IT-ADMINISTRATOR.DE

10/2012

€ 12,60 ISSN 1614-2888

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

Server-Sicherheit

4 196583 212605 10

Microsoft

WINDOWS SERVER 2012 HÄLT IHRE ANWENDUNGEN AM LAUFEN.

Optimieren Sie die Verfügbarkeit in Ihrem Rechenzentrum. Mit dem einzigartigen Server, der auf jahrelanger Cloud-Erfahrung basiert. Richten Sie Failover-Systeme innerhalb Ihres Rechenzentrums oder an entfernten Standorten ein. So sind Ihre Anwendungen jederzeit und überall verfügbar – wann immer Sie diese brauchen.

Windows Server 2012

INSPIRIERT VON DER CLOUD.

microsoft.com/ws2012

EDITORIAL

Vertrauen tut gut

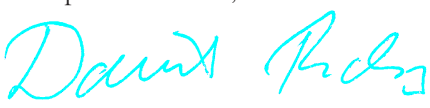
Liebe Leser,

kennen Sie das ungute Gefühl, etwas nicht unter Kontrolle zu haben? Stellen Sie sich vor, einer Ihrer Bekannten fährt Sie – aus welchem Grund auch immer – in Ihrem Wagen irgendwo hin. Kritisch beäugen Sie jeden Handgriff, jedes Verhalten im Verkehr: Warum bleibt er solange auf der linken Spur? Da war doch genug Platz. Muss er jetzt Strich 50 fahren? Und so weiter. Wirklich entspannen können Sie erst, wenn das Ziel erreicht ist und der Motor verstummt. Doch das Vertrauen war wieder einmal gerechtfertigt. Scheinbar können wir uns in unserer Zeit gar nicht genug absichern. Etwas nicht unter Kontrolle zu haben, wurmt uns. Und so versuchen wir, alle Eventualitäten zu bedenken und verlieren dabei nicht selten den Blick fürs Wesentliche.

Auch im Unternehmen spielt Vertrauen eine große Rolle. Stundenlang überprüfen Sie als Administrator an Ihren Servern die Sicherheitseinstellungen, überarbeiten Benutzer-Richtlinien, aktualisieren URL-Filter und wälzen Security-Logs. Dass Ihre Anwender währenddessen mit den vertraulichen Firmendaten auf ihren Galaxys und Co. in Richtung Unternehmensparkplatz spazieren, entgeht Ihnen möglicherweise. Eine Lücke, die Sie nicht wirklich unter Kontrolle haben. Und was ist mit Bars, in Zügen oder am Telefon, wo schnell geheime Details unachtsam ausgeplaudert sind?

Heißt das nun, dass Ihnen IT-Sicherheit egal sein sollte? Mitnichten! Es gibt genug Bösewichte, die es auf Ihre Infrastruktur abgesehen haben. Ihr Fahrzeug bringen Sie schließlich auch zum TÜV, auch wenn Sie Bekannte ans Steuer lassen. Vergessen Sie nur nicht, die Dinge manchmal mit etwas Abstand zu betrachten, allen voran den Mitarbeitern zu vertrauen. Das gilt natürlich auch für die Unternehmensleitung, denn motivierte und sensibilisierte Anwender sind die beste Sicherheitsmaßnahme. Sie identifizieren sich mit dem Unternehmen und achten allein deshalb auf "ihre" Daten. Vermitteln Sie ihnen zudem das nötige IT-Grundwissen, ist viel gewonnen. Damit Sie sicher ans Ziel kommen und mehr Zeit fürs Wesentliche haben, stellen wir Ihnen in der aktuellen Ausgabe unter anderem die praktischen Security-Helfer "Microsoft Security Compliance Manager" und "Best Practice Analyser für Windows Server 2012" vor.

Viel Spaß beim Lesen, Ihr



Stellv. Chefredakteur

PS: IT-Administrator ist jetzt auch auf dem iPad verfügbar! Neben dem komfortablen Lesemodus können Sie Ihre Ausgaben auf dem Gerät speichern und per Volltextsuche durchforsten. All-Inclusive- und ePaper-Abonnenten erhalten kostenlos Zugang.

Server-Sicherheit

Im Test: OCS Inventory NG

Netzwerke wachsen mit ihren Anforderungen. Zusätzliche Arbeitsplätze erweitern die Struktur, und durch den Austausch von defekten oder veralteten Computern fällt es immer schwerer, sämtliche installierte Hard- und Software im Auge zu behalten. Vom Administrator wird aber erwartet, dass er den Zustand installierter Geräte kennt. Statt der berüchtigten Excel-Tabelle sollen Inventarisierungs-Lösungen dabei helfen, den Überblick zu bewahren. Ob das auch mit dem unter Open Source-Lizenz veröffentlichten und somit kostenlosen Tool OCS Inventory NG gelingt, hat IT-Administrator in einem Praxistest herausgefunden.

Seite 24

Einkaufsführer: Hochverfügbarkeitslösungen

Hochverfügbarkeit ist heute in der IT, anders als noch vor wenigen Jahren, eine gängige Anforderung. Seit in allen Unternehmen und Organisationen die wesentlichen Geschäftsprozesse nur noch über die IT laufen, dürfen deren Systeme eben nicht mehr ausfallen, das gilt im Büro nicht anders als in der Fabrikhalle. Zur Realisierung von Hochverfügbarkeit für Server-Systeme stehen unterschiedliche Konzepte und Technologien zur Verfügung. Sie haben alle ihre Vor- und Nachteile – was für ein Unternehmen passt, hängt primär von den Risiken der Geschäftsprozesse ab. Welche Vorzüge und welches Manko die jeweiligen Ansätze zu bieten haben, zeigt dieser Artikel.

Seite 32

AKTUELL

PRODUKTE

PRAXIS

WISSEN

RUBRIKEN

Neuerungen in Microsoft System Center 2012 (1)

Die neue Version 2012 von Microsoft System Center konzentriert sich vor allem auf die Verwaltung von Private Clouds. Dabei hat Microsoft die PowerShell-Integration deutlich verbessert. Das soll das Scripten erleichtern und eine Automatisierung von Verwaltungsaufgaben ermöglichen. Auch die Lizenzierung hat Microsoft vereinfacht und Editionen zusammengefasst. Lesen Sie in unserer dreiteiligen Workshopserie, was das neue System Center 2012 zu bieten hat. Zunächst geben wir Ihnen einen Überblick und zeigen, wie Sie die Microsoft-Suite optimal austesten.

Seite 60

Best Practices Windows Server 2012

Über die Jahre hinweg hat Microsoft den Windows Server immer unternehmenstauglicher gemacht. Aber gerade wenn eine Installation zunächst besonders einfach erscheint, stellt sich die Frage, ob die zahlreichen Komponenten denn korrekt konfiguriert sind. Beim neuen Server 2012 bringt das Produkt selbst bereits viele Erfahrungen mit. Wir zeigen in diesem Workshop, wie Sie sich die Eigenintelligenz des Betriebssystems zu Nutze machen und die Software optimal für den produktiven Betrieb einrichten.

Seite 66

Themenübersicht

Du kommst hier net rein!

macmon secure gibt mit Release 4.0 den Startschuss für die aktuellste Version seiner **NAC-Software macmon**. Zu den wesentlichen Veränderungen gehört das **Footprinting. Dabei erkennt das Security-System die geöffneten TCP- und UDP-Ports eines Geräts** und listet diese in der Benutzeroberfläche auf einer Detailseite auf. Darüber hinaus lässt sich das Werkzeug so konfigurieren, dass es versucht, die an offene Ports gebundenen Dienste zu erkennen. Zudem kann der Nutzer generell Vorgaben machen, welche Ports geöffnet oder geschlossen sein müssen. Erkennt das Tool hier Abweichungen, stößt es die erforderlichen Sicherungsaktionen an. Weiterhin lässt sich in der neuen Softwareversion das Access-VLAN auch manuell direkt über die Benutzeroberfläche konfigurieren. Die NAC-Lösung erkennt dabei laut Hersteller, in welchem VLAN eine MAC-Adresse gesehen wurde und wie das VLAN am Interface gebunden ist. Dies soll es beispielsweise ermöglichen, **Fremdgeräte im Voice-VLAN gezielt auszusperren**. Darüber hinaus wurden verschiedene Funktionserweiterungen für den Guest Service vorgenommen, über den Firmenbesucher und externe Mitarbeiter einen kontrollierten und zeitlich begrenzten Zugang in das Unternehmensnetzwerk erhalten. Eine weitere technische Fortentwicklung betrifft das Authentifizierungsverfahren auf Basis des Standards 802.1X. Indem macmon die Option bietet, Geräte oder Benutzer anhand eines Zertifikates zu authentifizieren, soll das Tool komfortablere Bedingungen und gleichzeitig eine signifikant höhere Sicherheit schaffen. Besitzt ein Client ein gültiges Zertifikat, kann er sich im Netzwerk anmelden und erhält nach erfolgreicher Überprüfung Zugriff. Zertifikate, die auf einer angegebenen Certificate Revocation List stehen, werden hingegen abgelehnt. Was die Preise angeht, hat der Hersteller neue Pakete für KMUs geschnürt. So kostet etwa das Network Bundle mit Guest Service und virtueller Appliance für 50 MAC-Adressen 4.450 Euro. *(ln)*

macmon secure: www.mikadosoft.de

Redundante Kommunikation

LifeSize fügt seinem **Bridge-Portfolio für Videokonferenzen** zwei Erweiterungen hinzu: **LifeSize UVC Multipoint** ermöglicht virtualisierte Videokonferenzen mit mehreren Teilnehmern und ist jetzt laut Anbieter für die **Bildauflösung mobiler Endgeräte** optimiert. Die neue Funktion für **LifeSize Bridge** sorge dank eines **Hochverfügbarkeits-Clusters** zudem für mehr Stabilität bei Videokonferenzen mit vielen Teilnehmern. Der integrierte Hochverfügbarkeits-Cluster verbindet zwei oder mehr Bridges so miteinander, dass sie als eine Einheit agieren. Durch diese Kopplung mehrerer Bridges sei auch **bei Ausfall eines Gerätes eine gute Bildqualität sichergestellt**. Selbst bei Systemfehlern blieben Videokonferenzen über die Bridge erhalten. LifeSize Bridge ist mit acht beziehungsweise zwölf Ports erhältlich. Durch die Upgrade-Option lassen sich die Einstiegskapazitäten zu einem späteren Zeitpunkt an individuelle Bedürfnisse anpassen. Es ist keine zusätzliche Hardware nötig, ein Lizenzschlüssel reicht laut Hersteller zur Aktivierung. Ports können für 1.399 Euro pro Port einzeln gekauft und bei Bedarf nachgerüstet werden. Life Size Bridge ist ab sofort ab 32.759 Euro bestellbar, LifeSize UVC Multipoint ab sofort ab 1.399 Euro erhältlich. *(dr)*

LifeSize: www.lifesize.com

Speicherkünstler

Nach den Zwei- und Vier-Platten-Netzwerkspeichern bringt **Buffalo Technology Sechs- und Acht-Bay-Varianten der TeraStation 5000er-Reihe** auf den Markt. Die neuen Modelle arbeiten mit einem Intel Atom Dual-Core-Prozessor D2700 und 64 Bit-Architektur sowie 2 GByte DDR3 RAM und einer Datentransferrate von bis zu 140 MByte/s. Die neue Serie kann dabei als **NAS**, **iSCSI-Ziel** oder wahlweise auch **gleichzeitig als NAS und iSCSI-Ziel** eingesetzt werden. Dabei bieten die Geräte Funktionen wie ein automatisches Failover sowie die Möglichkeit, Amazon S3 zu integrieren und Festplatten als Wechselmedien oder als austauschbare Backupmedien zu formatieren. Für Datensicherheit soll die RAID-Funktionalität sorgen. Der Anschluss weiterer Geräte an die 5000er-Serie ist über die integrierten USB 3.0-Anschlüsse möglich. Damit auch unterwegs der reibungslose Zugriff auf die Geräte gelingt, bieten die TeraStations einen integrierten **FTP-Server und Web-Access** sowie Apps für Android, iOS und Windows Phone 7. Zugriffsbeschränkungen lassen sich entweder über die **integrierte Benutzerverwaltung** oder das Active Directory erstellen. Defekte Datenträger kann der Nutzer dank Hot-Swap-Funktionalität im laufenden Betrieb wechseln. Über die Management Software Buffalo Surveillance Server Client Bundle ist zudem die Einbindung von Sicherheits- oder IP-Kameras möglich, die das RTSP-Protokoll nutzen und ONVIF-konform sind. Die Software bietet eine Kamera- und Speicherplatzverwaltung sowie eine speicherübergreifende Suche und unterstützt laut Buffalo über 1.400 Kameramodelle von mehr als 180 Kameraherstellern. Schließlich liegen den TeraStations jeweils zehn Lizenzen von NovaBACKUP Business Essentials bei. Die Modelle TeraStation 5600 und 5800 sind ab sofort zu einem Einstiegspreis von 1.390 Euro sowie 1.740 Euro erhältlich. *(dr)*

Die TeraStation 5600 von Buffalo Technology eignet sich unter anderem zur Videoüberwachung

Buffalo Technology: www.buffalo-technology.com/de/

Vielfältig angebunden

ZTE bringt mit dem **USB-Stick MF820S2** und dem **Mobile Hotspot uFi MF91S** die nach eigenen Angaben weltweit ersten **Multi-Mode-Geräte** auf den Markt. Sie unterstützen je nach Bedarf die **Mobilfunkstandards FDD-LTE, TDD-LTE, TD-SCDMA** oder **EDGE**. Für TDD-LTE unterstützt das USB-Modem Download-Geschwindigkeiten von bis zu 68 MBit/s. Es ist zudem mit einem USB-Rotator mit einer Rotation von 270 Grad und einer internen Antenne ausgestattet. Die Datenkarte könne somit in der Mehrzahl der Netzsysteme weltweit genutzt werden und biete mobilen Mitarbeitern durch lokale Anpassungen in Netzwerken an verschiedenen Standorten Flexibilität. Der neue mobile Hotspot uFi MF91S unterstützt ebenfalls die Mobilfunkstandards FDD-LTE, TDD-LTE, TD-SCDMA und EDGE. Bei einem Gewicht von 105 Gramm und ausgestattet mit einem Lithium-Ionen-Akku mit 2.300mAh eigne sich das kleine Taschen-WiFi unterwegs für Nutzer von PC-Laptops, Macbooks oder mobilen Multifunktionsgeräten. Das LTE-Modem MF821D schließlich arbeitet mit den LTE-Spektren 800, 1.800 und 2.600 MHz. Es ermöglicht Kapazitätserweiterung

Der Hotspot uFi MF91S von ZTE dient als WLAN-Modem und arbeitet in LTE-Netzen

über Mikro-SD-Karten von bis zu 32 GByte, ist kompatibel zu Windows 7, XP, Vista und Mac OS X und enthält zwei Schächte für externe Antennen. Das Gerät steht bereits unter dem Namen "o2 Surfstick ZTE LTE 4G MF821D" bei o2 in Deutschland zur Verfügung. Zu Redaktionsschluss lagen noch keine Preise seitens des Herstellers vor. *(dr)*

ZTE: www.zte.com

Intrusion Prevention mit IBM

IBM lüftet den Vorhang für eine eigene **Intrusion Protection Appliance**. Die **Security Network Protection XGS 5000** wurde laut Hersteller speziell dafür konzipiert, gegen sich ständig weiterentwickelnde Bedrohungen von außerhalb – aber auch innerhalb des Unternehmensnetzwerks – anzugehen. Das neue Gerät gewährt **Einblick in alle Anwendungen, die über das Netzwerk genutzt werden und zeichnet die Bewegungen der Nutzer im Web auf**, inklusive der Möglichkeit zur Überwachung und Steuerung dieser Aktivitäten. Das System baut auf den Core Security Features im IBM Security Network Intrusion Prevention System auf und beinhaltet durch neue Sichtbarkeits- und Kontrollebenen über Netzwerk, Anwendungen, Daten und Nutzer Schutz gegen Zero Day Exploits, für die Verhütung von Missbrauch und die Identifizierung bisher nicht erkennbarer Bedrohungen. Diese Sichtbarkeit soll durch die Integration der IBM Advanced Threat Protection Plattform weiter erhöht werden. Diese Plattform nutzt die Erkennung von Anomalien und Event-Korrelationsfähigkeiten, um besser auf komplexere Angriffe wie Advanced Persistent Threats reagieren zu können. Als Datenbasis dazu dienen sowohl eine URL-Filterdatenbank als auch die Web Application Control-Datenbank. Über 16 GBit-Anschlüsse lassen sich bis zu acht verschiedene Netzwerke schützen. Weiterhin ist die Appliance IPv6-fähig – der Administrator kann das Gerät über IPv6 managen und sich Ereignisse und Angriffsziele und -quellen im IPv6-Format anzeigen lassen. Der Listenpreis für die Hardware beträgt rund 48.500 Euro, für ein Jahr Maintenance werden zusätzlich etwa 12.000 Euro fällig. *(ln)*

IBM: www.ibm.com/de/

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

AppSense erweitert seine **User-Virtualization-Plattform** um **DataNow Essentials** – eine virtuelle Appliance, die mobilen Anwendern über unterschiedliche Endgeräte wie Computer, Tablets oder Smartphones den Zugriff auf ihre Unternehmensdaten ermöglichen soll. Dies verhindere unter anderem, dass Nutzer ihre Daten für den mobilen Zugriff in einen privaten Cloud-Speicher kopieren. Ein Remote-Wipe entferne bei Verlust des Endgerätes zudem alle kritischen Dateien. Die Essentials-Version steht AppSense-Kunden kostenfrei zur Verfügung. In der darauf aufbauenden und bald erhältlichen Enterprise-Variante will AppSense zudem erweiterte Sicherheitsfunktionen integrieren. *(dr)*

www.appsense.com

SnapServer DX2, der Unified Storage-Server für NAS und iSCSI-SAN von **Overland Storage,** unterstützt nun auch SSDs. Mit dieser Option ist es ab sofort möglich, SSD-, SAS- und SATA-Festplatten in einem einzelnen Gehäuse gemischt einzusetzen. Besonders in Umgebungen mit einer hohen I/O-Rate soll diese Mischbestückung zu höheren Leistungszahlen verhelfen. SnapServer DX2-Speichersysteme lassen sich bis auf 288 TByte erweitern und bieten Features wie Snapshots, Replikation und Remoteverwaltung. Mit vier SSDs à 120 GByte ausgestattet kostet der Storage-Server rund 5.475 Euro. *(ln)*

www.overlandstorage.com

Fluke Networks bringt mit **AirMapper** eine Android-App auf den Markt, die auf einem Smartphone oder Tablet eine visuelle Heatmap der tatsächlichen WLAN-Durchsatzleistungen anzeigt. Während bestehende Lösungen Geschwindigkeiten und Signalstärken kartieren und stellenweise Leistungstests beim Durchsatz durchführen können, ist die AirMapper-App laut Hersteller die erste, die eine visuelle Durchsatzkarte anfertigen kann. Dies soll eine Optimierung des WLANs ermöglichen, da es die tatsächliche Benutzererfahrung der mobilen Geräte berücksichtigt. AirMapper Professional ist ab sofort im E-Store von Fluke Networks zu einem Preis von 199 US-Dollar zu beziehen. *(ln)*

http://de.flukenetworks.com

2X Software gibt die Verfügbarkeit von Version 10.5 der Virtualisierungssoftware **2X ApplicationServer XG** für Microsoft Hyper-V, VMware und Citrix XenServer bekannt. Der Anbieter integriert im neuen Release neben der zentralen Bereitstellung von Applikationen und VDI-Funktionen ein vollständiges Thin Client-Management. Die neue Version umfasst zudem eine Reihe neuer Features wie etwa die Second Level-Authentication auf Basis von RADIUS, eine URL-Redirection-Blacklist sowie RAW-Printing. Die Preise für 2X ApplicationServer XG betragen ab 900 Euro für die Small Business-Version. Das 2X ClientManager-Modul kostet ab 370 Euro für zehn Clients. *(ln)*

www.2x.com/de/

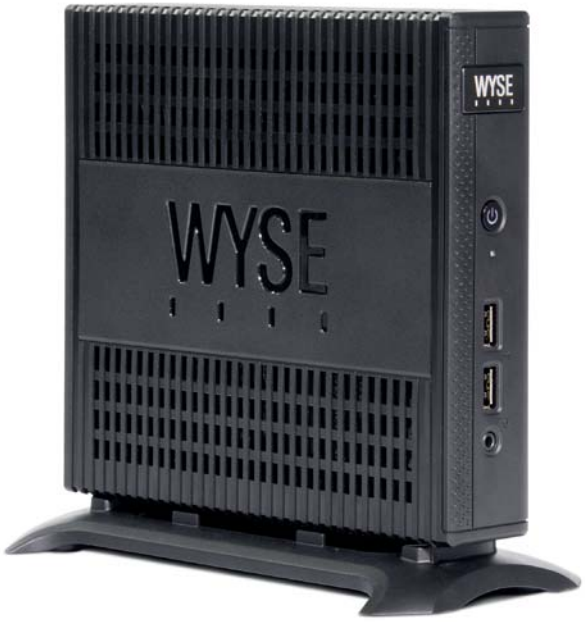
Passgenauer UTM-Schutz

WatchGuard will mit insgesamt vier neuen Varianten der XTM 5-Serie für mehr Performance beim UTM-Schutz sorgen

Mit dem Relaunch der **UTM-Serie XTM 5** (Extensible Threat Management) will **WatchGuard Technologies** vor allem an der Performance der Appliances gearbeitet haben. So konnte die **Geschwindigkeit der Paketfilterung laut Hersteller um fast 40 Prozent gesteigert** werden. Auch das Gateway Antivirus soll bis zu 190 Prozent schneller arbeiten, bei der Effizienz des Intrusion Prevention Systems meldet WatchGuard gar eine Steigerung von 220 Prozent. Mit den insgesamt **vier neuen Modellen** (XTM 515, XTM 525, XTM 535 und XTM 545) adressiert der Sicherheitsanbieter **Unternehmen mit 50 bis 500 Mitarbeitern**. Der allgemein zugrundeliegende Firewall-Durchsatz reicht von 2 GBit/s bei Version XTM 515 bis hin zu 3,5 GBit/s bei der Plattform XTM 545. Bei voller Ausnutzung sämtlicher UTM-Sicherheitsfunktionen liegt die Spanne laut Hersteller immer noch zwischen 850 MBit/s und 1,23 GBit/s. Der IT-Schutz richtet sich dabei konkret an der Bedrohung aus, die von einzelnen Anwendungen und deren Unterfunktionen im Zuge der jeweiligen Nutzung ausgeht. Über das Modul "Application Control" steuern Administratoren den Nutzerzugriff auf alle relevanten Anwendungen im Web 2.0 – unter anderem Facebook, Twitter oder LinkedIn – im Detail je nach Nutzergruppe und deren spezifischer Aufgabe direkt über die Unternehmens-Firewall. Darüber hinaus können Unternehmen die Einsatzmöglichkeiten von XTM 5 über weitere Funktionen an ihre Bedürfnisse anpassen und von Zusatz-Abonnements wie **Gateway Antivirus, WebBlocker, SpamBlocker und Reputation Enabled Defense** – dem cloudbasierten und kontextbezogenen Reputationsservice von WatchGuard – Gebrauch machen. Bereits im Standard bietet die neue Serie die Möglichkeit, sichere VPN-Tunnel für iOS-basierte Devices wie iPad und iPhone zu erstellen. Gleiches gilt für Smartphones oder Tablets, die mit Android ab Version 4.0 arbeiten. Der Preis für die neue XTM 5-Serie startet bei rund 1.740 Euro. *(ln)*

WatchGuard: www.watchguard.com/products/xtm-5/overview.asp

Schmale Clients für die Wolke



Aufgrund flexibler OS-Optionen soll sich die neue D Class von Dell Wyse nahtlos in zahlreiche Umgebungen integrieren lassen

Dell Wyse führt mit der **D Class** eine neue Midrange-Familie von Cloud Clients vor, die **sowohl Thin Clients als auch Cloud-PCs** enthält. Die neue Serie kombiniert laut Hersteller eine **hohe Systemleistung mit HD-Multimedia-Fähigkeiten** sowie gesteigerter Energieeffizienz. Der Thin Client D90D7 nutzt Firmware, die auf Microsoft **Windows Embedded Standard 7** basiert; das Modell D90DW nutzt Microsoft Windows Embedded Standard 2009. Beide Systeme unterstützen eine Vielzahl von Peripheriegeräten und verfügen über einen lokal installierten Internet Explorer sowie über lokale Terminal-Emulation. Beide Clients arbeiten in Infrastrukturen unter Citrix, Microsoft und VMware. Der Cloud-PC D00D soll eine vollständige Desktop-PC-Benutzererfahrung mit den Vorteilen des Cloud Computings vereinen. Grundlage hierfür ist die Provisionierungssoftware Dell Wyse WSM, die trotz zentraler Verwaltung alle Applikationen lokal ausführt. Das Thin Client-Modell D50D schließlich basiert auf einem erweiterten SUSE Linux Enterprise. Allen Geräten gemein ist die AMD-CPU, die mit 1,4 GHz taktet und damit **genug Leistung für rechenintensive Multimedia-Anwendungen** bieten soll. Die Dual Display-Unterstützung mit einem Display Port und einem DVI-I-Anschluss ermöglicht HD-Bilder bei einer Auflösung von bis zu 2.560 x 1.600 Pixeln für den Display-Port und bis zu 1.920 x 1.200 Pixeln für die DVI-I-Schnittstelle; bei der Nutzung beider Anschlüsse beträgt die Auflösung jeweils 1.920 x 1.200 Pixel. Die Netzwerkanschlüsse umfassen GBit-Ethernet, ein SFP-Modul für Fibre NIC, 802.11 a/b/g/n WLAN sowie Single- und Dual-Band Wireless und Bluetooth. **Vier USB 2.0-Anschlüsse** ermöglichen die Nutzung von Peripheriegeräten. Ferner ist die neue Serie gemäß der EPA Energy Star-Richtlinie zertifiziert und laut Hersteller um 13 Prozent effizienter als der nächstbeste Mitbewerber. Auch mit den geringen Abmessungen (170 mm hoch, 40 mm breit und 185 mm tief) will Dell Wyse gegenüber der Konkurrenz punkten. Die Preise für die neue Client-Familie von Dell Wyse beginnen bei 335 Euro. *(ln)*

Dell Wyse: www.wyse.com/products/overview/

Schnappschüsse im SAN

Veeam Software erweitert sein Flaggschiff-Produkt **Veeam Backup & Replication** um das Feature **Veeam Explorer für SAN-Snapshots**. Das Tool wurde gemeinsam mit HP entwickelt und soll es IT-Administratoren ermöglichen, virtuelle Maschinen und ihre Daten direkt von **HP LeftHand** und **HP StoreVirtual VSA Snapshots** wiederherzustellen. Da solche Snapshots über den Tag hinweg ohne nennenswerte Last auf Produktivsysteme erstellt werden können, ermöglicht die Wiederherstellbarkeit mit dem Werkzeug laut Veeam kürzere Recovery Point-Objectives. Das komme insbesondere häufig auftretenden Recovery-Szenarien zu Gute, etwa wenn Daten versehentlich gelöscht würden, Skripte Daten beschädigten oder Systemupdates Fehler verursachten. Veeam verfolgt dabei den Ansatz, SAN-Snapshots als Teil einer umfassenden Backup- und Recovery-Strategie einzusetzen, in der sich SAN-Snapshots und Image-Level Backups ergänzen. Anstatt SAN-Snapshots in Backups umzuwandeln, nutzt Veeam sie mit Explorer für SAN-Snapshots nativ. In allen Editionen von Veeam Backup & Replication 6.5 einschließlich der Free Edition ist das Feature kostenlos enthalten. *(dr)*

