IT-ADMINISTRATOR.DE

08/2011

€ 12,60 ISSN 1614-2888

iadministrator

Das Magazin für professionelle System- und Netzwerkadministration

Systemmanagement

4 196583 212605 08

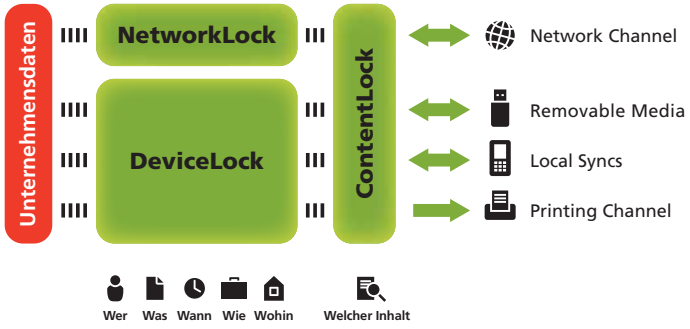
Macht kein großes Aufheben um ein paar Überstunden.

Oder um ein paar Datensätze.

Mitarbeiter sind auch nur Menschen.
Da kann es passieren, dass Daten unverschlüsselt in falsche Hände geraten. Oder gelöscht werden. Oder manipuliert. Oder mit Viren verseucht. Schützen Sie sich davor!

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

Die Datenflusskontrolle der DeviceLock Endpoint DLP-Suite



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

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security

EDITORIAL

Geteilte Cloud, geteilte Daten?

Liebe Leser,

glauben wir den Versprechen der Hersteller, so ist die Cloud sicherer als die selbst betriebenen Rechner im eigenen Unternehmen: weniger Ausfälle, stringentere Backups, neuere Hardware. Tag und Nacht kümmern sich zahllose IT-Spezialisten bei Amazon, Microsoft, Google und Co. um ihre Infrastruktur. Jedes Grad Abweichung im Serverraum, jeder Zutritt und jede einzelne CPU-Auslastung wird genauestens überwacht. Die Neunen hinter dem Komma wollen verdient sein. Das Ziel ist dabei klar: Firmen sollen ihre Daten möglichst umfassend und schnell in die Cloud verlagern. Praktisch ist dies allemal angesichts der zunehmenden Mobilität der Mitarbeiter.

Seit diesem Sommer ist nun auch Microsoft mit Office 365 in der Wolke präsent (siehe Seiten 8 und 13). So können sich Unternehmen aussuchen, ob sie lieber mit einem fest installierten Office-Paket arbeiten möchten oder mit dem virtuellen. Eigentlich prima – wenn das Thema Datenschutz nicht wäre. Microsoft-Manager Gordon Frazer musste schon kurz nach dem Start des Online-Dienstes zugeben, dass US-amerikanische Justizbehörden und Geheimdienste auch auf europäische Server Zugriff hätten. Microsoft als amerikanisches Unternehmen unterliegt nun mal US-Gesetzen, die einen verhältnismäßig freizügigen Datenzugriff erlauben. Und auch andere Vorfälle lassen Unternehmen aufhorchen. So etwa die Panne beim Online-Storage-Anbieter Dropbox. Für kurze Zeit konnten sich Nutzer mit beliebigen Passwörtern an jedem Account anmelden und auf die Daten zugreifen. Sicher sieht anders aus – zumal Dropbox im Nachgang auch noch seine AGB zum Nachteil der Kunden in Sachen Datenzugriff durch US-Behörden angepasst hat.

Grundsätzlich ist gegen den Trend, Dienste in der Cloud anzubieten, nichts einzuwenden. Doch scheinen sowohl Anbieter wie auch Gesetzgeber zumindest für Europa erst noch den richtigen Weg finden zu müssen. Ein Lösungsansatz für Unternehmen ist natürlich die durchgängige Verschlüsselung ihrer Daten. Doch das setzt auch eine entsprechend komplexe Infrastruktur im eigenen Netzwerk voraus. Wie Sie als Administrator derweil Ihre eigenen Server noch besser in den Griff bekommen, lesen Sie in dieser Ausgabe. So zeigen wir Ihnen, was die Eye Of The Storm Network Professional Edition zu bieten hat und wie Sie Gruppenrichtlinien mit AGMP 4.0 verwalten. Eine Neun mehr hinter dem Komma kann schließlich nie schaden.

Viel Spaß beim Lesen,

Ihr

Daniel Richey
Stellv. Chefredakteur

Systemmanagement

Im Test: Quest OnDemand Recovery for Active Directory

Das Online-Backup von Arbeitsdaten auf Speicherpools im Internet hat sich schon seit längerem etabliert. Jetzt bietet Quest einen vergleichbaren Dienst für die Sicherung des Microsoft Active Directory an. Schützen lassen sich einzelne Domänen, aber auch ganze Forests. Abgerechnet wird monatlich anhand der gesicherten Benutzerobjekte. IT-Administrator wollte wissen, ob dies tatsächlich so einfach und zuverlässig funktioniert, wie es auf den ersten Blick erscheint.

Seite 27

Gruppenrichtlinien-verwaltung mit AGPM 4.0

Die Group Policy Management Console – kurz GPMC – ist nach wie vor das Standardwerkzeug, um Gruppenrichtlinien zu bearbeiten. Aber auch bei Windows Server 2008 R2 hat Microsoft der GPMC keine neuen Funktionen spendiert, die den Umgang mit GPOs sicherer und einfacher gestalten würden. Abhilfe schafft die Advanced Group Policy Management Console (AGPM), die Software Assurance-Kunden von Microsoft zur Verfügung steht und einige wesentliche funktionale Lücken der Standard-Konsole füllt. Unser Workshop stellt die Neuerungen in AGPM 4 vor und wirft einen Blick auf die rollenbasierte Administration von Gruppenrichtlinien.

Seite 50

AKTUELL

PRODUKTE

PRAXIS

WISSEN

RUBRIKEN

SharePoint 2010 im Internet veröffentlichen (1)

SharePoint 2010 spielt seinen ganzen Nutzen dann aus, wenn auch mobile Anwender auf das System zugreifen können. Dazu ist es notwendig, die Dienste zu veröffentlichen. Neben dem Forefront Threat Management Gateway 2010 – TMG 2010 – bietet Microsoft für diese Aufgabe noch das Forefront Unified Access Gateway 2010 – UAG 2010 – an. Hierbei handelt es sich um eine erweiterte Version des TMG, die besser für SharePoint geeignet ist. Im Rahmen unserer Workshopserie veröffentlichen wir zunächst Schritt für Schritt eine SharePoint-Seite mit TMG 2010 und anschließend Seiten und Applikationen mit UAG 2010.

Seite 54

Systemmonitoring-Ansätze im Vergleich

Idealerweise weiß der IT-Administrator, dass mit einem System etwas nicht stimmt, bevor es die Benutzer merken. Doch der Alltag sieht meist anders aus: reaktives Handeln, fehlende Gesamtübersicht und umständliches Monitoring der Systemlandschaft durch einzelne Herstellertools oder gar manuell. Hier kann systematisches Systemmonitoring Abhilfe schaffen. Dabei müssen es nicht immer teure Monitoring-Suiten sein, auch der Open Source-Bereich hat inzwischen einiges zu bieten.

Seite 72

Themenübersicht

Sicherer Begleiter

Acer stellt die neuen **Notebook-Modelle TravelMate 7750 und 5760** vor. Die Geräte richten sich an Unternehmen sowie Small- und Home-Office-Nutzer. Verfügbar mit Bildschirmdiagonalen von 43,94 cm (17,3 Zoll) beim Acer TravelMate 7750 und 39,6 cm (15,6 Zoll) beim Acer TravelMate 5760, jeweils im Seitenverhältnis 16:9, sind die neuen Geräte mit einem entspiegelten High-Brightness-Panel inklusive LED-Hintergrundbeleuchtung ausgestattet. Die ebenfalls neue Acer FineTouch-Tastatur mit vergrößertem Anschlagsabstand soll zudem für komfortableres Schreiben sorgen. An Speicherplatz stehen bis zu **750 GByte** zur Verfügung. Das Modell TravelMate 7750 bietet zudem die Möglichkeit, zwei Festplatten zu integrieren. Ein DVD-Super Multi Double Layer-Laufwerk und der integrierte Multi-in-1 Card Reader, der die gängigen Formate unterstützt, sollen den Datenaustausch vereinfachen und bieten erweiterte Speichermöglichkeiten. An DDR3-Arbeitsspeicher stehen bis zu 8 GByte bereit. Eine Pre-Boot Authentication mit BIOS/HDD-Kennwort schützt die Notebooks vor unerwünschten Zugriffen. Die Sicherung mit einem BIOS-Passwort verhindert dabei ein nicht autorisiertes Hochfahren des Systems, während die HDD-Kennung zusätzliche Sicherheit bieten soll, falls die Festplatte aus dem Computer entfernt werden sollte. Außerdem verfügen die neuen Notebooks über die **Intel Anti-Theft-Technologie sowie Absolute Data Protection (ADP) von Absolute Software**. Die eingebaute Lösung ermöglicht die Sperrung des Notebooks per Fernzugriff bei Verlust oder Diebstahl. Während dieser Zeit ist das Notebook nicht betriebsbereit und der Zugriff auf verschlüsselte Daten nicht möglich. Findet der Rechner den Weg zurück zum Besitzer, kann die Sperre jederzeit problemlos wieder aufgehoben werden. Die Anti-Diebstahl-Software ermöglicht darüber hinaus jederzeit die Ortung des Gerätes. Ab 699 Euro (Acer TravelMate 7750) beziehungsweise ab 559 Euro (Acer TravelMate 5760) sind die Modelle erhältlich. *(dr)*

Die neuen Acer-Notebooks sollen dank Sicherheitsfeatures vor Datendiebstahl schützen

Acer: www.acer.de

Breites VPN-Tor

Funkwerk Enterprise Communications (FEC) präsentiert das neue **Central-Site-VPN-Gateway bintec RXL12500** und erweitert damit sein Produkt- und Lösungsportfolio um eine zentrale Komponente für flexible VPN-Filialvernetzungen. Ab Werk verfügt der bintec RXL12500 über eine Lizenz für 100 IPSec-Tunnel, die optional auf bis zu 2.500 erweiterbar sind. Mit einer optionalen Hardwareverschlüsselung erreicht das Gerät dabei bis zu 700 MBit/s (3DES/AES). Das Gateway im 19 Zoll-Metallgehäuse mit integriertem Schaltnetzteil verfügt über zehn GBit-Ethernet-Ports (acht RJ45 und zwei SFP), die sich frei für LAN, WAN oder DMZ konfigurieren lassen – Glasfaser-basierte Anbindungen werden über SFP-Slots ermöglicht. Die Anschaltung des optionalen Netzteileinschubes bintec PSU XL ermöglicht eine redundante Stromversorgung. Backup-Möglichkeiten, das bintec Router Redundancy Protocol (BRRP), Load Balancing sowie das Routing-Protokoll OSPF machen das Gateway zudem ausfallsicher und hochverfügbar. Der bintec RXL12500 ist als Basisgerät inklusive 100 IPSec-Tunneln ab sofort für 2.599 Euro erhältlich. *(dr)*

Funkwerk: www.funkwerk-ec.com

Erweiterte Verwaltung fürs WLAN

LANCOM stellt seinen Kunden ein kostenloses Update für ihre Access Points, WLAN Controller, Router und Gateways zur Verfügung. Die **Version 8.5** des **LANCOM Operating System** (LCOS) und des **LANCOM Management System** (LCMS) bringt unter anderem neue Funktionen im Bereich Management und Rollout. Das LCMS besteht aus den Windows-Programmen **LANconfig**, **LANmonitor** und **WLANmonitor** und dient zur Konfiguration und Überwachung aller LANCOM-Router und Wireless-LAN Access Points. LCOS und LCMS stehen kostenlos auf der LANCOM-Webseite zum Download bereit. Neu im LANCOM Management System ist der "LANCOM QuickFinder". Mit der Echtzeitsuche lassen sich einzelne Netzwerkgeräte, verwaltete Access Points, assoziierte WLAN-Clients oder auch Namen und Werte innerhalb von Konfigurationen ohne aufwändige Suchmasken intuitiv und komfortabel finden. Ein weiteres Management-Plus der neuen Version: Die Suche nach neuen LCOS-Versionen für die verwalteten Geräte und die Aktualisierung des LCMS selbst kann ab sofort automatisch online in LANconfig durchgeführt werden. Das Management System steht allen LANCOM-Kunden kostenlos zur Verfügung. Komplexe Netzwerkprojekte und große Rollouts sollen zudem von der neu implementierten Unterstützung des Online Certificate Status Protocol (OCSP) profitieren. Damit kann die Gültigkeit von Zertifikaten in Echtzeit überprüft werden. Über den ebenfalls neuen "Programmierbaren Rollout-Assistenten" für aktuelle LANCOM VPN-Router der 168x-, 17xx- und 18xx-Serien können Kunden individuelle Assistenten erstellen, die die sichere Inbetriebnahme von Netzen mit vielen Geräten erleichtern. Die Inbetriebnahme an den Standorten soll so auch durch Mitarbeiter ohne besondere Fachkenntnisse möglich sein. *(dr)*

LANCOM: www.lancom.de

Mehr Sicherheit mit weniger Klicks

WatchGuard Technologies präsentiert ein neues **Software-Update für seine XCS-Familie von Web- und Messaging-Security-Appliances**. Mit dem Release erhalten Unternehmen zusätzliche, einfach bedienbare Funktionen. Zudem umfasst die Erweiterung eine **Content- und Policy-Kontrolle für beschleunigten Webtraffic** sowie neue Technologien zur Vorbeugung von Spam und Phishing. Intuitive Kontrollen und grafische Anzeigen sollen ferner die schnelle Interpretation von Ergebnissen ermöglichen. Auch für die Definition von Content-Kontrollen sollen nur noch wenige Schritte notwendig sein. Benutzer werden durch eine verbesserte Bedienoberfläche und inkludierte Konfigurationshilfen Schritt für Schritt durch Messaging-Security-Szenarien und Aufgaben geleitet. Das jüngste Release beinhaltet dabei Möglichkeiten für jeden Anwendungsfall – von der simplen Policy bis zur fein abgestuften Datenverlust-Präventions-Kontrolle. Über ein Interface lassen sich auf diese Weise laut Anbieter binnen Minuten ein bidirektionales Scanning sowie die Kontrolle von über 400 Attachment-Typen anlegen. Darüber hinaus werden Administratoren über DLP-Verletzungen mit individuell anpassbaren regelbasierten Meldungen benachrichtigt und können feststellen, welche Regel die Verletzung ausgelöst hat. Das Release ist ab sofort verfügbar. Die WatchGuard-Appliances starten bei 2.511 Euro. *(dr)*

WatchGuard: www.watchguard.de

WatchGuard-Appliances sollen dank neuer Software intuitiver zu bedienen sein

Skalierbare Netzwerkspeicher

Synology bringt drei neue NAS-Systeme der xs-Serie auf den Markt, bestehend aus der 12-bay DiskStation DS3611xs und den 10-bay RackStations RS3411xs und RS3411RPxs. **Alle Modelle sind in punkto Speicherplatz und Leistung skalierbar**. Ein Volume ist mithilfe der Erweiterungseinheiten dabei dynamisch auf über 100 TByte ausbaubar. Über ein InfiniBand-Kabel, das ein 12 GBit/s SATA-Signal überträgt, soll zudem eine Verbindung mit hoher Bandbreite gewährleistet sein. Der Datendurchsatz lässt sich von einer 1 GBit-Netzwerkverbindung bis zu einer 4 GBit- oder auch einer dualen 10 GBit-Netzwerkverbindung aggregieren. Ausgestattet mit einem Intel Core-Prozessor liefern die NAS-Systeme der xs-Serie laut Hersteller einen Datendurchsatz von mehr als 1.000 MByte/s und 100.000 IOPS bei aktivierter Link-Aggregation. Betrieben mit dem Synology DiskStation Manager 3.1 richten sich die Systeme der xs-Reihe insbesondere an den professionellen Einsatz in mittleren und größeren Unternehmen. Ab sofort sind die NAS-Produkte erhältlich. Die Preise beginnen bei 1.849 Euro für das Modell RS3411xs und reichen bis cirka 2.520 Euro für die Variante RS3411RPxs. *(dr)*

Synology: www.synology.de

Die neuen NAS-Systeme der xs-Serie von Synology sind auf über 100 TByte skalierbar

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

PsiberData stellt die **Firmware-Version 3.6** für seine Kabelzertifizierungsgeräte vor. Der WireXpert von PsiberData wurde entwickelt, um alle Kupferdatenverkabelungen von Kategorie 5 bis 7a und Klasse C bis Fa zu zertifizieren. Er ist laut Hersteller der erste Tester, der darüber hinaus über einen erweiterten Frequenzbereich bis 1.600 MHz verfügt, um zukünftigen Anforderungen gerecht zu werden. Das kostenlose Update auf V3.6 soll Nutzern neben kleineren Verbesserungen eine landessprachige Bedienerführung in Deutsch sowie neun weitere Sprachen bieten. *(dr)*

www.psiberdata.de

LaCie bietet die neue **d2 Quadra-Festplatte** mit USB 3.0-Technologie an. Damit stehen zumindest theoretische Übertragungsraten von bis zu 640 MByte/s zur Verfügung. Die Harddisk ist zudem mit eSATA 3 GBit/s, USB 2.0 und FireWire 400 kompatibel. Im Betrieb lässt sich die Festplatte vertikal aufstellen, horizontal stapeln oder in einem Rack montieren. Das Modell LaCie d2 Quadra USB 3.0 mit einer Kapazität von 3 TByte ist für 268 Euro erhältlich. *(dr)*

www.lacie.com

McAfee erweitert sein Angebot an Sicherheitslösungen für tragbare Endgeräte um **McAfee Mobile Security** und **McAfee WaveSecure Tablet Edition**. Mobile Security vereint drei McAfee-Produkte: WaveSecure, VirusScan Mobile und SiteAdvisor for Android. Die WaveSecure Tablet Edition bietet Android-Nutzern mit WiFi die Möglichkeit, abhandengekommene Geräte mittels Alarm und Ortung wieder aufzufinden. Ein einjähriges Abonnement für McAfee Mobile Security kostet 29,99 US-Dollar bei McAfee und im Android Market. Für McAfee WaveSecure fallen 19,99 US-Dollar pro Jahr an. *(dr)*

www.mcafee.de

Panda Security hat die **Programmversion 1.5** seines kostenfreien Antivirenschutzes **Panda Cloud Antivirus** gelauncht. Das Release bietet unter anderem neue und erweiterte Konfigurationsoptionen zum Ausschluss von Dateien basierend auf Datei-Erweiterungen sowie zum Blockieren von potenziell unerwünschten Programmen. Ein neuer Aktivitäts-Monitor soll zudem detaillierte Informationen zu gescannten Dateien und erkannten Viren bieten. Panda Cloud Antivirus kann von Computer-Nutzern kostenfrei verwendet werden. *(dr)*

www.cloudantrivirus.com

Platzsparende Hochleistungskühlung

Mit **TopTherm LCP Rack** und **TopTherm LCP Inline** stellt Rittal zwei Kühlsysteme für Rechenzentren mit einer **Kühlleistung von bis zu 60 kW** vor. Die Systeme benötigen dabei eine Fläche von lediglich 0,36 Quadratmetern. Die Kaltluft wird auf einen oder zwei Serverschränke konzentriert, indem der anreihbare Luft/Wasser-Wärmetauscher sie über perforierte Seitenwände direkt vor die Server in den Schrank bläst. Im Inneren des Schranks, an der Rückseite der Server, wird die warme Luft abgesaugt und im TopTherm LCP Rack gekühlt. Somit bildet sich ein geschlossener Luftstrom ohne verlustreiche Vermischung von Kalt- und Warmluft. Die Klimalösungen sind modular aufgebaut, durch sechs modular einbaubare Lüfterkassetten kann die Kühlleistung an den tatsächlichen Bedarf angepasst werden. Redundante Temperatursensoren sowie zusätzliche Lüfter sorgen für hohe Ausfallsicherheit. Das Rittal TopTherm LCP Rack und das Rittal TopTherm LCP Inline sind ab dem 3. Quartal 2011 bei Rittal erhältlich. Die LCP-Varian-ten, die Kältemittel statt Wasser verwenden, sind ab dem 1. Quartal 2012 verfügbar. Die Preise standen zu Redaktionsschluss noch nicht fest. *(dr)*

Das TopTherm LCP Rack von Rittal sorgt für Kühlung und beansprucht 0,36 qm an Fläche

Rittal: www.rittal.de

Office aus der Cloud

Microsoft bietet **Office 365** nun als kommerzielles Cloud-Angebot in Deutschland und 39 weiteren Ländern an. Mit Office 365 greifen Unternehmen auf die aktuellen Versionen von **Microsoft Office, SharePoint Online, Exchange Online und Lync Online** zu und sollen dabei von monatlich kalkulierbaren Kosten profitieren. Office 365 gibt es in verschiedenen Versionen: Mit Office 365 für Kleinunternehmen und Selbständige erfolgt der Start von Office Web Apps, Exchange Online, SharePoint Online, Lync Online und einer externen Internetseite laut Microsoft in nur 15 Minuten für 5,25 Euro pro Benutzer und Monat. Microsoft bietet mit diesen Werkzeugen allen Anwendern Zugang zu E-Mail, Voicemail, Enterprise Social Networking, Instant Messaging, Webportalen, Extranets, Video Conferencing, Web Conferencing und anderen Produkten. Office 365 für Unternehmen bietet dagegen verschiedene Auswahlmöglichkeiten für mittelständische und große Unternehmen sowie Regierungsorganisationen. So steht die Basis-E-Mail-Funktion für 1,79 Euro pro Benutzer und pro Monat zur Verfügung. Office 365 für Unternehmen umfasst Microsoft Office Professional Plus Desktop Software auf einer Pay as you go-Basis und steht für 22,75 Euro pro Benutzer und pro Monat bereit. Microsoft-Partner und Dienstleistungsanbieter wollen Office 365 künftig in ihre bestehenden Angebote einbinden und bereitstellen. *(dr)*

Microsoft: www.office365.com

Mehr Schutz für den Collax Server

Collax kündigt **vier neue Sicherheits- und Netzwerklösungen für den Collax Platform Server** an: **Collax Gatekeeper, Collax Multi-Level-Firewall, Collax Advanced Networking** und **Collax SSL-VPN**. Das Modul **Gatekeeper** umfasst eine Firewall, die Stateful Paket Inspection leistet und eine integrierte Firewall-Matrix bietet. Die Firewall-Matrix ist eine interaktive grafische Darstellung aller Firewall-Regeln und ermöglicht somit eine besonders einfache und intuitive Administration. Sie bietet einen umfassenden Überblick über alle Regeln und ihre Auswirkungen und verhindert, dass versteckt enthaltene Regeln oder nicht korrekt angeordnete Regeln ungewollt Sicherheitslücken schaffen. Gatekeeper ermöglicht es darüber hinaus, VPNs einzurichten (IPsec, L2TP und PPTP). Ebenso wie eine Standard-Firewall soll die **Multi-Level-Firewall** unberechtigte Zugriffe auf das Unternehmensnetzwerk verhindern. Die Firewall identifiziert und authentifiziert zudem Benutzer, Anwendungen und Betriebssysteme. Damit können IT-Verantwortliche granular definieren, welche Benutzer oder Benutzergruppen mit welchen Anwendungen Verbindungen in das Internet aufbauen dürfen. Das Modul **Collax Advanced Networking** sorgt dafür, dass das Firmennetzwerk effizient, zuverlässig und performant arbeitet. Zu den Funktionen des Moduls zählen Policy Based Routing, Multi-WAN, IDS/IPS und Traffic Shaping. Mit Policy Based Routing können Administratoren den Datenverkehr klassifizieren und diesen über die gewünschte Verbindung weiterleiten. **Collax SSL-VPN** ermöglicht es schließlich Mitarbeitern, von unterwegs oder aus dem Home Office sicher auf die Unternehmensressourcen zuzugreifen. Die neuen Security- und Networking-Lösungen stehen für den Collax Platform Server ab Version 5.0.26 zur Verfügung und sind ab sofort erhältlich. Der Preis für die Basislösung beträgt 65 Euro für zehn User pro Jahr. Eine Erweiterung für fünf User kostet 20 Euro pro Jahr. *(dr)*

Collax: www.collax.com

Leise und günstig

ZyXEL stellt die neue **ES1100 Switch-Serie,** bestehend aus sechs Switches, vor. Sie ist speziell auf die Anforderungen und Bedürfnisse mittelständischer Unternehmen abgestimmt. Bei der Entwicklung standen einfache Installation und Konfiguration sowie Energie-Effizienz im Vordergrund. Die ES1100-Serie besteht aus drei Fast-Ethernet-Geräten: **ES1100-16, ES1100 24E** und **ES1100-24G** mit 16 Ports als Desktop-Gerät, mit 24 Ports sowie mit 24 Ports für den Rack-Einbau. Zudem gehören die zwei Power-Over-Ethernet-Geräte ES1100-8P und ES1100-16P mit acht respektive 16 Ports zur Serie. Entwickelt wurden die Switches laut ZyXEL zur Leistungs- und Effizienz-Steigerung von Netzwerken in kleinen und mittleren Unternehmen. Mit der N-Way Auto Negotiation-Funktion stellt der Switch automatisch die größtmögliche Datenrate bei der Verbindung her und aktiviert bei Bedarf auch den Duplex-Modus automatisch. Dank des lüfterlosen Designs können die Geräte der ES1100-Serie auch in lärmempfindlichen Büroumgebungen eingesetzt werden. Die Preise liegen je nach Modell zwischen 38 und 150 Euro. *(dr)*

Die neuen ZyXEL ES1100-Switches lassen sich dank Plug-and-Play einfach im Netzwerk installieren

ZyXEL: www.zyxel.de

Neue Datenverteiler von D-Link

D-Link präsentiert die nächste Generation **Layer 2-GBit-Switches** der xStack Business-Produkte. Die Modelle der **DGS-3120-Serie** adressieren mittelständische Unternehmen und eignen sich beispielsweise für den Einsatz als **Etagenswitche**. Die Reihe umfasst insgesamt fünf Modellvarianten und verfügt standardmäßig über das Software Standard Image (SI); ein erweitertes Enhanced Image (EI) ist ebenfalls auf Projektbasis verfügbar. Die Switche sollen den Aufbau eines modernen und sicheren Firmennetzwerkes unterstützen. So sind beispielsweise Schutzmechanismen wie Loopback Detection, Ethernet Ring Protection Switching (ERPS) sowie das Monitoringverfahren sFlow (beide nur EI-Version) integriert. Die Stack-Bandbreite von bis zu 40 GBit/s sorgt für redundante Anbindungsmöglichkeiten ohne Leistungsverluste. Das stapelbare IPv6-ready-Switchsystem erlaubt statisches Routing (EI) und kann auch direkt als Netzwerk-Backbone eingesetzt werden. Die Layer 2-GBit xStack Switches der Serie DGS-3120 sind ab sofort verfügbar. Die Preise beginnen bei rund 600 Euro. *(dr)*

D-Link: www.dlink.de

D-Link stellt neue Layer 2-GBit-Switches für mittelständische Unternehmen vor

Druckprozesse fest in Admin-Hand

ThinPrint gibt die Verfügbarkeit der **ThinPrint Engine 8.6** bekannt. Die neue Version soll eine verbesserte Druckfunktionalität, leistungsfähige Druckperformance, Erfassung der Druckkosten im Unternehmen sowie optimierte Mobilität bieten. Ab sofort unterstützt die Engine die **Finishing-Optionen** Lochen, Klammern, Binden sowie das Drucken von mehreren Seiten auf einem Blatt Papier. Mit dieser Verbesserung kann der Anwender den optimierten Druckprozess und zugleich alle Features seines Multifunktionsdruckers nutzen. Die Finishing-Optionen können auch im Zusammenspiel mit dedizierten und lokalen Druckservern zum Einsatz kommen. Das neue **VirtualCopy-Feature** ermöglicht es, mit einem Klick einen Ausdruck auf bis zu fünf verschiedenen Druckern zu starten. Zudem bietet die Version 8.6 eine komfortablere und einfache **Nutzer-Oberfläche**. Den Anwendern steht ein einheitliches Dialogfenster zur Verfügung, mit dem sie ihren Drucker konfigurieren und den Ausdruck starten können. Aufbauend auf der Geschwindigkeit und der Performance der Vorgängerversionen macht das neue **Speed-Cache-Feature** die ThinPrint Engine 8.6 noch einmal schneller. Durch das Cachen von Bildelementen, die sich in einem Druckjob wiederholen, etwa Logos, wird die Geschwindigkeit des Ausdrucks nochmals um 50 Prozent beschleunigt und zugleich die Netzwerklast verringert. Zusätzlich können Anwender innerhalb einer vom Administrator vordefinierten Skala selbst die Kompressionsraten ihrer Dokumente bestimmen. Die Möglichkeit, Webseiten ohne Bilder ausdrucken zu können, sorgt für eine deutliche Reduzierung des Toner- und Papierverbrauchs und spart Zeit. Als kostenloser Bestandteil der ThinPrint Engine ermöglicht die Tracking Report Engine ferner eine Kontrolle der Druckprozesse und der damit zusammenhängenden Kosten. Ab 2.980 Euro ist die ThinPrint Server Engine 8.6 verfügbar. *(dr)*

ThinPrint: www.thinprint.de/8-6

IT-Administrator Workshop "Windows Server 2008 R2" am 19. August in Lingen/Ems und 29. September in Langenfeld

Pflege für das Arbeitstier

von John Pardey

Wie seit diesem Jahr üblich, bieten wir unseren Workshop an zwei Terminen und Orten an. So haben Sie bessere Chancen, einen der Termine wahrzunehmen. Und doch ist der Workshoptermin am 19. August etwas Besonderes, bietet er doch wieder das Warmup zur ice:2011, einem der größten Events der deutschen IT-Community. Sollten Sie nicht zur ice reisen, steht Ihnen alternativ der Termin am 29. September in Langenfeld offen.

Zum Zeitpunkt des Erscheinens dieser Ausgabe des IT-Administrator wird die ice:2011 schon lange keinen Platz mehr frei haben – es sei denn, Sie werden zum glücklichen Gewinner unserer Verlosung (siehe Kasten "Gewinnen Sie Tickets für die ice:2011").

Exporte helfen administrieren

Im ersten Teil unseres Windows Server-Workshops bringt Ihnen Sascha Giebelhausen, Berater bei der adMERITia GmbH aus Langenfeld, die Vorzüge von Daten-Exporten aus dem Active Directory näher.

Denn fast täglich werden Exporte aus dem Active Directory benötigt. Sei es für normale administrative Tätigkeiten wie die Bereinigung von veralteten Benutzern, Computern oder IP-Adressen oder aber zur Vorbereitung auf Migrationen. Innerhalb des Workshops erfahren Sie, wie Sie schnell und einfach Informationen aus dem Active Directory exportieren und beispielsweise mit Excel weiterverwerten.

Methoden der Lizenzaktivierung

Anschließend wendet sich Thomas Gronenwald, ebenfalls Berater der adMERITia, den Key Management-Diensten unter Windows Server 2008 R2 zu. Derzeit stehen viele Unternehmen vor der Migration von Windows 2003 auf Windows 2008 Server beziehungsweise Windows XP zu Windows 7. Neben den zahlreichen Produktneuerungen gibt es aber auch wesentliche Veränderungen im Bereich der Lizenzaktivierung. Während dieses Workshops zeigen wir Ihnen auf, welche Unterschiede bestehen und erläutern die verschiedenen Methoden zur Bereitstellung einer funktionierenden Key Management-Infrastruktur in Ihrem Unternehmen.

Sicherheit für das Active Directory

Für den letzten Punkt der Workshoptagesordnung treten Gronenwald und Giebelhausen gemeinsam an, um den Teilnehmern zu vermitteln, in welchem Umfang das Active Directory Schutz benötigt und wie dieser optimal einzurichten ist. Da in nahezu jedem Unternehmen heutzutage die Active Directory-Dienste zur Verwaltung von Benutzern und Computern eingesetzt werden, ist das AD als Kernkomponente natürlich besonders schutzbedürftig. Innerhalb dieses Workshops erläutern wir Ihnen die Möglichkeiten verschiedener Härtungsmaßnahmen und zeigen Ihnen, wie Sie diese innerhalb Ihrer Infrastruktur umsetzen können.

Alle Informationen zur Anmeldung und zum Workshop finden Sie im Kasten "Workshop Windows Server 2008 R2". Die Anmeldung ist jeweils bis eine Woche vor dem jeweiligen Workshop-Termin möglich. Wir würden uns freuen, Sie in Lingen oder Langenfeld persönlich begrüßen zu dürfen.

Gewinnen Sie Tickets für die ice:2011

Für alle, die nicht nur unseren Workshop, sondern auch die ice:2011 am folgenden Tag besuchen wollen, verlosen wir zehn der heiß begehrten Eintrittskarten. Denn wie jedes Jahr war auch die ice:2011 innerhalb weniger Tage vollständig ausgebucht. Zentrale Themen sind neben den Standards Windows-Server, Virtualisierung oder IPv6 dieses Jahr soziale Netzwerke, Cloud Computing und mobile Endgeräte. Um an der Verlosung teilzunehmen, senden Sie eine E-Mail mit dem Betreff "iceBär" an redaktion@it-administrator.de. Einsendeschluss ist der 11. August. Die Gewinner werden schriftlich benachrichtigt.

Workshop Windows Server 2008 R2

iTANet
Die System und Netzwerk User Group

Agenda Workshop

13:00 Uhr: Begrüßung

13:15 Uhr: Windows, was kann ich dir entlocken? Windows Server-Exporte einmal anders.
Dozent: Sascha Giebelhausen

14:30 Uhr: Kaffeepause

14:45 Uhr: Key Management Services – Wieso, weshalb und warum? Die richtige Strategie für Unternehmen.
Dozent: Thomas Gronenwald

16:15 Uhr: Active Directory-Sicherheit – was brauche ich wirklich?
Dozenten: Thomas Gronenwald und Sascha Giebelhausen

17:30 Uhr: Ende der Veranstaltung

Ort

19. August: it emsland, Halle 31, Kaiserstraße 10b, 49809 Lingen

29. September: adMERITia GmbH, Gladbacher Straße 3, 40764 Langenfeld

Teilnahmegebühren

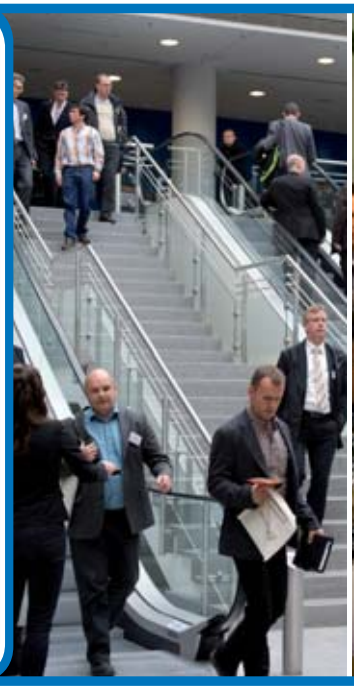
Für IT-Administrator-Abonnenten und ice:2011-Teilnehmer kostenlos.

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

Anmeldung bis zum 12. August (Lingen) beziehungsweise 22. September (Langenfeld) unter www.it-administrator.de/workshops.

Ihr direkter Weg zur IT-Sicherheit: Die IT-Security-Messe

www.it-sa.de



Nürnberg, 11.-13. Okt. 2011

Alles auf einen Blick:
Auf der it-sa 2011 finden Sie alle aktuellen Informationen, die Sie zum Thema IT-Security benötigen. Und die Angebote der IT-Security-Firmen, die zu Ihnen passen.

- 300 Aussteller mit Lösungen zu Informations-Sicherheit, Datenschutz, Hardware-Sicherung und Security-Awareness
- Non-Stop-Vortragsprogramm auf 3 großen Foren mit mehr als 250 Kurzreferaten, Podiumsdiskussionen und Live-Demos
- 20 Kongresse, Tagungen, Workshops, Seminare
- Guided Tours von unabhängigen Consultants
- Sonderflächen: Das perfekte Rechenzentrum, Convergence-Area, IAM-Area, Startups@it-sa, Campus@it-sa

Alle Details zu Veranstaltungen und Angeboten zur IT-Security finden Sie unter: **www.it-sa.de**.

Die IT·Security-Messe

Veranstalter: SecuMedia Verlags-GmbH, Postfach 12 34,
D-55205 Ingelheim, Telefon +49 6725 9304-0,
Fax +49 6725 5994 und NürnbergMesse GmbH,
Messezentrum, D-90471 Nürnberg

Gastkarte anfordern
www.it-sa.de/e-ticket
Code: 9NEM8739N3

Microsoft IT&DevConnections, 8. bis 10. Juni, Karlsruhe

Entwicklertreffen mit administrativen Schwerpunkten

von Klaus Bierschenk

Vom 08. bis 10. Juni lockte die "Microsoft IT&DevConnections" die Teilnehmer nach Karlsruhe. Neben anspruchsvollen Vorträgen, zum großen Teil für Entwickler, bot die Veranstaltung auch einiges Neues und Interessantes für Administratoren. Sie diente zudem als Plattform für den Informationsaustausch unter den facettenreichen Fachleuten. IT-Administrator war für Sie vor Ort.

Die Bezeichnung "Connections" ist unter IT-Veranstaltungen ein Begriff und steht für Konferenzen verschiedenster Microsoft-Technologien, die fast das ganze Server-Produktportfolio abdecken. Neben der regelmäßig stattfindenden Exchange- oder SQL-Connections ist die Windows Connections seit 15 Jahren eine der bekanntesten Veranstaltungen. Als Lokation dient meist eine Metropole in Nordamerika. Für die IT&DevConnections wählten die Organisatoren diesmal jedoch Karlsruhe als Ort für ihren Event, der für Entwickler ausgelegt ist und erstmalig einen administrativen Schwerpunkt versprach. Dies ist interessant in dem Zusammenhang, dass Microsofts TechED auf nächstes Frühjahr verschoben wurde [1] und neben der im Oktober stattfindenden TEC von Quest [2] nicht mehr viel bleibt für Administratoren, die es gewohnt sind ihr Wissen in Level 400-Vorträgen auf Konferenzen zu erweitern und die dabei nicht allzu weit reisen möchten.

Dave Mendlen (links), Senior Director Microsoft Developer Division, sprach die Entwickler an und zeigte mit Oliver Scheer, Developer Evangelist bei Microsoft, wie sich die Produktivität in Visual Studio verbessern lässt

Vielschichtige Inhalte

Neben den Tracks, ASP, Visual Studio und SQL für Entwickler gab es mit Beiträgen zu Exchange und SharePoint zwei Vortragsreihen für Admins. Zwar erwähnte die Konferenzbroschüre offiziell nur einen Admintrack für SharePoint. Exchange bietet aber entwicklerseitig wenig Inhalte, die die breite Masse ansprechen und somit enthielten die Vorträge vornehmlich Themen aus den Bereichen Management und Operations. Eine Übersicht aller Vorträge befindet sich auf der Webseite zur IT&DevConnections [3]. Die Teilnehmer konnten beliebig zwischen den Tracks wechseln und mussten sich nicht für einen der Themenbereiche entscheiden. Einige Vorträge wurde übrigens in deutscher Sprache präsentiert, da einige Referenten aus Deutschland kamen, ein Großteil von Microsoft Deutschland. Unter den Referenten tummelten sich nicht nur Visual Studio und ASP.net Gurus, sondern auch MVPs und Microsoft Entwickler. Gleiches galt für den Kreis der rund 500 Teilnehmer, was für ein insgesamt bunt gemischtes Publikum sorgte.

Keynote, Keynote, Keynote

Drei Keynotes, verteilt über die beiden Tage, zeigten, dass Microsoft eine Menge zu erzählen hat, was künftige Strategien und Entscheidungen betrifft. Dave Mendlen, Senior Director Microsoft Developer Division, sprach die Entwickler an und zeigte, unterstützt durch Oliver Scheer, Developer Evangelist bei Microsoft, wie

sich die Produktivität in Visual Studio verbessern lässt. Durch die Keynote unter dem Titel "SharePoint everywhere" führte Steve Fox, Director Developer and Platform Evangelism für SharePoint, ebenfalls aus den USA angereist. Er formulierte, wo für die Administratoren die Herausforderungen in der Zukunft liegen. Online Services und "Productivity everywhere" werden die Landschaften verändern. Eines der großen Schlagworte dabei sei Federation. Was in der Zusammenfassung nichts anderes bedeutet, als dass in der schnelllebigen Zeit die Identitäten immer zunehmender verteilt sein werden, wohingegen die Infrastrukturen zusammenwachsen.

Für die dritte Keynote erntete Scott Guthrie, Corporate Vice President .NET Developer Platform bei Microsoft, viel Applaus. Guthrie ist ein langjähriger Microsoft-Stratege, der einige Entscheidungen in Redmond mitgetragen hat. So zum Beispiel war er federführend bei der Entwicklung des .NET Frameworks beteiligt oder auch bei Silverlight. Er nahm die Zuhörer mit auf eine Reise in die Rechenzentren von Microsoft und zeigte, was technisch notwendig ist, um Azure, die Cloud Services-Plattform von Microsoft, mit einem Servicelevel von 99,95 Prozent bereitzustellen. Insgesamt beinhalten die Rechenzentren 200.000 Server. Eine Zahl, die beim ersten Hören absurd erscheint, beim genaueren Hinsehen aber plausibel wird. Ein Teil der Server schlummert und wartet darauf, dass Kunden mehr Rechenleistung hinzubuchen.

Ein wichtiges Verkaufsargument von Microsoft für ihre Cloud Services. Kunden können zum Beispiel im Weihnachtsgeschäft, wenn mehr Kapazität gefordert wird, diese kurzfristig ordern und danach, in der flaueren Zeit, wieder abbestellen. Das müsse ja schließlich irgendwie bewerkstelligt werden, so Guthrie. Die Rechenzentren sind redundant um den Globus verteilt: Jeweils zwei in Asien und den USA sowie zwei in Europa. Diese befinden sich in Dublin und Amsterdam. Teile der Rechenzentren sind in Form von Containern aufgebaut. So besteht zusätzlich die Möglichkeit, schnell Kapazitäten auf- und abzubauen. Die Container werden fix und fertig auf einem LKW angeliefert und an das Rechenzentrum quasi nur noch angedockt.

Pre-Conference Workshops für Admins

Den zwei Veranstaltungstagen vorgelagert waren Pre-Conference Workshops. Im SharePoint-Teil, der sich an Administratoren richtete, wurde jedoch nicht Hand angelegt, wie Admins es vielleicht in einem Workshop gewohnt sind. Vielmehr lauschten die Teilnehmer ganztägig den Worten von Dan Holme und nahmen Teil an seinen Erfahrungen. Holme ist SharePoint-Evangelist bei AvePoint und MVP für SharePoint. Zudem ist er Autor mehrerer Fachbücher, zum Beispiel der Microsoft SharePoint-Training MOC Unterlagen für die TS 70-667-Zertifizierung, die noch in diesem Jahr erscheinen werden. Holme kam aus Hawaii angereist und gab sein Know-how zum Besten. Der Workshop trug zwar den Titel "Masterclass", er richtete sich aber nicht nur an Administratoren mit viel Erfahrung, auch Neuankömmlinge in SharePoint 2010, die vor einer Migration stehen, erwartete Praktisches jeder Art und so gab es den einen oder anderen Aha-Effekt.

Zum Beispiel räumte er mit dem Thema Managed Service Accounts auf. Hierbei handelt es sich um ein neues Sicherheitsfeature in Windows Server 2008 R2 Active Directory. In SharePoint 2010 gibt es diesen Mechanismus für interne Konten in ähnlicher Form. Beides ermöglicht die automatisierte Verwaltung von Service Konten, statt diese wie bisher manuell zu administrieren, was zu ungewünschten Nebeneffekten führen kann – Beispiel: Passwortänderung. Bei SharePoint 2010 macht es Sinn, die Verwaltung der Passwörter ausschließlich über SharePoint zu steuern. Ein Zusammenspiel beider Funktionalitäten schließt sich aus und muss bei der Implementierung berücksichtigt werden. PowerShell in Verbindung mit SharePoint ließ er in dem Workshop außen vor. Zu diesem Thema verwies er auf den dedizierten Vortrag am letzten Veranstaltungstag.

Nicht ohne Office 365

Die Cloud ist mittlerweile überall, so auch auf der IT&DevConnections. Steffen Krause, Technical Evangelist bei Microsoft, zeigte in seinem Vortrag über Office365, wo Microsoft den Schwerpunkt legt. Wer weiß schon, welche Umgebungen Administratoren in zehn Jahren betreuen werden? Das Blech in den Betrieben wird vielleicht weniger, aber nicht die Notwendigkeit, die Infrastrukturen zu verwalten, philosophierte Krause. Eher wird es eine langsame Verlagerung der Tätigkeiten geben, wobei die Dienste weiter in den Vordergrund rücken.

Er zeigte während seiner Ausführungen anhand einiger Beispiele, wie sich die administrativen Rollen in der Betaversion von Office 365 präsentieren. Office 365 sei nicht ein einzelner Dienst, den es ganz oder gar nicht gibt. Vielmehr plant Microsoft Abonnements im Mischbetrieb mit koexistierenden Infrastrukturen. So soll es beispielsweise möglich sein, dass der Exchange- oder SharePoint-Administrator mit seiner Konsole die Cloud-Infrastruktur und den lokalen Server gleichermaßen verwaltet. Die Enterprise Edition bietet sogar ein Zusammenspiel mit vorhandenem Active Directory.

Fazit

Ohne Zweifel war die IT&DevConnections eine Veranstaltung mit viel Mehrwert. Entwickler und Administratoren konnten sich mit Informationen eindecken, die es eben nur auf Konferenzen mit direktem Zugang zu den Referenten gibt. Da die IT&DevConnections eine kleine Veranstaltung mit familiärer Atmosphäre war, ermöglichte sie den Teilnehmern leichten Zugang zu den Experten. Es bleibt am Schluss nur zu wünschen, dass die Connections-Veranstalter wieder einmal mit einer ihrer Konferenzen in unserem Land zu Gast sind. *(dr)*

[1] Microsoft TechEd
B8A31

[2] TEC Konferenzwebseite
B8A32

[3] IT&DevConnections-Webseite
B8A33

Link-Codes

Im Test: VMware vCenter Operations 1.0

Mächtiges Kontrollorgan

von Jürgen Heyer

Der Betrieb einer virtuellen Infrastruktur erfordert ein geeignetes Verwaltungswerkzeug, das die typische Dynamik dieser Umgebungen bei der Überwachung von Performance, Konfiguration und Kapazität berücksichtigt. Während einige Drittanbieter schon länger auf diesem Gebiet unterwegs sind, hat nun auch VMware mit vCenter Operations ein eigenes Automatisierungstool veröffentlicht, um das Management einer virtuellen Cloud zu vereinfachen. IT-Administrator wollte wissen, wie es um den Leistungsumfang dieses brandneuen Produkts in der Version 1.0 bestellt ist.

Schon seit einiger Zeit bieten diverse Drittanbieter Werkzeuge für das detaillierte Monitoring einer Virtual Infrastructure (VI) unter VMware vSphere an. Gerade in größeren, produktiven Umgebungen mit vielen ESX-Servern und einigen hundert virtuellen Maschinen (VM) reichen die in vCenter integrierten Überwachungsmöglichkeiten nicht mehr aus. Eine Herausforderung dabei ist, dass die meisten Umgebungen nicht statisch sind, sondern kontinuierlich wachsen und sich entsprechend dem Cloud-Gedanken sehr dynamisch ändern. Dadurch ist eine ständige Überwachung immanent wichtig, um beispielsweise drohende Engpässe, aber auch ungenutzte Bereiche rechtzeitig zu erkennen. Engpässe sind insofern kritisch, da sich ein Problem in einer VI meist auf mehrere VMs und damit größere Bereiche der Produktion auswirkt. Aufgrund unpassender Konfiguration nicht optimal genutzte Ressourcen dagegen mindern die Effizienz.

Mit vCenter Operations hat VMware nun ein eigenes Produkt veröffentlicht, das sich nahtlos in eine vSphere-Landschaft mit vCenter integriert und einen tiefen Einblick in eine VI und in Cloud-Umgebungen ermöglicht. Das Tool liefert Leistungs-, Konfigurations- sowie Kapazitätsdaten und erstellt Analysen, um dem Administrator Anhaltspunkte für den Betrieb zu geben. vCenter Operations gibt es in drei Ausbaustufen: Die Version vCenter Operations Standard 1.0 ist für Umgebungen bis zu 1.500 VMs konzipiert. Die Advanced-Version, die wir uns im Test näher anschauen, ist ein Bundle aus der Standard-Variante und dem auch als eigenes Produkt erhältlichen CapacityIQ zur umfassenden Kapazitätsplanung und Trendanalyse. Die Enterprise-Version letztendlich beinhaltet zusätzlich ein proaktives Management, anpassbare Dashboards und Schnittstellen zu Monitoring-Produkten von Drittherstellern.

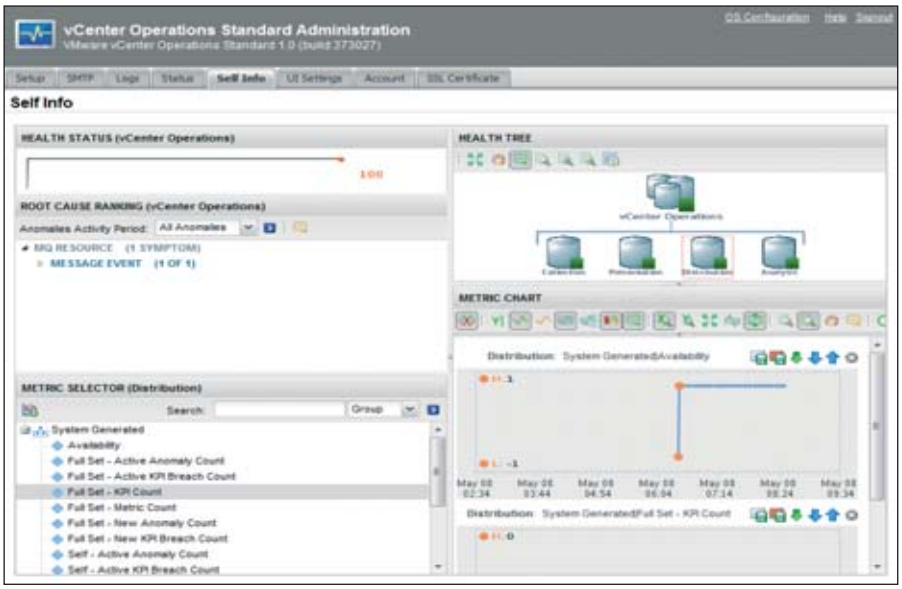


Bild 1: vCenter Operations besitzt eine Konsole für die Konfiguration und Überwachung

So gut wie installationsfreie Integration

vCenter Operations wird als vorkonfigurierte virtuelle Appliance geliefert, die das Betriebssystem sowie die Applikation fertig installiert enthält. Die Appliance basiert auf Suse Linux Enterprise Server 11 und benötigt zwei vCPUs, 8 GByte RAM und 124 GByte Plattenkapazität, wobei auch ein Thin-Provisioning möglich, wenn auch nicht empfohlen ist. Der Download ist knapp 700 MByte groß und wird als OVF-Vorlage direkt in vCenter importiert. An der vCenter-Konfiguration sind keinerlei Änderungen erforderlich. Beim ersten Start der Appliance holt sich diese per DHCP eine IP-Adresse und der Administrator kann sich über eine spezielle URL auf einer Administrationsseite anmelden. Das Wichtigste ist es, hier die IP-Adresse des vCenter-Servers und dessen Anmeldeinformationen anzugeben. Weiterhin kann der Administrator hier SMTP für Mailbenachrichtigungen aktivieren, die Log-Dateien der Appliance einsehen, ebenso deren eigenen Betriebszustand, und ein SSL-Zertifikat hochladen.

Anschließend ist über den vSphere-Client innerhalb von vCenter die Lizenz

zu aktivieren, dann ist vCenter Operations einsatzbereit. Der Zugriff erfolgt wahlweise direkt auf die Appliance über eine URL oder über ein Plug-In im vCenter, wo auf dessen Home-Ansicht unter "Lösungen und Anwendungen" ein entsprechendes Icon zu finden ist. Dass beim ersten Aufruf der Operations-Konsole kaum Objekte zu sehen beziehungsweise diese durchwegs gegraut sind, ist normal, denn es dauert eine gewisse Zeit, bis alle relevanten Objekte erfasst sind und erste Daten vorliegen. Um beispielsweise für Kapazitätsentwicklungen valide Werte zu erhalten, ist sogar ein zweiwöchiger Betrieb notwendig. Ansonsten sind die Aussagen noch zu unzuverlässig.

