als bei Exchange. Im entsprechenden Administrationsbereich werden Ressourcen als Raum oder Ausrüstung angelegt. Uns fehlte hierbei noch die Typisierung als Fahrzeug oder besser das Anlegen eigener Typisierungen. In der Terminplanung wird die benötigte Ressource dann einfach als solche gebucht. Schön ist, dass die zuvor als Raum angelegte und im Termin gebuchte Ressource dann auch im Termin unter Ort voreingestellt ist.

Der Einsatz von Outlook – im Test nutzten wir Outlook 2007 – erfolgt nach der Installation des Kerio Outlook Connectors.

Systemvoraussetzungen

Server ab 1 GHz CPU, 512 MByte Speicher (empfohlen 2 GHz und 1 GByte RAM); Windows ab Windows XP, Server ab 2003, Red Hat Linux ab 5.2, open SUSE 10.0-10.3 und ab 11.0, Debian ab 5.0, Ubuntu ab 8.04 TLS; Apple G4 oder G5 mit 2 GByte RAM (empfohlen), Mac OS X ab 10.4 Tiger

Dieser ist als On- und Offline-Version für den stationären oder mobilen Einsatz kostenlos verfügbar und wird auf jedem Client installiert, auf dem Outlook gestartet wird.

Der mobilen Unterstützung hat Kerio eine hohe Aufmerksamkeit gewidmet. Daher werden alle derzeit erdenklichen Smartphones – angefangen beim Apple iPhone, Windows Mobile-Geräte sogar mit dem OS vor Version 5.0, über den Treo Palm, BlackBerry bis hin zu Nokias Symbian OS – unterstützt. Dabei ist Direct Push genauso selbstverständlich wie die Synchronisation der jeweiligen System-Kalender und -Kontakte. Für alle anderen mobilen Telefone liefert der Hersteller eine Mini-Webmail-Version, die sich mit jedem mobilen Browser aufrufen lässt.

Der Webmailer selber, der als vollwertiger Ersatz für jeden anderen Client zu sehen ist, gibt in vollem Umfang alle Funktionen wieder. So greift der Nutzer mit dem Web-Frontend auf alle persönlichen und freigegebenen Daten zu. Im Gegensatz zu Exchange ist auch die webbasierte Rechtschreibprüfung lernfähig und der Einsatz von Firefox wird in vollem Umfang unterstützt.

Sicherheit dank Teergrube

Da mittlerweile mehr als 90 Prozent des täglichen E-Mailverkehrs Spam-Mails und Viren sind, ist es wichtig, in der Groupwarelösung ein Filter- und Schutzsystem zu integrieren. Neben dem effektiven Spamfilter auf Basis von SpamAssasin bietet Connect 7 auch die Prüfung von E-Mails mittels Caller-ID und SPF.

Als sehr effektiv hat sich der Einsatz von "Spam Repellent" gezeigt. Um ein großes Spam-Volumen zu versenden, kommunizieren automatische Spam-Programme nicht lange mit dem Mailserver. Daher gibt es in Kerio Connect die Funktion der verzögerten SMTP-Begrüßung. Das ist jedoch nur einsetzbar, wenn Connect als MX-Server eingetragen, E-Mails direkt an das System gesendet und nicht über einen separaten POP3-Server abgeholt werden müssen. Als optionalen Virenschutz integriert der Hersteller die McAfee-Engine und hat diese nahtlos in sein Produkt eingebunden.

Fazit

Im Funktionsumfang muss sich Kerio Connect 7 gegenüber Exchange nicht verstecken. Vor allem die Unterstützung mobiler Geräte ist besonders hervorzuheben. Im Detail betrachtet gibt es einige Abstriche. So können zum Beispiel Gruppen-E-Mails angelegt und Benutzern zugewiesen werden, doch gibt es kein zentrales Postfach für die ein- und ausgehenden E-Mails – diese landen bei jedem Gruppenmitglied im persönlichen Postfach. Der Nachteil: Gruppenmitglieder sehen nicht, ob und wie eine Nachricht beantwortet wurde. So muss Kerio auf jeden Fall noch an den Feinheiten feilen. Insgesamt aber bewies Kerio Con-

Hersteller
Kerio Technologies Inc.
www.kerio.de

Preis
Kerio Connect: 360 Euro (fünf Nutzer), 95 Euro je weitere fünf Nutzer. Kerio Connect mit McAffee Virenschutz: 432 Euro (fünf Nutzer), 114 Euro je weitere fünf Nutzer.

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

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

Systemanforderung	9
Flexibilität	8
Funktionsumfang Webmailer	10
Collaboration	9
Preis/Leistung	9
Gesamtwertung	**9**

Kerio Connect 7.0.2

nect 7 einen sehr stabilen, administrations- und anwenderfreundlichen Einsatz, der bei einer Groupwarelösung in dieser Preisklasse nicht selbstverständlich ist.

Collax Platform Server mit Zarafa Groupware

Ein anderes Konzept als die bisher vorgestellten Lösungen verfolgt Collax mit der Kombination des Platform Servers und Zarafa Groupware. In dieser Verbindung bekommt der Administrator eine skalierbare Groupware inklusive modular aufgebautem Betriebssystem auf Basis des Linux-Kernels.

Zarafa ist eine Lösung für Arbeitsgruppen, basierend auf dem Look & Feel von Outlook. Auf die Daten wird entweder direkt über Outlook oder durch das webbasierte Interface zugegriffen. Die Einrichtung und Administration erfolgt über das Collax-GUI der Server-Infrastruktur.

Installation per ISO-File

Collax liefert ein ISO-File zur Installation auf einer physikalischen oder virtuellen Maschine aus. Zur Grundeinrichtung des Betriebssystems werden nur die Basisdaten, wie die Server-IP und Kennwörter, abgefragt. Vor allem die weitergehenden Netzwerk-Einstellungen wie DNS und Gateway müssen später über die Administrations-Oberfläche nachgetragen werden. Nach dem Neustart steht das System in einer Grundausstattung für die erste Einrichtung zur Verfügung.

Collax Platform Server ist ein modular aufgebautes Produkt und wird nach den Bedürfnissen des Unternehmens erweitert. Nach der Aktivierung der Lizenz mussten wir das Kommunikations-Paket als Modul nachinstallieren. Danach wird das Anwendungs-Cabinet für Zarafa hochgeladen, wodurch die aktuellen Installations-Dateien heruntergeladen und installiert werden.

Systemvoraussetzungen

Intel Pentium oder kompatibel; bootfähiges CD-ROM-Laufwerk; Festplatte mit mindestens 8 GByte; 512 MByte RAM; VGA-fähige Grafikkarte (nur während der Installation)

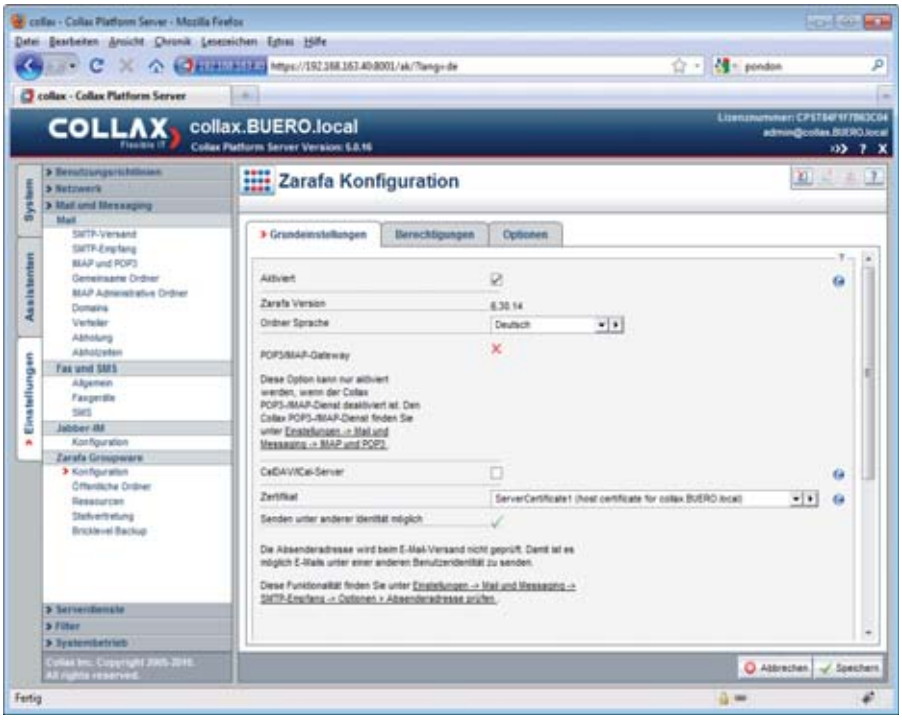


Bild 4: Die umfangreiche Server-Administration erfolgt komplett über das Web-Frontend von Collax

Uneinheitliche Administration

Da es sich bei Collax/Zarafa um eine komplette Server-Lösung inklusive Betriebssystem handelt, zeigt sich auch die Administration wesentlich umfangreicher als bei unseren bisherigen Test-Kandidaten. Wir konzentrieren uns jedoch auf die Administration des Groupware-Moduls von Zarafa. Die Struktur der Administration ist auf den ersten Blick nicht durchgängig. So werden einige Funktionen und Applikationen bezogen auf den Collax-Server, andere über das zusätzliche Modul von Zarafa konfiguriert. Der allgemeine Mailserver wird zum Beispiel im Collax-Basis-Paket mitgeliefert und dort mit einem der zahlreich vorhandenen Assistenten eingerichtet. Dabei kann das System auch als Mailserver fungieren, der E-Mails direkt empfängt – also als MX-Record einer Domain eingetragen ist.

Bei der Konfiguration der POP3-Konten lässt sich immer nur ein E-Mailkonto gezielt abrufen und an einen Benutzer oder einen Verteiler weiterleiten. Unternehmen, die aufgrund der hohen Anwenderzahl ein Wildcard-Konto betreiben, in dem alle an eine Domain gesandten E-Mails eintreffen, wünschen sich, dass die Verteilung auch anhand des Empfängers im Headers erfolgen kann – dies vermissen wir bei Zarafa gänzlich.

Wer im Netzwerk ein Active Directory (AD) einsetzt, kann die Benutzer entsprechend koppeln. Dazu muss der Collax-Server dem AD zugefügt und der ADS-Proxy aktiviert sein. Es ist nicht möglich, einzelne Benutzer zu übertragen, sondern nur ganze Gruppen. Dabei steht die AD-Standard-Gruppe "Benutzer" nicht zur Auswahl. Über einen Workaround legten wir daher im AD die Benutzergruppe "Zarafa" an und fügten dieser als Mitglied die Gruppe "Benutzer" hinzu. So stehen ohne Mehraufwand alle AD-User auf dem Collax-Server zur Verfügung.

Sehr umfangreich ist die grafische Oberfläche für Statistiken. Sie bietet detaillierte Auswertungen und eine grafische Auf-

bereitung aller Informationen, getrennt nach den jeweiligen Modulen wie Webserver und Mail.

Die integrierte Datensicherung unterscheidet wieder zwischen dem Backup des Servers und dem integrierten Bricklevel Backup von Zarafa. Diese auch in Exchange 2007 eingesetzte Sicherung benutzerbezogener Daten ermöglicht im Falle eines Datenverlustes, selektiv E-Mails, Kalendereinträge und Kontaktlisten wiederherstellen zu können, ohne ein Recovery des gesamten Datenbestands des betroffenen Benutzerkontos durchführen zu müssen.

Client- und Anwenderfunktionen fast wie bei Outlook

Auch Zarafa baut auf Outlook als Groupware-Client auf oder empfiehlt, das Web-Frontend einzusetzen. Jedoch besteht auch die Möglichkeit, mit anderen Mailclients wie Mozilla Thunderbird, Kmail oder Evolution auf die Daten zuzugreifen. In diesem Fall muss auf dem Server zusätzlich das IMAP/POP3-Gateway aktiviert werden und dem Anwender stehen Kalender und Aufgaben nicht zur Verfügung. Um das volle Funktions-Spektrum nutzen zu können, rät der Hersteller daher zum Einsatz von Outlook. Im Test stellten wir diese Verbindung zu Version 2003 und 2007 her.

Im gewohnten Bild zeigt sich die Nutzung der klassischen Groupware-Funktionen E-Mail, Kalender und Aufgaben. Auch Zarafa hat der Behandlung von Ressourcen eine höhere Aufmerksamkeit geschenkt als Microsoft. Schön gelöst ist das Anlegen über die Administrations-Oberfläche. Neben der Bezeichnung und einem Kommentar wird auch das Verhalten bei der Buchung festgelegt. So sind Parameter wie "Automatisch akzeptieren", "Konflikte ablehnen" und "Wiederkehrende Termine ablehnen" sinnvolle Zusatzangaben.

Das Anlegen und Verwalten von Mailing- beziehungsweise Verteilerlisten erfolgt wahlweise über das Kontakte-Menü von Outlook oder über das Webfrontend. Wird später mittels Webfrontend eine Nachricht an die Verteilerliste geschrieben, löst dieses die Eintragungen automatisch für die einzelnen Empfänger auf und versendet dann seperat. Genauso werden gemeinsame Adressen-Ordner über das Kontext-Menü von Outlook eingerichtet und gepflegt. Der Zugriff auf die Kalender anderer User erfolgt üblicherweise über die vorher erfolgte Freigabe und das Öffnen über den Weg der "anderen Kalender".

Der Webmailer irritiert den Anwender nach dem Login mit der Auswahl zwischen Squirrelmail und Zarafa Groupware. Squirrelmail ist der Webmailer, der mit der Collax-Basis-Funktion als Mailserver mitinstalliert wird. Nach der Wahl von Zarafa begegnet uns ein nahezu 1:1-Nachbau der Outlook-Oberfläche – sowohl im Internet Explorer als auch unter Firefox.

Der Zugriff mit mobilen Clients ist rudimentär möglich, aber nicht von Haus aus implementiert. Collax beziehungsweise Zarafa verweist auf die Open-Source Lösung Z-Push. Das Z-Push-Protokoll ist HTTP-basiert und kommuniziert über WBXML (WAP Binary XML). Dieses Format wird für die bidirektionale Kommunikation zwischen ActiveSync-kompatiblen PDAs beziehungsweise Telefonen und Zarafa verwendet. Seit kurzem bietet die linudata GmbH ein entsprechendes Collax Server-Modul an, das in die Collax-GUI integriert ist und das Setzen von Benutzerrichtlinien unterstützt.

Auf dem Mobilgerät – wie bei Nokia mit Mail4Exchange, dem Apple iPhone, Palm Pre und allen Windows-Mobile-Geräten – erfolgt die Einrichtung genauso wie für einen "echten" Exchange-Server. Danach steht der Synchronisierung von E-Mail, Kontakten, Kalendereinträgen und Aufgaben nichts im Weg.

Sicherheit

Den Schutz vor unerwünschten E-Mails gewährleistet Collax mit dem Mail- und

Security-Modul, das auf Basis von SpamAssasin und ClamAV den gesamten E-Mail-verkehr auf Schadprogramme prüft. Hierbei handelt es sich um OpenSource-Lösungen, deren zukünftige Aktualisierung mit Spam- und Viren-Informationen kostenlos ist.

Die Integration anderer Malware-Scanner ist theoretisch möglich, wird jedoch nicht über die Administrations-Oberfläche angeboten. Hierzu sind dann entsprechende Linux-Kenntnisse notwendig. Vor allem, da für das Collax-Betriebssystem regulär keine fertigen Installationspakete angeboten werden.

Fazit

Der Collax Plattform Server mit Zarafa ist im Hinblick auf die Groupware-Features sehr spartanisch. Das Konzept zielt auf eine andere Anwendergruppe als unsere weiteren Testkandidaten. Im Mittelpunkt steht der modular aufgebaute und über ein Web-Frontend administrierbare Server von Collax. Dieser bietet vielfältige Möglichkeiten, das System nach seinen Bedürfnissen einfach einzurichten. Das Zusatzmodul Zarafa ist noch nicht wirklich gut implementiert und auch sein Leistungsumfang lässt noch Wünsche offen. Als Pendant zu dem Gesamtkonstrukt ist eher der Small Business Server statt ein reiner Exchange-Server zu sehen. Mit dem Fokus auf die Groupware hat Collax noch einige Arbeit zu leisten, bis die Lösung in das Konzept des Plattform-Servers und des GUI richtig integriert ist. Um in der Funktion mit Exchange vergleichbar zu sein, wird bei Zarafa noch manche Programmierer-Stunde vergehen. Das Preis-/Leistungsverhältnis der E-Mail-plattform ist jedoch unschlagbar.

Hersteller
Collax GmbH
www.collax.com

Preis
28 Euro/User und Jahr, gestaffelt im Fünfer-Paket.

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

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

Systemanforderung	8
Flexibilität	7
Funktionsumfang Webmailer	10
Collaboration	7
Preis/Leistung	8
Gesamtwertung	**8,0**

Collax Plattform Server mit Zarafa Groupware

Ipswitch IMAIL Server 11

Mit IMAIL Server 11 Premium vom US-Hersteller Ipswitch testeten wir einen Kandidaten, der seit mehr als 15 Jahren auf dem Markt ist und schon einige Funktionserweiterungen durchlaufen hat. In der aktuellen Version 11 liefert Ipswitch das umfangreichste Paket der Suite aus. Neben den klassischen Groupware-Funktionen haben die Amerikaner ein großes Augenmerk auf das Thema Sicherheit durch Anti-Spam und Anti-Virus gelegt.

Installation mit Online-Aktivierung

Die Installation des ausschließlich in englischer Sprache verfügbaren Paketes erfolgt auf einem Windows-Server ab 2003. Dabei werden die Versionen mit 32- und 64-Bit unterstützt, wobei die Software selbst eine reine 32-Bit-Anwendung ist. Neben dem .NET Framework ab 3.5 SP1 setzt IMAIL auch einen betriebsbereiten IIS ab Version 6.0 voraus. Dieser bildet die Grundlage für das Webmail-Frontend und die Active Sync-Funktionen.

Schon zu Beginn der Installation muss die Version mittels Lizenzkey über das Internet aktiviert werden. Danach stehen die vier Komponenten "IMAIL Server", "Instant Messaging", "WorkgroupShare Client" und "Premium Anti Spam" zur Installation zur Verfügung. Im nächsten Dialog legten wir fest, über welche Datenbank IMAIL die User-Verwaltung durchführt. Zur Auswahl stehen "Windows NT User Database", "IMAIL User Database", "External Database (ODBC)" und natürlich "Active Directory".

Nach dieser Definition installiert das Setup den Server und konfiguriert den IIS. Danach ist es noch notwendig, den IIS einzurichten. Wenn mehrere Webseiten angelegt sind, so erkennt das der Setup-Assistent und fragt nach, unter welcher Webseite die Webclients erreichbar sein sollen. Kniffelig wird es noch bei der User-Angabe: Regulär wird der Dienst später mit dem default IIS User "IUSR_COMPUTERNAME" ausgeführt. Soll jedoch die Benutzer-Verwaltung über das Active Directory laufen, so verlangt IMAIL auch einen AD-User-Account, der IMAIL im IIS ausführt. Ein Neustart des Windows-Servers kann nötig sein, wenn zum Beispiel eine DLL nicht geschrieben oder aktualisiert werden konnte.

Administration über mehrere Wege

Die Administration erfolgt entweder über die Windows-Konsole oder mit dem Webfrontend. Sind die kleinen Hürden der Installation genommen, muss zunächst der System-Administrator angelegt werden. Dazu findet am besten die mitgelieferte Windows-Konsole ihren Einsatz. Der neue User erhält, neben den allgemeinen Zugriffsrechten auf Kalender, Aufgaben und E-Mail, auch den Status des System- und Domain-Administrators. Dabei ist nicht der Domänen-Administrator unter Windows gemeint, sondern die Berechtigung, auch die in IMAIL verwalteten Mail-Domains zu bearbeiten. Weitere Nutzer werden ebenfalls auf diesem Wege angelegt, sofern als Datenbank nicht das AD oder LDAP angebunden wurde.

Microsoft Windows 2003 Server oder Microsoft Windows 2008 Server (32/64 Bit); Microsoft Internet Information Services (IIS) ab 6.0; Windows Script 5.6; Microsoft Data Access Component (MDAC) ab 2.6; Microsoft .NET Framework 3.5 SP1

Systemvoraussetzungen

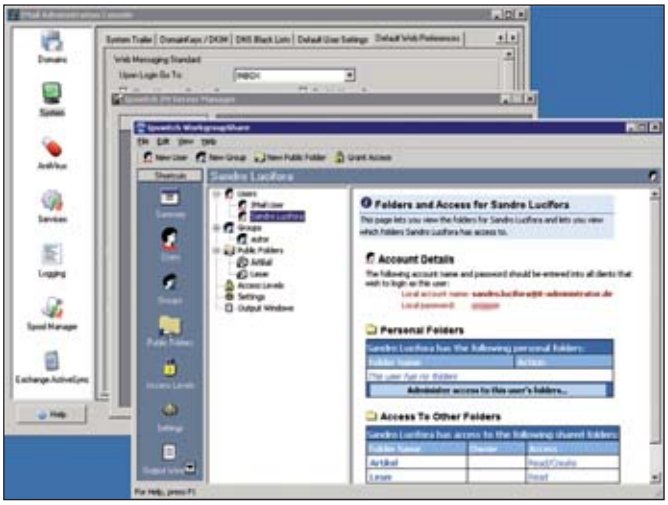


Bild 5: Über drei separate Management-Konsolen werden die verschiedenen Funktionen administriert

Ungeachtet dessen, wie die User in IMAIL eingerichtet werden, bekommen sie noch einige IMAIL-spezifische Parameter zugeordnet, da diese in keinem AD beziehungsweise LDAP gepflegt werden. Damit nicht jeder Benutzer einzeln angepasst werden muss, lassen sich Default-Einstellungen für das User-Setting, das Web-Messaging und ActiveSync vornehmen. Benutzer-spezifisch sind dann wahlweise noch Regeln für eingehende Nachrichten, ein Autoresponder und die Abwesenheits-Nachricht zentral, vom Administrator, einzustellen.

Im Konzept von IMAIL ist WorkgroupShare der Teil des Systems, der die Gruppen-Funktionen zur Verfügung stellt. In einer eigenen Administrations-Oberfläche werden Gruppen-Verzeichnisse für E-Mail, Kalender und Kontakte angelegt und entsprechende Zugriffsrechte auf Benutzer- oder Gruppenebene vergeben. Da es sich hierbei um einen in sich geschlossenen Programmteil handelt, muss sich der Client später immer wieder synchronisieren, um die aktuellen Daten zu erhalten. Wer es bisher gewöhnt ist – wie von Exchange –, dass dies in Echtzeit passiert, wird enttäuscht werden.

Unspektakuläre Client- und Anwenderfunktionen

Wie bei unseren anderen Test-Servern setzt auch Ipswitch auf Outlook als Client-Software. Um eine Verbindung wie zu einem Exchange-Server einzurichten, muss auf dem entsprechenden Arbeitsplatz das Client-Setup ausgeführt werden. Dieses Paket stellt IMAIL, sofern im Server-Setup ausgewählt, als WorkgroupShare zur Verfügung.

Während des Client-Setups werden einige Ports in der Client-Firewall geöffnet. Nach dem Start von Outlook erscheint ein Wizzard, der bei der ersten Einrichtung und Synchronisation der

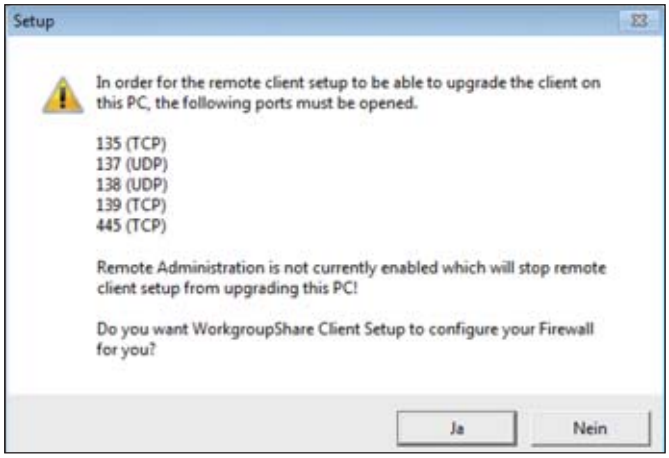


Bild 6: Für den Zugriff zwischen Outlook und IMAIL müssen Ports geöffnet werden

Daten behilflich ist. Wenn bereits eine PST-Datei vorhanden ist – diese kann auch Daten eines noch vorhandenen Exchange-Server-Kontos beinhalten – können die Inhalte auf den IMAIL-Server übertragen werden. Ansonsten legt WorkgroupShare eine neue Datei an und synchronisiert sich mit IMAIL. Danach stehen die Workgroup-Funktionen wie gewohnt zur Verfügung. Neben öffentlichen Ordnern für Kontakte und Kalender wartet dann auch die Frei/Verfügbar-Anzeige auf ihren Einsatz.

Die mobile Anbindung erfolgt über das ActiveSync-Protokoll und ist daher mit allen Smartphones und anderen Clients kompatibel, die auf dieser Basis Daten mit Groupware-Servern synchronisieren können. Dazu gehören in jedem Fall alle Geräte mit Windows Mobile und das iPhone.

Hersteller
Ipswitch, Inc.
www.imailserver.com

Preis
Ab etwa 215 Euro für zehn User.

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

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

Systemanforderung	7
Flexibilität	5
Funktionsumfang Webmailer	8
Collaboration	4
Preis/Leistung	8
Gesamtwertung	**6,4**

Ipswitch IMAIL Server 11.02

Sicherheit ohne Voreinstellungen

Ein Hauptaugenmerk ist bei IMAIL die Sicherheit der ein- und ausgehenden Informationen. Daher ist die Administration des "Domain Level Spam Filters" sehr umfangreich. Alle Filter sind zu Beginn sehr konservativ eingestellt und die Content-Filter komplett leer. Sie müssen, genau wie die Domain Black List, individuell mit entsprechenden Einträgen eingerichtet werden. Der Anhang-Filter verfügt schon über einige der üblichen Einträge wie SCR, BAT und EXE und filtert so – nach der Aktivierung – bereits E-Mails mit ungewollten Zusätzen.

Neben den umfangreichen Anti-Spam-Regeln unterstützt der Server auch DomainKeys. Diese Funktion dient dazu, das Verschleiern von E-Mail-Absendern zu erkennen und so herauszufinden, ob die eingehende E-Mail tatsächlich von der angegebenen Domain versendet wurde. Weiterhin bietet der Hersteller mit "IMail Anti-Virus powered by BitDefender" und "IMail Anti-Virus powered by Symantec" zwei umfangreiche Scan-Engines zum Schutz vor Viren an. Die Verwaltung und Konfiguration der Viren-Scanner ist komplett in die Administrations-Oberfläche von IMAIL integriert.

Fazit

IMAIL ist ein in den Funktionen gewachsener Mail-Server, der im Nachhinein um die klassischen Groupware-Funktionen erweitert wurde. Während das komplette Handling von E-Mails, inklusive Spam- und Viren-Filter, kaum Wünsche offen lässt, ist die als WorkgroupShare integrierte Groupware minimalistisch gehalten. Kalender, Kontakte und Aufgaben arbeiten fehlerfrei. Doch die üblichen Zusatzfunktionen, wie zum Beispiel das Handling von Ressourcen, fehlen komplett. Der Umstieg von Exchange gestaltet sich sehr mühsam und die Tatsache, dass das Produkt und die Anleitung nur in englischer Sprache verfügbar sind, machen den Einsatz nicht leichter.

Gesamtfazit

Unser Vergleichstest zeigt, dass die fünf getesteten E-Mail- und Groupware-Systeme nur vom Namen her die Davids gegen den Goliath Exchange sind. Technologisch unterschiedlich aufgestellt, zeigte doch jeder Kandidat seine Stärken ebenso wie seine Schwächen. Letztendlich muss jeder IT-Verantwortliche evaluieren, welche Anforderungen seine Infrastruktur oder auch sein Bugdet an E-Mail und Groupware stellt. Ein Umstieg erlaubt in jedem Fall, das Budget zu schonen, teilweise auch ohne dabei auf bekannte Features und den Administrationskomfort von Exchange zu verzichten. Zumal bei den Systemen, die auf Outlook als Frontend setzen, auch die Anwenderakzeptanz unproblematisch ist.