Veeam: www.veeam.com/de/

Genügsamer Profi-Switch

LANCOM Systems baut sein Switch-Portfolio um den **LANCOM GS-2326 aus**, einen **gemanagten Layer 2-Switch mit 24 GBit-Ethernet-Ports** und **zwei TP/SFP-Combo-Ports**. Mit einer Reihe Energiesparfunktionen wie der Abschaltung nicht benutzter Ports, einer automatischen Leistungsanpassung und lüfterlosem Betrieb soll der Switch **deutlich weniger Leistung** benötigen als vergleichbare Modelle. Dank einem Durchsatz von 56 GBit/s und Funktionen wie Quality of Service, Rapid Spanning Tree, Port Trunking, Bandbreitenbeschränkung, kurzen Latenzzeiten und einer GBit-Backbone-Anbindung richtet sich der GS-2326 an Umgebungen mit hohem Bandbreitenbedarf. Eine **portbasierte 802.1x-Zugangskontrolle** und die **TACACS+-Authentifizierung** sollen für Sicherheit sorgen. Zur Netzwerksegmentierung unterstützt der Switch bis zu **4.000 simultane VLANs**. Eine Port-Priorisierung erlaubt die individuelle Steuerung des Datenverkehrs etwa für Echtzeit-kritische Voice- oder Video-Anwendungen. Konfiguration und Verwaltung des Switches erfolgen über eine Web-Oberfläche, per Kommandozeile über Telnet oder den seriellen Port (RS 232). Eine verschlüsselte Verbindung mit SSH oder HTTPS ist ebenfalls möglich. Darüber hinaus integriert sich das Gerät in die LANCOM-Management-Tools LANconfig und LANmonitor sowie LANCOM Large Scale Monitor (LSM) und unterstützt dank integrierter MIB das Management via SNMPv3. Über das Virtual Stacking Management (VSM) lassen sich bis zu 16 Switches über eine gemeinsame IP-Adresse verwalten. Der GS-2326 ist ab sofort für knapp 600 Euro verfügbar. Das optionale SFP-SX-Modul SFP-SX-LC1 ist für 140 Euro, die LX-Variante SFP-LX-LC1 für 240 Euro erhältlich. *(dr)*

LANCOM Systems: www.lancom-systems.de

Der GS-2326 von LANCOM Systems unterstützt bis zu 4.000 VLANs

SSD-beschleunigte Speicherboliden

Nimble Storage fügt seinem **Portfolio an Speichersystemen** mit der Produktserie **CS400** einen neuen Baustein hinzu. Die auf **I/O-intensive Workloads** ausgelegten Modelle CS420, CS440, CS460 eignen sich laut Hersteller unter anderem für den Einsatz in der Oracle-gestützten Transaktionsverarbeitung oder in großen VDI-Installationen. Die einzelnen Varianten mit jeweils zwölf Festplatten-Slots unterscheiden sich in der mitgelieferten Speicherkapazität (brutto zwischen 12 und 36 TByte) sowie in der Größe des **SSD-gestützten Flash-Speichers**. Mit mindestens 640 und maximal 2.400 GByte an schnellem Flash will der Hersteller für besonders hohe Durchsatzraten sorgen. Allen Modellen gemein ist die Art der Netzwerkanbindung: Die Geräte finden pro Controller über sechs GBit-Ethernet-Ports und zwei 10 GBit-Ethernet-Ports Anschluss ins Netzwerk. Über zwei 6 GBit-SAS-Ports lässt sich das Storage-Array zudem mit Erweiterungseinheiten oder anderen Arrays der Serie koppeln. Nimble Storage verfolgt hierbei mit der "Scale-to-Fit"-Architektur den Ansatz, die CS-Systeme unterbrechungsfrei ausbauen zu können, um zunehmenden Kapazitäts- oder Leistungsanforderungen im Rechenzentrum zu begegnen. Mit weiteren Platten-Shelves lässt sich der Speicherplatz so mit 15 Festplatten pro Erweiterungssystem und maximal drei Einheiten auf mehrere hunderte TByte ausbauen. In einem Cluster zusammengeschlossene Arrays verfügen laut Hersteller über den Vorteil, Anwendungen und Workloads auf unterschiedliche Arrays aufteilen und Daten unterbrechungsfrei über die in einem Cluster eingerichteten Speicherpools hinweg migrieren zu können. Zu den weiteren Funktionen der neuen Serie zählen eine durchgängige Komprimierung, Thin Provisioning und die Möglichkeit, Snapshots zu erstellen. Version 2.0 des Betriebssystems soll schließlich für das einfache Management einzelner Arrays oder ganzer Cluster sorgen. Der Einstiegspreis für die neuen Modelle der CS400-Produktfamilie liegt bei rund 75.000 Euro. Die Preise für die Erweiterungssysteme beginnen abhängig von der Ausstattung bei rund 32.000 Euro. *(ln)*

Nimble Storage: www.nimblestorage.com

Wächter des Netzwerks

Mit **GFI LanGuard 2012** stellt **GFI Software** die neueste Version seiner **Software zur Schwachstellenanalyse, zum Patch Management und zur Inventarisierung** vor. Das Werkzeug verfügt laut Hersteller über leistungsstarke Überprüfungen, automatische Bereinigungen sowie eine ausführliche Schwachstellenbewertung sämtlicher im Netzwerk vorhandenen Geräte einschließlich Drucker, Router und Switches von Herstellern wie beispielsweise HP oder Cisco. Gemäß GFI **testet die Lösung Netzwerkkomponenten auf über 50.000 Schwachstellen** von Betriebssystemen sowie installierten Applikationen und sucht nach Sicherheitslücken und Fehlkonfigurationen. Darüber hinaus kann der Nutzer mit dem Tool **Netzwerk-Audits** durchführen, die auch iOS- oder Android-Geräte erkennen. Durch die Einführung der neuen Relay Agent-Technologie sollen sich selbst getrennte Netzwerksegmente innerhalb von kürzester Zeit überprüfen lassen sowie **Patches und Definitionsupdates vom zentralen Server ausrollen** lassen. Ziel sei hierbei, auch sehr große, verteilte Netzwerke bei einer minimalen Inanspruchnahme der Bandbreite schnell zu erfassen und auszuwerten. Nutzer können mit dem Programm zudem Patch- und Update-Aufträge von einer zentralen Konsole aus verwalten und überwachen. Mit GFI LanGuard 2012 können Administratoren weiterhin eine Bestandsaufnahme der im Netzwerk eingesetzten Geräte durchführen, Hardware- und Software-Komponenten erfassen und sich bei Veränderungen benachrichtigen lassen. Darüber hinaus stellt das Werkzeug sicher, dass alle eingesetzten Antivirus-Lösungen auf dem aktuellen Stand sind und beispielsweise der Echtzeitschutz aktiv ist. Der Preis der Software berechnet sich nach der Anzahl der überwachten IPs. Bei 300 IPs etwa ist mit 10 Euro pro IP zu rechnen. *(ln)*

GFI LanGuard 2012 scannt das Netzwerk auf über 50.000 Schwachstellen und hilft bei Inventarisierung und Patch-Management

GFI Software: www.gfi.com/network-security-vulnerability-scanner

Sicherer Fernzugriff

sayTEC Solutions hat seine **Client/Server-Fernzugriffslösung sayTRUST Access** ausgebaut und bringt sie in **Version 4** auf den Markt. Unternehmen können damit Mitarbeitern und Partnern **von extern Zugriff auf ihr Firmennetz, ein Teilnetzwerk oder auch nur einen einzelnen Rechner geben**. Das Werkzeug besteht aus einem Server, der als Appliance oder als Software angeboten wird, und einer Client-Lösung in Form eines USB-Sticks, der in drei Varianten erhältlich ist. Der Zugriff ist je nach Modell des Sticks per PIN und 2.048 Bit-Zertifikat sowie biometrisch gesichert, in der höchsten Sicherheitsstufe mit einer Zertifizierung nach FIPS 140-2 Level 3. Die GUI von sayTRUST Access wartet laut Hersteller mit einer runderneuerten Oberfläche und einer Reihe neuer Funktionen auf, mit der Anwender sich ein individuelles Menü aus Programmen, Dateien und Internet-Links zusammenstellen und persönlich gestalten können. Per Drag and Drop lassen sich beliebige Verknüpfungen erstellen und portable Apps in das Menü integrieren. Nutzer können Ordner und Anwendungen in Registerkarten ordnen und diesen individuelle Funktionen sowie persönliche Icons und Farben für Hintergrund und Text zuweisen. Für Programme und Dateien, die geschützt werden müssen, lassen sich verschlüsselte Container anlegen, deren Verwaltung und Einbindung der Nutzer über ein Encryption-Start-Tool handhaben kann. Ein integriertes Backup-Tool soll zudem dafür sorgen, dass keine Daten verloren gehen. sayTRUST Access ist in verschiedenen Leistungsstufen erhältlich. Die kleinste Konfiguration mit Server sowie Software und Lizenzen für fünf Named User liegt bei rund 1.300 Euro. Die USB-Clients sind in der einfachsten Ausstattung ab 30 Euro verfügbar. *(ln)*

Die Client-Komponente von sayTRUST Access kommt als USB-Stick daher, der je nach Variante auch mit einem Fingerabdruck-Scanner ausgestattet ist

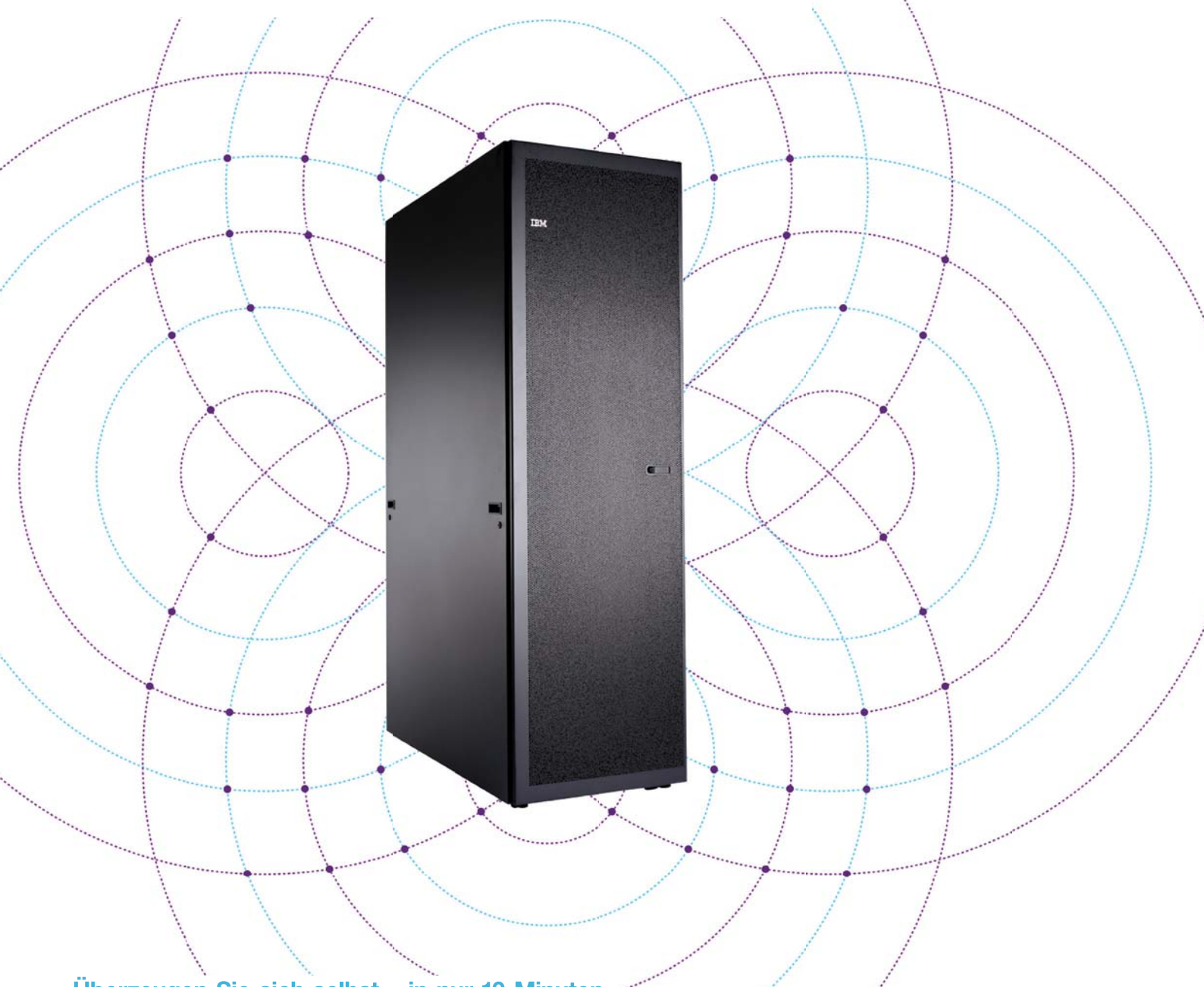
sayTEC: www.saytec.eu/produkte/saytrust-access/

Virtualisierung leicht gemacht.

Eine hohe Anzahl von Hardware-, Software- und Netzwerkkomponenten kann Virtualisierung sehr aufwendig machen. Die neue IBM BladeCenter® Foundation for Cloud mit Intel® Xeon® Prozessoren ändert das grundlegend.

Die vorkonfigurierte Plattform mit integriertem Management ist sofort einsatzbereit und einfach zu bedienen. Da sich das System problemlos in Ihre vorhandene Infrastruktur einfügt, können Sie direkt durchstarten, ohne wertvolle Ressourcen zu vergeuden.

Wechseln Sie einfach zu Ihren Konditionen in die Cloud und nicht zu denen Ihres Anbieters. Mit IBM BladeCenter Foundation for Cloud können Sie die Flexibilität Ihres Unternehmens erhöhen und Ihre IT-Kosten senken.



Überzeugen Sie sich selbst – in nur 10 Minuten.

Wie IBM BladeCenter Foundation for Cloud Komplexität reduziert, erfahren Sie unter **ibm.com**/systems/de/foundation

IT-Administrator Workshop "Windows Server 2012" im November in Hamburg und Frankfurt/Eschborn

Die Cloud ist nicht alles

von John Pardey

ITANet Workshop-Partner:

Microsoft preist seinen neuen Windows Server 2012 als Baustein für eine IT-Infrastruktur, die optimal auf den Einsatz von Public-Cloud Diensten vorbereitet ist und derartige Dienste intern zur Verfügung stellen kann. Diesen Anspruch bedient der Hersteller unter anderem mit der Version 3 von Hyper-V. Unser kostenloser Workshop gibt einen ersten Einblick, was sich beim Hypervisor unter der Haube getan hat. Doch auch abseits der Cloud hat Microsoft sein Server-Produkt weiterentwickelt. Unsere Dozenten untersuchen daher, wie der neue Server-Manager den Admin unterstützt. Backup & Recovery sowie ein Blick auf Neuerungen im Active Directory runden den Workshop ab.

Aus Administrationssicht ist der "Server-Manager" als neue zentrale Verwaltungskonsole die auffälligste Neuerung in Windows Server 2012. Von dort aus initiiert der Administrator wichtige Aufgaben wie etwas Sicherung und Wiederherstellung eines Domänencontrollers. Unser Workshop führt die Teilnehmer ausführlich in die Arbeit mit dem Server-Manager ein. Die Dozenten zeigen beispielsweise, wie sich neue Server einfügen lassen und auch wie das Monitoring funktioniert.

Evergreen Backup & Recovery

Wer ein neues Serverbetriebssystem in seine IT-Infrastruktur aufnimmt, sollte sich in einem der ersten Schritte mit Wegen zur Sicherung und Wiederherstellung vertraut machen, damit das schicke neue System nicht im schlimmsten Falle zum Klotz am Bein wird.

Daher befassen wir uns in den beiden Workshops intensiv mit den Aufgaben rund um Backup & Recovery von Windows Server 2012: Wir stellen die neuen Backup & Recovery-Funktionen sowie deren Installation und Verwaltung vor. Und als Anwendungsfälle wenden sich die Dozenten dem Disaster Recovery eines Mitgliedsservers, der Sicherung eines Domaincontrollers sowie der Wiederherstellung von Servern zu.

Active Directory und Hyper-V 3.0

Unseren Workshop runden dann noch zwei wichtige Windows Server-Features ab, die mit Windows 2012 einige Neuerungen erfahren haben. So lassen sich nun unter anderem mit Bordmittel Domänencontroller klonen. Und Hyper-V 3.0 schafft mit seinen erweiterten Management-Fähigkeiten den technologischen Anschluss an Marktführer VMware. In den letzten beiden Abschnitten des Workshops gehen wir detailliert auf die Neuerungen ein.

Wir würden uns sehr freuen, Sie zahlreich auf unseren kostenlosen Workshops in Hamburg und Frankfurt begrüßen zu dürfen. Alle Informationen zu den Veranstaltungen und der Anmeldung entnehmen Sie bitte dem Kasten auf dieser Seite.

Agenda

13:00 Uhr: **Begrüßung**

13:15 Uhr: **Mehr Effizienz mit dem neuen Server-Manager**

- Installation von Rollen und Features
- Hinzufügen zusätzlicher Server
- Remoteinstallation und Verwaltung von Rollen und Features
- Monitoring mit dem Server-Manager

Dozenten: Sascha Giebelhausen und Thomas Gronenwald, admeritia GmbH

14:15 Uhr: **Partnervortrag: Veeam – mehr als Backup!**

Dozent: Matthias Frühauf, Veeam Software

15:00 Uhr: **Kaffeepause**

15:15 Uhr: **Sichern und Wiederherstellen mit dem Windows Server 2012**

- Funktionsumfang
- Installation & Verwaltung
- Disaster Recovery eines Mitgliedsservers
- Sicherung eines Domänencontrollers
- Wiederherstellung von Servern

Windows Server 2012 und Active Directory

- Klonen von Domänencontrollern
- Die neue Verwaltung

Neuerungen in Hyper-V 3.0

Dozenten: Sascha Giebelhausen und Thomas Gronenwald, admeritia GmbH

17:30 Uhr: **Ende des Workshops**

Termin & Ort

15. November: Hamburg

Fast Lane Institute for Knowledge Transfer GmbH, Gasstraße 4a, 22761 Hamburg

19. November: Frankfurt/Eschborn

Fast Lane Institute for Knowledge Transfer GmbH, Ludwig-Erhard-Straße 3, 65760 Frankfurt/Eschborn

Teilnahmegebühr

Für IT-Administrator Abonnenten kostenlos.

Sollten Sie über ein Abonnement verfügen und einen oder mehrere Kollegen zum Workshop mitbringen wollen, erheben wir eine Schutzgebühr von 75 Euro (zzgl. 19% MwSt.) pro zusätzlichem Teilnehmer. Für Nicht-Abonnenten wird eine Schutzgebühr von 145 Euro (zzgl. 19% MwSt.) fällig.

Anmeldung

www.it-administrator.de/workshops

Workshop "Windows Server 2012"

it-sa 2012, 16. bis 18. Oktober 2012, Nürnberg

Kleine Begleiter im Blick

von Daniel Richey

Vom 16. bis 18. Oktober 2012 präsentieren zahlreiche Aussteller auf der it-sa im Nürnberger Messezentrum ihre Neuheiten rund um IT-Security. Im Mittelpunkt der it-sa 2012 stehen dabei aktuelle Themen wie Mobile Security einschließlich Bring Your Own Device, Identity- und Access Management und die Absicherung von industriellen Netzwerken. Mit Congress@it-sa will die Sicherheitsmesse zudem erstmals eine Kongress-Plattform für den Dialog und vertiefte fachliche Diskussionen bieten.

Die Vorbereitungen für die it-sa 2012 [1] sind in vollem Gange und die inhaltlichen Schwerpunkte stehen bereits fest: Zu den Top-Themen zählen Mobile Security, insbesondere die Trendthemen "Bring your own Device", Sicherheit in der Cloud, Internet- und Netzwerksicherheit sowie Identity und Access Management. Weitere Fokusthemen sind Rechenzentrumssicherheit und Sicherheit für industrielle Netzwerke, Datenschutz und Cybercrime. Die it-sa will so IT-Profis aus dem In- und Ausland eine Plattform bieten, um sich über die neusten Entwicklungen auf dem Markt für IT-Sicherheit auszutauschen.

Mehrere Sonderschauen informieren auf der Messe zu aktuellen Themen. Mit dabei ist beispielsweise die "Convergence Area". Sie soll die Integration von IT-Sicherheitstechnik in die moderne Gebäudetechnik beleuchten. Zu den Themen Identity und Access Management will die "IAM Area" praxisnah informieren. Die Sonderschau "Das perfekte Rechenzentrum" biete Besuchern einen umfassenden Überblick über Sicherheitsmaßnahmen im Rechenzentrum. Weitere Sonderschauen schlagen laut Veranstalter die Brücke zur akademischen Welt und zu jungen IT-Sicherheitsfirmen: "Campus@it-sa" bringt Vertreter aus Unternehmen und Hochschulen mit Studierenden zusammen und fördert den übergreifenden Austausch zur IT-Sicherheit. Unternehmen, die neu auf dem IT-Sicherheitsmarkt sind, erhalten mit "Startups@it-sa" eine eigene Plattform, um sich den Fachbesuchern optimal zu präsentieren.

Die it-sa 2012 öffnet Mitte Oktober ihre Pforten. Das Thema "Bring your own Device" steht dabei ganz oben auf der Agenda

Neu auf der it-sa: Congress@it-sa

Erstmals präsentiert die it-sa den Fachkongress Congress@it-sa. Er vertieft in hochkarätigen Vorträgen aktuelle Security-Themen. Ziel ist es, der IT-Security-Branche mit diesem Kongress noch mehr spezialisiertes Wissen zur Verfügung zu stellen. Experten aus der Branche beleuchten hierfür die Themen Sicherheit in der Cloud, Mobile Security – insbesondere mit "Bring your own Device" (BYOD) – und die industrielle IT-Sicherheit. Zielgruppe der vier halbtägigen Tracks sind IT-Sicherheitsverantwortliche, Geschäftsführer, Datenschutzbeauftragte und Produktionsverantwortliche. Am Messe-Dienstag steht das Thema "Sicheres Cloud-Computing – Gefahren, Planung, Praxis" auf dem Programm. Dies beinhaltet auch ein Live Hacking sowie einen Überblick über die bestehenden Zertifizierungen. Am Mittwoch dann Mobile Security und Bring your own Device. Für Donnerstag schreibt sich der Veranstalter die Themen " Industrielle IT-Sicherheit – Neue Angriffsziele, alte Konzepte?" und "Datacenter Expert Summit – Sicherheit im Rechenzentrum" auf die Fahnen. Allerdings müssen die einzelnen Tracks separat und kostenpflichtig gebucht werden.

[1] it-sa 2012
C9W44

Link-Codes

Im Test: Netop Remote Control 11

Fern, und doch ganz nah


Quelle: Benis Arapovic - 123RF

von Jürgen Heyer

Die Anforderungen an eine Fernsteuersoftware sind ebenso vielfältig wie die Lösungen, die der Markt bietet. Sobald es jedoch um den sicheren Zugriff auf Server geht, die Bereitstellung des Dienstes sowohl im lokalen Netz als auch via Internet, um Multiplattformfähigkeit und die Option, alles in Eigenregie zu betreiben, wird die Auswahl dünn. Ein Produkt, das all das bieten will, ist Netop Remote Control. IT-Administrator hat sich genauer angesehen, mit welchen Besonderheiten Version 11 dieses modularen Werkzeugs auftrumpfen kann.

Dank des integrierten RDP-Zugriffs ist für die Fernsteuerung von Windows-Servern innerhalb eines Intranets in der Regel kein zusätzliches Produkt erforderlich. Sobald es jedoch auch um nicht unter Windows laufende Systeme geht, muss der Administrator andere Wege gehen und verschiedene Verfahren nutzen. Daraus resultierende unterschiedliche Benutzerverwaltungen erhöhen den Pflegeaufwand. Weiterhin sind viele Fernsteuerungs-Tools nicht in der Lage, die Zugriffe umfassend und revisionssicher aufzuzeichnen, also die Sitzungen zu filmen. Gerade beim Support durch externe Firmen oder Berater ist dies jedoch oft gewünscht. Die nächste Herausforderung stellt der Zugriff via Internet dar. Hier gibt es diverse Anbieter von Diensten, die zu diesem Zweck eigene Plattformen betreiben, um das Routing zu bewerkstelligen und die Gegenstellen zu verbinden. Falls aber die Sicherheitsanforderungen eines Unternehmens so hoch sind, dass es den Verbindungsaufbau nicht anonymen, fremdadministrierten Servern überlassen will, erweisen sich diese Angebote als ungeeignet.

Genau hier kommt Netop Remote Control von Netop Solutions, ehemals Danware, ins Spiel. Netop ist schon seit vielen Jahren als Fernsteuertool bekannt und immer weiter verfeinert worden. Dank der langjährigen Entwicklung und der sich auch in der Vergangenheit immer wieder verändernden Anforderungen ist das Tool nicht nur Multiplattform-fähig, sondern unterstützt durch seine Kompatibilität bis hin zu den älteren Netop-Versionen 6.x/ 5.x unter anderem auch noch sehr alte Windows-Versionen wie Windows 95 und 98 sowie die früher verwendeten Verschlüsselungsmodi. Zusatzmodule wie Security und Name Server, WebConnect sowie Netop Gateway und Netop Mobile & Embedded ermöglichen eine individuelle Anpassung des Kernprodukts Remote Control an die jeweiligen Anforderungen. Umfassend unterstützt wird auch ein Einsatz in Verbindung mit Terminalservern, um unter anderem aus der Ferne auf laufende Terminalsitzungen zuzugreifen.

Um den Zugriff auf einen Host zu erlangen, kann ein Gast bei Netop dazu verpflichtet werden, bis zu sechs Sicherheitskriterien zu erfüllen: MAC-/IP-Adressprüfung, geschlossene Benutzergruppe, Authentifizierung, Callback, benutzerkontrollierter Zugriff und Autorisierung. Betrachtet haben wir in diesem Test das Kernprodukt in erster Linie unter dem Aspekt der sicheren Fernsteuerung von Servern. Dazu warfen wir auch einen Blick auf den Security Server sowie die Möglichkeit zur sicheren Fernsteuerung über das Internet.

Getrennte Konfiguration von Host und Gast

Nach wie vor verfolgt Netop den Ansatz eines individuellen Setups von Host (beispielsweise ein zu steuernder Server) und Gast (der Arbeitsplatz des Administrators) mit unterschiedlichen Installationsdateien. Es wird also nicht mit Zwittern gearbeitet, bei denen jede Seite beide Rollen einnehmen kann. Trotzdem ist es beispielsweise möglich, für Präsentationszwecke die Blick-

Betriebssysteme

Windows 95 bis Windows 7/2008 R2, 32 und 64 Bit, Server und Workstation-Versionen, Hardware-Voraussetzungen entsprechend des genutzten Betriebssystems. Mac OS X ab 10.5, Linux Redhat/SUSE Enterprise Desktop oder Server, OpenSUSE, CentOS, Ubuntu, Fedora, Mandrake. Sun Solaris ab Version 8, OS/2 Warp ab 3.0.