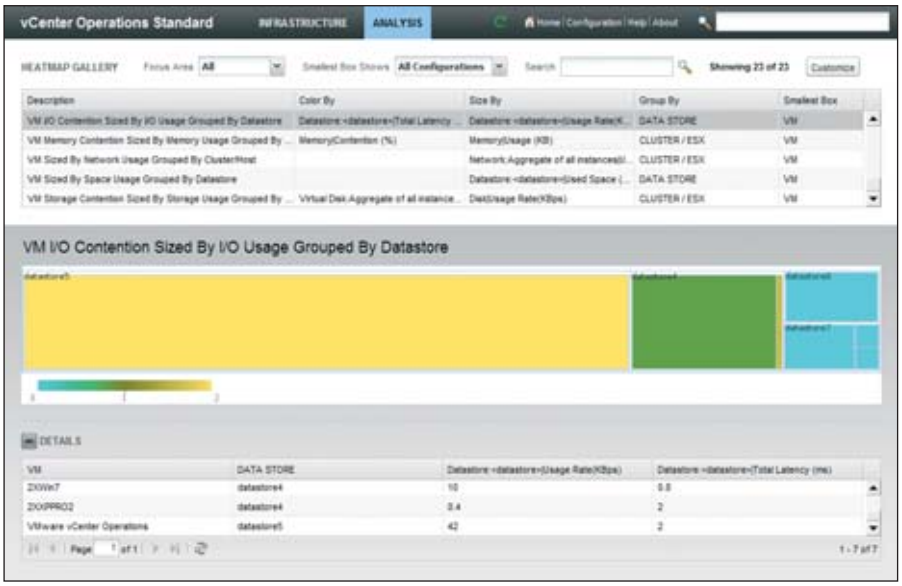


Bild 2: Die grafische Darstellung der Analysen ist recht gewöhnungsbedürftig und eher unübersichtlich

Dreigeteiltes Kennzahlensystem

Die Benutzeroberfläche von vCenter Operations erweist sich von Anfang an als sehr intuitiv bedienbar, auch wenn es sicher eine gewisse Zeit dauert, bis ein Administrator sie in vollem Umfang beherrscht und auch die Details schnell findet. Der Aufbau orientiert sich an den drei wesentlichen Messgrößen beziehungsweise Bewertungskriterien Auslastung (Workload), Kapazität (Capacity) und Gesundheit (Health) und stellt für jedes Kriterium eine eigene Ansicht bereit.

Jedem Kriterium ist ein eindeutiges Symbol (Zahnrad, Sechseck und Quadrat) zugeordnet und vCenter Operations bewertet jedes verwaltbare Objekt (vCenter, Datacenters, Clusters, ESXs und VMs) hinsichtlich der drei genannten Kriterien mit einer Kennzahl. Durch Anklicken eines dieser Symbole kann der Administrator die Ansicht umschalten. Die Kennzahlen innerhalb der Symbole, kombiniert mit den Farben grün, gelb, orange sowie rot, geben den aktuellen Status des betreffenden Objekts wieder und berücksichtigen dabei die vier wichtigsten Kenngrößen CPU, Arbeitsspeicher, Platten-I/O und Netzwerk-I/O.

Zur korrekten Interpretation der Zahlenwerte ist es allerdings erforderlich, das Handbuch zu lesen. Eine Auslastung (Workload) zwischen 0 und 100 steht für das Verhältnis der aktuell angeforderten Ressourcen zu den maximal möglichen. Beispielsweise bedeutet ein Wert von 100 bei der Speichernutzung, dass der Server den gesamten Arbeitsspeicher, der ihm zugewiesen ist, auch anfordert. Möglich sind aber auch Werte über 100, die bedeuten, dass das System hinsichtlich mindestens einer Kenngröße unter Volllast arbeitet und eigentlich noch weitere Ressourcen benötigen würde. Die Iconfarbe wechselt mit zunehmender Auslastung von grün über gelb nach orange und wird bei Erreichen des Wertes 100 rot. Dies verdeutlicht einen Engpass, der zumindest auf Dauer gesehen einer Analyse bedarf.

Der Aspekt Health dagegen ist umso besser, je höher die Kennzahl ist, die maximal auf 100 steigen kann. Sie sinkt, wenn bei einem Objekt irgendwelche Auffälligkeiten oder Fehlermeldungen auftreten. Bei der Kapazität bedeutet ein Wert von Null, dass eine oder mehrere der gemessenen Randbedingungen innerhalb der nächsten 30 Tage in einen Engpass laufen werden, ein Wert von 100 besagt, dass für das laufende Jahr kein Engpass zu erwarten ist. Gerade die Kapazitätsbewertung geht natürlich davon aus, dass sich die beobachtete Entwicklung in der Vergangenheit auch in der Zukunft kontinuierlich fortsetzt und keine unerwarteten Sprünge auftreten. Insofern benötigt die Interpretation der Zahlen zum einen etwas Erfahrung und zum anderen leitet sich daraus keine Garantie ab, dass alles genau so eintrifft.

Bei der Beurteilung einer VM oder eines ESX-Servers ist es wichtig, alle drei Werte im Zusammenhang zu sehen. Zeigt eine VM beispielsweise eine hohe Auslastung an, während der Health-Wert in Ordnung ist, so mag die aktuelle Last durchaus in Ordnung sein. Ist aber der Health-Wert gleichzeitig niedrig, so sollte zuerst geprüft werden, ob eventuell ein grundlegendes Problem vorliegt, das dann auch für die hohe Last verantwortlich ist.

vCenter Operations arbeitet für die Unterscheidung von normalen und kritischen Zuständen mit dynamischen Schwellenwerten (Dynamic Thresholds), die sich aufgrund der aktuellen und der in der Vergangenheit gemessenen Werte ergeben. Diese berücksichtigen regelmäßige Lastschwankungen, erzeugen aber einen Hinweis, wenn außergewöhnliche Lastsituationen auftreten. Manuelle Einstellungen sind hier nicht erforderlich, vielmehr ist dieser Prozess selbstlernend.

Systemvoraussetzungen

Für vCenter Operations Standard: Zwei vCPU ab 2,4 GHz, 8 GByte RAM, 124 GByte Festplatte für VMware vSphere 4.x.

Für vCenter Operations Advanced zusätzlich (= CapacityIQ): Zwei vCPU ab 2,4 GHz, 3,5 GByte RAM, 250 GByte Festplatte

VMware vCenter Operations Administrationsportal: Internet Explorer 7.0.x and 8.0.x, Mozilla Firefox ab 3.x, ESX-Hosts mit vSphere 4.0 U2 oder neuer.

Hierarchischer Aufbau als Basis

In der Hauptansicht sind alle verwalteten Objekte (vCenter, Datacenters, Clusters, ESXs und VMs) in einer hierarchischen Baumansicht mit ihrem Status in den Farben grün, gelb, orange und rot aufgelistet. Nicht berücksichtigt werden allerdings Ressourcenpools sowie vApps, die auch für alle nachfolgend beschriebenen Ansichten und Auswertungen nicht zur Verfügung stehen. In jeder Rubrik (Workload, Capacity und Health) ist nun jedes Objekt durch ein Symbol in der entsprechenden Statusfarbe, aber ohne eingeblendete Kennzahl vertreten. Welches Objekt sich hinter welchem Symbol verbirgt, eröffnet sich daher erst beim Darüberstreichen mit der Maus. Dann erscheint ein kleines Popup-Fenster mit dem System- oder Objektnamen und den drei Kenngrößen. Neben der Kennzahl der angewählten Rubrik ist auch dessen grober Verlauf als Kurve eingeblendet. Gerade am Anfang mag diese Ansicht sehr spartanisch erscheinen, sie ist dadurch aber auch für die gleichzeitige Darstellung sehr vieler Objekte geeignet und ergibt somit durchaus Sinn. Möglich ist eine Filterung entsprechend der Farben. Indem der Administrator beispielsweise alle grünen Symbole ausblendet, bleiben genau die Objekte übrig, die eines genaueren Blickes bedürfen. Eine Suche durch Eingabe des Namens ist aber auch möglich.

Streicht ein Administrator nicht nur über ein Objekt, sondern klickt es einmal an, erscheint ein Statusfenster, das auch geöffnet bleibt. Es zeigt wiederum die drei Rubriksymbole sowie deren Werte an und enthält weiterhin Links zu drei Registerblättern namens Detailansicht, Scoreboard und Metrik. Das am häufigsten genutzte, objektbezogene Fenster dürfte die Detailansicht sein. Diese öffnet sich auch beim Doppelklick auf ein Objekt. Dabei nutzt diese Ansicht immer das gleiche Layout, egal welches Kriterium den Administrator interessiert. Auch sind unabhängig von der Rubrik Teile der Ansicht immer identisch. Die Ansicht selbst teilt sich wiederum in mehrere Fensterbereiche, die auch bei einer hohen Auflösung wie beispielsweise 1.920x1.080 Pixel nicht allesamt zugleich dargestellt werden können. Gut ist hier, dass sich je nach Bedarf einzelne Abschnitte auf- und zuklappen lassen.

ALL-NET-FLAT

✓ FLAT FESTNETZ

✓ FLAT ALLE HANDY-NETZE

✓ FLAT INTERNET

29,99 ~~39,99~~ €/Monat*

connect Bestes Netz

In bester D-Netz-Qualität unbegrenzt ins gesamte deutsche Festnetz und in alle deutschen Handy-Netze telefonieren und mobil surfen. 24 Monate lang mit Ihrem Handy für 29,99 € anstatt 39,99 €/Monat. Oder mit einem kostenlosen Smartphone von 1&1 für 39,99 €/Monat.

1&1

Jetzt informieren und bestellen: 0 26 02 / 96 96

www.1und1.de

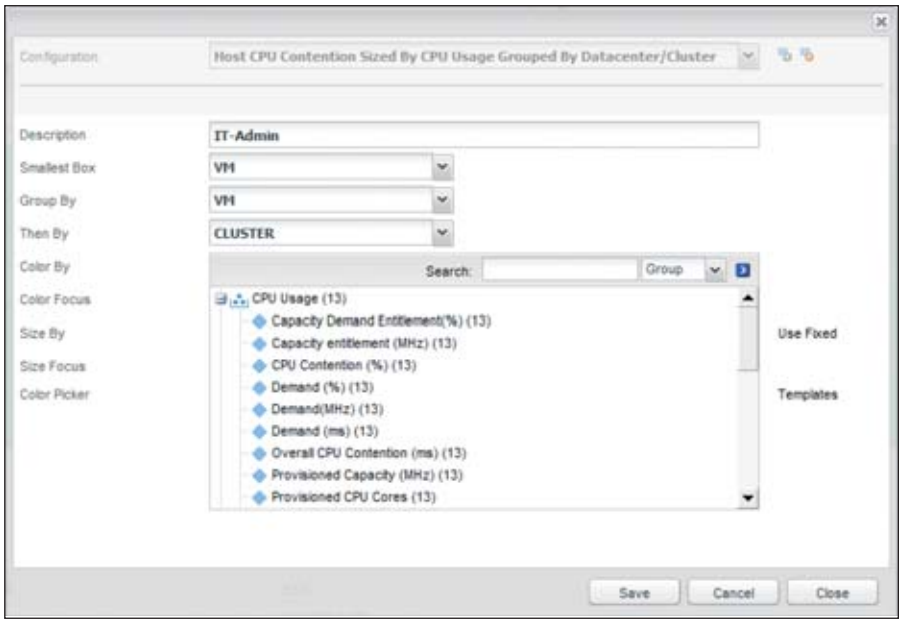


Bild 3: Das Erstellen von Analysen mit vCenter Operations erfordert nur wenige Mausklicks, die Gestaltungsmöglichkeiten sind allerdings begrenzt

Bewertungskriterien und Eckdaten im Blick

Immer gleich bleiben die beiden Bereiche links oben sowie im Fensterkopf. Hier findet der Administrator die drei Bewertungskriterien mit den Kennzahlen. Das Symbol der aktuell ausgewählten Rubrik ist dabei größer dargestellt. Darunter sind die Auslastungen der vier Kenngrößen dargestellt, weiterhin die wichtigsten Eckdaten des gewählten Objekts wie CPU-Anzahl sowie CPU- und Speicherkapazität. Das Fenster im Kopfbereich enthält die wichtigsten Kennkurven, wobei der Administrator den Fokus zwischen CPU, Speicher, Netz- und Festplatten-I/O ändern kann. Die dort sichtbaren Verlaufskurven vermitteln bereits einen groben Überblick. Indem der Administrator auf den zugehörigen Zahlenwert rechts neben der Kurve klickt, öffnet sich ein Detailfenster, das den Verlauf genauer darstellt und auch die Achsen aussagekräftiger beschriftet. Der Administrator kann innerhalb dieses Fensters die Kurve durch Wahl eines Ausschnitts oder eines vorgegebenen Zeitfensters vergrößern oder verkleinern. Das Fenster an sich besitzt eine feste Größe und ist unserer Meinung nach viel zu klein geraten. Es fällt schon schwer, überhaupt einen Ausschnitt zum Zoomen sicher auszuwählen, der dann wieder in das kleine Fenster gequetscht wird. Hier sollte VMware noch an der Darstellung feilen.

Alle Lastkurven sind nach einer gewissen Laufzeit von vCenter Operations mit einem dunkelgrauen Bereich hinterlegt. Dieser verdeutlicht die bereits erwähnten dynamischen Schwellenwerte. Es handelt sich letztendlich um den Bereich, in dem vCenter Operations die Ressourcennutzung oder -auslastung als normal ansieht. Aktuell bestehende Überschreitungen signalisiert ein zusätzliches kleines Symbol hinter der Kurve. Ebenso sind an den diversen Balkenanzeigen für den Workload blaue Klammern zu sehen, die den Normalbereich markieren. Bei neu in Betrieb genommenen Objekten werden die Schwellenwerte verständlicherweise erst nach einer gewissen Laufzeit eingeblendet, da das Programm erst einmal Vergleichswerte ermitteln muss.

Der Inhalt des Bereiches unterhalb des Kopffensters variiert entsprechend der gewählten Rubrik. Hier werden beispielsweise der aktuelle CPU- und Speicherverbrauch für das Objekt dargestellt, außerdem der Speicherverbrauch in Relation zum übergeordneten Objekt, so dass sich beispielsweise auf einen Blick herauslesen lässt, wie viel Speicher eine VM aktuell belegt und wie hoch dieser Wert aus Sicht des darunterliegenden ESX-Servers ist. Im Detail variieren die Inhalte etwas entsprechend dem gewählten Objekt. So ist bei einem ESX-Server die Hauptspeichernutzung durch die laufenden VMs als farbiger Balken dargestellt. Auch hier finden sich die blauen Klammern zur Markierung des normalen Betriebsbereichs.

Weiterhin zeigt vCenter Operations an, wo das aktuelle Objekt innerhalb der Gesamtstruktur angeordnet ist und wie der jeweilige Status der benachbarten sowie über- und untergeordneten Objekte ist (Parent, Peer und Child). Wird nun in einer der höheren Hierarchien ein Problem signalisiert, so kann der Administrator bereits dort die Detaildarstellung auswählen und sich dann durch Wahl des entsprechenden Child-Objekts zum eigentlichen Problemverursacher durchklicken. Nicht möglich ist es, aus vCenter Operations heraus die Konsolenansicht eines Servers oder einer VM zu öffnen, was den Zugriff für eine Analyse direkt am System vereinfachen würde. Hier muss der Administrator den vSphere-Client oder einen anderen Zugang wie RDP nutzen.

Zwei weniger wichtige Bereiche sind in der Detailansicht unten angehängt und normalerweise zugeklappt. Eine Ansicht stellt den Zusammenhang zwischen dem Status der gewählten Rubrik und den eingetretenen Ereignissen (Events) dar. Hier kann der Administrator herauslesen, welcher Event zu einer Statusänderung geführt hat. Die unterste Ansicht schließlich gibt Informationen zur Platten- und Netzwerknutzung preis. Es existieren Ansichten nach vDisks, Datastores und LUNs, beim Netzwerk wird nach Senden und Empfangen unterschieden, als Summe sowie nach vNICs getrennt.

Detaillierte Reports auf Wunsch

Das Registerblatt "Metrik" überschüttet den Administrator geradezu mit einer Vielzahl an grafischen Auswertungen. So stehen allein 14 CPU-bezogene Grafiken zur Auswahl, insgesamt sind es 54 Kurven. Angezeigt werden der Verlauf, eine Trendlinie sowie Minimal- und Maximalwerte, weiterhin gibt es diverse Gestaltungsmöglichkeiten hinsichtlich der Skalierung. Die Grafiken lassen sich als Schnappschuss im PNG-Format oder als CSV-Datei speichern. Neben den Grafiken ist auf dem Registerblatt Metrik noch der sogenannte Health Tree untergebracht. Von der hierarchischen Darstellung

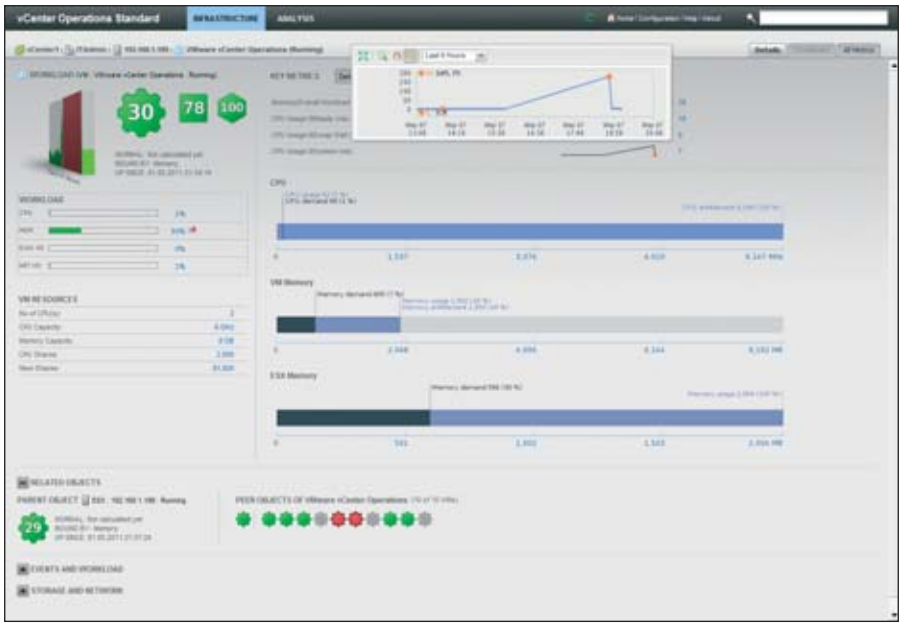


Bild 4: Die Konsolenansicht einer VM mit wenig Laufzeit liefert noch keine Schwellenwerte. Das Popup-Fenster zur Betrachtung eines der Lastverläufe besitzt eine feste Größe und ist recht klein geraten.

auf der Startseite unterscheidet sich dieser Baum in erster Linie dadurch, dass auch die Datastores mit eingeblendet sind. Außerdem sind durch eine andere Darstellung alle Objekte mit ihren Namen versehen.

Hinsichtlich einer Detailauswertung ist zu berücksichtigen, dass vCenter Operations die Werte im Fünfminutentakt mitschreibt – der möglichen Feinanalyse sind also Grenzen gesetzt. Zu beachten ist auch, dass Zeiträume, in denen die Appliance selbst nicht verfügbar war, nicht in allen Ansichten als Unterbrechung der Kurve dargestellt werden, sondern teilweise auch als Gerade zwischen dem letzten Messwert vor der Downtime und dem ersten Messwert nach dem erneuten Hochfahren. Auch Neustarts von VMs sind in der Regel nicht als Unterbrechung zu erkennen. Das lässt schon allein das fünfminütige Messintervall nicht zu. Recht gute Informationen bekommt der Administrator hierzu allerdings in der schon erwähnten Ansicht von Workload und Events. Die aufgetretenen Ereignisse hängen hier als blaue oder rote Kästchen an der Lastkurve. Beim Darüberstreichen erscheint ein Popup-Fenster mit genauen Informationen, hier sind also beispielsweise die typischen Meldungen bei einem Neustart herauslesbar.

Das dritte Registerblatt namens Scoreboard hilft bei der Suche nach über- und unterbeanspruchten Hosts und Clustern in der VI. Diese sind entsprechend der aktuell gewählten Rubrik mit ihrem Statuswert aufgeführt, wobei auch die Größe des Symbols diesen Wert abbildet. Hat der Administrator beispielsweise die Rubrik Auslastung gewählt und will er die Hosts vergleichen, so findet er die Hosts mit hoher Last weiter oben auf dem Scoreboard mit entsprechend großem Symbol, Hosts mit niedriger Auslastung rutschen weiter nach unten und haben ein kleineres Symbol. Im Gegensatz zur Startseite sind hier die Werte mit eingeblendet. Interessieren den Administrator mehr die Maschinen mit geringer Last, so kann er die Ansicht invertieren, so dass mit zunehmender Last das Symbol kleiner dargestellt wird.

Analyse mit vorbereiteten Abfragen

Neben der bisher beschriebenen Darstellung von Infrastrukturwerten besitzt vCenter Operations einen Analysebereich mit 23 vorbereiteten Abfragen, geordnet nach ESX, Datastore, VM und Cluster. Weitere Abfragen lassen sich leicht selbst generieren und auch speichern. Gewöhnungsbedürftig ist allerdings die Ergebnisdarstellung als farbige Blöcke unterschiedlicher Größe. Beispielsweise gibt es eine Auswertung anhand der Plattennutzung und Latenz für mehrere Datastores. Die Größe des Blocks gibt die Nutzung wieder, die Farbe steht

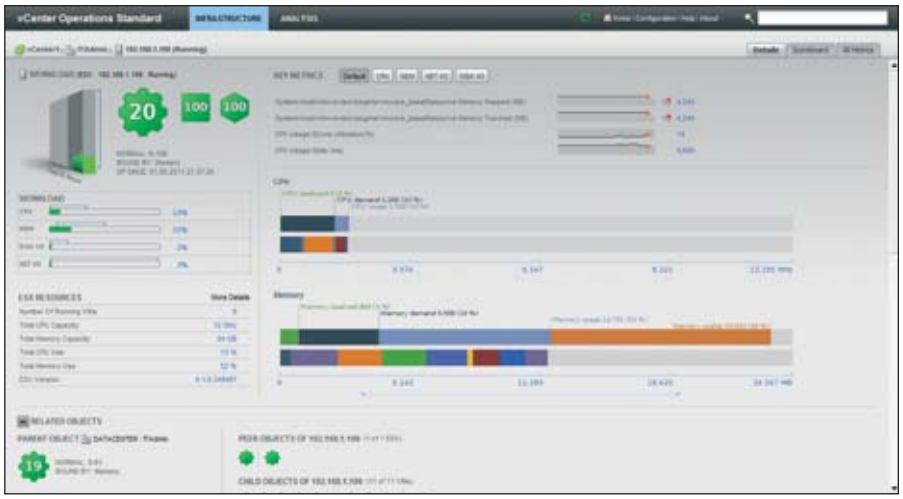


Bild 5: Die Standardansicht für ein Objekt liefert viele Informationen, an fast allen Balken sind blaue Klammern als Schwellenwertmarkierungen zu finden

für die Latenzzeit. Diese blockartige Darstellung ist sicher Geschmackssache, sie ist modern und wohl der Versuch, etwas Neues zu generieren. Uns hätten althergebrachte Balken- oder Kuchengrafiken besser gefallen, die Ansicht lässt sich aber nicht wählen. Leichter interpretierbar ist der unter der grafischen Darstellung angeordnete Detailbereich mit den entsprechenden Zahlenwerten. Über ein einfaches Konfigurationsfenster kann ein Administrator weitere Analysen definieren und speichern. Beim Anlegen eigener Analysen fiel uns auf, dass es nicht möglich ist, hier einen bestimmten Zeitpunkt oder Zeitraum anzugeben. Vielmehr handelt es sich immer um den aktuellen Status. Auch gibt es hier keinen Scheduler, mit dem sich Auswertungen regelmäßig erstellen lassen.

Um einen besseren Eindruck hinsichtlich der Aussagekraft von vCenter Operations zu bekommen, haben wir das Produkt eine Zeit lang in unserer Testumgebung mitlaufen lassen, während wir für andere Tests VMs klonten und mit diesen arbeiteten. Dabei ließ sich gut erkennen, dass am Anfang deutlich mehr Alarme und Schwellenwertüberschreitungen auftraten – begründet dadurch, dass es eine gewisse Zeit dauerte, bis sich die Werte eingependelt hatten. Auch haben wir die Erkenntnis gewonnen, dass es wenig Sinn macht, bei jedem orangen oder roten Symbol gleich in Aktionismus zu verfallen. Vielmehr empfiehlt es sich, das Problem in Ruhe anzugehen und beispielsweise bei einer VM auf das Gastbetriebssystem zu schauen, ob sich dort eine hohe Last auch bestätigt und negative Auswirkungen hat. So führte bei uns intensives Klonen regelmäßig zu hohen Lasten im Netzwerk, was aber letztendlich ignoriert werden konnte.

Kapazitätsplanung mit der Advanced-Version

Wie schon erwähnt, beinhaltet die Advanced-Version neben vCenter Operations Standard noch das Produkt CapacityIQ. Letzteres kommt ebenfalls als virtuelle Appliance fertig vorinstalliert. Der Download ist rund 500 MByte groß. Der Ressourcenbedarf zum Betrieb umfasst zwei vCPUs und 3,5 GByte Arbeitsspeicher. Für die Speicherung aller Messdaten werden immerhin 254 GByte Plattenkapazität reserviert. Auch hier ist Thin Provisioning möglich. Die Konfigurationsschritte zur Integration in das vCenter sowie zur Lizenzierung sind ähnlich wie bei vCenter Operations, der Aufruf erfolgt ebenfalls wahlweise im Webbrowser mit Angabe der IP-Adresse der Appliance oder dank eines Plug-Ins über den vSphere-Client.

Die Auswertungen von CapacityIQ leben von Messdaten über einen gewissen Zeitraum, so dass das Produkt mindestens zwei Wochen kontinuierlich laufen sollte, bis die gelieferten Trendanalysen valide sind und für Entscheidungen verwendet werden können. Abgesehen davon ist CapacityIQ nach der Inbetriebnahme ohne weitere Konfigurationsschritte nutzbar, da bereits praktikable Voreinstellungen für die Analysen hinterlegt sind. Diese sind in einem Konfigurationsbereich änderbar, es empfiehlt sich aber, hier erst mit entsprechender Erfahrung Anpassungen durchzuführen. CapacityIQ liefert wahlweise Ansichten oder vorbereitete Reports im PDF- und CSV-Format. Integriert ist auch ein Scheduler, der eine automatische Reporterstellung ermöglicht. Auswertungen können für das Datacenter, Cluster, ESX-Server oder VMs erstellt werden, Reports auf Basis von vApps oder Ressourcenpools sind nicht vorgesehen. Aus unserer Sicht besonders interessante Auswertungen sind das Wachstum der VMs allgemein sowie die Ermittlung unter- und überdimensionierter virtueller Maschinen, um so die Effizienz der Infrastruktur zu erhöhen.

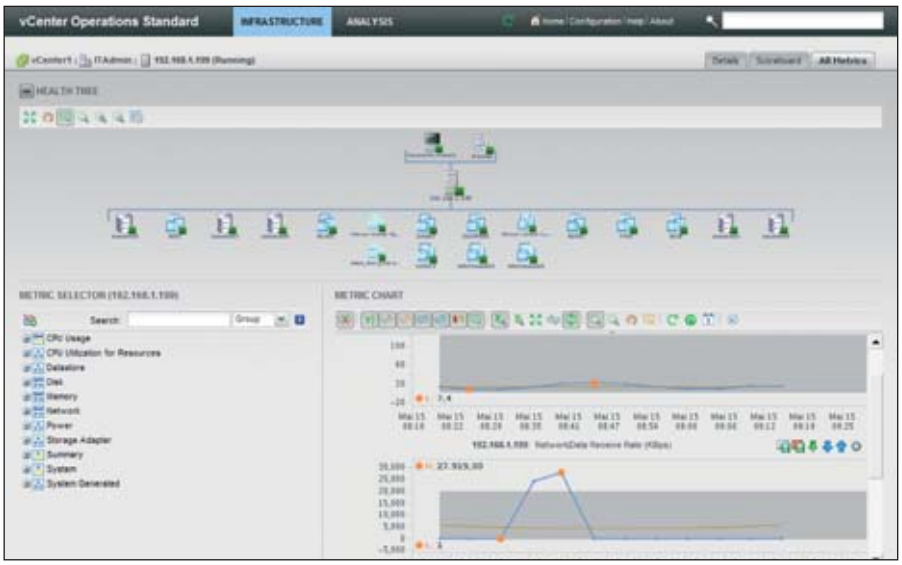


Bild 6: Aufgrund der Lastkurven ermittelt vCenter Operations sowohl dynamische Schwellenwerte (graue Unterlegung) als auch einen Trend (ockerfarbene Linie). Der Health Tree gibt die hierarchische Anordnung der Objekte wie VMs und Datastores in der VI wieder.

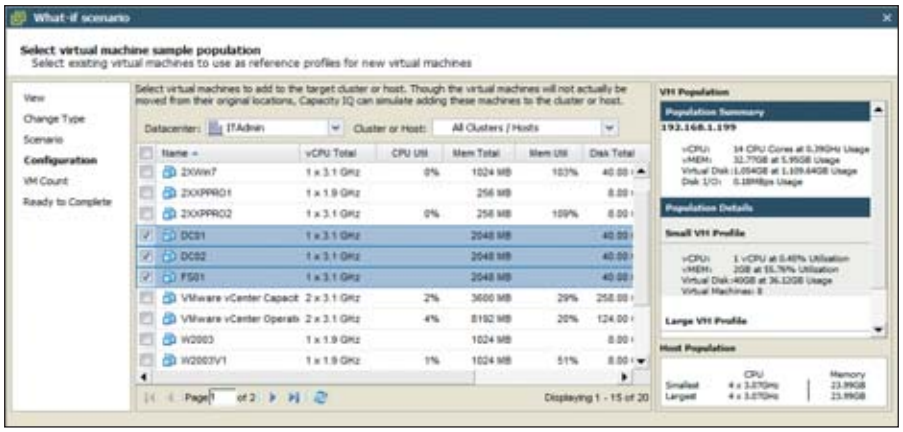


Bild 7: Für praxisnahe Zukunftsszenarien kann der Administrator Erweiterungen auch durch eine Vervielfachung eigener VMs planen

Nicht möglich ist allerdings eine Gruppierung für Auswertungen, um beispielsweise den Bedarf für eine Abteilung zu ermitteln. Auch ein Billing (Chargeback) ist nicht Bestandteil von vCenter Operations. Für Vorplanungen von Erweiterungen sind die integrierten "Was wäre wenn"-Analysen geeignet, die zwei Vorgehensweisen unterstützen. Entweder gibt der Administrator die Kennzahlen für geplante neue VMs direkt vor oder er geht den praxisnäheren Weg, indem er aus einer Liste der bereits vorhandenen VMs geeignete markiert unter der Annahme, dass eine bestimmte Anzahl derartiger Systeme hinzukommen soll. Das Ergebnis ist die voraussichtliche Entwicklung des Ressourcenbedarfs über die Zeitachse. Vermisst haben wir allerdings die Möglichkeit, die Lastkurven mehrerer VMs zu addieren und das Resultat dann den verfügbaren Ressourcen gegenüberzustellen. Es könnte ja sein, dass sich VMs mit sehr unterschiedlichem Lastverhalten auf einem ESX-Server betreiben lassen, solange die einzelnen Hochlastzeiten nicht zusammenfallen. Bei CapacityIQ ist leider nicht genau erkennbar, ob und wie das Programm so etwas berücksichtigt.

Fazit

VMware hat mit vCenter Operations in der Version 1.0 den ersten Wurf gelandet, um ein eigenes Monitoringwerkzeug anzubieten, anstatt dieses Geschäft ausschließlich diversen Drittanbietern zu überlassen. Das Produkt ist als virtuelle Appliance äußerst einfach in Betrieb zu nehmen, integriert sich vollständig in das vCenter und ist am besten über den vSphere-Client zu bedienen. Der Fokus der Standard-Version liegt auf Umgebungen mit bis zu 1.500 VMs. vCenter Operations liefert deutlich mehr Daten zur Last, Gesundheit und Kapazität der virtuellen Infrastruktur als das vCenter allein. Durch die Nutzung dynamischer Schwellenwerte, die kontinuierlich angepasst werden, sind kaum manuelle Anpassungen erforderlich, um normale und außergewöhnliche Lastsituationen unterscheiden zu können.

Unserer Meinung nach wird vCenter Operations aber erst mit der Advanced-Version richtig interessant, da dann mit CapacityIQ ein umfassendes Kapazitätsmanagement hinzukommt, das unter anderem zu klein und zu groß dimensionierte VMs ermittelt, generell die Trends der Umgebung hinsichtlich des Wachstums abbildet und auch "Was wäre wenn"- Analysen ermöglicht. Damit lassen sich geplante Erweiterungen hinsichtlich der Machbarkeit und eventuell erforderlicher Erweiterungen der ESX-Server im Vorfeld prüfen. Vermisst haben wir aber beispielsweise die Möglichkeit, mehrere VMs zu gruppieren, um deren Gesamtlastverhalten zu ermitteln. Die Bildung von vApps oder Ressourcenpools hilft auch nicht weiter, da diese Objekte bei den Auswertungen nicht berücksichtigt werden. Gewöhnungsbedürftig ist teilweise die Ergebnispräsentation, da VMware hier statt auf bewährte Balken- und Kuchendiagramme auf neue Darstellungsformen setzt.

Auch wenn vCenter Operations überaus einfach in Betrieb zu nehmen ist, so sollte ein Administrator den Einarbeitungsaufwand nicht unterschätzen, um die Resultate dann entsprechend nutzen zu können. Außer einigen Beispielen fehlt hier die umfassende Beschreibung.

Insgesamt hat uns vCenter Operations gut gefallen, der junge Entwicklungsstand macht sich allerdings noch bemerkbar und bietet unserer Meinung nach noch einigen Raum für diverse Optimierungen hinsichtlich Design und Funktionalität. Mit der weiteren Entwicklung werden sich die vorhandenen Kanten sicher noch abschleifen. Interessierte Administratoren können vCenter Operations in der Standard- und der Advanced-Version für 60 Tage testen. Da das Produkt nicht eingreift, sondern nur Informationen sammelt, ist ein Test in der produktiven Umgebung durchaus denkbar. *(dr)*

Produkt

Performance-Management einer Virtual Infrastructure unter vSphere.

Hersteller

VMware
www.vmware.com

Preis

vCenter Operations Standard für 25 VMs mit einem Jahr Basic-Support kostet rund 1.300 Euro, der Preis für das Advanced Bundle liegt bei 3.280 Euro

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Anzeige von Infrastrukturdaten	8
Analysemöglichkeiten	7
Ermittlung von Planzahlen	6
vCenter-Integration	9
Pflegeaufwand	9

Dieses Produkt eignet sich

optimal für sehr große Umgebungen, in denen sich auch der Einsatz der Advanced-Version rentiert.

bedingt für kleinere und mittlere Umgebungen. Je häufiger Änderungen an der virtuellen Infrastruktur erfolgen, desto interessanter wird der Einsatz.

nicht für (Virtualisierungs-) Umgebungen, die nicht auf vCenter setzen.

VMware vCenter Operations 1.0

Im Test: Entuity Eye Of The Storm 2010 NPE

Durchblick im Auge des Sturms

von Thomas Bär

Die Überwachung des Netzwerks und der wichtigsten Infrastrukturgeräte darin ist eine der zentralen Pflichtaufgaben des IT-Administrators. Glücklicherweise gibt es hierfür eine große Anzahl von Lösungen am Markt, die jedoch meist auch recht üppig und komplex ausfallen. "Eye Of The Storm 2010 NPE" vom US-amerikanischen Software-Hersteller Entuity darf mit Fug und Recht als ein kleines, aber professionelles Werkzeug angesehen werden, wie unser Test zeigt.

So unspektakulär Netzwerküberwachung zunächst aussehen mag, ist sie eine extrem wichtige Aufgabe. Veränderungen im Verhalten des Netzwerks können nur dann bemerkt werden, sofern der IT-Administrator ein Gefühl dafür hat, wie das normale Verhalten der gesamten Anlage aussieht. Der Ausfall von Komponenten sollte zudem nicht erst durch den Anruf eines aufgebrachten Benutzers auffallen. Besser ist dann schon die Antwort: "Ja, das Problem ist bereits bekannt, der zuständige Kollege arbeitet bereits daran." In diese Kerbe schlägt "Eye Of The Storm 2010 NPE", im Folgenden mit EYE NPE abgekürzt, als Überwachungssoftware für das Netzwerk.

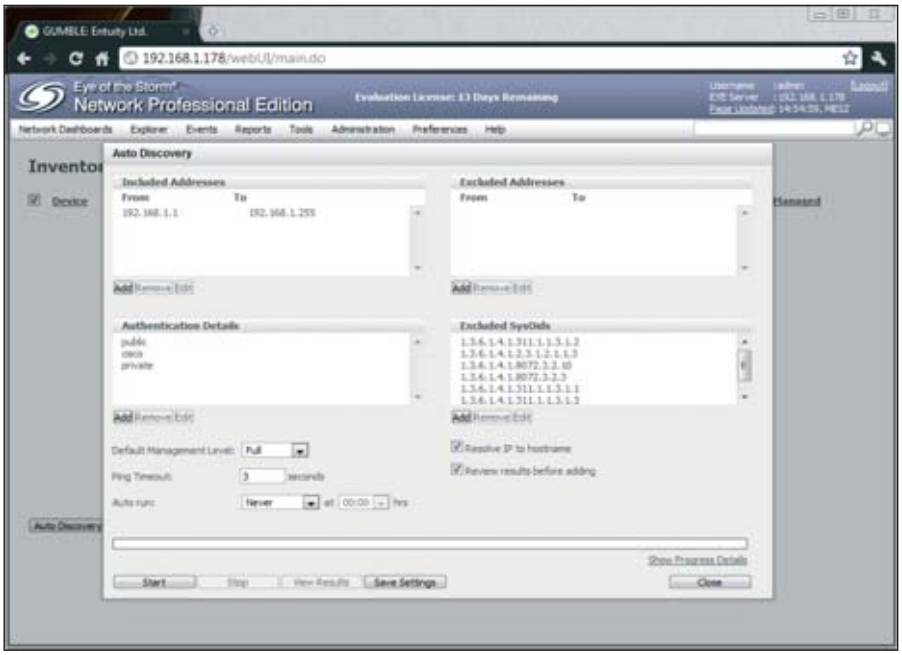


Bild 1: Die Suche nach Netzwerkgeräten, die per SNMP oder PING erreichbar sind, übernimmt Eye Of The Storm NPE weitgehend allein

Neben der reinen Prüfung der Erreichbarkeit von Geräten über ICMP-PING arbeitet EYE NPE über SNMP (siehe Kasten "Simple Network Management Protocol") mit detaillierten Informationen. Der Hersteller Entuity liefert EYE in zwei Ausprägungen: EYE Enterprise als komplette Netzwerkmanagementsoftware für große Umgebungen und EYE NPE als "Troubleshooting Tool" für eher kleinere Installationen. Die Enterprise-Edition bietet beispielsweise ein frei anpassbares Reporting, die SLA (Service Level Agreement)-Überwachung, Integration in BEM, Atrium, Remedy oder HP-Lösungen und analysiert die Routing-Protokolle BGP, EIGRP und OSPF. Die NPE-Edition beschränkt sich indes eher auf Umgebungen bis maximal 150 Geräte und bis zu 7.500 zu überwachende Objekte. Die Anzahl der verschiedenen Module, die sich bei Bedarf getrennt für die Enterprise-Version lizenzieren lassen, ist hoch. Die Module reichen von Cisco IP SLA, Cisco SSL Service, Blade Center, VPN Gateway, QoS Module, Wireless Controller, Power over Ethernet bis hin zu VMware ESX-Server. Hochverfügbarkeit (HA mit Failover) bleibt ebenfalls der Enterprise-Edition vorbehalten, ebenso die Verwendung auf Solaris-UNIX.

EYE ist eine webbasierte Software – anstelle einer zusätzlichen Management-Konsole verwendet der Administrator die Software beinahe ausschließlich über den Webbrowser. Hier unterstützt EYE alle gängigen Programme. Im Test arbeitete die Software mit dem Internet Explorer, Google Chrome und Apple Safari ohne erkennbare Schwierigkeiten. Mozilla Firefox in der jüngsten Version produzierte immer wieder das Phänomen, dass die Menüstruktur auf der linken Fensterseite plötzlich nicht mehr sichtbar war und erst nach einer erneuten Anmeldung wieder im Browser sichtbar wurde.

Installation in wenigen Minuten

Unsere Testinstallation haben wir auf einem Windows Server 2003 x86, virtualisiert unter VMware Workstation, durchgeführt. Der Maschine wiesen wir 1 GByte Arbeitsspeicher und eine CPU zu. Die Installation selbst war nach knapp 20 Minuten erledigt. Auch wenn die sehr detailliert beschriebene Installationsanweisung zunächst den Eindruck vermittelt,

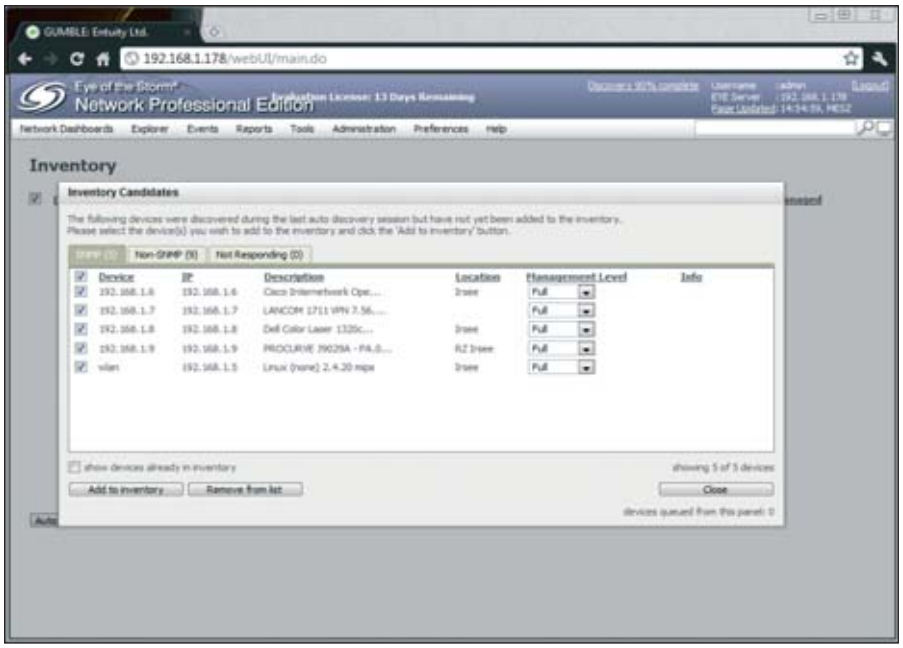


Bild 2: Die Suche nach aktiven Netzwerkkomponenten dauert in Abhängigkeit zur Netzwerkgröße einige Minuten bis Stunden

dass hier mit größeren Anpassungen und Konfigurationsschritten zu rechnen ist, so beschränkt sich der Installationsvorgang doch primär auf die Bestätigung der Vorschläge von Seiten des Installationsassistenten. Entuity EYE NPE läuft sowohl unter Windows als auch unter Unix/Linux auf jeder halbwegs aktuellen Standard-Hardware. Für den Betrieb in virtuellen VMware-Umgebungen ist das Produkt explizit freigegeben.

Alle benötigten Komponenten – eine MySQL Datenbank zur Speicherung der Informationen und einen Tomcat Webserver – installiert das Setup vollautomatisch. Zum Abschluss des Vorgangs gibt der Wizard noch einen Identifier aus, der die Installation eindeutig identifiziert und für die Erstellung einer Lizenzdatei durch den Hersteller von Interesse ist. In der 14-tägigen Testversion von EYE NPE ist durch den Anwender keine weitere Aktion erforderlich – die Testsoftware arbeitet den kompletten Testzeitraum ohne erkennbare Einschränkungen. Die einzige nennenswerte Auffälligkeit bei der Installation ist der Hinweis, dass in der Registry der Wert "MaxUserPort" auf den Wert 65534 erhöht werden soll. Aber auch ohne dass der Administrator diese Anweisung aus der ansonsten sehr genauen Installationsanweisung ausführt, endet der Vorgang mit dem Hinweis, dass der Installer eben diese Anpassung bereits vorgenommen hat. Hier scheinen Installer-Version und Handbuch in unterschiedlichen Ständen vorzuliegen.

Gemäß der Empfehlung des Herstellers soll EYE NPE auf einer dedizierten Maschine nicht zusammen mit anderen Ressourcen-intensiven Programmen eingerichtet werden. Weiter, so die Empfehlung, soll der Administrator automatisierte Update-Dienste deaktivieren, da diese sowohl die Verfügbarkeit als auch die Systemleistung negativ beeinflussen können. Da der EYE-Server insbesondere die Ping-Laufzeiten zu verschiedenen Systemen im Netzwerk protokolliert, muss sichergestellt sein, dass eine etwaige Verlangsamung nicht die Folge von Prozessen auf der EYE-Hardware ist. Das gilt insbesondere in Umgebungen, in denen EYE virtualisiert betrieben wird – möglicherweise ist ein Betrieb auf physikalischer Hardware im Zweifelsfall sinnvoller.

In den letzten Schritten der Installation muss der Administrator noch einen SMTP-Server für den Versand von automatisierten Alert-Meldungen und Reports festlegen und hat die Möglichkeit, einige weitere Parameter, wie beispielsweise die Kommunikations-Ports oder SSL-Verschlüsselung, festzulegen.

Verwaltung über den Browser

Wie erwähnt greifen IT-Mitarbeiter ausschließlich per Webbrowser auf EYE zu. Einzige Bedingung ist ein Java 6 Update 18 oder höher auf dem zugreifenden PC. Bei Bedarf startet EYE Java-Zusatzprogramme wie den "Component Viewer" oder den "Connectivity Viewer", der die logischen Verbindungen von Netzwerkgeräten grafisch darzustellen vermag. Laufen alle Dienste korrekt, erfolgt der Zugriff über die URL *http://{Name des EYE-Servers}*. Die Default-Credentials "admin / admin" kann und sollte der Administrator beim ersten Login im Menü unter "Administration / Account Management" ändern, um Unbefugten den Zugriff über Standardpasswörter zu nehmen. Dieser

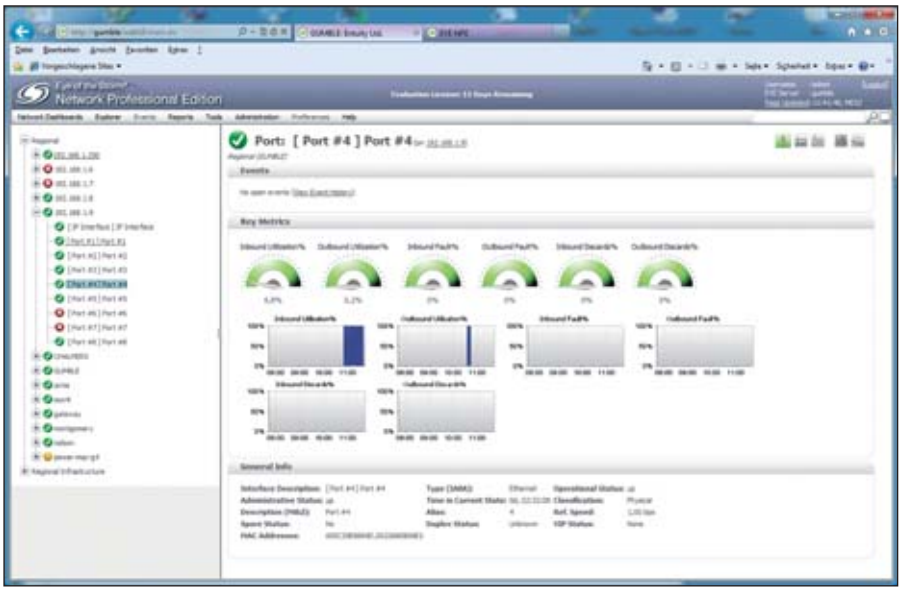


Bild 3: Grafische Übersichten zeigen dem Administrator auf einen Blick, wie es um die Geräte im Netzwerk steht

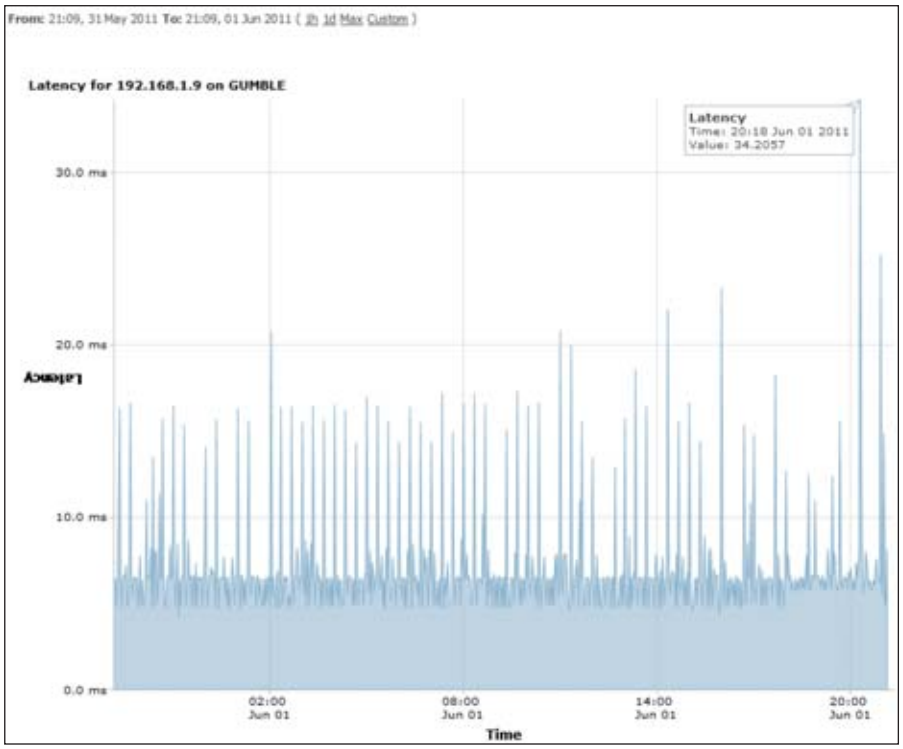


Bild 4: Auf Wunsch des Administrators geht EYE NPE auch grafisch bis tief in die Details – hier das rhythmische Auftreten von Latenzsteigerungen

Hinweis erfolgt leider nicht durch die Software. Hier haben wir schon andere Programme getestet, die den Administrator so lange mit Warnhinweisen nerven, bis dieser freiwillig ein neues Passwort festlegt.

Der erste wichtige Schritt für ein funktionelles Monitoring liegt darin, die gewünschten Geräte in die Software aufzunehmen. Glücklicherweise ist der Administrator hier nicht zur Handarbeit verdonnert, eine Suchfunktion unterstützt diesen Schritt. Typischerweise werden hierzu IP-Bereiche mit dem "Autodiscovery"-Befehl durchsucht. Die Suchfunktion verwendet einerseits die positive Reaktion auf einen ICMP-PING als Zeichen für die Existenz eines Geräts, andererseits versucht Entuity EYE NPE über SNMP-Community-Strings (siehe Kasten "Simple Network Management Protocol") weitere Informationen über das Zielgerät zu ermitteln.

- 2 GHz DualCore-Prozessor
- 4 GByte RAM
- 120 GByte Speicherplatz
- DVD-Laufwerk

Systemvoraussetzungen

Alle Geräte in unserer Testumgebung – diverse Switches und Router von HP und Cisco, Windows-Server, VPN-Gateways, ein FreeNAS und ein Dell-Netzwerkdrucker – wurden auf Anhieb entdeckt und in der Ergebnisliste angezeigt. Nicht alle Geräte, die der Scan zum Vorschein bringt, möchte der Administrator dabei in seiner regelmäßigen Überwachung finden. Client-Systeme, beispielsweise Mac- und Windows-Workstations, werden üblicherweise nicht in das Monitoring eingebunden, da deren Erreichbarkeit und Zuverlässigkeit kaum Aussagekraft haben. Anders sieht es indes aus, wenn auf einem Standard-Windows-PC unternehmenskritische Anwendungen, wie beispielsweise eine Schnittstellen- oder Kommunikationssoftware, aktiv sind. Zum Abschluss eines Suchvorgangs mit Entuity EYE NPE, der sich jederzeit wiederholen lässt, entscheidet der IT-Mitarbeiter, welche gefundenen Geräte überhaupt als "Managed Device" in die Überwachung aufgenommen werden sollen.

Ohne aktiviertes SNMP erscheinen Standard-Server mit Microsoft Windows als "Ping Only Device". Wie genau es um den Systemzustand bestellt ist, kann die Software somit nicht feststellen, da sie keine Kenntnis darüber hat. Die Windows Management Instrumentation (WMI) – die von Microsoft präferierte Methode, um Leistungs- und Messdaten abzufragen – unterstützt Entuity EYE NPE nicht. Da der Hersteller keinen Agenten für seine Software bietet und damit "agentless" arbeitet, bleibt nur SNMP zur Leistungsüberwachung.

Kleines Inventar, große Messdaten

Die automatische oder manuell angestoßene Erkennung von Geräten für das Monitoring darf nicht mit einer echten Inventarisierungslösung verwechselt werden. Dennoch sammelt die Software die wichtigsten Eckdaten, die für die Bearbeitung von Problemen nützlich sind. Eine FreeNAS-iSCSI-Maschine auf Basis eines Intel Celeron 800 MHz-Rechners von Fujitsu-Siemens mutierte in unserem Test jedoch zu einem Gerät des Herstellers "Fraunhofer FOKUS", Modell "i386" ohne "Serial Number". Aus der System-Description kann der Administrator die wichtigsten Details ablesen: "Hardware: i386 Intel Celeron running at 795 Software: FreeBSD 7.3-RELEASE (revision 199506)".