Das beste Gesamtpaket lieferte in unserem Test Kerio Connect 7, das Exchange in jeder Hinsicht das Wasser reichen kann und insgesamt gesehen am nutzerfreundlichsten ist. Auf den Plätzen rangieren IceWarp und MDaemon, die unterschiedliche Wege gehen, was den Umfang der möglichen Feineinstellungen betrifft. Die Kombination aus Collax und Zarafa hat einen puristischen Charme, konnte uns aber vor allem hinsichtlich der Implementierung der Groupware-Funktionen nicht überzeugen. Das Gleiche gilt auch für IMAIL, dem sein Schwerpunkt als reiner Mailserver einfach noch zu stark anzumerken ist. *(jp)*

E-Mail- und Groupware-Features im Vergleich

		Exchange 2007	Kerio Connect 7	Collax / Zarafa	Ipswitch IMAIL 11	IceWarp	Alt-N MDaemon
Unterstützte Server-OS	Windows	ja	XP/Vista/7, Server 2003/2008	nein	Server 2003/2008	ja	ja
	Linux	nein	Red Hat, open SUSE, Debian	nein	nein	ja	nein
	Unix/Derivate	nein	nein	nein	nein	nein	nein
	sonstige	nein	Apple Mac OS X	eigenes BS	nein	nein	nein
Unterstützte Clients	Standard-Client (POP3/SMTP)	nein	ja	ja	ja	ja	ja
	MS Outlook	ja	ja	ja	ja	optional	optional
	Web-Browser	ja	ja	ja	ja	ja	ja
	Eigene Clientsoftware	ja	nein	nein	nein	ja	nein
Unterstützung mobiler Geräte	ActiveSync	ja	ja	indirekt (Z-Push)	ja	ja	ja
	POP3/IMAP	nein	ja	indirekt (Z-Push)	nein	ja	ja
Administration	Web-Browser	nein	ja	ja	ja	ja	ja
	Kommandozeile	ja (PowerShell)	nein	ja	nein	ja	ja
	Remote Administration mit eigener Software	ja	ja	nein	ja	möglich	möglich
	SSL	ja	ja	ja	ja	ja	ja
	SNMP	ja		ja	nein	ja, eigene MIB	nein
	Eigene Konsole	ja	ja	nein	ja	ja	ja
	Telnet	ja	nein	nein	nein	über OS	über OS
	SSH	ja	nein	nein	nein	ja	nein
Anbindung an Verzeichnis-dienste	LDAP	ja	nein	ja	ja	ja	ja
	Active Directory	ja	ja	ja	ja	ja	ja
	NDS/Edirectory	nein	ja	nein	nein	ja	nein
	sonstige	nein	Apple Open Directory, Linux PAM	nein	nein	nein	nein
Unterstützte Mailprotokolle	SMTP	ja	ja	ja	ja	ja	ja
	ETRN	nein	ja	nein	nein	ja	ja
	POP3	ja	ja	ja	ja	ja	ja
	IMAP4	ja	ja	ja	ja	ja	ja
Storage	Datenspeicher für Mailboxen	Exchange-Datenspeicher	ja (eigener)	MySQL	ja (eigener)	SQLite	Filesystem
	Datenspeicher für gemeinsame Daten	Exchange-Datenspeicher	lokales Filesystem	lokales Filesystem	ja (eigener)	ja (öffentliche Ordner)	ja
	Quoten pro Postfach	ja	ja	ja	ja	ja	ja
	Quoten pro E-Mail	ja	ja	ja	ja	ja	ja
	Backup-Funktionen	nein	ja	ja	ja	ja	ja
Client-Dienste	Webmail	ja	ja	ja	ja	ja	ja
	Mobile Webmail	ja	ja	nein	nein	ja	ja
	Kalender	ja	ja	ja	ja	ja	ja
	Organizer (Aufgaben et cetera)	ja	ja	ja	ja	ja	ja
	Anwenderregeln und -filter	ja	ja	nein	ja	ja	ja
	Pushmail	ja	Direct Push	nein	nein	optional	ja
	Account Alias	ja	ja	nein	ja	ja	ja
Sonstige Dienste	Fax	ja	nein	Mail-2-Fax	nein	optional	optional
	Voice	ja	nein	nein	nein	optional	optional
	SMS	nein	nein	Mail-2-SMS	nein	optional	optional
Groupware-Funktionen	Benutzergruppen	ja	ja	ja	ja	ja	ja
	Kalender	ja	ja	ja	ja	ja	ja
	Kontakte	ja	ja	ja	ja	ja	ja
	gemeinsame Mail-Folder	ja	nein	nein	ja	ja	ja
Sicherheit	Verschlüsselte Datenübertragung	SSL	SSL	SSL	SSL	ja	ja
	Dateifilter für Attachments	ja	ja	nein	ja	ja	ja
	Spam-Filter	ja	ja	ja	ja	ja	ja
	Virenscanner-Interface	nein	McAfee	ClaimAV	ja	optional	optional
	Content-Filter	ja	nein	nein	ja	nein	nein

Im Test: Net at Work Mail Gateway 7.5.71

Sichere Mails garantiert

von Jürgen Heyer

Qualifizierte elektronische Signaturen sind eine zentrale Voraussetzung für den kostensparenden, elektronischen Rechnungsversand. Eine zuverlässige Verschlüsselung ist ebenso wichtig, wenn der Versand vertraulicher Informationen auf der Tagesordnung steht. Mit enQsig bietet Net at Work ein Mail Gateway an, das diese Aufgaben zentral übernimmt und so die einzelnen Anwender entlastet. IT-Administrator hat sich den Ablauf bei der Absicherung des Nachrichtenversands genauer angesehen und verrät, wo die Stärken und Schwächen der Software liegen.

Bekannt geworden ist die Net at Work Netzwerksysteme GmbH aus Paderborn durch die Anti-Spam-Lösung NoSpamProxy. Noch relativ neu ist das Programm enQsig zur E-Mail-Verschlüsselung und zum Erstellen qualifizierter elektronischer Signaturen. Der Hersteller hat nun beide Produkte unter einem neuen Namen als Net at Work Mail Gateway vereint, so dass hierfür nur eine Installation notwendig ist. Nur die Lizenzierung bestimmt letztendlich, ob ein oder zwei Produkte aktiv sind. Nutzer beider Funktionen haben den Vorteil, dass so der Ressourcenbedarf geringer ist und die Konfiguration weniger Aufwand erfordert. Für diesen Test haben wir uns auf die Komponente enQsig konzentriert.

Die digitale Signatur bietet dem Empfänger die Sicherheit über die Authentizität des Absenders. Eine Verschlüsselung sorgt dafür, dass nur der Adressat eine Nachricht auch lesen kann. Zudem schreibt das Umsatzsteuergesetz eine Validierung durch eine qualifizierte elektronische Signatur beim elektronischen Rechnungsversand und auch bei der Übergabe an ein Archivsystem vor. enQsig erledigt diese Aufgaben automatisch. Die Aktionen, die das Gateway auf eine E-Mail anwendet, gliedern sich also in die zwei Bereiche S/MIME-Unterstützung zur Verschlüsselung von E-Mails sowie das Ergänzen und Verarbeiten qualifizierter elektronischer Signaturen.

Variable Möglichkeiten zur Einbindung ins Netzwerk

Das Mail Gateway arbeitet als SMTP-Proxy und kann auf verschiedene Arten mit dem Mailserver im Unternehmen kombiniert werden. Das Studium der verschiedenen, im Handbuch aufgeführten Szenarien zeigt schnell, dass sich eine bestehende Umgebung erfreulich leicht um das Gateway ergänzen lässt.

Zuwachs in der DMZ

Bei der so genannten Einzelinstallation wird das Gateway auf einem eigenständigen Server installiert. Zusätzlich muss der Administrator das Routing im Netzwerk so konfigurieren, dass das Gateway die Mails auf Port 25 annehmen kann und erst anschließend an den eigentlichen Mailserver weiterleitet. Beim Versand muss der Mailserver die Mails wiederum zuerst an das Gateway senden, welches diese dann an die Adressaten, also die verschiedenen externen Mailserver, schickt. In einer größeren Umgebung mit DMZ empfiehlt es sich, das Gateway in der DMZ aufzustellen. Soll noch ein Virenscanner auf dem Transportweg eingebunden werden, so ist dieser zwischen dem Gateway und dem internen Mailserver anzuordnen. Eine Positionierung zwischen Gateway und Internet ist wenig sinnvoll, da hier Mails eventuell verschlüsselt sind und sich somit gar nicht scannen lassen. Alternativ kann der Virenscanner auch auf dem gleichen Server wie das Gateway laufen.

Anbindung über SMTP-Relay möglich

Verfügt ein Unternehmen über keine eigene, feste IP-Adresse, kommt meist ein Router mit NAT zum Einsatz. Die notwendige Namensauflösung wird dann am besten durch DDNS (dynamisches DNS) realisiert. Der Router muss nun so konfiguriert werden, dass Verbindungen auf Port 25 an die IP-Adresse des Gateways weitergeleitet werden. Während der Empfang in jedem Fall reibungslos funktionieren sollte, ist beim Versand eine Besonderheit zu beachten: Die meisten Mailserver weisen Mails von Servern mit einer dynamischen IP-Adresse zum Schutz vor Spammern ab. Um diese Tatsache zu umgehen, bietet es sich an, noch einen SMTP-Server beim eigenen Internet-Provider als

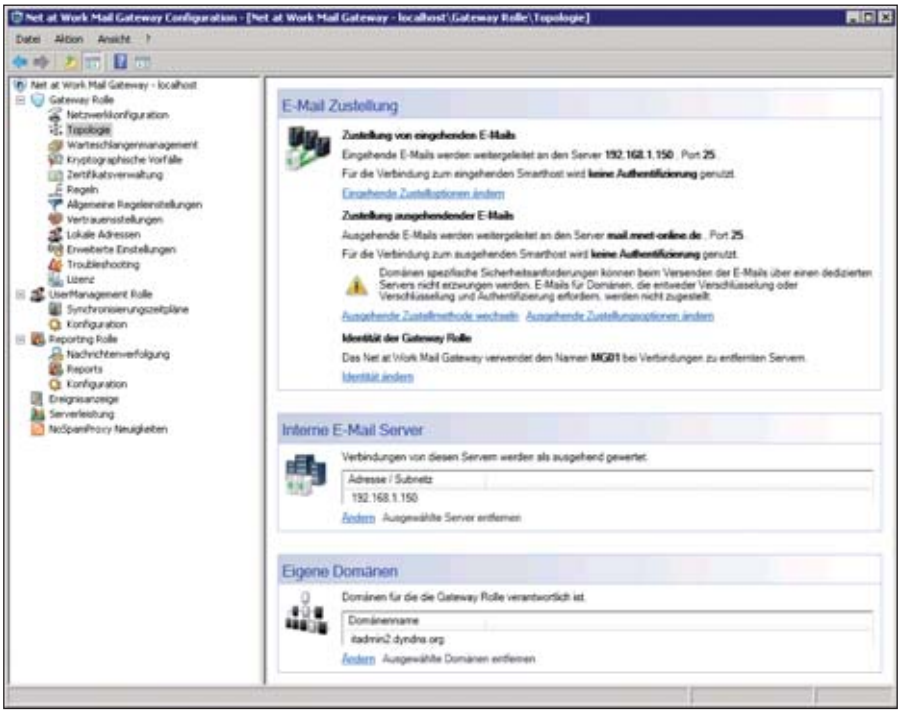


Bild 1: Die Einstellungen wie hier bei der E-Mailzustellung sind recht übersichtlich mit zusätzlichem, beschreibendem Text aufgelistet

SMTP-Relay zu nutzen, welcher dann letztendlich die Mail weitergibt. Das Net At Work Mail Gateway unterstützt diese Betriebsart mit optionaler Anmeldung am Relay ebenso wie den direkten Versand.

Für den kostensparenden Betrieb in kleineren Umgebungen ist es auch möglich, das Mail Gateway und den Mailserver auf dem gleichen System zu installieren. Hierbei muss der Mailserver nur so eingestellt werden, dass er nicht mehr auf Port 25, sondern auf einen anderen Port hört. Dann nimmt das Gateway die Mails selbst auf Port 25 an und gibt sie auf dem anderen Port über localhost weiter.

Läuft als Cluster und in virtualisierten Umgebungen

Für große Umgebungen und eine höhere Verfügbarkeit lässt sich enQsig als Cluster betreiben, indem das Gateway parallel auf mehreren Servern installiert wird. Die eingehenden Mails sind dann über DNS-RoundRobin, einen SMTP-Load-Balancer der Firewall oder die Windows-Funktion NLBS zu verteilen.

Jedes Gateway arbeitet in diesem Fall eigenständig, die Konfiguration wird pro Server in einer XML-Datei gehalten. Die Betriebsdaten aber werden am besten auf einem zentralen SQL-Server zusammengeführt. Außerdem wird der Betrieb des Mail Gateways auf virtuellen Maschinen unter VMware und Hyper-V offiziell unterstützt. Nicht möglich ist übrigens eine direkte Mailabholung per POP3 oder IMAP, es wird SMTP als Transportprotokoll vorausgesetzt.

Bedarfsgerechte Installation

Im Test entschieden wir uns für die Installation des Gateways auf einem eigenständigen Windows 2008-Server, 64 Bit, als virtuelle Maschine. Auf einer weiteren virtuellen Maschine richteten wir einen Mailserver (Kerio Connect) ein. Außerdem konfigurierten wir einen NAT-Router mit DDNS-Unterstützung, so dass die Domäne im Internet aufgelöst wurde und Mails direkt angenommen werden konnten. Ausgehende Mails leiteten wir wie beschrieben über den SMTP-Server eines Internet-Providers als Relay. Das Gateway gliedert sich funktional in drei Rollen (Gateway, Benutzermanagement und Reporting) sowie eine Management-Konsole, wobei alle Komponenten auf einem Server installiert, aber auch auf mehrere Systeme verteilt werden können. So sprechen Sicherheitsaspekte dafür, in einer größeren Umgebung auf einem oder mehreren Servern in der DMZ nur die Gateway Rolle zu installieren und das User Management sowie das Reporting auf einem Server im LAN. Für den Test installierten wir jedoch alle Komponenten des Gateways zusammen.

Das rund 3,5 MByte große Setup prüft die Installationsvoraussetzung und verlangte in unserem Fall zuerst die Einrichtung des Report Viewer Control 2008 SP1. Der passende Link war mit eingeblendet, so dass der Download und die Installation schnell erledigt waren. Anschließend fragte das Setup die gewünschte Datenbank ab. Zur Auswahl stehen entweder ein externer SQL-Server oder SQL Server 2005 Express, zu dessen Setup-Dateien der Administrator den Pfad angeben kann. Alternativ wird die Express-Version bei Microsoft heruntergeladen. Zuletzt fragt das Setup noch ein Passwort für den SA-Benutzer ab, installiert dann alles und richtet auch die notwendige Datenbankinstanz ein. Für die Lizenzierung muss der Administrator abschließend die erhaltene Lizenzdatei in ein Verzeichnis laut Handbuch kopieren.

Ordnung über Regeln und Rollen

Durch die Verwendung von Rollen für die verschiedenen Funktionsbereiche sowie Regeln für die Beschreibung des Umgangs mit den Mails ist die Konfiguration des Mail Gateways sehr übersichtlich strukturiert und weitgehend intuitiv zu bedienen. Im Rahmen der Erstinbetriebnahme sind diese Rollen und Regeln zu konfigurieren. Vorteilhaft ist, dass in der Dokumentation die notwendigen Schritte für einen Minimalbetrieb stichpunktartig aufgelistet sind. Im Test klappte die Einrichtung anhand dieser Übersicht auf Anhieb. Zuerst ist der Listener für den E-Mailempfang zu konfigurieren, wobei dieser auf alle oder auch

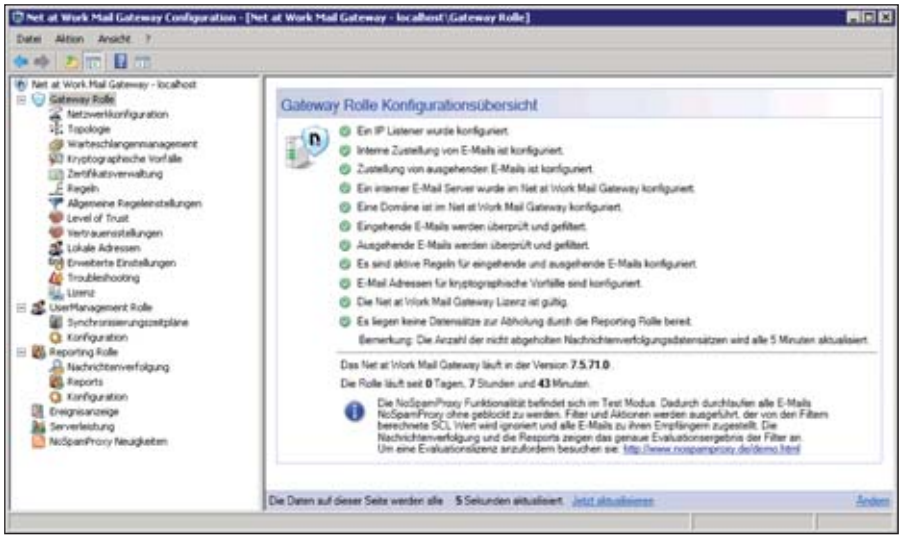


Bild 2: Die Konfigurationsübersicht der Gateway-Rolle bietet eine gute Zusammenfassung der bestehenden Einstellungen

nur eine bestimmte IP-Adresse hört. Der Listener unterstützt Tarpitting, um DoS-Attacken abzuwehren. Hierbei wartet der Listener bei ungültigen Anfragen zwischen zwei und zehn Sekunden, um so den Verkehr bewusst zu bremsen.

Der Umgang des Gateways mit ein- und ausgehenden Mails wird über Regeln definiert. Hilfreich ist hier, dass es die Möglichkeit gibt, über einen Link drei vorbereitete Standardregeln einrichten zu lassen. Diese lassen sich nachher bei Bedarf ergänzen oder modifizieren. Weiterhin kann der Administrator aus vier Optionen die gewünschte Transportsicherheit für die komplette SMTP-Verbindung auswählen (keine Anforderung, StartTLS erlauben oder erzwingen, Verwendung von SMTPS). Für eine Verschlüsselung sind entsprechende Zertifikate erforderlich.

Schwarze Listen in der Domänenverwaltung

Anschließend ist die Zustellung ausgehender Mails an fremde Mail-Server sowie an den oder die internen Mailserver einzurichten. Wichtig ist es hier, alle eigenen Mailserver in eine Liste einzutragen, damit das Gateway weiß, dass Mails von diesen IP-Adressen als ausgehend zu behandeln sind. Auch hier kann optional mit Verschlüsselung und Zertifikaten gearbeitet werden.

Ebenso wichtig ist es, alle eigenen Domänen bei der Domänenverwaltung einzutragen, damit enQsig weiß, welche E-Mails es annehmen und welche es abweisen soll. Darüber hinaus ist es möglich, die SMTP-Adressen über eine Verbindung zum Active Directory, aber auch mittels einer Benutzerliste als Datei abzugleichen. Die Einträge können sowohl in eine Positiv-Liste (zugelassene lokale Adressen) als auch in eine Negativliste (unerwünschte lokale Adressen) fließen.

Einfacher Import von Zertifikaten

Um das Gateway sinnvoll zu nutzen, sind schließlich noch Zertifikate notwendig, die importiert werden müssen. Eine Partnerschaft besteht hier zwischen Net at Work und TC Trustcenter, so dass ein Anwender auf Wunsch alles aus einer Hand beziehen kann.

Zertifikate können bei enQsig entweder durch öffentliche oder private Zertifikatsdateien importiert werden. Gibt es für eine Domäne beide Zertifikate, so wird das private bevorzugt. Liegt für eine Domäne bereits ein öffentliches Zertifikat vor und wird nun ein privates importiert, so wird das öffentliche entfernt. Gegebenenfalls sind beim Import entsprechende Passwörter anzugeben. Importieren lassen sich die Dateiformate CER, DER, PFX und P12. Sofern das Gateway eingehende, signierte E-Mails verarbeitet, importiert es die anhängenden, öffentlichen Zertifikate automatisch. Diese wiederum kann es nutzen, um zukünftig diesem Empfänger verschlüsselte Mails zukommen zu lassen.

Verschlüsselte Verbindung, verschlüsselte Mails

In der Rubrik "Vertrauensstellungen" trägt das Mail Gateway automatisch bei ausgehenden Mails die entsprechende Domäne ein. Die Domäneneinträge für viele große Provider werden bereits im Rahmen der Installation automatisch angelegt. Der Administrator hat nun die Möglichkeit, für jede Domäne eine individuelle Verbindungssicherheit vorzugeben, wobei vier Stufen zur Verfügung stehen, davon drei mit Verschlüsselung. Zu beachten ist hier, dass eine Verschlüsselung (der Verbindung, nicht der Mails) nur bei einer direkten Zustellung zum externen Mailserver möglich ist. Ist das Gateway so konfiguriert, dass es über ein SMTP-Relay, hier Smarthost genannt, Mails verschickt, so kann es nicht sicherstellen, dass die Kommunikation bis zum Empfänger verschlüsselt ist. Ein Mailversand wird dann fehlschlagen.

Um Probleme bei der Signierung gezielt bearbeiten zu können, gibt es einen eigenen Menüpunkt "Kryptographische Vorfälle", in dem alle Probleme in einer Liste aufgeführt sind. Im System ist eine Mailadresse zu hinterlegen, die bei jedem neuen Vorfall benachrichtigt wird.

Im Gegensatz zur Signierung und Verschlüsselung mit einem Mailclient am Arbeitsplatz hat der Einsatz des zentralen Mail Gateways einige deutlich sichtbare Änderungen zur Folge. So hat der Anwender keinen Einfluss darauf, ob seine Mails signiert und/oder verschlüsselt werden, dies entscheidet allein das Gateway anhand des vom Administrator definierten Regelwerks.

Umfangreiches Regelwerk erfordert Überblick

Im Test haben wir diverse E-Mails mit und ohne Signatur sowie Verschlüsselung

an verschiedene Empfänger versendet, wobei das Gateway von einigen den öffentlichen Schlüssel über eine eingegangene signierte E-Mail gespeichert hatte. Parallel dazu haben wir die Regeln verändert, um zu sehen, wie das Gateway bei verschiedenen Einstellungen arbeitet. Schnell zeigte sich, dass es sehr wichtig ist, die diversen Möglichkeiten genau zu studieren und an die individuellen Anforderungen anzupassen.

Als recht unkritisch erweist sich hier die Signierung. Indem der Administrator ein Zertifikat zu einem Gateway-Zertifikat hochstuft und gegebenenfalls persönliche Zertifikate von Anwendern hinterlegt, kann das Gateway für die Signierung vorrangig das persönliche und ansonsten das Zertifikat des Gateways verwenden. Bezüglich der Verschlüsselung muss der Administrator genauer abwägen, welche Einstellung er wählt. Ist beispielsweise die Verschlüsselung optional, so verschlüsselt das Gateway nur an Adressaten, von denen ein öffentlicher Schlüssel vorliegt, an andere aber nicht. Das passt aber eventuell nicht zu dem Wunsch, dass Mails mit vertrauenswürdigem Inhalt ausschließlich verschlüsselt übertragen werden sollen. Wird nun die Regel auf eine obligatorische Verschlüsselung umgestellt, können keine Mails mehr an Adressaten versendet werden, von denen kein Schlüssel vorliegt. Werden nun in einer Mail mehrere Empfänger aufgeführt und nur von einem liegt kein Zertifikat vor, so wird die Mail an niemanden versendet.

Plug-In für den Mailclient und PDF-Verschlüsselung geplant

In der jetzigen Version kann ein Anwender das Gateway noch nicht steuern, aber es ist ein Plug-In für Outlook geplant, damit der Versender Signierung und Verschlüsselung selbst vorgeben kann. Wann dieses aber verfügbar sein wird, steht noch nicht fest. Falls übrigens ein Anwender seine Mail gleich am Arbeitsplatz signiert, so hängt es von der Einstellung des Gateways ab, ob es die Signatur wieder entfernt oder nicht. Wird nämlich eine derartige Signatur mitgegeben, so besteht die Gefahr, dass der Empfänger seine Antwort damit verschlüsselt und das Gateway eine Mail erhält, welche es nicht entschlüsseln kann. Je nach Einstellung wird die Mail nun abgewiesen oder dem Anwender verschlüsselt zugestellt. Letzteres hat aber den Nachteil, dass die Mail vor der Zustellung nicht auf Viren gescannt werden kann.

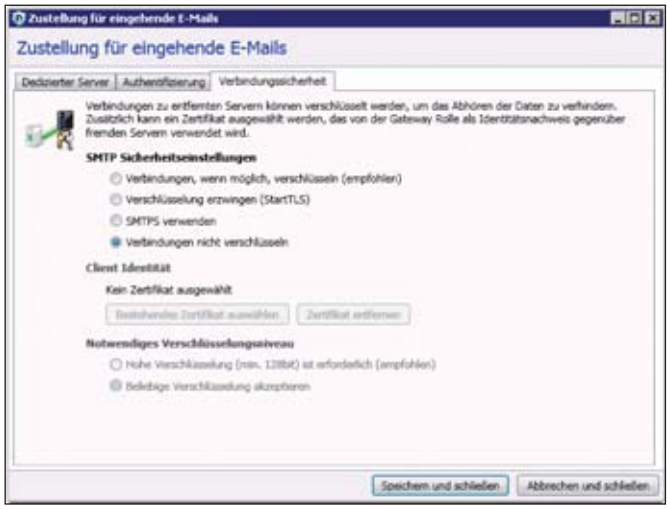


Bild 3: Bei der Verbindungssicherheit für eingehende Mails stehen vier SMTP-Sicherheitseinstellungen zur Verfügung

Ob ein Zertifikat bei der Verwendung noch gültig ist, prüft das Gateway mittels der CRL (Certificate Revocation List) des ausstellenden CA. In Zukunft ist eine Überprüfung mittels OCSP geplant, was in der Regel einen etwas aktuelleren Stand liefert als die CRL.

Kommt von einem Absender eine Mail an mehrere Empfänger im Unternehmen, so kann es sein, dass für die Verarbeitung dieser Mail für die Empfänger unterschiedliche Regeln greifen. Aufgrund des SMTP-Protokolls ist es nun nicht möglich, für die unterschiedlichen Empfänger entsprechend unterschiedliche Rückmeldungen zu liefern. Umgehen lässt sich das Problem durch die Aktivierung der so genannten "Strict Single Rule", die den Absender zwingt, jedem Adressaten eine eigene Mail zu schicken. Laut RFC ist das erst ab dem 101. Empfänger erlaubt, aber praktisch kein Mailserver stört sich daran, wenn es weniger Empfänger sind.

In der nächste Version 7.6 soll eine PDF-Verschlüsselung enthalten sein. Dazu wird das Dokument am Gateway mit einem Zufallscode verschlüsselt, der dem Empfänger parallel per SMS zugeschickt wird.

Vorbildliche Dokumentation und Reporting

Eine sehr umfangreiche und gut aufgebaute Dokumentation erleichtert sowohl die Installation und anschließende Einrichtung des Mail Gateways als auch die weitere Bedienung. Sehr hilfreich ist im Handbuch die Rubrik "Fehlersuche", die diverse detaillierte Hinweise zur Behebung von Problemen gibt. Dies beginnt mit Tipps, wie das Mail Gateway am besten hinsichtlich seiner Funktion kontrolliert wird. So sollte der Administrator zuerst den Statusbildschirm auf der Überblickseite der Management Konsole betrachten. Hier sind die Rollen mit ihrem Status aufgelistet. Sind dort nicht alle Positionen mit einem grünen Haken versehen, ist dies ein erster Hinweis auf eine Fehlfunktion. Dann kann der Administrator eine einzelne Rolle markieren und erhält wiederum eine detaillierte Übersicht zum Status beziehungsweise zu gefundenen Fehlern.