Kommunikation

Kommunikation per TCP/IP (IPv4, IPv6), IPX, NetBIOS, TAPI, CAPI oder Infrarot.

Systemvoraussetzungen

richtung umzudrehen, nur erfolgt der erste Verbindungsaufbau immer vom Gast zum Host. Die Installation beider Seiten läuft jedoch weitgehend identisch ab. Das Setup fragt den Lizenzschlüssel ab und gibt als Wahl eine typische, benutzerdefinierte und vollständige Installation vor. Dann kommt das Angebot, die Windows-Firewall passend zu konfigurieren und für spätere Änderungen der Konfigurationseinstellungen die Installationsdateien zu speichern.

Anschließend startet ein Assistent für die Vorgabe der Grundeinstellungen. Dieser fragt nach der Verbindungsgeschwindigkeit unter dem Aspekt, ob die typische Bandbreite größer oder kleiner 4 MBit/s ist. Aus der Historie heraus ist Netop durchaus in der Lage, auch über langsame Verbindungen wie Modem, Infrarot, Seriell oder ISDN zu operieren. Sofern eine Kommunikation über im System vorhandene Modems und serielle Geräte stattfinden soll, kann Netop automatisch danach suchen und passende Kommunikationsprofile anlegen. Zuletzt fragt der Assistent noch ab, ob auch das weiter später beschriebene Netop WebConnect genutzt werden soll. Ist dies der Fall, sind anschließend die URL des Verbindungsmanagers sowie die notwendigen Anmeldeinformationen einzugeben.

Beeindruckt hat uns im Test die Vielzahl der unterstützten Gast- und Hostbetriebssysteme, wobei der Administrator zum Teil auf ältere Netop-Versionen zurückgreifen muss. Von Vorteil ist, dass die Versionen untereinander kompatibel sind und auch noch die Verschlüsselungen von Netop 5.x/6.x unterstützt werden. Dies kann der Administrator je nach Bedarf aktivieren und deaktivieren. Im Windows-Umfeld werden alle Versionen bis hin zu Windows 95 unterstützt, die Kommunikation kann über TCP/IP, IPX, NetBIOS, Modem, ISDN/CAPI und Infrarot erfolgen. Weiterhin gibt es Host und Gast für Mac OS X, bezüglich Linux werden RedHat, SUSE, CentOS, Ubuntu, Fedora und Mandrake unterstützt. Außerdem ist Netop nutzbar mit Solaris und OS/2.

Unübersichtliche Optionsvielfalt

Wer das erste Mal mit Netop arbeitet, dürfte sich von dem gewaltigen Funktions- und Optionsumfang geradezu erschlagen fühlen. Auch haben sich die Benutzeroberflächen von Gast und Host im Laufe der Jahre von ihrem Konzept her kaum geändert, wurden aber funktional ständig erweitert. Dadurch wirkt alles etwas altbacken und zugleich unübersichtlich. Sicher lässt sich mit wenigen Klicks schnell eine Fernsteuerverbindung aufbauen, bis aber beide Seiten hinsichtlich der gewünschten Authentisierung, der Berechtigung für unterschiedliche Nutzer und des Verhaltens bei Ereignissen wie beispielsweise einem Verbindungsabbruch bedarfsgerecht konfiguriert sind, bedarf es einer umfassenden Einarbeitung. Auch ist es bei gelegentlicher Administration gar nicht so einfach, einmal gefundene Optionen beim nächsten Mal auch wieder zu finden. Eigene Notizen erscheinen uns da sehr hilfreich.

Bild 1: Geradezu erschlagend ist der Umfang der einstellbaren Optionen auf Gastseite, verteilt auf 21 Registerblätter

Wenden wir uns zunächst der Hostseite zu, die insgesamt über weniger Einstellmöglichkeiten verfügt. Im Normalfall ist der Host an einem kleinen Symbol in der Taskleiste erkennbar, es gibt aber einen soge-

nannten Tarnkappenmodus, bei dem diese Anzeige versteckt wird. Über das Icon lässt sich die GUI des Hosts öffnen. In sieben Registerblättern mit den weitgehend selbsterklärenden Bezeichnungen "Allgemein", "Verbindungen", "Verlauf", "Dienste", "Kommunikation", "Namen" und "Meldungen" finden Administratoren relevante Informationen.

Bezüglich des Namens, unter dem ein Host zu finden ist, stellt Netop verschiedene Möglichkeiten bereit: So ist ein Host immer unter seiner IP-Adresse erreichbar und es wird zusätzlich ein Netop-Name zugewiesen. Dieser wiederum kann identisch zum Computernamen mit oder ohne vorangestellter Arbeitsgruppe sein, von einer Umgebungsvariablen abhängen oder beliebig zugewiesen werden. Letzteres eröffnet die Möglichkeit, aus Sicht eines Gastes logische Namen unabhängig vom Computernamen zu vergeben. Das Hinzufügen der Arbeitsgruppe ist wiederum dann sinnvoll, wenn es notwendig ist, ein System innerhalb mehrerer Arbeitsgruppen oder Domänen eindeutig zu identifizieren. Die Verwendung einer Umgebungsvariablen für den Namen ist beispielsweise beim Einsatz in einer Terminalserver-Umgebung zu empfehlen, um dann der Sitzung den Benutzernamen zu geben, damit sie durch einen Gast eindeutig identifiziert werden kann. Bei Verwendung des Computernamens hätten alle Sitzungen auf einem Terminalserver die gleiche Bezeichnung. Als Folge wäre dann nur eine Sitzung möglich.

Selbstverständlich lässt sich die Host-Komponente beim Windows-Start automatisch mitstarten, was für eine Fernadministration von Servern besonders wichtig ist. Für eine Authentifizierung beispielsweise gegenüber dem Active Directory muss der Host-Dienst unter einem AD-Benutzer laufen, um so auch einen AD-Zugriff sicherzustellen, wenn am System kein Benutzer lokal angemeldet ist. Es ist hier übrigens sinnvoll, für die Dienstausführung ein eigenes Benutzerkonto anzulegen, Netop kann dann auch wöchentlich das Kennwort dieses Benutzers eigenständig ändern, was zugleich zufällige und damit sehr sichere Kennwörter gewährleistet. Ferner erlaubt der Host auch einen Audio-Video-Chat sowie einen Ferndruck, was aber für eine Fernsteuerung von Servern wohl eher selten benötigt wird.

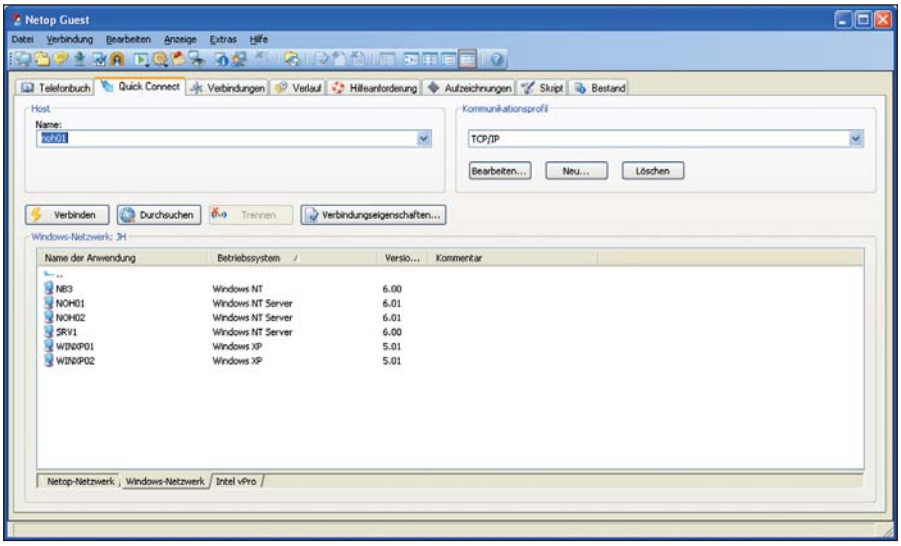


Bild 2: Die Quick-Connect-Ansicht ermöglicht durch die integrierte Suchfunktion im Netzwerk einen schnellen Verbindungsaufbau

Einen eigenen Optionsblock des Hosts bildet die Definition der Gast-Zugriffsrechte. Bei der Zugriffsmethode bietet Netop insgesamt fünf Verfahren an. Entweder alle Gäste bekommen Standardzugriffsrechte oder das Programm arbeitet mit individuellen Benutzern und Rollen. Letztere lassen sich wiederum mit einer Autorisierung via Netop, Windows-Sicherheitsmanagement oder einem Directory-Service verknüpfen. In diesen drei Fällen sind an jeden Host lokal Sicherheitsrollen und Benutzer oder Gäste anzugeben, denen explizite Rechte wie unter anderem Fernsteuerung, Dateiübertragung, Chat oder die Programmausführung gewährt werden. Diese Verfahren eignen sich in der Regel für eine Pflege weniger Hosts, da jeder einzeln zu administrieren ist. Eine zentrale Pflege ermöglicht die letzte Option, der Netop Security Server, der im weiteren Verlauf beschrieben ist. Neben der Autorisierung muss der Administrator die Richtlinien festlegen, wie das Trennen einer Verbindung etwa bei falscher Passworteingabe. So ist es möglich, dass sich ein Host bei mehrfacher falscher Passworteingabe gar selbst beendet.

Weiterhin ist das Filtern anhand von IP- und MAC-Adressen möglich, es kann eine Anmeldung per Smartcard verlangt werden und der Administrator kann zwischen sieben Verschlüsselungsoptionen beginnend von keiner Verschlüsselung bis zu einer starken Verschlüsselung mit 256 Bit AES und einem komplexen Schlüsseltausch (2.048 Bit Diffie-Hellmann, 256 Bit AES und 512 Bit SHA) wählen. Dabei lassen sich einzelne oder auch alle Optionen anwählen. Ein Gast und ein Host handeln dann eine geeignete Verschlüsselung aus. Wird kein auf beiden Seiten erlaubter Modus gefunden, wird keine Kommunikation aufgebaut. Damit die Einstellungen nicht von jedem geändert werden können, der einen Systemzugriff hat, lassen sich diese per Passwort schützen.

Direkter Rechnerzugriff

Der Optionsumfang des Netop-Gasts übertrifft den Host deutlich. Die Programmoptionen umfassen immerhin 21 Registerblätter, um alle möglichen Einstellungen unter anderem zur Fernsteuerung, Aufzeichnung, Programmausführung, Inventur und Anmeldung zu erfassen. Netop ermöglicht über einen SCS-Web-Service den Zugriff auf die Intel vPro-Funktion, um auch auf entsprechend ausgestattete, ausgeschaltete Computer zugreifen zu können, sofern diese mit dem Netzwerk verbunden sind. Ein eigenes Menü gibt es für die Optionen des Datei-Managers, um die Einstellungen für das Übertragen von Dateien sowie das Verhalten beim Überschreiben und Löschen von Dateien vorzugeben.

Beim Arbeiten mit dem Gast wird schnell offensichtlich, dass Netop weitaus mehr kann, als nur die Fernsteuerung eines Hosts durch Übertragung der Bildschirmanzeige.

So enthält Netop einen komfortablen Dateimanager, um Dateien in beide Richtungen zu übertragen. Dies kann bequem per Drag-and-Drop erfolgen. Weiterhin lassen sich Dateien und Ordner verschieben, synchronisieren und duplizieren, neben einer manuellen Bedienung ist auch eine skriptgesteuerte Ausführung möglich. Weitere Funktionen sind der Audio-Video-Chat, das Ausführen von Programmen oder Befehlen, das Überwachen mehrerer Hosts und der Bestandsabruf (Inventarisierung) eines Systems. Für eine Fernsteuerung von Servern weniger relevant dürfte die Möglichkeit sein, die Blickrichtung quasi umzudrehen, sodass der Gast dem Host etwas vorführen kann. Dabei kann der Gast dann sogar das zu übertragende Fenster vorgeben, sodass auf Hostseite nicht die gesamte Gastoberfläche zu sehen ist.

Eine andere spezielle Funktion ist der Aufbau eines Tunnels. Über diesen können einzelne Anwendungsports vom Host zum Gast umgeleitet werden. Der Tunnel ist dann sinnvoll, wenn der Host nicht ferngesteuert werden muss oder beispielsweise bei einem eingebetteten Linux-System wie einem Kassensystem gar kein konventioneller Desktop zur Verfügung steht. Der Gast kann dann eine lokale Anwendung ausführen, die über den getunnelten Port mit dem Host kommuniziert.

Gerade für den Zugriff auf Server hat uns im Test die Funktion "Remote Management" gut gefallen. Statt für eine Aktion auf einem System erst eine ferngesteuerte Sitzung zu starten und dann darin systemnahe Tools wie den Task-Manager oder die Diensteverwaltung aufzurufen, kann dies über das Remote Management direkt erfolgen. Die Remote Management-GUI läuft dann auf dem Gast und holt sich nur die relevanten Inhalte vom Host. Gerade bei Verbindungen mit wenig Bandbreite ist dann ein weitaus flüssigeres Arbeiten möglich.

Der Gast ist auf das Verwalten vieler Verbindungen ausgelegt, die zudem noch auf verschiedenen Wegen propagiert werden können. So kann der Gast über die Funktion "Quick Connect" das Netz nach Netop-Hosts durchsuchen, weiterhin in Windows-Netzwerken browsen und über den SCS-Web-Service sowie vPro auf Systeme zugreifen. Der Administrator kann einen Hostnamen direkt angeben und dabei zwischen unterschiedlichen Kommunikationsprofilen wählen, sofern ein System nicht über TCP/IP erreichbar

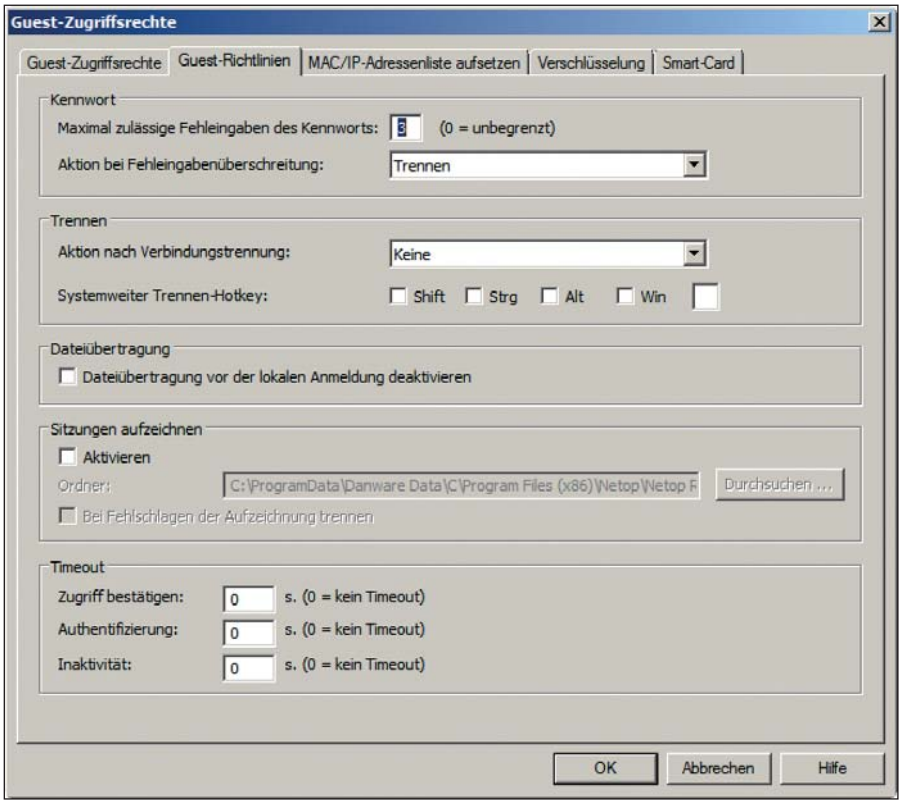


Bild 3: Auf Hostseite lassen sich diverse, individuelle Richtlinien für die Gastzugriffsrechte festlegen

ist. Das Profil "Web Connect" benötigt er, um auf einfachem Weg Systeme via Internet zu erreichen.

Zum Abspeichern ständig genutzter Verbindungen besitzt Netop ein Telefonbuch. Neben der Kommunikation via Netop lassen sich hier auch RDP-Verbindungen eintragen. Das hat für den Administrator den Vorteil, dass er auch bei der Nutzung unterschiedlicher Wege zu den Systemen den Aufruf aus einer Liste initiieren kann.

Der Start einer ferngesteuerten Sitzung erfordert im Idealfall nur einen Mausklick. Ähnlich wie die GUI des Gasts verfügt auch das Fernsteuerfenster über eine Kopfzeile mit diversen Icons, um etwa die Dateiübertragung oder das Remote Management parallel zu starten. Auch lassen sich hier über einzelne Schaltflächen die Kommandos Strg-Esc und Strg-Alt-Entf senden. Weiterhin gibt es die Möglichkeit, sich die Verbindungsliste anzeigen zu lassen und mehrere parallele Verbindungen zu unterbinden. So ermöglicht Netop durchaus den parallelen Zugriff mehrerer Gäste auf einen Host. Es gibt aber in der Praxis immer wieder Situation, wo dies zumindest temporär nicht gewünscht ist. Dann lassen sich die Verbindungen auf eine beschränken. Neben der beschriebenen Dateiübertragung kann der Administrator auch die Zwischenablage transferieren und hat weiterhin die Möglichkeit, Dinge auf dem Hostdesktop zu markieren oder zu zeichnen sowie den Cursor wie einen vergrößerten Zeiger darzustellen. Genauso wie auf Hostseite lassen sich auch am Gast die Einstellungen per Kennwort schützen.

Abgestufte Sicherheitsoptionen

Wie zuvor erwähnt, unterstützt Netop fünf unterschiedliche Autorisierungsverfahren, wobei vier davon lokale Vorgaben erfordern. Dies führt letztendlich dazu, dass die Einstellungen an jedem Host individuell zu pflegen sind. Diese Variante stellt die Verwendung des Netop Security Servers dar. Da es sich hierbei um einen erweiterten Host handelt, unterscheidet sich die Grundinstallation nicht, auch der Assistent stellt die gleichen Fragen.

Im Gegensatz zum normalen Host wird aber mit dem Security Server auch die Administrationskonsole, der Security Manager, installiert. Bei dessen ersten Aufruf sind diverse Einstellungen vorzunehmen, damit der Security Server ordnungsgemäß läuft. Sofern der Manager wie im Test auf einem Windows Server 2008 R2 installiert wird, ist darauf zu achten, dass er als Administrator ausgeführt wird. Der parallele Betrieb mehrerer Security Server zu Redundanzzwecken ist recht problemlos realisierbar, indem diese jeweils untereinander bei den Sicherheitsrichtlinien eingetragen werden.

Für eine Testumgebung reicht es, eine lokale Datenbank anzulegen, ansonsten eignet sich eine Datenbank mit ODBC-Anbindung. Weiterhin wird beim ersten Aufruf des Managers ein Public Key erzeugt, der an einem sicheren Ort verwahrt werden sollte. Wird dieser einmal verändert, müssen alle Hosts neu konfiguriert werden. Dann sind der bevorzugte Gast-Typ (Windows-Benutzer, Netop Gast-ID, RSA SecurID oder Directory Service) sowie Host-Typ (Windows Benutzer, Workstation, Netop Host-ID) auszuwählen.

Ist die Datenbank definiert, kann sich der Security Server daran anmelden. Im Test haben wir eine Anbindung an eine Windows-Domäne konfiguriert, um für die weitere Rechtevergabe die dort angelegten Benutzer und Gruppen zu verwenden. Zu diesem Zweck wird die Domäne im Security Manager aufgenommen, dann können die Gruppen und Benutzer sowie Workstations und auch Workstation-Gruppen importiert werden. Soll auch eine LDAP-Anbindung erfolgen, ist dieser Verzeichnisdienst ebenfalls einzutragen.

Um nun Rechte zuzuweisen, sind im Security Manager Rollen anzulegen. Diese Rechte beziehen sich auf die einzelnen Funktionen von Netop wie Fernsteuerung, Datenübertragung und Tunnel. Vier Rollen sind bereits vordefiniert, wobei zwei davon (Full Control, No Access) nicht verändert werden können. Über den Punkt Rollenzuweisungen erfolgt dann die Zuordnung einer Rolle zu einem Benutzer oder einer Gruppe.

Sofern es sich beim Einsatz von Netop um eine geschlossene Benutzergruppe handelt, bietet der Hersteller noch einen speziellen Schutz in Form einer zugewiesenen Seriennummer an. Eine geschlossene Benutzergruppe liegt dann vor, wenn das Produkt nur von einem fest umrissenen Benutzerkreis beispielsweise nur innerhalb eines Unternehmens genutzt werden soll. Mit einer derartigen Seriennummer akzeptieren die Gast- und Hostmodule nur Verbindungen untereinander. Eine Teilnahme von einem mit anderer Seriennummer versehenen Modul ist dann von vornherein nicht möglich. Netop stellt entsprechende Seriennummern auf Anfrage kostenlos bereit.

Mit der Version 11 neu hinzugekommen ist die Möglichkeit, sich über den Security Server auch gegen einen RADIUS-Server zu authentifizieren. Dadurch sind auch Multi-Faktor-Authentifizierungen beispielsweise mit Einmalpasswort oder speziellem Hardware-Token denkbar.

Revisionssicher dank Aufzeichnung

Geht es darum, Netop unternehmensübergreifend einzusetzen – etwa als Supportlösung bei Kunden oder um selbst von einem Produktlieferanten Unterstützung zu erhalten –, ist es für eine Revision wichtig nachvollziehen zu können, was in den Fernsteuersitzungen passiert ist. Hierzu ist Netop mit umfassenden Optionen zur Aufzeichnung von Sitzungen ausgestattet. Sowohl auf Gast- als auch auf Hostseite sind Aufzeichnungen möglich, auch gleichzeitig. Die Pflicht zur Aufzeichnung lässt sich fest vorgeben und es ist sogar einstellbar, dass eine Sitzung getrennt wird, wenn die Aufzeichnung nicht funktioniert.

Die Aufzeichnungen erfolgen in einem Netop-eigenen Format, wobei darauf zu achten ist, dass eine Wiedergabe nur über einen Gast erfolgen kann. Hintergrund ist, dass Netop die hostseitige Installation möglichst schlank halten möchte. Während auf Gastseite getätigte Aufzeichnungen übersichtlich in einem Fenster aufgelistet werden, gestaltet sich der Umgang mit Hostaufnahmen etwas umständlicher. Diese Dateien müssen zum Abspielen erst bei einem Gast in die Verzeichnisstruktur kopiert werden, wo auch dieser seine Filme ablegt. Im Test zeigte sich, dass dies gar nicht so

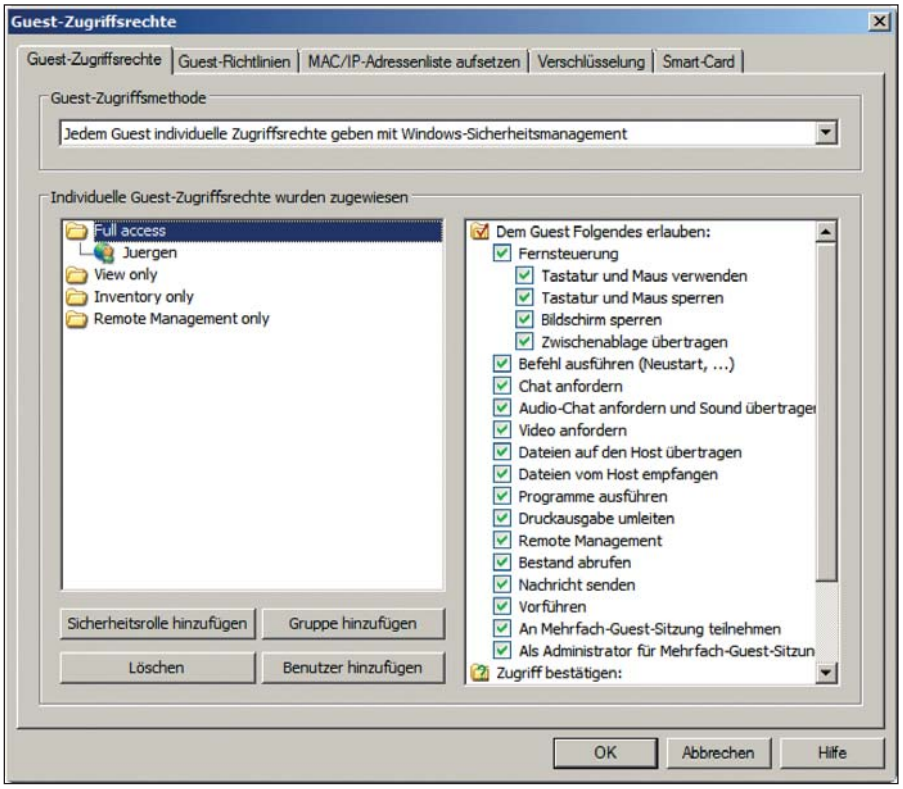


Bild 4: Neben lokal einzustellenden Zugriffsmethoden ermöglicht der Security Server eine zentrale Verwaltung

einfach ist. Während der Speicherort auf Hostseite frei vorgegeben werden kann, ist er beim Gast fest definiert und wird nirgendwo angezeigt. Wir mussten daher selbst auf die Suche gehen. Besser wäre es, der Administrator könnte über einen Gast die Verzeichnisstruktur durchsuchen und entsprechende Filmdateien öffnen.

Verbindung über Umwege

Sobald ein Administrator seine Server über das Internet administrieren möchte und dazu keinen VPN-Tunnel nutzen kann, übernimmt Netop die sichere Kommunikation in Verbindung mit zusätzlichen Modulen. Die grundlegende Funktion hierfür heißt WebConnect und ist in zwei Ausprägungen verfügbar. So bietet Netop das Produkt Netop on Demand an. Dazu betreibt der Anbieter eine Serverplattform im Internet, die die Verbindung zwischen Gast und Host abwickelt. Sowohl Gast als auch Host verbinden sich dann zu dem Connection Manager, auf dem für jeden Kunden ein kennwortgeschütztes Konto unterhalten wird. Ein Gast sieht nun alle über das Konto angemeldete Hosts und kann sich zu diesen verbinden. Netop on Demand ist dabei so programmiert, dass es über vorhandene Firewalls hinweg funktioniert.

Da sich wie erwähnt einige Unternehmen nicht auf fremdadministrierte Server verlassen wollen, gibt es die gleiche Funktionalität auch unter der Bezeichnung WebConnect als Produkt, bei dem der Administrator eine eigene Verbindungsplattform betreibt. Diese besteht aus mindestens zwei Servern, dem Connection Manager und dem Connection Server. Es ist zwar möglich, beide Komponenten auf einem System zu installieren, der Hersteller rät jedoch ausdrücklich davon ab. Der Connection Manager dient als Anmeldeserver, der Connection Server routet dann den Verkehr zwischen Gast und Host. Voraussetzung ist, dass der Connection Manager aus dem Internet erreichbar ist, damit sich Gast und Host anmelden können. Für das Datenmanagement benötigt der Connection Manager eine Datenbank auf einem MS SQL Server. Eine zusätzliche Kombination mit einem Security Server ist möglich.