Zu jeder Netzwerkkarte im System wird die tatsächliche Netzwerkgeschwindigkeit in MBps, die MAC-Adresse, IP-Informa-

Die Geschichte von SNMP geht auf das Jahr 1988 mit dessen Vorstellung als Ersatz für den RFC 1067 zurück. Mit SNMP schaffte die IETF (Internet Engineering Task Force) eine Grundlage für das herstellerübergreifende Management von Netzwerkinfrastrukturgeräten wie Router, Server, Switches oder Drucker. SNMP basiert auf UDP und gilt bis zur Version 3 als insgesamt unsicher, da es über keinerlei Sicherheitsfunktionen verfügt.

Zwar ist die im Dezember 2002 vorgestellte Version 3 (RFC 3410 bis RFC 3418) sicher gegen unerwünschten Missbrauch, konnte sich bisher aufgrund der gestiegenen Komplexität, beispielsweise der Schlüsselverwaltung, immer noch nicht durchsetzen. Faktisch verwenden heutige Geräte immer noch SNMP v1 und v2c. Anstelle von Benutzernamen und Passwörtern verwendet SNMP bis v2c so genannte "Communities". Hierbei handelt es sich um einfache Bezeichner wie "public", "private" oder "cisco". Da die SNMP-Kommunikation unverschlüsselt stattfindet, darf die Community-Bezeichnung eher als Zuordnung denn als Passwort gesehen werden. Weitere Infos finden sich unter [1].

Simple Network Management Protocol

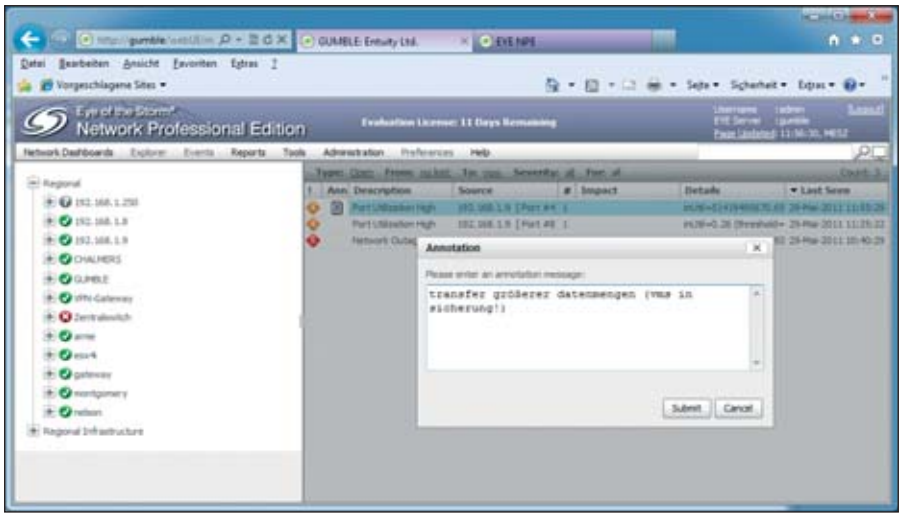


Bild 5: Äußerst praktisch, besonders wenn mehrere IT-Supporter gemeinsam mit dem System arbeiten: Die Möglichkeit, kurze Textnachrichten zu Ereignissen zu verfassen

tionen mit Subnetzmaske und gut ein Dutzend weiterer Detailinfos gespeichert. Die typischen Informationen aus der SNMP-Welt wie "Location", "System Contact", "System Name" und "Last Reboot Time" sind ebenfalls zu finden.

Wichtiger als die reine Auflistung der Eckdaten sind jedoch die über den Messzeitraum gewonnenen Informationen zur Auslastung. Bei der Free-NAS-Maschine sind das beispielsweise die durchschnittliche "Inbound Utilization", "Outbound Utilization", "ICMP Reachable Known%" und die Verfügbarkeitswerte in Stunden. Logischerweise ist die Informationsdichte bei Aktivkomponenten, beispielsweise einem Cisco Catalyst oder HP ProCurve Switch, höher. Pro Interface ermittelt die Software genaue Daten bezüglich der Auslastung oder des Durchsatzes an Netzwerkpaketen. Leider fehlt eine Suchfunktion in der Software, die es dem Administrator erleichtert, beispielsweise gezielt nach einer MAC-Adresse und deren Werte zu suchen.

Wie zu erwarten, bietet EYE NPE auch die Möglichkeit, die regelmäßige Überwachung spezifisch auf unterschiedlichen Ports durchzuführen. Typische Applikationen, wie SMTP-Mailversand oder HTTP-Web-Dienste auf Port 80, kann der Administrator so detaillierter überwachen. Die Applikations-Überwachung von EYE NPE beschränkt sich jedoch auf die Prüfung einer zu hohen Latenzzeit. In der Standard-Einstellung gönnt die Software einem Dienst eine Reaktionszeit von 3.000 ms – wird dieser Zeitraum überschritten, so wird ein Event ausgelöst. Spezielle Prüfungen, beispielsweise dass sich ein Mailserver in einer gewissen, zu erwartenden Art und Weise auf einem Port melden soll, können mit EYE NPE nicht vorgenommen werden.

Bei den Benachrichtigungen setzt die Software einzig auf den Versand von E-Mails. In den "Preferences" von EYE NPE kann der Administrator festlegen, in welchen Zeiträumen welche Personen bei welchem Ereignisgrad per E-Mail kontaktiert werden. Die Möglichkeiten beschränken sich hier auf die Festlegung von Wochentagen und Uhrzeiten – Urlaubszeiten oder SLA-Vereinbarungen sind über dieses Fenster nicht abzubilden.

Grafisch oder als Report

Die Möglichkeiten von Eye NPE für die grafische Auswertung oder die Erstellung von Reports sind nicht gerade überwältigend. Individuelle Anpassungen bleiben, wie eingangs bereits beschrieben, der größeren Produktversion vorbehalten. Dennoch kann der Administrator mit der Software problemlos verschiedene Geräte unter "Device Metrics" miteinander vergleichen. Welche Geräte berücksichtigt werden sollen, welche Zeitperiode (zwischen einer und 48 Stunden) und welche vier Datenreihen – von der Latenz, Verfügbarkeit bis hin zur CPU- und Speicherauslastung – verglichen werden sollen, klickt der Administrator einfach zusammen.

Bei den Reports bietet EYE NPE die Übersichten der Hersteller, Gerätetypen, VLAN-Konfigurationen oder die Aufstellung von IOS-Konfigurationen. Die Übersicht wird typischerweise als Kuchengrafik mit Prozentverteilung visualisiert und lässt sich mit einem Mausklick im PDF-, Excel-, CSV- oder Word-Format exportieren. Ein Drilldown von der Grafik hin zur Detailübersicht bietet die Software nicht.

Fazit

Eye Of The Storm NPE von Entuity ist eine schlanke, dennoch leistungsstarke und moderne Software. Wer sich schon mit anderen Monitoring-Lösungen auseinandergesetzt hat, findet sich schnell zurecht. Die Suchfunktion für Geräte arbeitet rasch und zuverlässig. Veränderungen in der Auslastung des Netzwerks identifiziert die Software weitgehend automatisch. Die Möglichkeit, zu jedem Event eine kurze Nachricht anlegen zu können, macht Sinn. Besonders gut gefiel uns im Test die Fähigkeit der Software, für jeden "Event"-Typ (hiervon bietet EYE NPE knapp 140) explizit festlegen zu können, nach wie vielen Sekunden das Ereignis nicht mehr von Interesse ist – das so genannte "Age Out".

Im direkten Vergleich zu anderen Lösungen am Markt – sei es Nagios, Whats Up Gold von Ipswitch oder "theGuard" von Realtech – sind die Möglichkeiten, die EYE in der Version NPE bietet, jedoch deutlich limitiert. Eine typische Root-Cause-Analyse, wie sie "theGuard" erlaubt, ist mit EYE NPE nicht so leicht, unter Umständen auch gar nicht umzusetzen.

Detaillierte Überwachungsmodule, wie sie Whats Up Gold für Microsoft SQL-Server oder Microsoft Exchange mitbringt, sind mit EYE NPE ebenfalls nicht realisierbar. Hier beschränkt sich die Software auf die Reaktion eines Dienstes, ohne die detaillierten WMI-Informationen auszuwerten. Auch wenn dieser Vergleich etwas hart ausfallen mag – geht es nur darum, die Verfügbarkeit von Geräten und Applikationen anhand von ICMP-PING und SNMP zu überwachen, so gibt EYE NPE ein recht gutes Bild ab. *(dr)*

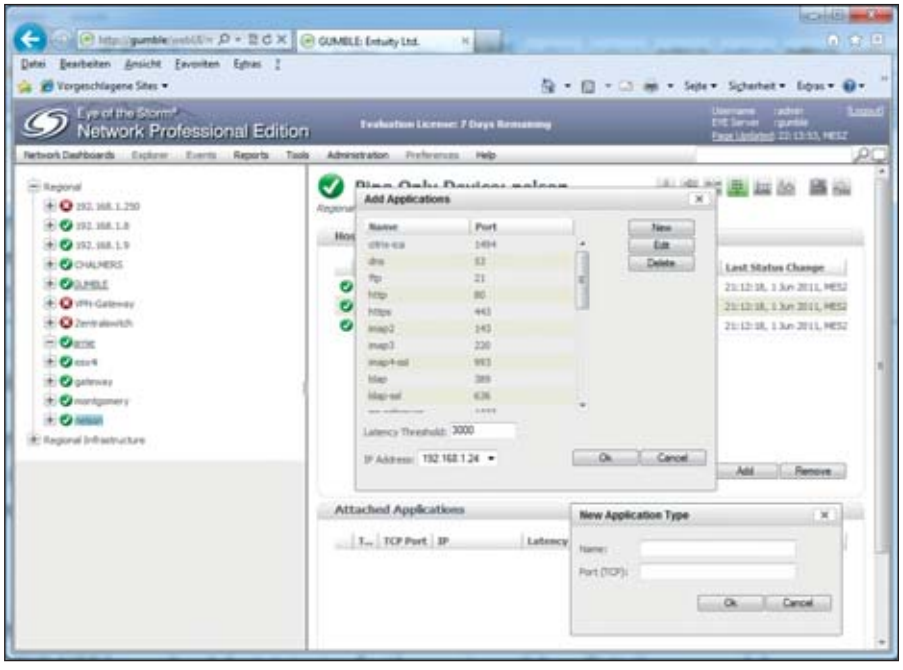


Bild 6: Die Überwachung von Applikationen beschränkt sich auf die Latenzmessung auf Port-Basis

Produkt
Software zur Überwachung von Netzwerkkomponenten und -verkehr.

Hersteller
Entuity
www.entuity.com

Preis
17.500 Euro

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

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

Flexibilität	8
Überwachung	6
Applikationsmonitoring	6
Benachrichtigungen	5
Installation	8

Dieses Produkt eignet sich

optimal für Unternehmen, die in großen Umgebungen verschiedenste Geräte und Applikationen zentral überwachen müssen.

bedingt für Unternehmen, die nur sehr wenig Kenntnis über Aktivkomponenten und SNMP besitzen.

nicht für Unternehmen, die kein Monitoring benötigen.

Entuity Eye Of The Storm NPE 2010

SNMP-Webseite
B8T21

Link-Codes

Im Test: Quest OnDemand Recovery for Active Directory

Online-Backup für das Active Directory

von Jürgen Heyer

Das Online-Backup von Arbeitsdaten auf Speicherpools im Internet hat sich schon seit längerem etabliert. Jetzt bietet Quest einen vergleichbaren Dienst für die Sicherung des Microsoft Active Directory an. Schützen lassen sich einzelne Domänen, aber auch ganze Forests. Abgerechnet wird monatlich anhand der gesicherten Benutzerobjekte. IT-Administrator wollte wissen, ob dies tatsächlich so einfach und zuverlässig funktioniert, wie es auf den ersten Blick erscheint.

Windows Server 2008 R2 erlaubt erstmals, im Active Directory gelöschte Objekte wiederherzustellen. Allerdings ist die Vorgehensweise nicht ganz trivial und greift auch nur, wenn ein Objekt tatsächlich gelöscht wurde. Das Zurücknehmen von Änderungen bei noch vorhandenen Objekten ist nicht vorgesehen. Seit kurzer Zeit bietet Quest mit OnDemand Recovery for Active Directory (ODR) einen Dienst an, um das Active Directory automatisch via Internet zu sichern und neben dem kompletten Wiederherstellen gelöschter Objekte auch Änderungen wieder auf einen früheren Stand zurückzusetzen. ODR arbeitet genauso wie ein Online-Backup-Dienst für Daten und wird nach Aufwand abgerechnet, wobei als Kriterium die gesicherten Benutzer-Accounts in der Domäne herangezogen werden.

Das Online-Backup-Verfahren hat grundlegende Vor- und Nachteile, die bekannt sein sollten, wenn eine Entscheidung dafür oder dagegen ansteht. Vorteile sind, dass nur die in Anspruch genommene Leistung zu bezahlen ist und die Lösung kontinuierlich wachsen, aber auch schrumpfen kann. Außerdem muss in keinen aufwändigen Backup-Prozess investiert werden, der zudem noch zu administrieren ist. Dadurch, dass sich die Ablage der gesicherten Informationen außerhalb des Unternehmensstandortes befindet, bietet die Sicherung auch einen Katastrophenschutz.

Bild 1: Über bis zu vier Sicherungen pro Tag werden auch mehrere Änderungen an den Objekten in kürzerer Zeit erfasst

Letztendlich birgt aber eben die Tatsache, dass die Daten außerhalb des Unternehmens im Internet gesichert werden, auch einen gewissen Nachteil, denn sie verlassen das Unternehmen und die Kontrolle des Administrators. Letzten Endes muss er dem Provider vertrauen, dass die Daten sicher verwahrt werden.

ODR ist erst seit kurzem auf dem Markt und war zum Testzeitpunkt in der Version 1.3.1 verfügbar. Dass es sich hier um ein noch sehr junges Produkt handelt, machte sich an einigen Stellen bemerkbar. Aufgrund schwerer Bugs in einer noch früheren Version hatten wir den Test sogar etwas verschieben müssen (siehe Kasten "Manche Software reift beim Kunden").

Installation im Handumdrehen

Aufgrund der Funktionsweise als Online-Produkt reduziert sich die Installation auf wenige Schritte. Zuerst ist eine Registrierung bei Quest erforderlich, um einen Account als Basis für den Sicherungspool anzulegen. Anschließend erhält der Administrator einen Link auf eine URL mit einem Installationsassistenten. Der Assistent veranlasst die Installation eines rund fünf MByte großen Agenten auf einem Server in der zu sichernden Domäne. Der gewählte Server muss unter Windows Server 2003 (R2) oder 2008 (R2), wahlweise 32 oder 64 Bit, laufen. Es muss sich nicht um einen Domänencontroller handeln, sondern kann ein beliebiger Server in der Domäne sein. Der Assistent fragt einen

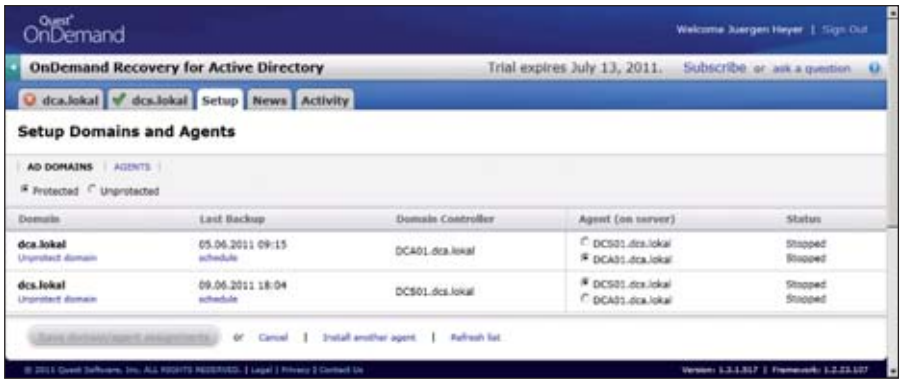


Bild 2: Über einen Account bei Quest lassen sich die Informationen von mehreren Domänen bis hin zu ganzen Forests sichern

Account mit Administratorrechten ab, der für alle Backup- und Restoreoperationen verwendet wird. Außerdem muss der Administrator die Domäne bestätigen und den Domänencontroller auswählen, auf dem letzten Endes der Zugriff erfolgt. Die Verteilung der FSMO-Rollen bei mehreren Domänencontrollern spielt dabei keine Rolle, hier muss nichts berücksichtigt werden.

Zuletzt fragt der Assistent die täglichen Backup-Zeiten ab, wobei bis zu vier Sicherungen pro Tag möglich sind, die der Administrator zeitlich nach Belieben verteilen kann. Indem er einzelne Termine deaktiviert, kann er die Anzahl der täglichen Backups auch reduzieren. Abschließend startet der Assistent die erste Sicherung oder lässt die Möglichkeit zu, mit dem nächsten Termin aus dem Zeitplaner zu beginnen. Zu beachten ist, dass sich ODR nicht an der lokalen Zeit orientiert. Im Test beobachteten wir einen Zeitversatz von zwei Stunden, und unsere Vermutung, dass der Dienst wegen des weltweiten Angebots mit UTC (Coordinated Universal Time) arbeitet, wurde vom Support bestätigt. Soll beispielsweise hierzulande um 12 Uhr mittags gesichert werden, ist 10 Uhr einzugeben. ODR sichert das AD im laufenden Betrieb, wobei die Verfügbarkeit nicht beeinträchtigt wird. Die Sicherung erfolgt außer beim allerersten Backup grundsätzlich inkrementell, so dass immer nur die Änderungen seit der letzten Sicherung übertragen werden müssen.

Server unter Microsoft Windows Server 2003 (R2) oder Microsoft Windows Server 2008 (R2), 32 oder 64 Bit, Mitglied in jeder zu sichernden Domäne eines AD-Forest, Internet-Zugang

Systemvoraussetzungen

Ist die Installation abgeschlossen, befindet sich der Administrator auf einem Webportal als Konsole von ODR. Wie bereits erwähnt, lässt sich über einen Account auch ein Forest mit mehreren Domänen sichern. Da die Abrechnung anhand der gesicherten Benutzer erfolgt, spielt es letzten Endes keine Rolle, auf wie viele Domänen sich die Benutzerkonten verteilen. Neben den Benutzern übernimmt ODR auch die Sicherung und Wiederherstellung der übrigen AD-Objekte wie Computer, Kontakte, Gruppen, Freigaben und OUs sowie den Objekttyp InetOrgPerson. Um wie viele Objekte es sich hier handelt, spielt für die Abrechnung keine Rolle.

Eine automatische Update-Prüfung kümmert sich um die Aktualität des Agenten. Ist das Webportal geöffnet, zeigt es deutlich sichtbar an, dass ein Update verfügbar ist. Es ist zu empfehlen, die Updates möglichst schnell zu installieren, denn im Test waren mit veraltetem Agenten keine Sicherungen mehr möglich, nur noch Wiederherstellungen. Während des Tests hatten wir allerdings einige Male das Problem, dass ein Update nicht klappen wollte, da meist noch Dateien in Benutzung waren, die ausgetauscht werden mussten. Indem wir den ODR-Dienst anhielten und das System neu starteten, klappte es dann meist doch. Einmal aber waren auf einem Server plötzlich zwei Agentenversionen gleichzeitig installiert und alle Deinstallationsversuche waren umsonst. Diesbezüglich ist es sehr zu empfehlen, den Agenten auf keinen Fall direkt auf dem Domänencontroller zu installieren, sondern auf einem anderen, eventuell weniger wichtigen System. Geeignet ist auch eine virtuelle Maschine, denn die Performanceanforderungen sind nicht sonderlich hoch. Dann lässt sich in so einem Fall die VM relativ einfach gegen eine andere mit neu installiertem Agenten austauschen.

Restore auf Knopfdruck

Die Bedienung von ODR über das Webportal erwies sich als überaus einfach. Wir sahen in einer Übersicht die vergangenen Sicherungen und konnten auf Knopfdruck unabhängig vom Zeitplaner jederzeit eine neue Sicherung starten. Für eine schnelle Prüfung ist hinter jedem erfolgreichen Backup ein "Compare"-Button zu finden, mit dem sich die gesicherten Objekte mit denen im AD vergleichen lassen und Änderungen sofort erkennbar sind. Zu beachten ist hier, dass seit der Sicherung neu hin-

Als wir mit dem Test von ODR begannen, waren wir guter Dinge, denn die Funktionsweise des Produkts erschien übersichtlich und sollte auch gut abzuschätzen sein. Bei Quest auf der Webseite waren zudem bereits Erfahrungsberichte zu lesen, die das Produkt umfassend lobten. Umso überraschter waren wir, dass unsere ersten Tests absolut enttäuschend verliefen. Allgemeine Informationen und die Adresse von Benutzern wurden bei Veränderungen wiederhergestellt, aber keinerlei Konto-Optionen. Geradezu katastrophal war auch das Verhalten beim Umgang mit Gruppen. Wurde die Anzahl der Mitglieder einer Gruppe geändert und anschließend ein älterer Stand wieder eingespielt, so hatte die Gruppe anschließend keinerlei Mitglieder mehr. Hier wurde mehr zerstört als repariert.

Als wir unseren deutschen Ansprechpartner beim Hersteller mit unseren Beobachtungen konfrontierten, konnte dieser das Verhalten prompt nachvollziehen. Auf seine Nachfrage in der Entwicklung stellte er uns für etwa eine Woche später eine überarbeitete Version in Aussicht, die auch tatsächlich nach rund zwei Wochen online war, so dass wir unsere Testsysteme über den integrierten Updateprozess aktualisieren konnten.

Tatsächlich waren die oben genannten gravierenden Fehler beseitigt, so dass wir uns entschlossen, den Test durchzuführen. Letztendlich aber stellte sich bei uns schon die Frage, wie ein derart fehlerhaftes Produkt überhaupt die Freigabe bekommt, um offiziell angeboten zu werden. Dass die von uns gefundenen, offensichtlichen Fehler bei der Qualitätsprüfung durchgerutscht sind, ist kaum vorstellbar. Hier fiel uns der Begriff der "Bananensoftware" ein: Software, die erst beim Kunden reift.

Manche Software reift beim Kunden

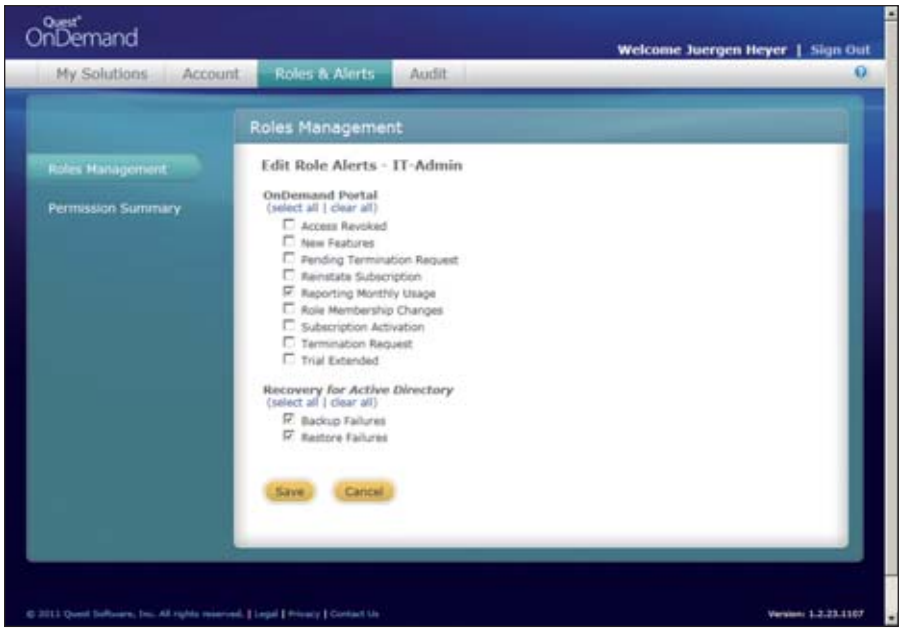


Bild 3: Über ein Rollenkonzept können verschiedene Benutzer individuelle Rechte erhalten, außerdem wird hier die E-Mailbenachrichtigung konfiguriert

zugekommene Objekte nicht berücksichtigt werden. Der Administrator kann also immer nur Änderungen oder Löschungen von bereits gesicherten Objekten erkennen. Wurde ein Objekt bereits vor einiger Zeit gelöscht, und der Administrator will es wiederherstellen, so muss er die Sicherungen soweit zurückverfolgen, bis er das Objekt gefunden hat und kann dann daraus den Restore starten. Wenn also keine Informationen zum genauen Löschzeitpunkt vorliegen, kann diese Suche etwas dauern.

Für einen genaueren Test legten wir in unserer Beispieldomäne gezielt einige Objekte wie Benutzer, Gruppen und auch Computer an, definierten Gruppenzugehörigkeiten, sicherten diese Konstellation und verglichen dann zunächst die Sicherung mit dem Stand des AD, wobei sich erwartungsgemäß keine Unterschiede ergaben. Anschließend änderten wir gezielt diverse Einstellungen, notierten uns diese und starteten einen erneuten Vergleich. Nun zeigte uns ODR die ermittelten Abweichungen an und eröffnete die Möglichkeit, diese anhand der Sicherung wieder auf den alten Stand zurückzusetzen. Dazu ließen sich die Objekte einzeln oder auch alle Differenzen auf einmal markieren. Nach dem Restore starteten wir einen erneuten Vergleich, um zu prüfen, ob die Änderungen tatsächlich rückgängig gemacht wurden. Hierbei fiel uns auf, dass manchmal noch einige Differenzen übrig blieben, wofür es aber durchaus Erklärungen gibt wie geänderte Zeitstempel oder Zähler, die durch einen Restore zurückgesetzt werden. Beispielsweise betraf das den Inhalt der Attribute badpwdcount, logoncount und lastlogon. Die Bewertung, ob diese Unterschiede in Ordnung sind, verlangt etwas Erfahrung. Diese ist auch insofern erforderlich, da ODR die in Windows genutzten Attributbezeichnungen wiedergibt, die nicht in jedem Fall auf Anhieb verständlich sind.

Weiterhin fiel uns auf, dass ODR beim Rücksetzen von Objekten einzelne, zum Sicherungszeitpunkt nicht gesetzte Attribute bei einem Restore nicht berücksichtigte, wenn zwischenzeitlich etwas eingetragen worden war. Ein Beispiel: Nach dem Backup trägt der Administrator bei einem Benutzeraccount in die leeren Adressfelder die entsprechenden Daten ein, außerdem ändert er einige Konto-Optionen. Anschließend stellt er diesen Benutzer aus der Sicherung auf den alten Stand zurück. Als Resultat haben die Konto-Optionen wieder den Stand der Sicherung, die eingetragenen Adressdaten aber bleiben erhalten. Wurde der Benutzer allerdings zwischenzeitlich komplett gelöscht, so wird natürlich der exakte Stand der Sicherung wiederhergestellt. Waren übrigens die Adressfelder zum Sicherungszeitpunkt gefüllt (also nicht leer) und wurden sie anschließend geändert, so wird der Inhalt beim Restore wieder auf den vorherigen Stand zurückgesetzt. Wichtig ist, dass dem Administrator diese Arbeitsweise bewusst ist, um abschätzen zu können, wie sich ein Restore im Detail auswirkt. Der Hersteller hat bestätigt, dass diese Arbeitsweise so beabsichtigt ist. Wir hielten es für geschickter, wenn der Administrator bei einer Wiederherstellung auswählen könnte, wie ursprünglich leere Attribute behandelt werden. Nicht möglich ist übrigens der komplette Restore einer Domäne mit ODR, das Ziel ist vielmehr die Sicherung und Wiederherstellung einzelner Objekte.

Sicherheit der Backup-Daten

Hinsichtlich der Datensicherheit wirbt Quest damit, dass die Daten bei der Übertragung und Speicherung durchgängig verschlüsselt sind. Verwendet werden SAML (Security Assertion Markup Language) zum Austausch der Authentisierung sowie WIF (Windows Identity Foundation) zum Identitätsmanagement. Gesichert wird auf einer Windows Azure Plattform.

Allen diesen Beschreibungen zum Trotz fiel uns auf, dass es außer dem Benutzernamen mit Passwort keinerlei Restriktionen gibt, um sich von überall mittels Webbrowser auf dem Portal anzumelden. Auch lässt sich das Passwort jederzeit ändern und es gibt einen Prozess, sich ein neues Passwort per E-Mail zusenden zu lassen, wenn das gültige vergessen wurde. Hat sich nun jemand unberechtigterweise die Anmeldedaten verschafft, so kann er gewisse Informationen wie die gesicherten Domänen sowie die dazu genutzten Domänencontroller herauslesen. Als wir aber nach Hackermanier versuchten, mit einem anderen als Domänencontroller installierten Server über eine Wiederherstellung an die gesicherten Daten heranzukommen, gelang uns dies nicht. ODR erkannte, dass es sich hier um eine zwar gleichnamige, aber nicht identische Domäne handelte. Letztendlich konnten wir nur das Konto übernehmen und die gesicherten Daten löschen, also Schaden anrichten, aber keine weiteren Daten ausspionieren.

Reporting per E-Mail

Zum Überprüfen der Sicherungen auf dem Webportal gibt es einen eigenen Reiter "Activity". Hier erhält der Adminis-

trator ausreichend Informationen zum Sicherungsverlauf. Ein grüner Haken oder ein rotes Kreuz signalisieren auf einen Blick, wie es um den Status bestellt ist.

Ein aktives Reporting kann per E-Mail über den Backupserver bei Quest erfolgen, dies ist aber standardmäßig nicht eingerichtet. Der Administrator muss hierzu auf dem Webportal unter dem Punkt "Roles&Alerts" neben den drei Standardgruppen, bei denen er die Benachrichtigungen nicht umkonfigurieren kann, eine weitere anlegen, dort die Mailadressen der zu benachrichtigenden Administratoren eintragen und auch auswählen, welche Vorkommnisse per E-Mail versendet werden sollen. Nachdem wir die Benachrichtigung einmal komplett konfiguriert hatten, wurden wir regelmäßig informiert und konnten bei Problemen auch gleich Hand anlegen. Eine interne Benachrichtigung über den Agent beispielsweise per SNMP ist nicht vorgesehen. Auch eine Auswertung der Windows-Ereignisanzeige durch eine geeignete Monitoringsoftware bringt wenig, denn es sind nur Einträge zum Starten und Stoppen des "Quest Backup and Restore Agent" zu finden.

Fazit

OnDemand Recovery for Active Directory beinhaltet eine innovative Idee vor allem für kleinere und mittlere Unternehmen, die Sicherung ihrer Microsoft-Domänen über einen Online-Dienst abzuwickeln. Der Vorteil ist offensichtlich, denn es muss für diesen Zweck keine Backuplösung angeschafft werden. Gefallen haben uns die einfache Bedienbarkeit und die Möglichkeit, mit wenigen Mausklicks einzelne Objekte aus dem Active Directory wiederherstellen oder auf einen Stand zur Zeit der Sicherung zu bringen. Nicht möglich ist die komplette Wiederherstellung einer Domäne bei Verlust des Domänencontrollers. Da die Steuerung von ODR über ein Webportal erfolgt, kann sich jeder von überall anmelden, sofern er Benutzerkennung und Passwort in Erfahrung gebracht hat. Er kommt dann zwar nicht auf die gesicherten Daten, kann aber die Sicherungen relativ einfach löschen. Ein zusätzlicher Schutz wäre hier wünschenswert. Vorteilhaft ist, dass der Agent nicht auf einem Domänencontroller installiert werden muss und dass es möglich ist, über einen Account mehrere Agenten zu verwalten und mehrere Domänen beziehungsweise einen ganzen Forest zu sichern.

Mit der getesteten Version 1.3.1 ist die Software nach unserer Einschätzung gerade dabei, die Kinderstube zu verlassen. So lieferte die Kernfunktion, also Backup und Restore an sich, im Test nach anfänglichen Problemen und einer Reklamation recht ordentliche Ergebnisse. Bei einigen Funktionen sowie bei der Zuverlässigkeit an sich sehen wir noch Optimierungspotential. So führt die Software zwar eine Prüfung auf Updates durch, es gibt aber keine Möglichkeit zur automatischen Installation. Auch hatten wir im Test mehrfach Probleme mit dem Einspielen der Updates.

Nicht optimal gelöst sehen wir das Wiederherstellungsverhalten bei Attributen, die zum Zeitpunkt der Sicherung nicht gesetzt waren. Hier sollte der Administrator wählen können, ob er eine exakte Wiederherstellung durchführen oder nachträglich definierte Attribute belassen möchte. Mehr als Schönheitsfehler betrachten wir die Tatsache, dass die Zeitangaben im Sicherungszeitplaner nicht mit der lokalen Zeit übereinstimmen.

Gefallen hat uns, dass sich ein Reporting über den Backup-Server bei Quest einrichten lässt. Dieses informiert unter anderem bei neuen Features sowie bei Fehlern beim Backup und Restore per Mail, so dass der Administrator aktiv werden kann. Interessenten können einen Account anlegen und sich eine 30 Tage lauffähige Trialversion herunterladen. Zum Testzeitpunkt wurde offensichtlich noch intensiv am Produkt gearbeitet, so dass in der nächsten Zeit einige Verbesserungen zu erwarten sind. *(jp)*

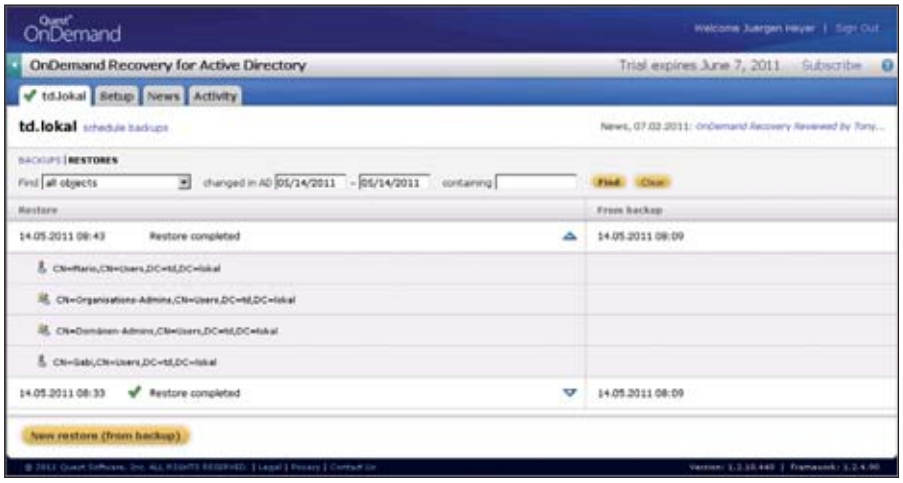


Bild 4: Nach erfolgter Rücksicherung listet ODR auf, welche Objekte geändert wurden

Produkt
Online-Backup und Restore für Objekte des Microsoft Active Directory.

Hersteller
Quest
www.quest.com

Preis
60 US-Cent pro Monat
pro gesichertem Benutzer-Account.

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

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

Einrichtung	8
Backup	7
Restore	6
Updateprozess	5
Reporting	6

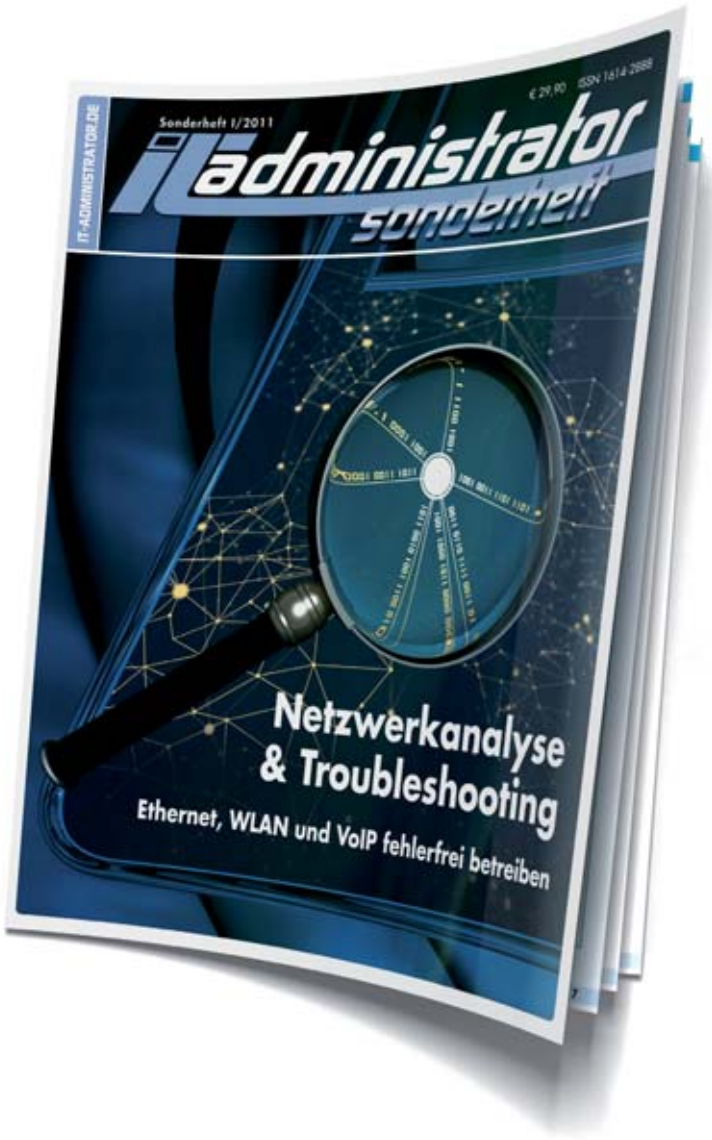
Dieses Produkt eignet sich

optimal für kleinere und mittlere Firmen, für die sich eine eigene Sicherungslösung für ihre Verzeichnisdienste nicht lohnt.

bedingt für große Unternehmen. Hier dürfte eine Inhouse-Lösung, wie sie Quest als eigenes Produkt anbietet, interessanter sein.

nicht für Firmen, die einen anderen Verzeichnisdienst als Microsoft Active Directory nutzen.

Quest OnDemand Recovery for Active Directory



Bestellen Sie jetzt

das IT-Administrator

Sonderheft I/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iadministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0811

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

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

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

leserservice@it-administrator.de

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

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

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

Im Test: openITCockpit 2.6.5

Kleines Cockpit für Nagios

von Thomas Bär

Einen stets aktuellen Zustandsbericht der IT-Netzwerkumgebung im Unternehmen zu erhalten, ist für den IT-Administrator von sehr hoher Bedeutung. Im Idealfall reagieren zuvor definierte Automatismen oder im Notfall auch der Administrator selbst auf Fehler und Missstände. Nagios hat sich als kostenlose Monitoring-Software bereits einen Namen in der Branche gemacht. openITCockpit, ebenfalls Open Source-Produkt, ist eine Erweiterung für Nagios für das einfachere System-Monitoring. In diesem Test untersuchten wir, inwieweit das kostenlose openITCockpit 2.6.5 die Inbetriebnahme und Verwaltung von Nagios vereinfacht.

Nagios, veröffentlicht von der Nagios Enterprises LLC, ist eine unter GNU-GPL Lizenz stehende Software für das Monitoring von IT-Infrastrukturen unterschiedlicher Größe. Auch wenn es dank der weiten Verbreitung nicht den Eindruck macht, so wurde die Software erst im Jahr 2007 erstmalig zum Download angeboten. In dieser doch recht kurzen Zeit hat sich eine extrem große Anzahl von Erweiterungen, den so genannten Modulen, für Nagios angesammelt. Das Werkzeug bietet, neben dieser Sammlung unterschiedlicher Module, die Technik für die Überwachung von Netzwerken, Hosts und Diensten und eine Web-Schnittstelle, um die gesammelten Daten abzufragen.

Nagios ist sehr wohl in der Lage, Windows-Server und auf ihnen betriebene Serverapplikationen zu überwachen, installiert und betrieben werden muss es jedoch auf einem Unix-ähnlichen Betriebssystem und liegt zudem ausschließlich in englischer Sprache vor. Die Produktdokumentation der aktuellen Version 3 macht keine näheren Angaben zur Linux-Distribution selbst. Abhängigkeiten bestehen lediglich hinsichtlich eines Webservers (üblicherweise Apache), der GD LIBRARY 1.63 oder höher von Thomas Boutell und eines C-Compilers, sofern das Paket auf der Maschine direkt kompiliert wird.

Aktuell stehen bereits über 2.000 kostenlose Plug-Ins und Module [1] zur Überwachung verschiedenster Systeme zum Download bereit. Hier finden sich neben

Bild 1: openITCockpit unterstützt die Bildung von Standorten mit verschiedenem Personal

bekannten und weit verbreiteten Komponenten und Serverdiensten auch eher seltenere Netzwerksysteme. Die Sammlung reicht von Plug-Ins für Antivirus-Enterprise-Lösungen von NOD, Symantec oder Kaspersky über Monitore für Datenbanksysteme von Ingres bis Oracle bis hin zum Lizenz-Management.

Steuerung über Normwerte

Üblicherweise überwacht die Nagios-Installation den Status von Diensten, beispielsweise HTTP, FTP oder SSH, Festplattenspeicherkapazitäten von Servern oder die CPU- und Speicher-Auslastung. Die Einrichtung der spezifischen Überwachungsmonitore für das eigene Unternehmensnetzwerk ist der wesentliche Teil der Arbeit für den Administrator. Es versteht sich beinahe von selbst, dass für diese Aufgaben das spezifische Wissen über die zu überwachenden Geräte, Software, Normalwerte und die zu erwartenden Abweichungen erforderlich ist.

Glücklicherweise hat die Auseinandersetzung mit einer Monitoring-Lösung einen überaus positiven Effekt auf das Know-how der beteiligten IT-Mitarbeiter. Erst wenn es darum geht, den maximalen Füllungsgrad einer E-Mail-Versandqueue automatisiert überwachen zu lassen, ist der

IT-Verantwortliche gezwungen, sich mit den Normwerten seiner Anlage intensiv auseinanderzusetzen. Die insgesamt sehr hohe Anzahl von verfügbaren Modulen erlaubt zudem den Aufbau einer einzigen zentralisierten Überwachung für das Unternehmen – konkurrierende Überwachungslösungen innerhalb einer IT-Installation sind üblicherweise keine wirkliche Hilfe.

Ermittelt die Nagios-Überwachung, dass ein zuvor definierter Wertekorridor für eine Komponente verlassen wird oder eine Komponente überhaupt oder teilweise nicht mehr erreichbar ist, alarmiert das System über unterschiedliche, definierbare Kommunikationskanäle die hinterlegten Kontaktpersonen. Ein Eskalationsmanagement für Kontaktpersonen ist mit Nagios ebenso realisierbar wie die Unterdrückung von Meldungen von abhängigen Diensten. Fällt beispielsweise ein Server komplett aus, so ist eine Konfiguration möglich, in der nicht für jeden einzelnen Serverdienst eine Meldung ausgesendet wird.

System-Monitoring mit reduzierter Komplexität

Die hohe Flexibilität von Nagios hinsichtlich der Möglichkeiten und Überwachung ist mitunter aber auch ein kleiner Fluch. Viele IT-Administratoren scheuen sich vor dem Einsatz von derart komplexen Projekten, da die berechtigte Angst mitschwingt, sehr viel Zeit für das System selbst einplanen zu müssen. Schlimmer noch: Projekte mit sehr hoher Komplexität münden nicht selten in zeitaufwändigen Softwareleichen, ohne dass je das gewünschte Ziel erreicht wird.

Um die Fähigkeiten von Nagios zu nutzen, ohne sich mit allen Details auseinandersetzen zu müssen, wurde im Sommer 2010 das Projekt "openITCockpit" (OITC) als Open Source-Systemmanagement-Projekt ins Leben gerufen. Hinter diesem Projekt steckt die it-novum GmbH, eigentlich auf die Integration von SAP mit Open-Source-Lösungen spezialisiert. OITC ist, laut Angaben der it-novum, aus mehreren Systemmanagement-Projekten bei verschiedenen größeren Unternehmen in Deutschland hervorgegangen.

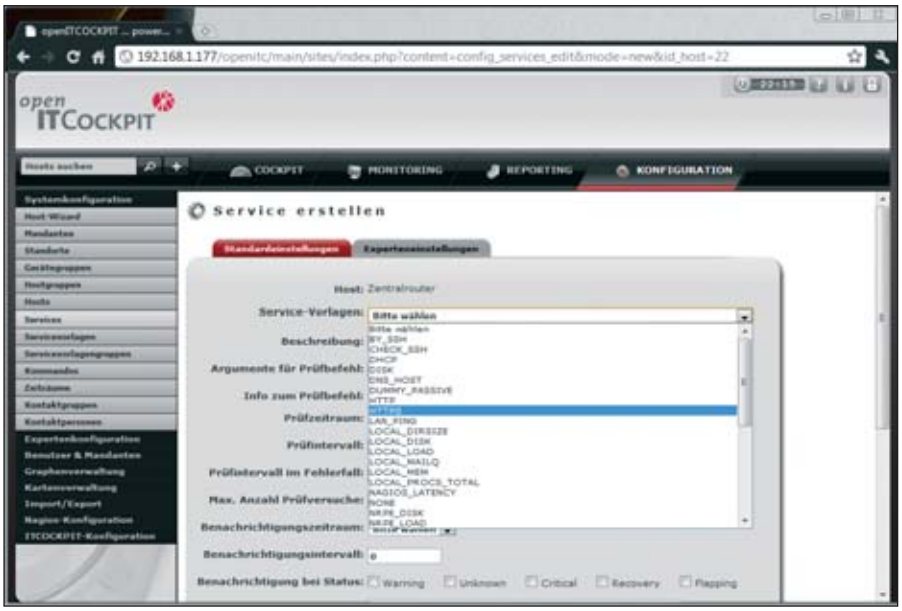


Bild 2: Dank Nagios als Basissystem ist eine Überwachung beinahe aller Komponenten mit dem openITCockpit möglich. Die wichtigsten Monitore und Plug-Ins sind bereits vorinstalliert.

Das openITCockpit-Framework basiert auf Nagios und ist wiederum über Module erweiterbar. In der Rubrik Betriebssysteme bietet OITC die Unterstützung für Microsoft Windows 2000 und höher, IBM AIX, HP UX, Solaris, Red Hat-, SuSE- und Ubuntu-Linux. Die Kategorie "Virtualization Monitors" ist unter anderem mit VMware Virtual Center, Microsoft Hyper-V und Citrix XenServer gefüllt. Die positiv anmutende Unterstützungsliste von Produkten zieht sich bei Datenbanken mit Oracle, MySQL, IBM DB2, Microsoft SQL-Server über Network Services mit DNS, SNMP, IMAP4 und POP3 bis hin zu Telekommunikation mit Asterisk, Hyla und Ferrari-Fax fort.

OITC ist im Vergleich zum puren Nagios mit einigen entscheidenden Mehrwerten ausgestattet: Die Konfiguration wird über eine intuitive Weboberfläche vorgenommen. Während Administratoren beim reinrassigen Nagios viele klassische Open Source-Tools für die Nagios-Basisinstallation erst hinzuinstallieren müssen, so ist dies bei OITC bereits geschehen. Der Fokus des openITCockpit-Projekts liegt eindeutig auf den Bedürfnissen von Administratoren, die nach einem einfachen und kostenfreien System-Monitoring suchen, das sich in einem einzigen Frontend administrieren lässt und heterogene und historisch gewachsene IT-Systemlandschaften einfach darstellt.

Klassische Installation oder Einsatz als virtuelle Maschine

Üblicherweise wird das OITC als TAR-Archiv von der Homepage heruntergeladen und auf einem bereits mit Nagios konfiguriertem Server installiert. Mit Blick in die vielen Foren-Einträge wird deutlich, dass es sich bei der Installation von Nagios im günstigsten Fall um einen frisch aufgesetzten SuSE-Enterprise-Server handelt. Im Hintergrund modifiziert die System-Monitoring-Lösung einige Einstellungen, die für den Betrieb erforderlich sind. Die Empfehlung lautet somit: Ein dedizierter Server für das Monitoring mit OITC. Grundsätzlich ist es empfehlenswert, den Überwachungs-Rechner nicht mit anderen Aufgaben zu versehen – er sollte einfach nur die IT-Umgebung im Blick haben und sicher informieren können. Ein eigener SMTP-Mailversand, unabhängig vom üblichen Mailserver, gehört bei OITC zur Grundausstattung.

Einfacher als die Installation von Hand geht es mit einem vorbereiteten Installer von Nezztek, der dem Administrator die manuelle Installationsarbeit abnimmt. Wer sich erst einmal einen Überblick über OITC verschaffen will, findet im Forum der Webseite eine bereits vorkonfigurierte virtuelle Maschine für VMware auf Basis von OpenSuse 11.1 mit PHP 5.2.1. Nach dem Download der zehn RAR-Dateien mit einem Gesamtumfang von

rund 1 GByte ist die VM mit einer 32 GByte HDD und 512 MByte Arbeitsspeicher innerhalb weniger Minuten einsatzbereit. Nachteilig an dieser VM ist lediglich die Tatsache, dass ein Account beim Webhoster Rapidshare erforderlich ist. Nach der Erstanmeldung ist lediglich über YaST die eigene feste IP-Adresse zuzuordnen. Die Hinweise in Bezug auf Probleme rund um das Nagios-Ramdrive in der VM können in einer Teststellung getrost überlesen werden. Alle Funktionen von OITC lassen sich mit dieser VM problemlos und in wenigen Minuten betrachten.

Neben der VM für VMware gibt es seit Mai 2011 eine weitere vorkonfigurierte virtuelle Maschine für Oracle VirtualBox mit openITCockpit 2.6.5. Diese wird in den zwei "Geschmacksrichtungen" openSUSE 11.1 oder Debian 6 angeboten und ist der ursprünglichen VMware-VM in Bezug auf die Aktualität überlegen. Zudem ersparen diese VMs die Nutzung eines Rapidshare-Accounts. Die technischen Daten der VM sind absolut ausreichend: 512 MByte Arbeitsspeicher und 32 GByte dynamisch wachsende Festplattendatei. Die Installation war denkbar einfach: Wir erstellten eine neue virtuelle Maschine in VirtualBox, wählten als Betriebssystem openSUSE oder Debian 64 Bit, setzten den Arbeitsspeicher auf 512 MByte und als Festplatte banden wir die heruntergeladene VDI-Datei ein. Abschließend setzten wir das Netzwerk auf "Netzwerkbrücke", ehe wir die VM starteten, und prüften zu guter Letzt noch einmal, ob die virtuelle Festplatte auch an "IDE Master" hängt. Nach dem Hochfahren mit YaST legten wir die IP-Adresse fest und aktivierten mit einem kleinen Shell-Skript *sh /root/start.sh* alle Server.

Mandanten und Standorte erleichtern verteilte Administration

Nachdem wir die Grundkonfiguration von OITC abgeschlossen hatten, griffen wir auf die Software ausschließlich per Webbrowser zu. Das optisch insgesamt gut gelungene und funktionelle Webinterface bietet eine einfache Menüstruktur und den "Host-Wizard", über den Geräte und zu überwachende Werte sehr einfach und unterstützt eingefügt werden.

Sehr angenehm für den Einsatz in größeren Umgebungen ist die Fähigkeit der Software, unterschiedliche Mandanten abzubilden, denen wiederum verschiedene Gerätegruppen und Standorte zugewiesen werden. Der Administrator stößt bei OITC nicht an Konfigurationsgrenzen und muss auch keine Kompromisse bei verschiedenen Standorten eingehen. Das Mandantenkonzept zieht sich durch bis in die Zuordnung von EDV-Mitarbeitern zu den verschiedenen Standorten.