Neben der Dokumentation und den beschriebenen Statusangaben der Rollen gibt es im Programm noch weitere Übersichten, die bei der Fehlersuche oder auch der Analyse des Mailverkehrs helfen. So steht dem Administrator eine Nachrichtenverfolgung zur Verfügung, mittels derer er nach bestimmten Kriterien suchen kann. Von der E-Mail sieht er allerdings nur den Betreff, daneben noch Absender, Empfänger und Zeit, aber nicht den Inhalt. Ein unberechtigtes Mitlesen ist also nicht möglich.

Eine Ereignisanzeige liefert Informationen zur Ausführung interner Aktivitäten, außerdem gibt es eine detaillierte Ansicht zur Serverleistung mit diversen statistischen Daten (Ressourcennutzung durch die Rollen, Datenbankgröße, empfangene und versendete Nachrichten sowie Belastung des Systems).

Fazit

enQsig übernahm in unserem Test fehlerlos die E-Mail-Verschlüsselung und versah Nachrichten bei Bedarf mit einer qualifizierten elektronischen Signatur. Da das Werkzeug als SMTP-Proxy arbeitet, ist es erfreulich einfach in bestehende Mailumgebungen zu integrieren. Dadurch, dass das Gateway bestimmt, inwiefern Mails an bestimmte Adressaten signiert und/oder verschlüsselt werden, lassen sich entsprechende Unternehmensrichtlinien gezielt durchsetzen, ohne dabei von Aktionen der Mitarbeiter abhängig zu sein. Letztendlich spart sich ein Anwender damit auch den Aufwand, seine Mails mit einer qualifizierten elektronischen Signatur zu versehen. Allerdings vermissen wir die Möglichkeit, dass ein Anwender steuern kann, ob signiert und verschlüsselt wird oder nicht. Dieses Feature ist aber für eine spätere Version geplant.

Von Vorteil ist weiterhin die Möglichkeit, die im Gateway angelegten Benutzer unter anderem mit einem Microsoft Active Directory zu synchronisieren. Gefallen haben uns auch die insgesamt intuitive Bedienung und das gute Reporting mit einer Nachrichtenverfolgung, abgerundet durch eine detaillierte Dokumentation, die diverse Hinweise und Tipps zur Analyse und Fehlersuche gibt. *(ln)*

Produkt
Programm zur E-Mail-Verschlüsselung und qualifizierten elektronischen Signatur, mit zusätzlicher Lizenz auch nutzbar als Anti-Spam-Lösung.

Hersteller
Net at Work
www.enQsig.de

Preis
Die Lizenz für enQsig kostet für 25 Benutzer 1.625 Euro.

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

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

Installation und Bedienung	8
Skalierbarkeit	8
Mail-Verschlüsselung	7
Mail-Signierung	9
Dokumentation	8

Dieses Produkt eignet sich

optimal für Unternehmen, die einen eigenen Mailserver betreiben, eine Mailverschlüsselung sowie automatische Signierung benötigen und in diesem Umfeld auf Windows als Betriebssystem setzen.

bedingt, falls ein Unternehmen im Internet-Mail-Umfeld auf Linux als Basis setzt. Hier lassen sich keine Funktionen auf einem Server zusammenfassen. Administratoren dürften dann eine durchgängige Linux-Umgebung bevorzugen.

nicht, wenn es keinen Bedarf für eine Mailverschlüsselung sowie für signierte Mails gibt.

Net at Work Mail Gateway 7.5.71

Im Kurztest: SyncEvolution EdocSync

Gleiche Daten für alle

von Sandro Lucifora

Das vernetzte Arbeiten an mobilen Arbeitsplätzen sowie die Zusammenarbeit mit Dritten stellt IT-Verantwortliche bei der konsistenten Datenhaltung vor neue Herausforderungen. Mit EdocSync liefert der französische Hersteller SyncEvolution eine Software, die beim Organisieren, Verteilen und Synchronisieren von verteilten Dateien zur Hand geht. Im Test musste die Lösung beweisen, wie gut sie die Daten in Griff hat.

Das auf dem Peer-to-Peer-Prinzip arbeitende EdocSync tauscht Daten direkt zwischen mehreren Computern aus. Ein zentraler Dateiserver entfällt. Im Test haben wir das Programm unter Windows XP und Windows 7 problemlos installiert und nach dem ersten Start unser Benutzerprofil angelegt. Dieses wird später als Zugangsberechtigung auf die verteilten Clients benötigt. Entgegen des derzeitigen Trends bei der Gestaltung von GUIs präsentiert sich EdocSync in einem Linux-ähnlichen Aussehen. Durch die einfache Bedienung findet sich auch der weniger versierte Anwender schnell zurecht. Das zweigeteilte Arbeitsfenster enthält auf der linken Seite die Punkte "Arbeitsgruppen", "Kontakte" und "Nachrichten", deren Inhalte rechts dargestellt werden. Das Hinzufügen neuer Kontakte oder das Erstellen von Arbeitsgruppen erfolgt über die Werkzeugleiste.

Die Basis: Arbeitsgruppen

Die Arbeitsgruppe ist die Basis für das Synchronisieren von Dateien. In der Arbeitsgruppe verbinden sich die Kontakte und die gemeinsamen Daten werden dort gesammelt. Durch das Vergeben eines Passwortes lassen sich die Dateien zusätzlich schützen. Den Kontakten können dabei verschiedene Berechtigungen wie "Nur Lesen" bis zu "Lesen, Schreiben, Ändern, Löschen" zugeteilt werden.

Ist die Arbeitsgruppe eingerichtet, kann durch jeden Kontakt via Drag-and-Drop eine Datei und ganze Ordner hinzugefügt werden. EdocSync kopiert die Dateien in den lokalen Arbeitsgruppen-Pfad und verteilt diese sofort im Hintergrund auf alle anderen Arbeitsgruppen-Clients. Der Aufruf zum Bearbeiten einer Datei erfolgt direkt über das Kontextmenü. Windows startet dann das mit dem Dateityp assoziierte Programm. Wird die geänderte Datei gespeichert, überträgt EdocSync diese sofort auf die anderen Clients. Um den Datentransfer so gering wie möglich zu halten, überträgt das Tool nicht die kompletten Dateien, sondern die geänderten Segmente – was vor allem bei der Anbindung über das Internet Vorteile bietet.

Stellt die Software fest, dass auf zwei Clients an derselben Datei gearbeitet wurde, können die unterschiedlichen Versionen automatisch oder manuell zusammengeführt werden. Dies funktionierte im Test jedoch nur mit den klassischen Office-Dateien problemlos. Die integrierte Versionsverwaltung ermöglicht es, die älteren Versionen einer Datei einzusehen und die komplette Historie, inklusive Datum und Bearbeiter, anzuzeigen. Komplettiert wird diese Funktion durch die Möglichkeit, einer Datei eine Notiz hinzuzufügen, die zum Beispiel den Grund der Bearbeitung festhält.

Fazit

Den Anspruch, Dateien über ein direktes Peer-to-Peer-Netzwerk zwischen mehreren Computern synchron zu halten, erfüllte EdocSync im Test anstandslos. Kleinere Wermutstropfen trüben jedoch das sonst sehr gute Bild von EdocSync: Neben dem Problem, größere Dateien zu synchronisieren – obwohl der Hersteller angibt, dass es keine Größenbeschränkung gibt –, und dem notwendigen Einsatz des Meeting Point-Servers für eine sinnvolle Nutzung in Unternehmen stellt der Preis eine kleine Anschaffungshürde dar. *(dr)*

Produkt
Software zur Organisation und Synchronisation von verteilten Dateien.

Hersteller
SyncEvolution S.a.r.l. Inc.
www.syncevolution.de

Preis
Eine Lizenz EdocSync Pro: 49,50 Euro
Team-Pakete ab 99 Euro für drei Mitarbeiter

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

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

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

Dieses Produkt eignet sich

optimal für den Datenabgleich zwischen wenigen Einzelplatz-Computern.

bedingt für den Einsatz in Unternehmen und der Synchronisierung im LAN und WAN.

nicht für den Abgleich überwiegend großer Dateien, wie etwa im Grafik-Bereich.

SyncEvolution EdocSync Pro 1.7

Einkaufsführer: Systeme zur E-Mailarchivierung

Rechts- und zukunftssicher

von Jerry J. Artishdad

Die Archivierung von E-Mails stellt für viele Unternehmen nach wie vor eine große Herausforderung dar. Angesichts stetig steigender Datenvolumina und der immer größeren Anzahl geschäftlich verschickter Nachrichten werden an die Archivierungslösungen zusehends höhere Ansprüche gestellt. So stehen IT-Verantwortliche vor der wichtigen Aufgabe, diese Datenmengen langfristig sinnvoll und auch rechtssicher zu verwalten und zu organisieren. Auf welche Aspekte Sie beim Thema E-Mailarchivierung achten sollten, zeigt dieser Einkaufsführer.

Zukunftssichere Archivierung sieht anders aus

Neben einer technisch sauberen Einbindung in die bestehende IT-Infrastruktur steht bei der Auswahl eines geeigneten Systems vor allem die Frage nach Rechtssicherheit und Compliance im Vordergrund. Denn die Abbildung der gesetzlichen Anforderungen und Aufbewahrungspflichten ist in den meisten Unternehmen häufig immer noch der ausschlaggebende Punkt, um sich erstmals mit der Thematik E-Mailarchivierung zu beschäftigen. IT-Leiter, Administratoren und Geschäftsführung sehen sich hier einer Vielzahl an Richtlinien und Verordnungen aus verschiedensten Bereichen gegenüber, die auf den ersten Blick kaum zu durchschauen sind. Eine wichtige Rolle spielen hier unter anderem die Abgabenordnung, die so genannten GDPdU-Regelungen (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) oder das Handelsgesetzbuch.

Neben dem rechtlichen Gesichtspunkt sollten bei der Entscheidungsfindung aber auch weitere Aspekte von Archivierungslösungen berücksichtigt werden. Durch eine bessere Organisation der E-Mailflut können diese beitragen, die lokalen Systeme erheblich zu entlasten und die Verwaltung und Organisation der E-Mails für Anwender und Administratoren gleichermaßen zu vereinfachen. Während sich die grundlegenden Funktionsweisen der verschiedenen Archivierungssysteme häufig ähneln, sind es letztlich die Features und Details, die auf lange Sicht über den Nutzwert entscheiden.

Software, Appliance oder Cloud

Eine erste grobe Einteilung des Angebots am Markt kann durch die Differenzierung nach reinen Software-Lösungen und Archivierungs-Appliances erfolgen. Während Software (nicht immer zu Recht) der Ruf größerer Flexibilität und besserer Skalierbarkeit vorauseilt, können Appliances durch ihre in sich geschlossene Konzeption häufig Vorteile hinsichtlich der Sicherheit aufweisen. Gerade die konsequente Umsetzung der gesetzlichen Vorgaben lässt sich durch ein fertig konfiguriertes, manipulationsgeschütztes System aus Hard- und Software oft leichter realisieren. Auch die schnelle, unkomplizierte Einbindung ins Netzwerk nach dem Plug-and-Play-Prinzip kann je nach Unternehmensgröße, Vorwissen und vorhandener IT-Infrastruktur für den Einsatz einer Appliance sprechen.

In jüngster Zeit treten am Markt auch die ersten IT-Dienstleister und Storage-Unternehmen in Erscheinung, die E-Mailarchivierung in der Cloud beziehungsweise als komplett in ein externes Rechenzentrum ausgelagerten Service anbieten. Es empfiehlt sich allerdings, Angebote dieser Art besonders sorgfältig auf ihre rechtliche Sicherheit hin zu überprüfen. Denn wenn die sensible Firmenkommunikation möglicherweise im Ausland gehostet wird oder sich ein Anbieter freiwillig oder unfreiwillig aus dem Marktsegment zurückzieht, können erhebliche Probleme entstehen. IT-Administratoren müssen hier in Abstimmung mit der Geschäftsleitung genau abwägen, ob sie das Risiko eingehen, interne, unternehmenskritische Daten und das damit verbundene Know-how auszulagern und sich somit in die Abhängigkeit eines bestimmten Anbieters zu begeben. Auch die Kostenrechnung sollte

dabei nicht vernachlässigt werden. Denn wenn pro User beziehungsweise nach benötigter Storage-Kapazität abgerechnet wird, können anfangs günstig erscheinende Konditionen unter Umständen auf lange Sicht zum teuren Bumerang werden.

Langfristigen Betrieb sicherstellen

Verglichen mit anderen Bereichen innerhalb der schnelllebigen IT-Branche mit ihren kurzen Innovationszyklen stechen E-Mailarchive durch eine extrem lange Laufzeit heraus. Für unternehmensrelevante Daten ergeben sich etwa aus den steuerrechtlichen Bestimmungen Aufbewahrungsfristen von teilweise mehr als zehn Jahren. Die wichtigste Konsequenz, die sich für Administratoren aus dieser Tatsache ergibt: Um einen langfristig problemlosen Betrieb sicherstellen zu können, sollte die Archivlösung möglichst unabhängig von bestimmten Anwendungen oder Speichertechnologien verwendbar sein und auf gängigen Standards basieren. Denn welcher Admin vermag heute schon mit absoluter Sicherheit zu sagen, welcher Mailserver und welche Clients in seinem Unternehmen in drei Jahren zum Einsatz kommen – von Zeiträumen von fünf, acht oder gar zehn Jahren ganz zu schweigen.

Gerade Administratoren in größeren Unternehmen, in deren Niederlassungen unter Umständen unterschiedliche E-Mailsysteme verwendet werden, sollten deshalb darauf achten, dass die Archivlösung unabhängig von bestimmten Servern lauffähig ist. Im Idealfall kann das System in verschiedensten Infrastrukturen eingesetzt werden und arbeitet mit allen gängigen Mailservern zusammen, so dass auch spätere Änderungen und Migrationen im Netzwerk problemlos durchführbar sind.

Sicherheit geht vor

Da im E-Mailarchiv sensible Firmendaten abgelegt werden, spielt das Thema Datensicherheit bei der Auswahl einer Archiv-Lösung eine besonders große Rolle. So versteht es sich eigentlich von selbst, dass die Maildaten nicht im Klartext, sondern ausschließlich verschlüsselt abzulegen sind. Häufig übersehen wird das potenzielle Sicherheitsrisiko, das Anwender mit weitreichenden Benutzerrechten oder auch der IT-Administrator selbst darstellen. Können von entsprechend legitimierten Usern ohne Dokumentation Änderungen am Archivbestand vorgenommen werden, bedeutet dies unter Umständen den Verlust der Rechtssicherheit für das gesamte Archiv. Unabhängig von der Unternehmensgröße sollte deshalb darauf geachtet werden, dass das Archiv vor derartigen Manipulationen geschützt wird und entsprechende Features aufweist. Denkbar ist hier beispielsweise ein Vorgehen nach dem Vier-Augen-Prinzip, bei dem entsprechende Aktionen nur von zwei berechtigten Benutzern zusammen vorgenommen werden können.

Bereits das Dateiformat, in dem eine Archivierungslösung die E-Mails ablegt, entscheidet mit darüber, inwieweit Rechtssicherheit erreicht werden kann. Bei E-Mails, die für die Archivierung in ein anderes Dateiformat wie etwa PDF konvertiert werden, handelt es sich je nach Rechtsauffassung streng genommen nicht mehr um ein Original. Dies gilt auch dann, wenn der eigentliche Inhalt der Mail selbst in keinster Weise verändert wurde. Es empfiehlt sich deshalb, ein System einzusetzen, das E-Mails direkt im Originalformat (SMTP, RFC 822) archiviert. Wichtig sind außerdem Vorkehrungen, um später den unveränderten Zustand der Daten belegen zu können, beispielsweise im Rahmen einer Betriebsprüfung oder wenn Verträge oder Angebotsschreiben als Beweise benötigt werden. E-Mailarchive ermöglichen dies zum Beispiel durch die Verwendung von digitalen Signaturen, durch die der Weg jeder einzelnen E-Mail exakt nachverfolgt werden kann.

Suchen, organisieren und verwalten

E-Mails zu archivieren ist das Eine, die spätere Wiederherstellung das Andere. Gute Lösungen zeichnen sich dadurch aus, dass auch der spätere Zugriff auf das Archiv und das Wiederauffinden einzelner Nachrichten komfortabel gestaltet sind. Der wahre Wert eines E-Mailarchivs zeigt sich in der Praxis häufig dann, wenn Anwender Jahre nach Beginn der Archivierung innerhalb kurzer Zeit eine bestimmte E-Mail auffinden möchten.

Die Suchfunktion sollte als Volltextsuche ausgelegt sein und sich möglichst nicht nur auf den Nachrichtentext, sondern auch über Dateianhänge erstrecken. Nur so kann gewährleistet werden, dass zügig auf den gesamten Datenbestand zugegriffen werden kann und auch große und sehr große Archive überschaubar und zugänglich bleiben. Wichtig für die Akzeptanz des Archivs beziehungsweise seiner Suchfunktion auf Anwenderseite ist zudem ein benutzerfreundliches Frontend mit einer komfortablen Suchmaske.

Eine zusätzliche Möglichkeit, ein E-Mailarchiv zu organisieren, stellt die Vergabe von individuellen Attributen beziehungsweise die Verknüpfung der archivierten E-Mails mit zusätzlichen Informationen dar. Ein Feature, das es gerade mittleren und großen Unternehmen ermöglicht, für bestimmte Projekte, Abteilungen und Arbeitsgruppen eigene Fachархive anzulegen und den Archivbestand optimal zu verwalten. Auch das "Einfrieren" von Informationen, die unter keinen Umständen aus dem Archiv gelöscht werden dürfen, etwa im Rahmen eines so genannten "Legal Holds", ist auf diese Weise umsetzbar. Erleichtert wird die Arbeit mit den archivierten E-Mails auch dann, wenn keine gesonderte Anmeldung erforderlich ist, sondern der Anwender mittels Single Sign-on bereits nach einmaliger Authentifizierung auf die Daten zugreifen kann.

Reduzierung der Ressourcenbelastung

E-Mailarchive können gerade in größeren Unternehmen entscheidend dazu beitragen, die von Anwendern häufig als "Filesystem" missbrauchten Posteingänge und Mailserver zu entlasten. Gängige Be-

helfslösungen wie die Speicherung von lokalen PST-Dateien oder das Einrichten strenger E-Mailquotas für die einzelnen Postfächer sind entweder rechtlich problematisch oder führen durch mehrfaches Vorhalten derselben Daten erst recht zur verstärkten Belastung der IT-Umgebung. Speziell bei höheren Anwenderzahlen kann dies mittelfristig zu einer explosionsartigen Zunahme des Storagebedarfs führen.

Als vorteilhaft können daher Archivierungslösungen gelten, die durch Single Instancing dafür sorgen, dass jede E-Mail und jeder Anhang nur ein einziges Mal gespeichert werden müssen, auch wenn beispielsweise ein Attachment an mehrere Anwender verschickt wurde. Das so genannte Stubbing, bei dem der eigentliche Content (Body) der E-Mail sowie Dateianhänge vom Header getrennt auf einem vom Mailserver unabhängigen Speichersystem gesichert werden, sollte von IT-Administratoren hingegen eher mit Vorsicht genossen werden. Denn mit zunehmender Anzahl an Einträgen in der Datenbank können auch durch die Stubs allein deutliche Performance-Einbußen auftreten, die die entsprechenden Applikationen stark ausbremsen. Zudem kann die Suchfunktion im Archiv durch die Beschränkung auf die Daten im E-Mailheader limitiert sein. Darüber hinaus wird bei solchen Lösungen die Infrastruktur sehr stark erweitert, was dann zu Lasten der Administrierbarkeit geht. Ein Backup einer solchen Lösung wird wider Erwarten nicht einfacher, sondern komplexer, da nicht nur der Mailserver, sondern auch die Archivkomponenten nebst Datenbanken zum gleichen Zeitpunkt gesichert werden müssen.

Fazit

Bei Lösungen für die E-Mail-Archivierung spielen die Faktoren Rechtssicherheit und Entlastung der IT-Ressourcen die entscheidende Rolle. Hinsichtlich der Ernsthaftigkeit und Detailtreue, mit der die Hersteller die umfangreichen gesetzlichen Anforderungen abzubilden versuchen, zeigen sich in der Praxis jedoch große Unterschiede. In Anbetracht der extrem langen Archivlaufzeiten sollte außerdem besonders auf zukunftssichere Standard-Technologien, den Verzicht auf proprietäre Dateiformate und Unabhängigkeit von spezifischen Anwendungen geachtet werden, damit das Archivsystem nicht zum limitierenden Faktor innerhalb der IT-Infrastruktur wird. *(dr)*

Jerry J. Artishdad ist Managing Director der ARTEC IT Solutions AG.

Auswahlkriterien für E-Mail-Archivierungslösungen

	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Lösung ist konsequent auf die aktuellen gesetzlichen Richtlinien abgestimmt	sehr wichtig	sehr wichtig	sehr wichtig
Einfache Installation ohne Änderung bestehender Komponenten	sehr wichtig	sehr wichtig	sehr wichtig
Flexibel mit verschiedenen Mailservern nutzbar	weniger wichtig	wichtig	sehr wichtig
Archivierung der E-Mails im unveränderten Originalformat (SMTP, RFC 822)	sehr wichtig	sehr wichtig	sehr wichtig
Möglichkeit, den unveränderten Originalzustand archivierter E-Mails zu belegen (etwa durch Einsatz von digitalen Signaturen)	sehr wichtig	sehr wichtig	sehr wichtig
Unabhängigkeit von bestimmten Storage-Lösungen	wichtig	wichtig	wichtig
Vermeidung von WORM-Medien	wichtig	wichtig	wichtig
Sichere Verschlüsselung archivierter E-Mails	wichtig	sehr wichtig	sehr wichtig
Leistungsfähige Suchfunktion, die sich auch auf Dateianhänge erstreckt	wichtig	wichtig	sehr wichtig
Schnelle und einfache Wiederherstellung archivierter E-Mails	wichtig	wichtig	wichtig
Mailserver-übergreifende Wiederherstellung archivierter E-Mails	wichtig	wichtig	sehr wichtig
Möglichkeit, individuelle Facharchive anzulegen	weniger wichtig	wichtig	wichtig
Möglichkeit von manueller oder automatischer Verschlagwortung beziehungsweise Vergabe von Attributen	weniger wichtig	wichtig	sehr wichtig
Schutz vor Manipulationen durch Nutzer mit Administrator-Rechten, beispielsweise durch ein Vier-Augen-Prinzip	sehr wichtig	sehr wichtig	sehr wichtig
Reduzierung des Speicherbedarfs durch Single Instancing	weniger wichtig	wichtig	sehr wichtig
Möglichkeit, zusätzliche Funktionen jederzeit nachzurüsten	wichtig	wichtig	sehr wichtig
Möglichkeit der Verknüpfung mit weiteren Content-Typen zu einem ganzheitlichen Unternehmens-Archiv	wichtig	wichtig	sehr wichtig
Investmentschutz durch nahtlose Upgrade-Möglichkeiten	sehr wichtig	sehr wichtig	sehr wichtig
Benutzer-Authentifizierung durch Single Sign-On	wichtig	wichtig	wichtig

it-sa 2010: Der Treffpunkt der IT-Security Branche

- 300 Aussteller mit Lösungen zu Informations-Sicherheit, Datenschutz, Hardware-Sicherung und Security-Awareness
- Non-Stop-Vortragsprogramm auf 3 großen Foren mit 170 Kurzreferaten, Podiumsdiskussionen, Live-Demos und Best-Practice-Beiträgen
- Guided Tours und Topic-Routen
- 20 Kongresse, Tagungen, Workshops, z.B.:
  – Workshop: Forensic Extreme
  – Hacking-Lab: Web Security Hand-on Training
  – Web 2.0 - Web Applications: Advanced

  Mehr Infos: www.it-sa.de/veranstaltungen

it sa

Die IT·Security-Messe

Nürnberg,
19.-21.Okt. 2010

Veranstalter: SecuMedia Verlags-GmbH
Postfach 12 34, D-55205 Ingelheim,
Telefon +49 6725 9304-0, Fax +49 6725 5994

Gastkarte anfordern
www.it-sa.de/e-ticket
Code: 9ADM9682N2

Virtualisierung von Windows-Domänencontrollern (1)

Spiel mit dem Feuer

von Florian Frommherz und Ulf B. Simon-Weidner

Durch Virtualisierung ist der Administrator heutzutage unabhängiger von der Hardware, kann die Infrastruktur verfügbarer gestalten und ist für einen Recovery-Fall bestens gerüstet. Soll jedoch ein Windows-Domänencontroller virtuell betrieben werden, benötigt der Administrator tiefgehendes Know-how des Systems und des Active Directory. Im ersten Teil unserer Workshopserie zur Virtualisierung von Domänencontrollern zeigen wir die spezifischen Probleme – etwa bei der Replikation oder der Netzwerkzeit – dieser Systeme auf und stellen Methoden vor, diese zu vermeiden.

Längst ist Virtualisierung nicht mehr nur ein Mittel, Produktivsysteme für Testzwecke nachzustellen oder neue Software vor dem Einsatz ausführlich auszuprobieren. Die Implementierung virtueller Maschinen und der Einsatz in produktiv genutzten Netzwerken gehört vielerorts bereits zum Alltag. Neben den Möglichkeiten, die Systeme zu konsolidieren, bietet die Virtualisierung noch einen sehr interessanten Nebeneffekt: Da die Hardware durch eine Virtualisierungsschicht abstrahiert ist, können virtuelle Gäste auf einem Virtualisierungshost heruntergefahren und auf einem neuen wieder gestartet werden. Virtualisierung auf VMware ESX oder Microsoft Hyper-V erlaubt sogar das Verschieben von virtuellen Systemen, fast ohne diese offline zu nehmen. Snapshot-Technologien speichern ein Abbild des Servers sogar im laufenden Betrieb. Das Recovery besteht darin, die komplette virtuelle Festplatte zurückzusichern und dann das System sofort wieder zu starten. Dabei ist nicht viel mehr notwendig, als das Computerkonto zurückzusetzen.

Geringe Last auf dem DC

Domänencontroller (DC) sind perfekte Kandidaten für Servervirtualisierung. Der Normalbetrieb von Domänencontrollern erzeugt, ausgenommen sind Großunternehmen mit umfangreichen Verzeichnissen, wenig Last auf den Prozessoren. Lediglich zyklische Dienste, die der Domänencontroller überwiegend mit der PDC-Emulator-FSMO-Rolle ausführt, benötigen mehr Rechenleistung. Der Bedarf an Leistung ist somit stark von der Benutzeranzahl und den allgemeinen Verzeichnisdienstanfragen abhängig. Anfragen auf Domänencontrollern sind absehbar und schwanken selten.

Die Allgemeinlast lässt sich jedoch indirekt durch die Verteilung der Dienste (DNS, DHCP) und die Anzahl der Domänencontroller steuern. Sind mehrere Domänencontroller verfügbar, teilen sie sich bei kluger Konfiguration Authentifizierungs- und DNS-Anfragen auf – es entsteht eine Lastenaufteilung. Der von DCs benötigte Arbeitsspeicher ist gut abschätzbar; neben dem Footprint des Betriebssystems muss Arbeitsspeicher für die Zwischenspeicherung des Verzeichnisses kalkuliert werden. Hier genügt in etwa die Größe der AD-Datenbank mit einem Zusatz für kommendes Wachstum. Obwohl Domänencontroller von Haus aus keine speicherhungrigen Dienste besitzen, sollten ihnen mindestens 2 GByte Arbeitsspeicher zur Verfügung stehen.

Um der "Best Practice"-Empfehlung gerecht zu werden, stets mindestens zwei Domänencontroller pro Domäne zu betreiben, setzen viele Administratoren auf Domänencontroller als VMs. Die DCs sind dabei schnell installiert und dank der zuverlässigen Replikation ist das Vorhaben schnell umgesetzt. Bei Domänencontrollern handelt es sich allerdings nicht einfach um Server, die einen Dienst tun, Sie sollten daher einige Besonderheiten beachten.