Gast und Host sind für die Nutzung von WebConnect sowie Netop on Demand einfach zu konfigurieren. Innerhalb des Setup-Assistenten ist nur die Frage danach zu bejahen, schon wird das notwendige Kommunikationsprofil hinzugefügt. Falls erforderlich, ist es jederzeit möglich, auch wechselweise Verbindungen via WebCon-

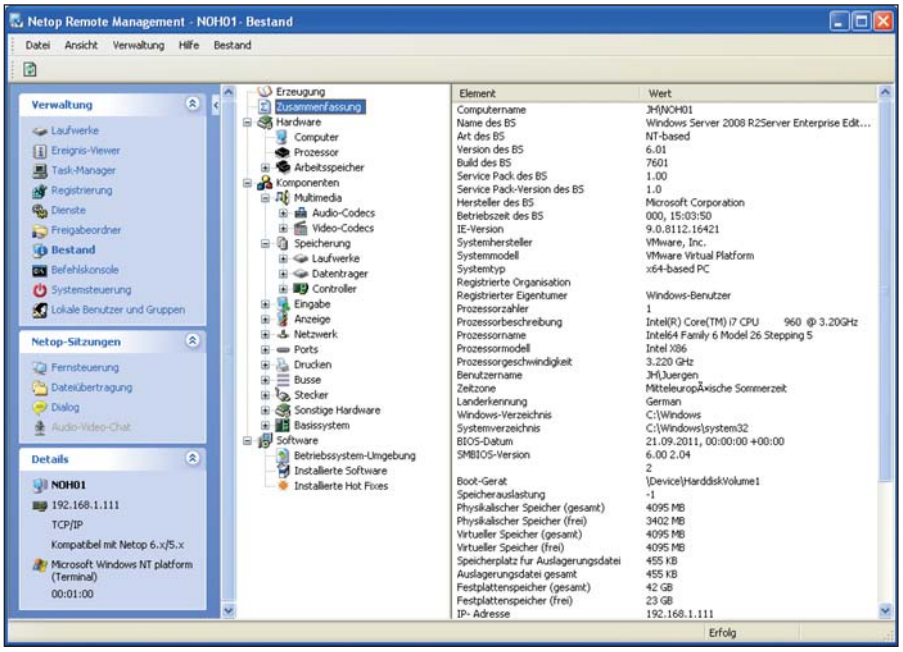


Bild 5: Das Remote Management beinhaltet den direkten Zugriff auf diverse Verwaltungsoptionen. Dies hilft vor allem beim Serverbetrieb, aufwändigere Fernsteuersitzungen auf ein Minimum zu beschränken.

nect sowie ins interne Netzwerk aufzubauen. Beim Test beschränkten wir uns darauf, eine Verbindung über die von Netop bereitgestellten Server aufzubauen. Dies klappte auf Anhieb und erlaubte auch eine flüssige Steuerung. Sofern es in großen Netzen oder auch über das Internet Probleme mit der Namensauflösung gibt, bietet sich der Netop Name Server an. Hierbei handelt es sich um einen erweiterten Host, der Netop-Module über segmentierte Netze verbinden kann, indem er die Netop-Namen in IP-Adressen auflöst. Ein weiteres Modul ist das Netop Gateway, welches das Routing des Netop-Datenverkehrs zwischen verschiedenen, an sich inkompatiblen Kommunikationsgeräten übernimmt. Ein Beispiel dafür ist eine Portübersetzung, wenn im Kommunikationsweg unterschiedliche Ports zu verwenden sind. Ein anderes Beispiel ist der Einsatz von Netop in einer Terminalserver-Umgebung. Sofern Gast und Host gemeinsam auf einem Terminalserver in unterschiedlichen Sitzungen laufen, ist eine direkte Kommunikation möglich. Um aber beispielsweise von einem Gast in einer TS-Sitzung auf einen externen Host zuzugreifen, muss die Kommunikation über solch ein Gateway stattfinden.

Fazit

Im Test erwies sich Netop als äußerst leistungsfähiges Werkzeug mit einem riesigen Funktionsumfang. Schnell zeigte sich aber auch, dass das über viele Jahre hinweg gewachsene Tool etwas unübersichtlich geworden ist, weil immer wieder neue Funktionen integriert wurden. Auch legt Netop mehr Wert auf Funktionalität und Performance als auf schicke Optik. So machen die verwendeten Icons einen etwas altbackenen Eindruck. Dafür bekommt der Anwender aber schlanke Komponenten, die zuverlässig und schnell reagieren, weil beispielsweise auf eine Ressourcen-verschlingende Javaprogrammierung sowie Browsernutzung verzichtet wurde.

Netop erwies sich im Test als ideal für die Serveradministration. Gut gefallen hat uns, dass sich viele Server-typische Pflegearbeiten bereits über das schlanke Remote Management erledigen lassen, sodass nicht in jedem Fall eine Fernsitzung erforderlich ist. Hervorzuheben ist auch der sehr breite Host-Gast-Support, mit dem wohl kein anderes Fernsteuertool mithalten kann. Zusätzliche Funktionen wie Netop on Demand und WebConnect ermöglichen einen problemlosen Zugriff auch über das Internet hinweg. Bei WebConnect stehen zudem alle Komponenten unter eigener Administration, sodass hier ein Sicherheitsrisiko durch Inanspruchnahme externer Dienstleistungen ausgeschlossen werden kann.

Im Test zeigte sich aber auch, dass eine umfassende Einarbeitung erforderlich ist, vor allem unter dem Aspekt, dass das Tool vielfach für spezielle Sicherheitsanforderungen beschafft wird und dann natürlich auch korrekt konfiguriert werden muss, damit keine unbewussten Sicherheitslücken entstehen. Wer letztendlich auf der Suche nach einer möglichst sicheren Fernadministration von Servern ist, sollte sich auf jeden Fall Netop genauer ansehen. *(dr)*

Produkt

Fernsteuerung von Servern und Desktops.

Hersteller

Netop
www.netop.com

Preis

Netop wird anhand der Host- und Gastinstallationen lizenziert. Es gibt verschiedene Lizenzmodelle, sowohl benutzer- als auch maschinenbezogen. Ein Host mit fünf Gastlizenzen kostet 170 Euro. Ab 100 Lizenzen kostet im Netop Open Licence Programm (NOLP) eine Gastlizenz für einen Server 25 Euro, für größere Mengen gibt es entsprechende Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Fernsteuerung	8
Flexibilität und Skalierbarkeit	9
Sicherheitsfunktionen	9
Verbindungsmöglichkeiten	8
Administrationsaufwand	5

Dieses Produkt eignet sich

optimal für Unternehmen, die bei der Fernsteuerung von Systemen hohe Sicherheitsanforderungen haben oder in einer inhomogenen Serverlandschaft unterschiedliche Betriebssysteme fernwarten möchten.

bedingt in Umgebungen, in denen gelegentlich Systeme ferngesteuert werden sollen und die Sicherheitsanforderungen nicht besonders hoch sind. Hier gibt es Lösungen, die mit weniger Aufwand realisierbar sind.

nicht für Unternehmen, die keinen Bedarf für eine Fernwartung haben oder denen die vorhandenen Bordmittel wie RDP bei Windows ausreichen.

Netop Remote Control 11

NEU!

HP MicroServer

Die günstigsten Dedicated Marken-Server der Welt

ECO Certification

webtropia.com

AKTION
Jetzt 99,99 € Setup Gebühr sparen
Gutscheincode:
IA-7T46E10s12-626

NEU

Ab 17,99 € im Monat erhalten Sie Ihren eigenen Dedicated Root-Server

	HP MicroServer S	HP MicroServer M	HP MicroServer L
Eigener Dedicated Server	✔	✔	✔
CPU	AMD N40L	AMD N40L	AMD N40L
Leistung	2 x 1,5 GHz	2 x 1,5 GHz	2 x 1,5 GHz
RAM	4 GB DDR3	8 GB DDR3	16 GB DDR3
Festplatten (7.200 rpm)	1 x 160 GB	2 x 500 GB	2 x 3.000 GB
Festplatten-Ausbau bis zu	4 x 3.000 GB	4 x 3.000 GB	4 x 3.000 GB
Optionaler Raid-Controller	✔	✔	✔
KVM over IP optional	✔	✔	✔
Anbindung	100 MBit Flatrate	100 MBit Flatrate	100 MBit Flatrate
IPv4 Adresse inkl.	✔	✔	✔
IPv6 Subnetz (/64) inkl.	✔	✔	✔
Betriebssysteme	Debian 6.0, Ubuntu 12.04 NEU	CentOS 6, openSUSE 12.1, FreeBSD 8.1, Windows 2008 R2 (19,99 € Aufpreis im Monat)	
Extras	50 GB Backup-Speicher, Monitoring, Reset- und Rescue-System		
Monatsgrundgebühr	**17,99 €**	**29,99 €**	**49,99 €**
Vertragslaufzeit	1 Monat	1 Monat	1 Monat
Einrichtungsgebühr	~~99,99 €~~	~~99,99 €~~	~~99,99 €~~

Jetzt informieren und bestellen Tel.: 0211 / 545 957 - 300 www.webtropia.com

powered by hp

Microsoft CERTIFIED SPLA MEMBER

Parallels PLATINUM PARTNER

IPv6 ready

Im Kurztest: Digittrade HS256S

Sicher im Kasten

von Thomas Gronenwald

Am Flughafen gestohlen oder in der Bahn liegengelassen – es ist äußerst ärgerlich, wenn das Notebook oder die externe Festplatte verschwindet. Eine wirkungsvolle Verschlüsselung tut deshalb not. Im Portfolio des Online-Händlers DIGITTRADE findet sich mit der HS256S eine angeblich hochsichere SSD-Festplatte mit integrierter Hardware-Codierung. IT-Administrator hat sich angesehen, ob der Flash-Speicher seine Daten wirklich für sich behält und ob auch unerfahrene Anwender gut damit arbeiten können.

Der Verlust mobiler Hardware wiegt zwar schwer, macht meist aber nur einen kleinen Teil des eigentlichen Gesamtschadens aus. Denn mit dem einhergehenden Datenverlust drohen zumeist ein erheblicher Reputationsschaden und neue Gefahren für das Unternehmen. Deshalb gehört es zum Pflichtprogramm der IT, den Zugriff auf vertrauliche Unternehmensdaten und die dazugehörige Hardware zu schützen und entsprechend zu verschlüsseln. DIGITTRADE hat hierzu eine portable Festplatte für den Profi-Einsatz mit integrierter Hardwareverschlüsselung im Angebot. Die High Security Festplatte HS256S wurde laut Hersteller in Übereinstimmung mit den neuesten Anforderungen des BSI an mobile Speichermedien entwickelt und soll jegliche Daten umfangreich und sicher vor unbefugten Zugriffen schützen.

Dreifach gesichert hält besser

Die Full-Disk-Verschlüsselungsplatte arbeitet mit drei wesentlichen Sicherheitsmechanismen: Verschlüsselung, Zugriffskontrolle / Zwei-Faktor-Authentifizierung sowie externer Verwaltung des kryptografischen Schlüssels. Sensible Daten werden auf der mit einer SSD ausgestatteten HS256S über ein integriertes Hardwareverschlüsselungsmodul nach AES mit 256 Bit im CBC-Modus gespeichert. Die Verschlüsselung erfolgt hierbei in Echtzeit. Nicht zuletzt sorgt die Hardware-seitige Verschlüsselung dafür, dass sich der Datenspeicher unabhängig vom Betriebssystem einsetzen lässt.

Darüber hinaus arbeitet die Festplatte mit einer Zwei-Faktor-Authentifizierung mittels Smartcard und einer mindestens achtstelligen PIN. Die Wahl einer kürzeren PIN ist aus Sicherheitsgründen nicht möglich. Diese Mechanismen gewährleisten, dass nur autorisierte Nutzer Zugang zu den Daten erhalten. Fehlt nur eines dieser Authentifizierungsmerkmale, ist kein Zugriff auf die Daten möglich. Der kryptografische Schlüssel befindet sich verschlüsselt auf der beiliegenden Smartcard und nicht auf der Festplatte selbst. Er wird nach korrekter PIN-Eingabe an das Verschlüsselungsmodul des Flash-Speichers übertragen.

Komplettpaket

Das Herzstück der in unserem Test genutzten HS256S bildete eine SSD-Festplatte von Samsung im 2,5 Zoll-Format mit 240 GByte Speicherplatz. Außerdem existieren Varianten mit 120 und 512 GByte. Darüber hinaus sind Modelle mit handelsüblichen Festplatten in den Größen 500 und 640 GByte sowie 1 TByte erhältlich. Nutzer der Flash-Technik sollen neben der hohen Lese- und Schreibgeschwindigkeit zusätzlich von einer hohen Stoßunempfindlichkeit profitieren. Serienmäßig im Lieferumfang enthalten sind zudem zwei Java-basierte Smartcards. Die Oberthur Cosmo 64 v5.4 ist eine nach FIPS 140-2 Level 3 zertifizierte Smartcard und ermöglicht das Erstellen, Kopieren, Ändern und Zerstören des kryptografischen Schlüssels. Die Schlüsselverwaltung auf der Smartcard erfolgt durch ein spezielles Applet.

Das Gehäuse der HS256S wirkt hochwertig, wartet mit einem beleuchteten Touchpad auf und fasst sich mit einem leicht gummierten Kunststoff angenehm an. Neben einem Mini-USB-Anschluss verfügt die Festplatte über einen FireWire 400/80-Port. Zum sicheren Transport eignet sich das beiliegende Hardcase-Etui. Im Paket befinden sich außerdem das Benutzerhandbuch und eine Treiber-CD.

Darüber hinaus spendiert der Hersteller eine Version der Backuplösung Acronis TrueImage OEM Quick Backup.

Leichte Inbetriebnahme

Die Inbetriebnahme der Festplatte gestaltete sich einfach. Die Verbindung zum Computer wird bei USB 1.1 mit dem beiliegenden USB-Y-Kabel hergestellt. Hierbei ist darauf zu achten, dass zuerst die A- und B-Stecker an den Computer angeschlossen werden und dann das Mini-USB-Kabel an die Festplatte. So ist gewährleistet, dass der Einschaltstrom beim USB 1.1-Anschluss zur Verfügung steht. Bei USB 2.0 hingegen genügt ein normales Mini-USB-Kabel. Ein zusätzliches Netzteil ist nicht notwendig und erleichtert den Transport ungemein.

Sobald die Festplatte ordnungsgemäß mit dem Computer verbunden ist, leuchten zunächst die Status-LEDs "Active", "Status" und "Error" kurz hintereinander auf. Der Flash-Speicher ist danach betriebsbereit, vom Nutzer jedoch noch durch die Eingabe der PIN und die mitgelieferte Smartcard zu entsperren. Die Smartcard wird nach acht Fehlversuchen automatisch für immer gesperrt und ist fortan unbrauchbar – alle Daten auf der Smartcard werden unwiderruflich gelöscht. Zur Authentifizierung schoben wir die Smartcard in den Smartcard-Reader ein, der fest mit der Platte verbaut ist. Mit Einlegen einer gültigen Smartcard leuchtete die Status-LED noch einmal auf. Anschließend nahmen wir auf dem beleuchteten Touchpad die Eingabe der PIN vor.

Advanced Encryption Standard

Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptosystem und wurde vom National Institute of Standards and Technology (NIST) als Standard definiert. Er gilt weltweit als praktisch berechnungssicher und ist in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe freigegeben. Im CBC-Modus wird jeder Sektor mit einem anderen AES-Schlüssel verschlüsselt. Darüber hinaus finden Informationen aus den bereits verschlüsselten Sektoren auch für jeden neuen verschlüsselten Sektor Verwendung. Zugleich werden zusätzlich zu den gespeicherten Daten sogar temporäre Dateien und Bereiche verschlüsselt – ein wesentlicher Unterschied zu anderen Verschlüsselungsvarianten.

Bei der Erstinbetriebnahme ist ein werkseitig voreingestellter PIN-Code einzugeben, den wir im Handbuch fanden. Um ein Maximum an Sicherheit zu erreichen, war es jedoch zwingend erforderlich, die Smartcard-PIN direkt im Anschluss zu ändern. Ebenso empfiehlt es sich, für die unterschiedlichen Smartcards auch unterschiedliche PINs zu nutzen. Nach erfolgreicher Authentifizierung erschien die Festplatte dann als Wechseldatenträger im Arbeitsplatz und die Smartcard konnte entfernt werden. Bei einer falschen Eingabe der PIN schlug die Authentifizierung fehl und es leuchtete die Error-LED auf. Mit Drücken der ESC-Taste konnten wir die Eingabe wiederholen.

Komfortable PIN-Verwaltung

Um die PIN der Smartcard zu ändern, schoben wir diese in den Reader der Festplatte. Dann starteten wir mittels der Taste "Change-PIN", gefolgt von der Taste "1", eine neue PIN-Vergabe. Nach Eingabe der aktuellen achtstelligen PIN tippten wir eine neue Zahlenfolge ein. Die Festplatte akzeptiert wie erwähnt nur mindestens achtstellige PINs und schiebt dem Sicherheitsrisiko einer zu kurzen PIN wirkungsvoll einen Riegel vor.

Schließlich veränderten wir noch die Administrator-PIN. Diese dient dazu, neue Smartcards für die Festplatte zu initialisieren. In der Regel ist dies nur notwendig, wenn beide Smartcards verloren oder defekt sind. Wichtig hierbei ist, die Änderung der Administrator-PIN vor der ersten Benutzung durchzuführen, also bevor die ersten Daten auf der Festplatte ihren Platz finden. Denn die Initialisierung neuer Smartcards bewirkt die Formatierung der Festplatte und alle darauf befindlichen Daten werden gelöscht.

Um die Administrator-PIN zu ändern, führten wir erneut die Smartcard in den Reader ein. Über die Taste "Change-PIN", gefolgt von einer "0", ließ sich dann die neue Admin-PIN vergeben. Auch hier war zunächst die Eingabe der bestehenden PIN erforderlich. Die werkseitig voreingestellte Administrator-PIN entnahmen wir ebenso dem Handbuch. Im Anschluss kann die Festplatte nach eigenen Wünschen formatiert und genutzt werden.

Aus Sicherheitsgründen empfiehlt es sich, die beiden Smartcards getrennt voneinander aufzubewahren. Zudem sollte die Administrator-PIN an einem geschützten Ort aufbewahrt werden, denn ohne diese Zeichenfolge wird die Festplatte bei Verlust oder Defekt beider Smartcards unbrauchbar.

Fazit

Die DIGITTRADE HS256S SSD bietet bei Einhaltung der empfohlenen Schritte ein hohes Maß an Sicherheit. Der Preis dieser Festplatten wirkt zu Beginn abschreckend, wiegt gegenüber einem möglichen Verlust der Daten jedoch gering. Durch die Zwei-Faktor-Authentifizierung sowie die integrierte Hardware-Verschlüsselung, gepaart mit einer leistungsstarken Solid State Disk, sind keine merklichen Verzögerungen bei der Arbeit bemerkbar. Wie immer sollte trotz der zuverlässigen SSD nicht auf ein regelmäßiges Backup der Daten auf ein zweites, idealerweise ebenfalls verschlüsseltes Medium verzichtet werden. *(ln)*

Digittrade HS256S

Produkt
Externe SSD-Platte mit integrierter Hardware-Verschlüsselung und Zwei-Faktor-Authentifizierung.

Hersteller
DIGITTRADE
www.digittrade.de

Preis
Je nach Speichertechnologie und Kapazität zwischen 500 und 1.260 Euro.

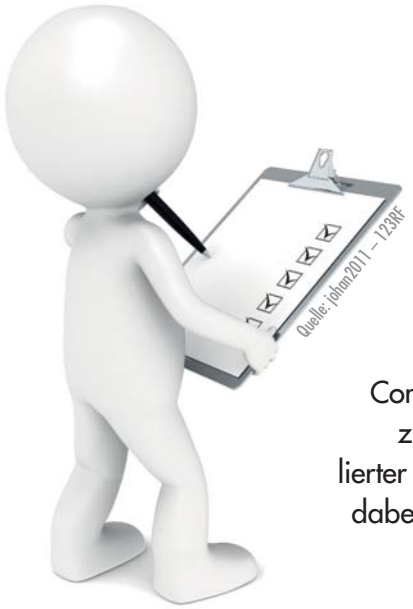
Technische Daten
www.it-administrator.de/downloads/datenblaetter

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

Lieferumfang	8
Inbetriebnahme	6
Administration	8
Verarbeitung	8
Sicherheit	10

Im Test: OCS Inventory NG

Kostenlose Bestandsaufnahme



von Sandro Lucifora

Netzwerke wachsen mit ihren Anforderungen. Zusätzliche Arbeitsplätze erweitern die Struktur, und durch den Austausch von defekten oder veralteten Computern fällt es immer schwerer, sämtliche installierte Hard- und Software im Auge zu behalten. Vom Administrator wird aber erwartet, dass er den Zustand installierter Geräte kennt. Statt der berüchtigten Excel-Tabelle sollen Inventarisierungslösungen dabei helfen, den Überblick zu bewahren. Ob das auch mit dem unter Open Source-Lizenz veröffentlichten und somit kostenlosen Tool OCS Inventory NG gelingt, hat IT-Administrator in einem Praxistest herausgefunden.

OCS Inventory NG (NG steht für Next Generation) ist ein freies Administratoren-Tool zur Inventarisierung von Hard- und Software im Netzwerk. Zusätzlich enthält das Paket eine Softwareverteilung für Windows, Mac OS X und Unix-artige Systeme. Um die Informationen über die Ausstattung von vernetzten Rechnern zu sammeln, setzt das System ein Client-Programm ein, den OCS Inventory Agent. Dieser ist für Windows, MAC OS X und Unix/Linux verfügbar. Zusätzlich kann OCS dazu verwendet werden, das Inventar über ein Webinterface zu visualisieren.

Der OCS-Server stellt die Datenbank- und Kommunikationsdienste bereit. Der Datenaustausch zwischen dem Agent und Server erfolgt per HTTP/HTTPS. Über dieses Protokoll werden die vom Agenten gesammelten Daten als ZLIB-komprimiertes XML übertragen. Der Kommunikationsserver ist in PERL geschrieben. Derzeit lässt sich nur MySQL als Datenbankserver nutzen.

Aufgrund der einfachen Programmstruktur und der Verwendung von mod_perl kann auch bei mehreren tausend Clientrechnern ein einfacher Computer als Server fungieren, wobei noch ausreichende Geschwindigkeit vorhanden ist. Das Installationspaket ist für Unix/Linux oder für Windows erhältlich. Letzteres basiert auf XAMPP und wird für Umgebungen mit bis zu 1.500 Clients empfohlen. Wer mehr Netzwerkgeräte inventarisieren will, sollte daher die Linux-Variante bevorzugen.

Ressourcenschonende Installation als VM

Alternativ zur Hardware bietet der Entwickler einen OC Inventory NG-Server als virtuelle Maschine (VM) für VMware an. Diese ist als freier Download erhältlich; der Nutzer kann zwischen Debian Squeeze, Ubuntu Linux oder CentOS wählen. Für diesen Test haben wir als Basis eine VM unter Ubuntu Linux 11 64 Bit gewählt. Sie lässt sich problemlos mit dem kostenlosen VMware Player auf jedem Server betreiben und benötigt mit 512 MByte Speicher, einem Prozessor und einer 8 GByte Festplatte kaum Ressourcen.

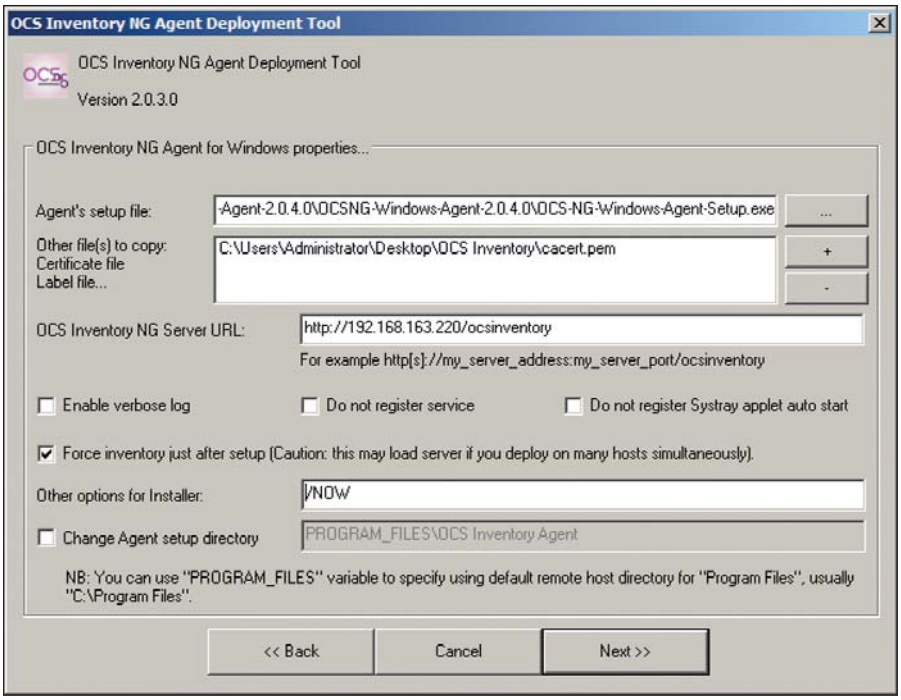


Bild 1: Das OCS-eigene Verteilungstool installiert die Agenten mit Hilfe von PsExec auf den Clients

Nach dem Download und Entpacken des *tar.gz* banden wir die VM in den VMware Player ein. Der Login erfolgte über den User "root" mit dem Standardpasswort "ocs". Dieses haben wir als Erstes über das Kommando *passwd* geändert. Als Nächstes mussten wir die IP an unser bestehendes Netzwerk anpassen. Da der OCS-Server mit der festen IP 10.10.10.10 ausgeliefert wird, unser Testlabor jedoch über einen DHCP-Server verfügt, passten wir die Datei */etc/network/interfaces* entsprechend an. Des Weiteren reservierten wir in unserem DHCP-Server eine feste IP für den Inventory-Server, sodass dieser immer dieselbe IP zugewiesen bekam. Die dafür notwendige MAC-Adresse der VM ist in den erweiterten Einstellungen der virtuellen Netzwerkkarte im VMware Player abzulesen. Nach dem Neustart des Interfaces mit *sudo ifdown eth0*, gefolgt von *sudo ifup eth0*, bezog die VM die zugewiesene IP. Über den Browser eines beliebigen Netzwerk-PCs konnten wir dann den OCS Management-Server aufrufen.

Die nächste Anpassung war am SAMBA-Server nötig. Hier mussten wir in der Datei *samba.conf* lediglich den Eintrag der Workgroup auf unsere Domäne anpassen. Nachdem wir sichergestellt hatten, dass der Servername "ocsinventory-ng" durch den internen DNS aufgelöst wird, war der letzte Schritt zur Konfiguration das Erstellen eines neuen SSL-Zertifikates. Dieses wurde notwendig, da der Management-Server und die Agenten über SSL kommunizieren und das bereits auf dem Server generierte Zertifikat abgelaufen war. Um diesen Prozess zu vereinfachen, liefert der Entwickler das Skript *apache_generate_cert.sh* mit. Dieses führten wir aus, beantworteten die Fragen nach dem Aussteller und ließen das neue Zertifikat durch das Skript für Apache einbinden.