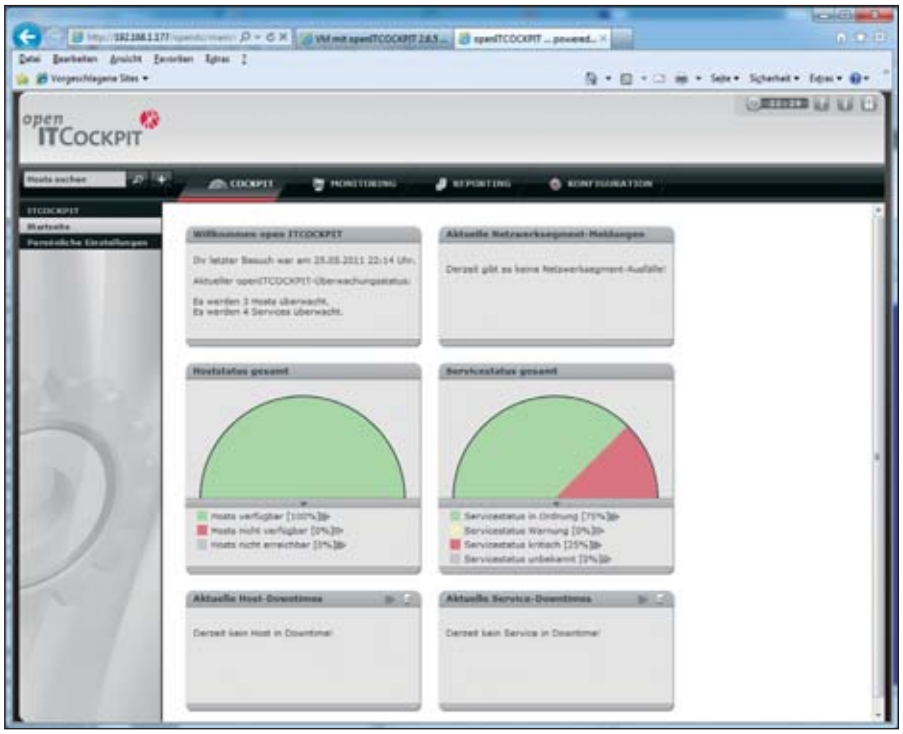


Bild 3: Darf auch bei openITCockpit nicht fehlen: Das Cockpit mit dem obligatorischen Dashboard, von dem openITCockpit seinen Namen hat

Überwacht eine verteilte IT-Abteilung verschiedene Standorte, so ist der lesende Zugriff durch standortferne IT-Mitarbeiter ein äußerst hilfreiches Mittel, das der Administrator in OITC problemlos konfiguriert. Unterschiedliche Zeitmodelle für das Monitoring sind nicht nur für die Abbildung von Benachrichtigungsketten von Interesse. Möchte der IT-Leiter unterschiedliche Service Levels (SLAs) abbilden, so sind verschiedene Zeitfenster, beispielsweise mit 24/7 oder 10/5 Stunden/Tage, schnell hinterlegt und zeigen diese verschiedenen vertraglichen Regelungen an.

Mitunter viel mühsame Handarbeit

Nach dem Hinterlegen von Mandant, Standort und zu informierenden Personal legten wir die verschiedenen IT-Systeme, die überwacht werden sollten, an. Die üblichen und von kostenpflichtigen Lösungen bekannten Suchroutinen für IP-Bereiche, SNMP-Scans oder Suchen über WMI suchten wir bei OITC leider vergeblich. Hier ist manuelle Handarbeit gefragt – und das kann, je nach Größe des Netzwerks, einige Zeit in Anspruch nehmen. Gerät für Gerät muss über die IP-Adresse oder Hostnamen manuell und eher mühsam eingegeben und gespeichert werden. Was genau bei einem Host untersucht werden soll, mussten wir im nächsten Schritt unter "Services" ebenfalls manuell festlegen.

OITC unterstützt, wie Nagios, sowohl ein agentenorientiertes als auch agentenfreies Monitoring der Umgebung. Dank der sehr zahlreichen Erweiterungen dürfte sich kaum ein aktuelles System finden, das sich nicht in der Kombination aus Nagios und OITC überwachen lässt. Alle Parameter der Überwachung, vom Intervall in der normalen Prüfung bis hin zu einem verkürzten Intervall bei Auftreten einer Anomalie, lassen sich über das Webinterface bequem und intuitiv einrichten.

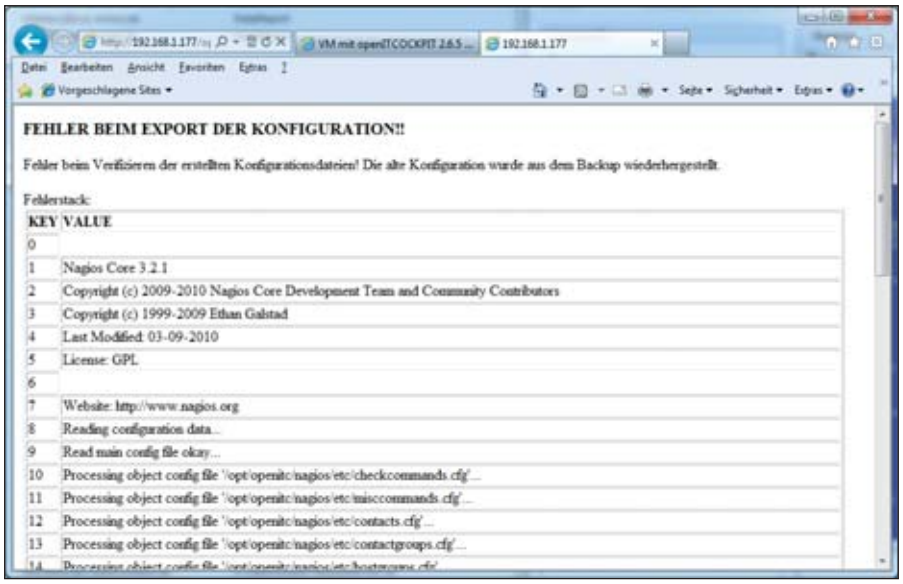


Bild 4: Fehlerhafte Konfigurationen bemerkt openITCockpit leider erst beim Export an Nagios

Die Aktivierung der Konfigurationsänderungen mit OITC ist für den Administrator zunächst etwas gewöhnungsbedürftig. Wie von ausgewachsenen Netzwerkgeräten bekannt, sind alle Konfigurationsänderungen zunächst einmal nicht aktiv. Leider fehlt in der grafischen Oberfläche ein entsprechend deutlicher Hinweis, dass die Konfigurationsänderung noch nicht durchgeführt wurde. Erst nachdem wir im Menü die neue Konfiguration an Nagios exportiert hatten, waren die neuen Anpassungen überhaupt nutzbar. Kommt es hierbei zu unlogischen Konfigurationsanpassungen – beispielsweise haben wir im Test versehentlich einen Host definiert, dessen Service von sich selbst als übergeordnetem Gerät abhängt –, so wurde dies erst beim Export an Nagios in Form einer überaus kryptischen Fehlermeldung bemängelt. Eine logische Prüfung der Anpassungen findet somit erst auf der Zielgeraden statt. Ein Umstand, mit dem der Administrator vor dem Hintergrund einer kostenfreien Lösung sicherlich leben kann.

Äußerst flexibles Monitoring

OpenITCockpit überwacht Netzwerke aller Größen. In komplexen Konstellationen und in verteilten Netzwerken mit vielen verschiedenen Arten von Geräten kommen die Vorzüge der Open Source-Lösung jedoch erst so richtig zum Vorschein. Selbst für die seltsamsten Hosts, wie einem digitalem Adapter in der Sensorik, findet der Administrator das passende Modul. OITC funktioniert über bidirektionale Kommunikationswege auch mit mehreren Servern, die im so genannten Master- oder Slave-Modus betrieben werden.

Neben der einfachen Verteilung der Last durch die Host-Prüfung auf mehrere verschiedene Server unterstützt die Software einen weiteren, alternativen Architekturansatz mit einer Multi-Layer-Strategie, bei der zwischen Monitoring-, Aggregation, Middleware- und Presentation-Layer unterschieden wird. Neben der einfachen Auswertung der Geschehnisse als Dashboard mit der Fähigkeit zum Drill-Down bietet die Grundkonfiguration der Software eine Darstellung in einer Kuchengrafik für einzelne Geräte oder Gerätegruppen. Listen kann der Administrator ohne optionale Zusatzprogramme direkt in PDF-Dateien konvertieren. Der bereits integrierte Postfix-Mailserver erlaubt mit einigen Konfigurationsschritten den Versand von Benachrichtigungs-E-Mails losgelöst vom primären E-Mailserver des Unternehmens.

Fazit

Im Vergleich zur Standardinstallation von Nagios ist das Netzwerkmonitoring mit openITCockpit doch deutlich einfacher. Die Weboberfläche erklärt sich dem Administrator weitgehend von allein und ist zudem auf Deutsch gehalten. Was uns sehr gut gefiel, ist die Umsetzung der Mandantenfähigkeit. Ohne größeren Zeitaufwand sind eine Überwachung und die Einrichtung von Benachrichtigungen in weniger als einem Nachmittag möglich. Alle Funktionen von Nagios zu ergründen, ist ein Unterfangen, das sicherlich Wochen an Zeit in Anspruch nimmt. Die Kombination von openITCockpit und Nagios ist eines der besten Open Source-Monitoring-Werkzeuge. In Bezug auf den Komfort gewinnen die traditionellen, käuflich zu erwerbenden Produkte jedoch (noch) das Rennen. *(jp)*

Produkt
Konfigurations- und Managementsoftware für das Open Source-Monitoringwerkzeug Nagios.

Hersteller
it-novum Deutschland
www.open-itcockpit.com

Preis
kostenlos (kostenpflichtige Einführung und Basisimplementierung durch den Anbieter möglich).

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

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

Installation	7
Anzahl Erweiterungen/Plug-Ins	9
Integrationsfähigkeit	8
Aufwand bei Integration	5
Reporting	6

Dieses Produkt eignet sich

optimal für Unternehmen mit kleinem Budget, die viele verschiedene Geräte an verschiedenen Standorten überwachen müssen.

bedingt für Unternehmen, die nur sehr wenige Geräte überwachen möchten.

nicht für Unternehmen, in denen kein geeignetes IT-Knowhow für die Einführung vorhanden ist.

openITCockpit 2.6.5

[1] Download Nagios Plug-Ins und Module
B8T41

Link-Codes

Im Test: bintec RT1202

Roter Tausendsassa

von Oliver Wagner

Mittlerweile gehört Unified Messaging zum Standard in Unternehmen: E-Mails, Faxnachrichten und Sprachnachrichten lassen sich unter einem Dach verwalten. Alles kein Problem, bis der UC-Server die Grätsche macht und ganz schnell der gespiegelte Server übernehmen muss. Der muss dann auch die teure ISDN-Hardware vorhalten. Oder es dauert Stunden, bis der Spiegelserver nach dem Umbau der ISDN-Hardware samt Installation und Konfiguration der zugehörigen Treiber betriebsbereit ist. Hier will Funkwerk mit dem bintec RT1202 Abhilfe schaffen. IT-Administrator hat das Gerät im Test untersucht, um festzustellen, ob der ISDN-Failover wirklich so unkompliziert verläuft.

Das bintec RT1202 ist ein externes Gerät, das im 19 Zoll-Schrank Platz findet und mittels Ethernet mit dem Server verbunden wird. So müssen IT-Verantwortliche die ISDN-Hardware nicht doppelt vorhalten und im Problemfall nicht einmal umstöpseln. Der Serverausfall reduziert sich in solchen Fällen dadurch auf wenige Sekunden und nicht Stunden. Eine solche Lösung klingt auf den ersten Blick zwar selbstverständlich, ist es aber keinesfalls. Der Haken an der Sache ist nämlich die berühmte CAPI. Über die läuft jede Software, die auf eine ISDN-Verbindung angewiesen ist. Und bisher war es so, dass die CAPI die zugehörige Hardware in dem Computer vorfinden musste, auf dem sie ausgeführt wurde. Da dies im Falle eines externen Gerätes jedoch nicht der Fall ist, funktioniert das ganze System auch nicht.

Eine CAPI für alle

Glücklicherweise haben die Entwickler von bintec eine Lösung für dieses Problem gefunden. Diese hört auf den Namen Remote-CAPI und ihr ist es egal, wo im Netz die Hardware steckt. Wir wollten wissen, ob dieses System in der Praxis hält, was der Hersteller verspricht, und auch, wie einfach das System zu installieren ist. Um dies herauszufinden, haben wir uns aus der vier Mitglieder umfassenden Familie von bintec den kleinsten Vertreter herausgesucht, das RT1202. Dieses Gerät verfügt über fünf Ethernetports und zwei ISDN-Ports. Darüber hinaus sind vier DSP-Prozessoren verbaut, je einer für jeden Faxkanal. Für kleine Netzwerke ist darüber hinaus ein DHCP-Server integriert, der natürlich deaktiviert werden kann. Sehr interessant sind auch die zehn bereits mitgelieferten IPsec-Tunnellizenzen, die sich bei Bedarf und gegen Aufpreis auf 110 erweitern lassen. Die Kosten dafür belaufen sich auf rund 250 Euro für je 25 Lizenzen.

Zum Lieferumfang des Geräts gehören Kabel – je eines für Ethernet, ISDN, seriell und Strom –, ein 19 Zoll-Montagesatz, vier selbstklebende Gummifüße, falls das Gerät nicht im Rack montiert werden soll, ein Installationsposter sowie eine DVD, auf der sich die komplette Dokumentation sowie einige Software befindet. Die Installation des RT1202 war schnell erledigt: Wir verbanden die BRI-Buchsen mit einer ISDN-Dose. Dabei spielt es keine Rolle, ob es sich um eine Amtsleitung oder eine interne Verbindung zur Telefonanlage handelt. Allerdings war uns an diesem Punkt nicht klar, warum nur ein ISDN-Kabel mitgeliefert wird, wenn zwei entsprechende Ports vorhanden sind. An eine der fünf Ethernetbuchsen kommt der Switch und an die vier verbliebenen lässt sich je ein DSL-Modem anschließen. Die zugehörigen Netz-Zugangsdaten werden dann in der RT1202 eingetragen. Noch das Stromkabel eingesteckt und fertig war die Installation.

Überschaubarer Konfigurationsaufwand

Um die Konfiguration so einfach wie möglich zu gestalten, haben sich die Entwickler mächtig ins Zeug gelegt. Das erste Problem bei Ethernetgeräten liegt häufig darin, dass der Hersteller eine IP-Adresse vergibt, auf die im eigenen Netzwerk nicht ohne weiteres zugegriffen werden kann. Um dieses Problem zu umgehen, findet sich auf der mitgelieferten DVD ein Programm namens Dime Manager. Dieses Tool spürt das RT1202 auch dann auf, wenn es eine netzwerkfremde IP-Adresse nutzt. In unserem Fall hat dies tadellos funktioniert. Über die HTTP-Konfiguration hatten wir dann unmittelbar Zugriff auf das Gerät und konnten auf DHCP umstellen. Damit war die erste Hürde genommen.

Wer ein solches Gerät übrigens für eine Filiale konfigurieren möchte, muss die Kollegen vor Ort lediglich das Gerät verkabeln lassen. Der Zugriff erfolgt dann per ISDN-Leitung, so dass sich der Administrator gar nicht erst vor Ort begeben muss. Aber Vorsicht – wer anschließend vergisst, für die MSN-Erkennung eine Rufnummer für die Konfiguration einzugeben, hat ein Problem. Von Haus aus ist das Gerät nämlich so eingestellt, dass Rufe auf allen MSNs angenommen werden. Wer also eine Telefonanlage am gleichen ISDN-Anschluss installiert hat, wird keine Rufe mehr empfangen, bis dieser Punkt konfiguriert ist. Allerdings weist das Handbuch auf diesen Umstand hin. Pech nur für diejenigen, die solche Dinge nicht lesen.

Für die weitere Konfiguration gibt es dann im Wesentlichen drei Alternativen. Entweder die per DVD mitgelieferte Doku-

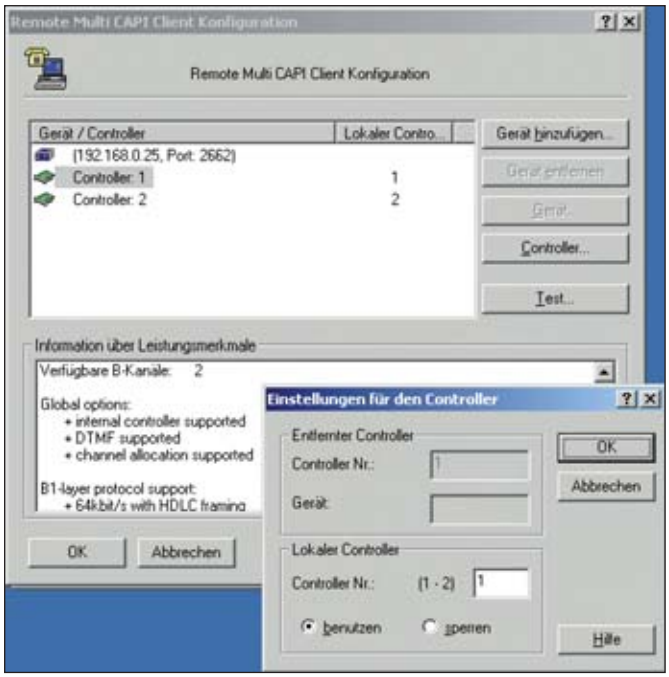


Bild 1: Die CAPI Client-Konfiguration ermöglicht es, die Reihenfolge der Controller zu ändern

mentation, in der alle erforderlichen Schritte gut verständlich beschrieben sind. Oder der Anwender lässt sich von einem der Assistenten führen, die in das RT1202 integriert sind. Als dritte Alternative finden sich auf der Homepage von bintec [1] Workshops in Form von HTML- oder PDF-Dokumenten. In unserem Fall haben wir die Grundkonfiguration per Dokumentation vorgenommen. Im zweiten Schritt haben wir uns dann von einem Workshop speziell für Tobit unter die Arme greifen lassen.

Mit dieser Kombination gelang uns die Konfiguration innerhalb weniger Minuten ohne Probleme. Vor allem die Installation der CAPI verlief erfreulich stressfrei. Einfach das entsprechende Programm gestartet – wie im Workshop aus dem Internet beschrieben – und fertig. Zu konfigurieren gibt es an dieser Stelle übrigens nichts Zwingendes. Einmal abgesehen davon, dass ein Username und Passwort für die CAPI vergeben werden sollte. Sonst kann jeder im Netzwerk die CAPI nutzen. Übrigens ist es in manchen Fällen von unschätzbarem Vorteil, dass sich die Reihenfolge der Controller ändern lässt (Bild 1), ohne dass ein Neustart des Systems erforderlich wäre. Eine solche Änderung ist beispielsweise für Anwendungen erforderlich, bei denen der Nutzer keinen Einfluss darauf hat, welcher Controller verwendet wird, weil immer automatisch der erste herangezogen wird. Anschließend mussten wir in Tobit nur noch die beiden Ports hinzufügen, die auch anstandslos gefunden wurden. Dann noch schnell die gewünschten MSNs für die Ports eingestellt und schon sind die ersten Faxnachrichten hereingekommen und konnten problemlos verschickt werden.

Unkomplizierter Remotezugriff

Natürlich wollten wir auch noch wissen, ob der Remotezugriff genauso einfach zu konfigurieren ist, wie es uns mit Tobit ergangen ist. Dazu wollten wir per Windows Remotedesktop auf den Server zugreifen und mussten hierfür das VPN im RT1202 konfigurieren. Der erste Schritt bestand darin, einen Account bei DynDNS einzurichten und diesen im RT1202 zu konfigurieren. Hierbei haben wir uns im ersten Durchlauf beim Benutzernamen verschrieben, was natürlich zu einer Fehlermeldung geführt hat. Leider hat es, zumindest laut Anzeige in der HTTP-Konfiguration, nicht geholfen, den falschen Benutzernamen zu korrigieren. Erst nachdem wir den Eintrag komplett gelöscht und neu erstellt hatten, wurde der Eintrag bei DynDNS korrekt aktualisiert und entsprechend im Interface auch angezeigt. An dieser Stelle hat sich übrigens zum ersten Mal gezeigt, dass es sehr sinnvoll ist, dass die Entwickler an allen relevanten Stellen entsprechende Symbole und Texte eingebaut haben, die zielführende Auskünfte erteilen.

Im nächsten Schritt erstellten wir dann den zugehörigen NAT-Eintrag. Leider mussten wir hier feststellen, dass die im Internet gefundene Anleitung nicht mehr den aktuellen Gegebenheiten entspricht, so dass Laien sicher vor einem Problem stehen. Wer allerdings einigermaßen mit der Materie vertraut ist, dem genügen die Angaben vollauf, um einen korrekten Eintrag zu erstellen. In einem dritten und letzten Schritt mussten wir dann noch eine neue Netzwerkverbindung erstellen. Auch hier zeigt die Anleitung im Detail, welche Einstellungen vorzunehmen sind. Ein anschließender Test hat auch gleich bestätigt, dass die Anleitung alle erforderlichen Schritte korrekt erklärt hat.

VPN schnell eingerichtet

Neben der Remoteverwaltung des RT-1202 wollten wir natürlich auch VPN-Zugänge für das lokale Netzwerk einrichten. Zu diesem Zweck findet sich im Internet bei den FAQs eine entsprechende Anleitung, anhand derer wir diesen Zugangsweg eingerichtet haben. Sie stellt sehr schön Schritt für Schritt dar, welche Einstellungen im RT1202 und anschließend am Client-Computer vorzunehmen sind. Zwar bezieht sich das Beispiel im Internet auf einen anderen Router von bintec, da die Softwarebasis aber auf allen Geräten aus dem Hause bintec dieselbe ist, sind die Unterschiede nicht so groß, dass wir mit der Anleitung nicht zurecht gekommen wären. So hat also auch diese Anleitung ohne Umwege schnell zum gewünschten Ziel geführt.

Nachdem wir fertig waren, stellten wir dann fest, dass wir dieses aufwändige Prozedere auch einfacher hätten haben können, und zwar in Form eines Assistenten. Dieser fragt die erforderlichen Informationen ab, sammelt sie und macht die zugehörigen Eintragungen an den richtigen Stellen, ohne dass wir uns durch die vielen Einträge hätten hangeln müssen.

Fazit

Die vom eigentlichen Server losgelöste ISDN-Hardware bietet gleich mehrere Vorteile. Den ersten hatten wir eingangs bereits erwähnt – das schnelle Umschalten im Falle eines Serverausfalls. Dank des externen RT1202 braucht der Ersatzserver keine eigene ISDN-Hardware vorzuhalten, die sehr teuer ist und den ganzen Tag lang nichts zu tun hat. Nicht unerwähnt bleiben darf auch, dass das RT1202 eine High End Encryption-Engine integriert hat. Diese sichert den Datenverkehr über VPNs, und

Die Produktvarianten im Detail				
	RT1202	RT3002	RT4202	RT4402
Empfohlener Netto-Preis	681 Euro	1.154 Euro	1.206 Euro	2.624 Euro
10/100/1000 Base-T	5	5	5	5
ISDN-Ports	2	4	4	2
ISDN-S2M	0	0	0	2
Analoge Ports	0	0	4	0
DSL-Modem	Nein	ADSL (2+)	Nein	Nein
DSP-Prozessoren	4	8	12	60
Faxkanäle	4	8	8	60
DHCP-Server	Ja	Ja	Ja	Ja
IPSec-Tunnel	10	10	10	10
IPSec Maximal	110	110	110	110
E-Mail-Alarmierung	Ja	Ja	Ja	Ja
Load Balancing	Ja	Ja	Ja	Ja
Logging	Ja	Ja	Ja	Ja

zwar ohne den Prozessor des Servers zu belasten. Für die Verschlüsselung hat der Administrator die Wahl zwischen Preshared Keys sowie X.509-Zertifikaten.

Ein weiterer Vorteil ist, dass bei einer Konfigurationsänderung der ISDN-Hardware der Server nicht neu gebootet werden muss. Auch ein Umstand, der dem Administrator das Leben ganz erheblich vereinfacht. Nicht zu verachten ist des Weiteren, dass die CAPI auch von anderen PCs im Netzwerk verwendet werden kann. Dazu genügt es, auf dem betreffenden Rechner die Brickware zu installieren sowie den richtigen Usernamen und das Passwort für den Zugriff auf die CAPI einzutragen. Ohne diese Lösung müsste jeder PC im Netzwerk, der auf ISDN-Hardware angewiesen ist, diese selbst vorhalten. Ein nicht zu unterschätzender finanzieller Vorteil also. Ganz abgesehen davon, dass die Treiber auch aktuell gehalten werden müssen.

Gut gefallen haben uns auch die zahlreichen Protokolle und Berichtoptionen. Während unseres Tests haben wir nämlich durch eine nicht mehr nachzuvollziehende Änderung unsere Konfiguration zerschossen. Anstatt auf eine gespeicherte Konfiguration zurückzugreifen, haben wir bewusst noch mal von vorne angefangen. Dabei ist uns im VPN dann ein Fehler unterlaufen, so dass wir keine Verbindung mehr zustande brachten. Die Einträge im so genannten "Internen Protokoll" haben uns dann aber recht schnell auf die richtige Fährte gebracht, wobei auch die Angaben auf der Statusseite mitunter schon sehr vielsagend sind.

Alles in allem war das Gerät sehr schnell und einfach in Betrieb zu nehmen. Für Konfigurationen, die etwas schwieriger oder aufwändiger sind, finden sich im Internet Anleitungen oder Assistenten im Gerät selbst, die bei der Arbeit helfen. Die Anleitungen sind zwar im Web nicht auf den ersten Blick zu finden und nicht immer hundertprozentig aktuell, aber dieses Problem ist nicht wirklich tragisch, da die entsprechenden Einstellungen trotzdem schnell gesetzt sind. Darüber hinaus sollte es für bintec sicher kein allzu großer Aufwand sein, die Anleitungen im Internet zügig zu aktualisieren – was auch permanent gemacht wird. Zudem bietet das Gerät ausreichende Sicherheitsvorkehrungen an, um auch Remotearbeiter guten Gewissens ins Firmennetzwerk zu lassen. Und das mit zehn mitgelieferten Lizenzen sicher auch in ausreichender Anzahl. Falls nicht, können jederzeit 100 weitere Lizenzen erworben werden. Alles in allem können wir den roten Teufel also jedem ans Herz legen, der sein Tobit oder auch Exchange mit ISDN-Hardware versorgen muss.

In unserem Test haben wir uns bewusst auf die ISDN- und VPN-Funktionen des RT1202 beschränkt. Darüber hinaus lässt sich die gesamte Gerätefamilie aber auch noch als VoIP Media Gateway einsetzen und bietet für diesen Bereich neben zahlreichen Funktionen auch die Unterstützung von elmeg-Systemtelefonen an. Zudem lassen sich Funkmodule für WLAN-Funktionalitäten anschließen, so dass sich das System auch in diese Richtung erweitern lässt. Das Produkt kann also noch einiges mehr, als wir in unserem Test unter die Lupe nehmen konnten. *(dr)*

Produkt
Media Gateway für ISDN, DSL und WLAN.

Hersteller
Funkwerk Enterprise Communications GmbH
www.funkwerk-ec.com

Preis
Inklusive zehn IPSec-Tunneln: 681 Euro.

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

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

Remote-CAPI	10
Sicherheit	6
Logging	7
RDP-Funktionen	8
Inbetriebnahme	8

Dieses Produkt eignet sich

optimal für Administratoren, die in einer redundanten Umgebung einfach und günstig für einen sicheren Zugang zu ISDN sorgen müssen.

bedingt für Administratoren, die im Ernstfall die Zeit aufbringen können, ISDN-Hardware in den Ersatzserver einzubauen.

nicht für Administratoren, in deren Netzwerkumgebung Redundanz keine Rolle spielt und eine ISDN-Verbindung zudem nicht essentiell ist.

Funkwerk bintec RT1202

[1] bintec-Homepage
B8T51

Link-Codes

Bleiben Sie in Verbindung!

Folgen Sie uns auf Twitter

twitter.com/ita_blog

Werden Sie ein Fan auf Facebook

www.facebook.de/itanet

Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet

Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

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

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

IT administrator
Das Magazin für professionelle System- und Netzwerkadministration

Clientmanagement mit Windows Intune

Administration aus der Cloud

von Christian Gröbner

Viele Unternehmen setzen auf die beliebten Windows Server Update Services, um ihre Clients mit aktuellen Updates für Microsoft-Produkte zu versorgen. Doch für das Clientmanagement bietet sich mit Windows Intune eine schlanke und cloudbasierte Alternative an. Der Vorteil dabei: Mit Windows Intune können Sie nicht nur Updates an Clients verteilen und deren Updatestatus überwachen. Sie erhalten auch ein erweitertes zentrales Management. Lesen Sie in diesem Workshop, wie Sie Ihre Infrastruktur mit dem Tool aus der Clod verwalten.

Auf dem Microsoft Management Summit in Las Vegas wurde Windows Intune im vergangenen März offiziell veröffentlicht und somit auch der Startschuss für das finale Produkt nach einem Jahr Beta-Phase gegeben. Bei Windows Intune handelt es sich um eine cloudbasierte Lösung von Microsoft zur Verwaltung von Unternehmens-PCs. Zielgruppe von Windows Intune sind hauptsächlich kleine und mittelständische Unternehmen, die entweder selbst keine eigene oder nur eine kleine IT-Infrastruktur besitzen. Mit Windows Intune leitet Microsoft somit eine neue Ära bei der Clientverwaltung ein. Der Dienst bietet in seinem Funktionsumfang neben einer Update-Verwaltung auch ein erweitertes zentrales Management für Clients an. Dies beinhaltet die Vorgabe von Sicherheitsrichtlinien, über welche die Windows Firewall und der Viren-scanner konfiguriert werden können, ein Reporting über den Status und der auf dem Client installierten Software beziehungsweise verwendeten Hardware und zu guter Letzt die Möglichkeit der Remoteunterstützung per Fernzugriff für Administratoren. All dies verdeutlicht, dass Windows Intune eine vielversprechende Cloudlösung zur Verwaltung von Clients darstellt.

Da es sich bei Windows Intune um einen cloudbasierten Dienst handelt, findet die gesamte Konfiguration mittels Browser statt. Doch wer denkt, dass es sich hierbei um eine übliche Website handelt, irrt. Die Oberfläche von Intune ist komplett in Silverlight geschrieben und bietet deshalb sehr viel Bedienerkomfort. Über die URL [1] gelangen Sie zur Anmeldemaske, die zunächst Ihre LIVE-ID wissen möchte, die Sie für die Nutzung von Windows Intune registriert haben. Direkt nach der Anmeldung gelangen Sie zur Systemübersicht, auf der Sie mit einem Blick den Status Ihrer Clients erkennen. Von ihrer Struktur her ähnelt die Verwaltung von Intune einer gewohnten Managementkonsole, wie sie von einem Windows-Server oder -Client bekannt ist. Auf der linken Seite befindet sich die Navigation, in der Mitte die Einstellungen zum gewählten Navigationspunkt und auf der rechten Seite mit dem Navigationspunkt verbundene Aufgaben und Informationen.

Systemübersicht mit schwarzem Brett

Die Systemübersicht ist aufgeteilt in die drei Bereiche Schwarzes Brett, Systemstatus und Warnungen. Anhand dieser drei Sektionen erkennen Sie, ob Handlungsbedarf an Clients besteht oder nicht. Das Schwarze Brett liefert stets aktuelle Informationen darüber, welche Aufgaben aktuell zu erledigen sind, wie zum Beispiel neue Updates für Clients zu genehmigen. Der Systemstatus zeigt Ihnen den Status für den Virenschutz Endpoint Protection, die Aktualität der Clients bezüglich Updates und die Integrität der Agenten auf den Clients an. Sofern Probleme auf einem Client erkannt werden, sind diese im Bereich Warnungen nach Typ aufgeführt.

Computer

Unter dem Punkt "Computer" finden Sie erwartungsgemäß alle Computer aufgelistet, die über Windows Intune verwaltet werden. Ähnlich den Windows Server Update Services können Sie hier zu den bereits bestehenden Gruppen "Alle Computer" und "Nicht zugewiesene Computer" weitere eigene Gruppen erstellen, denen Sie später die Clients zuweisen. In Windows Intune sind diese Gruppen allerdings nicht nur für die Zuweisung von Updates zuständig, sondern es ist auch möglich, bestimmte Sicherheitsrichtlinien, wie etwa Einstellungen für Endpoint Protection, auf Computer einer Gruppe anzuwenden. Die bereits vorhandenen Gruppen "Alle Computer" und "Nicht zugewiesene Computer" sind nicht veränderbar beziehungsweise löschbar. Sie können jedoch über die Auf-

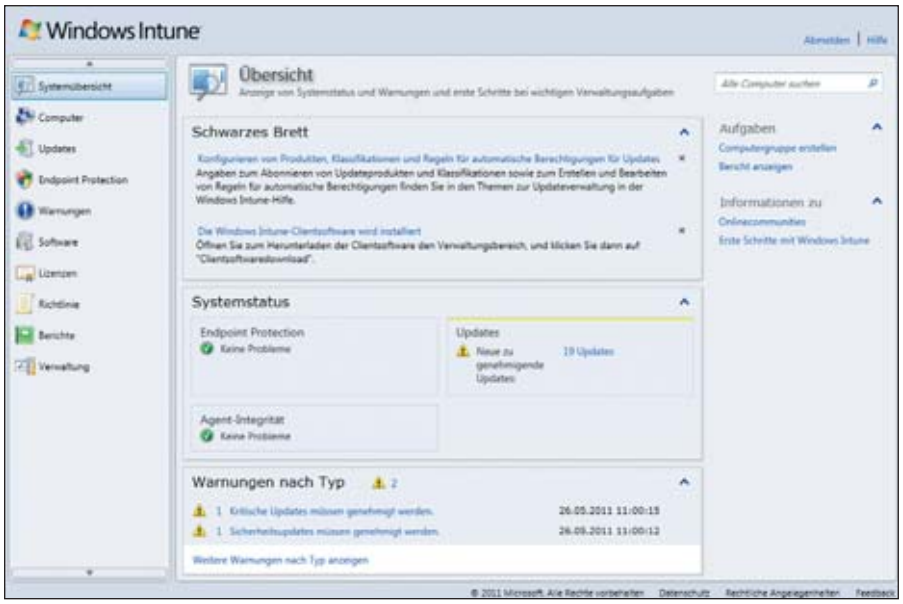


Bild 1: Die Verwaltungsoberfläche von Windows Intune ist in Silverlight programmiert und bietet hohen Bedienkomfort

gabe "Neue Gruppe erstellen" den bereits bestehenden Gruppen weitere hinzufügen und so Ihre Unternehmensstruktur abbilden. Neue Clients landen zunächst in der Gruppe der nicht zugewiesenen Computer. Damit ein Client in die richtige Gruppe gelangt, wählen Sie die entsprechende Gruppe aus und fügen über die Aufgabe "Gruppe bearbeiten" den Client hinzu. Des Weiteren zeigt der Navigationspunkt Computer pro Gruppe den Status der darin enthaltenen Clients an.

Updates

Über den Navigationspunkt "Updates" legen Sie fest, welche Updates den Clients zur Verfügung stehen und installiert werden. Bevor Sie beginnen, Updates zu genehmigen, sollten Sie über die Aufgabe "Klassifizierungen und Produkte" zunächst angeben, für welche Produkte Windows Intune Updates und welche Art von Updates (Servicepacks, Featurepacks, et cetera) bereitstellen soll. Damit Sie nicht jedes Update einzeln genehmigen müssen, können Sie über die Aufgabe "Einstellungen für die automatische Genehmigung" Regeln erstellen, die Ihnen neue Updates wie Definitionsupdates für Endpoint Protection für Ihre Clients automatisch genehmigt. Nachdem Sie die Produkte und Klassifizierungen konfiguriert haben, können Sie über den Navigationspunkt Updates die Updates für Clients genehmigen beziehungsweise gegebenenfalls ablehnen.

Endpoint Protection und Warnungen

Der Navigationspunkt "Endpoint Protection" ist rein informativer Natur und zeigt Ihnen die auf den Clients durch Endpoint Protection erkannten Bedrohungen an. Etwas mehr Informationen bietet der Navigationspunkt "Warnungen". Unter diesem finden Sie sämtliche Informationen und Warnungen, die durch den Windows Intune-Agenten übermittelt wurden. Darin enthalten sind zum Beispiel Warnungen über fehlgeschlagene Updateinstallationen, erkannte Softwareprobleme oder Schwierigkeiten bezüglich der Richtlinienumsetzung.

Software, Lizenzen und Berichte

Die Information darüber, welche Software auf Ihren Clients installiert ist, finden Sie im Navigationspunkt "Software". Übermittelt wird diese Information an Windows Intune durch den Agent. Der Navigationspunkt Software bietet allerdings keine Möglichkeit, Software an die Clients zu verteilen – dies ist mit Windows Intune (noch) nicht möglich. Ob Sie für die auf den Clients eingesetzte Software ausreichend Lizenzen besitzen, erfahren Sie im Navigationspunkt "Lizenzen". In diesem haben Sie die Möglichkeit, Ihre Vertragsdaten von Microsoft-Lizenzverträgen zu hinterlegen und mittels Bericht einen Abgleich zwischen der im Navigationspunkt Software ermittelten Anzahl zu erstellen. So führen Sie auf einfache Art und Weise eine Inventarisierung der eingesetzten Software durch. Weitere Berichte wie der Updatestatusbericht geben Auskunft darüber, welche Updates erfolgreich installiert wurden, fehlschlugen oder noch ausstehen.

Verwaltung

Der letzte Navigationspunkt betrifft die Verwaltung und beinhaltet wichtige Einstellungen für die Funktion von Windows Intune. Darunter fällt die Konfiguration der Warnungsbenachrichtigung, über die Sie einstellen, welche Ereignisse protokolliert werden sollen und bei welchen Ereignissen Intune eine Benachrichtigung per E-Mail auslösen soll. Zudem haben Sie hier die Möglichkeit, weitere Administratoren für die Weboberfläche von Intune anzulegen. Da die cloudbasierte Rechnerverwaltung den bereits erwähnten Agenten voraussetzt, steht dieser im Unterpunkt "Clientsoftwaredownload" zum Herunterladen bereit. Dieser Agent ist zwingend erforderlich für alle Clients, die Sie mit Windows Intune verwalten möchten, und muss somit auch auf diesen installiert werden.

Grundkonfiguration von Windows Intune

Bevor Sie nun loslegen und den Agenten auf Ihren Clients ausrollen, sollten Sie Windows Intune zunächst an Ihr Unternehmen anpassen. Im ersten Schritt aktivieren Sie hierfür die Microsoft-Produkte in der Updateverwaltung von Windows Intune, die Sie in der Firma einsetzen. Diese Einstellung finden Sie unter dem Navigationspunkt "Updates" über die Aufgabe "Klassifizierungen und Produkte auswählen". Sie erhalten daraufhin im Bereich "Produktkategorie" alle Produkte von Microsoft zur Auswahl und können diese durch Setzen eines Hakens im entsprechenden Kontrollkästchen für die Updateverteilung aktivieren. Standardmäßig sind hier bereits die Produkte wie Microsoft Office und die Betriebssystemversionen aktiviert. Kontrollieren Sie die voreingestellte Auswahl und fügen Sie gegebenenfalls weitere Produkte hinzu.

Die Updates von Microsoft werden in verschiedene Klassifizierungen unterteilt, die im Bereich Updateklassifizierung ausgewählt werden können. Durch Aktivierung einer Updateklassifizierung, beispielsweise Definitionsupdates, werden über Windows Intune die Signaturupdates für Endpoint

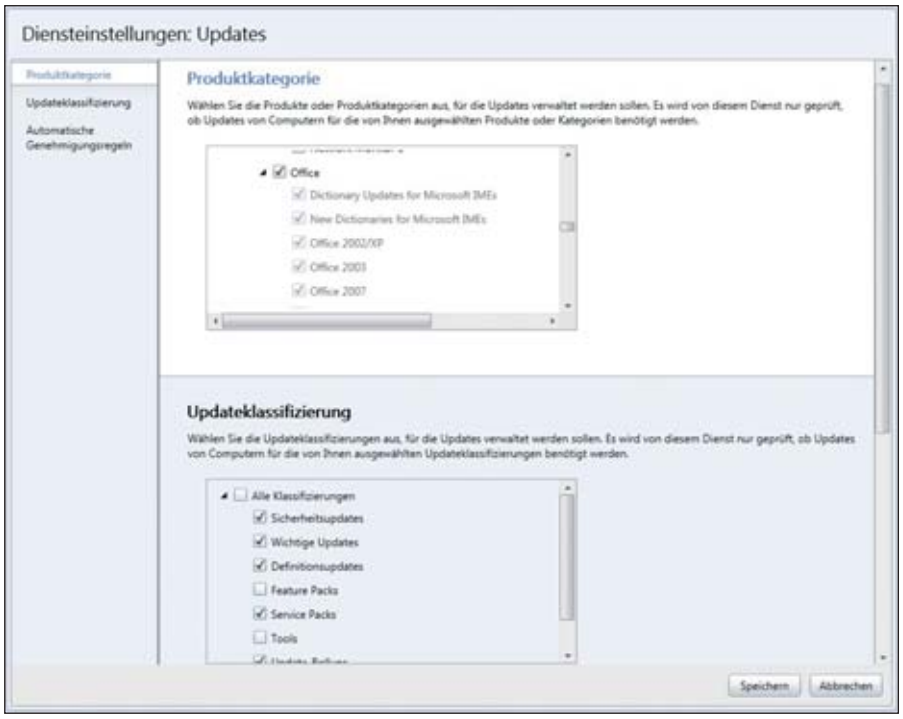


Bild 2: Die Konfiguration von Updates in Windows Intune erfolgt in Klassen

Protection ebenfalls verteilt. Da es mit sehr viel Aufwand verbunden wäre, jedes Update einzeln zu genehmigen, bietet Windows Intune ebenfalls die Möglichkeit, bestimmte Updates aus bestimmten Klassifizierungen und Produkten automatisch über eine Regel für die Installation auf den Clients zu genehmigen. Im Bereich "Automatische Genehmigungsregeln" können Sie über die entsprechende Schaltfläche neue Regeln hinzufügen, die etwa die Signaturupdates für Endpoint Protection automatisch durchwinken.

Nachdem Sie die Updatekonfiguration abgeschlossen haben, gilt es, die Unternehmensstruktur unter dem Navigationspunkt "Computer" abzubilden. Die Abbildung der Unternehmensstruktur in Windows Intune ist ein wichtiger Schritt, den Sie später für die Verteilung der Updates und die Zuweisung von Richtlinien benötigen. Nutzen Sie bereits die Windows Server Update Services (WSUS) und möchten diese durch Windows Intune ablösen, können Sie die Struktur von dort 1:1 abbilden. Über die Aufgabe "Computergruppe erstellen" fügen Sie den bereits vorhandenen Gruppen neue Computergruppen hinzu. Die Computergruppen können auch mehrere Ebenen besitzen, so dass Sie zum Beispiel zunächst zwischen den Standorten und darunter zwischen PCs und Notebooks unterscheiden.

Allein durch die Angabe der Updatekategorien und der Erstellung von Computergruppen werden noch keine Updates und Einstellungen an den Clients vorgenommen. Hierzu benötigen Sie Regeln, über welche die Konfiguration an den Clients vorgenommen wird. Unter dem Navigationspunkt "Richtlinie" ist es möglich über den Menüeintrag "Neu" neue Richtlinien für Ihr Unternehmen zu definieren. Es öffnet sich daraufhin ein Fenster, in dem Sie zunächst angeben müssen, welche Art von Richtlinie Sie erstellen möchten. Es stehen hierfür folgende drei Richtlinienarten zur Auswahl:

- Einstellungen des Windows Intune-Agents
- Einstellungen des Intune-Centers
- Windows Firewall-Einstellungen

Über die erste Art erstellen Sie eine Richtlinie, welche die Einstellungen für Endpoint Protection enthält, wie zum Beispiel den Echtzeitschutz oder die Überprüfungsoptionen, und legen die Einstellungen für Windows Update fest. Über die zweite Art von Richtlinie können Sie die Kontaktinformationen des Supportpersonals hinterlegen, welche die Mitarbeiter im Agenten von Windows Intune auf ihrem Client angezeigt bekommen, für den Fall, dass diese telefonischen Support benötigen. Die letzte Art der Richtlinien steuert das Verhalten der Windows Firewall. Darin konfigurieren Sie etwa, in welchen Netzwerken die Windows Firewall aktiviert sein muss und welche Ausnahmen gegebenenfalls existieren. Erstellen Sie eine neue Richtlinie

Bild 3: Das Definieren der Richtlinien für Clients in Windows Intune – hier für Endpoint Protection

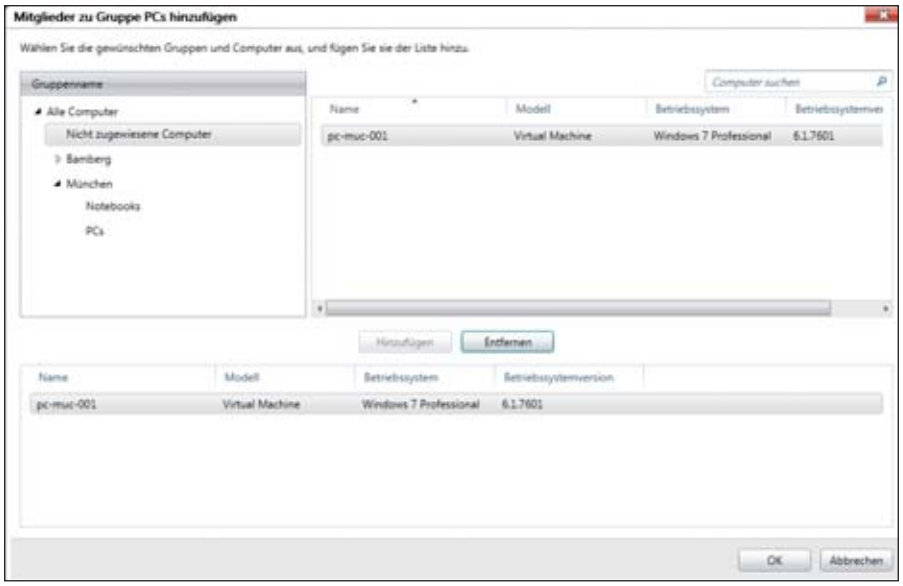


Bild 4: Das Zuweisen von Clients zu Computergruppen. Neue Rechner sind zunächst nicht zugewiesen.

mit den passenden Einstellungen, wie Sie diese für Ihr Unternehmen benötigen. Damit diese Richtlinien auch für bestimmte Computergruppen gültig sind, müssen diese damit verknüpft werden. Aus diesem Grund werden Sie beim Speichern der Richtlinie danach gefragt, mit welchen Computergruppen diese Richtlinie verknüpft werden soll. Durch Setzen der Haken in den Kontrollkästchen der jeweiligen Computergruppe wird die Richtlinie für diese aktiviert.

Agenten herunterladen und verteilen

Die Grundkonfiguration von Windows Intune ist somit erst einmal abgeschlossen und Sie können nun die Clients an Windows Intune anbinden. Dazu müssen Sie auf diesen den Agenten installieren, der unter dem Navigationspunkt "Verwaltung" im Unterpunkt "Clientsoftwaredownload" heruntergeladen werden kann. Entpacken Sie nach dem Herunterladen die komprimierte Datei in einen Ordner auf Ihrem PC. Darin finden Sie anschließend zwei Dateien, von denen eine die Installationsdatei für den Agenten ist. Führen Sie diese aus und folgen Sie den Anweisungen. Nach der Installation nimmt der Agent Kontakt mit Windows Intune auf und registriert sich. Kurz darauf werden auch schon erste Softwarepakete, die als obligatorische Updates gekennzeichnet sind, wie etwa Endpoint Protection oder das Windows Intune Center installiert. Nach spätestens 30 Minuten sollten alle Softwarepakete installiert sein und der Computer in Windows Intune angezeigt werden.

Für Unternehmen mit mehreren Clients ist die manuelle Installation des Agents allerdings nicht wirklich komfortabel. Deshalb kann der Agent auch per Gruppenrichtlinie ausgerollt werden. Dazu müssen Sie den Agenten zunächst entpacken, indem Sie *Windows_Intune_Setup.exe /extract {Ordnername}* in der Eingabeaufforderung eingeben. Sie finden daraufhin zwei MSI-Pakete, einmal für 32 und für 64 Bit, in diesem Ordner. Diese Dateien müssen Sie samt der Datei *WindowsIntune.accountcert* in einen freigegebenen Ordner auf einem Server kopieren, von dem aus der Agent installiert werden kann. Nachdem Sie die Dateien für die Installation bereitgestellt haben, benötigen Sie noch eine Gruppenrichtlinie, über die Sie den Agenten ausrollen. Fügen Sie in der Gruppenrichtlinie unter der Rubrik "Softwareeinstellungen /

Windows Intune ist ausschließlich als monatliche Abonnementlizenz erhältlich und kostet elf Euro im Monat pro PC. Bei größeren Mengen oder bei bereits bestehenden Verträgen, über die Sie bereits ein Clientbetriebssystem erworben haben, sind niedrigere Monatsraten möglich. Für einen Aufpreis von einem Euro können Sie zusätzlich das Microsoft Desktop Optimization Pack erwerben, über das Sie weitere Funktionen wie die Applikationsvirtualisierung (App-V) nutzen können.

Preise und Zusatzpacks

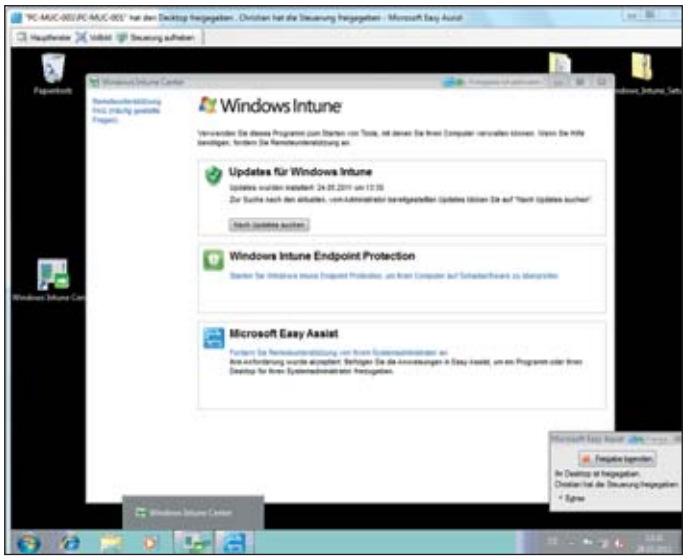


Bild 5: Die Remoteunterstützung von Windows Intune erlaubt den Fernzugriff

Softwareinstallation" das entsprechende MSI-Paket für 32 oder 64 Bit hinzu und weisen Sie anschließend die Gruppenrichtlinie den Organisationseinheiten zu, auf deren Clients der Agent installiert werden soll. Beim nächsten Start des Clients wird der Agent automatisch installiert.

Zuweisen des Clients zu einer Computergruppe

Nachdem der Agent erfolgreich auf dem Client installiert wurde, hat sich dieser zwischenzeitlich bei Windows Intune registriert und erscheint in der Computergruppe "Nicht zugewiesene Computer". Von dort aus müssen Sie ihn in die entsprechende Computergruppe verschieben, damit die von Ihnen definierten Richtlinien auf diesen angewendet werden. Wählen Sie dazu die entsprechende Computergruppe aus und klicken Sie auf die Aufgabe "Gruppe bearbeiten". Im Bereich "Mitglieder" finden Sie die Schaltfläche "Hinzufügen", über die Sie neue Computer der Gruppe hinzufügen. Es öffnet sich daraufhin ein weiteres Fenster, in dem Sie zunächst in der linken Spalte "Gruppenname" die Gruppe "Nicht zugewiesene Computer" auswählen. Sie bekommen daraufhin in der rechten Spalte alle Computer dieser Gruppe angezeigt. Markieren Sie anschließend den Computer und fügen Sie diesen über die Schaltfläche "Hinzufügen" der zu bearbeitenden, ausgewählten Gruppe hinzu. Der Client zieht nach kurzer Zeit die nun für ihn geltenden Richtlinien und wendet diese an. Ebenso werden Updates ermittelt, die für diesen Client genehmigt sind oder noch benötigt werden. Sofern weitere Updates für den Client ausstehen, bekommen Sie dies in Windows Intune angezeigt und müssen diese über den Navigationspunkt "Updates" genehmigen. Die neu genehmigten Updates werden dann zum nächsten Zeitpunkt installiert, der in den für den PC geltenden Richtlinien für Windows Update definiert ist. Sie können aber auch manuell auf dem Client über das Windows Intune Center nach Updates suchen lassen.

Funktionen des Windows Intune Centers

Durch die Installation der obligatorischen Upates für Windows Intune wird auf dem Desktop jedes PCs eine Verknüpfung mit dem Windows Center erstellt. Über dieses können Sie bestimmte Funktionen, wie eine manuelle Suche nach Updates, die Überprüfung des Clients auf Malware mittels Endpoint Protection oder die Anforderung zur Remoteunterstützung, vom Client aus aufrufen.

Sehr interessant ist die Funktion der Remoteunterstützungsanforderung, durch die ein Administrator über das Internet dem Anwender bei Problemen weiterhelfen kann. Nachdem der Benutzer auf den Link namens "Fordern Sie Remoteunterstützung von Ihrem Systemadministrator an" geklickt hat, wird die Anforderung an Windows Intune übermittelt und von dort aus kann diese auch vom Systemadministrator hergestellt werden. Sie bekommen daraufhin in der Systemübersicht von Windows Intune angezeigt, dass eine Remoteunterstützungsanforderung aussteht und können über diese die Verbindung mit dem Client herstellen. Die zugrundeliegende Technik basiert auf Microsoft Office Live Meeting, das die Möglichkeit bietet, untereinander zu chatten, Dateien auszutauschen oder sich den Desktop des Benutzers anzeigen zu lassen, um so in die Sitzung des Benutzers einzugreifen. Der Vorteil für den Administrator liegt darin, dass er fast von jedem Ort der Welt Support leisten kann, denn die Verbindung wird über eine gesicherte HTTPS-Verbindung hergestellt, welche in den seltensten Fällen ein Problem für Firewalls darstellt.