Problembereiche der Virtualisierung eines Dömenencontrollers

Domänencontroller stellen den zentralen Knoten der Infrastruktur dar: Sie übernehmen einerseits die Authentifikation von Benutzern, Computern und Diensten und beherbergen andererseits unternehmenskritische Daten wie E-Mailadressen oder Mitarbeiterinformationen. Den oder die Domänencontroller und damit ihre Domänendienste zu verlieren, ist tragisch und trifft Unternehmen härter als der Verlust anderer Dienste. Sind die Domänendienste nicht mehr verfügbar, scheitern nahezu alle Dienste, die auf Domänencontroller angewiesen sind oder die Authentifizierung von Benutzern bedingen: Exchange liefert keine Nachrichten mehr aus, Benutzer können sich nicht mehr an

der Domäne authentifizieren und der Zugriff auf Dateiserver ist nicht gestattet.

Replikationsmechanismen beachten

Vor den genannten Szenarien schützen virtuelle DCs nur indirekt. Zwar erlauben Virtualisierungstechniken, einfacher und kostengünstiger Domänencontroller zu erstellen, doch bergen virtuelle DCs besondere Schwierigkeiten, die es vorab bewusst zu evaluieren gilt. Legen Administratoren DCs auf wenigen oder gar einem einzigen Host ab, besteht die Möglichkeit eines Single Point of Failures (SPOF). Gehostete Domänencontroller sind aus diesem Grund direkt vom Host abhängig und bei einem Ausfall der Virtualisierungslösung nicht mehr erreichbar.

Um sich vor einem SPOF zu schützen und bei möglichen Problemen mit dem Host unabhängig zu bleiben, sollten Sie virtualisierte Domänencontroller auf mehrere Hosts verteilen. Hierbei ist auch zu beachten, dass eine "Replikation" eines virtuellen Hosts nicht ausreichen muss: Viele Unternehmen haben virtuelle Hosts, deren Gastsysteme in einem SAN gespeichert werden, welches in ein anderes Rechenzentrum repliziert wird und im Fehlerfall von dort wieder gestartet werden kann. Es ist jedoch auch schon vorgekommen, dass Fehler zwischen den SANs noch repliziert wurden und die Maschinen auf der anderen Seite sich auch nicht mehr starten ließen. Auch ein repliziertes SAN kann einen SPOF darstellen. Daher ist es wichtig, nicht nur eine Virtualisierungsinfrastruktur zu betreiben, sondern auch eine zweite, auf der die wichtigen Dienste repliziert werden. Steht nur eine Virtualisierungsinfrastruktur zur Verfügung, sollten Sie in Erwägung ziehen, nicht alle Domänencontroller zu virtualisieren und einen Teil als physische Server bestehen zu lassen.

Zu prüfen gilt außerdem, ob der virtuelle Host Mitglied der Domäne wird oder als Standalone-Server fungiert. Bei der Aufnahme in die Domäne kann ein Henne-Ei-Problem entstehen, falls sämtliche Domänencontroller als Gäste in VMs auf dem Host laufen. Wo soll sich der VM-Host anmelden, wenn sämtliche DCs noch nicht verfügbar sind? Das Gleiche gilt auch für die Backup-Server: Hier müssen Sie darauf achten, dass diese bei einem Gesamtausfall unabhängig von der Domäne die Wiederherstellung ermöglichen.

Zeitmanagement für Domänencontroller

Ein verbreitetes Problem während der Erstellung von virtuellen DCs oder des Umzugs von DCs in eine virtuelle Umgebung stellt die Uhrzeit dar. In einer Windows-Infrastruktur muss die Zeit stimmen, da das Authentifizierungsprotokoll Kerberos auf eine angeglichene Zeit besteht. Weicht die lokale Zeit der DCs mehr als die standardmäßig eingestellten fünf Minuten ab, verweigert Kerberos die Authentifizierung. Die Folge ist der Ausfall von Anmeldungen und der Stopp der Replikation zu diesem DC. Mitglieder der Domäne nutzen standardmäßig ihre Domänencontroller als Zeitgeber.

Driftet ihre Zeit ab, korrigieren diese Clients diese automatisch und passen sie der Vorgabe der Domänencontroller an. DCs untereinander synchronisieren ihre Zeit mit dem DC, der die PDC-Emulator-FSMO-Rolle ausübt. Existiert eine Mehr-Domänen-Gesamtstruktur, synchronisieren die PDC-Emulator-Besitzer ihre Zeit wiederum mit dem PDC-Emulator der Gesamtstruktur-Wurzeldomäne. Der für die Zeit verantwortliche Domänencontroller muss stets so konfiguriert sein, dass er eine verlässliche Zeitquelle kontaktieren kann, um anschließend die korrekte Zeit auf alle Systeme der Domäne zu propagieren. Ob diese Zeitquelle eine hardwarebasierte Lösung oder ein entfernter Zeitserver im Internet ist, spielt hierbei keine Rolle.

Das Problem "Zeit" beginnt mit einem Feature vieler Virtualisierungslösungen, das die Uhrzeit einer VM über den Host abgleicht. Der Host sorgt in regelmäßigen Abständen dafür, dass die Zeit seiner VMs mit der Hostzeit übereinstimmt. Es wird aktiv in die Zeit der Clients, also auch in die VM selbst, eingegriffen. Setzt der Administrator die Zeit manuell in der VM, überschreibt der Host sie kurzerhand, um die Zeitdiskrepanz zu minimieren. Das Feature kann zu Problemen führen, wenn die Zeit des Hosts von der Zeit der Domäne abweicht.

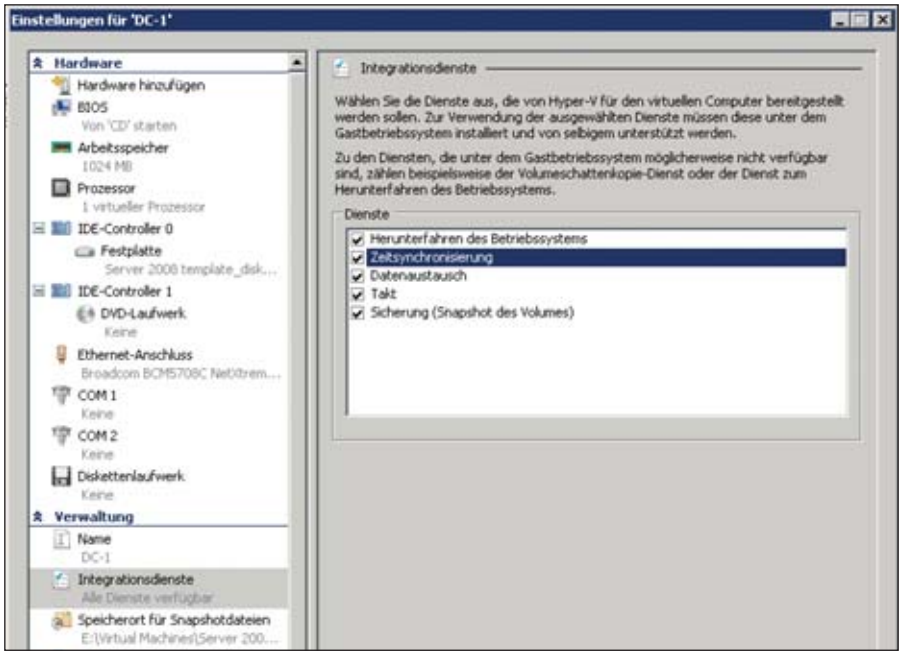


Bild 1: In den meisten Virtualisierungslösungen (hier Hyper-V) lässt sich die Zeitsynchronisation zwischen Host und VM steuern

Der eigentliche Mechanismus, die Zeit per Domäne zu propagieren, wird schließlich aktiv verletzt und kann für Inkonsistenzen sorgen. Wir empfehlen daher, die Zeitsynchronisation zwischen VM und Host abzuschalten. Eine weniger drastische Möglichkeit besteht darin, den Host, ob Domänenmitglied oder nicht, so zu konfigurieren, dass auch er einen Domänencontroller als Zeitquelle benutzt oder die Zeit vom gleichen Zeitserver bezieht wie der PDC der Rootdomäne.

Sicherheit durch Aufgabentrennung

Auch in Fragen der Sicherheit gibt es einige beachtenswerte Besonderheiten bei virtuellen Domänencontrollern. Oft werden mehrere unterschiedliche virtuelle Maschinen auf einem Host betrieben und von unterschiedlichen administrativen Gruppen im Unternehmen betreut. Teilweise kommt es sogar vor, dass diejenigen Mitarbeiter der IT, die für die Virtualisierung verantwortlich sind, nicht die gleichen Personen sind, die das Active Directory verwalten. Daher müssen Sie sich Gedanken um den Schutz der virtuellen Maschinen machen. Nicht jeder Daten-Admin, der seine virtuellen Fileserver administrieren will, soll Zugriff auf die DC-VM besitzen – oder sie gar umkonfigurieren können, um ihr Ressourcen zu stehlen.

Das gilt nicht nur für die virtuellen Maschinen, sondern auch für die Sicherung ihrer virtuellen Festplatten. Ihr Diebstahl lässt sich mit dem Raub eines Domänencontrollers vergleichen. Schlimmer noch: Ein gestohlener Domänencontroller fällt im Serverraum schnell auf, eine unbemerkte Kopie einer virtuellen Festplatte ist nicht so leicht zu entdecken. Angreifer können eine Kopie der virtuellen Maschine anfertigen und sie dann zur Kompromittierung der Infrastruktur verwenden. Unternehmen sollten daher die strenge Trennung der Administration beteiligter Dienste erzwingen: Service-Administratoren dürfen sich nur auf die virtuellen Maschinen ihrer Dienste verbinden, Virtualisierungs-Administratoren kümmern sich um die Konfiguration und den Betrieb der VM-Hosts sowie deren Hardware, während das Storage-Team den Zugriff sichert und den Betrieb der Speicherlösung mit den darauf betriebenen VHDs. In überschaubaren Umgebungen reicht es, den Zugriff auf den VM-Host und die Administrationsdienste abzuschotten und sie nur ausgewähltem Personal zugänglich zu machen.

Virtuelle DCs richtig sichern

Sind die virtuellen DCs ausgerollt, wird es höchste Zeit, sich um die Wartung zu kümmern. Ein Punkt, der bei virtuellen sowie physischen Domänencontrollern gleichermaßen wichtig ist, sind Sicherungen. Virtuelle Domänencontroller in Produktivumgebungen müssen Sie stets genauso sichern wie physische Domänencontroller. Eine korrekte Sicherung ist notwendig, um das Active Directory im Falle einer Wiederherstellung in einem konsistenten Zustand zu behalten.

Dabei ist es aber beim Active Directory nicht zwingend notwendig, dass jeder Domänencontroller gesichert ist. Wichtig ist, dass Sie genügend Domänencontroller jeder Domäne sichern, um in jedem Fall eine Sicherung vorrätig zu haben, von der Sie die Domäne wieder aufbauen können (oder einzelne Objekte wieder zurücksichern können). Empfehlenswert ist es auf alle Fälle, mindestens zwei nicht-FSMO-Rolleninhaber pro Domäne zu sichern und regelmäßig zu überprüfen, ob die Sicherung auch funktioniert und Sie auf die Daten zugreifen können. Andere Domänencontroller würden Sie dann durch eine Neuinstallation (oder erneutes DCPromo) zu einem DC heraufstufen, sobald ein oder zwei DCs wieder laufen. Manche Unternehmen bevorzugen es, jeden DC zu sichern und im Fehlerfall lieber mit einer Rücksicherung zu

Checkliste zum Einsatz von virtuellen Domänencontrollern

- Vermeiden Sie die Möglichkeit eines Single-Point-of-Failure.
- Zeitdienst: Entweder konfigurieren Sie für den Virtualisierungshost (für jeden, wenn es mehrere gibt) den gleichen NTP-Server oder Sie schalten die Zeitsynchronisation aus.
- Stellen Sie sicher, dass nur die gewünschten Administratoren Zugriff auf die DCs und deren Daten haben.
- Vermeiden Sie Snapshots, zum Beispiel über direkte Datenträger
- Partitionierung: Soll die AD-Datenbank auf eine eigene Partition? Sollen "lokale" NTBackup- oder Windows-Backups erstellt werden?

arbeiten, als das System neu zu installieren. Welchen Weg Sie wählen, ist Geschmackssache und hängt auch von den weiteren Diensten ab, die auf dem Domänencontroller laufen.

Obwohl die Replikation zwischen Domänencontrollern nahezu automatisch und sehr robust verläuft, reagiert sie auf inkonsistente Daten zwischen den DCs sehr sensibel. Microsoft liefert mit seinem Betriebssystem stets ein eigenes Sicherungswerkzeug, das Windows-Backups erstellen und zurückspielen kann. Bis Windows XP und Windows Server 2003 übernahm NTBackup diese Aufgabe, unter Windows Vista und Server 2008 dann Windows Backup. Die beiden Sicherungswerkzeuge unterscheiden sich in ihrer Grundfunktionalität dadurch, dass NTBackup dateibasierte, Windows Backup hingegen block- und imagebasierte Sicherungen des Systems erstellt. Für die Sicherung des Verzeichnisses wird der "Systemstatus" (englisch System State) benötigt, der neben systemkritischen Komponenten wie Start-, Registrierungs- und Komponentendienstdaten auch die Active Directory-Datenbank beinhaltet.

Ein Backup des Systemstatus reicht jedoch nicht aus, sondern Sie müssen auch weitere Inhalte sichern, um eine Rücksicherung praktikabel zu halten. Mehr zu diesem Thema finden Sie in den Workshops zum Directory Services Restore Mode, Windows Backup, Sicherung des Active Directory sowie Wiederherstellung des Active Directory im Sonderheft II/2010. Für Virtualisierungs-Infrastrukturen sind umfassendere Lösungen mittlerweile in der Lage, die virtuelle Umgebung mitsamt ihrer virtuellen Maschinen zu sichern. Microsoft Data Protection Manager (DPM) kann mit Hilfe des Volume Shadow Copy Service (VSS) virtuelle Maschinen während des laufenden Betriebes sichern – zum Beispiel alle 15 Minuten – und kümmert sich dabei um die besonderen Bedürfnisse von SQL Server-Datenbanken oder Exchange-Servern.

Als nicht unterstützte Backup-Varianten, die das Active Directory, aber auch andere datenbankbasierte Dienste wie Exchange oder SQL in einen korrupten Zustand bringen können, gelten Funktionen wie imagebasierte Sicherungen oder Snapshots der Festplatten beziehungsweise "Undo disks". Während Snapshots bei der Erstellung und dem Betrieb von Testumgebungen ein nutzvolles Feature für den Rücksprung zu einem älteren Betriebszustand sind, können sie für das Active Directory fatale Folgen haben: das Entstehen von sogenannten "lingering objects". Dies sind "übriggebliebene Objekte", die nicht zwischen DCs repliziert werden. Die Folge sind inkonsistente Objektbestände im Verzeichnis, die zwischen Domänencontrollern variieren.

Im zweiten Teil unserer Workshopserie lesen Sie, wie Sie bei virtualisierten Domänencontrollern USN-Rollbacks vermeiden. Außerdem stellen wir Ihnen einige ungewöhnliche, aber nützliche Einsatzmöglichkeiten virtualisierter DCs vor. *(jp)*

Open-Xchange Server 6 aufsetzen

Mailen wie die Großen

von Christian Egle

Der Open-Xchange Server hat sich hierzulande zur beliebtesten Linux-basierten E-Mail- und Groupware-Lösung gemausert. Dieser Workshop begleitet Sie durch den Versionsdschungel der Exchange-Alternative und beschreibt exemplarisch die Installation der freien Open-Xchange Server Community Edition.

Wie von einer Exchange-Alternative zu erwarten, bietet der Open-Xchange Server (OX) E-Mail, Termin-, Kontakt- und Aufgabenverwaltung. Hinzu kommt bei OX noch ein Dokumentenmanagement namens "InfoStore", das mit den übrigen Funktionen eng verknüpft ist. So kann beispielsweise in E-Mails, Aufgaben und Terminen per Infostore-URL auf Dokumente referenziert werden, ohne dass das entsprechende Dokument jeweils noch mit versendet wird. Endanwender greifen auf die Daten im OX entweder via AJAX-basiertem Webfrontend, Microsoft Outlook, WebDAV oder die Mac OS X-Anwendungen Mail, Address Book und iCal zu.

Einsatz im Unternehmen

Zudem etablierte OX mit "Social OX" ein neuartiges Groupware-Konzept: So können Sie mit OX auch E-Mails von externen Webmail-Accounts zentral bearbeiten. Zudem synchronisiert OX die Kontaktdaten des Netzwerks von XING, Facebook oder LinkedIn und stellt diese automatisiert im OX-Adressbuch zur Verfügung. Um die Team- und Projektarbeit mit externen Geschäftspartnern zu vereinfachen, stellt OX Kontaktinformationen und Dokumente auch Mitarbeitern ohne eigenen OX-Zugang sicher und geschützt bereit.

Die lizenzkostenfreie und im Funktionsumfang nicht beschränkte Community Edition gibt es für Fedora, openSUSE und Ubuntu. Auch wenn OX immer wieder aktualisierte Software-Pakete der Community Edition zur Verfügung stellt, sollten diese nicht in kritischen Umgebungen eingesetzt werden. Qualitätsgesicherte Updates, Fixes und Patches liefert OX im Rahmen von Maintenance-Verträgen nur für die OX Server Edition beziehungsweise Hosting Edition.

Abgerundet wird das Produktangebot durch zwei Lösungen, die auf Univention Corporate Server als Betriebssystem-Basis aufsetzen und beide die grafische Univention-Oberfläche zur Installation und Administration der Groupware nutzen: Während sich die OX Appliance Edition an Kleinunternehmen richtet, die selbst einen eigenen Mailserver betreiben wollen, adressiert die Multiserver-fähige Open-Xchange Advanced Server Edition mittelständische und große Unternehmen, die eine individuelle Kommunikationslösung im eigenen Haus realisieren wollen. Um diese evaluieren zu können, müssen Sie entsprechende Testkeys [1] per Mail anfordern. Gleiches gilt für die "OXtender" genannten Software-Erweiterungen, mit denen mobile Endgeräte, Microsoft Outlook und die nativen Mac OS X-Anwendungen Mail, Address Book und iCal als Clients an den OX angebunden werden können. Letztere lassen sich allerdings nicht mit der Community Edition betreiben.

Download und Installation

OX pflegt unter [2] Software-Repositories der Community Edition für verschiedene Ubuntu-, openSUSE- und Fedora-Distributionen. Im Folgenden wird die Installation der Open-Xchange Community Edition auf einem Server auf Basis von Ubuntu 9.10 exemplarisch dargestellt. Diese gilt jedoch analog für ältere Ubuntu-Versionen ebenso wie für openSUSE- und Fedora-Distributionen.

Ergänzen Sie in der Konsole das entsprechende OX-Repository als zusätzliche Installationsquelle am Ende des Files:

```
$ sudo vim /etc/apt/sources.list
[...]
deb http://download.opensuse.org/
  repositories/server:/OX:/ox6/
  xUbuntu_9.10/ /
```

Laden Sie nun den "Package Index" neu. Danach ziehen Sie die Paketbeschreibungen des Software-Repositories auf Ihre Maschine: *$ sudo aptitude update*. Der folgende Befehl startet Download und Installation aller benötigten Softwarepakete:

```
$ sudo aptitude install mysql-server
  open-xchange-meta-singleserver
open-xchange-authentication-database
  open-xchange-spamhandler-default
```

Systemvoraussetzungen

Bei der Hardware gibt sich OX relativ bescheiden und ist mit 2 GByte RAM und 500 MByte auf der Festplatte zufrieden. Hinzu kommt hier noch der Platz für die Daten der Nutzer. Neben einem der oben genannten Betriebssysteme sollten neben einer MySQL-Datenbank, einem Apache- und einem SMTP-Server auch Dovecot, Courier oder cyrus-imapd als IMAP-Server [3] installiert sein. Daneben braucht OX nur noch Sun oder IBM Java Runtime [4].

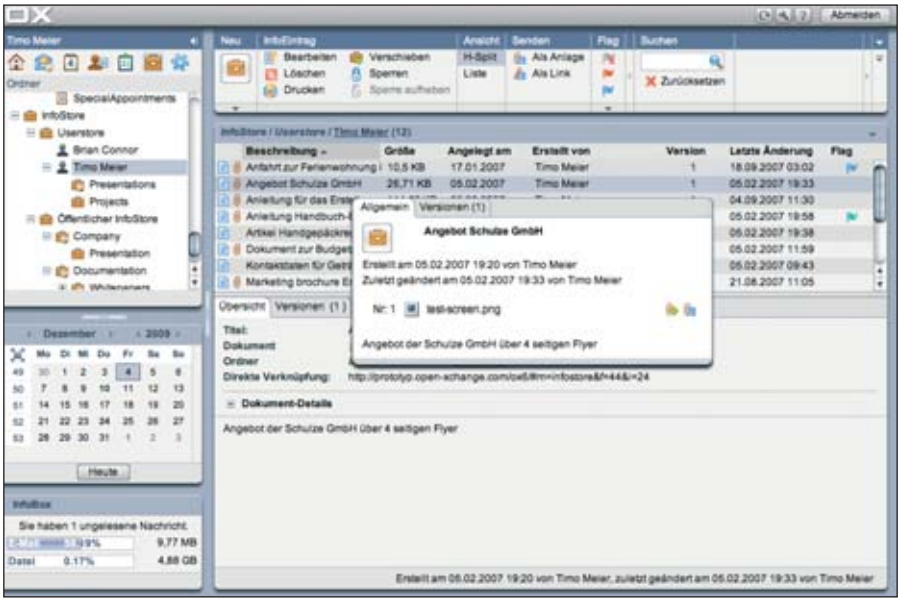


Bild 1: Dokumente werden in persönlichen oder globalen Ordnern versioniert abgelegt und können so gezielt ausgewählten Personen oder allen Mitarbeitern zugänglich gemacht werden

Abhängig von Ihren Systemvoraussetzungen müssen Sie jeweils eines der verfügbaren Spamhandler- und Authentication-Pakete auswählen. Natürlich können Sie alternativ auch alle Softwarepakete einzeln auswählen und installieren [5]. Da die OX-Pakete noch nicht mit einem kryptografisch signierten Schlüssel signiert sind, erscheint ein entsprechender Warnhinweis.

Konfiguration des Open-Xchange Servers

Bitte beachten Sie, dass OX verschiedene Administrationsebenen verwendet, für die Sie unterschiedliche Benutzernamen und Passwörter anlegen müssen. Nachfolgend finden Sie die Usernamen und Passwörter, die wir verwendet haben. Natürlich sollten Sie eigene und "stärkere" Passwörter einsetzen.

- MySQL Datenbank: Username "openexchange"; Passwort im nachfolgenden Beispiel: db_password (wird für alle Datenbank-Operationen benötigt)
- Open-Xchange Admin Master: Username: oxadminmaster; Passwort: admin_master_password (wird für die Verwaltung der einzelnen Kontexte und die Server-Konfiguration benötigt)
- Kontext-Admin: Username: oxadmin; Passwort: admin_password (wird für die Verwaltung von Nutzern, Gruppen und Ressourcen innerhalb eines Kontextes benötigt)

Für die Konfiguration ist eine laufende MySQL-Datenbank notwendig:

```
$ /etc/init.d/mysql start
```

Zudem wird empfohlen, die Open-Xchange Binaries dem PATH hinzuzufügen:

```
$  echo PATH=$PATH:/opt/
  open-xchange/sbin/ >> ~/
  .bashrc && . ~/.bashrc
```

Anschließend wird die Open-Xchange configdb-Datenbank durch Ausführen des initconfigdb-Skripts initialisiert:

```
$ /opt/open-xchange/sbin/
  initconfigdb
  -configdb-pass=db_password -a
```

Geben Sie zusätzlich die Option "-i" ein, wenn Sie eine bereits vorhandene Open-Xchange configdb entfernen möchten.

Der Parameter "-a" generiert zudem einen Administrator-Account in der MySQL-Datenbank, der benötigt wird, um die "oxdatabase" anzulegen. Sie werden Schwierigkeiten mit den nachfolgenden Beschreibungen haben, wenn Sie das MySQL Root-Passwort einsetzen oder diesen Administrator-Account nicht wie beschrieben anlegen.Bevor Sie einen Dienst starten, müssen alle Konfigurations-Files korrekt aufgesetzt sein. Die Option "--configdb-pass" zeigt das Passwort des openexchange Datenbank-Nutzers, während die Option "--master-pass" das Passwort des Benutzers oxadminmaster wiedergibt, das bei der Ausführung des oxinstaller-Skriptes erzeugt wird. Der oxinstaller sieht verpflichtend die Eingabe des Lizenzschlüssels vor:

```
$ /opt/open-xchange/sbin/
  oxinstaller -add-
  license={Lizenzschlüssel}
-servername=oxserver -configdb-
  pass=db_password
-master-pass=admin_master_password
  -ajp-bind-port=localhost
```

Wenn Sie OX nicht lizenzieren wollen, verwenden Sie hier die Option "--nolicense". Nach Initialisierung der Konfiguration starten Sie die OX Administration mit dem Befehl:

```
$ sudo /etc/init.d/
  open-xchange-admin start
```

Jetzt muss der lokale Server an der configdb-Datenbank angemeldet werden:

```
$ /opt/open-xchange/sbin/
  registerserver -n oxserver -A
  oxadminmaster -P
  admin_master_password
```

Anschließend erstellen Sie ein lokales Verzeichnis, in das alle Groupware-Objekte und InfoStore-Dokumente gespeichert werden, und geben dem System-Benutzer entsprechende Zugriffsrechte.

```
$ mkdir /var/opt/filestore
$ chown open-xchange:open-xchange
  /var/opt/filestore
```

Nun registrieren Sie das Verzeichnis als Filestore beim OX-Server:

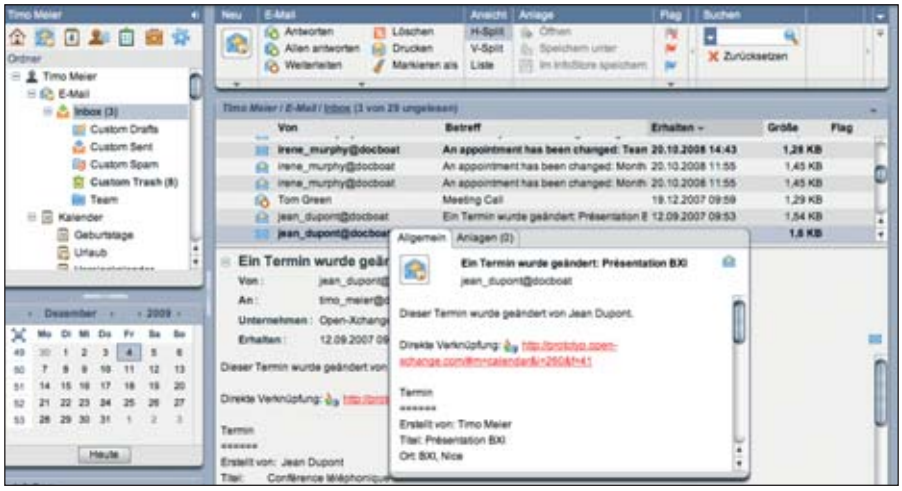


Bild 2: Statt große Dokumente an E-Mails anzuhängen, genügt eine URL zum Dokument im InfoStore. Das spart Bandbreite und ermöglicht zudem noch ein Weiterarbeiten am Dokument, ohne dass dieses jeweils neu versandt werden muss.

```
$ /opt/open-xchange/sbin/
  registerfilestore -A oxadminmaster
  -P admin_master_password
-t file:/var/opt/filestore
```

Zuletzt melden Sie auch noch die Groupware-Datenbank an, in der alle Groupware-spezifischen Informationen gespeichert werden:

```
$ /opt/open-xchange/sbin/
  registerdatabase -A oxadminmaster
  -P admin_master_password
-n oxdatabase -p db_password -m true
```

Webserver und Webfrontend konfigurieren

Nachdem nun der OX und die Datenbank zum Laufen gebracht worden ist, müssen Sie den Apache-Webserver und das Modul "mod_proxy_ajp" konfigurieren, um über das Webfrontend Zugriff auf den OX zu bekommen. Um die Performance des Webclients zu verbessern, empfehlen wir ausdrücklich die Verwendung von "mod_expires" und "mod_deflate". Diese Module limitieren die Zahl der Client-Anfragen und komprimieren die ausgelieferten Inhalte.

```
$ sudo a2enmod proxy
$ sudo a2enmod proxy_ajp
$ sudo a2enmod expires
$ sudo a2enmod deflate
$ sudo a2enmod headers
```

Nun aktivieren Sie diese Module mit:

```
$ sudo /etc/init.d/apache2 force-
  reload
```

Konfigurieren Sie das mod_proxy_ajp-Modul, indem Sie eine neue Apache Konfigurationsdatei anlegen (siehe Listing 1).Starten Sie nach der Konfiguration den Apache Webserver:

```
$ sudo /etc/init.d/apache2 restart
```

Starten Sie die OX Groupware:

```
$ sudo /etc/init.d/open-xchange-
  groupware start
```

Neue Kontexte und Benutzer anlegen

Da die Installation abgeschlossen ist und Sie zumindest schon einen Login-Screen erhalten, wenn Sie auf den Server über Ihren Webbrowser zugreifen, müssen Sie im letzten Schritt nur noch einen Kontext und einen Benutzer anlegen. Unter einem Kontext versteht OX eine geschlossene Benutzergruppe mit einem eigenen, eindeutigen Domainnamen. Ein Kontext wird jeweils für ein Unternehmen beziehungsweise einen Unternehmensbereich angelegt. OX ist mandantenfähig; entsprechend sind die Kontexte vollständig voneinander getrennt. Die Daten eines Kontextes können nur von den Benutzern dieses Kontextes mit den entsprechenden Berechtigungen eingesehen und bearbeitet werden.