OCS Inventory NG Agent unterstützt Microsoft Windows ab Windows 95 beziehungsweise NT 4.0 bis Windows 7 und Server 2008, diverse Linux-Distributionen (CentOS, Debian, Fedora Core, Gentoo, Knoppix, Mandriva, RedHat, Slackware, SuSE, Trustix, Ubuntu), zahlreiche BSDs (OpenBSD, NetBSD, FreeBSD) sowie Solaris, AIX und Mac OS X.

Systemvoraussetzungen

Agentenverteilung nur für Windows

Damit der OCS Inventory Management-Server die Daten eines Netzwerk-Rechners erhalten kann, müssen die entsprechenden Agenten auf den PCs installiert sein. Schon bei kleineren Netzwerken ist es sinnvoll, dass Administratoren die Agenten über eine Softwareverteilung auf die Computer bringen. Hierzu bietet sich zum einen die Verteilung mit Hilfe des Active Directory an. Dazu hat das OCS-Team ein entsprechendes Skript veröffentlicht.

Optional steht ein eigenes Verteilungs-Tool von OCS zum Download bereit. Wir haben uns auch diesen Weg angeschaut und die Software in der Version 2.0.3 auf unserem Netzwerk-Server installiert. Für das Ausrollen des Windows-Agenten benötigten wir zusätzlich noch das PsExec-Tool aus dem PsTool-Paket von SysInternals. Nach dem Download teilten wir dem Verteilungs-Tool die Pfade der Hilfsprogramme mit, bevor wir mit der Verteilung begonnen haben.

Die Verteilung auf Linux-Rechnern setzt zudem den bekannten SSH-Client Putty sowie PuttySC voraus. Obwohl der Button für die Linux-Softwareverteilung aktiv war, ist diese Option derzeit noch nicht implementiert. Eine Softwareverteilung für den Mac-Agenten fehlt vollständig.

Die Verteilung unter Windows gestaltet sich recht unkompliziert. Nach dem Start der Software und dem Eintragen des Pfades zur *psexec.exe* werden entweder alle Windows-Hosts eines IP-Bereichs oder zuvor ausgewählte Hosts mit dem Agenten bestückt. Im nächsten Schritt gaben wir den Pfad zur Agent Setup-Datei an und fügten dem Installationsprozess das zuvor erstellte SSL-Zertifikat für unseren Server hinzu. Dieses findet auch auf dem Client seinen Platz, wodurch der Agent und der Management-Server über SSL kommunizieren können.

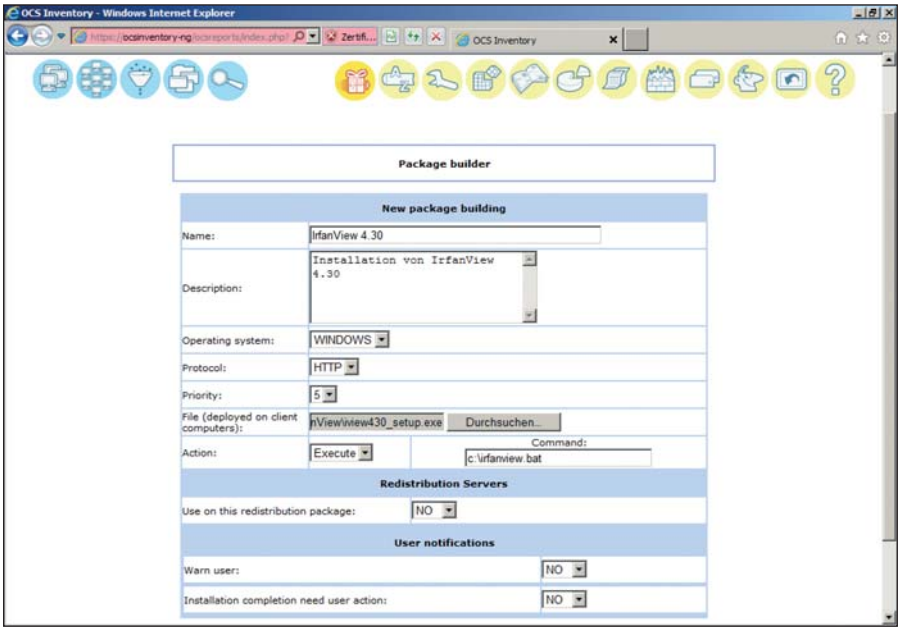


Bild 3: Zur Softwareverteilung mit OCS wird zunächst das Installationspaket auf dem Server erstellt

Handarbeit beim Offline-Rollout

Aus den möglichen Optionen haben wir noch "Force inventory just after setup" ausgewählt, um so einen sofortigen Austausch an Informationen zwischen Agent und Server anzustoßen. Leider hat dies im Test unter Windows 7 nicht funktioniert. Der Agent wurde erst nach einem Neustart des Arbeitsplatzes erkannt und meldete ab dann alle Informationen an den Management-Server. Um die Software zu verteilen, fragt das Tool übrigens nach den Login-Daten des globalen Administrators.

Der Nachteil dieser Verteilungs-Methode ist, dass die Arbeitsplatz-Rechner in dem Augenblick im Netzwerk online sein müssen, wenn die Verteilung erfolgt. Vor allem per VPN angebundene Rechner und Notebooks sind darüber schwer bis gar nicht erreichbar. In diesem Fall kann die Verteilung über ein Login-Skript oder per GPO im Active Directory erfolgen. Das Tool *OCSLogon.exe* wurde für diesen Einsatz entwickelt. Wird die EXE-Datei durch das Login-Skript aufgerufen, prüft sie, ob bereits ein Agent installiert ist, und installiert diesen bei Bedarf.

Sollte ein Rechner per Verteilung nicht erreichbar sein, so lässt sich der Agent natürlich auch manuell installieren. Dies muss mit dem Client für Linux und Mac grundsätzlich geschehen, da für diese beiden Betriebssysteme wie bereits erwähnt derzeit keine automatische Softwareverteilung zur Verfügung gestellt wird. Der Einsatz von Login-Skript und GPO über das AD kommen aufgrund der anderen Architektur nicht in Frage.

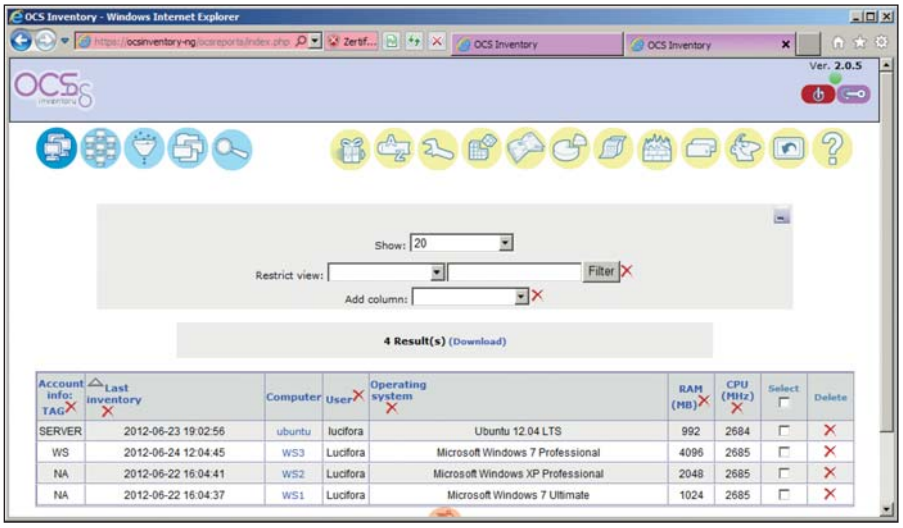


Bild 2: In der über den Browser anzusteuernden Übersicht sind die Computer mitsamt dem gemeldeten Inventar zu sehen

Da ein Netzwerk nicht nur aus Geräten mit Windows, Linux oder Mac OS X besteht, stellt sich die Frage, wie sich die Netzwerkperipherie wie Drucker, Switches oder Router in das System integrieren und auflisten lässt. Hierzu ist mit "IpDiscover" ein Tool implementiert, das zwar unabhängig arbeitet, sich aber perfekt in die OCS-Struktur einbindet. Die Funktionsweise ist etwas kompliziert, aber dennoch praktikabel. Die Informations-Ermittlung von Peripheriegeräten wird zudem über eine zusätzliche SNMP-Abfrage noch detaillierter.

Inventarliste über den Browser

Ist der Agent einmal gestartet, meldet er dem Server die Ausstattung des Arbeitsplatzes. In unserem Fall haben wir den Informationslieferanten als Service installiert, sodass er auch ohne Anmeldung eines Users funktionierte. Dadurch verbindet sich das Tool automatisch nach einer zufälligen Zeit mit dem Server. Diese Zufallsverteilung ist von den Entwicklern gewollt, damit nicht alle Clients zur selben Zeit den Server zu sehr auslasten.

Die Kernaufgabe von OCS Inventory ist die Darstellung der Hard- und Software innerhalb der Netzwerk-Infrastruktur. Im Test haben wir mehrere Windows-PCs mit unterschiedlicher Ausstattung als auch einen Linux-Server unter Ubuntu 12.04 und diverse Peripherie inventarisieren lassen.

Der OCS Management-Server lässt sich über den Browser aufrufen. Im Test funktionierte dies mit aktuellen Versionen des Internet Exporer, Firefox und Chrome ohne Probleme. Nach der Eingabe der URL oder der IP des Servers, gefolgt vom Verzeichnis "ocsreports" und dem Login, erhielten wir eine Übersicht der inventarisierten Geräte. Ein Klick auf den Namen öffnete eine neue Seite, über die wir an alle gespeicherten Detailinformationen kamen.

Dynamische Gruppen sorgen für Übersicht

Unter den generellen Informationen des ausgewählten Gerätes zeigte sich eine Liste von über 20 Kategorien. Über die administrativen Daten konnten wir individuelle Angaben für ein Gerät hinterlegen, etwa das Installationsdatum und Angaben zum Standort und zur Garantie.

Die mitgelieferte Suchfunktion ist sehr umfangreich. So lassen sich Geräte etwa nach Eigenschaften suchen, wie dem BIOS-Hersteller, der Grafikkarte, dem Monitorhersteller oder dem Betriebssystem. Hierzu sind auch Vergleichsoperatoren wie gleich, größer als, kleiner als, unterschiedlich, zwischen und außerhalb in Kombination erlaubt. Das erleichtert dem Administrator ungemein das gezielte Auffinden von Geräten mit bestimmten Ausstattungen.

Als Ergänzung zur klassischen statischen Gruppe mit fest zugewiesenen Geräten ist die Funktion der dynamischen Gruppe eine interessante Option. Sie besteht aus Computern, die zuvor festgelegten Kriterien entsprechen. Alle Computer mit diesen Kriterien werden in der dynamischen Computer-Gruppe eingebunden. Zum Beispiel haben wir einer dynamischen Gruppe das Kriterium "Mozilla Firefox" und "Windows 7" gegeben. Dadurch hatten wir immer alle Computer in einer Gruppe, die diese Kriterien erfüllten. Ein Rechner, der diesen Browser nicht installiert hatte, wurde automatisch der dynamischen Gruppe hinzugefügt, nachdem wir das Firefox-Setup ausgeführt hatten. Umgekehrt wurde ein anderer Computer aus der Gruppe entfernt, als wir Firefox deinstallierten.

Softwareverteilung inklusive

OCS Inventory NG kann nicht nur Daten sammeln, sondern auch Software verteilen. Neben der gezielten Installation auf einzelnen Computern lassen sich Installationspakete auf Gruppen – statisch und dynamisch – verteilen. In der Praxis lassen sich so alle Computer gruppieren und updaten, die die veraltete Version einer Software nutzen. So verteilten wir etwa an eine dynamische Gruppe mit Filter auf eine veraltete Adobe Reader-Version automatisch ein Update-Paket der Software.

Praktische Installationsketten

In einem weiteren Test schufen wir mit dieser Funktion ganze Paket-Abhängigkeiten. So erstellten wir eine dynamische Gruppe von Computern, die kein Photoshop und kein IrfanView installiert hatten. Dieser Gruppe ordneten wir das Paket "IrfanView430" zu. Eine weitere dynamische Gruppe enthielt

alle Computer mit bereits installiertem IrfanView. Dieser Gruppe wiederum wiesen wir ein Softwarepaket mit den IrfanView-Plug-Ins zu. Wurde einem Computer, der zuvor in der Gruppe ohne IrfanView war, nun die Software aufgespielt, wechselte dieser nach der Inventarisierung automatisch in die Gruppe der Rechner mit dem installierten Bildbetrachter. Dadurch kam dieser Computer wiederum in den Genuss der Plug-Ins.

Auf diese Weise lassen sich ganze Installationsketten erstellen, wenn die Installation einer Software auf dem Vorhandensein anderer Pakete beruht – wie zum Beispiel Libraries, Microsoft MFC oder ähnlichen Paketen. Sind die dynamischen Gruppen und Softwarepakete einmal angelegt, erhalten frisch und ausschließlich mit ihrem Betriebssystem installierte Rechner auf diese Weise automatisch eine Komplettinstallation nach Firmenrichtlinien. Es lassen sich so sogar Windows Service Packs updaten, ohne dass der Administrator stunden- oder tagelang davor sitzen muss.

Produkt

Programm zur Erfassung und Inventarisierung von Rechnern und Komponenten im Netzwerk.

Hersteller

OCS Inventory Team
www.ocsinventory-ng.org

Preis

Kostenfrei, da Open Source.

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

Einrichtung	5
Unterstützte Betriebssysteme	7
Benachrichtigungssystem	3
Skalierbarkeit	6
Hardwareanforderung	8

Dieses Produkt eignet sich

optimal für die Inventarisierung von Netzwerken mit bis zu mehreren 1.000 Clients.

bedingt beim Einsatz von dezentralen Netzwerken.

nicht für die Inventarisierung von Peripherie.

OCS Inventory NG

Einfach dicke Pakete schnüren

Um Software überhaupt verteilen zu können, muss sie als Paket vorliegen und auf dem OCS-Server bereitstehen. Hierzu benötigt das System zwei Dateien: Eine einfache Batch-Datei, die zum Beispiel das Kopieren und Ausführen der Installationsdatei bewirkt, und die als ZIP gepackte EXE-Datei selbst. Diese Pakete lassen sich für Windows als auch für Mac OS X und Linux individuell erstellen.

In unserem Test haben wir Pakete für die Installation von IrfanView als auch den Acrobat Reader und ein Windows 7 Service Pack 2 erstellt. Hierzu riefen wir den Package Builder auf und gaben dem Paket einen aussagekräftigen Namen und eine kurze Beschreibung. Danach wählten wir das Betriebssystem und die Priorität aus. Im Anschluss packten wir die Installations-EXE als ZIP und schrieben eine kleine Windows-Batch, um das Setup zu starten. Beide Dateien trugen wir in die entsprechenden Felder ein und bestimmten noch, dass die Installation ohne Userinteraktion erfolgen soll. Das Paket wurde daraufhin ohne Probleme erstellt und auf dem OCS-Server abgelegt.

Gezielte Rechtevergabe als Bonus

Für IT-Landschaften mittlerer Größe ist meist mehr als ein Mitarbeiter zuständig. Da auch bei OCS Inventory – gerade in Bezug auf die Paketverteilung – nicht jeder alles machen soll, ist die integrierte Userverwaltung dafür ausgelegt, User-Gruppen nur gezielte Rechte zu vergeben.

Das Profilmanagement ist hierfür in fünf Bereiche aufgeteilt. Im ersten Reiter definierten wir, von welchen Computern der User das Inventar sehen darf. Dabei richteten wir auch TAG-Filter ein und setzten Rechte für Black-Listen. Umfangreicher wurden dann die Rechte der Administration. Hier bestimmten wir, auf welche Menüpunkte der neue User zugreifen darf. Für detailliertere User-Rechte ist der Reiter "User Pages" zuständig. Hier konnten wir noch einmal detailliert angeben, welche Administrations-Seiten von der Gruppe genutzt werden dürfen.

Statt jeden User anzulegen und der entsprechenden Gruppe zuzuordnen, bietet OCS noch die Option einer LDAP-Synchronisation. Da OCS ein offenes System ist, müssen die Parameter zur Anbindung an die ADDS manuell eingetragen werden. Dies bedurfte im Test einiger Versuche, bis OCS die User aus dem Windows-LDAP angezeigt hat. Hier würden wir wir uns einen Assistenten wünschen, der den Administrator bei der Einrichtung unterstützt.

Fazit

OCS Inventory NG hat sich im Test als ein sehr umfangreiches und für den Administrator hilfreiches Tool herausgestellt. Die Installation nimmt allerdings etwas Zeit in Anspruch, auch wenn die Entwickler sich sehr viel Mühe dabei gegeben haben, dem Nutzer Skripte und gute Anleitungen an die Hand zu geben. Die Art der Agenten-Verteilung ist Geschmackssache und kann angepasst an die Notwendigkeiten der eigenen Netzwerkstruktur erfolgen. Durch die IpDiscover- und SNMP-Funktion werden sogar Geräte im Netzwerk erfasst, auf denen kein Agent läuft.

Da die Agenten die Daten auf den Ports 80 oder 443 senden, sind keine eingehenden Ports auf der Firewall zu öffnen. Die Nutzung von HTTP-Verbindungen zur Kommunikation zwischen Server und Client belastet den Netzwerkverkehr kaum. Die flexible Softwareverteilung, die durch den gezielten Einsatz von dynamischen Gruppen auch abhängige Installationen ermöglicht, rundet die Software ab.

Lediglich die Möglichkeit von Benachrichtigungen per E-Mail, zum Beispiel bei sich nicht mehr anmeldenden Clients oder bei der Veränderung von Konfigurationen, hat uns sehr gefehlt. Die bei OCS fehlende und in anderen Systemen enthaltene Visualisierung in Form von Netzwerkdiagrammen beeinträchtigt aber die Leistungsfähigkeit des Systems nicht sonderlich. So muss sich OCS Inventory NG als Open Source Projekt nicht hinter kommerziellen Alternativen verstecken. *(ln)*

1&1 DOMAINS

AKTION: JETZT OHNE EINRICHTUNGSGEBÜHR!

DIE GRÖSSTE AUSWAHL FÜR IHRE WUNSCH-DOMAIN.

VERTRAUEN SIE DER NUMMER 1

1&1 ist einer der größten Webhoster weltweit. Mit über 11 Mio. Kundenverträgen, 2 Milliarden € Jahresumsatz, 5.000 Mitarbeitern und 5 Hochleistungs-Rechenzentren in Deutschland, Europa und den USA. Und weil wir mit mehr als 18 Mio. registrierten Domains auch ein führender Registrar sind, profitieren Sie von außerordentlich günstigen Preisen!

GROSSE AUSWAHL

Mehr als 30 Domainendungen verfügbar: .de, .eu, .com, .net, .org, .us, .at, .info, .biz, .mobi, .name, .ch, .li, .co.uk, .me.uk, .org.uk, .co, .tv, .ws, .cc, .be, .as, .lt, .lv, .nu, .ph, .hn, .vc, .sc, .ag, .to, .vu

1&1 DOMAIN APP

Domaincheck und Domainregistrierung mit der 1&1 Domain App auch mobil möglich.

VOLLE DNS-KONTROLLE

Einfach über Verwaltungstool.

24/7 SUPPORT

Unser Experten-Team ist rund um die Uhr per Telefon und E-Mail erreichbar.

.de
.eu
.info
.at

12 MONATE
0,29 €/Monat*
1 Jahr für 0,29 €/Monat, danach ab 0,49 €/Monat*

.com
.net
.org

12 MONATE
0,99 €/Monat*
1 Jahr für 0,99 €/Monat, danach 1,49 €/Monat*

Inklusive bei allen 1&1 Domains:

- Kostenlose Domain-Umleitung
- Domain Kontakt-Management
- Kostenlos Subdomains einrichten und umleiten

1&1

Internet made in Germany

DOMAINS | E-MAIL | WEBHOSTING | E-SHOPS | SERVER

0 26 02 / 96 91 (DE) 0800 / 100 668 (AT)

www.1und1.info

* .de, .eu, .info, .at Domain 12 Monate 0,29 €/Monat, .com, .net, .org 12 Monate 0,99 €/Monat. Danach .de 0,49 €/Monat, .at, .info 1,99 €/Monat, .eu, .com, .net, .org 1,49 €/Monat. Einrichtungsgebühr von 9,60 € entfällt. 12 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.

Im Kurztest: Double-Take Availability 6

Hochverfügbarkeit die Sechste

von Thomas Bär

Quelle: Nataliia Natykach – 123RF

Clustering von Windows-Servern ist problemlos möglich. Die Technik erfordert aber einiges an Hintergrundwissen und ist alles andere als günstig. Wenn ein paar Minuten Downtime zu verkraften sind, so ist möglicherweise "Double-Take Availability", deren Version 6 erst kürzlich erschien, eine kostengünstige Alternative.

Bereits im vergangenen Jahr konnten wir uns im Rahmen eines Tests von der soliden Funktionalität der Software überzeugen. "Double-Take Availability für Windows" des Herstellers Vision Solutions bietet die Möglichkeit, eine relativ kostengünstige Alternative zu Cluster-Systemen aufzubauen. Kern des Systems stellt dabei die laufende Replikation der Daten von produktiven Windows-Servern auf Replikate dar. Diese Replikate sind typischerweise virtuelle Maschinen, die durch die Software entweder in einer VMware ESX- oder in einer Microsoft Hyper-V-Umgebung automatisiert eingerichtet werden. Mit Blick auf das zur Verfügung stehende Budget und die Lizenzpolitik von Microsoft eignet sich insbesondere die Hyper-V-Variante für den kleineren Geldbeutel.

Statt einen ausgefallenen Server durch die Wiederherstellung von Backups in Stunden wieder einsatzfähig zu machen, startet die Software ein Replikat als virtuelle Maschine. Wie lang das Programm die Nichterreichbarkeit des Quellservers toleriert, ehe das Replikat startet, ist pro Maschine durch den Administrator einstellbar. Ob es sich bei dem Quellserver um eine Windows-Installation auf einem physikalischen Server handelt oder um eine virtualisierte Maschine, spielt für die Software letztendlich keine Rolle. Einzig die Grundanforderungen müssen erfüllt werden: Windows Server 2003 oder höher. Applikationsseitig unterstützt das Programm Exchange 2007 und höher, SQL 2005 Server und höher, Oracle, SharePoint und den Blackberry Enterprise Server (BES).

Installation ohne Hürden

Die Installation der Software beginnt mit dem Download und dem Start auf einer aktuellen Workstation unter Windows. Von dieser aus wird der Programm-Agent auf alle beteiligten Server verteilt. Wir wählten für den Test eine aktuelle Windows 7 Enterprise-Maschine in der x64-Ausprägung. Die Einrichtung verlief weitgehend ohne besondere Vorkommnisse, allein die Fehlermeldung, dass der Aktivierungscode unzulässig sei, sorgte kurz für Verwirrung. Schlussendlich muss für die Konsole der Software kein Code eingegeben werden – der besagte Code ist ausschließlich für die Server gedacht. Die Verteilung auf die Testmaschinen – Windows Server 2003 und Server 2008 R2 – verlief ohne Besonderheiten.

Verbesserte Bedienung

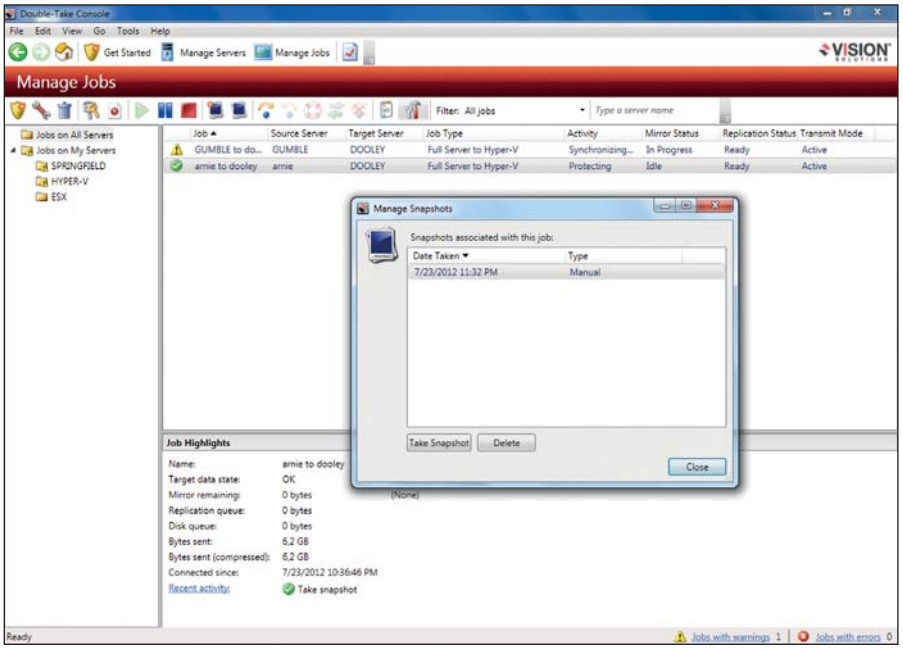
An Version 5.3 bemängelten wir besonders das kaum nachzuvollziehende Konzept der fünf verschiedenen Konsolenprogramme, die für die Bedienung der Software erforderlich waren. Zudem ließen sich diese wiederum über eine zentrale Konsole aufrufen. Dies hat der Hersteller in der neuesten Version überarbeitet. Im Windows-Startmenü gibt es nun einen Eintrag "Double-Take" und darin eine einzige Konsolensoftware.

Die Reiter und Menüs in der auf Englisch gehaltenen Oberfläche erklären sich weitgehend von allein. Es gibt einen Assistenten, der einen neuen Benutzer zielsicher durch die Dialoge führt. Erfahrene Benutzer verwenden indes die Option "Manage Servers", um Anpassungen an den Zielsystemen vorzunehmen, oder "Manage Jobs", um Replikationsänderungen durchzuführen. Das Job-Management wurde mit der Version 6 vereinheitlicht – alle Vorgänge unterliegen stets einer einzigen Vorgehensweise. Wer lieber mit Konsolenbefehlen arbeitet oder alle Schritte der Absicherung vollautomatisch durchführen muss, kann sich an der neuen PowerShell-Unterstützung von Double-Take 6 erfreuen.

Neu ist zudem die Einführung des "P2V Point in Time Supports". Hierbei handelt es sich um zusätzliche Snapshots im Replikat auf dem Zielsystem. Damit lassen sich gesicherte Systeme auf definierte Zeit-

Systemvoraussetzungen

Windows Server 2003 / 2008 Standard, Enterprise und Datacenter Edition (32 Bit / 64 Bit). In Hyper-V-Umgebungen: Microsoft .NET 3.5 SP1, VMs auf einem Standard-NTFS-Dateisystem, TCP/IP mit statischen IP-Adressen oder DHCP mit reservierten Adressen für Hyper-V-Hosts. Die Anforderungen unter VMware sind VirtualCenter 2.x oder höher und ESX Server 3.x oder höher.



Neu in Double-Take Availability 6 ist die Funktion, Snapshots gezielt im Replikat erzeugen zu können

punkte zurücksetzen (Point in Time Recovery). In Hyper-V-Umgebungen unterstützt Double-Take nun Clustered Shared Volumes (CSV) einschließlich Failover und Failback. So können virtuelle Maschinen bei Bedarf von einem Cluster-Host auf den anderen verschoben werden. Neu ist ebenfalls die vorkonfigurierte Universal-Virtual-Recovery-Appliance für VMware ESX-Umgebungen, die Installation und Konfiguration der Verfügbarkeitsumgebung automatisiert. Das Auto-Provisioning der virtuellen Umgebung für die Appliance spart laut Hersteller Zeit und reduziert die Fehlerwahrscheinlichkeit.