Weitere Bestandteile und Lizenzierung

Das Gesamtpaket von Windows Intune bietet zusätzlich weitere interessante Vorteile für Ihr Unternehmen. Neben den bereits genannten Funktionen enthält es eine Upgradeberechtigung auf Windows 7 Enterprise für alle lizenzierten PCs. Voraussetzung hierfür ist eine vorhandene Betriebssystemlizenz, die als Basis für die Nutzung der Upgradelizenz dient. Ähnlich wie bei Software Assurance von Open-Verträgen sind Sie berechtigt, während der Laufzeit des Windows Intune-Abonnements immer die aktuelle Version des Client-Betriebssystems einzusetzen. Zudem enthält Intune bereits die Lizenz für Endpoint Protection, das Sie somit ebenfalls während der Laufzeit des Intune-Abonnements nutzen dürfen.

Fazit

Windows Intune bietet eine gute Möglichkeit, die Unternehmens-PCs zu verwalten. Auch für Systemhäuser ist Windows Intune interessant, da es damit bei Kunden problemlos möglich ist, externen Support zu leisten oder Updates zu genehmigen. Schade ist allerdings, dass Windows Intune offiziell nur Client-Betriebssysteme unterstützt und die eventuell vorhandenen Server nicht über Intune verwaltet werden können. Da das Zeitalter der cloudbasierten Lösungen noch am Anfang steht und es sich um die erste Version von Windows Intune handelt, bleibt die Hoffnung, dass sich in einer der nächsten Versionen auch Server offiziell damit verwalten lassen. *(dr)*

[1] Anmeldeseite für Windows Intune
B8P11

Link-Codes

Administration virtualisierter Infrastrukturen mit Archipel

Inselverwaltung

von Thorsten Scherf

Virtuelle Maschinen-Instanzen laufen heutzutage auf einer Vielzahl unterschiedlicher Hypervisor-Systeme. Ein einheitliches Management-Tool ist notwendig, um den Zoo an virtuellen Systemen und deren Hosts im Überblick zu behalten und entsprechend zu verwalten. Mit Archipel steht nun ein recht neues Tool dieser Gattung zur Verfügung, das durch seine administrationsfreundliche Oberfläche besticht. Dieser Workshop stellt die Fähigkeiten des Management-Werkzeugs vor und zeigt dessen Inbetriebnahme.

Quelle: pixelio.de

Neben dem Platzhirschen VMware hat auch das Open Source-Umfeld viele sehr elegante und leistungsstarke Virtualisierungswerkzeuge zu Tage gefördert. Die beiden Zugpferde sind hier sicherlich KVM (Kernel-based Virtual Machine) und XEN. Daneben existieren jedoch weitere Lösungen wie beispielsweise VirtualBox, OpenVZ oder auch Linux-Container (LXC). Setzt ein Unternehmen nun unterschiedliche Technologien ein, bedeutet dies im Umkehrschluss auch den Einsatz unterschiedlicher Management-Tools. Dass dies jedoch nicht zwangsläufig der Fall sein muss, ist spätestens seit Erscheinen des Virtualisierung-Frameworks libvirt bekannt. Das Framework bringt diverse Treiber für den Zugriff auf die unterschiedlichsten Virtualisierungstechnologien von Hause aus mit [1] und gestattet somit einen einheitlichen Zugriff auf virtuelle Maschinen unabhängig davon, auf welchem Hypervisor diese laufen.

Als Management-Tools stehen für libvirt auf der Kommandozeile *virsh* und *virt-install* zum Verwalten und Erzeugen von virtuellen Maschinen-Instanzen zur Verfügung und mit virt-manager existiert ein grafisches Frontend. Die Tools müssen dabei nicht zwingend auf dem jeweiligen Hypervisor installiert sein und ein Remote-Zugriff ist ohne weiteres möglich. Um die Daten zwischen der Workstation und dem Hypervisor zu übertragen, existieren diverse Möglichkeiten: So lässt sich beispielsweise der IP-Traffic sowohl über eine ungesicherte wie auch mit TLS geschützte TCP-Verbindung übertragen. Auch der Einsatz eines SSH-Tunnels ist von Haus aus denkbar. Eine Authentifizierung erfolgt wahlweise mittels eines passenden SASL-Plug-Ins, beispielsweise Kerberos, oder aber auch mit Hilfe von X.509-Zertifikaten.

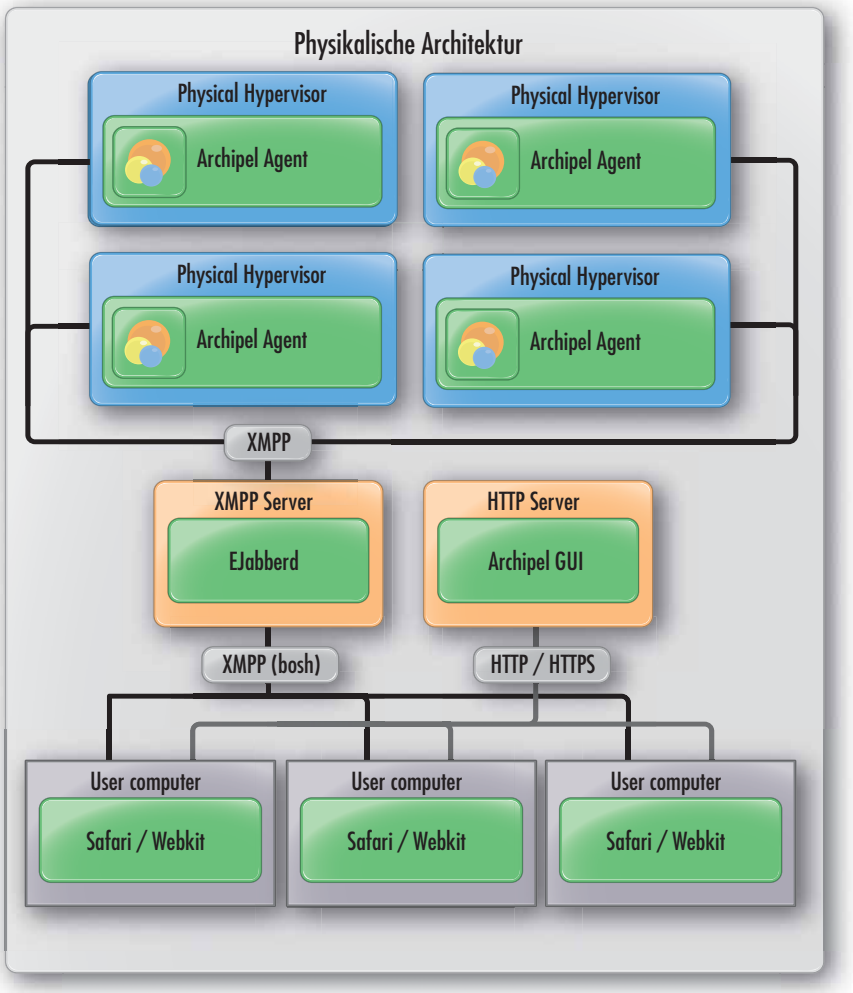


Bild 1: Bei Archipel kommen diverse OpenSource-Komponenten zum Einsatz. Die zentrale Rolle spielt dabei ein XMPP-Server, der für die Echtzeit-Kommunikation zwischen den einzelnen Komponenten verantwortlich ist.

Dank der großen Flexibilität von libvirt kommt es in diversen anderen Virtualisierungs-Projekten zum Einsatz, so beispielsweise in oVirt [2] oder aber auch in Archipel [3]. Archipel ersetzt dabei die etwas angestaubte GTK+-Oberfläche des virt-managers durch eine schicke und moderne Cappuccino-basierte Oberfläche und fügt weitere Features, die beispielsweise virt-manager nicht besitzt, hinzu. Dank des JavaScript-basierten Frameworks erfolgt der Zugriff auf Archipel über nahezu jeden beliebigen Webbrowser – eine zusätzliche Anwendung oder eine lokale libvirt-Installation sind dabei nicht notwendig.

XMPP-Server als zentrale Architektur-Komponente

Archipel besteht aus mehreren Komponenten, die untereinander über das bekannte XMPP-Protokoll (ehemals Jabber) kommunizieren. Die Zustellung von Nach- richten findet somit nahezu in Echtzeit statt. Zentrale Komponente der gesamten Architektur ist ein XMPP-Sever, der als eine Art Nachrichtenzentrale agiert. Die Archipel-Entwickler empfehlen den Einsatz des ejabberd-Servers, jedoch sollte auch jeder andere XMPP-Server funktionieren. Die ejabberd-Software ist Bestandteil sämtlicher Linux-Distributionen und lässt sich somit recht einfach über den jeweiligen Paket-Manager installieren.

Über die Download-Seite von Archipel [4] stehen dann die beiden Komponenten Archipel-Agent und Archipel-Client zur Verfügung. Beim Agent handelt es sich um die Komponente, die auf jedem Hypervisor-System zu installieren ist und als eine Art Bindeglied zwischen dem XMPP-Server und dem libvirt-Framework des Hypervisors dient. Der Agent selbst kommuniziert gar nicht mit dem Hypervisor, sondern überlässt diese Aufgabe libvirt. Somit ist ein Zugriff auf sämtliche Hypervisoren möglich, die libvirt unterstützt. Der Archipel-Client ist dabei die Komponente, die – meistens zusammen mit dem XMPP-Server – auf einem zentralen Management-Server läuft und die jedem zugreifenden Client eine hübsche Weboberfläche präsentiert. Der komplette Client ist dabei in Javascript geschrieben und basiert auf dem Strophe.js-Framework. Archipel erzeugt zur Weiterverarbeitung Cappuccino-Objekte. Diese lassen sich dann mit nahezu jedem beliebigen Javascript-fähigen Webbrowser abrufen. Bild 1 zeigt die Architektur des Archipel-Frameworks.

```
cd /usr/local/src
wget http://ejabberd.jabber.ru/files/
   contributions/xmlrpc-1.13-ipr2.tgz
tar -xzf xmlrpc-1.13-ipr2.tgz
cd xmlrpc-1.13/src
make
cp - a ebin/*.beam /usr/lib/ejabberd/ebin/
```

Listing 1: Installation des ejabberd_xmlrpc-Moduls

```
cd /usr/local/src
svn checkout http://svn.process-one.net/
   ejabberd-modules/
cd mod_admin_extra/trunk/
./build.sh
cp ebin/mod_admin_extra.beam
   /usr/lib/ejabberd/ebin/
```

Listing 2: Installation des mod_admin_extra-Moduls

Installation

Kommt der ejabberd-Server als XMPP-Komponente zum Einsatz, so ist darauf zu achten, dass dieser die beiden Module "mod_admin_extra" und "ejabberd_xmlrpc" enthält. Ist dies nicht der Fall, müssen Sie diese manuell nachliefern. Hierzu verwenden Sie die Sourcen der ejabberd-Module und das Erlang-XMLRPC-Archiv und übersetzen diese. Unter Umständen sind noch die Dateisystem-Pfade im Makefile anzupassen, dies hängt von der eingesetzten Linux-Distribution ab. Die resultierenden beam-Dateien gehören dann in das ebin-Verzeichnis des ejabberd-Servers (Listing 1 und Listing 2).

Hat dies soweit funktioniert, müssen Sie schließlich noch die Konfigurationsdatei des XMPP-Servers anpassen. Hierbei handelt es sich um die Datei */etc/ejabberd/ejabberd.cfg*. Wichtig ist hierbei, dass Sie den lokalen Rechnernamen und die zusätzlich installierten ejabberd-Module korrekt angeben. Listing 3 zeigt eine beispielhafte Konfiguration (die ejabberd Default-Konfiguration wollte in unserem Praxis-Test nicht mit Archipel zusammenarbeiten).

Der Aufruf von */etc/init.d/ejabberd start* aktiviert schließlich den Server. Sollten Fehler auftreten, so finden Sie die entsprechenden Logeinträge in der Datei */var/log/ejabberd/*

```
# /etc/ejabberd/ejabberd.cfg
{loglevel, 4}.
{hosts, ["rawhide.tuxgeek.de","tuxgeek.de",
   "localhost"]}.
{listen,
 [
  {5222, ejabberd_c2s, [
           {access, c2s},
           {shaper, c2s_shaper},
           {max_stanza_size, 65536}
            ]},
  {5269, ejabberd_s2s_in, [
             {shaper, s2s_shaper},
             {max_stanza_size, 131072}
            ]},
  {5280, ejabberd_http, [
            captcha,
            http_bind,
            http_poll,
            web_admin
           ]}
 ]}.
{auth_method, internal}.
{shaper, normal, {maxrate, 1000}}.
{shaper, fast, {maxrate, 50000}}.
{max_fsm_queue, 1000}.
{acl, local, {user_regexp, ""}}.
{access, max_user_sessions, [{10, all}]}.
{access, max_user_offline_messages, [{5000,
   admin}, {100, all}]}.
{access, local, [{allow, local}]}.
{access, c2s, [{deny, blocked},
          {allow, all}]}.
{access, c2s_shaper, [{none, admin},
            {normal, all}]}.
{access, s2s_shaper, [{fast, all}]}.
{access, announce, [{allow, admin}]}.
{access, configure, [{allow, admin}]}.
{access, muc_admin, [{allow, admin}]}.
{access, muc_create, [{allow, local}]}.
{access, muc, [{allow, all}]}.
{access, pubsub_createnode, [{allow, local}]}.
{access, register, [{allow, all}]}.
{language, "en"}.
{modules,
 [
  {mod_adhoc,    []},
  {mod_caps,     []},
  {mod_disco,    []},
  {mod_irc,      []},
  {mod_http_bind, []},
  {mod_last,     []},
  {mod_muc,      [
          {access, muc},
          {access_create, muc_create},
          {access_persistent, muc_create},
          {access_admin, muc_admin}
         ]},
  {mod_offline,  [{access_max_user_messages,
   max_user_offline_messages}]},
  {mod_ping,     []},
  {mod_privacy,  []},
  {mod_private,  []},
  {mod_pubsub,   [
          {access_createnode, pubsub_createnode},
          {last_item_cache, false},
         ]},
  {mod_register, [
          {welcome_message, {"Welcome!",
                     "Hi.\nWelcome to this XMPP
   server."}},
          {ip_access, [{allow, "127.0.0.0/8"},
                  {deny, "0.0.0.0/0"}]},
          {access, register}
         ]},
  {mod_roster,   []},
  {mod_shared_roster,[]},
  {mod_stats,    []},
  {mod_time,     []},
  {mod_vcard,    []},
  {mod_version,  []}
 ]}.
```

Listing 3: Die Konfigurationsdatei des XMPP-Servers

Bild 2: Nach der Installation des Management-Systems steht dieses für erste Zugriffe bereit

ejabberd.log. Um die Installation des Servers abzuschließen, legen Sie noch ein entsprechendes admin-Konto an:

```
# ejabberdctl register admin
  {rawhide.tuxgeek.de} {password}
```

Den Rechnername und das Passwort passen Sie dabei natürlich entsprechend an.

Die Archipel-Client-Installation gestaltet sich um einiges einfacher. Hier laden Sie lediglich die gewünschte Version [4] herunter und entpacken diese in ein beliebiges Verzeichnis. Wichtig ist, dass der Webserver Zugriff auf dieses Verzeichnis erhält. Sollte auf dem Management-System ein aktiviertes SELinux zum Einsatz kommen, so ist nach dem Entpacken des Client-Archives zwingend der richtige SELinux Context auf den Ordner zu setzen, ansonsten kann der Webserver nicht auf die Dateien zugreifen und erzeugt eine Vielzahl von AVC-Deny-Meldungen. Den richtigen SELinux Context setzen Sie wie folgt:

```
# chcon -R -t public_content_r
  /var/www/html/Archipel/
```

Hiermit ist die Installation des Management-Servers beendet. Ein Zugriff mittels eines Webbrowsers sollte zu diesem Zeitpunkt bereits möglich sein. Hierzu bauen Sie einfach eine HTTP-Verbindung zum Management-Server auf. Das Archipel-Client-Installationsverzeichnis geben Sie dabei in der URL an – also beispielsweise *http://rawhide.tuxgeek.de/Archipel/* für eine Installation des Clients auf dem Rechner "rawhide.tuxgeek.de" im Verzeichnis "/var/www/html/". Das DocumentRoot des Webservers kann hier natürlich auch wieder zwischen den einzelnen Linux-Distributionen variieren. Alle in diesem Artikel vorgestellten Beispiele basieren auf einer Fedora 15-Installation. Zur Anmeldung am Archipel-Management-System geben Sie den oben erzeugten Admin-Account an. Wichtig dabei ist, dass Sie den Account mit Domänennamen verwenden, also beispielsweise admin@tuxgeek.de. Als Boch-Server nutzen Sie die URL *http://Management-Server:5280/http-bind/*.

Einbindung der Hypervisoren

Ein Log-In in das System ist zu diesem Zeitpunkt jedoch noch nicht sehr hilfreich, da natürlich noch die Hypervisor-Systeme fehlen. Ohne diese Systeme lassen sich natürlich auch keine virtuellen Maschinen erzeugen. Für den Betrieb eines Hypervisors kommt üblicherweise ebenfalls ein Linux mit libvirt-Installation zum Einsatz. Der gewünschte Hypervisor ist dann entsprechend hinzuzufügen, also beispielsweise XEN, KVM, QEMU oder LXC. Die einzelnen Abhängigkeiten sollte der Paket-Manager der eingesetzten Linux-Distribution selbstständig auflösen. So benötigt ein KVM beispielsweise ein QEMU als Hardware-Emulator sowie einige weitere Python-Tools.

Auf diesem System ist nun der Archipel-Agent als eine Art Proxy zwischen dem XMPP-Server und der lokalen libvirt-Installation zu installieren. Auch hier geht die Installation recht einfach vonstatten: Je nach Vorliebe und Experimentierfreude nutzen Sie entweder den letzten NightlyBuild oder den letzten StableBuild [4]. Noch einfacher gelingt die Installation über den zentralen Python Package Index (PyPi) – dies setzt jedoch eine Internet-Verbindung und das Paket python-setuptools auf den Hypervisor-Systemen voraus. Über den Aufruf von *easy_install archipel-agent* installieren Sie dann den Archipel-Agent auf dem lokalen System.

In der Konfigurationsdatei */etc/archipel/archipel.conf* müssen Sie wieder darauf achten, dass der richtige Rechnername für den lokalen Hypervisor und den zentralen XMPP-Server zum Einsatz kommt. Auch das zuvor eingerichtete admin-Konto des XMPP-Servers geben Sie in der Datei an. Für das Berechtigungs- und Tagging-System auf dem XMPP-Server richten Sie noch zwei PubSub-Nodes ein. Dies geschieht auf den Hypervisor-Systemen durch den Aufruf von:

```
# archipel-tagnode –jid=admin@xmpp-
  server –password=password –create
# archipel-rolesnode
  –jid=admin@xmpp-server
  –password=password –create
```

Ein */etc/init.d/archipel* startet schließlich den Agent-Dienst. Mögliche Fehlermeldungen finden Sie in der Logdatei */var/log/archipel/archipel.log*.

Hypervisor-Management

Nachdem die Installation sämtlicher Archipel-Komponenten abgeschlossen ist, besteht die nächste Aufgabe darin, die Hypervisor-Systeme auf dem Management-Node bekannt zu machen. Da bei Archipel alles ein XMPP-Objekt (oder Jabber-Objekt) ist, sind natürlich auch die Hypervisoren so zu behandeln, indem diese als reguläre XMPP-Kontakte dem Manage-

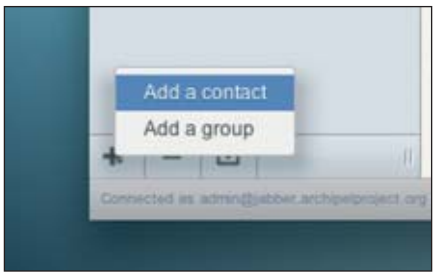


Bild 3: Hypervisor-Systeme werden in Archipel als reguläre XMPP-Kontakte behandelt

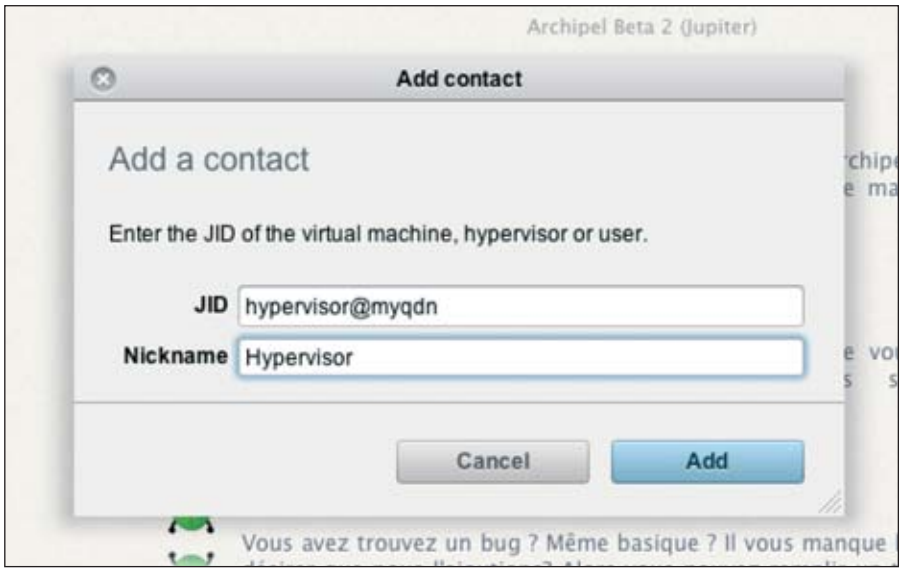


Bild 4: Als JIT-Name ist zwingend der String "hypervisor" gefolgt vom Domänennamen zu verwenden

ment-System hinzugefügt werden. Nach dem Login klicken Sie dazu in der linken unteren Ecke auf das "+"-Zeichen, um den ersten Hypervisor hinzuzufügen. Als JIT-Name verwenden Sie hier Hypervisor@hypervisor-fqdn (also etwa hypervisor@hv01.tuxgeek.de), zusätzlich ist die Angabe eines Alias-Namens möglich. Durch einen Klick auf das Symbol "New VM" in der Icon-Leiste erzeugen Sie eine neue virtuelle Maschine. Hierzu definieren Sie alle notwendigen Eigenschaften entsprechend, also beispielsweise die Größe der virtuellen Disk, den Arbeitsspeicher, Boot-Medium und Netzwerkkonfiguration. Libvirt stellt standardmäßig ein NAT-Gerät zur Konfiguration zur Verfügung, aber natürlich besteht auch die Möglichkeit, eine Bridge einzurichten, sodass Sie die virtuellen Gäste direkt erreichen können.

Zur eigentlichen Installation des Betriebssystems kommt üblicherweise eine virtuelle CD zum Einsatz, oft in Form einer Image-Datei. Diese sucht Archipel im Verzeichnis "/vm/iso/". Das Verzeichnis "/vm" sollte deshalb allen Hypervisor-Systemen zur Verfügung stehen. Dies ist auch deshalb notwendig, da im Verzeichnis "/vm/drives/" die Speicher-Backends der virtuellen Systeme liegen, bei einer Live-Migration zwischen zwei Hypervisor-Systemen müssen diese natürlich Zugriff hierauf haben.

Sollten die hinzugefügten Hypervisor-Systeme bereits über virtuelle System-Instanzen verfügen, so erkennt Archipel diese leider nicht automatisch. Glücklicherweise bringt es aber ein Import-Tool für diese Aufgabe mit. Dieses benötigt zum einen die Deskriptor-Datei der SQLite-Datenbank des Hypervisors (üblicherweise */var/ lib/archipel/hypervisor.sqlite3*) und zum anderen die UUIDs der zu importierenden virtuellen Systeme. Diese ermitteln Sie durch eine einfache libvirt-Abfrage. Mittels *virsh dumpxml {VMName}* präsentiert libvirt sämtliche Konfigurationsdaten der angegebenen VM. Da an dieser Stelle jedoch nur die uuid interessant ist, filtert grep diese entsprechend heraus:

```
# virsh dumpxml webserver01|grep -i
  uuid
<uuid>7f0bbaae-8ac2-11e0-be38-
  00216ab8187e</uuid>
```

Nach einem Stopp des Archipel-Dienstes lässt sich die gewünschte VM nun in die Archipel-Datenbank importieren und taucht danach, neben dem Hypervisor, als regulärer XMPP-Kontakt in der Archipel-Weboberfläche auf:

```
# /etc/init.d/archipel stop
* Stopping Archipel: [OK]
# archipel-importvirtualmachine
  -file /var/lib/archipel/
    hypervisor.sqlite3 \
  -uuid 7f0bbaae-8ac2-11e0-be38-
    00216ab8187e -xmppserver=
    rawhide.tuxgeek.de \
  -name webserver01
SUCCESS: Virtual machine webserver01
  has been inserted with JID \
  7f0bbaae-8ac2-11e0-be38-
  00216ab8187e@rawhide.tuxgeek.de
# /etc/init.d/archipel start
* Starting Archipel: [OK]
```

Da als Echtzeit-Protokoll zwischen allen beteiligten Archipel-Objekten das XMPP-Protokoll zum Einsatz kommt (Bild 6), lässt sich jeder XMPP-fähige IM-Client zur Kommunikation mit den einzelnen Objekten verwenden. Bild 7 zeigt ein Beispiel mit einem konfigurierten Empathy-Client, der hier einfache Status-Abfragen an die VM "webserver01" sendet. Das Tool vnc-viewer stellt schließlich eine Verbindung zum VNC-Server des Hypervisors her, um so einen grafischen Zugriff auf die virtuelle Maschine zu bekommen. Beide Funktionen, also VNC-Viewer und Chat-Client, sind jedoch auch im Archipel-Client selbst integriert. Besonders der Javascript-ba-

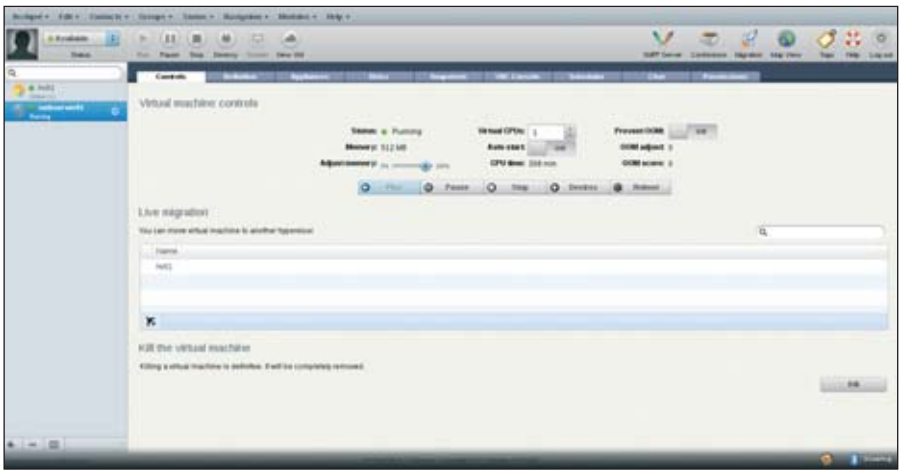


Bild 5: Nach erfolgreichem Import der virtuellen Maschine lassen sich sämtliche Eigenschaften nun über Archipel definieren

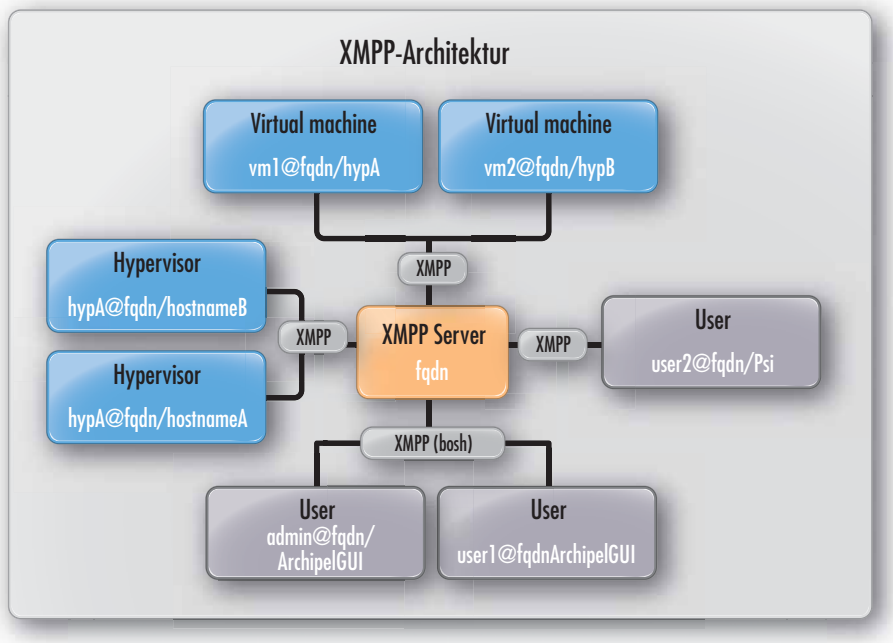


Bild 6: Alle Archipel-Komponenten kommunizieren über das Protokoll XMPP miteinander...

sierte VNC-Viewer innerhalb des Webbrowsers sieht sehr schick aus.

Der integrierte IM-Client ist dabei nicht nur in der Lage, mit dem internen XMPP-Server zu sprechen, sondern unterstützt auch externe Server. Dies kann recht hilfreich sein, falls Sie einmal einen Ratschlag der Archipel-Entwickler benötigen, die immer hilfsbereit Fragen auf dem IRC Freenode Kanal #archipel beantworten.

Zusätzliche Features

Neben dieser netten Spielerei bietet Archipel natürlich auch Funktionen wie das Clustering der Umgebung. Leider bezieht sich dieser Punkt bisher lediglich auf den XMPP-Server, die Hypervisor-Systeme bilden somit aktuell noch einen Single-Point-of-Failure, der sich aber durch den Einsatz weiterer Tools, wie beispielsweise der Red Hat Cluster Suite, beheben lässt. VMCasts erlauben es dem Administrator, vorgefertigte Appliances zu erstellen und zu konfigurieren. Diese stellt Archipel dann über RSS-Feeds den Hypervisoren zum Download zur Verfügung. Dies, und auch der Einsatz von Templates, beschleunigt das Bereitstellen von virtuellen Maschinen enorm.

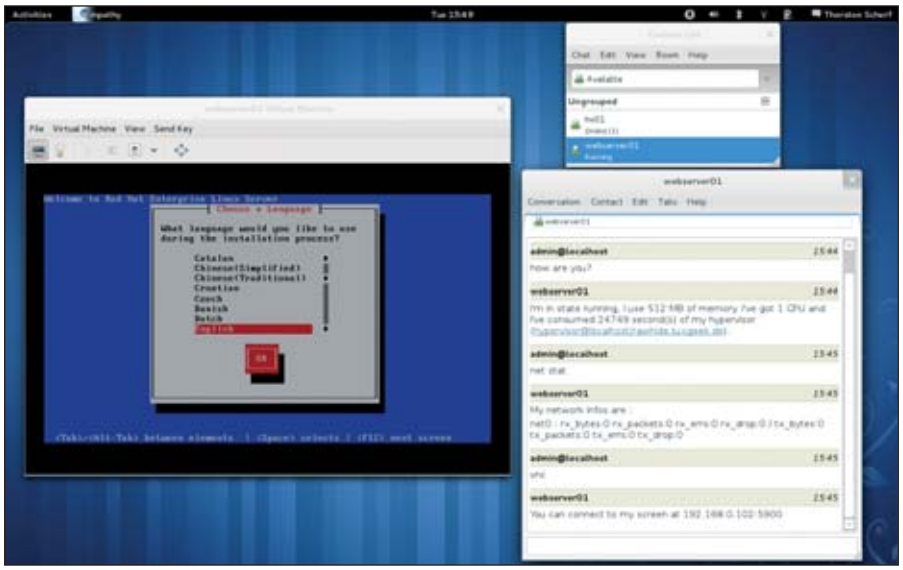


Bild 7: ...dies ermöglicht die Kommunikation mit den einzelnen Komponenten sowie mit einem regulären XMPP-/Jabber-Client, wie beispielsweise Empathy oder Pidgin

Über eine eingebaute Google Maps-Karte lassen sich die Archipel-Objekte geographisch positionieren. Eine Migration von Objekten soll dann auch über das Verschieben auf der Landkarte möglich sein, in der aktuellen Version hat diese Funktion aber leider noch nicht funktioniert. Ein weiteres nützliches Feature von Archipel ist die Möglichkeit, ein einzelnes oder auch mehrere Kommandos an eine Vielzahl von Systemen abzusetzen. Diese lassen sich nämlich in bestimmte Gruppen eingliedern, etwa in die Gruppe Webserver. Kommandos, wie beispielsweise das Starten, Stoppen oder eine Migration, lassen sich dann auf sämtliche Objekte dieser Gruppe anwenden.

Fazit

Abschließend lässt sich festhalten, dass Archipel ein interessantes Tool ist, wenn es um die Verwaltung von vielen virtuellen Maschinen und deren Hypervisor-Systemen geht. Die schicke und ansprechende Weboberfläche bietet keines der anderen Tools, die in dieser Liga spielen. Auf der anderen Seite hat Archipel noch einige technische Mängel und bestimmte Funktionen sind noch nicht implementiert. Auch fehlende Software-Pakete und die mangelhafte Dokumentation machen die Installation und den Betrieb des Frameworks nicht unbedingt einfacher. Schließlich muss sich der verantwortliche Administrator fragen, ob die genannten Features einen zusätzlichen Komplexitätslevel durch den Einsatz von Archipel rechtfertigen. Die meisten grundlegenden Funktionen, die Archipel bietet, sind bereits von Tools wie virt-manager [5] bekannt. *(jp)*

Link-Codes

[1] libvirt-Projektseite
B8P41

[2] oVirt-Projektseite
B8P42

[3] Archipel-Projektseite
B8P43

[4] Archipel-Download
B8P44

[5] virtmanager-Projektseite
B8P45

Gruppenrichtlinienverwaltung mit AGPM 4.0

Lückenfüller

von Klaus Bierschenk

Die Group Policy Management Console – kurz GPMC – ist nach wie vor das Standardwerkzeug, um Gruppenrichtlinien zu bearbeiten. Auch bei Windows Server 2008 R2 hat Microsoft der GPMC keine neuen Funktionen spendiert, die den Umgang mit GPOs sicherer und einfacher gestalten. Abhilfe schafft die Advanced Group Policy Management Console (AGPM), die Software Assurance-Kunden von Microsoft zur Verfügung steht und einige wesentliche funktionelle Lücken der Standard-Konsole füllt. Dieser Artikel stellt die Neuerungen in AGPM 4 vor und wirft einen Blick auf die rollenbasierte Administration von Gruppenrichtlinien.

Gruppenrichtlinien (GPO) sind seit der ersten Stunde des Active Directory ein heikles Thema, denn schließlich dienen sie dazu, mit nur wenigen Mausklicks weitreichende Konfigurationen für Computer oder Benutzer zu verteilen. Dieser Segen kann sehr schnell zum Fluch werden, wie der eine oder andere Administrator sicherlich schon feststellen durfte. Änderungen an einem GPO erfolgen direkt und ohne wenn und aber. Es gibt keinen "Sind Sie sicher?"-Dialog oder einen Hinweis darauf, dass die Änderungen sofort für alle Zielsysteme gelten, die im Wirkungsbereich der geänderten Richtlinie liegen. Je nach Implementierung können tausende Benutzer oder Computer betroffen sein.

Und trotz stetig zunehmender Konfigurations- und Einstellmöglichkeiten, die Microsoft für die verschiedensten Produkte über GPOs bietet, haben die Entwickler zu wenig an die Administratoren gedacht. In Windows Server 2008 R2 präsentieren sich die Werkzeuge, um Gruppenrichtlinien zu bearbeiten, immer noch unverändert und wie zu Zeiten von Windows Server 2003, also weder zeitgemäß noch sicher. Es fehlen Funktionen, die das Testen von Richtlinien unterstützen ebenso wie die Möglichkeit, GPOs offline zu bearbeiten. Eine komfortable Möglichkeit, Berichte zu erstellen, ist ebenfalls nicht vorhanden.

Gerade im Enterprise-Umfeld wäre es für Administratoren hilfreich, Rollen zu bilden, die bestimmten Tätigkeiten im Team entsprechen. Mit Bordmitteln ist dies jedoch nicht möglich und diese Lücken lassen sich nur mit Produkten diverser Hersteller schließen. Microsoft selber hat im Jahr 2006 das Softwarehaus "Desktop Standard" mitsamt dessen Produkt "GPOVault" übernommen [1] und entwickelt es seither unter dem Namen AGPM weiter. Es ist als eines der Produkte im Microsoft Desktop Optimization Pack (MDOP) für Software Assurance-Kunden erhältlich [2].

Installation

AGPM 4.0 [3] kommt mit einer schlanken Installation daher. Je ein Paket für die 32- oder 64-Bit-Variante, entsprechend der Server- oder Clientinstallation. Obendrein gibt es einiges an Dokumentation, etwa einen Planning- wie auch einen HowTo-Guide. Das Serverpaket muss nicht unbedingt auf einem Windows-Server installiert sein, ein Windows-Client (mindestens Windows Vista SP1) ist ausreichend – Microsoft empfiehlt allerdings einen Server. Dieser sollte dann wenigstens mit Windows Server 2008 laufen, besser R2. AGPM-Server bezeichnet übrigens den Computer, auf dem das zentrale Archiv für die Offlinebearbeitung der GPOs liegt und auf den die AGPM-Clients über Port 4600 zugreifen. Genauso kann der AGPM-Client auf einem Windows-Server installiert werden. Eine Übersicht über die möglichen Konstellationen bei der Installation und die jeweiligen Voraussetzungen enthält der mitgelieferte Planning Guide.

Ein SQL Server wird für das Archiv übrigens nicht benötigt, dies liegt auf dem AGPM-Server in Form von XML-Dateien. Das vereinfacht Aspekte wie Datensicherung oder Migration (mehr dazu später im Artikel). Die Installation kommt ohne weitreichende Eingriffe im Active Directory aus. Zum Beispiel sind keine Modifikationen am Schema notwendig. Selbst das Dienstkonto, unter dessen Kontext der AGPM-Service läuft, kommt ohne Domänenadministrator-Privilegien aus. Eventuell nicht vorhandene Komponenten wie das .NET Framework installiert die Setuproutine selbstständig.

Die Installation der AGPM auf einem Server bedeutet nicht, dass nun generell und überall in der Domäne auf Basis der AGPM gearbeitet werden muss. Der Einsatz von AGPM-Client und -Server stellt lediglich ein Hilfsmittel dar. Es verhindert nicht, dass ein anderer Administrator – quasi ohne AGPM – eine Policy an den AGPM-Prozessen vorbei bearbeitet. Dass dies Probleme verursachen kann und wie sich dem begegnen lässt, besprechen wir im weiteren Verlauf.

Funktionslücken der GPMC geschlossen

Nach dem Abschluss der Setuproutine des AGPM-Servers sieht der Administrator lediglich den "AGPM Service"-Dienst und das bereits erwähnte Archivverzeichnis. Soll auf dem Server gleichfalls mit der AGPM gearbeitet werden, muss der Client ebenfalls installiert sein. Nach dessen Installation wird es schon spannender, wenn es auch auf den ersten Blick nicht viel zu sehen gibt. Die

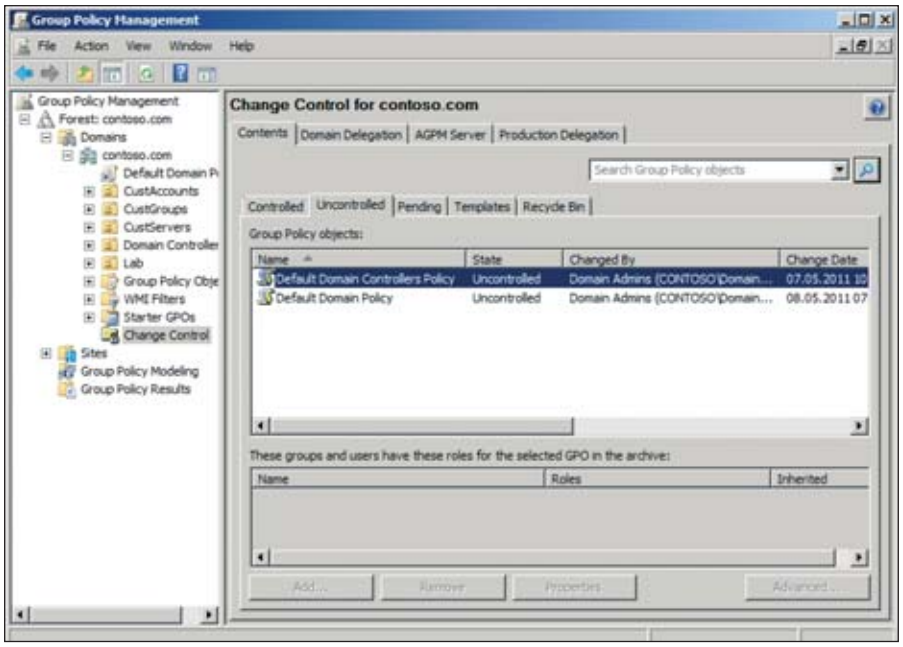


Bild 1: Die AGPM-Verwaltungskonsole integriert sich in die GPMC

AGPM-Funktionen werden nämlich allesamt in der bekannten GPMC integriert. Sie finden sich unter dem Knoten "Change Control" in der Konsolenstruktur wieder und schließen hier an zentraler Stelle genau die eingangs erwähnten Funktionslücken.

Ein Klick auf "Change Control" stellt eine Verbindung mit dem beim Setup angegebenen Server her und der erste Blick auf die AGPM hinterlässt einen aufgeräumten Eindruck. Die oben angeordneten Register enthalten die elementaren Einstellungen der AGPM: "Domain Delegation" bietet neben der Angabe eines SMTP-Servers für den Versand von Mitteilungen die Möglichkeit, Benutzer und Gruppen in der AGPM mit bestimmten Rollen auszustatten. Hier existieren neben "Full Control" die Rollen "Reviewer", "Editor" und "Approver". Die Namen der Rollen lassen vermuten, welche Möglichkeiten ihre Mitglieder haben. Im Register "AGPM Server" wird der Archivserver samt Port bestimmt. Hier legt der Administrator auch fest, wie mit zu löschenden GPOs verfahren wird, um beispielsweise eine definierte Anzahl von Versionen eines gelöschten GPOs aufzubewahren.

Rollenbasierte Administration

Die administrativen Rollen der AGPM verwalten Sie im Register "Domain Delegation". Beim ersten Start der AGPM ist hier lediglich die Gruppe oder der Benutzer enthalten, den Sie bei der Installation angegeben haben. Unter diesem Kontext lassen sich nun alle weiteren Rollen je nach Bedarf hinzufügen.

Für Emil, ein Beispiel-Administrator mit der Rolle "Editor", könnte sein Benutzerkonto direkt zugewiesen sein (vergleiche Bild 2). Seine Rollenzugehörigkeit kann aber auch genauso über seine Mitgliedschaft in einer Active Directory-Gruppe zustande kommen, die in der AGPM einer Rolle zugeordnet ist. Die ansonsten im AD bekannte Arbeitsweise bei der Vergabe von Rechten und der Suche nach Objekten wird hier nahtlos fortgeführt.

Ein Administrator in der Rolle "Editor" darf sich in der AGPM frei bewegen. Kommt es irgendwo zu einer Konfiguration, bei der seine Rechte nicht ausreichen, beispielsweise beim Hinzufügen eines GPOs zum AGPM-Archiv, erscheint ein Dialog mit dem Hinweis darauf, dass eine Benachrichtigung an ein Approver-Postfach versendet wird. Eine Anforderung landet unterdessen im Register "Pending" als Request und wartet auf die Freigabe durch einen "Approver" (ist bei den Einstellungen kein SMTP Server eingetragen, landet der Request lediglich im Ordner "Pending").

Der "Approver" kann dann schließlich die Änderungen final freigeben, hat aber nicht das Recht, GPOs zu bearbeiten. Je nach Kontext sind Menüpunkte und Befehle deaktiviert. Öffnet ein Administrator in der Rolle "Approver" das Kontextmenü für ein GPO, ist der Befehl zum Editieren einer Gruppenrichtlinie ausgegraut. So ergänzen sich die Rollen in der AGPM und verschiedene Admins können unterschiedliche Aufgaben wahrnehmen. Vom Vieraugenprinzip bis hin zur Abteilung, die für eine Qualitätssicherung zuständig ist, ist in der AGPM alles möglich.

Sollte es erforderlich sein, bestimmte Rollen nur für einzelne GPOs anzuwenden, dürfen Rollen auch auf Ebene der Policies zugewiesen werden. In diesem Fall gilt das Gleiche, als würden die Rollen übergeordnet definiert, nur eben für das einzelne GPO.

Administratoren, die in den Rollen "Approver" und gleichzeitig "Editor" sind, können zwar GPOs bearbeiten und die Modifikationen selber auch gleich freigeben, haben aber nicht das Recht, Berechtigungen zu vergeben. Dies darf nur ein Mitglied der Rolle "Full Control", die auch gleichzeitig Mitglied in allen anderen Rollen ist. Als letzte Rolle steht noch der "Reviewer" zur Verfügung, der eine reine Lesefunktion innehat, beispielsweise um einen Bericht zu erstellen oder die Historie auszuwerten. Alle Rollen im Überblick:

- AGPM Administrator (Full Control): Diese Rolle bündelt alle anderen Rol-

Die wichtigsten Funktionen von AGPM im Überblick

- Offlinebearbeitung
- Kein direktes Editieren der GPOs im Produktivsystem
- Rollenbasierte Administration
- Bearbeiten und Freigeben von Änderungen über eigene Rollen
- Verbessertes Reporting
- Berichte von GPOs älteren Datums und Vergleiche mit älteren Versionen
- Volle Integration in die GPMC
- Keine zusätzlichen Admintools
- Papierkorb
- Kein direktes Löschen von Policies mehr
- Export- und Importmöglichkeiten
- Einfacher Transfer von GPOs mittels CAB-Files über Forest-Grenzen hinweg

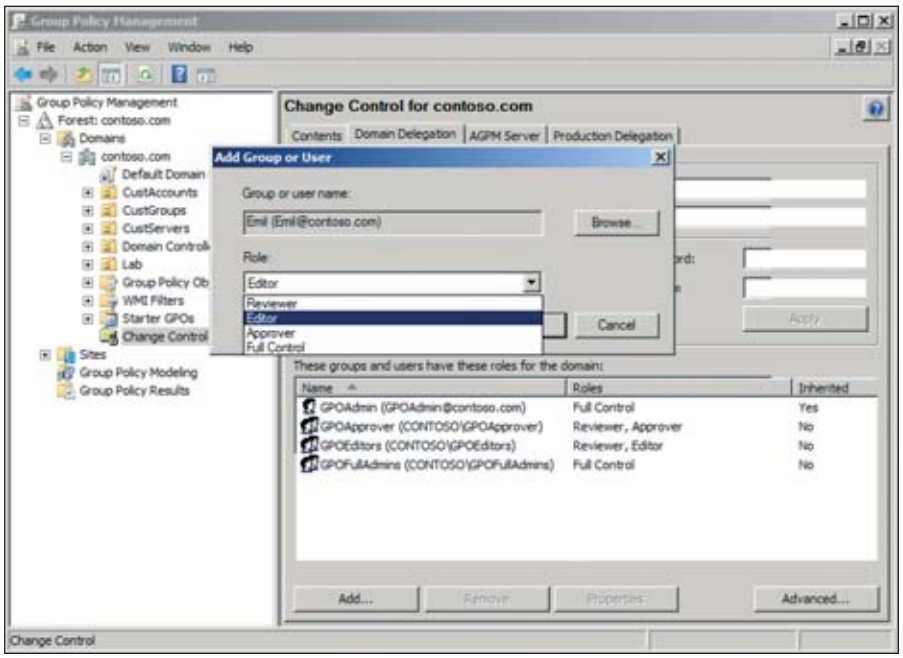


Bild 2: Unserem Beispiel-Admin Emil wird die Rolle "Editor" in AGPM zugewiesen

len und hat zusätzlich das Recht, Rollen und Berechtigungen zu verwalten.

- Editor: Diese Rolle bearbeitet GPOs. Jede Änderung muss von einem Approver freigegeben werden, bevor sie in das Active Directory zurückgeschrieben wird.
- Approver: Die Rolle gibt Änderungen frei, die durch einen Editor erfolgt sind.
- Reviewer: Kann GPOs anzeigen und Reports erstellen. Alle anderen Rollen sind Mitglied dieser Rolle.

GPO-Bearbeitung in der Praxis

Wie das in der Praxis aussieht, betrachten wir an unserem Beispiel-Admin Emil in seiner Funktion als "Editor" und seinem Kollegen "Anton" als denjenigen, der Änderungen freigeben kann. Sind Emil und Anton gleich qualifiziert und in einem Team, wäre es durchaus auch denkbar, die Rollen von Zeit zu Zeit zu wechseln. So ließe sich dauerhaft nach dem Vieraugenprinzip arbeiten und die Wahrscheinlichkeit von Flüchtigkeitsfehlern verringern.

Emil navigiert in der AGPM unter "Change Control" im Register "Controlled" zu dem gewünschten GPO und selektiert es mit der rechten Maustaste. Über das Kontextmenü wählt er "Check Out". In dem "Check Out"-Dialog trägt er dann einen Kommentar ein. Dieser taucht in späteren Reports auf und verbessert die Nachvollziehbarkeit von Änderungen. In der Liste mit den GPOs [4] wird das ausgecheckte Objekt rot markiert dargestellt. Emil wählt jetzt wiederum über das Kontextmenü den Befehl "Edit" und der Group Policy Editor öffnet sich. Ab hier ist alles wie gewohnt und das Richtlinienobjekt wird bearbeitet. Der Unterschied zur Arbeitsweise ohne AGPM ist lediglich der, dass die Modifikationen nicht am "lebenden" Objekt erfolgen, sondern im Offlinearchiv. Auch wenn Emil fertig ist und das GPO wieder eincheckt, sind die Änderungen immer noch nicht produktiv. Dies geschieht erst über den Befehl "Deploy". Zumindest würden Sie dies, wenn Emil an dieser Stelle ebenfalls "Approver" wäre. Da er das aber nicht ist, wird im nächsten Dialog die erwähnte Benachrichtigungsmail generiert, die Anton über die benötigte Freigabe informiert.

Antons Aufgabe ist es nun, im Register "Pending" seiner Arbeit nachzugehen. Da die Policy auf die ganze Webserverfarm wirkt, möchte er auf Nummer sicher gehen und prüfen, ob Emil alles richtig gemacht hat. Der Status des GPOs ist "Pending deploy" und das Kontextmenü enthält alle Befehle, die für Anton gemäß seiner Rolle Sinn machen.

Eine zusätzliche Möglichkeit, die Qualität zu überprüfen, bietet sich Anton in Form eines "Differences Report". Dieser listet alle Änderungen seit dem letzten Deploy auf und zeigt sehr schnell Änderungen an dem GPO an. Über Hyperlinks navigiert Anton komfortabel in dem Report. Möchte Anton noch mehr wissen, kann er auch die Historie zu dem GPO anzeigen. Dort lassen sich zwei beliebige Zeitpunkte selektieren und ein Bericht mit Unterschieden gibt Aufschluss darüber, was zu einem bestimmten Datum und was heute in dem GPO enthalten ist. Die Unterschiede sind in dem Bericht in grüner Farbe dargestellt. Wenn sich Anton sicher ist, dass alles passt, gibt er die Änderungen mittels "Deploy" frei und erst jetzt sind die Änderungen im Active Directory und werden von den Zielsystemen sukzessive verarbeitet.

Überschneidende Änderungen an GPOs verhindern

Administratoren, die mit einer der ersten Versionen der AGPM gearbeitet haben, kennen das Problem, dass sich GPOs, obwohl sie unter Kontrolle der AGPM waren, nebenbei und direkt bearbeiten ließen, beispielsweise von einem Domänen-Admin auf einem Domain Controller ohne AGPM-Client. Dies hat den Nachteil, dass, wenn eine auf direktem Wege modifizierte GPO über die AGPM bearbeitet wird, die Änderungen überschrieben werden. Denn es wird immer zuerst das Original aus dem Offlinearchiv geladen und bearbeitet. Dies vollzieht sich zum Ärger für denjenigen, der das GPO direkt bearbeitete.

Das Ganze ließe sich verhindern, indem der Administrator vor den Änderungen über den Befehl "Import from Production" die Version im Archiv durch das Original aus dem Active Directory ersetzt. Das ist jedoch in den meisten Fällen nicht gewünscht, da

AGPM-Datensicherung

Das Offlinearchiv befindet sich auf dem AGPM-Server in Form von XML-Dateien. Neben der grundlegenden Sicherung des Servers macht es Sinn, das komplette Verzeichnis zu kopieren. Tests haben gezeigt, dass es bei einer Neuinstallation ausreicht, wenn vor dem Setup die gesicherten Dateien in das Archiv-Verzeichnis zurückkopiert werden. Wird bei der Installation genau dieses Verzeichnis angegeben, erkennt dies das Setup und übernimmt das darin enthaltene Archiv. Das Verfahren funktioniert auch bei einer Migration von einer älteren AGPM-Version auf die aktuelle Version 4.0. Fällt der Server aus und muss neu installiert werden, ist die AGPM-Funktionalität schnell wiederhergestellt.

so niemand nachvollziehen kann, wer welche Änderungen vorgenommen hat. Dieses Verhalten lässt sich zwar immer noch provozieren, allerdings lässt sich technisch ein Riegel davorschieben. Die Lösung liegt im Register "Production Delegation". Hier werden die Zugriffsrechte für GPOs eingeschränkt, die in der AGPM eingecheckt sind. Damit lässt sich technisch verhindern, dass jemand ohne AGPM ein GPO modifiziert. Ein mögliches Szenario könnte sein, die "Domain Admins" zu entfernen und stattdessen zum Beispiel die Gruppe AGPM-Admins einzutragen. So wird verhindert, dass zweierlei Änderungen an einem GPO stattfinden, weil das Thema mit den Gruppenrichtlinien in zentraler Hand liegt.