Durch die Verwendung von *defaultcontext* können Sie diesen Kontext als Standardkontext für das ganze System nutzen, so dass sich Anwender am OX anmelden können, ohne sich mit ihrer Domain am Login melden zu müssen. Nur ein Kontext kann jeweils als defaultcontext spezifiziert werden. Der oxadmin-User, der mit diesem Befehl generiert wird, ist der Administrator dieses Kontexts. Dieser Account verfügt

```
$ vim /etc/apache2/conf.d/proxy_ajp.conf
<Proxy *>
Order deny,allow
allow from all
</Proxy>
ProxyPass /axis2 ajp://127.0.0.1:8009/axis2 smax=0
   ttl=60 retry=5
ProxyPass /ajax ajp://127.0.0.1:8009/ajax smax=0
   ttl=60 retry=5
ProxyPass /servlet ajp://127.0.0.1:8009/servlet
   smax=0 ttl=60 retry=5
ProxyPass /infostore ajp://127.0.0.1:8009/
   infostore smax=0 ttl=60 retry=5
ProxyPass /publications ajp://127.0.0.1:8009/
   publications smax=0 ttl=60 retry=5
```

Modifizieren Sie die Standardeinstellungen, um den OX Webclient anzuzeigen:

```
$ vim /etc/apache2/sites-available/default
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/
        <Directory /var/www/>
                AllowOverride None
                Order allow,deny
                allow from all
                RedirectMatch ^/$ /ox6/
        </Directory>

   ExpiresActive On
   ExpiresByType image/gif "access plus 23 hours"
   ExpiresByType image/png "access plus 23 hours"
   ExpiresByType image/jpg "access plus 23 hours"
   ExpiresByType image/jpeg "access plus 23 hours"
   ExpiresByType text/javascript "access plus 23
   hours"
   ExpiresByType text/css "access plus 23 hours"
   ExpiresByType text/html "access plus 23 hours"
   ExpiresByType application/x-javascript "access
   plus 23 hours"
   <Files ~ "\.(js|css|gif|jpe?g|png)$">
        Header append Cache-Control "public"
   </Files>
   DeflateFilterNote ratio
   AddOutputFilterByType DEFLATE text/html
text/plain text/xml text/css text/x-js
   application/x-javascript application/javascript
        BrowserMatch ^Mozilla/4 gzip-only-
             text/html
        BrowserMatch ^Mozilla/4\.0[678] no-gzip
        BrowserMatch \bMSI[E] !no-gzip !gzip-only-
             text/html
        Header append Vary User-Agent env=!dont-
   vary
</VirtualHost>
```

Listing 1: Apache-Konfigurationsdatei

über zusätzliche Rechte, die im frei verfügbaren Administrationshandbuch [6] beschrieben sind. Der context id-Parameter muss eindeutig und numerisch sein – andernfalls beschwert sich der Server, wenn Sie versuchen, einen Kontext zu generieren. Weitere Kontexte müssen mit dem oxadminmaster angelegt werden. Neue User-Accounts innerhalb eines Kontextes werden mit dem oxadmin generiert, der zum entsprechenden Kontext gehört. Die Eigenschaft access-combination-name beschreibt die OX-Module und -Funktionen der Nutzer eines Kontextes.

```
$ /opt/open-xchange/sbin/
  createcontext -A oxadminmaster -P
  admin_master_password -c 1
-u oxadmin -d "Context Admin" -g
  Admin -s User -p admin_password -L
  defaultcontext
-e oxadmin@example.com -q 1024
  –access-combination-name=all
```

Zum Anlegen von Nutzern zu Testzwecken verwenden Sie den Befehl:

```
$ /opt/open-xchange/sbin/createuser
  -c 1 -A oxadmin -P admin_password
  -u testuser
-d "Test User" -g Test -s User -p
  secret -e testuser@example.com
–imaplogin testuser –imapserver
  127.0.0.1 –smtpserver 127.0.0.1
```

Log-Files und Problemverfolgung

Unerwartetes und fehlerhaftes Verhalten wird entsprechend dem konfigurierten Loglevel protokolliert und im entsprechenden Ordner des jeweiligen Betriebssystems gespeichert. Ereignisse, die durch die Groupware ausgelöst wurden, finden sich in *Open-Xchange.log*. Werden Ereignisse durch die OX-Administration verursacht, so finden sich diese unter *Open-Xchange-admin.log*. Bei der Fehlersuche sollten Sie diese Files zuerst auswerten:

```
$ tail -f -n200 /var/log/
  open-xchange/open-xchange.log.0
$ tail -f -n200 /var/log/
  open-xchange/
  open-xchange-admin.log.0
```

Alternativ unterstützt OX auch das Logging mittels Syslog, das auf Apache log4j aufbaut, einem Standard-Framework für das Logging von Applikations- und Fehlermeldungen. Mit log4j können Fehlermeldungen direkt lokal oder remote an einen Syslog-Demon oder einen anderen Dienst weitergeleitet werden [7]. Bitte beachten Sie, dass die Standardordner "/var/log/open-xchange" zur Speicherung von Fehlermeldungen nicht mehr genutzt werden, falls log4j-Programme zum Einsatz kommen. Detaillierte Anleitungen für die Syslog-Konfiguration finden Sie unter [8].

Auch wenn die Community Edition von OX nicht offiziell unterstützt wird, so bietet das Unternehmen vielfältige und kostenlose Online-Hilfe mittels umfangreicher Dokumentationen, einer Support-Datenbank [9] und einem Forum [10]. *(jp)*

Links

[1] **Download Open-Xchange und Testkeys**
www.Open-Xchange.com/de/try/download-de/

[2] **Software-Repositories der Community Edition**
http://download.opensuse.org/repositories/server/OX/ox6/

[3] **Unterstützte IMAP-Server**
http://oxpedia.org/wiki/index.php?title=SupportedIMAPServers

[4] **Unterstützte Java-Umgebungen**
http://oxpedia.org/wiki/index.php?title=SupportedJavaRuntimes

[5] **Spamhandler- und Authentication-Pakete**
http://oxpedia.org/index.php?title=Main_Page_CE#quickinstall

[6] **Administrationshandbuch**
http://software.Open-Xchange.com/OX6/doc/OX6-Installation-and-Administration.pdf

[7] **Apache log4j**
http://logging.apache.org/log4j/

[8] **Anleitungen für die Syslog-Konfiguration**
http://oxpedia.org/wiki/index.php?title=Syslog_Configuration

[9] **Supportdatenbank**
http://sdb.Open-Xchange.com/faq/

[10] **Open-Xchange-Forum**
www.Open-Xchange.com/forum/


Quelle: Fabrice Mosca – Fotolia.com

Logdaten mit Splunk auswerten und verwalten (2)

Der Log-Detektiv

von Holger Sesterhenn

Der erste Teil unserer Workshop-Serie zur Logdaten-Analyse mit Splunk führte in die Funktionsweise des Tools ein. Im zweiten und abschließenden Teil nehmen wir Splunk in Betrieb und suchen in Logdaten nach den Ursachen für ein typisches IT-Problem. Nachdem uns das Analysewerkzeug hierbei zur Lösung geführt hat, blicken wir abschließend noch auf Fähigkeiten von Splunk in Sachen Skalierung und Sicherheit.

Nachdem klar geworden ist, wie das System arbeitet, geht es nun an die praktische Anwendung. Unser Szenario ist ein Internet-Shop, basierend auf Apache als Frontend, einem Weblogic-Server als Mittelschicht und einer MySQL-Datenbank im Backend.

Fehlersuche mit Splunk

Das Supportteam erreicht die Beschwerde eines Kunden, dessen Transaktion nicht erfolgreich durchgeführt werden kann ("Error 503"). Üblicherweise beginnt jetzt das Zuschieben des Schwarzen Peters und die am Shop beteiligten Abteilungen starten mit der Suche nach dem Verursacher. Die wenigen Informationen am Anfang – eine IP-Adresse wie 10.2.1.44 – genügen fürs Erste. Mehr geht natürlich immer: Hostname, MAC-Adresse, E-Mail-adresse, Error Code oder etwa die Uhrzeit.

In der "Search Bar" geben wir die uns als Indiz bekannte IP-Adresse ein, wählen als "Matching Term" in unserem Beispiel *<10.2.1.44>* aus und setzen die Suchzeit auf die letzten vier Stunden. Wir suchen also nach dieser IP-Adresse in allen Logdaten von allen angeschlossenen Datenquellen. Noch während die Suche läuft, werden die ersten Suchergebnisse angezeigt (siehe Bild 1). In der Zeitleiste sehen wir die Verteilung der Events im gesuchten Zeitraum. Anomalien im Event-Aufkommen über den Zeitverlauf hinweg können Sie so unmittelbar erkennen. Ein Balken in unserer Sicht repräsentiert eine Minute. Verdächtige Spitzen würden darauf hinweisen, dass jemand versucht, unser System zu attackieren. In diesem Fall sieht alles sehr normal aus: Kunden browsen durch unsere Website.

Im blau hinterlegten Bereich sehen wir die in den gefundenen Events erkannten Felder. Auf der rechten Seite befinden sich im aktuellen Event die extrahierten Felder wie "sourcetype", "source", "host" und "status". Das Feld "status_description" ist allerdings in dem Event überhaupt nicht enthalten, sondern ein Beispiel für "Metadaten". Sie definieren den Wert des Feldes über einen sogenannten "Lookup", bei dem Sie über eine in Splunk hinterlegte CSV-Datei den Werten aus dem Feld "status" einen Text zuweisen und damit ein neues, zusätzliches Feld mit neuem

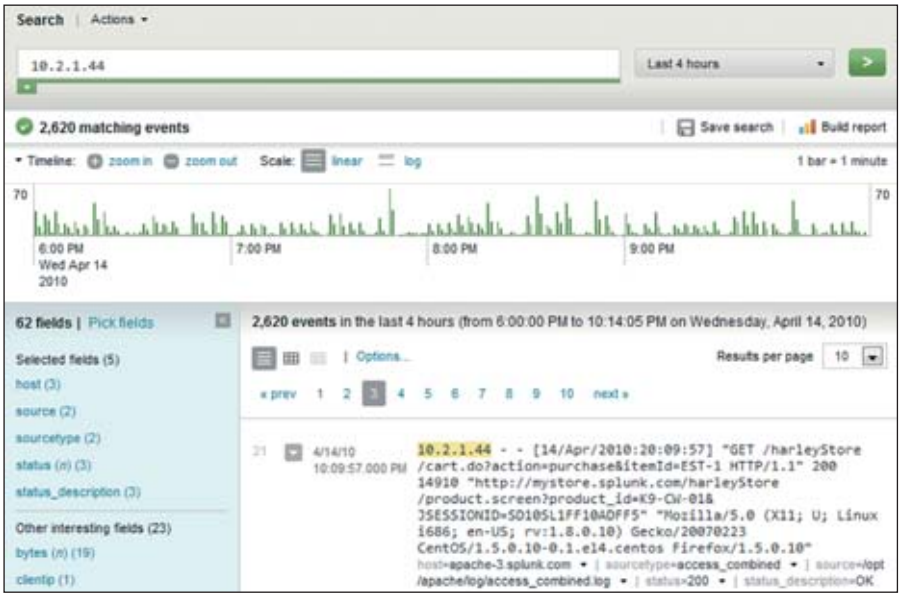


Bild 1: In der Search Bar werden parallel zur Analyse erste Ergebnisse angezeigt

Namen "status_description" erzeugen. Den hier angegebenen http-Status "200" kennt ein erfahrener Administrator natürlich: Alles ist in Ordnung. Aber für jemanden, der nicht sofort etwas mit diesem Wert anfangen kann, ist zusätzliches Wissen automatisch während der Suche hinterlegt.

Durch unsere einfache Suche nach einer IP-Adresse werden natürlich auch sehr viele Events gefunden, die uns im ersten Moment nicht weiterhelfen. Bild 2 zeigt ein Event, das vom Paketfilter des Webservers erzeugt wurde und das wir für die weitere Suche ausblenden wollen. Wir könnten dieses Ziel durch manuelle Ergänzung unserer Suchanfrage um den Ausdruck *NOT sourcetype='iptables'* erreichen, aber viel einfacher ist es, die Möglichkeiten des Web-GUIs zu nutzen und durch die Kombination Alt-Taste und Mausklick auf den Text "iptables" unterhalb des Events eine weitere Bedingung hinzuzufügen. Da alle HTTP-Events mit dem Status 200 und 302 erfolgreiche Zugriffe sind, blenden wir diese ebenfalls aus. Das Web-GUI lässt uns mit allen Daten sehr einfach interagieren. Wir müssen nicht bis ins kleinste Detail die Syntax für eine erfolgreiche Suche kennen, sondern können einfach mit den gegebenen Daten arbeiten.

Während der Kunde die Transaktion anstößt, erhält er vom Webserver die Statusmeldung 503 "Service Unavailable". Über das Feld "status" wählen Sie diesen Wert aus und sehen im Ergebnis ausschließlich Meldungen dieses Typs, die der Anwender im Suchzeitraum erhalten hat. Aus Sicht der Business Owner ist das selbstverständlich vollkommen inakzeptabel – aber machen wir erst einmal weiter.

Wenn wir das Host Field auswählen, sehen wir, dass mehrere Hosts die Anfragen entgegennehmen. Bei dem Versuch, die eigentliche Fehlerursache herauszufinden, begeben wir uns auf die buchstäbliche Suche nach der Stecknadel im Heuhaufen. Es interessiert uns brennend, was sonst

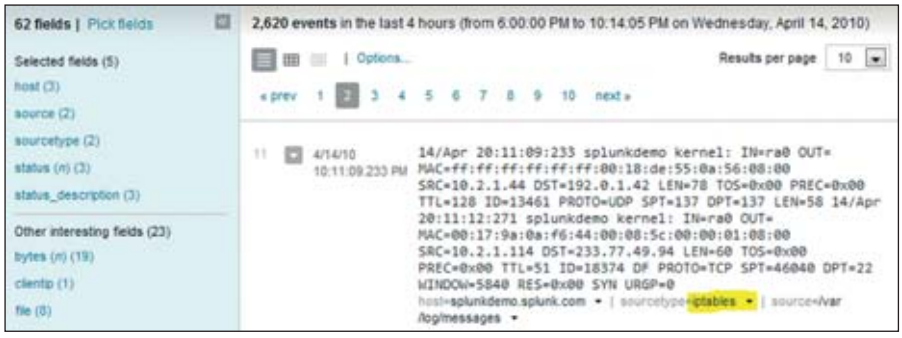


Bild 2: Der Paketfilter des Webservers erzeugt ein Event

noch zur angegebenen Zeit auf anderen Systemen, die zur Web-Applikation gehören, passiert ist. Dazu klicken wir auf den Zeitstempel des "503"-Events und ersetzen die bisherige Suchbedingung durch eine sehr mächtige Bedingung, nämlich ganz einfach "*". Damit wird der angezeigte Zeitraum auf eine Sekunde begrenzt und uns werden alle Daten angezeigt, die in dieser Sekunde erfasst wurden. Das können mehrere hundert Events sein. Splunk macht es uns aber recht einfach, diese zu beherrschen. In unserem Fall bekommen wir im verdächtigen Zeitraum 1.555 Meldungen angezeigt und entdecken: Die Datenbank "mysqld" hat ein Verbindungsproblem. Die Ursache liegt also im Backend, in der Datenbank. Damit haben wir die Fehlerursache innerhalb weniger Minuten lokalisiert und uns viele Stunden mühsamer manueller Loganalyse gespart.

Fehler mit Reports eingrenzen

Bleiben wir weiter bei unserem Fallbeispiel: Wir möchten nun alle Zeitpunkte sehen, zu denen unsere 503-Fehlermeldung in den letzten vier Stunden aufgetaucht ist, und setzen dazu die vom Anfang unserer Suche bekannte Suchbedingung status="503" und den Zeitraum auf "Last 4 hours". Proaktiv erzeugen wir ein neues Dashboard zur leichteren Überwachung des jetzt bekannten Fehlerbildes. Der schnellste Weg hierzu führt über die Option "Build a Report". Ein integrierter Report Builder ermöglicht es auf sehr einfache Weise, neue Dashboards und Reports zu erzeugen. Der Berichtszeitraum für die letzten vier Stunden wurde automatisch übernommen. Im nächsten Schritt erstellen wir ein Chart, das Ihnen die Anzahl der Events für die 503-Fehler grafisch aufbereitet, und klicken dazu auf "Next Step: Format Report", damit das Chart automatisch generiert wird. Nach Klicken auf "Save Report" vergeben Sie einen sinnvollen Namen ("My 503 Report") und haben nun einen gespeicherten Report, den wir innerhalb eines Dashboards verwenden können (siehe Bild 3).

Zur Erstellung des Dashboards klicken Sie oberhalb der Suchzeile auf "Actions" und wählen "Create Dashboard" aus. Nach "Edit the Dashboard" und der Auswahl "Paneltyp=Chart" benutzen Sie Ihre gespeicherte Suche ("My 503 Report") und klicken auf "Add panel". Außerdem können Sie noch ein weiteres Panel für eine andere gespeicherte Suche hinzufügen und wählen hierfür "Add Panel" und erneut "Chart" als Paneltypen. Hier können Sie zum Beispiel eine gespeicherte Suche nach Fehlermeldungen des MySQL-Servers hinzufügen. Die korrekte Positionierung ist per "Drag&Drop" möglich. Damit haben Sie im Handumdrehen eine Ansicht erstellt, die für Ihre Arbeit von Relevanz ist und können dieses Wissen sehr einfach mit anderen Mitarbeitern und/oder Abteilungen teilen.

Einsatz in verteilten Architekturen

Für den Einsatz in verteilten Systemen bringt Splunk die beiden Komponenten "Splunk Forwarder" und "Light Forwarder" mit. Forwarder sind Splunk-Server, die Logdaten vorverarbeiten und dann an einen zentralen Splunk-Server weiterleiten können. Der Light Forwarder ver-

zichtet auf eine Vorverarbeitung, bietet aber trotzdem noch die Möglichkeit, Daten komprimiert und verschlüsselt weiterzuleiten. Im Falle eines Netzwerkausfalls werden die Daten grundsätzlich gepuffert. Beide Varianten können in Architekturen eingesetzt werden, in denen die Logdaten zum Beispiel nicht einfach über das Netzwerk transportiert werden können. Splunk Forwarder können lokale Anwendungs-Logs überwachen, die Ausgabe von Status-Befehlen nach Zeitplan sicherstellen, Performance-Metriken von virtuellen oder nicht-virtuellen Quellen abgreifen oder Filesysteme im Hinblick auf Änderungen von Konfigurationen, Berechtigungen und Attributen überwachen. Forwarder übertragen die Daten in komprimierter Form und SSL-verschlüsselt zum zentralen Splunk-Server.

Wachstum, Sizing, Lastverteilung und HA

Wenn die täglichen Logvolumina und die Anzahl der Datenquellen wachsen, können Sie die Indexierungsleistung steigern, indem Sie einfach weitere Indexer auf Standard-Hardware hinzufügen. Die Lastverteilung übernimmt das Splunk-interne Loadbalancing. Vielleicht noch wichtiger, weil unmittelbar zu spüren, ist die Suchperformance. Die Geschwindigkeit von Suchabfragen hängt allgemein von der Anzahl der gleichzeitigen Suchanfragen, deren Komplexität, dem zu durchsuchenden Logdatenvolumen und dessen Verteilung auf verschiedene Systeme sowie von der Hardware-Performance ab. Splunks Search-Performance wächst nahezu linear mit der Anzahl der integrierten Indexer.

Eine absolut exakte Hardware-Dimensionierung macht wenig Sinn, da der Performance-Bedarf unterschiedlicher Suchen sehr stark variieren kann. Index Volume und Search Load sind die bestimmenden Faktoren des Hardware-Sizings. Ebenso ist die Geschwindigkeit der Harddisk I/O-Zyklen maßgeblich. Die gute Nachricht: Aktuelle Standard-Server-Hardware ist völlig ausreichend. Bei bis zu 100 GByte am Tag im Mittel (und das ist schon hoch angesetzt) und maximal vier Benutzern (Searchers) genügt nur eine Maschine in Multifunktionskonfiguration.

Sicherheit im Blick

Klassische Host- und Netzwerk-Intrusion-Detection-Systeme (HIDS, NIDS) waren technisch bislang kaum in der Lage, Angriffe etwa in Form von Rechtemissbrauch, Missbrauch von Benutzeridentitäten und Insider Threat zu erkennen, da sie in erster Linie mit wissensbasierten Erkennungsmethoden (Signaturen) arbeiten. Hinzu kommt, dass die Sinnhaftigkeit eines Einsatzes von HIDS/NIDS dann in Frage gestellt werden muss, wenn an den derzeit technisch möglichen Integrationspunkten überwiegend verschlüsselter Datenverkehr keine effektive Angriffserkennung zulässt.

Die effiziente Erfassung und Auswertung von Loginformationen jeglicher Datenquellen – die sicherheitsrelevante Ereignisse aufzeichnen, auswerten, melden, speichern und archivieren – ermöglicht oft einen wesentlich höheren Gewinn an Sicherheit und kann auch unter Compliance-Aspekten im Sinne einer Erkennung und/oder Verhinderung von Eindringversuchen durchaus als "Intrusion Detection System" betrachtet werden. Beispielsweise findet sich folgende Aussage in der Compliance-Vorschrift PCI DSS 1.2.1: "Zur Konformität mit Anforderung 10.6 können Protokoll-, Harvesting-, Analyse- und Alarmtools eingesetzt werden." Branchen, die Kreditkarteninformationen verarbeiten und somit PCII DSS unterliegen, nutzen jedoch in hohem Maße eigenentwickelte Lösungen mit proprietären Logformaten. Hier bietet sich der Einsatz von Universal Indexing in Verbindung mit intelligenten Searches und Reporting geradezu an.

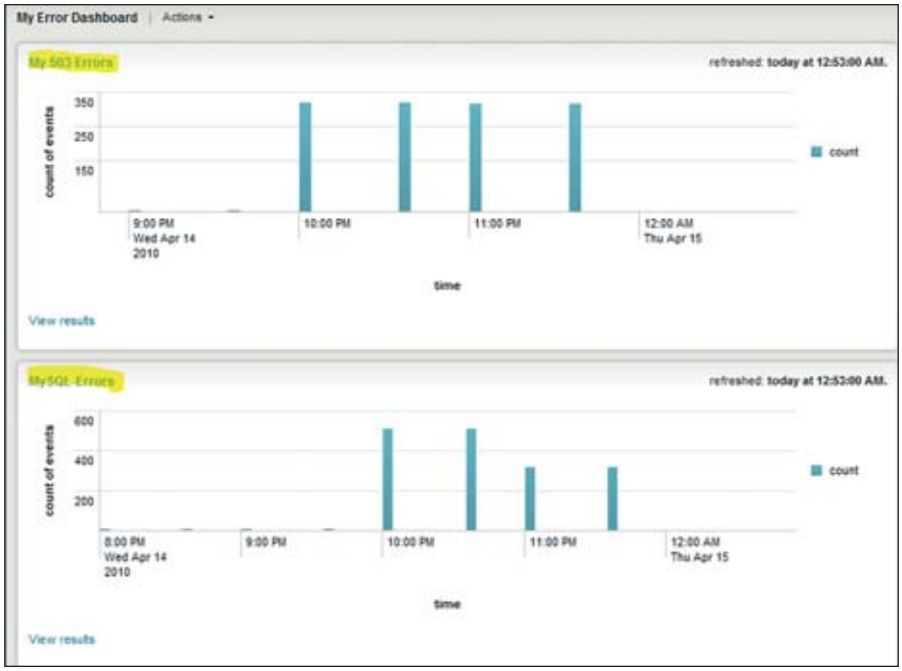


Bild 3: Ein integrierter Report Builder ermöglicht es auf sehr einfache Weise, neue Dashboards und Reports zu erzeugen

Fazit

Log-Management-Systeme ermöglichen IT-Administratoren den zentralen Zugriff auf umfangreiche Logdatenbestände. Mit intelligenten Suchfunktionen können Probleme effizienter analysiert und Ursachen schneller aufgedeckt werden. Durch nachweisbar verringerte Reaktionszeiten, sinkende Ausfallhäufigkeit und -dauer sowie zentralisierte Verwaltung der Logs können Betriebsabläufe optimiert und IT-Teams wirksam entlastet werden. *(dr)*

Dipl.-Ing. (FH) Holger Sesterhenn, CISSP, ist Consultant IT-Security bei IT-CUBE SYSTEMS, einem auf IT-Security spezialisierten Systemintegrator.

Erscheinungstermin:
Ende Oktober 2010

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/

---

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 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 0910

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

Externen Zugriff auf Exchange Server 2010 einrichten

Reisebegleiter E-Mail

von Oliver Ebel

Der sichere Zugriff auf das Exchange-Postfach von unterwegs per Microsoft Outlook, Outlook Web Access oder Smartphone ist schon seit einigen Jahren fester Bestandteil der Messaging-Infrastruktur vieler Unternehmen. Mit den aktuellen 2010er-Versionen von Exchange, Forefront TMG und Outlook baut Microsoft auf dieser bewährten Basis auf. Die Konfiguration einer solchen Kommunikations-Umgebung erfordert aber eine detaillierte Betrachtung aller beteiligten Komponenten. IT-Administrator zeigt Ihnen, wie Sie den Remote-Zugriff einrichten.

Mit den richtigen Einstellungen steht das Exchange-Postfach auch unterwegs zur Verfügung

Unter Exchange Server 2010 dient die Clientzugriffs-Serverrolle als Kommunikationsschnittstelle zwischen den unterstützten Clients und der Exchange-Gesamtstruktur. Zusätzlich beinhaltet die Serverrolle auch den Verfügbarkeitsdienst für Frei-/Gebucht- Informationen und den Auto-Ermittlungsdienst ("Autodiscover", stellt automatische Konfigurationseinstellungen für Outlook-Clients bereit). Die folgenden Zugriffsmethoden stehen dabei unter Exchange 2010 zur Verfügung: RPC-Clientzugriff (Outlook Anywhere), Outlook Web App, POP3, IMAP4 und Exchange ActiveSync.