Robustes Konzept

Wie bereits im vergangenen Jahr wiederholten wir auch für diesen Test die Sicherung von physikalischen oder unter VMware ESX 4i virtualisierten Servern auf eine Hyper-V-Umgebung. Die damals auftauchenden Probleme, dass einzelne Server nicht gefunden werden konnten, gibt es in der neuesten Version nicht mehr. Der grundlegende Ablauf bleibt in der jüngsten Version unverändert: Welche Laufwerke gesichert werden sollen, welche Netzwerkkarte auf dem Hyper-V-Server im Fehlerfall für die Anbindung der VM ins Netzwerk genutzt wird und welche Netzwerkparameter zum Einsatz kommen – Gateway, DNS oder IP-Adressen –, richtet der Administrator gestützt durch den Assistenten ein. Je nach Bandbreite und Datenmenge auf dem Quellserver dauerte die Replikation Minuten bis Stunden. Alternativ erlaubt die Software die Sicherung einzelner Enterprise-Applikationen oder die Erstellung der Replikate in der ESX-Landschaft.

Zur Replikation klinkt sich das Werkzeug in die IO-Prozesse des Betriebssystems ein. Aufgrund dieser Unabhängigkeit von Applikationen lassen sich jegliche Inhalte in der virtuellen Maschine replizieren. Gleichzeitig ist dies aber auch die logische Einschränkung des Verfahrens: Daten, die sich noch nicht in einer Datei befinden, also im Arbeitsspeicher der Maschine gehalten werden, sind solange nicht Teil der Replikation, bis sie gespeichert wurden. Für die gängigen Microsoft-Produkte –SQL-Server und Exchange – bietet Double-Take aus diesem Grunde eine spezielle Variante der Software, die sich direkt in die Anwendung einklinkt.

In Tests animierten wir die Software mehrfach zur ungeplanten Übernahme des Serverbetriebs durch das Replikat. Je nach Einstellung der Wartezeit, bis die Software auf den Ausfall reagiert, und der Datenmenge dauert der Start des Ersatzsystems im besten Fall lediglich drei Minuten. Mitunter sind die spezifischen Treiber für die Virtualisierung noch zu installieren. Der auf dem Testserver installierte SQL-Server war jedoch bereits wieder über ODBC von außen erreichbar und einen Datenverlust konnten wir im Test nicht feststellen. Ein Failback auf das Quellsystem ist entweder unter Verwendung des "Checksum Mode" schnell erledigt oder es bedarf eines neuen Ersatzsystems, auf das die Daten der virtuellen Festplatten zurückübertragen werden müssen – ein eher manueller Prozess.

Fazit

Mit der neuen Version von Double-Take Availability ist es dem Hersteller gelungen, verschiedene kleinere Mängel der Vorgängerversion zu beseitigen. Die Bedienung ist nun deutlich einfacher, da nicht mehr eine große Anzahl von Konsolen für unterschiedliche Zwecke geliefert wird, sondern eine monolithische Konsole für alle Einsatzbereiche existiert. Das verbesserte Konzept der Sicherung auf Replikat-Server auf Hyper-V oder ESX-Systeme und die Hardwareunabhängigkeit gefällt. Die Exchange 2003- und SQL 2000-Unterstützung wurde jedoch auf "Full Server Failover" reduziert – für einzelne Applikationen gibt es nun keine Sicherungsfunktion mehr. *(ln)*

Produkt
Software für Hochverfügbarkeit und Disaster Recovery unter Windows-Systemen.

Hersteller
Vision Solutions
www.visionsolutions.com

Preis
Der Preis für die Standard-Edition von Double-Take Availability ist abhängig von der Anzahl der zu sichernden Maschinen und beginnt bei rund 3.300 Euro. Für kleine Umgebungen bietet der Hersteller darüber hinaus die "Foundation Edition" ab 1.800 Euro an.

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

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

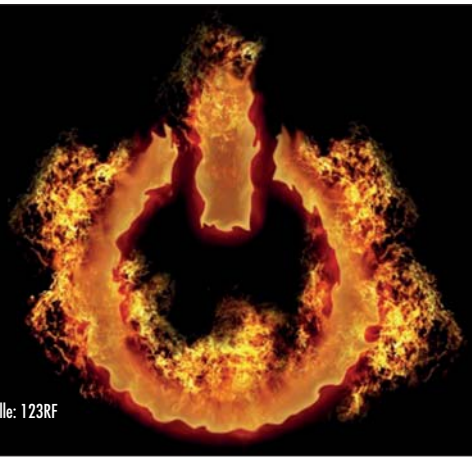
Einrichtungsdauer	7
Bedienkonzept	6
Integrationsfähigkeit	9
Failover zu Hyper-V	9
Failback	6

Double-Take Availability 6

Einkaufsführer: Hochverfügbarkeitslösungen

Gewappnet für den Fall der Fälle

von Ulrich Lenz



Quelle: 123RF

Hochverfügbarkeit ist heute in der IT, anders als noch vor wenigen Jahren, eine gängige Anforderung. Seit in allen Unternehmen und Organisationen die wesentlichen Geschäftsprozesse nur noch über die IT laufen, dürfen diese Systeme eben nicht mehr ausfallen, das gilt im Büro nicht anders als in der Fabrikhalle. Zur Realisierung von Hochverfügbarkeit für Server-Systeme stehen unterschiedliche Konzepte und Technologien zur Verfügung. Sie haben alle ihre Vor- und Nachteile – was für ein Unternehmen passt, hängt primär von den Risiken der Geschäftsprozesse ab. Welche Vorzüge und welches Manko die jeweiligen Ansätze zu bieten haben, zeigt dieser Artikel.

Der Aufwand, den Anwender treiben müssen, um ihre Systeme verfügbar zu halten, relativiert sich am jeweiligen Risiko: Je größer ein Schaden an Geld, Image oder schlimmstenfalls an Gesundheit und Leben durch Ausfall der unterstützenden Server sein kann, desto besser muss die Absicherung gegen das Eintreten eines Schadensfalls sein. Eine einfache Büroanwendung kann vielleicht einen halben Tag nicht verfügbar sein, ohne dass das betreffende Unternehmen in Schwierigkeiten gerät. Das automatische Hochregallager eines Automobilzulieferers muss dagegen ständig verfügbar sein, und bei den Systemen der Flugsicherung erübrigt sich jedes Abwägen. Verfügbarkeit bemisst sich daher an den jeweiligen Prozessen und den mit ihnen verbundenen Risiken. Hinsichtlich nicht geplanter Stillstandzeiten lässt sich eine einfache Formel aufstellen: Die Verfügbarkeit A eines Systems wird gemessen als Verhältnis der mittleren Zeit zwischen zwei Stillständen (MTBF – Mean Time between Failure) und der Summe von MTBR und der mittleren Reparaturzeit (MTTR – Mean Time to Repair):

A = MTBF / (MTBF + MTTR) <= 1

Die MTTR selbst setzt sich wieder aus den Zeiten für die Ersatzteilbeschaffung und der Wiederherstellung – in der Regel Datenrücksicherung und Beheben von inkonsistenten Datenzuständen – zusammen. Ein System, das zum Beispiel im Durchschnitt acht Stunden pro Jahr nicht verfügbar ist, hat demnach eine prozentuale Verfügbarkeit von etwa 99,9 Prozent. Die Verfügbarkeit eines aus mehreren Komponenten zusammengesetzten Systems, bei dem die Funktionstüchtigkeit von jeder einzelnen Komponente abhängt, berechnet sich als Produkt der einzelnen Verfügbarkeiten. In Kürze: je mehr voneinander abhängige Komponenten, desto schlechter die Verfügbarkeit.

Hochverfügbarkeit definiert

Der Begriff Hochverfügbarkeit ist nicht so eindeutig gefasst und wird oft unterschiedlich interpretiert. Generell darf ein System als hochverfügbar bezeichnet werden, wenn eine Anwendung trotz Fehlerfall ohne manuelle Eingriffe verfügbar ist. In der Konsequenz heißt dies, dass der Anwender keine oder nur eine kurze Unterbrechung wahrnimmt. Der wesentliche Punkt bei der Hochverfügbarkeit ist also die Forderung nach einem automatischen Umschalten im Fehlerfall und nahezu unterbrechungsfreier Fortführung der Verarbeitung.

Da Hardware-Fehler technisch nie ausgeschlossen werden können, also auch nicht in Server-Systemen, ist zur Realisierung einer Server-Hochverfügbarkeit erforderlich, dass Server aus redundanten, sprich mindestens doppelt ausgelegten und voneinander weitestgehend unabhängigen Komponenten bestehen. Damit kann die Verarbeitung parallel erfolgen und im Störungsfall die automatische Fortführung der Prozesse nach einer kurzen Umschaltzeit sichergestellt werden.

Ohne auf die weitere mathematische Betrachtung zur Berechnung der Verfügbarkeit von zusammengesetzten Systemen, zu denen auch Server zu rechnen sind, einzugehen, lässt sich schon aus der oben erläuterten einfachen Formel ablesen, dass die Verfügbarkeit drastisch zu verbessern ist, je kleiner die Wiederherstellungszeit (MTTR) ausfällt. Denn je kürzer die Zeit für Beschaffung und Austausch des Ersatzteiles ausfällt und desto schneller die Anwendung wieder auf die Daten zugreifen kann, desto höher wird die Gesamtverfügbarkeit.

Service Level Agreements (SLAs) sind daher für die Realisierung einer hohen Verfügbarkeit von entscheidender Bedeutung. Wenn Austauschteile nicht erst nach Tagen, sondern schon nach Stunden beim Anwender eintreffen, steigt die Verfügbarkeit. Das gilt natürlich erst recht, wenn die betreffenden Teile schon vor einem Ausfall bereitstehen, wie das heute mit proaktiver Fehleranalyse in Verbindung mit einem guten Service-Management ohne weiteres

machbar ist. Wer bei Einführung einer Hochverfügbarkeitslösung auf solchen Service verzichtet, verschenkt prinzipiell wesentliche Vorteile, die sich aus der HA-Lösung ergeben können. Technisch aufwändige Systeme mit schlechtem Service sind unterm Strich dann weniger verfügbar als technisch relativ simple Lösungen, die aber sehr gut betreut werden.

HA-Technologien mit Vor- und Nachteilen

Die im Markt verfügbaren Lösungen für die Realisierung von Hochverfügbarkeit gehen von unterschiedlichen Konzepten aus. Da Verfügbarkeit wie erwähnt vor dem Hintergrund der jeweiligen Geschäftsprozesse und ihrer spezifischen Risiken zu sehen ist, lässt sich eine endgültige Antwort auf die Frage nach der "besten Lösung" ebenso wenig geben wie bei der Anschaffung eines PKW. Auch hier hat jeder Ansatz Vor- und Nachteile, die der Anwender selbst bewerten muss. Folgende Konzepte behandeln wir im Einkaufsführer:

- Single Server und Cold Standby,
- Cluster und
- Fehler-Toleranz.

Um den Vergleich der Systeme übersichtlich zu halten, gehen wir bei den folgenden Beschreibungen als Software-Umgebung vom Betriebssystem Windows Server, der Datenbank Microsoft SQL Server und bei der Betrachtung von Virtualisierungsansätzen von VMware vSphere aus.

Single Server und Cold Standby

Betriebswirtschaftlich lässt sich ein Single Server-Konzept mit der Unterlassungsalternative vergleichen: Die Notwendigkeit, einen Geschäftsprozess gegen Server-Ausfall abzusichern ist zwar bekannt, doch der potenzielle Schaden wird geringer eingeschätzt als der Aufwand für das Einrichten und Betreiben einer Hochverfügbarkeitslösung. Mit Zusatzoptionen wie doppelten Netzteilen, redundanten Netzwerkanschlüssen oder gespiegelten Platten lässt sich der nicht hochverfügbare Server zumindest robuster gegen Ausfälle von Einzelkomponenten machen.

In die Rubrik Single Server fällt auch das sogenannte Cold Standby-System. Hier wird ein zweites, möglichst identisches System vorgehalten, das im Fehlerfall des Produktionssystems mit den erforderlichen Programmen und Daten gestartet wird und dann den Notfallbetrieb übernimmt. Diese Absicherung ist mehr eine Gewissensberuhigung als eine ernst zu nehmende Strategie. Im Fehlerfall ist mit hoher Wahrscheinlichkeit das Ersatzsystem nicht auf dem neuesten Software-Stand, die letzte Datensicherung liegt einige Zeit zurück oder eine Hardwarekomponente wurde zwischenzeitlich in einem anderen Server verbaut. Die Wiederherstellungszeit kann entsprechend lange dauern – erfahrungsgemäß deutlich länger als bei Trockenübungen ermittelt. Hochverfügbarkeit sieht anders aus, daher gehen wir hier nicht weiter auf die Cold Standby-Alternative ein. In der Praxis dürfte diese Variante allerdings auf die meisten Installationen kommen. Vorteile sind ein kostengünstiger Betrieb und Anschaffung sowie die leichte Administrierbarkeit und geringe Komplexität. Zu den Nachteilen zählt die notwendige manuelle Reaktion zur Wiederherstellung. Auch gibt es lange Wiederherstellungszeiten nach einem Ausfall und die Wartung erfordert eine Betriebsunterbrechung.

Cluster

Bei Cluster-Lösungen sind mehrere Varianten zu unterscheiden: die Herstellung von Hochverfügbarkeit durch die Nutzung von Betriebssystem-Diensten, durch Anwendungen mit einprogrammierter Hochverfügbarkeit sowie Hochverfügbarkeit auf Basis von Virtualisierungstechnologien.

Nutzung von Betriebssystem-Diensten

Ein Hochverfügbarkeitscluster besteht in der Regel aus zwei oder mehreren identischen Server-Systemen (Cluster-Knoten) und einem im gemeinsamen Zugriff liegenden externen Daten-Speicher, etwa in einem SAN. In den Cluster-Knoten sind neben den standardmäßigen Betriebssystem-Diensten zusätzliche Cluster-Dienste zur gegenseitigen Überwachung der Server gestartet. Die Cluster-Dienste überwachen die abzusichernden Ressourcen (Hardware-Komponenten und Anwendungen) des Systems. Die Kommunikation der beiden Server erfolgt über eine redundant ausgelegte, vom Produktionsnetzwerk unabhängige Netzwerkverbindung. Welche Komponenten überwacht werden, wird durch den Cluster-Administrator definiert. In der Regel werden dazu umfangreiche Scripting-Prozeduren erstellt.

Fällt eine Komponente (Cluster Ressource) aus, wird ein Failover initiiert und die Verarbeitung auf dem anderen Knoten wieder aufgenommen. Für einen SQL-Server zum Beispiel wäre dieser Failover mit einem Stoppen auf dem einen Knoten und dem Wiederanlauf auf dem anderen Knoten verbunden, das heißt, es wird ein normales Recovery mit Rollback offener Transaktionen angestoßen. Je nach Anzahl offener Transaktionen kann das wenige Minuten bis zu mehreren Stunden dauern. Der Anwender kann weiterarbeiten, sobald die Datenbank wieder einen logisch konsistenten Zustand besitzt. Es gehen nur die letzten Eingaben von nicht abgeschlossenen Transaktionen verloren. Zu beachten ist dabei, dass eine Client-Anwendung sich in diesem Fall am Datenbank-Server neu anmelden muss. Geschieht das automatisch, weil es bei der Programmierung der Anwendung berücksichtigt wurde, spricht man von einer Anwendung, die Cluster-aware ist.

Wird das Umschalten von einem Knoten auf den anderen durch den Administrator angestoßen, ist von einem Switchover die Rede, um diesen geplanten Vorgang vom ungeplanten Failover zu unterscheiden. Bei einem Switchover können Dienste ordnungsgemäß gestoppt werden. Das Verfahren wird beispielsweise genutzt, um geplante Wartungsarbeiten an einem Knoten vorzunehmen. Die Vorteile liegen darin, dass Standard-Software und -Hardware genutzt werden kann und im Fehlerfall ein automatisches Umschalten möglich ist. Ebenso stellt sich die Wartung im laufenden Betrieb weitestgehend problemlos dar. Demgegenüber steht ein hoher administrativer Aufwand bei der Einrichtung und Pflege durch große Komplexität, weshalb geschultes IT-Personal unabdingbar ist. Zudem gibt es Betriebsunterbrechung während des Failovers und die Anwendungen müssen Cluster-Aware sein. Für das Unternehmen fallen zudem doppelte Lizenzen für Betriebssystem, Datenbank und Anwendung an. Auch ein externes Speichersystem ist notwendig.

Für Hochverfügbarkeit programmierte Anwendungen

Wird bereits bei der Anwendungsentwicklung berücksichtigt, dass das Gesamtsystem hochverfügbar sein soll, lässt sich so mancher administrativer Aufwand im späteren Betrieb vermeiden. Die Programme werden dabei von vornherein so geschrieben, dass regelmäßig relevante Zustandsinformationen von einem Master-Prozess an einen auf einem zweiten Server laufenden Slave-Prozess übermittelt werden. Fällt der Master aus, übernimmt der Slave die weitere Verarbeitung. Allerdings ist das Entwickeln von hochverfügbaren Anwendungen und deren Pflege alles andere als trivial und ausgesprochen kostenintensiv.

So können beispielsweise bei Datenbanksystemen, die Hochverfügbarkeit auf diese Weise vorsehen, allein die Lizenzkosten durchaus im sechsstelligen Bereich liegen. Derartige Ansätze gibt es daher vor allem dort, wo der Failover der Standard-Cluster-Lösungen zu viel Zeit beansprucht und in dieser Zeit wichtige Daten nicht verarbeitet werden können. Typische Einsatzgebiete sind Anwendungen in der Automatisierungstechnik, wo Echtzeitverhalten unabdingbar ist. Von Vorteil bei dieser Variante sind das automatische Umschalten im Fehlerfall und die im laufenden Betrieb weitestgehend mögliche Wartung. Auch gibt es keine Betriebsunterbrechung beim Failover und das Echtzeit-Verhalten kann berücksichtigt werden. Von Nachteil sind die hohen Entwicklungs- und Wartungskosten sowie die nötigen doppelten Lizenzen für Betriebssystem und Datenbank. Damit decken derartige Anwendungen nur ein sehr spezifisches Einsatzgebiet ab.

Hochverfügbarkeit auf Basis von Virtualisierung

Virtualisierung dient neuerdings häufig zur Herstellung von Hochverfügbarkeit. Hier sei exemplarisch das Verfahren im Fall von VMware vorgestellt. Dabei werden (mindestens) zwei physische Server mit dem VMware-Hypervisor vSphere als Betriebssystem aufgesetzt. Alle Server haben Zugriff auf einen gemeinsam genutzten, externen Daten-Speicher. Zusammen mit dem Datenspeicher bilden die Server einen so genannten High Availability Cluster. Über einen Heartbeat-Mechanismus überprüfen beide Hypervisoren, ob der physische Partner-Server noch ordnungsgemäß arbeitet. Die virtuellen Maschinen (Konfigurationsdateien und Daten) werden im gemeinsamen Daten-Speicher abgelegt und sind für beide physischen Maschinen sichtbar. Eine virtuelle Maschine wird nun im ersten Server gestartet, das heißt, es läuft zunächst das Betriebssystem an, anschließend wird die Applikation gestartet. Diesen Vorgang kann man sich wie bei einem nichtvirtuellen System vorstellen; die virtuelle Maschine wird gebootet, die Datenbank wird gestartet und schließlich die Anwendungsdienste hochgefahren – der ganze Prozess benötigt eine gewisse Zeit, deren Dauer von der Komplexität der Anwendung abhängt.

Fällt ein physischer Server aufgrund einer Störung aus, zieht dies den Ausfall aller virtuellen Maschinen auf diesem Server nach sich. Von außen ist der Ausfall einer virtuellen Maschine mit einem Servercrash, also einem ungeplanten und plötzlichen Stillstand des Systems, vergleichbar. Alle Daten, die sich im virtuellen Hauptspeicher (RAM) der virtuellen Maschine befinden, und alle nicht auf dem Datenspeicher abgesicherten Datenbank-Veränderungen gehen dann verloren. Der Austausch mit den Clientsystemen ist unterbrochen, die weitere Verarbeitung damit nicht mehr möglich. In der HA-Cluster-Verwaltung des vCenter-Servers hat der Administrator zuvor festgelegt, welche VMs in welchen verbliebenen physischen Servern nachgestartet werden sollen. Nachstarten einer VM heißt, es wird gebootet, die Datenbank gestartet – mit den dann üblichen, zeitintensiven Mechanismen zum Bereinigen von inkonsistenten Transaktionen – und zum Schluss werden die Anwendungsdienste neu gestartet. Erst ab diesem Zeitpunkt ist der Anwender wieder in der Lage weiterzuarbeiten, wobei noch eine Prüfung der nicht durchgeführten Transaktionen erfolgen muss. Je nach Anwendung und Datenbank kann diese Wiederanlaufzeit also erheblich sein – zusätzlich zum erhöhten Zeitbedarf durch den konkurrierenden Anlauf mehrerer virtueller Maschinen. Mittels einer Life Migration – bei VMware vMotion – können bei ungestörter Funktion beider Server die VMs von einem auf den anderen physischen Server unterbrechungsfrei verschoben werden und somit ein Server für die Wartung außer Betrieb genommen werden.

In diese Kategorie der HA-Lösungen fallen auch Software-Angebote wie Stratus Avance, bei dem die Daten zwischen zwei physischen Servern laufend synchronisiert werden. Bei dieser Lösung kommt ein Servercrash seltener vor, weil der Zustand der Hardwarekomponenten im laufenden Betrieb proaktiv analysiert und mit einer Fehlermusterdatenbank abgeglichen wird. Bei Überschreiten vorgegebener Toleranzen wird automatisch eine Life Migration angestoßen und das Service-Management entsprechend informiert. Den gefährdeten Server kann der Administrator dann reparieren, bevor eine Unterbrechung der Verarbeitung stattfindet. Anschließend synchronisieren sich die Server automatisch wieder. Diese Lösung kommt im Unterschied zu VMware ohne externes Speichersystem aus. Vorteile sind die Nutzung von Standard-Software und -Hardware und ein automatisches Umschalten im Fehlerfall. Auch ist die Wartung eines physischen Servers bei Nutzung von Life Migration im laufenden Betrieb möglich. Nachteilig wirken sich die zusätzlichen Kosten für die Hypervisor-Lizenzen und für die Hardware und Lizenzen des Management Servers (VMware vCenter Server) aus. Auch ist ein externes Speichersystem erforderlich und es gibt längere Betriebsunterbrechung während des Failovers.

Fehler-Toleranz

Den gravierenden Nachteil der relativ langen Betriebsunterbrechung des VMware HA Clusters vermeidet die vSphere Fault Tolerance (FT) Option. VMware FT bietet im Fall eines Serverausfalls fortlaufende Verfügbarkeit für Anwendungen. In einem HA-Cluster wird von einer virtuellen Maschine eine Schatteninstanz in einem zweiten Server erstellt. Jeder Verarbeitungsschritt der primären Instanz wird durch Record and Replay (vLockstepping) in der Schatteninstanz nachgespielt. Fällt der primäre Server aus, arbeitet die Schatteninstanz nun als neue primäre virtuelle Maschine ohne Betriebsunterbrechung und Datenverlust weiter. Sind weitere physische Knoten im HA-Cluster konfiguriert, wird automatisch eine neue

Schattenkopie erstellt, um die virtuelle Maschine weiter redundant zu halten.

Allerdings hat diese softwarebasierte Technologie, die ähnlich auch von anderen Anbietern verfügbar ist, eine gravierende Einschränkung: Für das Record und Replay ist in erheblichem Umfang zusätzliche CPU-Leistung erforderlich und die Überwachung von Multiprozessor-VMs ist nicht möglich. Damit sind die Anwendungsfälle für diese Alternative sehr begrenzt. So lassen sich Standard-Software und -Hardware nutzen und auch hier gibt es ein automatisches Umschalten im Fehlerfall sowie keine Betriebsunterbrechung. Zudem ist die Wartung eines physischen Servers bei Nutzung von Life Migration im laufenden Betrieb möglich. Doch bringt dieses Verfahren zusätzliche Kosten für die Hypervisor-Lizenzen und die Hardware und Lizenzen des Management Server (VMware vCenter Server) mit. Ebenso ist auch hier ein externes Speichersystem erforderlich und es

Vergleich der HA-Lösungen

	Single Server	MS Cluster-Dienst	Cluster-Anwendung	VMware HA	VMware FT	ftServer
Abzusicherndes Risiko	kein	mittel	hoch	gering	hoch	hoch
Verfügbarkeit	99,9	99,99	99,999	99,95	99,999	99,999
Mittlere Ausfallzeit pro Jahr	8,7 h	52,6 min	5,3 min	4,4 h	5,3 min	5,3 min
Kostengünstig in der Anschaffung	++	-	--	+	-	+
Kostengünstig im Betrieb	-	--	+	-	-	+
Einfach zu administrieren und geringe Komplexität	++	--	-	+	+	++
Keine manuelle Reaktion zur Wiederherstellung erforderlich	--	-	++	-	++	++
Keine langen Wiederherstellungszeiten nach Ausfall	--	-	++	-	++	++
Wartung erfordert keine Betriebsunterbrechung	--	+	++	++	++	++
Standard-Software kann genutzt werden	++	+	--	++	+	++
Automatisches Umschalten im Fehlerfall	--	++	++	++	++	++
Kein spezielles Know-how erforderlich	++	--	-	-	-	++
Keine Betriebsunterbrechung während des Failovers	--	-	++	-	++	++
Keine doppelten Lizenzen für Betriebssystem, Datenbank und Anwendung erforderlich	++	--	+	-	-	++
Kein externes Speichersystem notwendig	+	-	+	-	-	+
Echtzeit Verhalten kann berücksichtigt werden	-	-	+	-	+	+
Geringe Entwicklungs- und Wartungskosten	++	+	--	+	-	++
Keine zusätzlichen Kosten für Clusterverwaltung	++	-	-	--	--	++
Skalierbar und kein Ressourcen-Overhead	++	-	+	-	--	++

besteht ein hoher CPU Performance-Overhead. Schließlich ist das System nicht skalierbar und beschränkt auf Single-Prozessor-Anwendungen.

Fehler-Toleranz Hardware-basierend

Fehlertolerante Serversysteme wie etwa die ftServer von Stratus eliminieren Single Points of Failures (SPOF) dadurch, dass alle Komponenten redundant vorhanden sind. Mittels der Lockstep-Technologie werden zwei CPU / Memory-Einheiten, jede für sich wieder mit einem oder zwei Multicore-Prozessoren, in synchronem Zustand gehalten. Jede Einheit führt zum gleichen Zeitpunkt die gleiche Verarbeitung durch. Auf der I/O-Seite kommen redundante PCI-Busse mit marktgängigen PCI-Adaptern (etwa SAS, Ethernet oder Fibre Channel) zum Einsatz. Für jede logische I/O-Transaktion stehen also mindestens zwei Wege zur Verfügung, sodass im Fehlerfall jede Operation über einen alternativen Pfad wiederholt und abgeschlossen werden kann. Die Netzwerkanbindung wird beispielsweise über Adapter Faulttolerant Teaming realisiert, die internen Platten sind gespiegelt, optionaler externer Speicher wird über iSCSI oder Fibre Channel Multipathing angeschlossen.