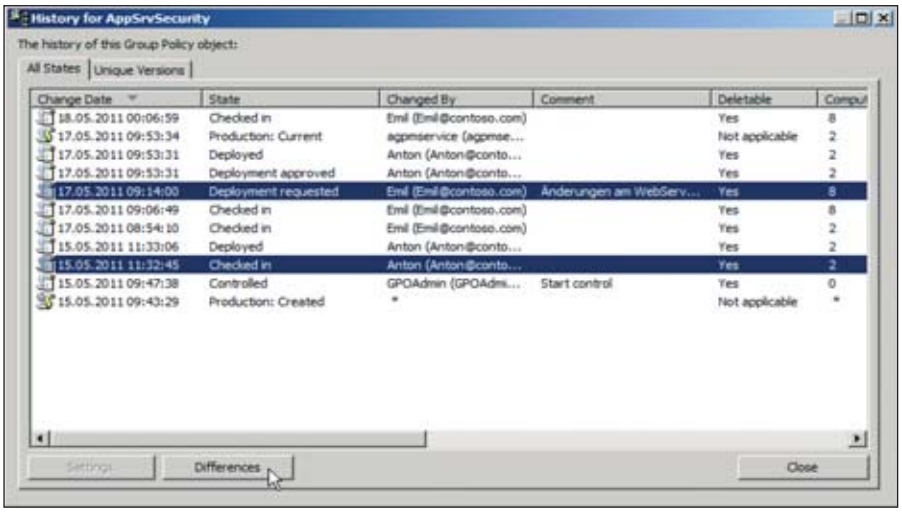


Bild 4: Alle Arbeiten an GPOs dokumentiert AGPM ausführlich

Weitere Funktionen

Bei genauerem Hinsehen zeigen sich dem Administrator weitere Möglichkeiten, die zwar nicht zu den Kernfunktionen der AGPM gehören, die aber die tägliche Arbeit vereinfachen. Da wäre zunächst einmal die Möglichkeit der Filterung und der Suche. Befindet sich in den Registern, wie beispielsweise "Controlled", eine größere Anzahl an Richtlinien, kann die Liste der angezeigten Objekte durch Angabe eines sogenannten komplexen Suchstrings eingeschränkt werden. Dieser folgt der gleichen Syntax wie die Suche im Windows Explorer. Dies dürfte in Umgebungen willkommen sein, die eine hohe Anzahl Gruppenrichtlinien besitzen. Der Suchstring ist wie folgt aufgebaut: *Spaltenname:Suchstring*, wobei "Spaltenname" exakt dem Namen aus der angezeigten Spalte entspricht. Dadurch wird die Filtermöglichkeit zwar komplex, ist aber wegen der einfachen Syntax alles andere als kompliziert.

Hilfreich sind auch die mitgelieferten Administrativen Templates, um eine Protokollierung bei Problemen mit der AGPM zu steuern oder auch um bestimmte Funktionen in der GUI auszublenden. Die Settings selber sind im Gruppenrichtlinieneditor an verschiedenen Stellen zu finden. Welche Einstellungen wo liegen und was sie bewirken, darüber gibt die mitgelieferte Dokumentation Auskunft.

Eine weitere interessante Funktion bietet der Export einer Gruppenrichtlinie. Dieser ermöglicht den Transport von GPOs über Forest-Grenzen hinweg. Hierzu wird die Policy in eine CAB-Datei exportiert und in einer anderen Umgebung wieder importiert. Dies erfordert auf beiden Seiten den AGPM-Client und dient wohl eher für Testzwecke. Interessant ist es aber trotzdem, da es eine sinnige und mitunter zeitsparende Funktion sein kann, insbesondere wenn es darum geht, umfangreiche Templates im Lab zu bauen.

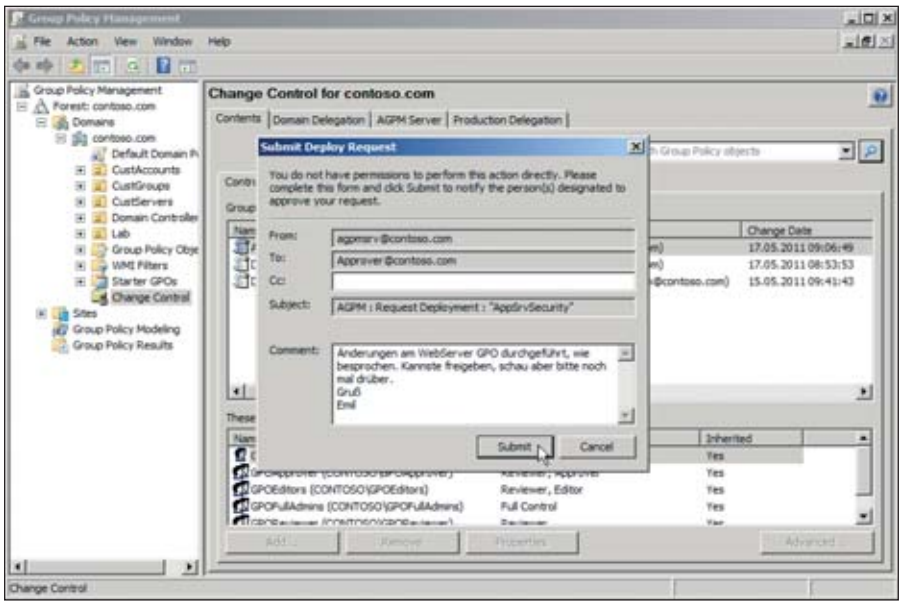


Bild 3: Administrator Emil hat seine Änderungen in der AGPM fertig gestellt und sendet diese zur Freigabe

Fazit

Die AGPM bietet eine Menge Vorteile für die Verwaltung domänenbasierter Gruppenrichtlinien. Dazu zählt insbesondere die intuitive Integration in die GPMC. Administratoren, die bis dato noch ohne eine Erweiterung ihre GPOs verwalten, sei ein Blick auf die AGPM empfohlen. Der Implementierung muss freilich ein solides Rollenkonzept zugrunde liegen, aber dann liefert sie gekonnt die Funktionen, die in der GPMC von Haus aus nicht enthalten sind. Ein erster Blick im Lab ist einfach, ist doch die Installation mit wenigen Handgriffen erledigt. Auch in der Produktion kann sie bedenkenlos getestet werden, solange hierfür eigene Testobjekte herhalten. *(jp)*

[1] Desktop Standard Bought by Microsoft
B8P21

[2] Microsoft Desktop Optimization Pack (MDOP)
B8P22

[3] Advanced Group Policy Management
B8P23

[4] Windows Server Gruppenrichtlinien
B8P24

Link-Codes

SharePoint 2010 im Internet veröffentlichen (1)

Applikationen weltweit

von Thomas Joos

SharePoint 2010 spielt seinen ganzen Nutzen dann aus, wenn auch mobile Anwender auf das System zugreifen können. Dazu ist es notwendig, die Dienste zu veröffentlichen. Neben dem Forefront Threat Management Gateway 2010 – TMG 2010 – bietet Microsoft für diese Aufgabe noch das Forefront Unified Access Gateway 2010 – UAG 2010 – an. Hierbei handelt es sich um eine erweiterte Version des TMG, die besser für SharePoint geeignet ist. In diesem Workshop veröffentlichen wir zunächst Schritt für Schritt eine SharePoint-Seite mit TMG 2010 und anschließend Seiten und Applikationen mit UAG 2010.

Der Vorteil der größeren Forefront Unified Access Gateway 2010 (UAG)-Version ist die Unterstützung von AAM (Alternative Access Mappings, alternative Zugriffszuordnungen). Mit dieser Funktion können Sie URLs zu SharePoint frei definieren und zu den internen Webanwendungen umleiten. Dazu leiten Sie die externe Adresse zum UAG, zum Beispiel *https://www.it-administrator.de*. UAG schickt diese Anfrage dann an die interne URL zu SharePoint weiter (etwa *http://sps01.it-administrator.local*). Zusätzlich kann das UAG die Webanwendungen von SharePoint direkt unterstützen und in die Veröffentlichung einbinden. Das Veröffentlichungskonzept des UAG 2010 funktioniert etwas anders als im TMG, wo Sie einzelne Websites im Internet zur Verfügung stellen. Das UAG bietet hingegen eine eigene Portalanwendung an.

Dabei ist keine weitere Authentifizierung mehr notwendig, da sich die Anwender bereits beim Portal angemeldet haben. Der Datenverkehr zwischen internem Netzwerk und dem Client läuft verschlüsselt ab. Wollen Sie nur eine Website veröffentlichen, reicht in den meisten Fällen das TMG aus. Seine Vorteile spielt das UAG 2010 aus, wenn Sie mehrere Websites, Dateifreigaben, Remote Desktops oder OWA anbinden wollen. Allerdings ist der Preis des UAG wesentlich höher als der von TMG 2010.

Service Packs und Updates installieren

Haben Sie das TMG 2010 installiert, sollten Sie zusätzlich noch das aktuelle Service Pack aufspielen sowie zusätzliche Updates, die auf das Service Pack aufbauen. Das TMG 2010 unterstützt erst ab dem Service Pack 1 [1] optimal SharePoint 2010. Haben Sie die 22 MByte große Datei für das SP1 heruntergeladen, installieren Sie dieses per Doppelklick auf die *.msp-Datei. Damit SharePoint 2010 optimal mit dem TMG 2010 zusammenarbeitet, sollten Sie zusätzlich zum TMG 2010 SP1 noch das Software Update 2 für Forefront Threat Management Gateway (TMG) 2010 Servicepack 1 [2] installieren. Microsoft veröffentlicht ständig Updates für TMG, die Sie auch regelmäßig einspielen sollten.

Wie für Exchange gibt es auch für den ISA/TMG ein kostenloses Analysetool von Microsoft, das die Installation und Konfiguration eines ISA/TMGs überprüfen kann. Der TMG Best Practise Analyzer [3] analysiert dabei auf Basis der Konfigurationsdaten, ob ein TMG fehlerfrei installiert wurde und gibt im Bedarfsfall entsprechende Meldungen aus.

Weblistener für SharePoint konfigurieren

Soll ein TMG-Server Anfragen aus dem Internet entgegennehmen, zum Beispiel um diese an interne SharePoint-Server weiterzuleiten, benötigen Sie einen Weblistener. Zuvor sollten Sie das Zertifikat, das Sie für SSL auf dem SharePoint-Server verwenden, exportieren und auf dem TMG importieren. Dazu gehen Sie vor wie bei einer Veröffentlichung von Exchange. Achten Sie aber beim Einsatz einer zweiten Firewall darauf, SSL-Anfragen aus dem Internet zum Port 443 des TMG weiterzuleiten.

Bevor Sie SharePoint veröffentlichen, sollten Sie daher einen solchen Weblistener konfigurieren, mit dem das TMG auf Anfragen aus dem Internet wartet. Diesen erstellen Sie in der TMG-Verwaltungskonsole, indem Sie zunächst in der Konsole auf "Firewallrichtlinie" klicken und dann auf der rechten Seite die "Toolbox" aufrufen. Wählen Sie dann "Netzwerkobjekte" aus und klicken Sie mit der rechten Maustaste auf "Weblistener" und wählen Sie "Neuer Weblistener". Anschließend klicken Sie auf der Seite Weblistener auf "Neu", um die notwendigen Konfigurationen vorzunehmen. Geben Sie dem Listener zunächst einen Namen, wie zum Beispiel "SharePoint-Listener".

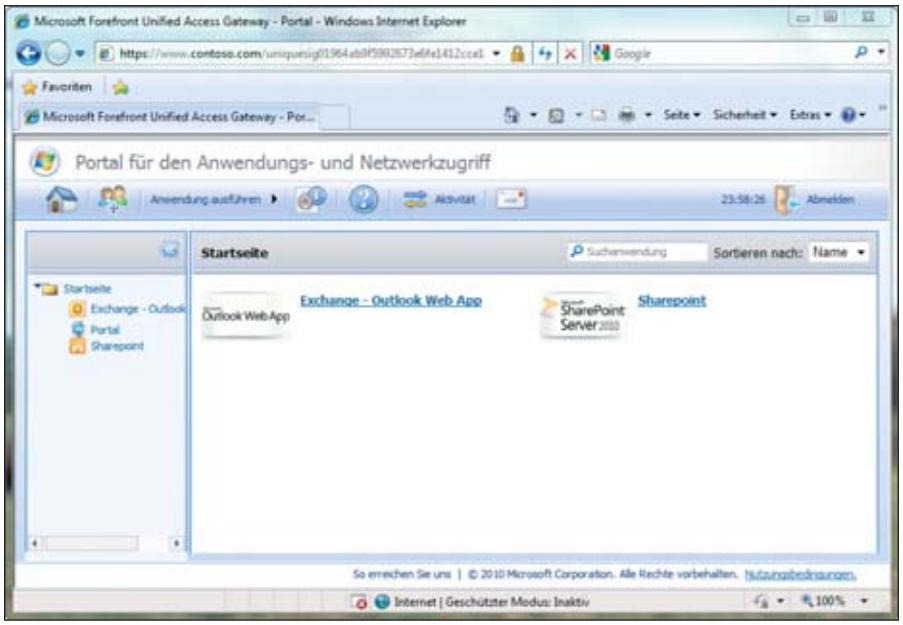


Bild 1: Das Portal des UAG 2010 stellt nicht nur Seiten, sondern auch Webanwendungen bereit

Als Nächstes legen Sie fest, ob der Listener auf SSL hören soll. Aktivieren Sie daher die Option "Sichere SSL-Verbindung mit Clients erforderlich". In diesem Fall bauen die Anwender über das Internet per SSL eine Verbindung zum TMG auf, unabhängig davon, ob Sie zwischen TMG und SharePoint oder auch intern für den SharePoint-Zugriff SSL aktiviert haben. Auf der nächsten Seite legen Sie die Schnittstelle fest, auf die Ihr neuer Listener hören soll, also das "Netzwerk Extern". Hierbei handelt es sich um die Schnittstelle, die mit dem Internet verbunden ist. Klicken Sie danach auf die Schaltfläche "IP-Adressen auswählen" und aktivieren Sie die Option "Angegebenen IP-Adressen auf dem Forefront TMG-Computer im ausgewählten Netzwerk". Wählen Sie die IP-Adresse aus, mit der Ihr TMG-Server mit dem Router oder dem Internet verbunden ist. Klicken Sie auf "OK" und wechseln Sie anschließend auf die nächste Seite des Assistenten.

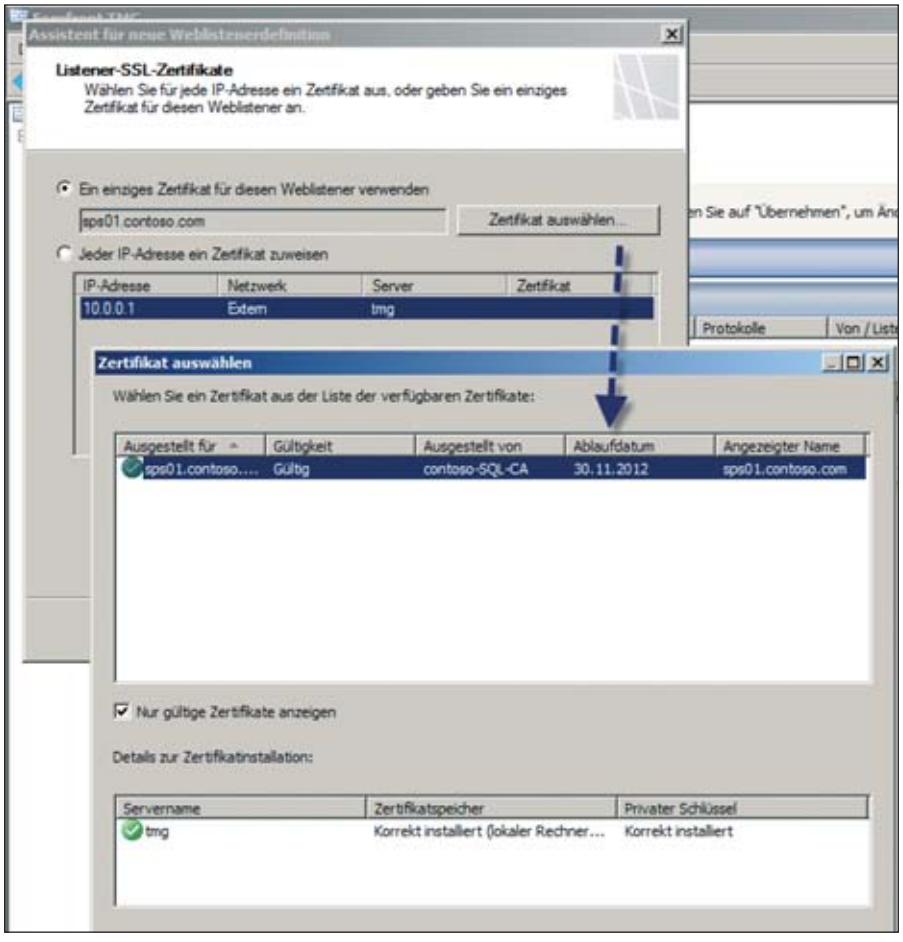


Bild 2: Auswahl eines Zertifikats für den SSL-Verkehr

Auf der nächsten Seite legen Sie zunächst die Option "Ein einziges Zertifikat für diesen Weblistener verwenden" fest. Danach klicken Sie auf "Zertifikat auswählen" und wählen das zuvor importierte Zertifikat von den SharePoint-Servern aus. Es ist wichtig, dass das Zertifikat den Namen der externen URL erhält, ansonsten zeigt der Browser bei den Anwendern eine Zertifikatewarnung an. Auf der nächsten Seite legen Sie die Authentifizierungseinstellungen fest, mit denen sich Anwender am TMG authentifizieren sollen. Diese Authentifizierung gibt das TMG anschließend an den SharePoint-Server weiter, um den Anwender anzumelden. Hier können Sie die Option "HTTP-Formularauthentifizierung" aktiviert lassen oder diese aktivieren, wenn sie deaktiviert wird. Aktivieren Sie zusätzlich im unteren Bereich noch die Optionen "Integriert" und "Windows (Active Directory)", wenn das TMG Mitglied im Active Directory ist. In diesem Fall kann das TMG direkt mit den Domänencontrollern die Authentifizierung durchführen. Handelt es sich beim TMG um einen alleinstehenden Server, verwenden Sie die Option "Standard".

Sie können diese Einstellungen nach der Erstellung des Weblisteners jederzeit über dessen Eigenschaften anpassen. Alternativ verwenden Sie die Option "HTML-Formularauthentifizierung". In diesem Fall erhalten Anwender zur Authentifizierung ein HTML-Formular des TMG angezeigt, ähnlich zu OWA in Exchange Server 2010. Auch bei der HTML-Formularauthentifizierung verwenden Sie am besten Windows (Active Directory). Auf der nächsten Seite können Sie noch Single Sign-On (SSO) für eine bestimmte Anzahl an veröffentlich-

Bild 3: Der erste Schritt zur Veröffentlichung von SharePoint mit dem TMG

ten Webseiten aktivieren. Auf diesem Weg veröffentlichen Sie zum Beispiel mehrere Webseiten gleichzeitig und müssen sich nur einmal am TMG authentifizieren. SSO ist nur bei Verwendung der formularbasierten HTML-Authentifizierung verfügbar. Tragen Sie im Feld anschließend die Domäne ein, die Sie für SSO verwenden wollen.

Veröffentlichen einer SharePoint-Site

Anwender greifen per SSL über das Internet auf das TMG zu. Zwischen TMG und SharePoint können Sie entweder ebenfalls SSL verwenden oder normalen HTTP-Verkehr. URLs für den Zugriff in SharePoint tragen die Bezeichnung "Alternative Zugriffsordnungen" (Alternative Access Mappings, AAM). Ist AAM nicht korrekt konfiguriert, können die Anwender unter Umständen nicht auf SharePoint zugreifen, obwohl die Veröffentlichung korrekt gesetzt ist. Einfach ausgedrückt müssen Sie in der Zentraladministration die URLs angeben, mit denen Anwender auf SharePoint zugreifen. Um SharePoint zu veröffentlichen, klicken Sie im Aktionsbereich der TMG-Verwaltungskonsole auf die Registerkarte "Aufgaben" und wählen den Menüpunkt "SharePoint-Sites veröffentlichen" aus.

Auf der ersten Seite geben Sie der Veröffentlichungsregel einen Namen. Wählen Sie dann auf der nächsten Seite "Einzelne Website oder Lastenausgleich veröffentlichen" aus. In größeren Umgebungen können Sie auch komplette Farmen publik machen, wenn Sie "Serverfarm mit Webserver-Lastenausgleich veröffentlichen" auswählen. Alternativ können Sie auch über den Assistenten zur Serververöffentlichung im TMG die Serverfarm veröffentlichen. Dazu geben Sie im Veröffentlichungsassistenten einen Webserver ein, zu dem das TMG die Anwender weiterleiten soll.

Wählen Sie auf der nächsten Seite "SSL verwenden", um eine Verbindung zum veröffentlichten Webserver oder zur Serverfarm herzustellen. Diese Option erfordert die Installation eines SSL-Serverzertifikats auf dem SharePoint-Server. Sie können zwischen TMG und den SharePoint-Servern aber auch HTTP einsetzen, wenn Sie kein SSL für SharePoint konfigurieren wollen. In diesem Fall ist der Verkehr zwischen Client und TMG durch SSL geschützt, aber der Verkehr zwischen TMG und SharePoint läuft über HTTP ab.

Geben Sie auf der nächsten Seite den Hostnamen ein, den Sie intern verwenden, um die SharePoint-Site zu erreichen. Zu dieser Adresse leitet das TMG die Anfragen aus dem Internet weiter. Veröffentlichen Sie einen einzelnen SharePoint-Server, dessen Namen sich nicht über DNS auflösen lässt, aktivieren Sie "Name oder IP-Adresse eines Computers verwenden", um eine Verbindung zum veröffentlichten Server herzustellen, und geben Sie anschließend den auflösbaren Computernamen oder die IP-Adresse des veröffentlichten Servers ein.

Haben Sie nicht die Veröffentlichung eines einzelnen Servers gewählt, sondern die Veröffentlichung einer Serverfarm, können Sie diese über den Veröffentlichungsassistenten konfigurieren und in der TMG-Verwaltungskonsole neu erstellen. Im Fenster geben Sie einen Namen für die Farm ein und hinterlegen alle SharePoint-Server, die Sie veröffentlichen wollen. Wählen Sie bei der Bestätigung zur Kommunikationsüberwachung die Option "HTTP/HTTPS-GET-Anforderung senden" aus.

Tragen Sie auf der nächsten Seite den öffentlichen vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse ein, die externe Benutzer verwenden, um auf die veröffentlichte SharePoint-Site zuzugreifen. Dieser Name muss mit dem Namen des konfigurierten Zertifikats übereinstimmen. Stimmt der gemeinsame Name im Zertifikat nicht mit der URL überein, erhalten Anwender eine Zertifikatewarnung, können nach der Bestätigung der Warnung aber trotzdem auf den Server zugreifen.

Als Nächstes müssen Sie den Weblistener auswählen, der die Regel für den Zugriff verwendet. Hier nehmen Sie den Weblistener, den Sie erstellt haben (ist noch keiner erstellt, können Sie das an dieser Stelle nachholen). Auf der nächsten Seite definieren Sie, wie das TMG die Authentifizierungsdaten der Clients an den

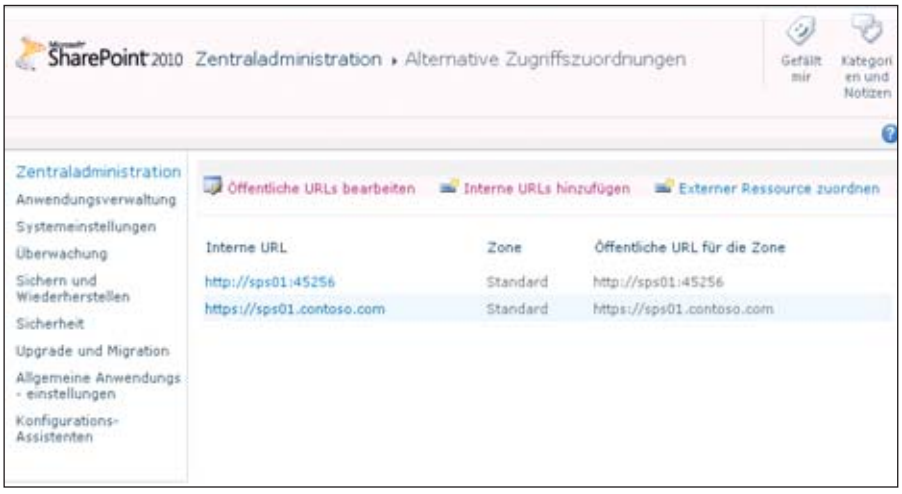


Bild 4: Die alternativen Zugriffsordnungen (AAM) von SharePoint 2010 ermöglichen die Veröffentlichung von Webanwendungen

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2011!

180 Seiten Praxis-Know-how rund um das Thema

SharePoint 2010 für Administratoren

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Liefertermin:
Ende Oktober 2011

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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

iladministrator
Das Magazin für professionelle System- und Netzwerkadministration

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0811

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

SharePoint-Server weiterleiten soll. Aktivieren Sie entweder keine Delegierung und direkte Authentifizierung der Clients oder noch besser die Option "NTLM-Authentifizierung" (diese ist standardmäßig ausgewählt).

Auf der folgenden Seite legen Sie fest, ob Sie die "Alternative Zugriffsordnung" (AAM) bereits konfiguriert haben. Welche URLs SharePoint dabei unterstützt, konfigurieren Sie in der Zentraladministration von SharePoint 2010. Klicken Sie dazu auf "Anwendungsverwaltung / Alternative Zugriffszuordnungen konfigurieren". Hier müssen Sie URLs hinterlegen, die Anwender für den internen Zugriff und den externen Zugriff auf SharePoint 2010 verwenden. Grundsätzlich muss an dieser Stelle eine URL als Standard definiert sein. Diese URL kann auch als interne URL dienen. Greifen Anwender mit anderen URLs zu, auch über das Internet, legen Sie an dieser Stelle neue URLs als öffentliche URL an. Haben Sie AAM konfiguriert, aktivieren Sie die Option "AAM für SharePoint wurde bereits auf dem SharePoint-Server konfiguriert". Klicken Sie anschließend auf den Link "Öffentliche URLs bearbeiten" und stellen Sie sicher, dass der Link, mit dem Anwender über das Internet zugreifen, hier hinterlegt ist.

Auf der nächsten Seite legen Sie die Anwender fest, die Zugriff auf SharePoint erhalten sollen. Sie können zum Beispiel eine eigene Gruppe im Active Directory anlegen und die entsprechenden Benutzerkonten aufnehmen. Diese Windows-Gruppe nehmen Sie dann in einen neuen Benutzersatz auf, den Sie an dieser Stelle hinterlegen. Den Benutzersatz erstellen und konfigurieren Sie dann auch direkt in diesem Fenster. Klicken Sie im Fenster Benutzersätze auf "Hinzufügen", um Benutzern den Zugriff zu ermöglichen. Hier ist es nicht möglich, direkt eine Windows-Gruppe zu hinterlegen, sondern Sie müssen den Windows-Gruppen erst Benutzersätze hinzufügen. Schließen Sie die Erstellung der Regel ab und übernehmen Sie deren Konfiguration. Sie können die Konfiguration der Regel jederzeit anpassen. Sie finden die Veröffentlichungsregel, wenn Sie in der TMG-Konsole auf "SharePoint-Veröffentlichungsregel" klicken. Haben Sie die Veröffentlichung als Serverfarm konfiguriert, rufen Sie nach der Erstellung und Übernahme der Regel noch deren Eigenschaften auf. Auf der Registerkarte "Webfarm" deaktivieren Sie die Option "Ursprünglichen Hostheader anstelle des Standortnamens weiterleiten". Durch diese Konfiguration leitet das TMG Anfragen, die von extern kommen, mit dem Namen weiter, der dem internen Zugriff dient.

Anschließend können Sie von extern auf SharePoint zugreifen. Arbeiten Sie mit einem internen Zertifikat von den Active Directory-Zertifikatsdiensten, erhalten Anwender, die über das Internet zugreifen, eine Zertifikatewarnung, wenn das Zertifikat der Zertifizierungsstelle nicht auf dem Client hinterlegt ist.

Verwenden Sie andere Ports für den Zugriff als die Standardports 80 oder 443, müssen Sie in den Eigenschaften der Firewallrichtlinie, mit der Sie die Veröffentlichung durchführen, auf der Registerkarte "Linkübersetzung" noch Einstellungen vornehmen. Klicken Sie auf dieser Registerkarte auf "Konfigurieren", sehen Sie die lokalen Zuordnungen zu SharePoint. Diese Adressen sollten Sie bearbeiten und den benutzerdefinierten Port hinten anhängen.

Erhalten Sie im Browser beim Zugriff den Fehlercode 500, überprüfen Sie in der Ereignisanzeige, ob Sie Fehler bezüglich der Richtlinie finden. Das TMG überprüft, ob die internen URLs funktionieren und verwendet dabei meistens den RPC-Zugriff. Gelingt der interne Zugriff nicht, beendet das TMG die Veröffentlichung. Diese Einstellung finden Sie unter "Überwachung / Konnektivitätsverifizierung".

Geben Anwender die externe URL ein, erhalten diese das Anmeldefenster des TMG, wenn Sie die formularbasierte Anmeldung aktiviert haben. Das Formular verhält sich ähnlich wie die Anmeldung an OWA. Nach der erfolgreichen Anmeldung verbindet das TMG den Anwender mit der SharePoint-Farm.

So lassen Sie sich aktuelle Verbindungen in der TMG-Verwaltungskonsole anzeigen:

1. Klicken Sie auf "Protokolle und Berichte" und öffnen Sie die Registerkarte "Protokollierung".
2. Klicken Sie im Aktionsbereich bei Aufgaben auf "Abfrage starten".
3. Sobald sich Anwender verbinden, sehen Sie den Datenverkehr und auch Details.

Protokollierung in Echtzeit und Fehlersuche

Über den Menüpunkt "Überwachung" in der TMG-Konsole sehen Sie den aktuellen Datenverkehr des TMG. Sie erkennen auf verschiedenen Registerkarten, welche Anwender und Computer aktuell

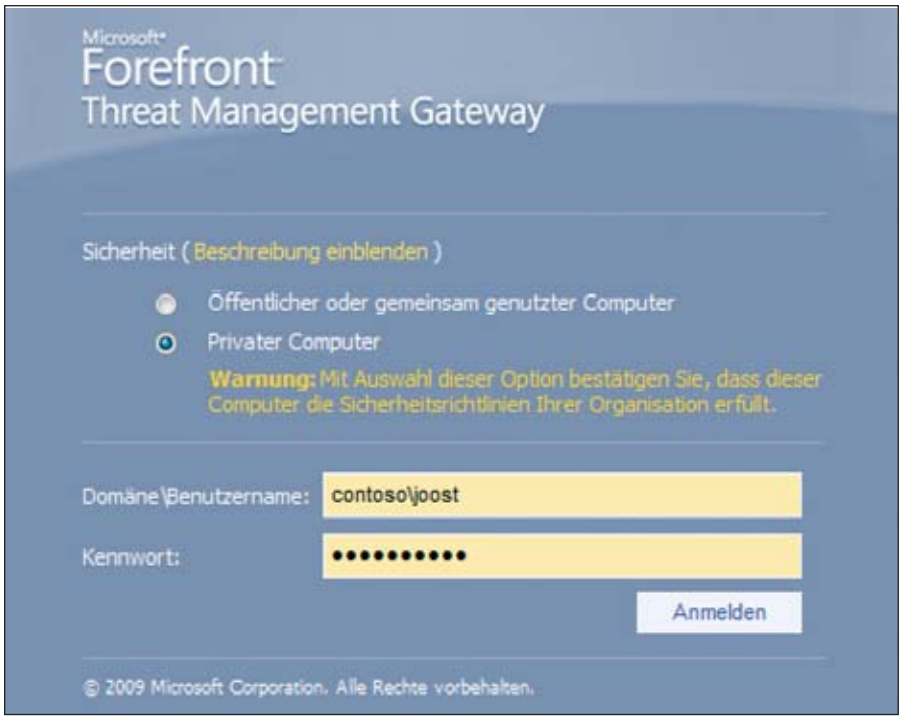


Bild 5: Die Anmeldemaske der HMTL-Authentifizierung des TMG

eine Verbindung über das TMG aufbauen. In der TMG-Konsole finden Sie über den Menüpunkt "Übersicht" eine Zusammenfassung des aktuellen Datenverkehrs, Warnungen und Fehler. Durch Doppelklick auf einzelne Bereiche erhalten Sie mehr Informationen.

Nutzen Sie den Menüpunkt "Protokolle und Berichte" im Navigationsbereich des TMG, um Abfragen des Echtzeitverkehrs nachzuvollziehen. An dieser Stelle können Sie beispielsweise genau einsehen, warum eine Serververöffentlichung nicht funktioniert oder was beim Verbindungsaufbau genau passiert. Außerdem erkennen Sie hier, welche Firewallregeln aktuell den Verkehr filtern und welche Aktionen diese durchführen.

In der Konfiguration der Protokollierung lässt sich ein Filter setzen, damit nur bestimmte Aktionen angezeigt werden. Zusätzlich kann eine Abfrage gestartet und wieder beendet werden, um den Echtzeitbetrieb des Servers zu überwachen. Den Filter grenzen Sie auf Basis zahlreicher Vorgaben ein – zum Beispiel hinsichtlich der Ziel-IP oder der Regel. Damit der Datenverkehr in Echtzeit angezeigt wird, müssen Sie auf den Link "Abfrage starten" klicken. Auf die gleiche Art beenden Sie die Anzeige des Verkehrs wieder.

SharePoint und das Forefront Unified Access Gateway 2010

Microsoft empfiehlt für die Veröffentlichung von SharePoint Server 2010 die Verwendung des Forefront Unified Access Gateway 2010 [4]. Während der Installation des UAG 2010 installiert der Assistent automatisch noch das TMG 2010. Sie müssen vor der Installation von UAG 2010 also nicht manuell das TMG 2010 installieren. Technische Informationen und Anleitungen erhalten Sie unter [5], die Technet-Seite des UAG erreichen Sie über [6]. Die wohl beste Hilfeseite für ISA, TMG und UAG ist die englischsprachige Seite [7], hier finden Sie zahlreiche Anleitungen zu allen ISA-Versionen, inklusive TMG und UAG.

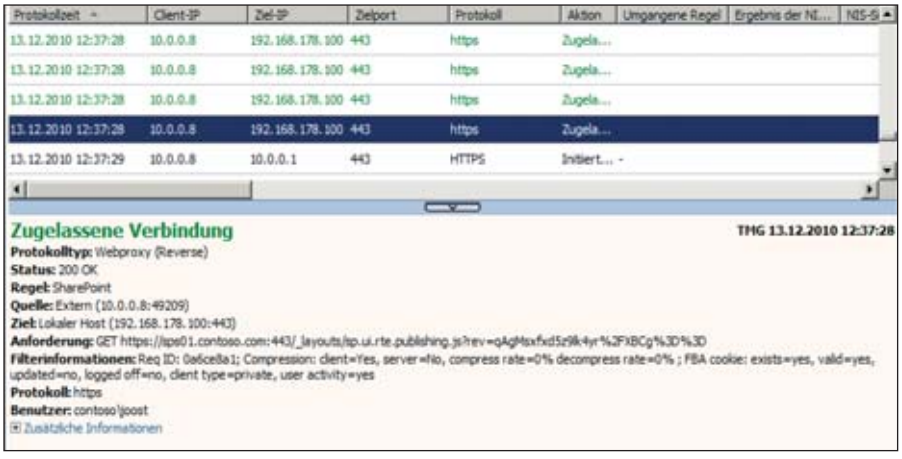


Bild 6: In der Verbindungsübersicht des TMG-Servers lassen sich Fehler aufspüren

Sie müssen beim Einsatz des UAG 2010 also keinen zweiten Server mit TMG betreiben, da ein gemeinsamer Betrieb auf einem Server optimal ist. Sie haben nach der Installation des UAG die Möglichkeit, auch herkömmliche TMG-Firewallregeln zu erstellen. Dazu verwenden Sie die TMG-Verwaltungskonsole auf dem UAG-Server. Alle Aufgaben, die das UAG betreffen, nehmen Sie wiederum in der UAG-Verwaltungskonsole vor. Sie können den Netzwerkverkehr im UAG auch mit den Möglichkeiten der TMG-Verwaltungskonsole überwachen sowie des Netzwerkmonitors des UAG 2010.

Da das UAG 2010 auf das TMG 2010 aufbaut, können Sie problemlos das TMG 2010 SP1 auf UAG 2010 installieren. Auch das Update 2 für TMG 2010 SP1 lässt sich installieren. SharePoint Server 2010 arbeitet erst nach der Installation von TMG 2010 SP1 und mindestens der Installation des Updates 1 für das TMG 2010 problemlos mit dem UAG 2010 zusammen. Betreiben Sie das UAG 2010 in einem Array, empfiehlt Microsoft die Installation von TMG 2010 SP1 auf jedem Arraymitglied. Rufen Sie auf dem UAG-Server die TMG-Verwaltungskonsole auf, können Sie sich über die Hilfe den Versionsstand des TMG anzeigen lassen. Dieser muss nach der Installation von SP1 für TMG 2010 den Wert 7.0.8107.200 haben. Vor der Installation sollten Sie alle Dienste das UAG in der Dienstesteuerung beenden. Erhalten Sie während der Installation des SP1 eine Fehlermeldung, dass Dateien in Verwendung sind, setzen Sie die Installation fort.

Nachdem Sie die TMG-Komponente des UAG aktualisiert haben, führen Sie die Aktualisierung der UAG-Komponenten durch. Sie müssen hier mindestens das UAG-Update 2 [8] installieren, damit UAG 2010 problemlos mit SharePoint 2010 zusammenarbeitet. Unter Umständen erhalten Sie eine Fehlermeldung während der Installation des Updates 2 für das UAG 2010, die besagt, dass auf das Verzeichnis "C:\Program Files\Microsoft Forefront Unified Access Gateway\ von\ monitor" nicht zugegriffen werden kann. Das Problem liegt an fehlenden Berechtigungen. Sie können dies leicht umgehen, indem Sie zunächst den Besitz des Verzeichnisses übernehmen, dann dem Benutzer "Jeder" das Recht Vollzugriff auf das Verzeichnis geben und das Recht dann auf die unteren Ordner vererben lassen. Klicken Sie nach dieser Aktion auf "Retry", führt der Assistent die Installation von Update 2 für UAG 2010 fort.

Haben Sie die Installation abgeschlossen, startet der Einrichtungsassistent des UAG. Dieser verhält sich wie der Assistent des TMG. Im ersten Schritt richten Sie die verschiedenen Netzwerkverbindungen ein. Zunächst müssen Sie im Assistent den Haken bei der Netzwerkverbindung setzen, die den internen Datenverkehr und den externen Datenverkehr regelt. Aus diesem Grund ist es auch für das UAG empfehlenswert, die Beschreibungen in den Netzwerkeinstellungen in Windows Server 2008 R2 bereits so zu wählen, wie Sie den Einsatz planen.

Auf dem nächsten Fenster geben Sie die IP-Bereiche ein, die zum internen Netzwerk gehören. Tragen Sie hier alle Subnetze ein, die Sie im Unternehmen intern einsetzen. Die vorgegebenen Subnetze können Sie löschen. Schließen Sie dann den Einrichtungsassistenten ab. Im nächsten Schritt konfigurieren Sie die Servertopologie der UAG-Server. Während der Einrichtung legen Sie fest, ob Sie den Server als Single Server betreiben wollen oder ob er Mitglied eines Arrays sein soll. Betreiben Sie ein Array mit mehreren UAG-Servern, müssen diese Mitglieder einer Domäne sein.

Das Veröffentlichungskonzept von UAG 2010

Das Veröffentlichungskonzept des UAG 2010 funktioniert etwas anders als das des TMG. Während Sie mit dem TMG einzelne Websites im Internet zur Verfügung stellen, bietet das UAG eine eigene Portalanwendung an. Bei der Veröffentlichung über das TMG verbinden sich die Anwender direkt mit dem Webserver, den Sie veröffentlichen. Verwenden Sie das UAG-Portal, verbinden sich die Anwender mit dem Portal und können von dort eine Verbindung zu den verschiedenen veröffentlichten Websites aufbauen. Dabei ist keine weitere Authentifizierung mehr notwendig, da sich die Anwender bereits beim Portal angemeldet haben. Das heißt, je mehr Websites Sie veröffentlichen wollen, umso mehr lohnt sich die Portalseite des UAG, die übersichtlich alle Anwendungen zur Verfügung stellt. Sie können über diesen Weg zum Beispiel auch zusätzlich noch Outlook Web App zur Verfügung stellen, beim Einsatz mehrerer Exchange-Versionen sogar parallel Outlook Web Access von Exchange Server 2003/ 2007 und Outlook Web App in Exchange Server 2010.

Bei der Veröffentlichung von SharePoint arbeiten Sie mit sogenannten Trunks. Ein Trunk verbindet Endpunkte, also Clients, per HTTP oder HTTPS mit der Portalseite, die Sie über das UAG veröffentlichen. Um einen neuen Trunk (eine neue Veröffentlichung) zu erstellen, klicken Sie mit der rechten Maustaste auf "HTTP Connections" oder "HTTPS-Connections", abhängig davon, ob Sie ein Portal über SSL oder nur mit Port 80 veröffentlichen wollen. Bei einer typischen Verbindung authentifizieren sich Clients aus dem Internet per HTTPS am UAG-Server. Dieser leitet die Anfragen dann zu den SharePoint-Servern weiter, ebenfalls mit HTTPS.

Um SharePoint über das UAG zu veröffentlichen, müssen Sie innerhalb von SharePoint die gleichen Konfigurationen vornehmen wie bei der Veröffentlichung über das TMG. Sie sollten für SharePoint daher SSL aktivieren. Der UAG-Server muss außerdem der gleichen Zertifizierungsstelle vertrauen wie der SharePoint-Server. Hier bietet es sich zum Beispiel an, mit einer internen Zertifizierungsstelle zu arbeiten. Setzen Sie die Active Directory-Zertifikatsdienste ein, vertraut ein UAG-Server automatisch der Zertifizierungsstelle, wenn der Server Mitglied der Domäne ist. Betreiben Sie den Server als alleinstehenden Server, müssen Sie das Zertifikat der Stammzertifizierungsstelle auf einem anderen Server exportieren und auf dem UAG-Server importieren. Das Gleiche gilt für den Client, der über das UAG auf SharePoint zugreift. Auch dieser muss der gleichen Zertifizierungsstelle vertrauen. Exportieren Sie das SSL-Zertifikat, das Sie für SharePoint verwenden, und importieren Sie das Zertifikat auf dem UAG-Server. Die Vorgehensweise ist identisch mit dem Import auf einem TMG-Server. Im Menüpunkt "Admin" in der UAG-Verwaltungskonsole verstecken sich weitere wichtige Befehle für die Einrichtung und Veröffentlichung.

Lesen Sie im zweiten Teil unserer Workshopserie, wie Sie die Veröffentlichung von SharePoint vorbereiten. Hierfür sind auf dem UAG noch einige Schritte notwendig. *(jp)*

[1] SP1 zu SharePoint 2010
B8P01

[2] Software Update 2 für Forefront Threat Management Gateway 2010 Servicepack 1
B8P02

[3] TMG Best Practise Analyzer
B8P03

[4] Produktseite zu Forefront Unified Access Gateway 2010
B8P04

[5] Technische Informationen und Anleitungen zu UAG 2010
B8P05

[6] Technet-Seite zu UAG
B8P06

[7] Webseite zu ISA, TMG und UAG
B8P07

[8] UAG-Update 2
B8P08

Link-Codes

Citrix Provisioning Server gegen Ausfälle schützen

Dienstbare Geister – ausfallsicher

von Matthias Wessner

Quelle: 123RF

In einer Terminal Server-basierten Infrastruktur ist es sehr wichtig, die Server auf einem identischen Stand zu halten. Denn damit spielt es für die Anwender keine Rolle, auf welchem Server sie arbeiten. Doch Änderungen sind in solchen Infrastrukturen an der Tagesordnung und Administratoren müssen innerhalb kürzester Zeit die Workloads ändern. Eine Möglichkeit, um dies zu erreichen, stellt die vollständige Automation der Installation dar. Eine Lösung hierfür kann der Citrix Provisioning Server sein. Das Prinzip dahinter ist, dass der Terminal Server keine eigene Festplatte mehr benötigt, sondern von einer Festplatte aus dem Netzwerk bootet. Wurde das Image einmal erstellt, ist es praktisch unendlich skalierbar. Wie Sie eine ausfallsichere Provisioning Server-Infrastruktur einrichten, lesen Sie in diesem Workshop.

Der Provisioning Server bietet drei Arten von Images: Private-, Standard- und Differenz-Images. Das Private-Image hat eine 1:1-Beziehung zu einer Maschine. Das Standard-Image kann im Gegensatz dazu von beliebig vielen Servern genutzt werden, die dann von ein und demselben Image booten. Die Personalisierung des Images – die hauptsächlich darin besteht, dem Server einen neuen Namen zu geben und im Active Directory zu veröffentlichen – erledigt dann der Provisioning Server. Das Ergebnis ist eine Farm, in der alle Server tatsächlich identisch sind. Läuft dann einmal doch ein Server aus dem Ruder, starten Sie ihn einfach neu. Alle Änderungen sind damit verworfen und nur die Einstellungen und Anwendungen vorhanden, die auf dem sogenannten Golden Image getätigt wurden. Im Falle des Differenz-Images starten mehrere Server von einem Image und die Änderungen bleiben durch die Nutzung eines speziellen Caches auch nach einem Reboot erhalten.

Gefahr durch Ausfall einzelner Komponenten

Die große Gefahr bei der Implementierung einer Provisioning Server-Infrastruktur ist eigentlich nur die fälschliche Annahme, dass diese Technologie alle Probleme der Vergangenheit löst. Denn der Teufel steckt wie so oft im Detail. Um mögliche Gefahren etwas näher kennen zu lernen, schauen Sie sich am besten die einzelnen Komponenten genauer an und spielen durch, was passiert, wenn diese jeweils ausfallen.

Wie schon beschrieben, booten die Server von einer virtuellen Festplatte im Netzwerk. Dazu muss der Server, der die Rechenleistung zur Verfügung stellt, dieses Image im Netzwerk finden. Dies wird in der Regel über einen PXE-Boot gelöst. Den PXE-Server können Sie übrigens gemeinsam mit dem Provisioning Server installieren. Wer sich mit PXE schon mal auseinandergesetzt hat, weiß, dass für PXE auch ein DHCP-Server und ein Boot-Image, das über einen TFTP-Server bereitgestellt wird, notwendig sind. Das Boot-Image verweist dann auf den Provisioning Server, der in seiner Datenbank nach der MAC-Adresse des anfragenden Gerätes schaut und diesem das zugewiesene Image heraussucht. Danach kann der Server von dieser virtuellen Festplatte booten.

Fällt eine der genannten Komponenten aus, so kann der zukünftige Terminal Server nicht seine Festplatte finden, von der er starten will. Wenn Sie alle Server zum Beispiel im Wartungsfenster booten, führt dies zum Ausfall der gesamten Farm. Um dem entgegenzuwirken, müssen die Komponenten also ausfallsicher gestaltet werden.

Ausfallsicheres DHCP

Die dynamische IP-Adressverteilung spielt auch in unserer Workshop-Umgebung eine bedeutende Rolle. Nehmen wir den Microsoft DHCP-Server als Bei-

spiel, so lässt sich dieser als Cluster definieren. Dafür benötigen Sie jedoch eine Enterprise-Lizenz, da Cluster-Dienste nur in der Enterprise-Version zur Verfügung stehen. Eine andere Möglichkeit wäre es, zwei DHCP-Server mit unterschiedlichen IP-Adress-Bereichen zu definieren, also zum Beispiel einen DHCP-Server für den Bereich 10.10.10.10 bis 10.10.10.100 und einen DHCP-Server für 10.10.10.101 bis 10.10.10.200. Der Nachteil bei dieser Variante ist, dass sie insgesamt doppelt so viele IP-Adressen belegt, wie eigentlich für den Bereich notwendig wären. Denn fällt einer der DHCP-Server aus, soll der zweite schließlich nahtlos mit seinem Adressbereich übernehmen können.

Eine weitere Möglichkeit ist es daher, zwei DHCP-Server mit dem gleichen Bereich zu definieren und eine IP-Adresskonflikterkennung am DHCP-Server einzuschalten. Soll in dieser Konstellation eine IP-Adresse vergeben werden, die bereits im Netzwerk aktiv ist, wird eine andere gewählt. Hier kann es natürlich einige Zeit dauern, wenn etwa nur noch eine IP-Adresse aus dem gesamten Bereich frei ist. Damit bleibt aber in Server-Umgebungen noch der Umstand, dass die Server wechselnde IP-Adressen erhalten. Sie können daher auch bestimmten Rechnern anhand ihrer MAC-Adresse feste IP-Adressen zuweisen. So nutzen die Server stets die gleiche IP-Adresse, was auch einen Vorteil für den XML-Dienst der XenApp-Server darstellt, da dieser anhand der IP-Adresse des Servers identifiziert wird. Welches die beste Variante für Ihre Infrastruktur ist, lässt sich natürlich nicht pauschal sagen. Dies hängt immer von den jeweiligen Umständen ab.

Damit das startende Gerät nicht nur eine IP-Adresse erhält, sondern auch sein Boot-Image findet, muss der DHCP-Server mit den sogenannten Optionen "66" und "67" konfiguriert sein. Die Option 66 definiert den TFTP-Server und die Option 67 das Boot-Image, welches das anfragende Gerät nutzen soll. Bei der Option 66 lässt sich allerdings keine Liste an Servern hinterlegen, sondern nur eine IP-Adresse. Dies bedeutet wiederum einen Single Point of Failure, den Sie eigentlich nur mit einem Load Balancer umgehen können. Zum Glück gibt es schon Freeware Load Balancer wie etwa "Herkules", so dass Sie hier nicht allzu tief ins Portemonnaie greifen müssen. Häufig gibt es aber in größeren Umgebungen schon Load Balancer, die Sie für solche Zwecke natürlich auch nutzen können. Es lässt sich beispielsweise auch NetScaler nutzen, dann muss aber der TFTP Server das Gateway als Default-Gateway definiert haben.

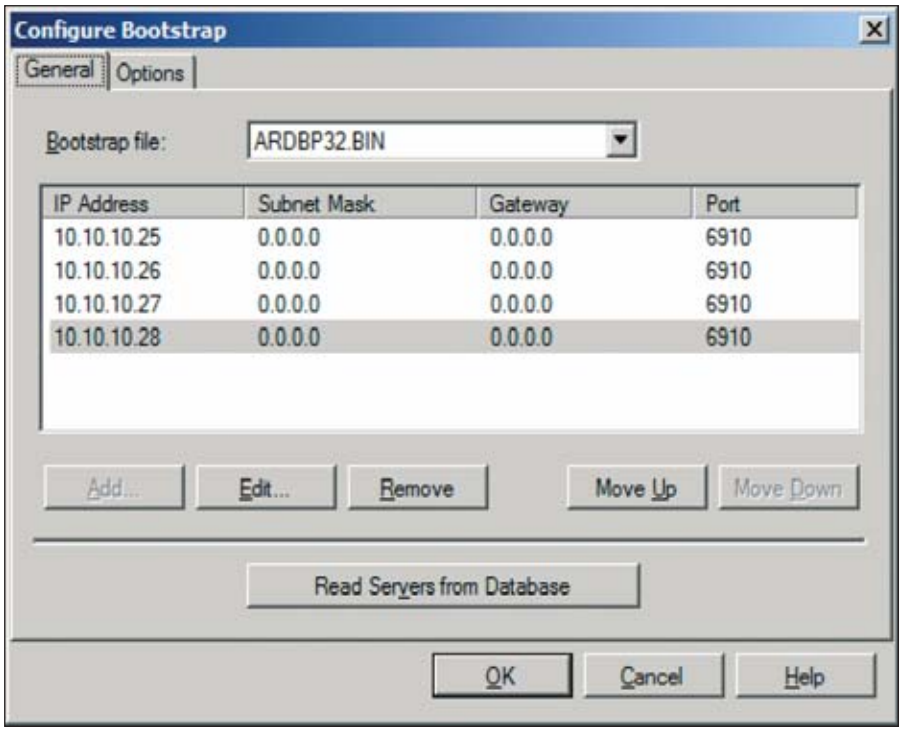


Bild 1: XenApp nutzt für das Booten die Datei *ARDBP32.BIN*

Der weitere Vorteil der Optionen 66 und 67 ist, dass der TFTP-Server nicht im gleichen Subnetz stehen muss, sondern sich auch hinter einem Router befinden kann. Besteht diese Anforderung nicht, kann beim DHCP-Server auch gar nichts konfiguriert sein und der PXE-Server einfach im gleichen Netzwerksegment stehen. Hier lassen sich einfach mehrere PXE-Server mit dem gleichen Boot-Image konfigurieren. Fällt einer der Server aus, antwortet einfach ein anderer. Funktionieren alle, gewinnt der schnellste.