Zugriffe unter Exchange 2010

Die Verwendung des Outlook-Clients stellt zweifelsohne die meistgenutzte Form des Exchange-Zugriffs dar, womit auch der RPC-MAPI-Clientzugriff überwiegt. Dabei ist zu beachten, dass Exchange 2010 in der Standardeinstellung nur verschlüsselte RPC-Verbindungen zulässt. Dies bedeutet für die Praxis, dass Outlook 2003 für die Verschlüsselung explizit konfiguriert werden muss, während Outlook 2007 und 2010 diese Einstellung standardmäßig bereits aktiviert haben. Die Verschlüsselungsanforderung können Sie serverseitig per PowerShell deaktivieren – aus Gründen der Sicherheit ist dies jedoch nicht empfehlenswert. Weitere Informationen zum Thema RPC-Verschlüsselung und deren Konfigurationsmöglichkeiten finden Sie bei Microsoft in einem dedizierten KB-Artikel unter [1]. Zur Anbindung von Outlook Express oder E-Mail-Applikationen von Drittherstellern wie etwa Eudora unterstützt Exchange 2010 zudem die Protokolle POP3 und IMAP4. Standardmäßig sind diese deaktiviert, weshalb Sie vor der Nutzung zunächst die POP3- und IMAP4-Dienste des Exchange-Clientzugriffsservers starten müssen.

Der webbasierte Zugriff auf das Postfach erfolgt unter Exchange 2010 mittels "Outlook Web App", früher Outlook Web Access. Dabei werden neben dem Internet Explorer nun auch Firefox, Safari und Chrome vollständig unterstützt. Exchange ActiveSync ist ein auf HTTP und XML basierendes Synchronisierungsprotokoll für geringe Bandbreiten und hohe Latenzzeiten. Es eignet sich damit perfekt zur Anbindung von Mobiltelefonen (Windows Mobile 5.0 und höher) sowie Smartphone-Geräten von Drittherstellern wie Nokia, Palm oder Apple. Mittels Direct Push-Technologie werden dabei geänderte Exchange-Postfachdaten (etwa neue Email-Nachrichten) via HTTPS-Verbindung auf das Endgerät übertragen.

Einrichtung der Komponenten

Im Folgenden betrachten wir den grundlegenden Aufbau einer Exchange-basierten Kommunikationsinfrastruktur. In der Praxis wird häufig noch eine zusätzliche Dritthersteller-Firewall vor dem TMG 2010 betrieben; dies ist allerdings für die primäre Konfiguration der Microsoft-basierten Komponenten nachrangig.

Neben dem Domain Controller sind die Microsoft-Zertifikatsdienste in Form einer Active Directory-integrierten Unternehmens-Stammzertifizierungsstelle auf einem separaten Server installiert. Diese können in einer Testumgebung auch zusätzlich auf dem Domain Controller betrieben werden. Alle Server verwenden als Betriebssystem Windows 2008 R2, sind Mitglied einer Active Directory-Domain und mit aktuellen Microsoft-Updates versehen. Die TMG 2010-Firewall stellt mit zwei Netzwerkkarten die Konnektivität zwischen internem Unternehmensnetz und dem Internet sicher. Auf dem Ex-

change 2010 Server sind die Standard-Exchange-Rollen Clientzugriffsserver, Hub-Transport-Server und Postfachserver installiert.

Zur Authentifizierung und zum Schutz der übermittelten Daten ist ein Zertifikat erforderlich, das die Kommunikation per HTTPS (TCP Port 443) für Outlook Web App, Outlook Anywhere (RPC/HTTPS) und Exchange ActiveSync ermöglicht. Hierfür sollte ein sogenanntes SAN-Zertifikat (Subject Alternative Name) verwendet werden – also ein Zertifikat, das für mehrere Server-Namen beziehungsweise URLs gültig ist. Prinzipiell lassen sich auch normale Single-Name-Zertifikate einsetzen, die Konfiguration gestaltet sich dann jedoch wesentlich komplexer. Wegen der mit zusätzlichen Kosten verbundenen Nutzung einer öffentlichen Zertifikatsstelle (Certificate Authority, CA) verwenden wir im Folgenden eine interne Windows-basierte, AD-integrierte CA zur Erstellung eines SAN-Zertifikats. Falls in einer produktiven Umgebung noch eine CA auf Basis von Windows 2003 zum Einsatz kommt, müssen Sie die Ausstellung von SAN-Zertifikaten zuerst mit dem Befehl

```
certutil -setreg policy\EditFlags
  +EDITF_ATTRIBUTESUBJECTALTNAME2
```

aktivieren und anschließend die Zertifikats- und IIS-Dienste neu starten. Das Erstellen einer Zertifikatsanforderung können Sie wie unter Exchange 2007 per PowerShell mit dem Befehl *New-ExchangeCertificate* ausführen:

```
New-ExchangeCertificate
  -GenerateRequest -Domainname
  servername.domain.local,servername,
  autodiscover.domain.local,mail.
  domain.de,autodiscover.domain.de -
  PrivateKeyExportable $True |
  Set-Content -Path c:\CertRequest.req
```

Die fertige Zertifikatsanforderung liegt nun in Form einer Textdatei vor (definiert durch die Option "-Path"). Beachten Sie dabei, dass Sie all diejenigen Namen aufführen (Option "-DomainName"), unter deren Verwendung auf den Exchange-Server zugegriffen werden soll. Dies schließt alle internen und externen Namen ein, wobei mit Ausnahme des internen Server-NETBIOS-Namens ausschließlich Full Qualified Domain Names (FQDN) zum Einsatz kommen:

- interner Server-FQDN (servername.domain.local)
- interner Server-NETBIOS-Name (servername)
- interner Autodiscover-FQDN (autodiscover.domain.local)
- externer Server-FQDN (mail.domain.de)
- externer Autodiscover-FQDN (autodiscover.domain.de)

Diese Liste ließe sich mit zusätzlichen Namen erweitern; ein Beispiel wäre die Veröffentlichung von Outlook Web App über die URL *owa.domain.de* als weiterer externer Server-FQDN. Bei einer Veröffentlichung des Exchange-Servers mittels ISA oder TMG sollte sich der interne Server-FQDN an erster Stelle befinden. Die im obigen Beispiel verwendete interne AD-Domain und öffentliche DNS-Domain müssen Sie entsprechend abändern.

Neu in Exchange 2010 ist die Möglichkeit, die Zertifikatsanforderung über die "Exchange Management Tools" ohne Zuhilfenahme der PowerShell zu erstellen. Hierfür starten Sie im Aktionsbereich unter "Serverkonfiguration" den entsprechenden Assistenten mit dem Menüpunkt "Neues Exchange-Zertifikat …", geben die oben bereits angeführten Daten ein und erhalten zum Schluss ebenfalls eine Zertifikatsanforderung in Form einer Textdatei. Mit dieser können Sie nun über die Webschnittstelle der internen Zertifikatsstelle (*https://ca-servername.domain.local/certsrv*) das eigentliche Zertifikat ausstellen. Als Zertifikatvorlage wählen Sie dabei "Webserver" aus. Eine weitere Möglichkeit zur Zertifikatsausstellung liefert im Übrigen das MMC-Zertifikats-Snap-In ("Alle Aufgaben / Neues Zertifikat anfordern …"). Abschließend muss noch das Zertifikat in den Zertifikatsspeicher des Exchange-Servers importiert und aktiviert werden. Auch dies kann wiederum über die Exchange Management Tools, per MMC-Zertifikats-Snap-In oder PowerShell, erfolgen:

```
ImportExchangeCertificate -FileData
  ([Byte[]]$(Get-Content -Path
  c:\certificate.cer -Encoding Byte
  -ReadCount 0)) | Enable-Exchange-
  Certificate -Services IIS
```

Weitere Informationen zur Handhabung von Zertifikaten im Exchange-Umfeld finden Sie unter [2].

Firewall-Konfiguration

Vor Beginn der Konfiguration von Zugriffsregeln in TMG 2010 muss zunächst das für den Exchange-Server ausgestellte Zertifikat in den Zertifikatsspeicher des TMG-Servers importiert werden. Dies erfolgt am einfachsten per MMC über das Zertifikats-Snap-In.

Mit Hilfe der Forefront TMG-Verwaltungskonsole können Sie nun den externen Zugriff auf den Exchange-Server konfigurieren. Dies wollen wir zunächst für die Komponente "Outlook Web" tun. Hierfür wählen Sie im Aktionsfeld des Bereichs "Firewallrichtlinie" den Punkt "Exchange-Webclientzugriff veröffentlichen", wodurch der Assistent für neue Exchange-Veröffentlichungsregeln gestartet wird. Als Namen für die zu erstellende Regel verwenden Sie "Exchange-OWA" (da wir zunächst den Zugriff per Web aktivieren möchten), wählen anschließend als Exchange-Version "Exchange Server 2010" und im Bereich Webclient-E-Mail-Dienste "Outlook Web Access" aus. Nachfolgend sind noch der korrekte Veröffentlichungstyp ("Einzelne Website oder Lastenausgleich veröffentlichen") und die Sicherheit der Server-Verbindung (SSL) zu definieren. Der interne Sitename (interner Server-FQDN des Exchange-Servers) muss ebenso wie der externe Name, unter dem der OWA-Dienst von außen angesprochen werden soll, in identischer Schreibweise im Zertifikat aufgeführt sein.

Bild 1: Die clientseitigen RPC/HTTPs-Einstellungen für den externen Outlook Anywhere-Zugriff. Dabei lassen sich die RPC-Pakete in HTTP einbetten.

Innerhalb des Assistenten konfigurieren Sie anschließend einen neuen Weblistener, der die eingehenden Anfragen abhört. Nach Angabe eines Namens wählen Sie auch hier als Sicherheitsoption für die Weblistener-Clientverbindung "SSL" aus. Nach Auswahl des externen Netzbereichs (oder einzelner externer IP-Adressen) und des zuvor importierten Zertifikats ist noch die Art der Authentifizierung festzulegen – wir wählen die HTML-Formular-Authentifizierung sowie die Überprüfung gegen Active Directory. Damit ist die Erstellung des Weblisteners abgeschlossen und Sie können mit der Konfiguration der Veröffentlichungsregel fortfahren. Diese schließen Sie mit der Auswahl der Authentifizierungsdelegierung (Standardauthentifizierung) und der Benutzersätze (Alle authentifizierten Benutzer) ab. Damit ist nun der Zugriff auf die Exchange-Postfächer per Outlook Web App unter der externen Adresse *https://mail.domain.de/owa* aktiviert. Beachten Sie: In der Standardeinstellung kann der Benutzer sein Kennwort aus Sicherheitsgründen nicht per OWA ändern; dies kann jedoch in den Eigenschaften des zugehörigen Weblisteners unter dem Reiter "Formulare" aktiviert werden.

Auch den externen Zugriff mit Hilfe des Outlook-Clients auf das jeweilige Exchange-Postfach können Sie auf analoge Weise per Assistent konfigurieren. Hierfür wählen Sie für den Regel-Namen "Exchange-OA" als Webclient-E-Maildienst "Outlook Anywhere (RPC/HTTPs)" und aktivieren außerdem die Option "Zusätzliche Ordner für Outlook 2007 veröffentlichen". Wie zuvor kommt auch hier als Veröffentlichungstyp "Einzelne Website oder Lastenausgleich veröffentlichen" und "SSL" für die Sicherheit der Serververbindung zum Einsatz. Als internen Sitenamen verwenden Sie den internen Server-FQDN sowie *autodiscover.domain.de* als externen Autodiscover-FQDN. Auch an dieser Stelle hilft wieder ein dedizierter Weblistener weiter, der mittels SSL-Verschlüsselung auf der externen Netzwerkkarte unter Nutzung des bereits importierten SAN-Zertifikats sichere Verbindungen von außen annimmt. Abweichend zur Konfiguration des OWA-Weblisteners wird nun aber die HTTP-Standard-Authentifizierung genutzt. Falls alle Clients Mitglied der internen Active Directory-Domain sind, können Sie auch die integrierte HTTP-Authentifizierung verwenden. Zum Abschluss der Veröffentlichung von Outlook Anywhere aktivieren Sie noch die Standardauthentifizierung für alle authentifizierten Benutzer und einer externen Nutzung von Outlook ohne klassische VPN-Verbindung steht nichts mehr im Wege.

Zugriff für Smartphones

Zuletzt wollen wir noch die Anbindung für Mobilgeräte einrichten. Hierfür wählen Sie im Exchange-Veröffentlichungs-Assistenten den Dienst "Exchange ActiveSync" aus (als Regel-Namen legen wir "Exchange-AS" fest) und bestimmen wie bereits bei den beiden vorherigen Exchange-Zugriffsregeln als Veröffentlichungstyp "Einzelne Website" und für die Sicherheit "SSL". Analog zur Veröffentlichung von Outlook Anywhere definieren Sie für den internen Sitename den internen Server-FQDN sowie *autodiscover.domain.de* als externen Autodiscover-FQDN. An dieser Stelle lässt sich der bereits bestehende Weblistener verwenden, der zuvor für Outlook Anywhere erstellt wurde. Analog dazu vervollständigen Sie die Konfiguration durch Auswahl der Standardauthentifizierung für alle authentifizierten Benutzer und können ab sofort Mobilgeräte mit dem Exchange-Server verbinden.

In der Tabelle "Freigabepfade der TMG-Zugriffsregeln" sind die Freigabepfade aller oben konfigurierten Exchange-Veröffentlichungsregeln zusammengefasst. Diese

Freigabepfade der TMG-Zugriffsregeln

Exchange-Dienst	Freigabepfade
Outlook Web App (OWA)	/owa/* /public/* /exchange/* /ecp/*
Outlook Anywhere (RPC/HTTPs)	/rpc/* /oab/* /ews/* /autodiscover/*
Exchange ActiveSync	/microsoft-server-activesync/*

Pfade werden dabei automatisch vom Assistenten für die Veröffentlichung konfiguriert und sollten bei auftretenden Problemen auf Korrektheit überprüft werden.

Einrichtung des Outlook-Clients

Die Konfiguration von Outlook erfolgt normalerweise automatisch unter Nutzung des von Exchange 2010 bereitgestellten Autodiscovery-Features. Wir wollen im Folgenden jedoch eine manuelle Konfiguration der wesentlichen Kontoeinstellungen für den externen Outlook-Zugriff vornehmen. Hierzu öffnen Sie in Outlook 2010 unter "Datei / Informationen / Kontoeinstellungen / E-Mail" die bestehende Exchange-Postfach-Konfiguration über den Menüpunkt "Ändern" und wechseln über den Button "Weitere Einstellungen…" in den Reiter "Verbindung". Das Menü zur Eingabe der relevanten "Outlook Anywhere"-Einstellungen öffnet sich durch Aktivierung der Option "Verbindung mit Microsoft Exchange über HTTP herstellen" und den Button "Exchange-Proxyeinstellungen…".

Hier nutzen Sie die externe Autodiscover-URL, die sich auch in der Namensliste des Zertifikats befindet. Weiterhin aktivieren Sie den Punkt "Bei langsamen Netzwerken zuerst eine Verbindung über HTTP herstellen, dann über TCP", damit beim Betrieb am internen (schnellen) LAN zuerst ein regulärer Verbindungsaufbau initiiert wird. Bei Problemen mit der externen Verbindung von Outlook zum Exchange-Server empfiehlt sich ein Blick in den aktuellen Verbindungsstatus; der Aufruf erfolgt bei gedrückter Strg-Taste mit einem rechten Mausklick auf das Outlook-Icon in der Taskleiste und der Auswahl des Menüpunkts "Verbindungsstatus…".

Neben der manuellen Konfiguration bietet Microsoft auch verschiedene Wege, diese Einstellungen automatisiert auf den Clients anzubringen. Eine Möglichkeit stellt dabei das Office-Anpassungstool (OAT) [3,4] dar, mit dem Sie eine MSP-Datei erzeugen und während der Office-Installation die gewünschten Einstellungen vornehmen können. Eine bestehende Installation kann ebenfalls mit diesem Werkzeug geändert werden, und zwar durch Erstellung einer PRF-Datei direkt aus dem OAT heraus. Diese Text-Datei (lässt sich also auch manuell per Texteditor ändern) speichert Outlook-Profil-Einstellungen, die Sie importieren können:

```
outlook.exe /importprf
  \\server\freigabe\outlook.prf
```

Fazit

Die Kombination Outlook, Exchange und TMG bietet in den aktuellen 2010er-Versionen eine optimale Kommunikationsplattform für Mitarbeiter auch außerhalb des Firmennetzes ohne die Notwendigkeit einer klassischen VPN-Verbindung. Dabei wurden die bekannten Zugriffsmöglichkeiten aus Exchange 2007 beibehalten und weiterentwickelt. Aus Sicht der IT-Administration hat sich insbesondere die Konfiguration der TMG-Firewall durch den Exchange-Veröffentlichungs-Assistenten im Vergleich zum Vorgänger ISA 2006 erheblich vereinfacht. Einen entscheidenden Punkt stellt nach wie vor die Handhabung des Zertifikats dar, das Basis für die gesicherte externe Verbindung ist; auch in diesem Bereich hat Microsoft mittels eines Assistenten die notwendigen Arbeitsschritte im Vergleich zur Vorgängerversion entscheidend erleichtert. *(dr)*

Links

[1] RPC-Verschlüsselung mit Konfigurationsmöglichkeiten
http://support.microsoft.com/kb/2006508/

[2] Verwalten von SSL für einen Clientzugriffsserver
http://technet.microsoft.com/de-de/library/bb310795.aspx

[3] Office-Anpassungstool in Office 2010
http://technet.microsoft.com/de-de/library/cc179097.aspx

[4] Outlook Automatic Account Configuration
http://go.microsoft.com/fwlink/?linkid=79065&clcid=0x407

Linux-Systeme mit Spacewalk verwalten (2)

Software im Fluss

von Thorsten Scherf

Der zweite Teil unserer Workshopserie zum Systemmanagement mit Spacewalk führt uns zunächst in die Welt der Software-Kanäle. Diese dienen innerhalb von Spacewalk zur komfortablen Softwareverteilung. Nach der Konfiguration der Kanäle müssen nur noch die Clients mit diesen verbunden werden und schon verfügt der IT-Verantwortliche über eine State of the Art-Softwareverteilung. Zum Abschluss des Workshops wenden wir uns schließlich noch möglichen Wegen der automatischen Softwaredistribution zu.

Zu Beginn useres zweiten Workshopteils und nach dem Spacewalk-Setup richten Sie den ersten Software-Kanal für die Client-Systeme ein. Bei deren Registrierung müssen Sie genau einen Basiskanal für das System angeben, aus dem es die Betriebssystem-Pakete und deren Updates beziehen kann. Natürlich lassen sich zu diesen Basis-Kanälen weitere Subkanäle einrichten, die Sie ebenfalls den Clients zuordnen können. Über diese Subkanäle können Sie wiederum weitere RPM-Pakete auf die Systeme verteilen. Dies sind sowohl selbstgebaute Pakete als auch RPMs aus anderen Repositories.

Software-Kanäle für den Paketfluss

Software-Kanäle richten Sie am einfachsten über das Webinterface ein unter "Channels / Manage Software Channels / Create". Dank der Spacewalk-API besteht auch die Möglichkeit, diese Aufgabe über ein Skript zu erledigen. Ein beispielhaftes Python-Skript finden Sie unter [1]. Dieses lässt sich wie folgt aufrufen:

```
# ./create_channel.py –label=fedora-
  12-i386 –name "Fedora 12 32-bit"
  –summary "32-bit Fedora 12 channel"
```

Einen Software-Kanal richten Sie am einfachsten über das grafische Webinterface ein. Im Skript geben Sie dazu den Fully-Qualified-Domain-Name (FQDN) des Spacewalk-Servers sowie einen Benutzer-Account zum Erzeugen der Kanäle an, beispielsweise den im ersten Workshop-Teil erzeugten Spacewalk-Administrator. Unter dem Reiter "Users" haben Sie jedoch auch die Möglichkeit, weitere Benutzer mit bestimmten Rechten einzurichten. Über das Webinterface sollte der so eingerichtete Kanal jetzt unter dem Tab "Channels" sichtbar sein, natürlich noch ohne jegliche Software-Pakete. Diese lassen sich auf mehrere Arten auf den Server uploaden. Welche Methode Sie wählen, hängt davon ab, ob die Pakete bereits lokal vorliegen, beispielsweise auf einer DVD, oder Sie ein entferntes yum-Repository mit dem Spacewalk-Server abgleichen wollen. Für den ersten Fall existiert das Tool rhnpush. Der Aufruf sieht wie folgt aus:

```
# rhnpush -v –channel=fedora-13-i386
  –server=http://localhost/APP
  –dir=/pfad/zu/den/paketen
```

Für die Synchronisation mit einem entfernten Software-Repository geben Sie im Webinterface auf den Eigenschaften Ihres Software-Kanals unter "Channels / Manage Software Channels / Fedora 12 32-bit" einfach die URL zum entfernten Repository an. Die Synchronisation kann dabei natürlich einige Zeit in Anspruch nehmen. Als Kommandozeilen-Werkzeug sei hier "spacewalk-repo-sync" erwähnt. Auch hiermit holen Sie sich entfernte Software-Pakete eines yum-Repositories auf den eigenen Spacewalk-Server.

Um Ihren Server aktuell zu halten, können Sie das unter [2] aufgeführte Skript regelmäßig über den cron-Dienst aufrufen lassen. Das Skript schaut sich Ihre konfigurierten Software-Quellen an und lädt neue Pakete automatisch herunter. Somit ist ein manueller Abgleich nicht mehr notwendig. Subkanäle lassen sich übrigens ebenfalls über die hier beschriebene Methode einrichten. Dazu noch der Hinweis, dass selbst erzeugte RPM-Pakete zwingend mit einer digitalen Signatur zu versehen sind. Sowohl der Spacewalk-Server als auch die Client-Anwendung yum verweigern in der Standard-Einstellung die Zusammenarbeit mit nicht signierten Paketen. Diese Funktion lässt sich zwar deaktivieren, aus Sicherheitsgründen sollten Sie Ihre eigenen Pakete jedoch immer mit einer Signatur versehen. Hierfür nutzen Sie den Befehl *rpm --resign {RPM-Paket}*. Die rpm-Anwendung setzt hierfür einen entsprechenden GPG-Schlüssel voraus. Die Datei *~/.rpmmacros* gibt dabei Auskunft über Namen und Speicherort des Schlüssels:

```
# cat .rpmmacros
%_signature gpg
%_gpg_name Thorsten Scherf
  <tscherf@redhat.com>
```

Damit Client-Systeme die mit diesem Schlüssel signierten Pakete auch verifizieren können, sollten Sie den öffentlichen Teil auf dem Spacewalk-Server ablegen. Am besten im Verzeichnis */var/www/html/pub*, denn von dort aus kann jeder Client auf die Datei zugreifen. Der Export des öffentlichen Schlüssels aus dem GPG-Schlüsselbund erfolgt dabei wie folgt:

```
# gpg –armor –export tscherf@
  redhat.com > /var/www/html/pub/
  rpm-gpg-key
```

Client-Registrierung

Damit vorhandene Client-Systeme auf die soeben hochgeladenen Software-Pakete zugreifen können, müssen Sie diese zuerst auf dem Spacewalk-Server registrieren. Hierzu installieren Sie zunächst das Spacewalk Client-Repository RPM auf den betroffenen Clients. Für Fedora 12-Systeme findet sich das passende RPM unter [3], für RHEL5 oder CentOS5 unter [4]. Auf RHEL- und CentOS-Systemen ist hier auch zwingend das RPM für das EPEL-Repository (Enterprise Packages for Enterprise Linux) einzuspielen, da ansonsten Abhängigkeiten der Client-Tools eventuell nicht aufgelöst werden können. Der folgende Befehl installiert die entsprechende yum-Datei für ein 32 Bit Fedora 12-System:

```
# rpm -Uvh
  http://spacewalk.redhat.com/yum/
  1.0/Fedora/12/i386/spacewalk-
  client-repo-1.0-2.fc12.noarch.rpm
```

Im Anschluss installieren Sie mittels yum die Spacewalk Client-Tools:

```
# yum install rhn-client-tools
  rhn-check rhn-setup rhnsd m2crypto
  yum-rhn-plugin
```

Damit Sie das System nun auf dem Server registrieren können, rufen Sie im einfachsten Fall die Anwendung "rhnreg_ks" auf. Diese benötigt einen sogenannten Registrierungsschlüssel, den Sie im Vorfeld auf dem Spacewalk-Server erzeugen müssen ("Systems / Activation Key / Create Key"). Beim Erzeugen des Schlüssels können Sie diverse Ressourcen an diesen binden, beispielsweise den soeben erzeugten Fedora 12 Software-Kanal oder aber, falls schon vorhanden, Konfigurations-Kanäle. Auch System-Gruppen lassen sich diesem Schlüssel zuweisen. Alle Systeme, die diesen Schlüssel zur Registrierung verwenden, erhalten somit Zugriff auf die Ressourcen. Den generierten Schlüssel geben Sie dann bei der Registrierung einfach mit an:

```
# rhnreg_ks –serverUrl=http://space-
  walk.server.tld/XMLRPC
  –activationkey=key
```

Hat alles geklappt, erscheint das System nun in der Weboberfläche des Servers unter dem Tab "Systems". Unter den Eigenschaften des Systems sollten Sie nun auch den konfigurierten Software-Kanal sehen. Ob der Zugriff hierauf wie gewünscht funktioniert, testen Sie im einfachsten Fall durch die Installation eines Paketes aus diesem Kanal. Sollte dies nicht funktionieren, so ist eine mögliche Fehlerquelle, dass das Client-System nicht das passende CA-Zertifikat des Spacewalk-Servers verwendet. Dieses liegt auf dem Server unterhalb von *http://spacewalk.server.tld/pub/* und ist auf dem Client unterhalb von */usr/share/rhn* zu speichern. Aus der Datei */etc/sysconfig/rhn/up2date* verweisen Sie dann auf dieses Zertifikat. Hier tragen Sie auch den Namen des Spacewalk-Servers ein. Diese Schritte müssen Sie nur auf bereits installierten Systemen durchführen. Systeme, die Sie über den Spacewalk-Server neu installieren, werden automatisch als Teil der Installation auf dem Server angemeldet und können somit sofort auf diesen zugreifen.

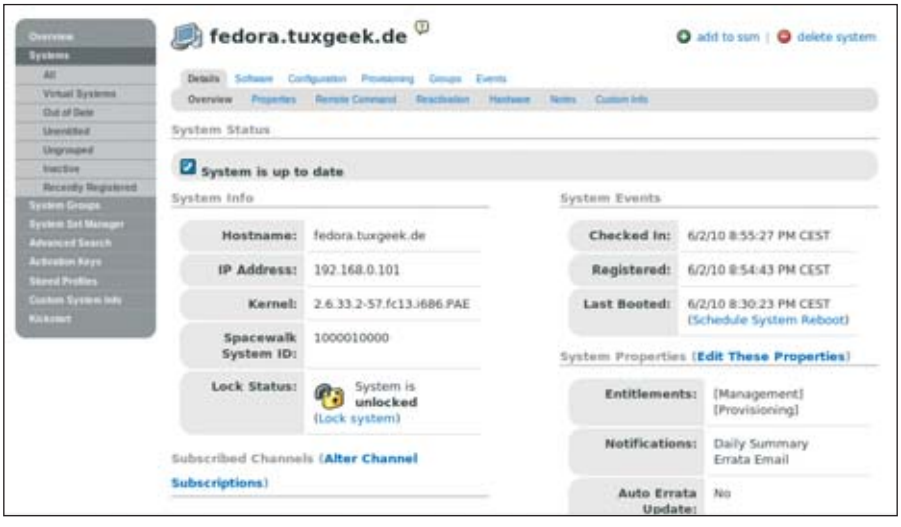


Bild 1: Unter den Eigenschaften eines Systems lassen sich sehr viele Administrationsaufgaben bequem vom Spacewalk Server aus steuern

Zündung dank Kickstart

Zur automatisierten Installation von neuen Client-Systemen müssen Sie auf dem Spacewalk-Server eine Kickstart-Datei mit den notwendigen Angaben darüber bereitstellen, wie die Installation des neuen Systems ablaufen soll. Hierzu gehören beispielsweise die Partitionierung, Software-Auswahl und weitere Einstellungen, die bei einer manuellen Installation ebenfalls anzugeben sind. Eine solche Kickstart-Datei erzeugen Sie im einfachsten Fall in der Weboberfläche über den Menüpunkt "Systems / Kickstart / Profiles". Neben einer Übersicht bereits vorhandener Profile besteht hier auch die Möglichkeit, neue Profile zu erzeugen.