Die gesamte Fehlerüberwachung findet ohne Beteiligung des Betriebssystems, also ohne zusätzlichen Ressourcenverbrauch der CPUs, auf der Hardware-Ebene statt. Damit können Standardbetriebssysteme wie Microsoft Windows Server, Red Hat Enterprise Linux oder VMware vSphere ohne Anpassung zum fehlertoleranten Einsatz kommen. Eine kostenintensive Migration von Applikationen für den fehlertoleranten Betrieb ist nicht erforderlich.

Fehler-Toleranz und Desaster-Toleranz

Fehler-Toleranz

Ist im Fehlerfall selbst eine kurze Unterbrechung nicht mehr gegeben, spricht man von Fehler-Toleranz. Ein fehlertoleranter Server arbeitet also trotz Einzelkomponentenfehler unterbrechungsfrei weiter. Die Verfügbarkeit fehlertoleranter Systeme liegt bei 99,999 Prozent, was einer mittleren Ausfallzeit von fünf Minuten pro Jahr entspricht.

Desaster-Toleranz

Hochverfügbare beziehungsweise fehlertolerante Serverlösungen bezeichnen Systeme, die gegen interne Fehler, insbesondere Komponentenfehler, sehr gut abgesichert sind. Externe Störungen, wie Feuer, Wasser, Erdbeben oder Stromausfall, werden als Desaster bezeichnet. Lösungen für die Vermeidung von Betriebsunterbrechungen durch Desaster werden hier nicht behandelt.

Für den Administrator stellt sich das fehlertolerante Serversystem auf der Betriebssystemebene wie ein einzelner Rechner dar, es wird also nur ein Betriebssystem installiert, die Anwendungen müssen nur einmal installiert werden, die Lizenzierung erfolgt dementsprechend auch nur für einen Rechner. Der Verwaltungsaufwand ist sogar geringer als bei der Single-Server-Lösung, denn es gibt keinen Wiederherstellungsaufwand nach Störfällen. Weniger Verwaltungsaufwand und nur halb so viele Lizenzen führen zu zusätzlichen Kosteneinsparungen gegenüber einer Clusterlösung. Außerdem entfällt das fehleranfällige und testintensive Scripting für die Clusterinstallation. Hardware-Fehlfunktionen einzelner Komponenten registriert und behandelt die Überwachungslogik der Hardware automatisch und zwar ohne Failover-Verzögerung oder gar Datenverlust. Wird ein Problem erkannt, isoliert die Überwachungslogik die betreffende Baugruppe im System. Das restliche System arbeitet ohne Performance-Einbußen und vor allem ohne jede Unterbrechung weiter.

Die kritische Baugruppe wird dann einem Selbsttest unterzogen. Fällt das Ergebnis des Selbsttests positiv aus, wird sie wieder mit dem Rest des Systems synchronisiert und die Redundanz ist wiederhergestellt. Stellt der Test einen nicht behebbaren Fehler fest, wird zum einen eine Alarmmeldung in die Event Logdatei geschrieben, optional kann zusätzlich ein SNMP-Trap abgesetzt werden, und zum anderen wird automatisch eine Fehlermeldung an den Service-Dienstleister abgesetzt. Weil der Rest des Systems weiterläuft, ist es auch in der Lage, das defekte Bauteil exakt zu identifizieren und vom Serviceprovider anzufordern. Aufgrund des modularen Hardwaredesigns kann das Ersatzbauteil dann mit wenigen Handgriffen im laufenden Betrieb gegen das defekte Teil getauscht werden. Das neue Bauteil synchronisiert sich automatisch, ohne dass ein Zugang zur Systemkonsole erforderlich ist, mit dem restlichen System und die Redundanz ist wiederhergestellt. Die geringe Komplexität der Administration des Servers erhöht zusätzlich die Verfügbarkeit. Die Vorteile sind damit die Nutzbarkeit von Standard-Software ohne Anpassung und keine Unterbrechung im Fehlerfall.

Auch ist die Wartung im laufenden Betrieb möglich und es besteht nur ein sehr geringer administrativer Aufwand bei der Einrichtung und Pflege. Lizenzen müssen nur jeweils einfach für das Betriebssystem, die Datenbank und Anwendungen vorgehalten werden. Zudem ist eine solche Lösung gut skalierbar. Lediglich spezielle Rechner-Hardware ist erforderlich.

Fazit

Welche Lösungen die passenden sind, lässt sich aus einem Vergleich von Aufwand für die Lösungen und dem bewerteten Risiko ermitteln – vorausgesetzt Sie sind sich über die Implikationen der jeweiligen Technologie im Klaren. Wenn der Ausfall des Servers keinen oder nur einen geringen Schaden verursacht, ist der Single Server mit 99,9 Prozent Verfügbarkeit eine ausreichende und bestimmt die kostengünstigste Alternative. In der produzierenden Industrie mit 24 x 7-Betrieb und einem Schaden von 2.000 Euro pro Stunde Ausfall beträgt der durchschnittlich pro Jahr zu erwartende Schaden aber schon 17.520 Euro und damit wesentlich mehr als die Investitionen in eine Hochverfügbarkeitslösung.

Wer es sich leisten kann, für den Dauerbetrieb mehrere gut ausgebildete Cluster-Administratoren im Drei-Schicht Betrieb einzusetzen, kann die Alternative des Betriebssystem-Clusters implementieren. Im Sinne der Hochverfügbarkeit sollten jedoch nicht nur die Hardwarekosten im Vordergrund stehen, sondern auf einfach zu administrierende, in sich schlüssige Lösungen zurückgegriffen werden, damit die gerade in kritischen Situationen auftretenden Bedienungsfehler vermieden werden. Hier bieten fehlertolerante Server bei vergleichbaren Anschaffungskosten eine viel einfachere Administration bei bester Verfügbarkeit von 99,999 Prozent – ob nun mit nativem Betriebssystem oder als Host für virtuelle Maschinen. *(dr)*

Dipl.-Math. Ulrich Lenz ist Leiter EMEA Availability Consulting bei Stratus Technologies GmbH in Eschborn.

FrontRange: Desktop & Server Management-Lösung bereit für Windows 8

FrontRange, Weltmarktführer bei Softwarelösungen für das hybride IT-Servicemanagement (ITSM) für Unternehmen jeder Größe mit Lösungen für On-Premise- und Cloud-Betrieb, bringt jetzt die neue Version von Desktop & Server Management 7 (DSM 7.2) auf den Markt: Das Release 7.2 unterstützt Unternehmen auf dem Weg zu Microsoft Windows 8, bietet erhöhte Skalierbarkeit und fortschrittliche Patch-Verwaltung.

Advanced Patch Management für FrontRange DSM 7

Mit dem Release 7.2 der Front-Range DSM-Software wird das Verwalten von Patches noch einfacher und wirkungsvoller. Jetzt werden Verwundbarkeiten in allen Clients automatisch erkannt. Es gibt ein neues Add-On als Alternative zur bisherigen nur für Microsoft verfügbaren Patch Management Option. DSM 7.2 lädt automatisch Patches herunter und packetiert sie. Patches mit hoher Priorität werden automatisch eingespielt. Administratoren erhalten eine umfassende Übersicht über den Status der Patches und Berichte über offene Angriffsflächen.

Unterstützung für Windows 8

Out of the Box arbeitet DSM 7.2 mit dem Windows 8 Operating System Deployment (OSD) zusammen. Die Windows 8 Quelldateien werden identifiziert. Es gibt Unterstützung für das Windows Preinstallation Environment 4.0 (PE), das als Minimalvariante von Windows 8 für Aufgaben des Systemmanagements gedacht ist.
Windows 8 Clients werden von DSM 7.2 mit zusätzlichen Funktionen erweitert. Plug N Play (PNP) wird unterstützt. Es gibt eine Service Interaktion mit der neuen Windows 8 Benutzeroberfläche. Der Anwender wird mittels des Windows 8 Notification Systems über Pop-up Messages und Shell Tray Icon Messages informiert. Zudem wird Windows Server 2012 als Managed Client Platform unterstützt.

Enterprise Skalierbarkeit > 100.000 Clients

Auch große Unternehmen mit mehr als 100.000 Arbeitsplätzen können jetzt mit dem Release 7.2 der FrontRange DSM-Software problemlos alle Verwaltungsaufgaben lösen. Zusätzliche Funktionen sind das Load-Balancing und die Fehlertoleranz für alle Web Services Zugangsmodule, im Einzelnen die Konsole, den Business Logic Proxy Server (BLP), die Relay Proxies und die DSM Clients. Neu sind preferred Server Einstellungen für die Konsole und den Business Logic Proxy Server (BLP). Es gibt jetzt eine Priorisierung im Verhältnis 80:20 zwischen aktiven Servern und Stand by Servern, die rein für Disaster Recovery (DR) vorgesehen sind.

Das Release steht für Partner des Unternehmens und DSM-Kunden mit Service-Verträgen zum Download auf der FrontRange-Website bereit:
www.frontrange.com/de/
Weitere Informationen finden Sie zudem auf www.frontrange.com/itam/testdsm.

Über FrontRange:

FrontRange ist Weltmarktführer bei Softwarelösungen für das hybride IT-Servicemanagement (ITSM) für Unternehmen jeder Größe. Mit seiner HEAT-Suite ist FrontRange der einzige ITSM-Anbieter weltweit, der über Servicemanagement-Software mit voll integrierter Sprachautomation und Client-Verwaltungsfunktionalität lokal und in der Cloud verfügt. HEAT verwaltet Millionen von Servicedialogen am Tag bei über 15.000 führenden Unternehmen. Mit HEAT erreichen unsere Kunden mehr betriebliche Effizienz und reduzieren Kosten und Komplexität. FrontRange hat seinen Sitz in Pleasanton (Kalifornien). Im Internet findet man FrontRange unter www.frontrange.com.

frontrange™
The HEAT is on

Server härten mit Microsoft Security Compliance Manager

Externe Sicherheitsberater

von Thomas Joos

Möchten Administratoren ihre Server absichern, geschieht das in Windows-Netzwerken vor allem über Gruppenrichtlinien. Doch gestalten sich diese meist recht komplex und aufwändig. Kein guter Anfang, wenn es um die Sicherheit geht. Daher helfen Vorlagen und Tools dabei, Systeme besser abzusichern. Microsoft bietet dazu das kostenlose Tool Microsoft Security Compliance Manager an. Was das Werkzeug zu bieten hat und wie Sie es optimal einsetzen, erfahren Sie in diesem Workshop.

In der neuen Version 2.5 beherrscht der Microsoft Security Compliance Manager (SCM) auch die Absicherung von Exchange Server 2007 SP3/ 2010 SP2. Um die Server zu schützen, laden Sie zunächst den Security Compliance Manager kostenlos herunter [1]. Sie installieren das Tool auf einem Server, importieren die bestehenden Gruppenrichtlinien im Active Directory in das Tool und können anschließend die Einstellungen der Richtlinien mit den Konfigurations-Empfehlungen aus dem SCM vergleichen.

Einsatzgebiete

Weitere Tools, die bei der Optimierung der Sicherheit helfen sollen, sind der Microsoft Attack Surface Analyzer und der Microsoft Baseline Security Analyzer. Beide Werkzeuge stehen ebenfalls kostenlos zur Verfügung. Bestandteil von Windows Server 2008 R2 ist der Security Configuration Wizard (SCW). Auch mit diesem Produkt lassen sich Server absichern. Alle diese Tools arbeiten Hand in Hand und lassen sich auch parallel einsetzen. SCM unterstützt die Absicherung von Windows Server 2003/2008/2008 R2 sowie die Client-Betriebssysteme Windows XP/Vista und Windows 7. In der Version 2.5 des SCM ist noch keine Absicherung für Windows 8 und Windows Server 2012 möglich. Microsoft dürfte hierfür jedoch eine neue Version veröffentlichen.

Neben Windows-Servern lassen sich aber auch andere Programme und Microsoft-Server-Systeme mit SCM absichern. Internet Explorer 8 und 9, Office 2007 sowie 2010 und Exchange Server 2007 und 2010 inklusive der aktuellen Service Packs unterstützen SCM. Das neue Office 2013 sowie Internet Explorer 10 werden aktuell noch nicht unterstützt, genauso wie Windows 8 und Windows Server 2012. Sie können SCM auch auf einer Arbeitsstation installieren, für den Betrieb ist kein Server oder Agent notwendig. Die Absicherung erfolgt komplett über eine Gruppenrichtlinieninfrastruktur. Alleinstehende Server können Sie aber auch absichern. Dazu lesen Sie die Richtlinien von SCM in eine lokale Sicherheitsrichtlinie ein. Damit Sie SCM verwenden können, müssen Sie das .NET Framework 4.0 [2] installieren. Installieren Sie außerdem die kostenlose Datenbank SQL Server 2008 R2 Express Edition [3], inklusive der Verwaltungstools, bevor Sie den Installationsassistenten von SCM starten.

Abischerung eines Servers

Anschließend richten Sie SCM auf Ihrem Rechner ein. Verwenden Sie am besten einen Rechner mit Windows 7 SP1 oder Windows Server 2008 R2 SP1. Nachdem Sie das Tool installiert haben, starten Sie es und lassen die Vorlagen der Richtlinien einlesen. Der Vorgang kann einige Minuten dauern. Auf der linken Seite wählen Sie anschließend das Produkt aus, das Sie absichern möchten. Sie können zum Beispiel auch für Windows Server 2008 R2 einzelne Serverrollen besonders absichern. Klicken Sie auf eine Baseline, sehen Sie im rechten Bereich, welche Einstellungen bereits gesetzt sind.

Um einen Server abzusichern, klicken Sie auf eine vorhandene Standard-Baseline und erstellen mit dem Befehl "Duplicate" im rechten Bereich eine Kopie der Vorlage. Die neue Richtlinie erscheint anschließend bei "Custom Baselines" im oberen Bereich der Konsole. Der nächste Schritt besteht darin, dass Sie die Einstellungen der Richtlinie an Ihre Bedürfnisse anpassen. Die meisten Einstellungen belassen Sie so wie sie sind, um den entsprechenden Server optimal abzusichern. Der Vorteil im Vergleich zu einer leeren Gruppenrichtlinie ist, dass alle Einstellungen in der Richtlinie bereits so gesetzt sind, wie sie Microsoft als optimal und sicher betrachtet.

Haben Sie alle Einstellungen vorgenommen, besteht der nächste Schritt darin,

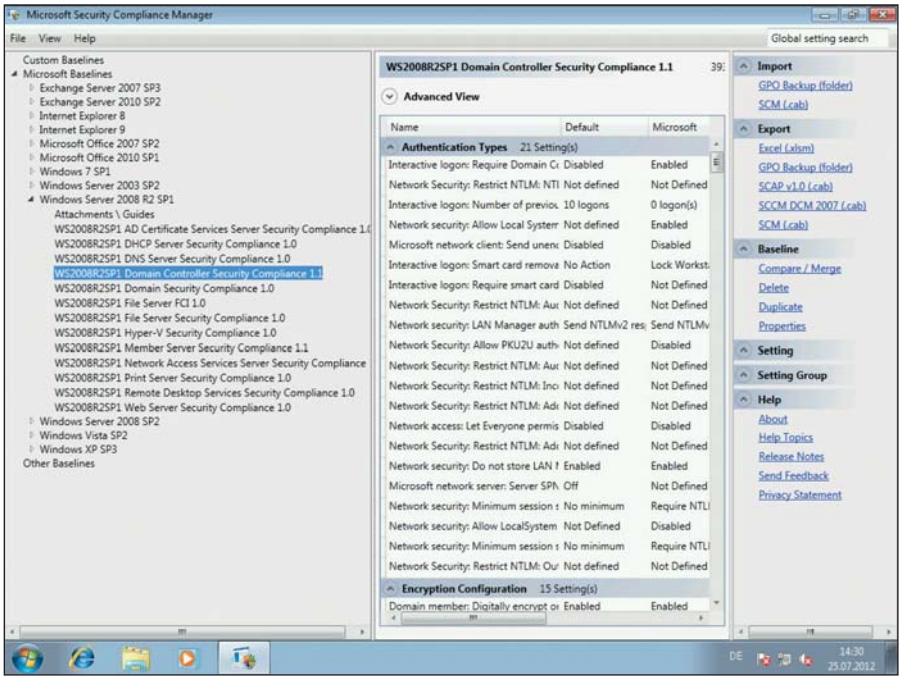


Bild 1: Der SCM zeigt die Einstellungen für eine Richtlinie übersichtlich an

dass Sie die Baseline als Gruppenrichtlinie exportieren. Sie können aber auch mit anderen Techniken die Richtlinie einlesen. Der Import als Gruppenrichtlinie ist aber am einfachsten für Active Directory-Domänen. Das Verzeichnis mit dem Export integrieren Sie später in der Gruppenrichtlinienverwaltungskonsole entweder als neue Richtlinie oder Sie integrieren die Einstellungen in eine bereits vorhandene Richtlinie. In eine bestehende Gruppenrichtlinie übernehmen Sie die Einstellungen durch Auswahl von "Einstellungen importieren" im Kontextmenü. Setzen Sie im Unternehmen System Center Configuration Manager ein, können Sie die Einstellungen aber auch in einem kompatiblen Format für SCCM exportieren und einlesen.

In SCM können Sie über den Bereich "Import" exportierte Gruppenrichtlinien aus dem Active Directory auch in SCM einlesen. Diese Richtlinien führen Sie dann später mit einer von Ihnen erstellten Richtlinie in SCM zusammen und exportieren diese Richtlinie wiederum. Mit der Gruppenrichtlinienverwaltung (GPMC) können Sie einzelne Gruppenrichtlinien sichern und wiederherstellen, ohne eine Datensicherung des Active Directory verwenden zu müssen. Da die Datensicherung von Gruppenrichtlinien in Dateien gespeichert wird, können Sie die Sicherung auch zum Erstellen neuer Gruppenrichtlinien verwenden.

GPO sichern und exportieren

Um eine Datensicherung einzelner oder aller Gruppenrichtlinien durchzuführen, klicken Sie in der GPMC auf den Knoten Gruppenrichtlinienobjekte. Dieser Knoten enthält alle Gruppenrichtlinien, die in dieser Domäne erstellt wurden. Klicken Sie mit der rechten Maustaste auf eine Gruppenrichtlinie und wählen Sie im Kontextmenü den Befehl "Sichern" aus. Bei der Sicherung von Gruppenrichtlinien werden die Einstellungen in eine Datei exportiert. Sie können auch direkt auf den Knoten "Gruppenrichtlinienobjekte" klicken und im Kontextmenü den Befehl "Alle sichern" auswählen, um sämtliche Gruppenrichtlinien einer Domäne auf einmal zu sichern. Danach erscheint ein Fenster, in dem Sie ein Verzeichnis auf der Festplatte auswählen und eine Beschreibung der Sicherung hinterlegen können. Wenn Sie die Eingaben bestätigen, beginnt der Sicherungsassistent mit der Datensicherung der Gruppenrichtlinie und speichert diese im ausgewählten Verzeichnis der Festplatte.

Um eine exportierte SCM-Richtlinie in eine Gruppenrichtlinie zu importieren, öffnen Sie den Gruppenrichtlinienverwaltungs-Editor und erstellen entweder eine neue GPO oder klicken mit der rechten Maustaste auf eine bestehende GPO. Wählen Sie danach "Einstellungen importieren" und navigieren Sie in das Verzeichnis, in das Sie die Einstellungen exportiert haben. Schließen Sie danach den Import-Vorgang ab. Klicken Sie auf eine Gruppenrichtlinie im Gruppenrichtlinienverwaltungs-Editor, lassen Sie sich auf der Registerkarte Einstellungen die neuen Einstellungen anzeigen. Um Gruppenrichtlinien von Active Directory in SCM zu integrieren, klicken Sie diese zunächst im Gruppenrichtlinienverwaltungs-Editor an und sichern Sie die Richtlinie. Kopieren Sie das Sicherungsverzeichnis auf den PC mit SCM und lassen Sie die Richtlinie importieren.

Setzen Sie kein Active Directory ein oder wollen Sie einen alleinstehenden Server absichern, haben Sie auch die Möglichkeit, die Baseline in eine lokale Sicherheitsrichtlinie zu integrieren. Dazu verwenden Sie das Befehlszeilen-Tool LocalGPO aus der Programmgruppe Microsoft Security Compliance Manager. Mit diesem lassen sich Einstellungen lokal aus SCM in eine Richtlinie auf dem Server importieren.

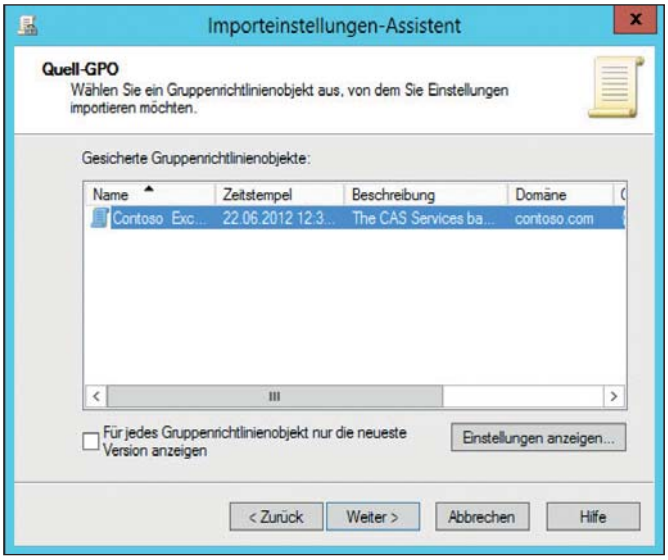


Bild 2: Das Importieren von Einstellungen des SCM in eine neue Gruppenrichtlinie geschieht über einen Assistenten

Nutzen Sie mehrere Baselines, können Sie diese auch miteinander vergleichen oder in eine gemeinsame Baseline zusammenführen. Dazu verwenden Sie den Menüpunkt "Compare / Merge" in der Verwaltungsoberfläche des SCM. Wählen Sie dort aus, mit welcher Baseline Sie die aktuell ausgewählte Baseline vergleichen möchten. Sie können hier auch selbst erstellte Baselines mit den Standardbaselines vergleichen. Auf diesem Weg sehen Sie die Unterschiede zwischen den Baselines. Sind Baselines miteinander kompatibel, können Sie auf diesem Weg mit "Merge Baselines" die Einstellungen zusammenführen. Diese Einstellungen wiederum können Sie exportieren und in eine GPO importieren. Während der Zusammenführung erstellen Sie eine neue Baseline, deren Namen Sie im Assistenten angeben.

Um eine bessere Übersicht zu erhalten oder einzelne Einstellungen in produktive Umgebungen nicht zu übernehmen, klicken Sie diese in der Baseline an und wählen dann im rechten Bereich "Delete". Auf diese Weise entfernen Sie Einstellungen aus der Baseline. Über "Add" können Sie Einstellungen auch wieder hinzufügen. Mit "Lock" verhindern Sie die Möglichkeit, Einstellungen für eine Baseline zu ändern, die Bearbeitung aktivieren Sie dann wieder mit "Edit".

Sichere Einstellungen: Security Configuration Wizard

Mit dem integrierten Sicherheitskonfigurations-Assistenten (Security Configuration Wizard, SCW) in Windows Server 2008 R2 können Sie ebenfalls Server absichern. Der Assistent deaktiviert verschiedene Systemdienste sowie Registry-Einträge und setzt Firewall-Einstellungen. Neben den Standardrollen bietet Microsoft auch Erweiterungen für die verschiedenen Serverdienste an. Der Sicherheitskonfigurations-Assistent dient der Absicherung eines Servers über einen Assistenten, der Sicherheitsrichtlinien anwendet. Änderungen, die der SCW an einem System durchführt, können Sie leicht auch wieder rückgängig machen. Der SCW verfügt über einen integrierten Assistenten, mit dem sich die Einstellungen eines Servers einfach steuern lassen.

Microsoft hat in den Security Configuration Wizard eine automatische Erkennung von Microsoft-Serverdiensten eingebaut. Zusätzliche Serverdienste binden Sie über Manifeste ein, wie im Fall von SharePoint Server 2010. Diese können Sie entweder direkt bei Microsoft herunterladen oder die Dateien befinden sich im Installationsordner der entsprechenden Lösung. Mit dem kostenlosen SharePoint 2010 Administration Toolkit [4] erhalten Sie die entsprechende Datei für SharePoint. Das Manifest des Sicherheitskonfigurations-Assistenten fügt SharePoint zum Sicherheitskonfigurations-Assistenten (SCW) von Windows Server 2008 x64 SP2 oder Windows Server 2008 R2 hinzu.

Sichern Sie einen Server mit dem SCW ab, arbeiten Sie hauptsächlich mit der grafischen Oberfläche des Programms. Das Befehlszeilentool Scwcmd dient zum Automatisieren des SCW. Mit diesem Tool können Sie Skripte erstellen und damit mehrere Server mit einer Sicherheitsrichtlinie versorgen. Damit lassen sich auch Richtlinien wieder rückgängig machen, wenn Probleme auftreten. Sie finden im Ordner "C:\ Windows \ Security \ Msscw \ KBs" eine Sammlung von XML-Dateien. Diese Dateien enthalten alle wichtigen Informationen über Dienste, Serverrollen und Ports, mit deren Hilfe Sie den Server absichern können.

Um Microsoft SharePoint 2010 in den SCW einzubinden, müssen Sie zunächst das Administration Toolkit installieren. Anschließend registrieren Sie die Manifestdateien zur Absicherung:

1. Öffnen Sie eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den folgenden Befehl *cd C:\Programme\Microsoft\SharePoint 2010 Administration Toolkit\SCWManifests* ein.
3. Verwenden Sie Windows Server 2008 Service Pack 2, geben Sie *scwcmd register /kbname:SPF2010 /kbfile:SPF2010W2K8.xml* ein.
4. Setzen Sie Windows Server 2008 R2

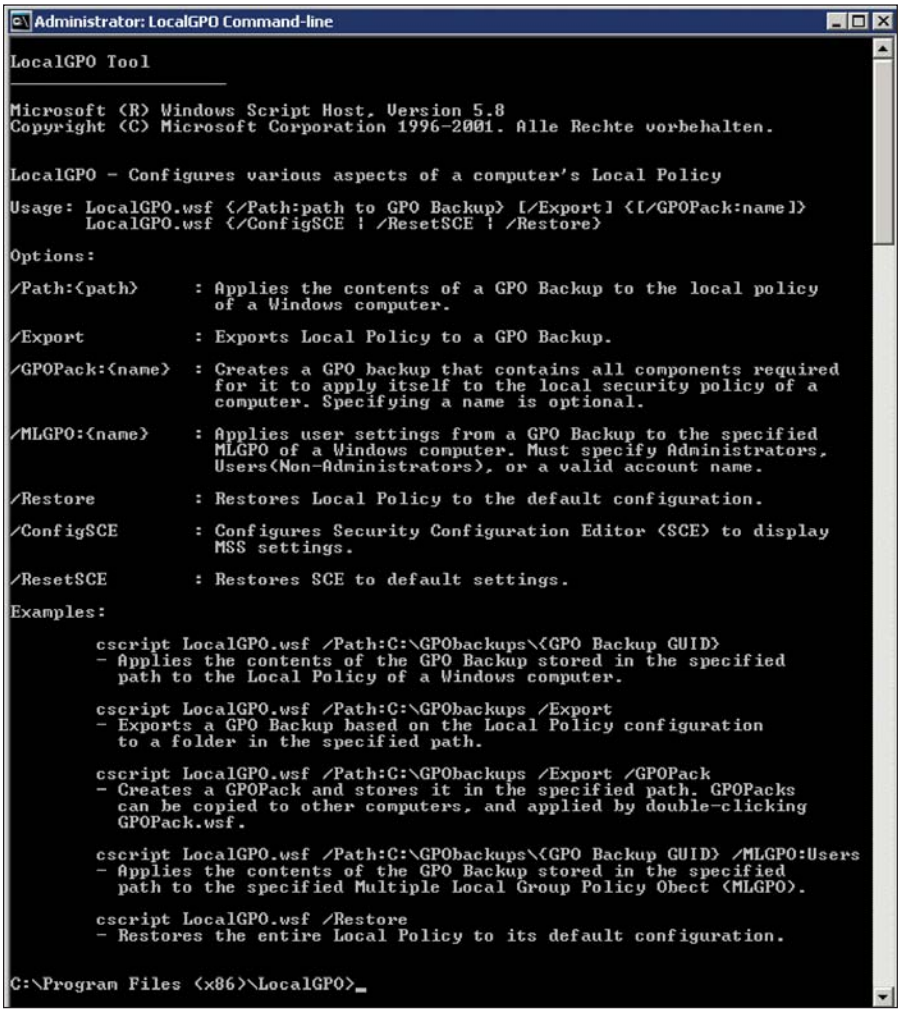


Bild 3: Auch über die Kommandozeile ist das Einlesen von Richtlinien möglich

ein, dann tippen Sie *scwcmd register /kbname:SPF2010 /kbfile:SPF2010W2K8R2.xml* ein.