Im nächsten Schritt wird das TFTP-Boot-Image geladen. Dieses Image verweist nun auf den Provisioning Server respektive auf die Provisioning Server. Sie haben die Möglichkeit, eine Liste von bis zu vier Servern zu definieren. Steht einer der Server nicht zur Verfügung, übernimmt ein anderer Provisioning Server die Anfrage. Häufig wird für den Bootprozess ein separates LAN definiert, so dass keine Konflikte mit anderen PXE-Servern entstehen und die volle Bandbreite für das Streaming zur Verfügung steht. Eine Möglichkeit, diese generellen Boot-Herausforderungen zu meistern, ist es, ein ISO-Image zu erstellen, von dem die Server starten. In diesem Image ist praktisch das TFTP-Boot-Image enthalten, so dass der Server nicht im Netzwerk danach suchen muss. Das Problem dabei ist, dass Sie bei einer Änderung an der Provisioning Server-Infrastruktur auch das ISO-Image neu erstellen und zuweisen müssen.

XenApp ausfallsicher einrichten

Hat der Client nun einen funktionierenden Provisioning Server gefunden, so muss dieser Server auch auf die Festplatte zugreifen können, die für den Server vorgesehen ist. Nutzen Sie mehrere Provisioning Server, so muss diese Festplatte also von verschiedenen Servern zugreifbar sein. Die einfachste Möglichkeit ist, das Image auf jeden Provisioning

Server zu kopieren. Dieses Konzept ist simpel, ermöglicht aber, dass es verschiedene Versionen der virtuellen Festplatte auf verschiedenen Server gibt.

Häufig werden die virtuellen Festplatten im VHD-Format im Storage abgelegt. Dabei empfiehlt sich aufgrund der Performance kein CIFS-basierter Storage – die beste Lösung ist ein Active-Active-Filecluster basierend auf iSCSI oder Fibre Channel. Diese kosten natürlich einiges, bieten aber die beste Performance. In gewissen Konstellationen können die VHDs nur auf einem Read Only-Storage abgelegt werden. Der Read Only-Storage impliziert aber auch einen erhöhten Aufwand für das Management der VHDs, da das Storage in einen Write-Modus versetzt werden muss, damit sich die VHDs ändern lassen. In dem Moment können aber die Provisioning Server nicht auf das bestehende Image zugreifen. Nutzen Sie einen Storage-Virtualisierer wie zum Beispiel DataCore oder Sanbolic Melio FS, haben Sie dieses Problem nicht. Sie können nämlich in diesem Fall einfach weitere VHDs auf die LUNs kopieren, diese neu zuweisen und dann die PVS von der neuen VHD booten.

Sind diese Punkte berücksichtigt, haben Sie die Voraussetzungen für eine stabile Infrastruktur geschaffen. Doch es gibt noch weitere Aspekte zu bedenken. Schauen Sie sich einen XenApp-Server an, so hat dieser verschiedene Ausfallmechanismen eingebaut, zum Beispiel den Local Host Cache. Dieser hält einen Teil der XenApp-Datenbank vor, so dass der Server auch ohne zentrale Datenbank arbeiten kann. Wie sieht dieses Verhalten bei einem goldenen Image aus? Der Server bootet neu, die zentrale Datenbank steht nicht zur Verfügung und – der Local Host Cache ist leer, da der Server ja von einem neutralen goldenen Image bootet. Der Server ist damit nicht funktionsfähig. Ähnlich verhält es sich mit den Citrix-Lizenzen. Hat ein XenApp-Server einmal Kontakt zu einem Citrix-Lizenzserver aufgebaut, so kann er 30 Tage ohne Lizenzserver arbeiten. Stellen Sie sich vor, dass der Lizenzserver 30 Tage nach Erstellen des goldenen

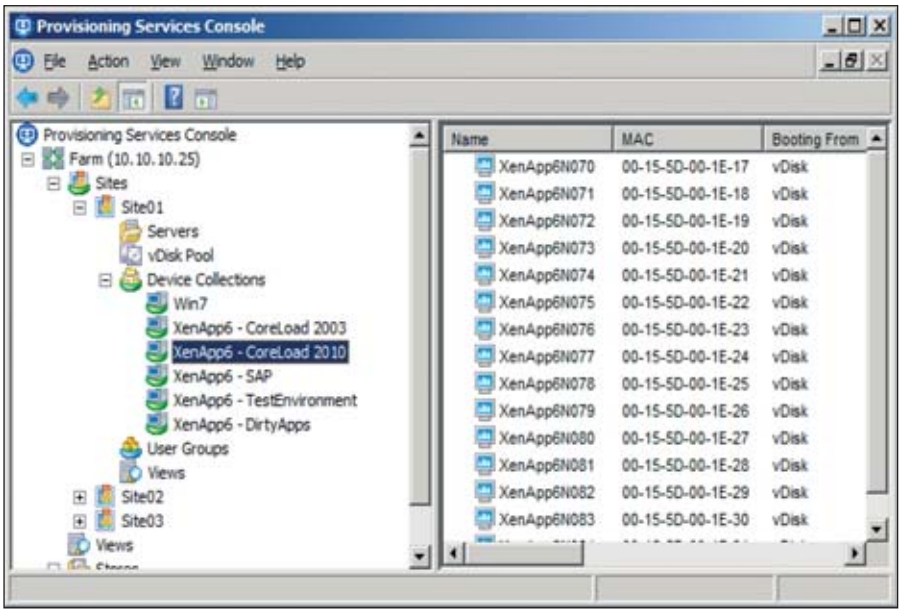


Bild 2: In der Provisioning Services Console finden Sie einen Überblick darüber, welche XenApp-Instanzen es gibt und wie diese booten

Images ausfällt und der XenApp-Server dann neu startet, so sind die 30 Tage vergangen und der Server kann keine Anwender annehmen. Problematisch kann auch das Debugging von Problemen sein. Denken Sie etwa an ein Problem, bei dem der Server auf Grund eines Fehlers rebootet, so ist der Crashdump weg und das Eventlog ist leer.

Abhilfe für all diese Probleme kann eine zweite Partition schaffen, die dauerhaft vorhanden ist und damit auch nach einem Reboot die entsprechenden Informationen vorhält. Diese zweite Partition kann wiederum an verschiedenen Orten liegen: der lokalen Festplatte des Hypervisors, einem CIFS-Storage oder einem "echten" iSCSI- oder Fibre Channel-Storage. Liegt die Partition lokal auf dem Hypervisor, kann die Maschine nicht so ohne weiteres auf einen Hypervisor verschoben werden. Das macht aber in einer XenApp-Umgebung meist auch nicht viel aus, da Sie ja noch weitere Server von dem gleichen Image starten. Die persistente Partition auf einen CIFS-Storage zu legen, kann wiederum zu Performance-Problemen führen. Am besten und teuersten ist es, die zweite Partition auf ein leistungsfähiges Storage zu legen, womit dann auch die XenApp-Server auf einen anderen Hypervisor verschoben werden können. Die oben genannten Daten müssen dann nur auf diese dauerhafte Partition ausgelagert werden und schon sind sie nach einem Neustart verfügbar. Die Informationen über die Citrix Lizenzen liegen zum Beispiel in der Datei *%programfiles%\Citrix\MPSWSXICA_MPS-WSXICA.INI*. Diese INI-Datei wird in einem Cache-Verzeichnis abgelegt. Den Pfad zum Cache-Verzeichnis legen Sie in der Registry unter "HKLM/ Software/(WOW6432 NODE)/CITRIX/ INSTALL" im Wert "CacheLocation" fest, so dass durch Modifikation des Registry-Wertes die zwischengespeicherten Lizenzinformationen auf die spezielle Partition umgeleitet werden können.

Zweite Partition für Edge Sight nötig

Möchten Sie das Produkt Edge Sight von Citrix zur Performance-Überwachung in einer Provisioning Server-Infrastruktur einsetzen, so benötigen Sie in jedem Fall diese zweite Partition, damit Edge Sight den Server wiedererkennt und damit sinnvoll Daten über die Auslastung sammeln kann. Für die Dauer des Betriebs eines Provisioning Servers schreibt er die Änderungen in einen Write Cache. Den Write Cache können Sie in den Arbeitsspeicher des Servers, auf eine lokale Partition oder das SAN legen. Hier müssen Sie wiederum Kosten versus Nutzen rechnen. Das Schnellste ist sicherlich der Arbeits-

speicher, damit aber auch eine sehr teure Lösung. Den Cache auf das Storage zu legen, ermöglicht hohe I/O-Performance und die Möglichkeit, den Serverload auf einen anderen Hypervisor zu verschieben. Liegt der Cache auf einer lokalen Partition, haben Sie diese Möglichkeiten nicht. Dafür ist diese Lösung kostengünstig und trotzdem effizient. Wie schon beschrieben, erreichen Sie die Ausfallsicherheit in einer XenApp-basierten Infrastruktur sowieso eher durch mehrere XenApp-Server als durch die Möglichkeit, die Workloads über eine Virtualisierungsplattform hin und her zu verschieben. Als Zielplattform für die virtuelle Festplatte sollten Sie übrigens am besten eine virtuelle Infrastruktur nutzen. Der Vorteil ist dann, dass die Hardware für das Image immer die gleiche ist. Dabei spielt es eine untergeordnete Rolle, von welchem Hersteller der Hypervisor stammt. Natürlich funktionieren auch physikalische Zielsysteme, hier müssen Sie aber mehr Rücksicht auf Treiber innerhalb des goldenen Images nehmen.

Auch um die Microsoft-Lizenzen müssen Sie sich Gedanken machen. Am einfachsten ist der Einsatz eines KMS-Servers. Ist dieser nicht vorhanden, so hat der XenApp Server erst einmal keine gültige Microsoft-Lizenz, da der Provisioning Server ihn individualisiert. MAC-basierte Lizenzen lassen sich auch einsetzen, verlieren aber die Zuweisung, sobald das Image einer neuen Maschine zugewiesen wird.

Eine weitere Herausforderung bei der Verwaltung von goldenen Images ist es, die Anzahl der Neuerstellungen zu reduzieren. Um etwa den Datenbankpfad für eine Anwendung zu ändern, müssten Sie normalerweise ein komplett neues Image erstellen. Abhilfe schafft hier die Trennung der Installation von der Konfiguration. Damit wird der Datenbankpfad nicht bei der Installation selbst geschrieben, sondern landet in einer nachgelagerten Konfiguration. Diese Konfigurationsschicht wird bei jedem Neustart der Server ausgeführt und darf nur kleinere Änderungen vornehmen wie das Kopieren einer INI-Datei oder das Importieren eines Registry-Schlüssels. Dabei müssen die Änderungen so beschaffen sein, dass sie auch bei hunderten Ausführungen das gleiche Ergebnis erzielen.

Berücksichtigen Sie all diese einzelnen Punkte, erhalten Sie eine gut skalierbare und ausfallsichere Provisioning Server-Infrastruktur, die keine zusätzlichen Probleme bereitet, sondern die Infrastruktur um eine gehörige Portion Dynamik erweitert. In Enterprise-Umgebungen hat sich gezeigt, dass es auch Sinn macht, die Erstellung des goldenen Images zu automatisieren, damit Sie nicht die Kontrolle über den Inhalt des Images verlieren. Der Mehrwert der Provisioning Server-Infrastruktur liegt dann in der Möglichkeit, das Image sehr dynamisch bereitzustellen. Eine Neuinstallation im Fehlerfall bedeutet dann nur einen Reboot, anstatt die Maschine für zwei bis vier Stunden aus der Farm zu entfernen. Auch ein Rollback auf eine ältere Version ist einfach per Zuweisung des Images im Provisioning Server möglich, der dann durch den Neustart der Server durchgeführt wird.

Die Schritte im Überblick

1. DHCP im Netzwerk ausfallsicher einrichten.
2. TFTP-Bootimage laden.
3. Image an die Clients verteilen.
4. Zweite Partition für dauerhafte Informationen schaffen.
5. Write Cache im Arbeitsspeicher oder im SAN anlegen.
6. Microsoft-Lizenzen anpassen.

Virtueller Unterbau

Wie bereits erwähnt macht es Sinn, die Plattformen, auf denen die virtuellen Disks gebootet werden, zu virtualisieren, damit das Image immer die gleiche Hardware vorfindet. Wie sieht es nun mit erweiterten Funktionalitäten, wie dem Verschieben einer virtuellen Instanz auf einen anderen Server aus – sei es für Wartungszwecke oder für die dynamische Lastverteilung? Das bringt in einer XenApp-Umgebung wenig Nutzen, da die Ausfallsicherheit und Lastverteilung Kernfunktionen der XenApp-Umgebung sind. Auch gäbe es bei einem dynamischen Verschieben eventuell Probleme mit den Microsoft-Lizenzen, so dass es häufig Sinn ergibt, eine Microsoft Windows Server Enterprise-Lizenz für jeden physikalischen Host zu erwerben, da Sie dann auf diesem Host vier virtuelle Windows Betriebssysteme hosten können.

Das Provisioning Server-Konzept ist natürlich auch in einer XenDesktop-Umgebung sehr gut nutzbar. Hier sind Funktionalitäten wie das Verschieben von virtuellen Desktops nützlich, wenn Sie persistente Desktops nutzen, da bei einem Ausfall des hostenden Servers der virtuelle Desktop für den entsprechenden Anwender ansonsten nicht mehr zur Verfügung steht. Bei persistenten Desktops benötigen Sie auch die genannte Extra-Partition nicht, da durch die persistente Festplatte oder im Provisioning Server-Jargon das "private Image" nach einem Reboot die Daten noch enthält. Für Standard-Images im XenDesktop-Umfeld gilt aber das Gleiche wie für die XenApp-Server: Auch hier bringt eine zweite Partition für gewisse Daten wie das Eventlog Vorteile.

Fazit

Der Citrix Provisioning Server ist ein sehr leistungsfähiges Produkt, dessen vermeintliche Einfachheit einem leicht Kopfschmerzen bereiten kann. Dieser Workshop sollte die Punkte aufzeigen, die Sie nicht in einem Standardwerk über Provisioning Server-Planung finden. Natürlich müssen Sie sich auch über die Netzwerksegmentierung und Storage-Performance Gedanken machen. Aber das sind Herausforderungen, die etwa bei einer PXE-Lösung oder einer VDI-Umgebung zum Tragen kommen. Mit den genannten Tipps sollten Sie gut auf unerwünschte Überraschungen vorbereitet sein. *(dr)*

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

Kompetentes Schnupperabo sucht neugierige Administratoren

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

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

Damit Sie sich Zeit, Nerven und Kosten sparen.

Teamwork in Bestform. Überzeugen Sie sich selbst!

6 Monate lesen

3 Monate bezahlen

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

Microsoft PowerShell v2

Grafische Oberfläche für die PowerShell

von Rolf Masuch

Die PowerShell v2 kann auch grafische Oberflächen erzeugen. Doch welches ist der beste Weg zur eigenen GUI? Je länger Sie die PowerShell nutzen, desto wahrscheinlicher ist es, dass Sie Informationen an die Anwender Ihrer Skripte in einer mehr oder weniger aufwändig gestalteten Benutzeroberfläche ausgeben möchten. Lernen Sie in diesem Workshop die unterschiedlichen neuen Wege im Vergleich kennen.

Natürlich steht Ihnen bei der Arbeit mit der PowerShell nach wie vor die Möglichkeit offen, Ausgaben in HTML-Form zu erzeugen und mit dem Standardbrowser anzuzeigen. Die Befehle dazu sehen dann beispielsweise folgendermaßen aus:

```
get-eventlog -logname "Windows
  PowerShell" | ConvertTo-html >
  c:\ps\pslog.htm
invoke-item c:\ps\pslog.htm
```

Dabei sind die Gestaltungsmöglichkeiten allerdings auf die Elemente beschränkt, die Sie über das Cmdlet "ConvertTo HTML" ansprechen oder erzeugen können. Echte Applikationen, wie Sie sie früher gegebenenfalls als HTA bereitgestellt haben, sind auf diesem Weg nicht sinnvoll erzeugbar. Außerdem ist die Kommunikation bei diesem Beispiel einseitig.

Mehr Möglichkeiten bietet Ihnen die auch weiterhin zur Verfügung stehende Visual Basic-Klasse. Beachten Sie dabei jedoch, dass auf einem neueren Windows 7-System mit aktuellen Applikationen die Visual Basic-DLL möglicherweise fehlt. Nachfolgend ein Beispiel, um ein einfaches Popup-Fenster zu erzeugen. So soll je nach gedrückter Schaltfläche die Variable "$Test" gefüllt werden:

```
$WSH = new-object -comobject
  wscript.shell
$Test = $WSH.popup("Dies ist ein
  Test",0,"Test Message Box",1)
```

Windows Forms mit viel Code

Über den Zugriff auf das .NET Framework kann jede Art von nativen Dialogen oder allgemein Fenstern ermöglicht werden. Der erste Schritt dazu ist das Laden der entsprechenden Assemblies:

```
[reflection.assembly]::loadwithpar-
  tialname("System.Drawing") |
  Out-Null
[reflection.assembly]::loadwithpar-
  tialname("System.Windows.Forms") |
  Out-Null
```

Dabei dient "System.Windows.Forms" dem Zugriff auf die einzelnen Controls und "System.Drawing" der genauen Positionierung von Controls beziehungsweise ihrer Größen oder zur Arbeit mit Schriftobjekten. Die Weiterleitung an das Cmdlet "Out-Null" dient der Kosmetik. Es unterdrückt die Rückmeldung, aber eben auch eventuelle Fehlermeldungen. Allein um jetzt ein einfaches Formular darzustellen und die Titelzeile mit einem individuellen Wert zu füllen, sind, je nach späterem Verwendungszweck, bis zu sieben Zeilen Code notwendig:

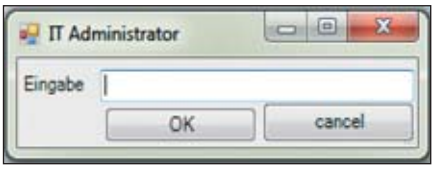


Bild 1: Auch ein einfacher Eingabedialog kann komplex im Aufbau sein

```
$System_Drawing_Size = New-Object
  System.Drawing.Size
$System_Drawing_Size.Height = 55
$System_Drawing_Size.Width = 266
$form1.ClientSize = $System_
  Drawing_Size
$form1.DataBindings.DefaultData
  SourceUpdateMode = 0
```

```
<Window x:Class="WpfInput.MainWindow"
        xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
        xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
        Title="IT Administrator" Height="97" Width="233">
    <Grid>
        <Label Content="Eingabe" Height="28" HorizontalAlignment="Left" Name="label1" VerticalAlignment="Top" Width="50" />
        <TextBox Height="23" HorizontalAlignment="Left" Margin="56,0,0,0" Name="textBox1" VerticalAlignment="Top" Width="153" />
        <Button Content="OK" Height="23" HorizontalAlignment="Left" Margin="57,28,0,0" Name="button1" VerticalAlignment="Top" Width="75" />
        <Button Content="cancel" Height="23" HorizontalAlignment="Right" Margin="0,28,2,0" Name="button2" VerticalAlignment="Top" Width="75" />
    </Grid>
</Window>
```

Bild 2: Struktur einer XAML-Datei, die mit Visual Studio erzeugt wurde

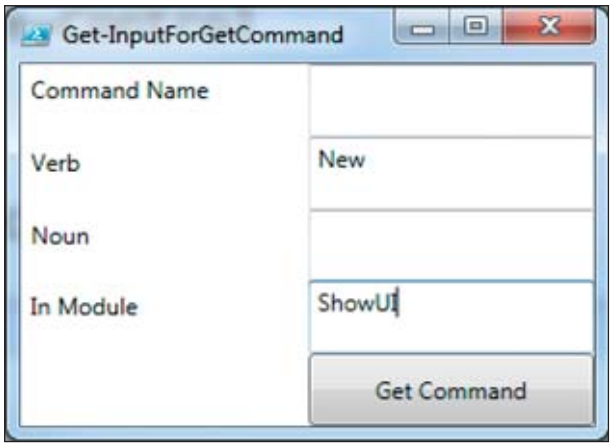


Bild 3: Ein komplexer Dialog mit ShowUI

```
$form1.Name = "form1"
$form1.Text = "IT Administrator"
```

Ein einfacher Button kommt auf bis zu 14 Zeilen Code. Dabei ist mit der Zeile *$button2.add_Click($button2_OnClick)* der Verweis auf den Skriptblock anzugeben, der beim Klicken auf die Schaltfläche ausgeführt werden soll. Die Zeile *$form1.Controls.Add($button2)* fügt die Schaltfläche "Button2" der Control-Liste des Formulars hinzu. Selbstverständlich muss der Skriptblock *$button2_OnClick* auch noch mit der notwendigen Applikationslogik ausgestattet werden. Aber allein um das in Bild 1 dargestellte Fenster zu erzeugen, sind über 100 Zeilen Code erforderlich – und darin ist noch keine Zeile Logik enthalten. Schlussendlich muss der ganze Codebereich noch in eine große Funktion eingebettet werden, um mit dem Aufruf dieser Funktion dann endlich zum eigentlichen Fenster zu kommen. Der Übersichtlichkeit halber sollten Sie die beschreibenden Anteile mit dem Aufbau des Formulars und der enthaltenen Controls in ein separates Skript auslagern und die Funktionalität in Ihr Kernskript einbauen.

Windows Presentation Foundation

Der Weg zum eigenen Fenster führt bei der Windows Presentation Foundation (WPF), wie auch bei den Windows Forms, über das Laden des entsprechenden Assemblies. Danach können Sie über eine XAML-Datei die Struktur des Fensters einlesen. Sollten Sie diese Datei etwa mit Visual Studio erzeugt haben, kann sie diese Form, wie in Bild 2 dargestellt, haben.

Wenn Sie diese Datei jetzt mit Get-Content einlesen und danach laden wollen, müssen Sie das Attribut "x:Class" entfernen. Die PowerShell kann diese Klassenanweisung nicht verarbeiten, da sie aus der Definition des eigenen Programms stammt. Das kann zur Laufzeit des Skripts im Arbeitsspeicher erfolgen (Zeile 2). Die folgenden Zeilen stellen den gesamten Aufruf des Formulars dar:

```
Add-Type -AssemblyName Presenta-
  tionFramework
[XML]$XAML = Get-Content c:\ps\
  InputboxWPF.xaml
$XAML.Window.RemoveAttribute
  ("x:Class")
$Reader = New-Object
  System.Xml.XmlNodeReader $XAML
$Input = [Windows.Markup.Xaml
  Reader]::Load($Reader)
$Input.ShowDialog() | Out-Null
```

Wenn Sie das Formular mit seinen Controls verändern möchten, steht Ihnen die XAML-Datei zur Verfügung. Somit trennen Sie das Layout vom Code. Innerhalb Ihres Codes legen Sie dann wie gewohnt Ihre eigenen Funktionen und Programmabläufe fest.

Show-UI für mehr Logik

Das als separates Modul erhältliche Show-UI [1] kapselt die Logik des WPF ab und führt den Ansatz des Moduls WPK aus dem PowerShellPack fort. Für den Aufbau eines eigenen Formulars mit darin enthaltenen Controls steht Ihnen jeweils ein Cmdlet pro Control zur Verfügung. Diese können ineinander verschachtelt und zusammen aufgerufen werden. Sie können sehr leicht Events und die damit verbundene Applikationslogik in Ihre Skripte einbauen. Damit lassen sich mit wenigen Zeilen auch komplexe Dialoge erzeugen:

```
Import-Module ShowUI
$getCommandInput = UniformGrid
  -ControlName 'Get-InputForGet
  Command' -Columns 2 {
    "Command Name"
    New-TextBox -Name Name
    "Verb"
    New-TextBox -Name Verb
    "Noun"
    New-TextBox -Name Noun
    "In Module"
    New-TextBox -Name Module
    " " # Some Empty Space
    New-Button "Get Command"
  -On_Click {
        Get-ParentControl |
Set-UIValue -passThru |
Close-Control
    }
} -show
```

Fazit

Um das Erzeugen von Eingabemasken zur Kommunikation mit dem Anwender Ihres Skriptes werden Sie auch mit der PowerShell nicht herumkommen. Der veraltete Aufruf von VB beziehungsweise VBS-Komponenten ist schon heute nicht konsistent auf allen Systemen durchführbar. Wenn Sie keine zusätzlichen Module auf ihre Arbeitsplatzrechner bringen können, scheint der Windows Forms-Ansatz am vielversprechendsten zu sein. Aber er ist sehr Code-intensiv und erfordert die Einarbeit in die MSDN-Dokumentation.

Der native Einsatz des Windows Presentation Framework ist auf allen Systemen möglich, auf denen das .NET Framework 3.51 installiert ist. Ein separates Modul ist nicht erforderlich. Sehr wohl aber müssen Sie die genaue Syntax zur Programmierung kennen. Diese kann wiederum auch aus dem MSDN entnommen werden. Die Lösungen über das WPK und ShowUI als jeweils separate Module benötigen genau diese Module auf allen Systemen, auf denen Ihr Skript genutzt werden soll. Beachten Sie dabei die Skript-Signing-Richtlinien für Ihr Unternehmen. Die Einarbeitung in die Syntax geht sehr zügig und die Ergebnisse sind schnell nutzbar. *(dr)*

[1] Show-UI auf Codeplex
B8PF1

Link-Codes

Tipps & Tricks ohne Gewähr

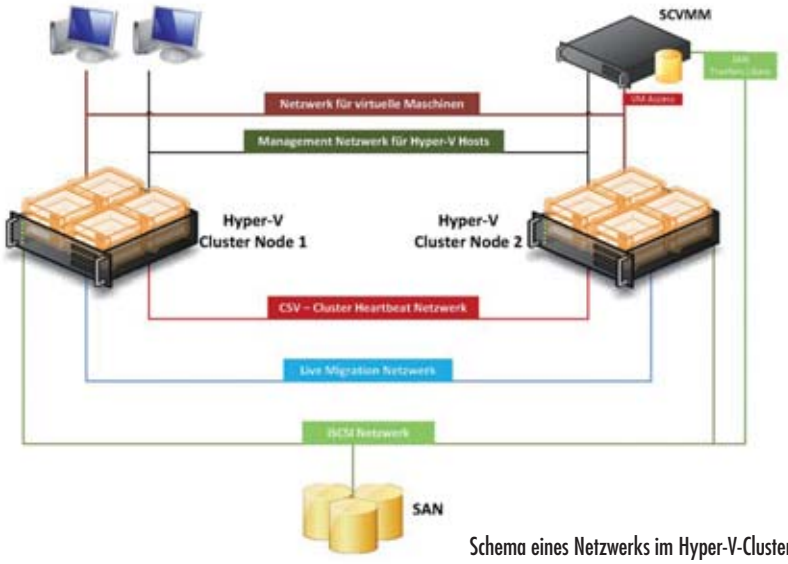
In jeder Ausgabe präsentiert Ihnen IT-Administrator Tipps, Tricks und Tools zu den aktuellen Betriebssystemen und Produkten, die in vielen Unternehmen im Einsatz sind. Wenn Sie einen tollen Tipp auf Lager haben, zögern Sie nicht und schicken Sie ihn per E-Mail an tipps@it-administrator.de.

Microsoft Windows

Wenn ich mir im **Microsoft Hyper-V** die **Netzwerkkonfiguration** einer Netzwerkkarte anschaue, frage ich mich, ob ich all diese **Protokolle und Bindungen** wirklich bei den verschiedenen Hyper-V-Karten benötige. Welche Haken soll ich am besten bei einem Cluster mit VM-Netz, Management-Netz, Live Migrations-Netz, CSV-Netz und iSCSI-Netz setzen?

Dazu machen Sie sich in der Tat berechtigterweise Gedanken. Um zu veranschaulichen, welche Konfiguration sinnvoll ist, betrachten wir zunächst das Bild "Schema eines Netzwerks im Hyper-V-Cluster": Es zeigt eine lehrbuchartige Netzwerkkonfiguration in einem Hyper-V-Cluster. In der Mitte finden Sie, stellvertretend für alle Cluster-Knoten, zwei Hyper-V-Server. Diese sind in der unteren Bildhälfte durch ein Live Migrations-Netz, ein CSV-Netz und ein iSCSI-Netz verbunden. Diese Netze haben gemeinsam, dass sie nicht geroutet werden und in ihnen nur die Clusterknoten vertreten sind. Eine Ausnahme bildet gegebenenfalls das iSCSI-Netzwerk, denn in diesem können weitere Systeme, die direkt auf das Storage zugreifen (im Bild stellvertretend durch den System Center Virtual Machine Manager dargestellt, der seine Library auf dem Storage liegen hat), vorhanden sein. Oberhalb der Cluster-Knoten sind das Management-Netz und das VM-Netz eingezeichnet. Diese Netze werden gegebenenfalls geroutet.

Über das Management-Netzwerk wird mit den Hyper-V-Hosts kommuniziert. Hierzu gehören unter anderem Dateizugriff, WMI-Zugriffe, das Backup und Kommunikation der System Center-Agenten. Dieses Netz hat deshalb sowohl "IP" wie auch den "Client für Microsoft Netzwerk" und die "Datei und Druckfreigabe" gebunden. Über das CSV- oder Heartbeat-Netzwerk stellt der Cluster einerseits fest, ob es den anderen Cluster-Knoten gut geht (Heartbeat) und andererseits wird hierüber bei Ausfall einer Storageanbindung eines Hosts der Traffic zum Storage über einen anderen Host umgeleitet. Ebenso wird dieses Netz benutzt, wenn beispielsweise beim Backup eines CSV-Volumes über die Koordinator-Node exklusiv auf das Storage zugegriffen wird. Für dieses Netz müssen Sie deshalb sowohl "IP" wie auch den "Client für Microsoft Netzwerk" und auch die "Datei und Druckfreigabe" konfigurieren. Über das VM-Netzwerk kommunizieren die virtuellen Maschinen mit ihrem "normalen" Netzwerk. Im Hyper-V sollten diese Karten nichts gebunden haben, außer das "Protokoll für Microsoft virtuelle Netzwerk-Switch". Über das Live Migration-Netzwerk wird bei der Live Migration der Speicher der VM von einem Cluster-Knoten auf den anderen übertragen. Da die VM weiterläuft und dadurch noch während der ersten Übertragung des Speichers schon wieder Veränderungen am Speicher vorkommen, sollte dieses Netz sehr performant angebunden sein. In der Beispielkonfiguration ist sowohl "IP" wie auch den "Client für Microsoft Netzwerk" und auch die "Datei und Druckfreigabe" angelegt. Die letzten beiden sind aus Gründen der Redundanz für das CSV-Netz vorhanden



Quelle: Carsten Rachfahl

Schema eines Netzwerks im Hyper-V-Cluster

und können auch wegfallen. Das letzte Netzwerk ist die iSCSI-Anbindung: Sie dient als Anbindung der Cluster-Knoten an ein vorhandenes iSCSI-Storage-System. Hier ist nur die IP-Bindung notwendig. *(Carsten Rachfahl/jp)*

Weitere Informationen zu Microsoft Hyper-V finden Sie unter www.hyper-v-server.de.

Ich arbeite im Client-Support unseres Unternehmens und durch eine Umstrukturierung supporten wir nun auch unseren – weltweit aktiven – Außendienst. Diese Anwender berichten mir häufig von unglaublich **langsamen Netzwerkverbindungen** oder fast **kriminell hohen Kosten** für einen **Internetzugang**. Dennoch sind diese Kollegen, die teilweise wochenlang unterwegs sind, auf Outlook und eine **Verbindung zu Exchange** angewiesen. Ich empfehle den Kollegen dann im Offlinemodus zu arbeiten und erst bei einer geeigneten Gelegenheit mit Outlook online zu gehen. Doch ist das wirklich der Weisheit letzter Schluss?

Beim Arbeiten mit Outlook und Exchange-Server im Onlinemodus empfangen und versenden Sie neue Nachrichten sofort. Aber Sie haben Recht, manchmal ist es besser, nicht im Onlinemodus zu arbeiten. Denkbare Beispiele sind etwa Situationen, in denen der Anwender keine Netzwerkverbindung hat oder die Gebühren für eine solche Verbindung – etwa in einem Hotel – die Schmerzgrenze des Spesenkontos überstrapazieren. Um Ihren Anwendern Hinweise geben zu können, wann sie auf den Onlinemodus verzichten sollten oder können, lassen Sie uns einen Blick auf die Funktionsweisen von On- und Offlinemodus werfen: Verbindet sich ein Konto mit Microsoft Exchange, werden die Nachrichten im Postfach des Servers gespeichert. Im Normalfall – bei hergestellter Verbindung zum Server und beim Arbeiten im Onlinemodus – stehen den Anwendern alle Funktionen von Outlook zur Verfügung (insbesondere das Öffnen/Löschen von Elementen und das Verschieben von Elementen zwischen Ordnern). Arbeiten Ihre Kollegen jedoch offline, verlieren sie den Zugriff auf alle Elemente auf dem Server. In diesem Fall sind Offlineordner nützlich, die Outlook in einer Offlineordnerdatei (OST-Datei) auf dem Computer speichert. Die OST-Datei ist eine Kopie des Exchange-Postfachs und wird im Onlinemodus automatisch mit dem Server synchronisiert. Sie können Outlook zum automatischen Starten im Offlinemodus konfigurieren, wenn keine Verbindung zu Exchange besteht. Zudem haben die Anwender die Möglichkeit, zwischen dem Offline- und Onlineverbindungsstatus manuell zu wechseln, und können angeben, welche Exchange-Ordner lokal auf dem Computer stets aktualisiert werden sollen. Verwenden die Anwender ein Exchange-Konto, empfiehlt sich das Arbeiten im Exchange-Cache-Modus. Dies ist insofern sehr vorteilhaft, als dass der Exchange-Cache-Modus die meisten Gründe für den Offlinebetrieb beseitigt. Eine unterbrochene Netzwerkverbindung beeinträchtigt die Arbeit im Grunde nicht, da weiterhin mit den Elementen gearbeitet werden kann. Im Detail erstellt und verwendet der Exchange-Cache-Modus eine Offlineordnerdatei (OST) und lädt eine synchronisierte Kopie der Elemente aller Ordner des Postfachs herunter. Die Anwender arbeiten also mit den Informationen auf dem Computer, während Outlook die Synchronisierung mit dem Server vornimmt. Selbst bei einer Unterbrechung einer aktiven Verbindung mit Exchange können die Außendienstler trotzdem mit ihren Daten weiterarbeiten. Bei Wiederherstellung der Verbindung werden Änderungen automatisch von Outlook synchronisiert, so dass die Ordner und Elemente auf dem Server wieder mit den auf dem Computer befindlichen identisch sind. Das Management der Serververbindung und das Aktualisieren der Daten nimmt Outlook dabei automatisch vor. Anwender müssen weder in den Offlinebetrieb wechseln noch versuchen, die Verbindung zum Server wiederherzustellen. Im Exchange-Cache-Modus müssen Sie auch keine Übermittlungsgruppen einrichten, da in diesem Modus die Ordner ausgewählt werden, die offline verfügbar sein sollen, und diese regelmäßig synchronisiert werden. Ein möglicher Grund, dennoch offline zu arbeiten, ist die bessere Kontrolle darüber, welche Elemente in die lokale Kopie des Exchange-Postfachs heruntergeladen werden. Dies könnte bei einem Verbindungsgerät beziehungsweise einem Verbindungsdienst relevant sein, bei dem Gebühren nach übertragener Datenmenge berechnet werden. *(jp)*

Bei **Terminal-Diensten** und **XenApp-Umgebungen** kommt es bei uns gelegentlich zu Problemen bei Druckaufträgen – meist verursacht durch **schlechte Multithreading-Leistung** der nicht-nativen Herstellertreiber. Kann ich das Installieren aller Druckertreiber auf XenApp-Servern unterbinden?

Ja, das ist in der Tat möglich. Das vollständige Unterbinden der Installation kann ein sinnvoller Schritt sein, da Druckertreiber von unterschiedlichen Quellen aus auf den Server gelangen können. Dazu zählen beispielsweise RDP-Verbindungen, Netzwerkdrucker, Nutzerprofile sowie erstellte Kopien. Bevor Sie die Installation neuer Drucker verhindern, möchten Sie unter Umständen zunächst alle bisherigen nicht-nativen Drucker deinstallieren. Verwenden Sie dazu am besten das Tool "Print Detective", das Citrix online bereithält. Um die künftige Treiberinstallation zu unterbinden, müssen Sie eine Änderung in der Registry vornehmen (es empfiehlt sich daher, sicherheitshalber vorher ein Backup der Datei anzufertigen):

1. In der XenApp Advanced Configuration Console zunächst den Punkt "Policies / Create Policy" auswählen und die Richtlinie entsprechend benennen.
2. Die neu erstellte Richtlinie auswählen und die Verzeichnisse "Printing" beziehungsweise "Drivers" ausklappen.

3. Wählen Sie "Native printer driver auto-install".
4. Im Anschluss "Enabled und Do not automatically install drivers" selektieren. So wird das XenApp-Drucksystem an der Installation von nativen Druckertreibern gehindert, wenn sich Nutzer neu verbinden.
5. Mit einem Rechtsklick auf die Richtlinie wählen Sie im Dropdown "Apply this policy to".
6. Mittels des Filters "Servers" wenden Sie die Policy auf einen oder mehrere Server der Umgebung an.
7. Öffnen Sie den folgenden Registry-Key auf den Servern, auf denen die soeben erstellte Policy Anwendung finden soll: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Environments\Windows NT x86\Drivers\Version-3
8. Mit einem Rechtsklick auf den Version-3-Schlüssel setzen Sie nun die Rechte für alle Accounts auf der ACL auf "Lesen". Die vererbten Standard-Rechte müssen vor den Anpassungen kopiert werden. Um zusätzlich auch das Installieren von 64-Bit-Treibern zu verhindern (unabhängig davon, ob es sich um ein 64-bit System handelt), nehmen Sie die gleichen Änderungen auch im Version-3-Key unter "Windows x64" vor.

Bei künftigen Versuchen, Treiber zu installieren, sollte dieses Vorhaben nun mit einer "Zugriff verweigert" Fehlermeldung abgelehnt werden. *(Citrix/jp)*

Linux

Ich **installiere regelmäßig meine Linux-Systeme mittels PXE-Boot** aus dem Netzwerk heraus. Hierzu laden die Systeme eine individuelle TFTP-Konfigurationsdatei von einem zentralen Server. In dieser Datei sind sämtliche Informationen, die ein System zum Installieren benötigt, enthalten. In letzter Zeit ist es öfters vorgekommen, dass Systeme, die einen SAN-Anschluss haben, **Daten auf dem SAN zerstört haben**. Die Installation sollte dabei aber auf den lokalen Platten stattfinden, anscheinend war dies aber nicht der Fall, stattdessen wurde die Installation auf den SAN-Platten durchgeführt. Wie kann ich in Zukunft verhindern, dass während der Installation versehentlich auf die SAN-Platten geschrieben wird?

Die Lösung für das beschriebene Problem ist recht einfach. Der **Linux-Installer Anaconda** kennt eine Option, mit der der Zugriff auf die SAN-Festplatten während der Installation unterbunden wird. Hierfür sind lediglich die Treiber, über die der Zugriff stattfinden würde, zu blacklisten. Diese Option ist in der TFTP-Konfiguration für ein zu installierendes System als weiteres Kernel-Argument mit anzugeben. Kommt beispielsweise ein QLogic HBA zum Einsatz, so lautet der entsprechende Eintrag für die Konfigurationsdatei:

```
blacklist=lpfc blacklist=qla2xxx
```

(Thorsten Scherf/jp)

Ich arbeite im Client-Support und wir **migrieren** in unserem Unternehmen **aktuell von XP nach Windows 7**. Dabei führen wir auch die aktuelle Version des MS Internet Explorer ein. Allerdings gibt es auch eine gewisse Anzahl von Kollegen in bestimmten Fachabteilungen, die **weiter den IE 6 nutzen müssen**, um mit ihren Applikationen arbeiten zu können. Nun möchten wir allerdings vermeiden, dass zukünftig zwei Client-Betriebssysteme im Unternehmen supportet werden müssen. In einem Gespräch mit einem Kollegen, der sich um unsere virtualisierten Server kümmert, erfuhr ich nun, dass wir VMwares Thinapp lizenziert haben und dass sich mit diesem Tool meine Aufgabenstellung lösen ließe. Stimmt das?

Jedes Unternehmen, das eine Migration von einer Internet Explorer-Version auf eine andere Version durchgeführt hat, weiß um die Herausforderungen, die damit einhergehen. Einige Webapplikationen benötigen zeitaufwendige Anpassungen, um mit aktuellen Internet Explorer-Versionen kompatibel zu werden. VMware Thinapp als Werkzeug der **Applikationsvirtualisierung** erlaubt es, durch einen Pre-Scan und einen Post-Scan Snapshot-Pakete zu erstellen, die in einer "virtuellen Blase" isoliert und ausgeführt werden. Dadurch vermeiden Sie Konflikte mit der lokal installierten Version. So lässt sich der Internet Explorer 6 auch auf Windows 7 ausführen und für inkompatible Webapplikationen nutzen. Alles, was sie hierfür brauchen, ist eine virtuelle Maschine (mit Windows XP SP2) mit dem Thinapp Setup Capture Client. Die Erstellung der Capture Umgebung ist sehr leicht [1] und nachfolgend müssen Sie nur wenige Schritte ausführen:

1. Starten der Capture-Maschine, um diese bis zu dem gewünschten Stand mit Security Patches zu aktualisieren.
2. Starten des Setup Capture Clients, Ausführen des Pre-Scans der Betriebssysteminstallation.
3. Klicken Sie auf den Internet Explorer-Button, um den IE aus dem Betriebssystem zu ziehen.
4. Optional können Sie nun alle Plug-Ins installieren, die noch in das Paket integriert werden sollen.
5. Ausführen des PostScans der Betriebssysteminstallation inklusive der Anwendungsinstallation.

Als Ergebnis erhalten Sie eine einzige EXE- und/oder MSI-Datei, die Sie in Ihrer Softwareverteilung oder durch einfaches Kopieren nutzen können. Mehr Informationen hierzu finden Sie unter [2]. *(VMware/jp)*

Link-Codes: [1] B8PE1, [2] B8PE2

Tools

Wenn der IT-Verantwortliche sehr große Datenmengen zu bewältigen hat, muss oft auch sein Budget den Kauf einer vergleichsweise teuren Software oder Appliance bewältigen. Doch im Open Source-Bereich finden sich **Storage-Werkzeuge**, die professionelle Features wie **Deduplizierung** und die Verwaltung mehrerer TBytes bieten. Und wenn dieses Tool dann noch auf dem äußerst leistungsfähigen und zukunftssicheren **ZFS-Dateisystem basiert**, lohnt unter Umständen eine interne Teststellung.

Die Community-Edition von **NexentaStor**, eine Storage-Software auf Open Solaris-Basis, ist in Version 3.0 gratis als Download verfügbar. Dabei bringt NexentaStor die angesprochene Deduplizierung für das verwendete Dateisystem ZFS mit und erlaubt das Anlegen von Quotas für User und Gruppen. Dabei ist die Nutzung der Community-Edition bis zu 12 TByte verwendetem Speicherplatz kos-

Über das Dashboard des freien Storage-Tools NexentaStor lassen sich Funktionen wie etwa die Deduplizierung steuern

tenlos. NexentaStor steht als CD- und als VMware-Image zum Download bereit. Die Installation des ISO CD-Images erfolgt dabei auf nackter x86/64-Hardware, wobei der Installer die Kompatiblität im Rahmen der Installation prüft. Das herausstechende Merkmal von Nexenta ist das Dateisystem ZFS. Es verbindet die sonst voneinander getrennt operierenden Massenspeicherkomponenten RAID, Volume-Manager und Dateisystem. Dadurch, dass das RAID zum Dateisystem gehört, fallen Rebuilds ausgefallener Platten ungeheuer schnell aus, da das Dateisystem nur bereits belegte Blöcke und nicht pauschal alle wiederherstellt. ZFS verwaltet zudem auf Verzeichnisebene sogenannte "Generationen", die einem Anwender, der versehentlich eine Datei löscht oder ändert, erlauben, über Funktionen des Dateisystems auf eine frühere Version der Datei zurückzugreifen. Als 128-Bit-Dateisystem kennt ZFS zudem keine Grenzen für Datei- oder Volume-Größen, welche sich mit heutiger oder künftiger Hardware erreichen ließen. *(jp)*

Link-Code: B8PE3

Im Arbeitsalltag spielen **virtuelle Festplatten** mittlerweile eine wichtige Rolle, denn in ihnen werden die virtuellen Maschinen, seien es nun Server oder Clients, abgelegt und gespeichert. Nicht selten müssen Administratoren diese virtuellen Festplatten vom Format eines Anbieters in ein anderes **konvertieren**, beispielsweise von VHD nach VMDK. Dafür gibt es auch zahlreiche, bewährte Tools. Doch was tun, wenn einmal eine Rückkonvertierung notwendig wird?

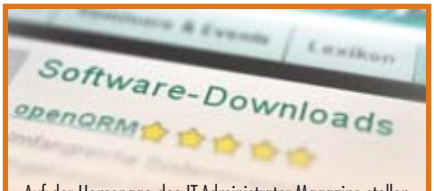
Die freie Software **Starwind V2V-Converter** wandelt VHD in VMDK um und beherrscht auch den Weg in die andere Richtung. Darin unterscheidet sie sich von den Tools anderer Anbieter, die Konvertierung nur in eine Richtung erlauben. Das Tool kopiert das Quell-Image Sektor für Sektor in das Zielformat, ohne die Ausgangsdatei zu verändern. Es unterstützt sowohl beim VMDK- als auch beim VHD-Format die dynamische und statische Variante (Erstere wächst mit steigenden Platzbedarf, die Größe der Zweiteren ist von Anfang an fest vorgegeben). Zudem erlaubt der Starwind V2V-Converter die einfache Migration von virtuellen Maschinen aus dem Direct Attached Storage in den Shared Storage. So lassen sich VMDK- und VHD-Images sicher in das SAN verschieben. Dadurch ermöglicht das Tool dem Administrator, VMware-Features wie VMotion, DRS und VCB zu nutzen. Das Produkt ist nach Registrierung kostenlos erhältlich. *(jp)*

Link-Code: B8PE4

Windows Server Core ist die bevorzugte Installationsvariante, um einen Hyper-V-Server einzurichten, da sie weniger Ressourcen als die Vollversion des Servers erfordert. Zudem bietet Server Core durch die seltenere Notwendigkeit des Patching und eine kleinere Angriffsfläche ein Mehr an Sicherheit. Dem steht auf Administrations-Seite jedoch die **Abwesenheit einer vollwertigen GUI** gegenüber und so ist das lokale Management eingeschränkt. Gleiches gilt für den kostenlosen Hyper-V Server 2008 R2, bei dem es sich im Prinzip um Server Core mit Reduktion auf die Hyper-V-Rolle handelt. Gegenüber der spartanischen Ausstattung von Server Core 2008 legte Server Core 2008 R2 immerhin *sconfig.exe* nach, ein menügeführtes Konfigurationsprogramm im Textmodus. In kleineren Umgebungen ist für die Administration der VMs der Hyper-V-Manager vorgesehen, der remote entweder auf einer Vollinstallation von Windows Server ausgeführt wird oder sich als Teil von RSAT auf einer Workstation installieren lässt.

Der kostenlose **5nine Manager for Hyper-V** füllt als GUI-Tool die Lücke bei der Verwaltung virtueller Maschinen. Das Werkzeug deckt weitgehend die Funktionen ab, die Microsofts Hyper-V-Manager im Rahmen der Remote-Verwaltung bietet. Es ermöglicht dem Administrator grundlegende Operationen wie Starten, Stoppen oder Anhalten einer VM. Ebenso ist das Editieren der Einstellungen und das Erstellen von Snapshots möglich. Im Vergleich zum Hyper-V-Manager bietet 5nine ausführlicheres Monitoring von CPU-, Speicher- und Netzwerknutzung. Darüber hinaus gibt das Tool im Detail Auskunft über die virtuelle Hardware eines Gastsystems. Besonders hilfreich ist 5nine bei der Konfiguration von Netzwerken, da sich mit einer lokal ausgeführten Software im Vergleich zum Remote-Management hier Probleme besser beheben lassen. Das .NET-Programm ist nur etwas mehr als 1 MByte groß, lediglich das .NET-Framework muss nachinstalliert werden, was aber das Setup von 5nine selbst erledigt. Der kostenlose Download ist nach Registrierung verfügbar. *(jp)*

Link-Code: B8PE5



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

Systemmonitoring-Ansätze im Vergleich

Alles im grünen Bereich

von Stephan Hucke

Idealerweise weiß der IT-Administrator, dass mit einem System etwas nicht stimmt, bevor es die Benutzer merken. Doch der Alltag sieht meist anders aus: reaktives Handeln, fehlende Gesamtübersicht und umständliches Monitoring der Systemlandschaft durch einzelne Herstellertools oder gar manuell. Hier kann systematisches Systemmonitoring Abhilfe schaffen. Dabei müssen es nicht einmal immer teure Monitoring-Suiten sein, auch der Open Source-Bereich hat inzwischen einiges zu bieten.

Quelle: Vsty - Fotolia.com

Zwar lassen sich viele unterschiedliche TCP/IP-Protokolle zur Übermittlung der Daten verwenden, SSH etwa zum Anstoßen eines lokalen Skriptes oder auch Telnet, das im Vergleich zu SSH aber keine Verschlüsselung nutzt. In der Praxis läuft es jedoch meist auf das SNMP-Protokoll hinaus. Das Protokoll stellt die kleinste gemeinsame Einheit zur Überwachung und Steuerung jeglicher Hardware dar. Es agiert auf dem Session-Layer mit dem Monitoring-Tool. Neben der Lese- und Schreibfähigkeit unterstützt es die Datenlieferung in SNMP v1 über TCP, SPX oder UPD, allerdings sind die Authentifizierungsmöglichkeiten gering. Schutz bieten lediglich die in "Lese-/Schreibzugriff" und "reiner Lesezugriff" aufgeteilten Communities mit ihren eigenen, in Klartext übertragenen Passwörtern. SNMP existiert bereits in Version 3. Neben allen v2-Funktionalitäten beherrscht es 64-Bit-Zähler, Benutzerkonten und Authentifizierung, zusätzlich die Verschlüsselung in DES oder AES unter Nutzung von VACM.

SNMP ist Standard

Aktuellere Hardware unterstützt meist alle Varianten, in der Praxis wird aber SNMP v1 innerhalb von LANs hinter der Firewall bevorzugt eingesetzt. Die Gründe sind Performance, Einfachheit und Kompatibilität. Bei SNMP v1 werden lediglich ein oder zwei "Community-Namen" konfiguriert. Nur bei besonderem Bedarf wie beispielsweise der ISO27001-Zertifizierung ist es sinnvoll, SNMP v3 zu nutzen. V3 bietet zwar Abwärtskompatibilität, ist aber sehr komplex und zeitaufwendig zu konfigurieren.

Funktionen wie SNMP-WALK prüfen, welche Geräte, Objekte und Informationen sich abfragen lassen. Die anschließende Konfiguration von Parametern, Schwellenwerten, Ausführungszeitplänen und das Hinterlegen von verantwortlichen Kontaktpersonen dienen der Auswertung und der Benachrichtigung im Bedarfsfall. Die Benachrichtigung kann über Telefon, E-Mail, SMS oder Instant-Messaging erfolgen. Das Entsenden von aktiven SNMP-Checks durch das Monitoring-Tool liefert Statusdaten in fest konfigurierten Intervallen und validiert sie nach einer fixen Anzahl an Prüfungen von Soft-State- zu Hard-State-Zuständen. Diese sogenannten SNMP-GETS fragen Daten im Auftrag der Anwendung aktiv ab.

Eine moderne Überwachungslösung sollte jedoch zusätzlich den Empfang von passiven SNMP-TRAPS unterstützen. Bei diesem Verfahren werden die Gerätekomponenten so konfiguriert, dass sie bei zeitkritischem Status selbständig Ereignisse über einen aktiven Agenten übermitteln. Die Kommunikationsmöglichkeiten zwischen SNMP und Hardware ergeben sich durch die hardwareseitig integrierten und in der Monitoring-Anwendung migrierten MIBs (Management-Information-Base, also Beschreibungsdateien) der Hersteller oder können durch die menschlich lesbaren Object Identifier (OIDs) manuell eingepflegt werden. OIDs sind meist in umfangreichen Listen im Internet zu finden.

Agentenbasierte Überwachung

Durch den Einsatz von SSH- oder tooleigener Daemons können lokal installierte Skripte etwa in Shell oder Perl mit ihren Commands ausgeführt werden, um Antworten zu erhalten. Der Login kann dabei per Public Key-Verfahren erfolgen. Auch Syslog-Events lassen sich über aktive Checks direkt abfragen. Eine andere Methode ist der Einsatz eines lokalen Agenten. Er wird vom Monitoring-Server aktiv angefragt, sämtliche ungefilterte Informationen zu liefern. Für Linux/Unix-Umgebungen bietet sich NET-SNMP ab Version 5 mit eigenem Daemon an. Er enthält eine Vielzahl an nützlichen Kommandozeilen-Tools, Agenten und Bibliotheken, welche die Grundlage für die SNMP-Implementierung im Open Source-Bereich darstellen.