Als Teil einer solchen Profildatei ist unter anderem auch eine Kickstart-Distribution anzugeben. Hierbei handelt es sich nicht um die eigentlichen RPM-Pakete, die zu einer zu installierenden Distribution wie Fedora 12 gehören, sondern um die grundlegenden Installationsdateien. Dazu zählt beispielsweise auch das Tool Anaconda. Eine solche Kickstart-Distribution ist üblicherweise nicht Bestandteil eines zuvor synchronisierten Software-Repositories und ist somit erst auf dem Spacewalk-Server zu erzeugen. Hier navigieren Sie erneut in der Weboberfläche zum Menüpunkt "Systems / Kickstart / Distributions" und verweisen auf die notwendigen Dateien. Diese erhalten Sie am einfachsten, indem Sie von der gewünschten Distribution eine Installations-CD/DVD über das Loopback-Device einbinden:

Bild 2: Über eine XMLRPC-Schnittstelle stehen Ihnen sehr viele Funktionen des Spacewalk-Servers auch über eine programmierbare API zur Verfügung

```
# mount -o loop /var/iso-images/
  Fedora-23-i386-DVD.iso /var/
  distro-trees/Fedora-12
```

Beim Erstellen einer Fedora 12 Kickstart-Distribution verweisen Sie den Spacewalk-Server nun einfach auf das Verzeichnis */var/distro-trees/Fedora-12*. Vor der Installation eines Systems ist zuerst die entsprechende Kickstart-Distribution für das gewünschte Betriebssystem zu erzeugen. Hat alles funktioniert, können Sie nun beim Anlegen einer Kickstart-Datei auf die so erzeugte Distribution verweisen. Client-Systeme beziehen bei einer Neuinstallation dann automatisch die richtigen Dateien aus dieser Quelle.

Um nun ein neues System mit Fedora 12 zu installieren, bestehen mehrere Möglichkeiten. Im einfachsten Fall verweisen Sie mittels der Anweisung *next-server* auf einem DHCP-Server alle PXE-Anfragen eines Clients an den Spacewalk-Server. Dank der Integration von Cobbler läuft hier bereits ein TFTP-Server und hält alle zuvor eingerichteten Kickstart-Profile vor. Auf der Kommandozeile lässt sich dies mittels *cobbler profile list* bestätigen. Wenn Sie nun ein Client-System über eine PXE-fähige Netzwerkkarte booten, so erscheint automatisch eine Liste aller vorhandenen Kickstart-Profile. Zur Installation des Clients wählen Sie nun einfach das passende Profil aus der Liste aus. Eine Registrierung auf dem Spacewalk-Server erfolgt im Anschluss automatisch. Bereits bestehende Systeme lassen sich ebenfalls sehr leicht mittels

```
koan –replace-self –server=
  spacewalk.server.tld
–profile=kickstart-profile
```

neu installieren. Hierbei erfolgt ein entsprechender Eintrag im Boot-Loader-Menü, der nach einem Reboot des Systems automatisch ausgewählt wird. Weitere Informationen zu Cobbler finden Sie unter [5].

Management von Systemen

Sämtliche Systeme, die auf dem Spacewalk-Server registriert sind, beziehen ihre Software-Pakete nun aus dieser Quelle. Ein Zugriff auf externe Repositories ist nicht mehr notwendig. Dies erhöht nicht nur die Sicherheit, sondern schont auch die Netzwerk-Bandbreite. Unter den Eigenschaften eines registrierten Systems lassen sich nun vielfältige Einstellungen vornehmen. Beispielsweise können Sie neue Software- oder Konfigurationskanäle einem System zuordnen, die installierte Software mit den Profilen anderer Systeme vergleichen oder aus Sicherheitsgründen Snapshots anlegen, zu denen Sie zu einem späteren Zeitpunkt zurückrollen können. Auch die Installation von neuer Software oder die Verteilung von Konfigurationsdateien kann nun von zentraler Stelle aus erfolgen. Da sich registrierte Systeme in Gruppen einordnen lassen, funktioniert dies sogar auf einer großen Anzahl von Systemem mit einem einzelnen Klick.

Zum Schluss sei noch auf die sehr umfangreiche Spacewalk-API [6] verwiesen. Hiermit erhalten Sie Zugriff auf viele Funktionen, die selbst über das Webinterface gar nicht zur Verfügung stehen. Der Zugriff auf die API erfolgt dabei über XMLRPC, somit bieten sich Perl oder Python zur Entwicklung eigener Skripte an.

Fazit

Mit Spacewalk erhalten Sie ein sehr leistungsstarkes Tool zur Verwaltung von großen Linux-Systemlandschaften. Viele alltägliche Arbeiten wie die Installation von Software-Updates oder das Einspielen von Konfigurationsdateien gelingt hiermit sehr einfach. Auch fortgeschrittene Funktionen wie das Klonen von Kanälen sind möglich. Somit kann die verwendete Software einen QA-Prozess durchlaufen, bevor diese auf produktiven Systemen zum Einsatz kommt. Dank der sehr umfangreichen API lassen sich viele Aufgaben auch in Form von Skripten erledigen. *(dr)*

Links

[1] Spacewalk API-Skript zum Anlegen eines Software-Kanals
https://fedorahosted.org/spacewalk/attachment/wiki/UploadFedoraContent/create_channel.py

[2] Skript zum automatischen Update über cron
http://fedorahosted.org/spacewalk/attachment/wiki/UploadFedoraContent/sync_repos.py

[3] Fedora12 Spacewalk Client Repository RPM
http://spacewalk.redhat.com/yum/1.0/Fedora/12/i386/spacewalk-client-repo-1.0-2.fc12.noarch.rpm

[4] RHEL5 und CentOS5 Client Repository RPM
htttp://spacewalk.redhat.com/yum/1.0/RHEL/5/i386/spacewalk-client-repo-1.0-2.el5.noarch.rpm

[5] Cobbler Projektseite
http://fedorahosted.org/cobbler/

[6] Spacewalk-API
http://fedorahosted.org/spacewalk/wiki/ApiDocs

Desktop-Verwaltung mit dem Microsoft Desktop Optimization Pack (4)

Vorbeugen ist besser als abstürzen

von Thomas Joos


Quelle: BCkid - Fotolia.com

In unserer Workshopserie zum Microsoft Desktop Optimization Pack (MDOP) stellen wir Ihnen in der letzten Folge das Microsoft System Center Desktop Error Monitoring (SCDEM) vor. Das Werkzeug hilft bei der Fehlersuche, wenn sich auf den Arbeitsstationen Abstürze des Betriebssystems oder von Anwendungen ereignen. So lassen sich selbst dann zentral die Probleme einzelner Computer und der darauf laufenden Applikationen erfassen, wenn Anwender durch einen Neustart in Eigenregie versuchen, die Schwierigkeiten zu lösen. Dann ist das Symptom zwar momentan aus der Welt, aber die Ursache des Problems bleibt im Verborgenen und kann jederzeit wieder zu einem Fehler führen. Wir bringen Ihnen in diesem Workshop näher, wie Ihnen SCDEM bei der Datensammlung und dem Finden von Fehlerursachen hilft.

Grob gesagt handelt es sich bei SCDEM um eine Light-Version des System Center Operations Manager 2007 (SCOM) R2 ohne Agentenunterstützung und mit einer eingeschränkten Verwaltung. Sie erhalten auf einer grafischen Oberfläche den Status aller angebundenen Rechner angezeigt und können sich sofort an die Problemlösung machen, wenn bestimmte Fehler auftauchen. Da die Software alle konnektierten Computer überwacht, lassen sich zentral Probleme von Anwendungen oder von einzelnen PCs im Netzwerk nachverfolgen. Fehlt eine solche automatisierte Überwachung, fallen viele Schwierigkeiten erst dann auf, wenn zum Beispiel die Benutzer keine Verbindung mehr mit einem Server aufbauen können. Die konsequente Überwachung ist einer der Bausteine, welche die Stabilität und Ausfallsicherheit eines Netzwerks gewährleisten und die Arbeitsfähigkeit der Anwender sicherstellen.

Workstations überwachen, Fehlermeldungen protokollieren

Mit SCDEM können Sie automatische Gegenmaßnahmen wie den Neustart eines Dienstes, das Ausführen von Skripten oder das Versenden von E-Mails einleiten. Da das Produkt im MDOP enthalten ist, sind keine weiteren Lizenzen notwendig. Für die Installation von SCDEM benötigen Sie allerdings eine Datenbank. Empfohlen wird SQL Server 2005 SP1 oder 2008 SP1. Der aktuelle SQL Server 2008 R2 steht nicht auf der Kompatibilitätsliste und hat bei unserem Test auch nicht funktioniert. Außerdem muss der Server, auf dem Sie SCDEM installieren, über den IIS verfügen.

Die Installation erfolgt auf Basis des Installationsassistenten von SCOM 2007 R2. Um SCDEM zu verwenden, ist aber keine Infrastruktur mit SCOM 2007 R2 nötig. Das Tool funktioniert vollkommen selbständig, auch wenn der Installationsassistent an verschiedenen Stellen stark an SCOM 2007 R2 erinnert. Analog dazu entspricht die Konsole von SCDEM nach dem Start der Konsole von SCOM 2007 R2, benötigt aber keinen SCOM-Server und ist zudem deutlich eingeschränkt.

Sie können mit dem Tool nach Fehlern von bestimmten Applikationen, etwa Outlook, im Netzwerk suchen und erhalten eine Zusammenfassung aller gefundenen Probleme. Auch wer sich nicht mit SCOM auskennt, kommt mit der intuitiven Oberfläche schnell zurecht. Die angezeigten Fehler auf den Client-Computern erhalten meist noch

einen Hinweis zur Behebung und einen Link zu entsprechenden Problemlösungen in der Microsoft Knowledge Base. Neben der reinen Überwachung in der SCOM-Konsole können Sie Benachrichtigungen über E-Mail oder SMS konfigurieren, wenn bestimmte Fehler auf den Clients auftreten. Ebenso sind automatische Vorgehensweisen beim Erscheinen von festgelegten Problemen möglich, zum Beispiel das Starten von ausgesuchten Skripten.

Monitoring ohne Agenten

Eine weitere Funktion ist das Erstellen von Berichten, zum Beispiel eine Liste aller Applikationen, die im Netzwerk und auf den Arbeitsstationen am meisten Fehler verursachen. SCDEM nutzt zur Abfrage der Clientcomputer die Windows-Technologie "Windows-Fehlerberichterstattung", erkennt Fehler-Pop-Ups auf den Clients und leitet diese an den Server weiter. Die Anbindung erfolgt über Gruppenrichtlinien. Auf den Clients ist kein Agent erforderlich. Die entsprechenden Einstellungen liefert SCDEM als Gruppenrichtlinienvorlage mit, die Sie einfach in die Gruppenrichtlinien der Domäne importieren. Die Überwachung entspricht dem Agentless Exception Monitoring (AEM) im System Center Operations Manager 2007 R2 und lässt sich exakt gleich verwalten.

Die Datenspeicherung auf dem SCDEM-Server erfolgt in einer SQL-Datenbank und ermöglicht dadurch detaillierte SQL-Berichte und -Abfragen. Unternehmen, die SCDEM einsetzen, können relativ leicht eine Aktualisierung auf SCOM 2007 R2 durchführen und dabei alle Daten aus der zentralen Datenbank übernehmen.

SCDEM-Installation bedarf einiger Voraussetzungen

Die Installation selbst gestaltet sich nicht so einfach wie bei den anderen Produkten von Microsoft. Fehlt der Software eine Voraussetzung, meldet der Assistent einen Fehler und Sie müssen sich durch die einzelnen Bedingungen hangeln, bis alles installiert ist. Hilfreich bei der Komplettierung der Vorbedingungen ist das Tool *prereqviewer.exe*

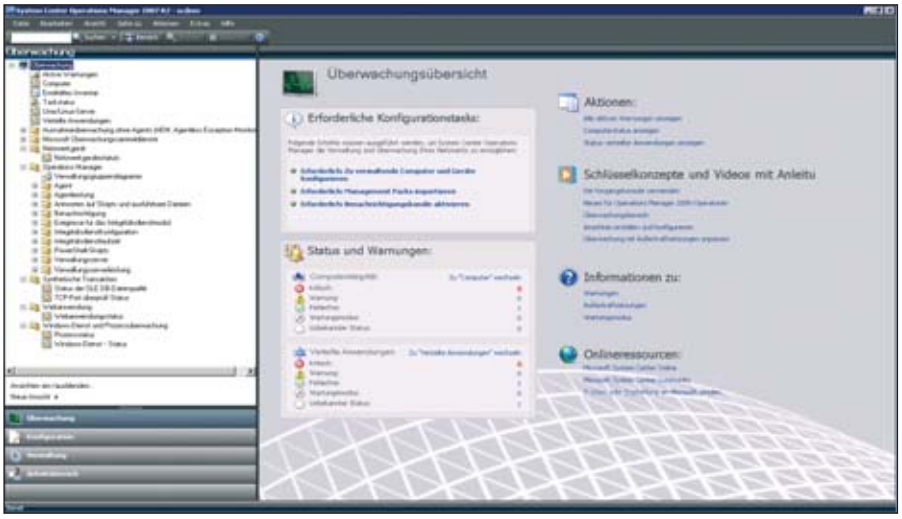


Bild 1: Die Verwaltungskonsole von SCDEM entspricht der Konsole von SCOM 2007 R2

im Verzeichnis "\DEM\Installers\Prereq\amd64" der MDOP-Installations-DVD. Mit diesem Werkzeug überprüfen Sie, welche Voraussetzungen SCDEM benötigt, und schaffen diese vor dem eigentlichen Setup. Wählen Sie dazu einfach die Komponenten aus, die Sie auf dem Server installieren wollen, und klicken Sie dann auf "Prüfen". Zwar können Sie auch direkt mit der Installation beginnen, allerdings startet der Assistent zum Überprüfen der Voraussetzungen erst sehr spät, so dass Sie immer wieder von vorne anfangen müssen, bis auf dem Server alles installiert ist.

Fehlt ein bestimmtes Tool oder stimmt die Konfiguration nicht, erhalten Sie ausführliche Hinweise und Download-Links. Wollen Sie keinen vollwertigen SQL-Server installieren, lässt sich die kostenlose Express-Edition von SQL Server 2008 SP1 nutzen. Für eine Testumgebung reicht diese vollkommen aus. Nach erfolgreichem Test starten Sie die Installation über die Datei *DEMSetup.exe* im Verzeichnis "\DEM\Installers". Bei der Installation müssen Sie lediglich ein paar Fenster bestätigen und Benutzerkonten mit entsprechenden Administratorrechten in der Domäne angeben. Wichtig ist die erfolgreiche Integration der Gruppenrichtlinienvorlage für SCOM. Sie finden die Vorlage nach dem Import über "Computer Configuration \ Administrative Templates\ Microsoft Applications". Nach der Installation konfigurieren Sie per Gruppenrichtlinie die Clients für die Übermittlung der Fehlermeldung und legen verschiedene Einstellungen für die Fehlerübermittlung an den SCDEM fest.

Über die Richtlinien bestimmen Sie weiterhin, ob Windows nur Fehler des Betriebssystems an SCDEM melden soll oder auch die Fehler der installierten Applikationen. Auf der Webseite [1] finden Sie ein Word-Dokument zur Fehlersuche, wenn die Anbindung der Client-Computer nicht funktioniert. Im SCDEM-Verzeichnis auf der MDOP-DVD sind zudem einige Hilfsdokumente für SCOM 2007 vorhanden, die auch für SCDEM gültig sind. Neben der Verwaltung über die grafische Oberfläche wartet auch die PowerShell auf ihren Einsatz. Zusätzlich zur grafischen Oberfläche und zur PowerShell-Erweiterung steht eine Webkonsole für die Konfiguration zur Verfügung. Generell entspricht die Verwaltung von SCDEM den Möglichkeiten von SCOM 2007 R2. Allerdings stehen wie bereits angedeutet nicht alle Möglichkeiten von SCOM in der Konsole zur Verfügung, zum Beispiel die SNMP-Abfragen von zusätzlichen Netzwerkgeräten oder verschiedene Assistenten zur Anbindung von Client-Rechnern.

Anbindung von Client-Computern

Die Überwachung der Computer im Netzwerk durch SCDEM funktioniert ohne Agenten. Haben Sie die Serverlösung

installiert, sollten Sie zunächst in der Verwaltungskonsole über "Verwaltung \ Clientüberwachung konfigurieren" den Assistenten zur Erstellung der Überwachungsfreigabe durchführen.

Konfigurieren Sie die entsprechenden Einstellungen im Assistenten und legen Sie die Freigabe fest, in welcher die Computer die Daten zur Überwachung ablegen sollen. Diese müssen Sie nicht vorher erstellen, der Assistent erledigt dies nach entsprechender Eingabe automatisch. Im letzten Fenster des Assistenten bestimmen Sie, wo die Vorlage für die Gruppenrichtlinie hinterlegt werden soll. Diese benötigen Sie, um eine Gruppenrichtlinie zu erstellen, mit der Sie Clientcomputer an den SCDEM-Server anbinden. Die Vorlage enthält alle spezifischen Einstellungen Ihrer Domäne und den Speicherort der Freigabe sowie den Port für die Verbindung der Client-Computer. Haben Sie die Vorlage geschaffen, importieren Sie diese in eine Gruppenrichtlinie. Klicken Sie dazu im Gruppenrichtlinienverwaltungs-Editor mit der rechten Maustaste auf "Administrative Vorlagen" und wählen Sie "Vorlagen hinzufügen".

Nach dem Import stehen die Einstellungen über "Administrative Vorlagen \ Klassische administrative Vorlage \ Microsoft Applications" zur Verfügung. Aktivieren Sie an dieser Stelle die einzelnen Einstellungen. Die Daten des Verwaltungsservers von SCDEM sind bereits automatisch hinterlegt. Nachdem auf den Clients die entsprechende Richtlinie durch Neustart eingelesen worden ist, findet bereits die Überwachung statt. Wichtig sind die Einstellungen für die verschiedenen Betriebssysteme vor und nach Windows Vista. Die Einstellungen finden Sie in der Vorlage über "SCOM Client Monitoring node". Die Konfiguration für Windows XP und Windows Server 2003 nehmen Sie über "Configure Error Reporting for Windows Operating Systems older than Windows Vista" vor. Stellen Sie sicher, dass die Einstellung aktiv ist und die Daten Ihres Servers korrekt hinterlegt sind. Für Windows Vista und Windows 7 sind die Einstellungen unter "Configure Error Reporting for Windows Vista or later operating systems" wichtig. Sorgen Sie auch hier dafür, dass der Verwaltungsserver korrekt hinterlegt ist.

Auf den Clients können Sie ab Windows Vista und Windows Server 2008 in der Registry über "HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Microsoft \ Windows \ WindowsErrorReporting" kontrollieren, ob Servername und Port korrekt sind. Im bereits erwähnten Word-Dokument finden Sie ausführliche Hinweise zur Anbindung der Clients. Die Hilfedateien auf der MDOP-DVD unterstützen Sie ebenfalls bei der Client-Anbindung. Bevor Sie SCDEM in einer produktiven Umgebung einsetzen, sollten Sie in einer Testumgebung zunächst ausführlich proben. Vor allem die Anbindung der Client-Computer und die Übertragung der Daten kann ein Netzwerk schnell auslasten. Außerdem sollten Sie SCDEM auf einem dedizierten Server installieren. Die Datenbank muss nicht unbedingt auf dem gleichen Server liegen.

Fazit

Natürlich gibt es jede Menge kostenpflichtiger Überwachungswerkzeuge auf dem Markt, die ähnliche Möglichkeiten wie SCDEM bieten. Allerdings unterstützen nicht alle Produkte die Windows-Fehlerberichterstattung so gut wie SCDEM. Unternehmen, die überlegen, den großen Bruder SCOM einzusetzen, erhalten mit SCDEM einen ersten Einblick in die Möglichkeiten und die Verwaltung, da die Management-Werkzeuge komplett übereinstimmen.

Unserer Meinung nach sind die Werkzeuge des MDOP teilweise deutlich unterschätzt. Extra einen Vertrag für MDOP einzugehen, ist dann aber wohl zu viel des Guten. Doch probieren geht über studieren: Microsoft stellt unter [2] eine 120 Tage gültige Testversion des MDOP zur Verfügung. Den Blog der MDOP-Entwickler finden Sie unter [3], zahlreiche Hilfen und Anleitungen im Microsoft Technet [4]. *(ln)*

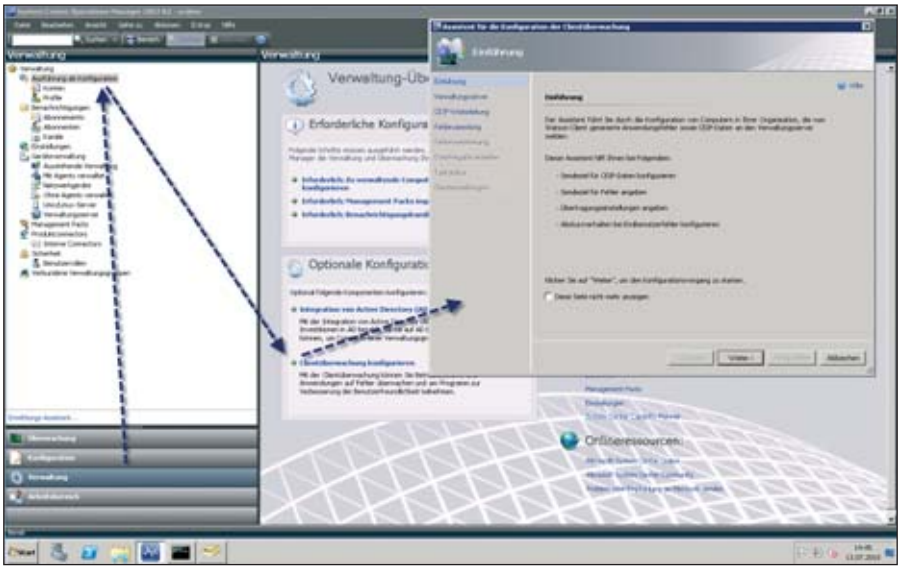


Bild 2: Über einen Assistenten konfigurieren Sie in SCDEM die Client-Überwachung

Links

[1] Troubleshooting für Microsoft Error Reporting und Windows Error Reporting
http://blogs.technet.com/b/momteam/archive/2008/05/23/troubleshooting-agentless-exception-monitoring-aem-and-desktop-error-monitoring-dem-features.aspx

[2] Informationen zum MDOP und Download der Testversion
www.microsoft.com/germany/windows/mdop/

[3] Offizielles MDOP-Blog
http://blogs.technet.com/b/mdop/

[4] Technet-Seiten zu MDOP
http://technet.microsoft.com/de-de/windows/bb899442.aspx

Tipps & Tricks ohne Gewähr

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

Microsoft Windows

In unserem Unternehmen soll eine bestimmte Gruppe von Administratoren das Recht erhalten, **Group Policy Objects auf OUs zu verlinken** und auch die Reihenfolge der GPOs zu verändern. Die Administratoren sollen **die GPOs selbst aber nicht editieren** können. Wie lässt sich dies bewerkstelligen?

GPOs werden immer wichtiger und komplexer. Kaum eine große Umgebung kommt noch ohne deren gezielten Einsatz aus. Doch die Vielfältigkeit hat nicht nur Vorteile: Falsche Konfigurationen können schnell zum Super-GAU führen. Darum tun Sie gut daran, bestimmte Aktionen nur reguliert durchführen zu lassen. Die Lösung für Ihr Problem liegt in der Delegation des AD-Schreibzugriffes auf das Attribut "gpLink" der OUs. Sowohl das Verlinken als auch die Reihenfolge der GPOs steuern Sie über dieses Attribut und verhindern so gleichzeitig, dass ein Mitarbeiter die GPOs selbst modifizieren kann. Mehr nützliche Tipps und interessante Neuigkeiten rund um System-Administration und Virtualisierung finden Sie in den Blogs von Sepago: *http://blogs.sepago.de* *(ln)*

Wenn ich auf einem PC mit Windows 7 eine **Datei öffnen will, die noch nicht mit einem Programm verknüpft ist**, bietet das Betriebssystem immer die Option an, ein lokales Programm auszuwählen oder **im Web nach einer geeigneten Software zu suchen**. Von letzterer Möglichkeit habe ich allerdings noch nie Gebrauch gemacht und sehe dazu auch in Zukunft keinen Anlass. Lässt sich diese **Option abschalten?**

Mit einem Eintrag in der Registry können Sie die von Ihnen nicht erwünschte Option deaktivieren. Gehen Sie dazu mit *regedit* in die Registrierungsdatenbank und navigieren Sie in das Verzeichnis HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer. Dort erstellen Sie nun einen neuen DWORD-Wert mit der Bezeichnung "NoInternetOpenWith" und weisen diesem Vermerk den Wert "1" zu. In Zukunft bleiben Sie beim Doppelklick auf nicht verknüpfte Dateien vom Angebot nach einer Programm-Suche im Internet verschont. *(ln)*

Microsoft Exchange

Exchange 2010 ist in unsere Active Directory-Umgebung integriert. Mit dem Cmdlet *Get-DistributionGroupMember* wollte ich – wie in der TechNet-Dokumentation beschrieben – **alle Mitglieder einer bestimmten Verteilergruppe herausfinden**. Dies funktioniert jedoch nicht. Stattdessen wirft der Rechner eine **Fehlermeldung** aus und gibt an, dass das gewünschte Objekt nicht existieren würde. Wo liegt hier das Problem und was kann ich dagegen unternehmen?

Das von Ihnen beschriebene Problem tritt bei einer bestimmten Konstellation auf: Im Netzwerk existieren neben einer übergeordneten Active-Directory-Domäne, etwa "contoso.com", noch zwei untergeordnete Domänen, zum Beispiel "us.contoso.com" und "eu.contoso.com". Wenn nun auf der einen untergeordneten Domäne die Serverrolle Exchange Server 2010 installiert ist und sich auf der anderen Domäne Postfächer der Benutzer befinden, gibt das Kommando *Get-Distribution-Group-Member* nicht alle Mitglieder der Verteilergruppe zurück, wenn die Topologie mehrere Active Directory-Domänen enthält. Die erwähnte Fehlermeldung ist die Folge. Damit das richtige Ergebnis ausgegeben wird, müssen Sie vor dem Ausführen des Befehls als Abfragebereich die gesamte Struktur festlegen. Dies erledigen Sie mit folgendem Kommando:

```
Set-ADServerSettings
  -ViewEntireForest $True
```

Dieser Befehl ist neu in Exchange Server 2010. Standardmäßig ist der Parame-

ter "False" eingestellt – was jedoch in Topologien mit mehreren Active Directory-Domänen nicht sinnvoll ist. *(ln)*

Citrix XenApp 6 ermöglicht laut Hersteller ja durch HDX RealTime auch die serverbasierte **Ausführung des Microsoft Office Communicator**. Darüber haben wir versucht, **Videochats durchzuführen**, was jedoch entweder gar nicht oder nur mit äußerst mäßiger Qualität funktioniert hat. Was gilt es hier zu beachten?

Es müssen einige Voraussetzungen berücksichtigt werden, damit Voice- oder Videochat im Office Communicator problemlos funktionieren. Zunächst sollten Sie den ICA-Client ab Version 12.0 nutzen – Webcams werden mit älteren Versionen generell nicht unterstützt. Außerdem müssen die folgenden Citrix Active Directory-Policies auf "Enabled" gestellt werden: Client Audio Redirection, Client Microphone Redirection, HDX MediaStream, Multimedia Acceleration und Multimedia Conferencing. Videokonferenzen und Echtzeit-Voice- oder Videoübertragungen sind äußerst ressourcenintensiv. Weisen Sie deshalb jedem aktiven Anwender einen virtuellen oder physischen Prozessorkern zu. Die Anforderungen sind weniger hoch, wenn nicht jeder Benutzer gleichzeitig die Videokonferenzfunktionen nutzt. Konfigurieren Sie bidirektionales Audio so, dass der "Optimized for Speech"-Audio Codec zum Einsatz kommt. Er verbraucht nur 34 Kbit/s an Bandbreite und ist damit für diese Zwecke ideal geeignet. Eine Videokonferenz benötigt pro User Bandbreiten von 300 bis 600 KBit/s für den Upstream und 800 bis 1.000 KBit/s für den Downstream. Selbst Latenzen mit 200 ms bereiten in der Praxis kaum Schwierigkeiten. Auf dem genutzten Gerät muss allerdings der richtige Webcam-Treiber installiert sein. Für den XenApp Host gilt dies nicht. Installieren Sie am besten die neuesten Dateien des Webcam-Herstellers. Sie sind meist erheblich besser als die Standardversionen, die beim erstmaligen Anschließen des Gerätes automatisch installiert werden. Oft lasten diese den Prozessor wesentlich stärker aus. *(Citrix/ln)*

Theoretisch sollte es doch möglich sein, ein **XenDesktop- oder Provisioning Server-Zielgerät mit dem System Center Configuration Manager (SCCM) zu verwalten.** Bei einem Probelauf traten dabei aber diverse Probleme auf. Kann ich den SCCM für den oben beschriebenen Zweck überhaupt einsetzen und wenn ja, wie gehe ich dabei vor?

Soll bei einem gestreamten Betriebssystem der SCCM zum Einsatz kommen, gibt es einiges zu beachten. So ändert SCCM die GUID des Images, wenn es auf neue Hardware trifft. Dies ist notwendig, weil der SCCM-Server die Verbindung vom Betriebssystem zur Hardware hierüber definiert. Die GUID findet man in der Datei *%systemroot%\windows\smscfg.ini*. Per WMI können Sie hier die GUID auslesen, etwa mit folgendem VB-Script:

```
strComputer = "."
strNameSpace = "root\ccm" strClass =
  "CCM_Client=@" Set objClass = get-
  Object("Winmgmts:{impersonationle-
  vel=impersonate}!\\" & strComputer
  & "\" & strNameSpace & ":" &
  strClass)
strGUID = objClass.ClientID
Wscript.Echo strGUID
Set objClass = Nothing
```

Daraus wird folgende Problematik beim Provisioning Server ersichtlich: Haben Sie den SCCM-Client in einem Golden Image installiert, kommt er bei mehrfachem Streamen immer mit der gleichen GUID zum Zielgerät. Dies veranlasst den SCCM Client, *smscfg.ini* bei jedem Bootvorgang neu zu generieren. Um das Problem zu umgehen, müssen Sie ein Skript ausführen, wenn es beim eigesetzten OS-Image zum Wechsel vom "private mode" in den "standard mode" kommt. Ein solches Skript stoppt die SCCM-Dienste und löscht die vorhandene *smscfg.ini*-Datei:

```
Stop SCCM client strServiceName =
  "CCMExec"
Set objWMIService =
  GetObject("winmgmts:
  {impersonationLevel=impersonate}!
  \\.\root\cimv2")
Set colListOfServices =
  objWMIService.ExecQuery("Select *
  from Win32_Service Where Name =
  '" & strServiceName & "'")
For Each objService in colListOfSer-
  vices objService.StopService()
  Next ' Cleanup SCCM Set fso =
  CreateObject("Scripting.FileSys-
  temObject") Set aFile = fso.GetFi-
  le("c:\windows\SMSCFG.ini")
  aFile.Delete
```

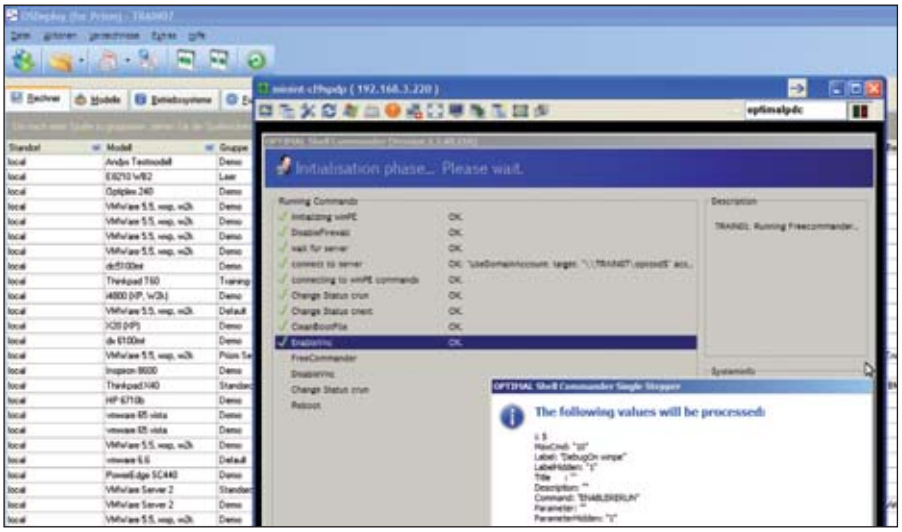
Nun benötigen Sie noch ein Shutdown- und ein Startup-Skript, das die *smscfg.ini*-Datei beim Herunterfahren auf ein Cached-Laufwerk kopiert und beim Starten überprüft, ob die Datei im Cached-Laufwerk vorhanden ist. Wenn nicht, würde sich der SCCM-Client wieder neu beim SCCM-Server registrieren und eine neue INI-Datei anlegen – was Sie ja vermeiden wollen. Im Folgenden steht "G" für das Cached-Laufwerk, hier das Startup-Skript:

```
IF EXIST G:\SMSCFG.ini COPY
  G:\SMSCFG.ini
  C:\Windows\SMSCFG.ini /y >
  c:\smserror.txt
```

Das Shutdown-Skript sieht analog dazu folgendermaßen aus:

```
Shutdown Script (G:\ steht für das
  cached Laufwerk)
COPY c:\windows\SMSCFG.ini
  G:\SMSCFG.ini /y > g:\smserror.txt
```

Diese einfachen Skripte können Sie nun zum Beispiel per Active Directory auf die OUs anwenden, in denen die XenDesktop-Rechner untergebracht sind. Viele nützliche und praktische Tipps zum SCCM im Zusammenspiel mit Citrix-Produkten finden Sie in der Microsoft Knowledge Base unter *http://support.microsoft.com/kb/837374/* und in den Blogs von Sepago: *http://blogs.sepago.de* *(ln)*



OSDeploy erlaubt, während eines Kommandos oder einer Installation die Aktion über VNC zu überwachen

Tools

Bei der **Installation von Windows-Betriebssystemen** reichen die Hilfsmittel des Administrators von Turnschuh und CD bis hin zur ausgewachsenen Enterprise-Systemmanagementlösung. Welcher Weg hierbei optimal ist, hängt von vielen technischen Faktoren, Unternehmens-Policies – beispielsweise zur Sicherheit – oder auch der Anzahl der Clients ab. Oft bieten jedoch die Werkzeuge, die für kleinere Infrastrukturen konzipiert sind, nicht den Komfort und die Möglichkeiten der Enterprise-Lösungen.

Die für bis zu 10 Clients freie Verteilungssoftware **OSDeploy** bietet dem IT-Verantwortlichen diesen Komfort. OSDeploy verwendet Standards wie **PXE, Microsoft Unattanded Setup, Microsoft ImageX und Microsoft System Image Manager (SIM) zum Ausrollen** des Betriebssystems. Das Programm ist für den Rollout und die Migration von Windows 7, Vista und XP sowie Windows 2008 Server, Windows 2000, Windows 2000 Server und Windows 2003 Server verfügbar. Tablet PCs lassen sich per Remote Installation über PXE bedienen. Administratoren sind mit OSDeploy in der Lage, beliebige Kommandos per PXE Boot und per Windows Preinstallation Environment (Windows PE) auszuführen. Image-Lösungen können problemlos eingebunden und Betriebssysteme rasch wiederhergestellt werden. Mit dem grafischen Editor bearbeitet der Nutzer automatische Konfigurationsdateien schnell und unkompliziert. Zudem erlaubt die "Hierarchie-Vererbung", die Installation differenziert zu steuern. Dabei richtet der Administrator Vererbungen objektorientiert auf verschiedenen Ebenen ein, etwa Unternehmen, Standorte, Funktionsgruppen, Gruppen, Modelle und Rechner. Neben der freien Version liefert der Hersteller auch ein kostenloses Handbuch als PDF mit über 100 Seiten, die den Einstieg erheblich erleichtern. *(jp)*

Quelle:www.optimal.de/produkte/osdeploy/freeware-version

Auch unser zweites Tool ist ein Fall von "Leistung der Großen kostenlos für kleine Unternehmen". Denn wenn es um die **Abrechnung von Supportkosten** geht, dürfte in Organisationen, die nicht auf ein dediziertes Help-Desk-Tool zurückgreifen können, MS Excel das Mittel der Wahl sein. Dieses oder vergleichbare Werkzeuge führen jedoch zu einem nicht gerade geringen Aufwand, wenn es darum geht, die Supportleistungen abzurechnen: die Werte müssen gepflegt, Kosten errechnet und an die Kunden versandt werden.

Doch das **pcvisit SupportJournal FREE** bietet hier Abhilfe. Mit diesem Werkzeug steht Supportern und Administratoren ein kostenloses Produkt für die **Erfassung, Auswertung und Abrechnung von Support-Leistungen** zur Verfügung. Das SupportJournal FREE erstellt nach jeder Support-Sitzung einen Leistungsbericht. Dies erfolgt vollautomatisch oder individuell per Knopfdruck und auf Wunsch kann der Supporter eine E-Mail zum Versand des Berichts automatisch vorbereiten. Nach dem gleichen Prinzip lassen sich am Ende des Monats mit wenigen Klicks alle Support-Sitzungen abrechnen. Die Software erstellt dabei für jeden Kunden eine fakturierbare Auflistung der erbrachten Support-Leistungen. Mühsame Routinearbeiten, die früher Stunden kosteten, schrumpfen so auf wenige Mausklicks zusammen. *(jp)*

Quelle:www.SupportJournal.de

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

Konfigurieren von Windows 7

Während hier bislang meist sehr technische Ratgeberbücher besprochen wurden, ist "Konfigurieren von Windows 7" ein Lehrbuch – das Original "Microsoft Training 70-680" bereitet auf die entsprechende Prüfung vor. Im Buch steht daher die Lernzielkontrolle ganz oben auf der Prioritätsliste, Text und Übungen sind immer so aufgebaut, dass sie am Ende eine "Richtig/Falsch"-Beurteilung erlauben. Der Leser muss nicht unbedingt die Zertifizierung anstreben, um von diesem Konzept zu profitieren. Aber es sorgt für ein recht knackiges Lerntempo. Kurz mal über die Seiten blättern und die Zusammenfassung lesen kommt nicht infrage. Die Kapitel und die enthaltenen Lektionen sind sehr detailliert und umfassend. So lernt der Leser den Umgang mit Windows 7 äußerst gründlich. Die Autoren nehmen sich das Betriebssystem und seine Funktionen der Reihe nach vor und verweisen auch auf kaum bekannte Features. Oder wussten Sie, dass sich der Strombedarf der angeschlossenen USB-Geräte im Gerätemanager über den "Erweitert"-Tab des USB-Hostadapters ermitteln lässt?

Thematisch geht das Buch den bewährten Weg: Die Autoren beginnen mit der Installation und Migration, erklären Systemabbilder, wie und womit sie erstellt werden, und gehen dann zur Verwaltung von Geräten und Treibern über. Die weiteren Kapitel behandeln Anwendungen, Windows Firewall, Netzwerkeinstellungen, Windows Update Datensicherung, DirectAccess, BitLocker und BrancheCache. Nach jeder Lektion folgen eine Zusammenfassung und eine Lernzielkontrolle. Am Kapitelende folgt eine weitere Zusammenfassung, die Schlüsselbegriffe im Text sowie einige Übungsaufgaben. Auch der Hinweis, Übungstests mithilfe der beigelegten CD des Buchs zu absolvieren, fehlt nicht. Die Aufgaben zeigen recht schnell, wie gut der Leser die vorangegangenen Seiten verstanden hat, oft lassen sich die Übungen erst nach einem weiteren Schnelldurchlauf des Kapitels lösen. Übrigens: Im Gegensatz zu älterer Microsoft-Kurslektüre haben die Lektoren hier ganze Arbeit geleistet. Der Text liest sich bei Weitem weniger hölzern als frühere Übersetzungen.

Fazit: Wer auf eine Zertifizierung aus ist oder einfach im klassischen Schulstil an das Lernen gehen will, findet hier einen passenden Begleiter. Das Buch setzt einiges an Grundkenntnissen voraus und fordert viel Konzentration, vermittelt aber auch enormes Wissen über die Windows 7-Interna.

Elmar Török

Autor:	Ian McLean, Orin Thomas
Verlag:	Microsoft Press
Preis:	79 Euro
ISBN:	978-3-86645-980-9
Bewertung:	★★★★☆

Windows Essential Business Server 2008

Der Windows Essential Business Server 2008 (WEBS) ist mehr als nur der große Bruder von Windows Small Business Server. Durch die Aufteilung auf mehrere Server, eine integrierte und leistungsfähige Firewall sowie Softwareverteilung und Systemüberwachung enthält dieses Produkt einen eigenen kleinen Microsoft-Produktkosmos. Genau das macht das Unterfangen, ein Buch für jede enthaltene Software zu schreiben, ziemlich ambitioniert. Doch Thomas Joos hat viel Erfahrung mit Microsoft-Produkten. So steigt er mit einer sehr brauchbaren Zusammenfassung von WEBS ein und legt die Grundlage für die folgenden 1.000 Seiten. Danach folgen Planungshinweise, die eines schnell klar machen: Der Leser muss bei Windows-Servertechnologien zumindest einigermaßen sattelfest sein. Joos erläutert die wesentlichen Dinge und wird bei erfahrenen Admins auf offene Ohren stoßen. Wer hingegen noch Klärungsbedarf bei Dingen wie Active Directory hat, muss sich anderweitig informieren.

Da er alle Elemente von WEBS anspricht, muss der Autor ein paar Abstriche in der Detailtiefe machen. So stehen für die Konfiguration von Exchange (ohne Spam- und Virenschutz) etwa 50 Seiten zur Verfügung. Das reicht, wenn der Leser sich mit dem Thema bereits beschäftigt hat und alles glatt läuft. Trotzdem schafft es der Autor, auch Infos für Fortgeschrittene einzubauen. So beschreibt Joos unter anderem die Diagnose per SMTP-Befehlen. Natürlich kann das Buch dabei nicht die gleiche Tiefe erreichen wie ein dedizierter Titel – das gilt auch für die späteren Kapitel wie Hyper-V, Forefront Security, Netzwerkkonfiguration und Remote-Webarbeitsplatz. Wirklich zu knapp sind die 40 Seiten für SharePoint, hier geht es wirklich nur um einen ersten Überblick. Und auch die Gruppenrichtlinien werden recht stiefmütterlich behandelt. Trotzdem: In einem großen Funktionsumfang hat der Autor die richtigen und wichtigen Kernpunkte gefunden.

Fazit: Äußerst umfangreich und sehr informativ. Das Buch liefert den Zugang zu zahlreichen Microsoft-Serverprodukten im Schnelldurchgang. *Elmar Török*

Autoren:	Thomas Joos
Verlag:	Microsoft Press
Preis:	59 Euro
ISBN:	978-3-86645-131-5
Bewertung:	★★★★☆

www.internet-sicherheit.de

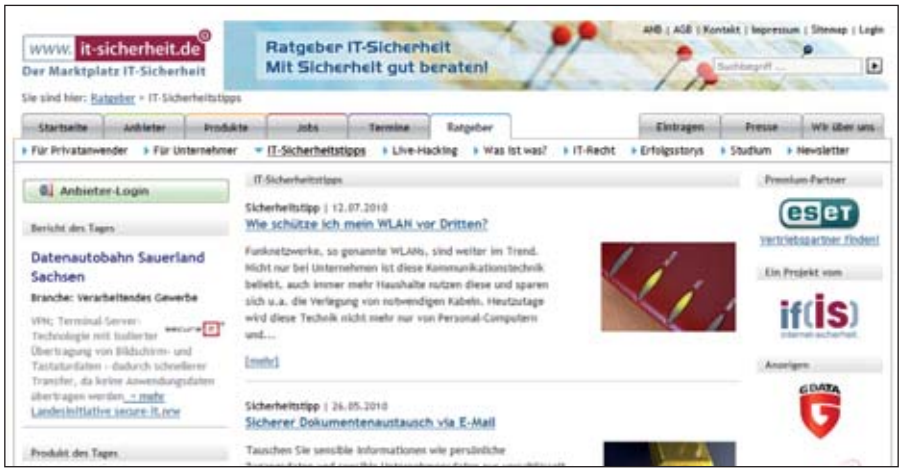
Sicherer Marktplatz

Der Markt für Dienstleistungen und Produkte wächst rasant und damit nimmt auch die Unübersichtlichkeit im selben Maße zu. Umso erfreulicher, wenn sich dem IT-Verantwortlichen ein Online-Portal bietet, das zum einen relevante IT-Sicherheitsprodukte zusammenträgt und darüber hinaus unverdächtig in Sachen Voreingenommenheit ist. Das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen bietet unter www.internet-sicherheit.de ein solches Portal. Hier findet der Administrator Anbieter, Produkte, Termine und Ratgeber rund um die IT-Sicherheit.

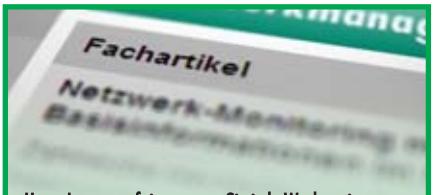
Zwar ist dieses Internetangebot noch recht jung und manche Bereiche sind bei weitem nicht so gut gefüllt wie spezialisierte Seiten zur IT-Security, doch seinem Anspruch als Marktplatz wird internet-sicherheit.de auf jeden Fall gerecht. Gerade im Bereich "Anbieter" sollte kein Wunsch unerfüllt bleiben.

Sucht der IT-Verantwortliche zum Beispiel bundesweit nach Dienstleistern zum Thema "Data Leakage Prevention", so liefert die Seite 125 Treffer, wird dieses Ergebnis dann etwa auf den Raum München eingegrenzt, bleiben noch immer 16 Unternehmen zur Auswahl. Zu jedem dieser Unternehmen ist ein kurzes Unternehmensprofil inklusive Kontaktdaten hinterlegt, so dass der Besucher sich schnell ein Bild machen kann, ob der jeweilige Anbieter den eigenen Anforderungen gerecht wird. Und wer selbst als Dienstleister in diesem Markt unterwegs ist, sollte hier über eine eigene Listung nachdenken.

Ganz ähnlich funktioniert auch das Produktverzeichnis der Site. Auch hier befördert eine Suche nach einem spezifischen Produkt zahlreiche Treffer in die Anzeige. Kritisch anzumerken ist hier allerdings, dass offensichtlich die Produkte der Sponsoren der Site eine gewisse Priorität genießen. Allerdings lässt sich die Auswahl über eine "Klassifizierung" und ein Tagwolke komfortabel eingrenzen, so dass auch hier schnell ein passendes Ergebnis zu finden sein sollte. Darüber hinaus bietet die Webseite eine Jobbörse und einen sehr gut gepflegten Terminkalender aktueller Veranstaltungen zur IT-Sicherheit. Der Bereich "Ratgeber" besteht hingegen eher in den seltensten Fällen den Vergleich mit alteingesessenen Seiten zum selben Thema. Hier besteht sicher noch Ausbaubedarf – sehenswert sind aber allemal die Videos rund ums Live-Hacking und dem eigenen Anspruch, ein Marktplatz der IT-Sicherheit zu sein, tut dies auch keinen Abbruch. *(jp)*



Ob Anbietersuche, Produktinformationen oder Ratgeber – it-sicherheit.de deckt den Security-Markt gut ab



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:**

Grundlagen einer leistungsstarken Unified Communications-Umgebung

Eine genaue Kenntnis der ITK-Infrastruktur ist unabdingbar für den Aufbau einer Unified Communications-Infrastruktur. Gefragt ist an dieser Stelle Daten- und Netzwerk-Knowhow, um klassische TK-Anlagen mit IP-Telefonie zu kombinieren. In unserem Online-Beitrag werfen wir einen genaueren Blick auf die Architektur einer möglichst problemfreien UC-Lösung, beschäftigen uns mit der Rolle von Medien-Gateways und erörtern, ob Unternehmen mit einer internen oder einer externen Lösung besser beraten sind.
www.it-administrator.de/themen/kommunikation/fachartikel/86562.html

SharePoint 2010 – Collaboration auf der Höhe der Zeit?

Seit Mai ist SharePoint 2010 auf dem Markt. Aber hält die neue Version, was Microsoft verspricht? Erste Erfahrungen und Berichte von Anwendern zeigen, dass sich ein Wechsel durchaus lohnen kann. Clevere Neuerungen erleichtern die Zusammenarbeit im Unternehmen und in Teams, indem sie zum Beispiel Enterprise 2.0- und Social Networking-Funktionen deutlich stärker als bisher ermöglichen. Unser Online-Fachartikel gibt einen Überblick über den Nutzen, aber auch die Einschränkungen der Business-Plattform.
www.it-administrator.de/themen/kommunikation/fachartikel/86563.html

Wichtige Versicherungen für IT-Dienstleister

Bei den unzähligen Spezialthemen, mit denen sich Unternehmer aus der IT-Branche heute beschäftigen müssen, bleiben andere wichtige Angelegenheiten wie Versicherungen nicht selten auf der Strecke. Selbständige sollten jedoch die Risiken der Informationsbranche kennen und sich absichern – gerade da Geschäftsführer für Versäumnisse vor Gericht persönlich haftbar gemacht werden können. In unserem Web-Fachartikel zählen wir auf, welche Versicherungen Sie keinesfalls vergessen sollten und welche Details dabei zu beachten sind.
www.it-administrator.de/themen/sicherheit/fachartikel/86564.html

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

»Sicherheit und Datenschutz wird zu wenig Aufmerksamkeit geschenkt«

Thomas Reitinger arbeitet im IT-Team von Inergy Automotive Systems, einem weltweit führenden Automobilzulieferer für Kraftstoffsysteme mit Standorten in 25 Ländern. In Deutschland betreut der Systemadministrator aus Hessen sechs unterschiedliche Standorte.

Welche Ausbildung haben Sie gemacht?

Ich habe eine Ausbildung zum Anlagenenergieelektroniker begonnen und erfolgreich abgeschlossen.

Warum sind Sie IT-Administrator geworden?

Weil ich schon immer sehr technikbegeistert war und es auch heute noch bin. Seitdem ich PCs besitze, habe ich alle meine IT-Systeme selbst zusammengebaut, installiert, administriert sowie Fehler gesucht und auch behoben. Mein Beruf ist eine logische Folge meiner Technik-Begeisterung.

Welche IT-Umgebung betreuen Sie?

Ich bin Systemadministrator für unsere produktiven Just in Time / Just in Sequenz-Systeme sowie Level 1 und Level 2-Supporter für unsere Office-Anwender. Darüber hinaus betreue ich im Team mit zwei Kollegen unsere kritischen Systeme in einem 24/7-Dienst. Unsere IT-Umgebung basiert auf 25 Servern, 120 Office PCs inklusive Laptops sowie 50 Produktions-Systemen. Als Betriebssystem setzen wir Microsoft Server und Windows XP-Clients ein. Bei den Applikationen im Office-Bereich verwenden wir ebenfalls hauptsächlich Microsoft-Produkte, ansonsten haben wir noch speziell für unsere Systeme entwickelte Software im Einsatz.

Welches Netzwerk- und Systemmanagement setzen Sie ein?

Wir setzen im Bereich Netzwerk und Netzwerk Management ausschließlich auf Cisco-Systeme. Das System-Management wird von einer auf unsere Anforderung entwickelten Software übernommen.

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

Wirklich ungern mache ich nichts. Aber es gibt natürlich immer einige Dinge, durch die man abgelenkt wird, beispielsweise die Beschaffung von Hard- und Software. Dafür ist im Vorfeld ein Genehmigungsvorgang notwendig, der natürlich Zeit beansprucht.

Geburtstag: März 1978
Familienstand: in einer Beziehung
Hobby: Fotografie

Thomas Reitinger, IT-Administrator

Spielt Messaging und Collaboration in Ihrem Unternehmen eine Rolle und wenn ja, welche Optionen nutzen Sie dafür?

Wie jedes andere große und mittelständische Unternehmen setzen wir auf mehrere interne Kommunikationwege. Darunter zählen neben den Windows-Tools auch Telefon, E-Mail und Messaging-Systeme.

Was tun Sie für Ihre Fort- und Weiterbildung?

Ich besuche interne sowie externe Fortbildungen. Hinzu kommen auch eigene Recherchen beispielsweise im Internet oder in Fachmagazinen.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Die Weiterentwicklung unseres Systems steht auf der Prioritätenliste ganz weit oben. Hinzu kommt die Entwicklung und Installation eines Standort-übergreifenden Traceability Tools, das sehr viel Sorgfalt erfordert.

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

Während meiner ersten Monate bei meinem jetzigen Arbeitgeber hatten wir noch ältere Geräte im Einsatz und mussten das Backup per Batch-Datei starten. Eines Tages gingen in einem Server der RAID-Controller sowie zwei der drei Festplatten gleichzeitig kaputt. Das war es dann für das RAID 5 und die darauf gespeicherten Daten. Glücklicherweise gab es noch ein relativ aktuelles Backup, so dass sich der Schaden in Grenzen hielt.

Was war Ihr größter Erfolg als IT-Administrator?

Auf die Entwicklung einer Software zum Monitoring unserer Systeme bin ich stolz, denn sie zeigt uns auf einen Blick wirklich schnell und zuverlässig den Status aller wichtigen Server an allen Standorten an. Von dem System werden auch die SQL-Datenbanken erfasst.

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

Das ist schon einige Jahre her. Bei der Installation einer Software (damals noch auf Disketten) habe ich während des Prozesses den User angerufen und ihn gebeten, Diskette 2 einzulegen. Leider teilte ich ihm nicht ausdrücklich mit, vorher doch bitte die erste Diskette herauszunehmen. Das war ungeschickt, denn die zweite Diskette ließ sich zwar noch hineinschieben, aber beide gleichzeitig nicht wieder auswerfen.

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

Für uns intern wird die größte Herausforderung sein, die Virtualisierung unserer Systeme anzugehen. Allgemein würde ich sagen, dass der Sicherheit der IT-Systeme und auch dem Datenschutz zu wenig Aufmerksamkeit zuteil wird.

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 10/10 erscheint am 4. Oktober 2010

Schwerpunktthema:

Sicherheit für virtualisierte Infrastrukturen

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

Unsere Ausgabe im **November** steht unter dem Schwerpunkt **Storage**. In unseren Tests betrachten wir die Storage-Geräte AssuredSAN und sayFUSE. In der Praxisrubrik erfahren Sie außerdem, wie Sie ein hochverfügbares SAN im Eigenbau errichten.

Als Schwerpunkt im **Dezember** folgt dann das Thema **WiFi, VoIP und WLAN-Management**.

***Im Test:* McAfee Total Protection for Virtualization**

***Im Test:* Active Directory-Berechtigungen dokumentieren und verwalten mit 8Man 2.0**

***Workshop:* Sichere VLAN-Konfiguration unter VMware**

***Workshop:* Sicherheit bei APP-V, VDI und Desktopvirtualisierung**

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, Jerry J. Artishdad, Thomas Bär, Oliver Ebel, Christian Egle, Florian Frommherz, Jürgen Heyer, Thomas Joos, Sandro Lucifora, Thorsten Scherf, Holger Sesterhenn, Elmar Török, Ulf B. Simon-Weidner

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

Es gilt die Anzeigenpreisliste Nr. 7 vom 01.11.2009

LAC/2008

Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik
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

Diese Ausgabe enthält eine Teilbeilage der Firma ppedv und eine Teilbeilage der Firma EUROFORUM.

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

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.

INNOVATIONSPREIS-IT
KATEGORIESIEGER
2009
initiative mittelstand
STORAGE/NETZWERKE

LANCOM OAP-310agn

it & business
26.–28.10.2010
MESSE STUTTGART

LANCOM
Systems

www.lancom.de