Unter Windows müssen die Daten des Eventlog auf eine andere Art als in der Unix-Syslog abgefragt werden. Hier besteht keine direkte Transfermöglichkeit der Plug-Ins. Grundsätzlich bieten windowsbasierte Systeme unterschiedliche Möglichkeiten zur Abfrage an, beispielsweise NSClient++, OpMon-Agent, NC_Net. Dazu kommen die herstellerspezifischen Möglichkeiten des jeweiligen Tools. Wichtig dabei ist, dass der entsprechende Agent auf dem Windows-System aktiv ist.

Checks ohne Agenten

Bei der Frage nach clientless oder client-based Monitoring ist ein grundlegendes Problem, dass die binäre Implementierung von Clientsoftware einen Eingriff in das bestehende System darstellt und möglicherweise Probleme hervorruft. Deshalb kommen häufig agentenlose Standardmethoden zum Einsatz. Windows-basierte Workstations und Server bringen die WMI-Schnittstelle bereits mit, so dass eine direkte lokale Installation auf dem Client-PC unnötig ist. Die Schnittstelle besitzt Lese- und Schreibfähigkeit und kann auf fast alle Einstellungen des Systems zugreifen – sowohl auf Betriebs- als auch Anwendungsebene. Zur Überwachung werden daher häufig Perfmon-Werte, Ereignis-Protokolle, Inventardaten oder Dienste und Prozesse ausgewertet. Es handelt sich dabei um eine Query-Language, die eine Anmeldung am System erfordert und für die Administration und Fernwartung besonders hilfreich ist. Voraussetzung ist ein bestehender Windows-Server, der alle WMI-Skripte installiert hat. Er stellt das Kommunikationsprotokoll für die Übermittlung der Daten zwischen WMI-Proxy und Monitoring-Tool bereit. Das Protokoll sorgt dafür, dass die Parameter an die lokalen Plug-Ins übergeben werden.

SAP über CCMS verwalten

CCMS (Computer Center Management System) ist ein SAP-eigenes Monitoringwerkzeug, das der zentralen Überwachung der SAP Netweaver-Komponenten dient. Dadurch lässt sich das Verhalten von SAP-Systemen bewerten und ihre größtmögliche Verfügbarkeit sicherstellen. Der SAP-Alert-Monitor als Monitorsammlung empfängt Daten unter anderem von Agenten der Satellitensysteme, die Auskunft über Performance- oder Zustandsdaten abliefern. Dazu gehören unter anderem Speicher-/CPU-Auslastung, Disk I/Os, Datenbanken, Antwortzeiten, Ausgabesteuerung oder Security-/Systemlogs. SAP liefert dazu verschiedene sinnvolle Templates, die sich manuell ergänzen lassen. Auf der Monitoring-Seite ist ein Client installiert, der mit aktiven Plug-Ins die CCMS-Daten über eine der RFC-Schnittstellen abfragt. Voraussetzungen für den Remotezugriff sind die Installation der SAP-Bibliotheken auf Windows und Linux/Unix. Je nach Tool können auch SLA-Reportings, Business-Process-Monitoring und Trendanalysen zur Funktionalität gehören.

Systemnahe Applikationen

J2EE-, Web-, Domain-Name-, E-Mail-, Fileserver, Proxies und entsprechende Queues lassen sich problemlos über die netzwerkfähigen Protokolle SMTP, HTTP, DNS, DIG, POP3, IMAP oder FTP abfragen (mit oder ohne Verschlüsselung). Nicht jedes Protokoll besitzt passende Plug-Ins. Individuell bestehende Plug-Ins nutzen die Protokolle, um zu prüfen, ob der TCP- oder UDP-Port offen ist und dort ein Dienst existiert. Für eine Überwachung in die Tiefe finden spezifische Agenten Verwendung. Die Antworten wertet das Monitoring-Tool aus.

Auch ESX-, KVM-, Citrix- oder Xen-Farmen können im Bereich der Auslastung einzelner Komponenten überwacht werden, desweiteren Traffic, eingeloggte User, Lizenzen oder laufende Sessions. Abfragen

Eine gute Monitoring-Lösung sollte für Überblick sorgen und wesentliche Informationen auf einen Blick ausgeben

Sensoren vor Ort

Rechenzentren und Serverräume unterliegen besonderen Sicherheitsvorschriften. Schon ein Kabelbrand im Serverschrank kann katastrophale Folgen für ein Unternehmen haben. Für entsprechende Hardware oder potentialfreie Schaltungen, etwa an Zugangstüren, können Zustände über einen Agenten über das SNMP-Protokoll abgeholt, ausgewertet, validiert und an die hinterlegte Kontaktperson oder -Gruppe gesendet werden. Um Auskunft über klimatische und räumliche Gegebenheiten, seismographische Aktivitäten, Statusinformationen der USV bis hin zu kompletten Produktionsanlagen zu bekommen, gibt es unterschiedliche Module etwa für Rauch, Gas, Wasser, Erschütterung oder Bewegung.

werden über die vom Hersteller gelieferten APIs abgewickelt, so dass keine zusätzliche systemseitige Installation nötig ist.

Das passende Produkt finden

Der Monitoring-Markt bietet viele Lösungen. Während sich in großen Unternehmen meist HP OpenView oder IBM Tivoli wiederfinden, greift der Mittelstand gerne auf What's Up Gold oder SolarWinds "Orion" zurück. Das Unix-basierte HP OpenView ist besonders auf große IT-Landschaften ausgelegt und stellt eigentlich eine Suite dar, die um unzählige Einzelwerkzeuge erweitert werden kann. In Überwachungsszenarien findet der HP Network Node Manager Verwendung. Er spielt seine Stärken bei HP-Komponenten aus und bietet viele Automatisierungen und eine einfache Konfiguration. Die Kehrseite: Durch die umfangreichen Funktionalitäten und Wertedarstellungen wird es schnell komplex, weshalb langwierige Einarbeitungen und Schulungen nötig sind.

Zu den sehr hohen Lizenzkosten addieren sich Support und Folgekosten, etwa Subscription oder Zusatzmodule. Gleiches gilt für IBM Tivoli. Bei entsprechender Unternehmensgröße bewegen sich die Kosten daher schnell im sechsstelligen Bereich. Die ausgeprägte Funktionalität führt also zu einer starken Abhängigkeit zum Hersteller. Firmen mit weniger üppigem Budget bedienen sich daher gerne kleinerer Überwachungsalternativen. Das Windows-basierte What's Up Gold sowie Orion steigen mit wesentlich niedrigeren Lizenzkosten ein. Erweiterungen und Monitoringaufwand (beispielsweise die Anzahl zu überwachender Geräte) werden extra abgerechnet, genauso wie der kostenpflichtige Support.

Vor diesem Hintergrund stellt Open Source eine interessante Option zu teuren und häufig überdimensionierten kommerziellen Lösungen dar. Da kann die ehrliche Beantwortung der Frage nach dem eigentlich Benötigten helfen, Kosten zu sparen und gleichzeitig effizienter und flexibler zu agieren. Neben quelloffenen Tools wie Cacti, openNMS oder MRTG sticht das Linux-basierte Framework Nagios hervor. Gründe für dessen Beliebtheit sind die sehr starke Community, die lange Entwicklungshistorie und eine große Funktionsvielfalt, die zu der hohen Marktakzeptanz und breiten Etablierung auch im Enterprise Umfeld beigetragen haben. Nagios deckt Anforderungen an halb- oder vollautomatisches Discovery mit Filterregeln, Eventkorrelation oder Visualisierung der Systemlandschaft genauso ab wie Business-Reportings, Geschäftsprozessmonitoring, Eskalationsmanagement, Recovery et cetera. Die Integration von Drittsystemen wie CMDB oder Ticketsysteme ist durch die offenen Schnittstellen jederzeit möglich.

Eine auf Nagios basierende Variante ist das relativ neue Projekt openITCOCKPIT. Der Fokus liegt hier auf der einfachen Überwachung komplexer IT-Landschaften: Das Tool (siehe Test ab Seite 32) ermöglicht plattformabhängige Visualisierung durch eine eigene intuitive Websoftware, einfache Installer und eine grafische Oberfläche. Dadurch kompensiert es die komplizierte, über Kommandozeilen erfolgende Konfiguration und Installation von Nagios. Neben eigens entwickelten Modulen, individuellem Consulting, Workshops und technischem Support gewährleisten diese Dienstleister eine sehr gute Projektumsetzung der Anforderungen an die eigene Infrastruktur, ohne dabei allzu tiefgreifendes eigenes Know-how im Linux-Bereich vorauszusetzen.

Ob Closed oder Open Source: Die Lösungen unterscheiden sich neben dem Lizenz- und Supportmodell maßgeblich im Funktionsumfang. Dazu zählen die Visualisierung etwa mit einer Graphenerstellung oder einer individualisierbaren Infrastruktur-/Monitoringübersicht. Auch die Umsetzung einer einfachen Konfiguration ist eine entscheidende Voraussetzung für Bedienbarkeit und Leistung. Die eigenen Anforderungen sollten Administratoren daher genau mit denen der favorisierten Lösung abgleichen, denn langfristig kann die Kostenschere stark auseinanderklaffen.

Fazit

Gute Monitoring-Lösungen überwachen die Systeme zentral und einheitlich. Sie helfen, die täglichen Routinearbeiten am System zu automatisieren – und damit letztendlich zu verringern. Die IT bleibt dabei individuell skalierbar und zeigt rechtzeitig bedenkliche Entwicklungen. Eine solche Überwachung führt langfristig zu einer wertschöpfenden IT, die Stabilität, Qualität, Effizienz und Transparenz schafft. Neben einer einfachen Konfiguration sollte eine moderne Lösung die Möglichkeit bieten, auch komplexe Prozesse, Dienste oder SLAs übersichtlich zu visualisieren. *(dr)*

Stefan Hucke ist Consultant für Systemmanagement bei it-novum.

Lizenzmanagement für Administratoren

Überblick behalten

von Horst Speichert

Ein effektives Lizenzmanagement ist im IT-Betrieb einerseits notwendig, um die Kontrolle über das Budget zu behalten, andererseits, um rechtlich sauber dazustehen und so Unterlizenzierung zu vermeiden. Doch was leicht klingt, ist in der Praxis ein komplexes Feld mit zahlreichen Fallstricken. Dieser Beitrag stellt daher die rechtlichen Grundlagen des Lizenzmanagements ebenso dar wie die notwendigen Prozesse.

Ein Verstoß gegen eine Softwarelizenz ist schneller begangen als gedacht, wie auch ein von Aagon erstellter Leitfaden [1] zeigt. Denn schon die Installation eines gerade benötigten Programms von einem Originaldatenträger kann einen Lizenzverstoß verursachen, wenn keine entsprechende Nutzungslizenz für das Programm (mehr) frei ist. Die Gesetzeslage ist bei solchen Lizenzverstößen eindeutig, denn das Urheberrecht stellt die unrechtmäßige Nutzung von Software unter Strafe. Haftbar sind dabei sowohl die Unternehmen selbst als auch die für die Einhaltung von Lizenzverträgen verantwortlichen Personen.

Und es wird noch vertrackter: Denn um zu beweisen, dass der Anwender auch tatsächlich über eine gültige Lizenz für ein Programm verfügt, müssen die entsprechenden Lizenzen zu den installierten Programmen gut verwahrt und bei Bedarf nachweisbar sein. In Unternehmen mit einer Vielzahl von Nutzern stellt dies allein bereits eine eigene Verwaltungsaufgabe dar. Ohne ein effizientes Lizenzmanagement ist diese Herausforderung praktisch nicht zu meistern.

Über- und Unterlizenzierung

Grundsätzlich unterscheiden wir beim Thema Lizenzmanagement zwischen drei Situationen: der Überlizenzierung, der Unterlizenzierung und der korrekten Lizenzierung. Bei einer Unterlizenzierung sind weniger Lizenzen vorhanden, als tatsächlich benötigt würden. Das bedeutet, dass bei Unterlizenzierung strafbare Verstöße gegen das Urheberrecht begangen werden, die im Rahmen von IT-Compliance mit rechtmäßigen Unternehmensprozessen unvereinbar sind. Erkennt ein Softwarehersteller beispielsweise im Rahmen eines Audits eine Unterlizenzierung bei einem Kunden, führt dies meist zu kostspieligen Nachlizenzierungen. Komplexe Lizenzverträge führen hingegen häufig zu wirtschaftlich nachteiligen Überlizenzierungen, da Unternehmen im Zweifel lieber zu viele Lizenzen erwerben, um auf der sicheren Seite zu sein. Zudem wird ein hoher Prozentsatz von ursprünglich notwendiger Software nach einem gewissen Zeitablauf im Unternehmen nicht mehr verwendet. Fehlt es an einem effizienten Lizenzmanagement, kommt es hierdurch zu kostspieliger Überlizenzierung.

Daher ist das Ziel von Lizenzmanagement, der perfekten Lizenzierung so nahe wie möglich zu kommen. Im Idealfall sind dann jederzeit genauso viele Lizenzen in Nutzung, wie auch vorhanden sind. Jeder Installation einer Software geht immer eine Lizenzprüfung voraus. Und regelmäßige Kontrollen stellen sicher, dass nicht Mitarbeiter versehentlich oder vorsätzlich gegen Lizenzbedingungen verstoßen haben.

Lizenzmanagement gehört zu IT-Compliance

IT-Compliance ist schon lange kein Marketing-Schlagwort mehr, sondern fordert von Unternehmen und Organisationen ganz konkrete Maßnahmen rechtlicher, organisatorischer und technischer Art. Der Begriff bedeutet dabei allgemein gesprochen die IT-spezifische Rechtskonformität, also die Einhaltung rechtlicher Vorgaben im IT-Umfeld. Hierzu zählen auch die lizenz- und urheberrechtlichen Bestimmungen, welche erst durch ein effizientes Lizenzmanagement überwacht und eingehalten werden können. Verbunden mit IT-Compliance ist die Etablierung von Prozessen und Verfahren zur Erlangung dieser Rechtstreue. Konkret bedeutet IT-Compliance die Konformität mit

- gesetzlichen Standards, das heißt eine Einhaltung von Gesetzen und eine Beachtung der Rechtsprechung.
- Vertragspflichten, insbesondere aus Verträgen mit Kunden, Geschäftspartnern, Betriebsvereinbarungen et cetera.
- Standards (auch selbstgesetzte): Hierzu zählt die Einhaltung anerkannter Standards wie BSI oder ISO, aber auch von eigenen Policies, Nutzungsrichtlinien, Organisationshandbüchern et cetera.

Aus der Blickrichtung der angestrebten Ziele definiert sich IT-Compliance als die wirksame Verhinderung von Informationsverlust (Wirtschaftsspionage), Rechts- und Lizenzverstößen, Straftaten und Falschbilanzierung. Damit stellen IT-Compliance und Lizenzmanagement auch einen wichtigen Baustein für das

Risikomanagement eines Unternehmens dar, da andernfalls gravierende Schäden durch Rechtsverletzungen und Imageverluste drohen.

Zentrale gesetzliche Vorschriften für das Informations- und Risikomanagement sind etwa das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), der Deutsche Corporate Governance Kodex, Basel II, die Mindestanforderungen an das Risikomanagement (MaRisk), die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) sowie die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Die Aufzählung ist dabei bei weitem nicht abschließend, sondern benennt nur wichtige Bestimmungen. Der Deutsche Corporate Governance Kodex bestimmt beispielsweise in Punkt 4.1.3: "Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)".

Die Vorschrift benennt hier deutlich den Zusammenhang zwischen Compliance und der Einhaltung gesetzlicher Vorschriften und stellt klar, dass IT-Compliance und Lizenzmanagement originäre Aufgaben der Unternehmensleitung sind.

Lizenzmanagement als Prozess

Software macht sowohl bei den IT-Kosten wie auch beim Anlagevermögen eines Unternehmens einen immer größeren Prozentsatz aus. Um das Anlagevermögen eines Unternehmens im Bereich Software bewerten zu können, muss dessen Buchhaltung entsprechend wissen, welche Software (Lizenzen) das Unternehmen tatsächlich besitzt. Anders gesagt: Erst durch ein effizientes Lizenzmanagement lässt sich das eigene Anlagevermögen im Bereich der Software-Assets detailliert und beweissicher führen. Der angenehme Nebeneffekt des Software-Asset-Managements ist, dass IT-Verantwortliche dann auch auf Forderungen von Softwareherstellern nach Lizenzierungsnachweisen revisionssicher und konfliktfrei reagieren können. Sofern im Unternehmen oder Konzern eine interne Verrechnung von IT-Dienstleistungen erfolgt, kann das moderne Lizenzmanagement schließlich auch dafür eine gute Unterstützung sein. Denn Lizenzmanagement verbessert auch die Budgetplanung und -kontrolle im IT-Umfeld.

Inventarisierung vorhandener Software und Lizenzen

Der erste Schritt eines Software-Asset-Managements ist die Inventarisierung aller im Unternehmen vorhandenen Programme und Lizenzen. Mit Hilfe eines Clientmanagement-Systems (CMS) ermittelt hierbei ein Software-Agent regelmäßig auf allen Arbeitsplatzrechnern und Servern die dort installierte Software und speichert diese in einer zentralen Datenbank ab.

Im nächsten Schritt muss ein Administrator, Lizenzverwalter oder eine andere dazu ermächtigte Person die im Unternehmen vorhandenen Lizenzen in dem Lizenzmanagement-Modul des CMS erfassen. Hierfür ist oftmals die rechtliche Prüfung und Auslegung der vorhandenen Lizenzverträge erforderlich, was sowohl Fachwissen als auch große Sorgfalt erfordert. Denn Software- oder Lizenzverträge können eine Vielzahl von Chancen wie eine Ausdehnung von Nutzungsrechten (zum Beispiel bis wann ist ein Update kostenlos), aber auch Risiken wie Abmahnungen, Vertragsstrafen bis hin zu Strafanzeigen bei Falschauslegung für das Unternehmen enthalten. Bei vielen und komplexen Lizenzverträgen bietet es sich an, diese durch ein angebundenes Vertragsmanagement zu berücksichtigen und der internen Planung zuzuführen.

Gegenüberstellung und Bilanzierung

Sind inventarisierte Programme und vorhandene Lizenzen im Lizenzmanagement erfasst, ordnet im nächsten Schritt ein technisch versierter Mitarbeiter die bei der Inventarisierung gefundenen Softwarepakete den entsprechenden Lizenzpaketen zu. Dies kann in bestimmten Fällen ganz einfach und fast automatisch ablaufen. In komplexeren Szenarien wie beispielsweise bei besonderen Up- oder Downgrade-Rechten ist hier jedoch Handarbeit angesagt. Ist diese Zuordnung abgeschlossen, kann das Lizenzmanagement schließlich die Ergebnisse der Software- und Lizenzinventur gegenüberstellen. Das Ergebnis ist eine Lizenzbilanz, die aufzeigt, welche Lizenzen aktuell fehlen oder überflüssig sind.

Horst Speichert ist Rechtsanwalt in der Kanzlei esb Rechtsanwälte in Stuttgart und auf IT-Recht spezialisiert.

Compliance-Check

Sofern Lizenzen fehlen, kann zudem ein Compliance-Check darüber informieren, ob in der Folge Rechtsverstöße begangen wurden. Da Compliance nicht nur Rechtskonformität, sondern auch eine prozessorientierte Lösung im Blick hat, sind darüber hinaus Wege aufzuzeigen, wie künftige Rechtsverstöße vermieden werden.

Lizenzrechtlicher Rahmen

Eine der grundlegenden Weichenstellungen in Lizenzverträgen unterscheidet, ob eine Lizenz nur eine Bereitstellung erlaubt (Einzel-Lizenz) oder eine Mehrfach-Bereitstellung (Mehrfach-Lizenz) zulässig ist.

Lizenzmodelle der Softwarehersteller

Je nach verwendeter Lizenzmetrik können Mehrfachlizenzen dabei unterschiedlich definiert sein:

- Volumenlizenz (umfasst eine bestimmte, festgelegte Anzahl von Lizenzen)
- Standortlizenz (alle Bereitstellungen innerhalb eines festgelegten Standortes)
- Unternehmenslizenz (alle Bereitstellungen innerhalb eines Unternehmens)

Eine urheberrechtliche Lizenz, also eine urheberrechtliche Nutzungs- beziehungsweise Verwertungserlaubnis, ist bei Computerprogrammen grundsätzlich jedoch nur dann erforderlich, wenn eine Nutzung erfolgen soll, die nicht bereits durch eine

gesetzliche Erlaubnis gemäß § 69d Urheberrechtsgesetz (UrhG) gedeckt ist. So darf beispielsweise gemäß Absatz 2 des § 69d UrhG einer Person, die zur Benutzung eines Programms berechtigt ist, die Erstellung einer Sicherungskopie vertraglich nicht untersagt werden, wenn sie für die Sicherung der künftigen Benutzung erforderlich ist.

Wirksamkeit von Lizenzbedingungen

Während der Installation von Software werden dem Benutzer häufig Verträge angezeigt, die dieser bestätigen muss, um mit der Installation fortfahren zu können. Hierbei handelt es sich um so genannten Endbenutzer-Lizenzverträge, englisch "End User License Agreement", kurz EULA genannt. Diese erzwungenen Vereinbarungen sind jedoch nach europäischen Rechtsmaßstäben nur eingeschränkt gültig.

Schutzhüllenlizenzen (Shrink Wrap License) wiederum sind Lizenzbestimmungen, die nach der Vorstellung des Softwareherstellers automatisch durch das Öffnen der Verpackung akzeptiert werden, obwohl der Nutzer den genauen Wortlaut erst nach dem Öffnen der Verpackung lesen kann. Ihre Wirksamkeit ist daher stark umstritten.

CPU-Klauseln schließlich sind Lizenzbestimmungen, welche die Benutzung der Software an eine bestimmte Hardware bindet. In der Praxis verbreitet sind vor allem nachfolgende Arten von CPU-Klauseln:

- Die Software darf ausschließlich auf einem bestimmten Rechner genutzt werden.
- Die Software darf nur gegen ein zusätzliches Entgelt auf einem anderen, insbesondere leistungsfähigeren Rechner eingesetzt werden.
- Nutzung auf einem anderen Rechner nur gestattet, wenn die ursprünglich lizenzierte Hardware defekt ist.

CPU-Klauseln sind dann wirksam, wenn sie individuell mit dem Anwender vereinbart wurden und nicht Teil von AGB sind. Die Rechtsprechung hält CPU-Klauseln nach § 307 Abs. 2 Nr. 1 und 2 BGB überwiegend für unwirksam, wenn Kaufrecht auf die Programmüberlassung anwendbar ist. Nur ausnahmsweise können CPU-Klauseln durch ein schutzwürdiges Interesse des Softwareherstellers gerechtfertigt sein, beispielsweise wenn das Programm in seiner Ablauffähigkeit auf einen bestimmten Computertyp angewiesen ist und ein Einsatz auf einem anderen Rechner mit Ablaufschwierigkeiten verbunden ist, die den Ruf des Softwareherstellers gefährden würden.

Im Ergebnis zeigt sich, dass viele Lizenzbedingungen rechtlich angreifbar oder unwirksam sind, auch wenn sie üblicherweise in der Praxis von den großen Softwareherstellern verwendet werden.

Einzelplatzlizenz versus Netzwerknutzung

In Lizenzbedingungen häufig anzutreffen sind so genannte Netzwerkverbote. Hierunter sind vertragliche Beschränkungen der Nutzung von Software über das lokale Netzwerk, beispielsweise im Rahmen einer Remote-Control-Sitzung, zu verstehen. Urheberrechtlich ist dabei zweifelhaft, ob die Nutzung von Software über lokale Netzwerke überhaupt in die Verwertungsrechte des Softwareherstellers eingreift.

Wird hingegen eine Software auf verschiedenen Rechnern fest gespeichert, liegt in der mehrfachen Festspeicherung in der Tat eine urheberrechtlich unzulässige Vervielfältigung durch den Nutzer vor. Das direkte Verbot der Nutzung über ein Netzwerk ist daher häufig unwirksam. Auch unzulässig sind sogenannte Site-, Installations- oder Gebäudelizenzen, die den Einsatzort einer Software festlegen. Zweifelhaft sind auch sogenannte Service-Büro-Beschränkungen sowie vertragliche und technische Beschränkungen auf eine bestimmte Anzahl von Nutzern. Trotzdem muss natürlich für jeden Nutzer eine entsprechende Lizenz vorhanden sein.

Umgang mit Gebrauchtsoftware

Ebenfalls unter Juristen umstritten ist die Zulässigkeit des Handels mit gebrauchter Software. Der BGH entschied in einem richtungsweisenden Urteil aus dem Jahr 2000, dass der Weiterverkauf von datenträgerbasierter Software grundsätzlich nicht über Lizenzbedingungen von den Herstellern eingeschränkt werden kann. In seinem Urteil vom 11.02.2010 (veröffentlicht im Oktober 2010) hat es der BGH jedoch für zulässig gehalten, dass der Hersteller eines Computerspiels den Weitervertrieb durch bestimmte Vertragsklauseln unmöglich macht, was im Ergebnis einem Verbot des Weiterverkaufs entspricht.

Im Kern geht es bei der Entscheidung darum, ob der Weitervertrieb von Software überhaupt untersagt werden darf. Dagegen spricht der so genannte "Erschöpfungsgrundsatz", der einem Softwarehersteller verbietet, die weitere Verbreitung eines einmal willentlich in den Verkehr gebrachten Softwareproduktes zu reglementieren. Der "Erschöpfungsgrundsatz" dient dem allgemeinen Interesse an einem freien Warenverkehr und gilt nur für verkörperte Werke, also beispielsweise wenn eine Software auf einem Datenträger in den Handel kommt, nicht aber bei unkörperlichen Werken, also zum Beispiel beim bloßen Online-Vertrieb per Download. Angesichts der aktuell unklaren Rechtslage empfiehlt es sich hier, Gebrauchtsoftware im Rahmen der Lizenzverwaltung gesondert auszuweisen.

Sonderfall Open Source-Software

In der Praxis finden sich verschiedene Open Source-Software (OSS)-Lizenzen, die sich durch die dem Nutzer der Software auferlegten Pflichten unterscheiden. Zu den gängigen OSS-Lizenzen gehören unter anderem folgende Lizenzformen:

- Die General Public License (GPL) verlangt, dass Software, welche GPL-Bestandteile verwendet, wiederum nur unter der GPL (also nicht proprietär) vertrieben werden darf ("Copyleft").
- Charakteristisch für die BSD-Lizenz (Apache Software License) ist hingegen ihr geringer Pflichtenumfang. Mangels Copyleft ist es zulässig, Modifikationen und Weiterentwicklungen auch als proprietäre Software zu vertreiben.
- Eine abgeschwächte Form des Copyleft beinhaltet die Lesser General Public License (LGPL), die insbesondere für die Lizenzierung von Programmbibliotheken gedacht ist.

Trotz des großen wirtschaftlichen Vorteils, den freie Software Unternehmen bietet, hält ihr Einsatz in der Praxis zahlreiche juristische Fußangeln und Risiken bereit. So hat zwar das Landgericht München I in einem Urteil vom 19. Mai 2004 entschieden, dass OSS wie jede andere Soft-

ware urheberrechtlichen Schutz genießt – und die General Public License rechtlich wirksam ist.

Doch sind die mit der freien Software aufgeworfenen Rechtsfragen noch nicht abschließend geklärt, woraus sich eine erhebliche Rechtsunsicherheit ergibt. So ist zum Beispiel, wenn nur Bestandteile von OSS in eine andere Software übernommen oder mit dieser verbunden werden, nicht sicher abgrenzbar, ob die neu entstandene Software proprietär verwertbar ist oder das Copyleft gilt. Das programmierende und investierende Unternehmen weiß also unter Umständen nicht, woran es ist, zumal auch Verstöße gegen OSS-Lizenzen zunehmend stärker verfolgt werden.

Insgesamt ist festzustellen, dass sich freie Software keineswegs im rechtsfreien Raum bewegt, sondern genauso wie proprietäre Software an Lizenzbedingungen gebunden ist. In der Praxis werden dabei häufig durch Missverständnisse bedingte Rechtsverstöße begangen, weil unter freier Software irrtümlich "frei von Lizenzpflichten" verstanden wird.

Lizenzkontrolle und Beweisproblematik

Häufig lassen sich die großen Softwarehersteller in ihren Lizenzbedingungen Auditrechte gegenüber ihren Kunden einräumen. Diese Auditrechte berechtigen die Hersteller, beim Kunden die Einhaltung ihrer Lizenzbestimmungen zu überprüfen. Dabei bedienen sich die Softwarehersteller häufig der großen Wirtschaftsprüfungsgesellschaften, um vor Ort beim Lizenznehmer die Lizenzunterlagen sowie dessen Hardware und Software zu kontrollieren.

Audits durch Softwarehersteller

Nach dem Besichtigungsanspruch gemäß § 809 BGB kann der Rechteinhaber, der gegen den Besitzer einer Sache einen Anspruch in Ansehung der Sache hat oder sich Gewissheit verschaffen will, ob ihm ein solcher Anspruch zusteht, verlangen, dass ihm der Besitzer die Sache zur Besichtigung vorlegt oder die Besichtigung gestattet, wenn die Besichtigung der Sache für den Rechteinhaber von Interesse ist.

So lässt sich zusammenfassend feststellen, dass sowohl vertragliche wie auch gesetzliche Pflichtenstrukturen bestehen, welche Softwareherstellern die Möglichkeit für Lizenzaudits eröffnen.

Mitwirkungspflichten

Ob die Kunden beziehungsweise Lizenznehmer jedoch verpflichtet sind, das vertraglich bestehende Auditrecht zu dulden, oder die entsprechenden Lizenzklauseln AGB-rechtlich unzulässig sind, ist im Einzelnen stark umstritten. Denn die Auditrechte könnten als überraschende Klauseln unzulässig sein, weil nach dem Urheberrecht verdachtsunabhängige Überprüfungen nicht vorgesehen sind. Eingewandt wird auch, dass durch die Kontrollvorgänge beim Lizenznehmer die Rechte Dritter gefährdet oder verletzt werden.Doch werden letztlich solche rechtlich unsicheren Einwände dem Lizenznehmer in der Praxis nur wenig weiterhelfen, da er im Falle einer Weigerung mit Rechtsstreitigkeiten oder der Beendigung der Geschäftsbeziehung rechnen muss. Faktisch ist der Lizenznehmer daher gerade gegenüber den großen Softwareherstellern an die Lizenzbedingungen gebunden und tut gut daran, sich frühzeitig auf Lizenzaudits einzurichten.

Lizenznachweis und Beweislast

Ein Lizenznachweis ist eine dokumentierte Nutzungsberechtigung, die vom Hersteller oder Händler unmittelbar oder indirekt erteilt wird. Für die Frage, was bei einer Lizenzprüfung als gültiger Nachweis anerkannt wird, haben sich bislang soweit ersichtlich keine allgemein gültigen Standards herausgebildet. Trotzdem kann sich der Lizenznehmer bei Beachtung der nachfolgenden Maßgaben rechtlich sicher aufstellen.

Häufig werden in den Unternehmen wertvolle Belege wie Quittungen, Rechnungen, Überweisungsträger et cetera weggeworfen, die als Lizenznachweise dienen (können). Doch im Zweifel muss der Lizenznehmer beweisen, dass er für seinen Softwarebestand über gültige Lizenzen verfügt. Ebenfalls kommen als Lizenznachweise beispielsweise in Betracht:

- Original-Datenträger (CD-ROM, DVD et cetera) und Lizenzdokumente aller Art, zum Beispiel der "Endbenutzer-Lizenzvertrag" (EULA)
- Siegel, etwa als Aufkleber des Softwareherstellers, sowie Echtheitszertifikate und Lizenzverträge
- Handbücher, Dokumentationen, Anleitungen et cetera
- Schriftverkehr (auch per E-Mail) bei der Vertragsanbahnung

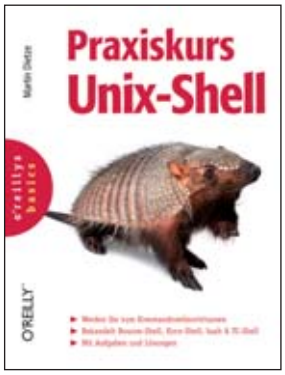
Bei der geordneten Verwahrung der notwendigen Lizenznachweise ist es hilfreich, wenn sich diese in digitaler Form direkt im Lizenzmanagement den dort erfassten Lizenzpaketen zuordnen lassen. Per Mausklick kann dann ein Administrator, Einkäufer, Auditor oder CIO sofort sehen, auf welcher Vertragsgrundlage das entsprechende Lizenzpaket beruht. Für den Nachweis, dass Software rechtmäßig erworben wurde, ist also neben den Belegen auch eine jederzeit verfügbare Übersicht über den aktuellen Softwarebestand durch eine Inventarisierung sowie die Darstellung einer Lizenzbilanz im Rahmen einer Lizenzverwaltung erforderlich.

Das Einscannen von Belegen im Rahmen von Dokumentenmanagementlösungen (DMS) führt bei Schriftstücken formalrechtlich zu einer Minderung der Beweisqualität, da der Vollbeweis durch den Medienwechsel beim Scannen verloren geht. Dies wird in der Praxis aber unschädlich sein, da gescannte Belege akzeptiert werden, sofern der Scanprozess in einem geordneten Verfahren organisiert wird. Hierzu gehört nach den Maßgaben der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme: Eine genaue Organisationsanweisung und Dokumentation, wer was wann einscannt, sowie unveränderliche Formate, zum Beispiel Bildformate oder PDF/ A, sowie die Speicherung auf WORM-Medien (Write Once Read Multiple) wie CD-R und DVD+-R. Darüber hinaus sind eine ausreichende Fehlerkontrolle mit Dokumentation, Datensicherheits- und Berechtigungskonzepte sowie eine Verfahrensdokumentation notwendig. *(jp)*

[1] Lizenzmanagement-Leitfaden von Aagon
B8W31

Link-Codes

Praxiskurs Unix-Shell



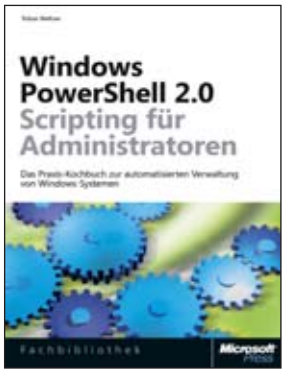
Die Shell als Benutzerschnittstelle ist nach wie vor das Administrationswerkzeug schlechthin für Unix-Systeme. Im Zeitalter der grafischen Benutzeroberflächen wirkt die Arbeitsweise mit der Shell für jüngere Semester allerdings wie ein Kulturschock, dem der Inhalt dieses Buches entgegenwirken möchte. Hierfür erläutert der Autor in den Einstiegskapiteln die Grundlagen zu den Shell-Familien sowie die notwendigen ersten Schritte. Erfreulich ist, dass der Titel nicht zuviel verspricht und die Praxis im Vordergrund steht. Die vermittelten Kenntnisse lassen sich so auf allen modernen Unix-Systemen wie AIX, Solaris, Linux oder BSD einsetzen. An den relevanten Stellen geht der Autor auch auf die jeweiligen Unterschiede ein. Aufgebaut ist das Buch dabei chronologisch, und zwar in der Reihenfolge, wie die Arbeit am System vonstatten geht. Aus diesem Grund lernen die Leser zunächst neben den Dateitypen, Standarddateien und Dateisysteme die Zugriffsrechte, Benutzer- und Gruppenverwaltung sowie Dateioperationen kennen. Die Erweiterungs- und Kombinationsmöglichkeiten von Befehlen stellt die erste Stufe zur Souveränität über das System dar: Ein- und Ausgabeumlenkung, die Arbeit mit Variablen und Aliasen sowie das richtige Einsetzen von Werkzeugen und Prozessen lassen Leser die Möglichkeit der Unix-Shell erkennen.

Einem kurzen Abriss zur Anpassung der Arbeitsumgebung folgt die Beschreibung des Anwendungspotenzials zur Verarbeitung von Daten. Filter und reguläre Ausdrücke sind im Fokus dieses Kapitels, das etwas knapp gehalten ist und durchaus noch weitere Beispiele verkraftet hätte. Der Abschnitt "Arbeiten im Netzwerk" wird leider nur auf zehn Seiten abgehandelt, so dass leider nur auf ganz wenige Aspekte (Telnet, SSH, FTP, SCP, SFTP) bei der Netzwerkadministration via Shell eingegangen wird. Erfreulich die Einführung in das Scripting, die sich an Anfänger richtet, die noch keine Programmiersprache beherrschen. Der Autor erläutert geschickt die Verarbeitung von Kommandofolgen, Verzweigungen sowie den Einsatz von Schleifen.

Fazit: Mit "klein, aber oho" lässt sich das knapp 300 Seiten umfassende Büchlein am besten beschreiben. Der Autor, der bereits als Dozent tätig war, wirft seine Erfahrung in die Waagschale und vermittelt sowohl das Wesentliche im Umgang mit der Shell wie auch die dahinterliegenden Konzepte. Übungen vertiefen den gedruckten Inhalt. *Frank Große*

Autor	Martin Dietze
Verlag	O'Reilly
Preis	19,90 Euro
ISBN	978-3-89721-565-8
Bewertung (max. 10 Punkte)	***9***

Windows PowerShell 2.0



Der Autor Tobias Weltner, MVP für PowerShell, zählt zu den bekannten deutschen Skripting-Gurus, der seine Erfahrungen und sein Know-how in zahlreichen Büchern und Roadshows präsentiert hat. Das vorliegende Buch beinhaltet einen gut gefüllten Bauchladen an sofort einsetzbaren PowerShell-Beispielen, um Windows-Systeme automatisiert zu verwalten. Das Werk ist dabei ohne eine Einführung in die Programmiersprache aufgebaut, so dass grundlegende Kenntnisse der Nutzung der PowerShell vorausgesetzt werden. Ziel ist es, die 250 Befehle (Cmdlets) der PowerShell und ihre Effektivität vorzustellen. Da der PowerShell über zusätzliche Module keine Grenzen gesetzt sind, gibt es Erweiterungen für Exchange Server, SQL Server, Active Directory, Gruppenrichtlinien oder auch 3rd-Party-Produkte. Einsatzmöglichkeiten hierzu werden neben den Basic-Cmdlets in insgesamt neunzehn Kapiteln auf 560 Seiten vorgestellt.

Gleich die ersten Kapitel lohnen sich, da diese die Grundlagen für komplexe Skripte liefern: Textauswertungen sowie Datum und Zeit. Hier finden sich Codeschnipsel zum Einlesen, zur Umwandlung, zum Auswerten von Texten, aber auch zur Verarbeitung diverser Datumsformate inklusive deren Gültigkeitsprüfung. Mit Listen und Arrays sowie dem effektiven Einsatz der Pipeline, ergänzt durch Bedingungen und Schleifen und die Elemente der Fehlerbehandlung erfährt der Leser alles Notwendige, um selbst ein Skriptguru zu werden. Ambitionierte Steilvorlagen hierzu liefern die nachfolgenden Themenschwerpunkte: Dateisystem (Manipulation an Dateien, Ordnern, Attributen und Berechtigungen), Registrierdatenbank (Bearbeitung und Analyse der Registry), Prozesse und Anwendungen, Dienste, Ereignisprotokoll, Zugriffsberechtigungen, Benutzerverwaltung und Active Directory (Benutzerkonten- und Gruppenbearbeitung), die einen Großteil der täglichen Arbeit als Windows-Administrator betreffen. Das Finale bieten die Kapitel Snap-Ins und Module, Remoting und Hintergrundjobs, die den Skript-Experten ansprechen.

Fazit: Dem Autor ist eine umfangreiche Lösungssammlung für unzählige häufig auftretende Probleme bei der Arbeit mit der PowerShell gelungen. Grundkenntnisse der PowerShell-Skriptsprache werden jedoch vorausgesetzt. Erfreulich ist, dass sich das Buch bei der Handhabung und inhaltlich problembezogen durchforsten und nutzen lässt. *Frank Große*

Autoren	Tobias Weltner
Verlag	Microsoft Press
Preis	49,90 Euro
ISBN	978-3-86645-680-8
Bewertung (max. 10 Punkte)	***10***

http://vmware-forum.de

Inoffizielles VMware-Wissen

VMware ist – allen Angriffen von Microsoft und Co. zum Trotz – noch immer der unbestrittene Marktführer in Sachen Virtualisierung. Dementsprechend häufig sind VMware-Produkte in Unternehmen zu finden. Doch auch die Produkte des Marktführers sind nicht immer frei von Fehlern oder sofort verständlich in ihrer Administration. Zum einen bietet sich in diesem Fall die Unterstützung des Herstellers an. Doch reicht diese nicht aus oder möchten Sie als Admin nur mal kurz etwas nachlesen, kann vmware-forum.de eine Alternative sein. In diesem "inoffiziellen, unabhängigen" VMware-Forum finden Besucher zahlreiche Threads mit Fragen zu den verschiedenen VMware-Produkten sowie Problemen mit diesen. Dabei sind alle namhaften Vertreter wie ESX, ThinApp, View oder Workstation mit von der Partie.

Die Tatsache, dass täglich oft mehrere neue Threads im Forum eröffnet werden und Antworten sich meist innerhalb desselben Tages finden, zeugt von der Userbeteiligung. Und auch die Fragen und Antworten selbst lassen an ihrer professionellen Ausrichtung keine Zweifel. So drehen sich im Unterforum zu ESX 4i die Themen beispielsweise um Port-Trunking, Logfiles, Backup oder Snapshots. Doch auch an die Weiterbildung im VMware-Umfeld ist gedacht. Im Unterforum "Zertifizierung" tauschen die User ihre Erfahrungen und Fragen zu den verschiedenen Weiterbildungsprogrammen von VMware aus. Auch hier gilt, dass sich rasch Antworten auf gestellte Fragen finden, und stets ein professioneller und freundlicher Ton gewahrt bleibt – nicht in allen Foren unbedingt selbstverständlich.

Auch wenn der Zusatz "inoffiziell" zunächst etwas anderes vermuten lässt, finden sich auf der Webseite absolut seriöse und hilfreiche Tipps. Nach geheimen Tricks, Cracks und Ähnlichem hingegen sucht man auf der Webseite vergebens. Die rund 16.000 Mitglieder sind vielmehr an einem seriösen und neutralen Austausch interessiert. Lediglich das Design der Webseite ist für ein Forum auf den ersten Blick etwas gewöhnungsbedürftig. So begrüßt die Besucher nicht etwa eine Gesamtübersicht der einzelnen Unterforen mit einer kurzen Beschreibung, der Anzahl der Threats et cetera. Vielmehr findet sich auf der Startseite eine Liste der Unterforen ohne weitere Erklärungen. Erst danach finden sich die User in einer Foren-typischen Übersicht wider. Auch verweisen einige der externen Links ins Leere. An Professionalität und Inhalt mangelt es im VMware-Forum dennoch nicht – und darauf kommt es letztlich an. *(dr)*

Im VMware-Forum findet ein reger Austausch rund um die Virtualisierungsprodukte statt

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

Sicherer Netzwerkzugang durch TPM-Chips

Die Authentifizierung der im Netzwerk betriebenen Endgeräte bietet einen wirksamen Schutz vor externen Angriffen. Gängige Verfahren sind die Identifikation über die MAC-Adresse oder der Einsatz von Zertifikaten. Diese Methoden versprechen einen guten Grundschutz, sind allerdings nicht völlig fälschungssicher. Lesen Sie in unserem Fachartikel im Web, wie Sie mit einem Trusted Platform Module für eine zuverlässige Authentifizierung im Netzwerk sorgen und was beim Management des TPM-Chips zu beachten ist.
www.it-administrator.de/themen/sicherheit/fachartikel/99019.html

Mit Tiered Storage in die Cloud

Die Nutzung von Storage in der Cloud verspricht viele Vorteile, birgt aber auch Risiken in sich. Denn ohne ein sinnvolles Konzept, das etwa Sicherheit, Performance und Provider-Wechsel adressiert, kann Cloud Storage schnell zum Desaster werden. In unserem Online-Artikel erläutern wir, wie sich der Speicher in den Wolken nahtlos in eine Tiered Storage-Architektur einbinden lässt und welche Rolle dabei Single Path Access über ein Dateisystem wie CIFS spielt.
www.it-administrator.de/themen/storage/fachartikel/99020.html

Anwenderbericht: Sichere Cloud für den Mittelstand

Ein vertrauenswürdiges Rechenzentrum in der Cloud setzt Maßnahmen wie eine Anbindung über verschlüsselte VPN-Leitungen sowie eine mandantenfähige Infrastruktur voraus – nur so lassen sich verschiedene Kunden auf einer gemeinsamen Hardware sicher gegeneinander abschotten. Erfahren Sie in unserem Anwenderbericht im Web, wie der Dienstleister extend-it dazu das Unified Computing System von Cisco einsetzt und so mit wenig Aufwand virtuelle Server inklusive Speicher und Netzwerkanbindung bereitstellt.
www.it-administrator.de/themen/server_client/fachartikel/99021.html

Hochverfügbare Systeme ausfallsicher überwachen

Hochverfügbarkeit ist ein Thema, das für Firmen aller Größen immer mehr an Bedeutung gewinnt. Nicht vergessen werden darf dabei, dass die Überwachung der HA-Systeme mittels einer Monitoring-Lösung unverzichtbar ist. In unserem Online-Fachartikel stellen wir Ihnen Strategien vor, wie Sie das Monitoring optimal mit Ihrer IT-Struktur kombinieren und dabei auch virtuelle Systeme im Auge behalten. Dabei gehen wir besonders auf das Netzwerk-Monitoring durch Failover-Clustering ein, das selbst im Fehlerfall eine nahezu nahtlose Überwachung garantiert.
www.it-administrator.de/themen/netzwerkmanagement/fachartikel/99022.html

Besser informiert: Fachartikel auf der Website des IT-Administrator

»Das menschliche Umfeld ist ein entscheidender Faktor«

Ronald Ebel (47) ist am Standort Hamburg der Tallence GmbH als Systemadministrator für die Belange der internen Entwickler sowie der Mitarbeiter aus der Verwaltung verantwortlich. Darüber hinaus unterstützt er auch den Support komplexer Kundeninstallationen. Das 1999 in Regensburg gegründete Unternehmen bietet seinen Kunden von der ersten Beratung bis zur finalen Implementierung von komplexen Business-Projekten alle notwendigen Dienstleistungen aus einer Hand.

Warum sind Sie IT-Administrator geworden?

Ich hatte die Wahl, mich zwischen Programmieren und Administration zu entscheiden. Also bin ich meiner Vorliebe mit Menschen zu arbeiten gefolgt.

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

Zu 40 Prozent besteht die Arbeit aus der Betreuung von Hardware und Netzwerk, 60 Prozent entfällt auf die Zusammenarbeit mit den Menschen. Diese 60 Prozent machen mir riesigen Spaß - die Technik zwar auch, aber das menschliche Umfeld ist der entscheidende Faktor.

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

Würde ich nicht. Es ist besser, erst etwas Anständiges zu lernen und herauszufinden, was man gerne mag – zum Beispiel Programmierer oder Systemkaufmann, so dass ein qualifizierender, technischer Abschluss in der Tasche steckt. Ist der Spaß an der Technik und den Menschen danach nicht verflogen, wird sich auch der Weg in die Systemadministration ergeben.

Was sind die nervigsten System-Management-Aufgaben?

Das Erfassen der Seriennummern von abgehender Hardware. Warum werden die immer so klein gedruckt?

Welche System-Management-Werkzeuge nutzen Sie?

Wir setzen vi, Putty, Winscp und Remote Desktop ein.

Wie dokumentieren Sie Ihre Netzwerkumgebung?

Dafür nutzen wir ein internes Wiki.

Wo sehen Sie Stärken und Schwächen typischer System-Management-Werkzeuge?

Die proprietären sind meist zu teuer oder nur für Konzerne ausgelegt. Die Open Source-Anwendungen haben sich netterweise zu einer sehr guten Alternative gemausert. Aber man muss auch dazu bereit sein, selber Hand anzulegen.

Welche Faktoren treiben das Thema System-Management bei Ihnen am meisten voran?

Der Bedarf meiner Anwender. Da sie weit vorne mit Ihrer Entwicklung stehen, brauchen sie aktuelle Hardware. Aber auch neueste Betriebssysteme und aktuelle Tools für die Entwicklung. Ich versuche Ihnen unkompliziert und schnell die Umgebung dafür zu schaffen.

Nehmen Sie Ihre Arbeit auch ins Wochenende mit?

Nein. Aber generell gilt folgende Regel, dass ich mich lieber einmal zu viel anrufen lasse, als dass ich hinterher alles in einer Nachtschicht neu installieren muss. Ich arbeite zumeist mit Entwicklern zusammen. Also mit Menschen, die mit etwas Übung und Lust auch meine Arbeit machen könnten. Dies gestaltet meinen Arbeitsalltag erheblich einfacher, als wenn ich nur Fachanwender zu betreuen hätte. Klar, wenn eine VMware-Instanz nur außerhalb der Arbeitszeit verschoben werden kann, dann mache dies eben morgens um 5 Uhr von zu Hause aus. Dafür erarbeiten meine Kollegen, damit der nächste Launch rechtzeitig beim Kunden stattfinden kann, ja auch mein Gehalt.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Singen ist ein hervorragender körperlicher Ausgleich. Wenn ich drei Wochen lang keine Probe habe, dann merke ich wie meine Haltung schlechter wird und der Nacken sich verspannt. Zweimal die Woche versuche ich mit dem Fahrrad zur Bahn zur fahren. Der wichtigste Ausgleich ist allerdings, zu zweit auf dem Sofa sitzend fernzusehen.

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

Ich würde gerne einmal sehen, was aus der guten alten AS/400 geworden ist. Die modularisierten Blade-Center iSeries Maschinen sind aber für den Hobbykeller leider zu teuer.

Wie und als was möchten Sie in zehn Jahren arbeiten?

Wie in den letzten Jahren mit klugen und netten Menschen den Tag verbringen und zusammenarbeiten. Natürlich auch die Maschinen streicheln, Server installieren und einreißen und was mir sonst noch Spaß bringt. Also als Administrator mein Umfeld hegen und pflegen.

Das Interview führte Petra Adamik.

Geburtstag: 7.11.1963
Admin seit: 20 Jahren
Hobbys: Chorsingen und Chinesisch

Ronald Ebel, IT-Administrator

Ausbildung und Tätigkeit

- Nach Abbruch eines Philosophiestudiums Umschulung zum "Organisationsprogrammierer mittlere Datentechnik, Schwerpunkt IBM /36 und AS/400"
- lokaler Systemadministrator für die Entwickler und die Verwaltung
- Supportmanager für Kundeninstallationen

Betreute Umgebung

- Mit VMware virtualisierte Entwicklungsumgebungen, zumeist Linux Derivate mit den entsprechenden ESXi Hosts
- Kleines AD für die lokalen Windows 2008 Server
- Grundinstallation der Entwickler-Laptops
- Verschiedene Backupsysteme wie Bacula und BackupPC
- Im Netzwerkbereich Router, VPN, IP, DHCP und DNS
- Externen Dienstleister für den Mailverkehr

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

Was haben Sie zu sagen?

Die Ausgabe 9/11 erscheint am 5. September 2011

Schwerpunktthema:

E-Mailmanagement und Collaboration

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

Die Ausgabe im **Oktober** hat sich zum Schwerpunkt das Thema **Netzwerksicherheit** gesetzt. In unseren Tests nehmen wir unter anderem Norman Network Protection unter die Lupe. In den Workshops lesen Sie, wie Sie Forefront TMG als Secure Web Access Gateway betreiben.

Als Schwerpunkt im **November** folgt dann das Thema **Storage**.

***Im Test:* Bitrix Intranet 10.0**

***Im Test:* Zimbra Collaboration Suite 7**

***Workshop:* Lync Server 2010 im Netzwerk integrieren**

***Systeme:* VoIP und NAT in Einklang bringen**

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, Klaus Bierschenk, Christian Gröbner, Frank Große, Jürgen Heyer,Stephan Hucke, Thomas Joos, Thorsten Scherf, Horst Speichert, Rolf Masuch, Oliver Wagner, Matthias Wessner

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

Es gilt die Anzeigenpreisliste Nr. 8 vom 01.01.2011
Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik, Gero Wortmann
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99

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

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

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

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

Erscheinungsweise
monatlich

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

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

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

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

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

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

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

INSERENTENVERZEICHNIS

Die Ausgabe enthält eine Gesamtbeilage 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

Netezza. Läuft schon nach 24 Stunden.

IBM Netezza Data Warehouse läuft innerhalb von 24 Stunden und rechnet sich ebenso schnell. Denn IBM Netezza Data Warehouse ist so leistungsstark, dass es anspruchsvolle Analysen in kürzester Zeit erstellt. So können Sie Ihr Unternehmen nicht nur schneller machen, sondern auch Ihre Ergebnisse beschleunigen.

ibm.com/netezza/de

Erleben Sie Leistung live
IBM Break Free Tour 2011

20.09. | Commerzbank Arena FFM
21.09. | Allianz Arena München
27.09. | Imtech Arena Hamburg

Jetzt anmelden:
ibm.com/de/breakfree