Die letzten beiden Befehle enthalten die Sicherheitseinstellungen für SharePoint Foundation 2010. Um auch die Funktionalitäten von SharePoint Server 2010 zu unterstützen, müssen Sie weitere Dateien integrieren. Setzen Sie Windows Server 2008 Service Pack 2 ein, verwenden Sie als Nächstes die folgenden Kommandos:

```
scwcmd register /kbname:MSS2010
  /kbfile:MSS2010W2K8.xml
```

Beim Einsatz von Windows Server 2008 R2 nutzen Sie

```
scwcmd register /kbname:MSS2010
  /kbfile:MSS2010W2K8R2.xml
```

Nach dieser Maßnahme können Sie Richtlinien für SharePoint 2010 erstellen, um den Server abzusichern. Haben Sie auf einem Server eine Sicherheitsrichtlinie erstellt und abgespeichert, können Sie diese auf einem anderen Server mithilfe des SCW importieren. Nach dem Start des SCW fragt der Assistent, ob er eine bestehende Richtlinie importieren, eine neue Richtlinie erstellen, eine vorhandene Richtlinie vor dem Importieren bearbeiten oder schließlich die Durchführung der letzten Richtlinie zurücknehmen soll. Sie starten den SCW über den Server-Manager. Klicken Sie im Bereich "Serverübersicht / Sicherheitsinformationen" auf "Sicherheitskonfigurations-Assistenten ausführen".

Die Konfiguration der Sicherheitsrichtlinie unterteilt sich in unterschiedliche

Bild 4: Der Sicherheitskonfigurations-Assistent ermöglicht auch das Starten des SCW in Windows Server 2008 R2

Bereiche. Sie sollten in jedem Fenster genau überprüfen, ob der Assistent alle Dienste und Funktionen erkannt hat. Sie können jederzeit einzelne Punkte aktivieren oder deaktivieren. Nach dem Start erstellen Sie zunächst eine neue Sicherheitsrichtlinie, wählen den Server aus und wechseln zur Seite Serverrollen auswählen. Der erste Bereich, den Sie konfigurieren, ist die rollenbasierte Konfiguration. Hier untersucht der Assistent die einzelnen Dienste und Funktionen des Servers und teilt diese den Rollen zu, die in der Sicherheitskonfigurationsdatenbank hinterlegt sind. Auch wenn Sie hier falsche Eingaben machen und diese später anwenden, sollte kein Problem auftreten, da Sie die Richtlinie jederzeit wieder deaktivieren können. Um Sie als Administrator bei der Auswahl von Serverrollen zu unterstützen, hat Microsoft in SCW für jede verfügbare Rolle eine Beschreibung hinterlegt, die helfen soll, entsprechende Rollen eindeutig zuzuordnen.

Sie können die Anwendung einer Sicherheitsrichtlinie wieder zurücknehmen. Auch diesen Vorgang nehmen Sie über den SCW vor. Wenden Sie die Richtlinie sofort an, führt der SCW die XML-Datei aus und legt die eingestellten Sicherheitsvorgaben fest. Nach Abschluss der Anwendung müssen Sie den Server neu starten. Am besten erstellen Sie eine Sicherheitsrichtlinie in einer Testumgebung und speichern diese ab. Die abgespeicherte Sicherheitsrichtlinie können Sie dann entweder manuell über die grafische Oberfläche installieren oder per Batchdatei und Befehlszeilentool Scwcmd verteilen lassen. Um eine Richtlinie lokal anzuwenden, geben Sie den Befehl

```
scwcmd configure /p:Pfad zur
  XML-Datei
```

ein. Um eine Sicherheitsrichtlinie auf einem Remotecomputer ausführen zu können, verwenden Sie ebenfalls das Befehlszeilentool Scwcmd. Nutzen Sie dazu in der Eingabeaufforderung den Befehl

```
scwcmd configure /m:IP-Adresse oder
  Name des Remoteservers /p: Pfad
  zur XML-Datei
```

Tippen Sie in der Eingabeaufforderung *scwcmd configure* ein, erhalten Sie weitere Informationen über die Anwendung des Sicherheitskonfigurations-Assistenten über die Eingabeaufforderung.

Haben Sie auf einem Server eine Sicherheitsrichtlinie angewendet, sehen Sie zunächst keine Änderung. Eine Analyse führen Sie wieder am besten mit dem Befehlszeilentool Scwcmd durch. Greifen Sie dazu in der Eingabeaufforderung auf den Befehl

```
scwcmd analyze /m: IP oder Name des
  Servers /p: Pfad zur Richtlinienda-
  tei /o: Ausgabeordner der Analyse
```

zurück. Die Analyse erstellt eine XML-Datei, welche die Änderung der Richtlinie enthält. Haben Sie die Datei geschaffen, können Sie entweder die XML-Datei betrachten oder über den Befehl *scwcmd view /x:Name der erstellten XML-Datei* die Anzeige durch den SCW formatieren und anzeigen lassen.

Möchten Sie die Ausführung einer Sicherheitsrichtlinie wieder vollständig zurücknehmen, können Sie entweder wieder über die grafische Oberfläche die Maßnahme durchführen oder über die Eingabeaufforderung die Sicherheitsrichtlinie zurücknehmen. Um die Sicherheitsrichtlinie über die grafische Oberfläche zurückzunehmen, starten Sie den Sicherheitskonfigurations-Assistenten. Wählen Sie die Option "Rollback für letzte angewendete Sicherheitsrichtlinie durchführen" aus. In diesem Fall wird die letzte Sicherheitsrichtlinie komplett zurückgenommen. Hatten Sie zuvor keine Sicherheitsrichtlinie durchgeführt, erhalten Sie exakt den Stand vor der Einführung der Richtlinie. Alternativ können Sie auch eine Sicherheitsrichtlinie in der Eingabeaufforderung zurücknehmen. Verwenden Sie dazu in der Eingabeaufforderung den Befehl

```
scwcmd rollback /m:Name oder IP
  des Servers
```

Angriffsfläche mit Attack Surface Analyzer und Baseline Security Analyzer verkleinern

Ein weiteres Tool, um Server im Netzwerk abzusichern, ist der Microsoft Attack Surface Analyzer [5]. Das Tool scannt den lokalen Computer auf Sicherheitslücken. Haben Sie die Überprüfung abgeschlossen, lassen Sie im nächsten Schritt einen Bericht erstellen. Dazu liest der Analyzer die erstellten CAB-Dateien der einzelnen Scanvorgänge ein und erstellt einen Bericht. Nach der Installation startet das Tool zunächst einen "baseline"-Scan. In weiteren "product"-Scans überprüft das Tool, ob nach der Installation von Anwendungen Unterschiede vorhanden sind. Den Bericht zeigt das Tool im Browser an. Über verschiedene Schaltflächen und Unterteilungen in Sektionen sehen Sie, wie Sie die Sicherheit im System verbessern.

Der Microsoft Baseline Security Analyzer (MBSA) 2.2 scannt einzelne Computer, IP-Bereiche oder Domänen auf Windows-Computer. Verfügen Sie über Administratorberechtigungen, scannt das Tool alle PCs auf fehlende Patches, Sicherheitslücken und fehlerhafte Sicherheitskonfigurationen. Laden Sie das Tool von der Microsoft-Seite [6], installieren Sie es und scannen Sie den gewünschten IP-Bereich. Anschließend erhalten Sie einen umfassenden Bericht, welche Patches auf den Computern fehlen und wie Sie die Sicherheit der Computer erhöhen.

Nach der Installation können Sie über die Option "Mehrere Computer überprüfen" das gesamte Netzwerk nach fehlenden Patches und kritischen Sicherheitslücken durchsuchen. Nachdem Sie diese Option ausgewählt haben, geben Sie entweder einen IP-Bereich oder eine Domäne an, die auf Sicherheitslücken untersucht werden soll. Aktivieren Sie den Scanvorgang per Klick auf die Schaltfläche "Suche starten", lädt der MBSA zunächst aktuelle Sicherheitsinformationen aus dem Internet herunter. Danach beginnt das Tool, den konfigurierten IP-Bereich nach Sicherheitslücken zu durchsuchen.

Im Anschluss zeigt das Tool einen detaillierten Bericht über die fehlenden Aktualisierungen und Sicherheitslücken an. Aus diesem Bericht lässt sich ein Maßnahmenkatalog erarbeiten, zum Beispiel die Einführung der Windows Server Update Services 3.0. Der Scanvorgang des MBSA kann durchaus einige Minuten oder sogar Stunden dauern, abhängig von der Anzahl der Rechner, die im konfigurierten Subnetz integriert sind. Die Berichte werden gespeichert und können über das Startfenster des MBSA jederzeit erneut angezeigt werden. Zu jedem Überprüfungspunkt zeigt der MBSA eine Detailansicht an. Gibt es Probleme oder findet der MBSA Sicherheitsgefahren, erhalten Sie einen Hinweis zur Lösung des Problems für jeden einzelnen Rechner.

Fazit

Microsoft stellt mit dem Security Compliance Manager ein hilfreiches Werkzeug zur Verfügung. Mit ihm sind Sie in der Lage, Gruppenrichtlinien zur Absicherung Ihrer Server zu verwenden – und das in einer übersichtlichen Art und Weise. Bedienen lässt sich das Tool nicht nur über die GUI, sondern auch via Kommandozeile und Skripte. Damit automatisieren Sie bei Bedarf viele Vorgänge. In Kombination mit dem Attack Surface Analyzer und dem Baseline Security Analyzer sorgen Sie so für ein deutliches Plus an Sicherheit in Ihrer Windows-Umgebung. *(dr)*

Link-Codes

[1] Security Compliance Manager herunterladen
COP41

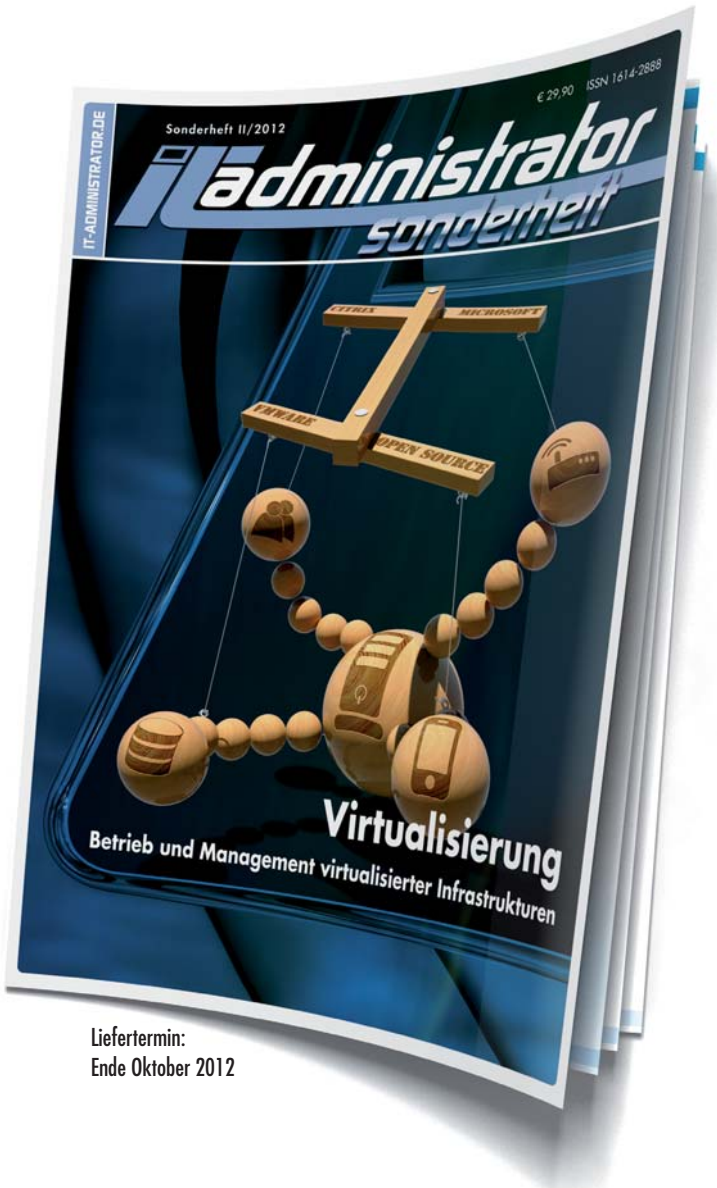
[2] .NET Framework 4.0 herunterladen
COP42

[3] Datenbank SQL Server 2008 R2 Express Edition
COP43

[4] SharePoint 2010 Administration Toolkit
COP44

[5] Microsoft Attack Surface Analyzer herunterladen
COP45

[6] Microsoft Baseline Security Analyzer herunterladen
COP46



Liefertermin:
Ende Oktober 2012

Bestellen Sie jetzt

das IT-Administrator

Sonderheft II/2012!

180 Seiten Praxis-Know-how rund um das Thema

Virtualisierung

Betrieb und Management virtualisierter Infrastrukturen

zum Abonnenten-Vorzugspreis von*

nur € 24,90!

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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____ BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

ITA 0712

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

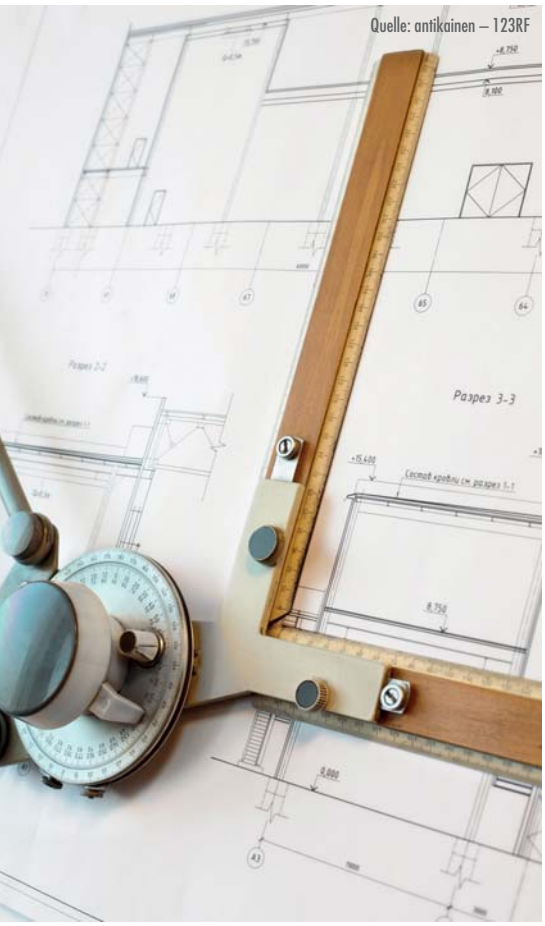
Heinemann Verlag
Leopoldstraße 85
D-80802 München
Tel: 089-4445408-0
Fax: 089-4445408-99
Geschäftsführung:
Anne Kathrin Heinemann
Matthias Heinemann
Amtsgericht München HRB 151585

Microsoft Active Directory sicher aktualisieren

Der Plan macht den Unterschied

von Fabian Müller und Nils Kaczenski

Seit seinem Erscheinen mit Windows 2000 entwickelt sich der Verzeichnisdienst Active Directory ständig weiter und erhält neue Funktionen und Möglichkeiten. Bei der Integration eines neuen Domänencontrollers mit einem höheren Betriebssystemstand können daher beispielsweise bei den Applikationen Komplikationen auftreten. Ein Migrationsplan vermeidet solche Probleme und stellt die neuen Funktionen sauber bereit. Dieser Artikel führt Schritt für Schritt durch die notwendigen Planungs- und Update-Prozesse.



Mit Windows Server 2012 führt Microsoft bereits die fünfte große Version seines Verzeichnisdienstes Active Directory (AD) ein. Verglichen mit anderen Komponenten des Betriebssystems hat sich das AD über die Jahre nur behutsam weiterentwickelt; insbesondere hat der Hersteller auf Kompatibilität Wert gelegt. Gleichwohl gibt es viele Funktionen, die den Umstieg auf das aktuelle Server-Windows sinnvoll machen, etwa den AD-Papierkorb in Windows Server 2008 R2.

Es reicht allerdings nicht aus, einfach einen Server mit dem neuesten Windows zu installieren und als Domänencontroller (DC) in die Domäne zu bringen. Vorher müssen Sie das AD vorbereiten, damit Alt und Jung sich auch verstehen. Auch wenn das insgesamt gut beherrschbar ist, sollten Systemverwalter in größeren Umgebungen sorgfältig planen und testen.

Plane und prüfe

Eine Aktualisierung des Active Directory erfolgt nicht als Selbstzweck, sondern etwa um dessen Betrieb effizienter zu gestalten oder um verschiedene Anwendungen und Ressourcen zu integrieren. Zuerst sollte das IT-Management daher eine "Vision" erarbeiten, aus der sich langfristige Ziele für die gesamte IT ableiten lassen. Viele Firmen sehen die IT mittlerweile als internen Dienstleister an, der seine Dienste an den Geschäftsprozessen des Auftraggebers beziehungsweise Kunden orientiert. Aus den Anforderungen des Kunden entsteht so ein Pflichtenheft, anhand dessen Sie die Umsetzung der AD-Migration planen können. Bei der Migration ist nicht der Weg das Ziel – vielmehr geht es um die Umsetzung konkreter Anforderungen: Neue Funktionen lassen sich sinnvoll einsetzen, wenn sie nicht zufällig, sondern geplant ins Haus kommen.

Neue Domänencontroller geben einen guten Anlass, die Struktur des Netzwerks zu überprüfen. Häufig sind frühere Entscheidungen über den Aufbau der Serverlandschaft im Unternehmen auf der Basis von Vorgaben getroffen worden, die heute nicht mehr zutreffen. Bisweilen hatten ältere Betriebssysteme auch Beschränkungen, die in den neueren Fassungen überwunden sind.

Besonders deutlich wird dies, wenn wir die Vorsichtsmaßnahmen betrachten, die Microsoft in der ersten Version des AD in Windows 2000 getroffen hatte. Der technische Aufbau entsprach den damaligen Infrastrukturen, die auf 10 MBit-Netzwerken und langsamen WAN-Verbindungen beruhten. So war es in der Frühzeit des AD üblich, den Verzeichnisdienst mit mehreren hierarchisch angeordneten Domänen zu planen, weil der Vorgänger Windows NT noch kein Standort-Konzept kannte und auch nur vergleichsweise wenige Objekte in einer Domäne verwalten konnte. Heute lautet die verbreitete Empfehlung, stets von einer Einzeldomäne aus zu planen und nur in sehr speziellen Situationen einen Tree oder Forest aus mehreren Domänen aufzubauen [1].

Auch die Verteilung des Netzwerks auf mehrere Lokationen erfordert heute weder separate Domänen noch eine Vielzahl lokaler DCs. Durch AD-Standorte ("Sites") lässt sich der Replikationsverkehr gut steuern, und ein eigener DC ist in einer kleinen Niederlassung meist unnötig. Seit Windows Server 2008 steht mit dem "Read-Only Domain Controller" (RODC) eine Alternative für Außenstellen bereit, die ein höheres Sicherheitsniveau bietet, falls die Server vor Ort nicht ausreichend zugangsgesichert sind.

Schon mit Windows Server 2003 hatte Microsoft einige Bremsen aus dem System

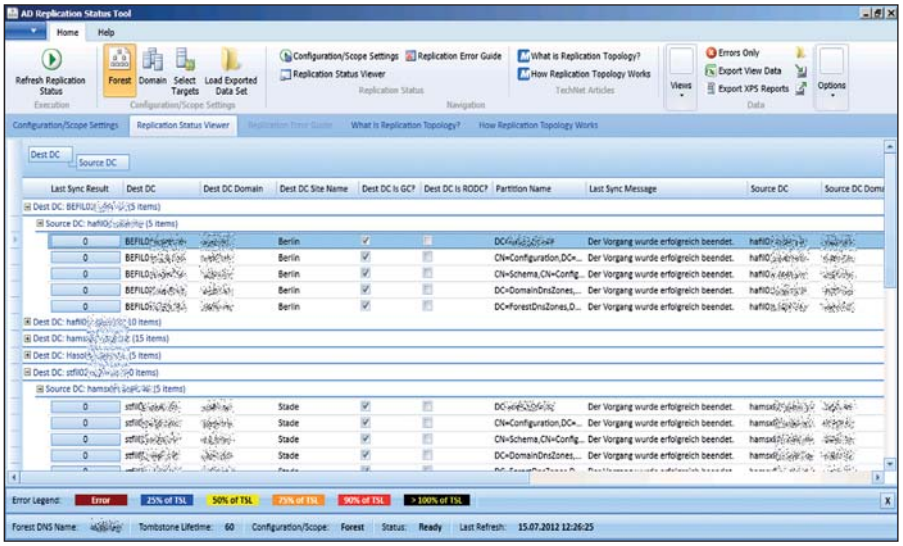


Bild 1: Sauber übertragen: Das kostenlose "AD Replication Status Tool" von Microsoft zeigt den Zustand der AD-Replikation in einer grafischen Konsole. Sollten Fehler bestehen, liefert es Hinweise zu deren Behebung.

entfernt, die sich angesichts besserer WAN-Verbindungen als unnötig erwiesen hatten. Seit damals läuft die Replikation innerhalb eines LAN und auch über WAN-Strecken deutlich fixer. Zudem sind vormals ausgesprochene Empfehlungen zur Rollenverteilung mehrerer DCs überholt: Es spricht in der Regel nichts mehr dagegen, alle Betriebsmaster-Rollen (Flexible Single Master Operations, FSMO) auf einem einzigen DC zu konzentrieren. Gleichfalls wird heute auf allen DCs der Globale Katalog aktiviert, weil der (meist überschaubare) zusätzliche Datenverkehr nicht mehr ins Gewicht fällt.

Dank der 64 Bit-Technik können Domänencontroller mit großem RAM die AD-Datenbank oft vollständig im Arbeitsspeicher halten und auch Such- und Anmeldevorgänge sehr schnell ausführen. Dabei reichen in den meisten mittelständischen Umgebungen 2 oder 4 GByte RAM völlig aus. Große Netzwerke geben den DCs 8 GByte oder mehr und erreichen so eine deutlich geringere Zahl an Servern als früher. Netzwerke mit vierstelliger Benutzerzahl lassen sich bezüglich der Last heute durchaus mit zwei DCs betreiben, mehr Server erhöhen dann die Ausfallsicherheit zusätzlich.

Zusammenfassend empfiehlt es sich, bei einem AD-Upgrade die bestehende Struktur nicht einfach zu übernehmen, sondern sie mit dem Ziel der Konsolidierung zu überprüfen. Dabei sollten Sie auch gleich die Empfehlung berücksichtigen, dass ein DC keine weiteren Dienste betreibt: Es erleichtert viele Wartungs- und Troubleshooting-Vorgänge, wenn ein DC nur das AD, DNS sowie bei Bedarf WINS ausführt. So ist ein Neustart oder Austausch ohne Rücksicht auf weitere Abhängigkeiten möglich.

Test im Labor – aber richtig!

Bevor es an die technische Umsetzung in der Produktionsumgebung geht, empfiehlt sich insbesondere in größeren IT-Umgebungen der Aufbau der zukünftig geplanten Umgebung in einem Testlabor, dessen Konfiguration dem Produktionsnetz entspricht. Hier können Sie nicht nur die notwendigen Prozesse zur Umstellung vorbereiten, sondern auch eigene Dienste und Anwendungen mit dem neuen Betriebssystem, seinen neuen Funktionen und Konfigurationen testen. Besonderes Augenmerk erhalten die sogenannten "Line-of-Business-Anwendungen" (LOB), ohne die eine Produktion nicht denkbar ist. Ohne diese Vorab-Tests stellt die Einführung eines neuen Betriebssystems immer ein Risiko für die Produktionsumgebung dar.

Die Realisierung eines Testlabors weitet sich schnell zu einem eigenständigen Projekt aus. Für das Active Directory ist vom simplen "Klonen" der Produktionsumgebung – etwa durch VM-Kopien der Domänencontroller – dringend abzuraten. Zwei der wichtigsten Gründe lauten: Kommt die geklonte Domäne mit dem realen Netzwerk in Berührung, kann dies zum Verlust der Produktions-Domäne führen, wenn sich etwa Löschvorgänge oder Konfigurationsfehler aus der Testumgebung durch einen Unfall in die Realumgebung replizieren. Zusätzlich ist die AD-Sicherheit gefährdet, da im Klon ja eine Kopie der AD-Datenbank läuft. Hieraus ergeben sich ernste Risiken, da alle Kennwörter in der Testumgebung identisch sind, Administrations- und Dienstkonten offenliegen und auch ein direkter Zugriff auf die AD-Datenbank möglich ist.

Besser ist es, die Umgebung in ihren wichtigsten Parametern für das Testlabor nachzubilden. Einen guten Startpunkt dafür schaffen die Skripte *CreateXMLFromEnvironment.wsf* und *CreateEnvironmentFromXML.wsf* aus den "GPMC Sample Scripts" [3], die OU-Strukturen, Benutzer, Gruppen und Gruppenrichtlinien aus dem Produktions-AD in eine Testumgebung exportieren. Vor allem sind die eigenen Applikationen und Dienste ins Testlab zu übertragen – denn genau für diese ist der Test da.

Neue Funktionen im Active Directory

Das Active Directory hat über die Jahre dazugelernt. Die folgende Liste nennt Beispiele neuer Funktionen; eine umfangreichere Übersicht finden Sie unter [2].

Windows Server 2008

- Active Directory lässt sich beenden und starten, ohne den Domänencontroller herunterzufahren
- Die "Active Directory Federation Services" zentralisieren die Anmeldung an Cloud-Diensten
- Durch "Fine-Grained Password Policies" lassen sich verschiedene Kennwortrichtlinien innerhalb einer Domäne umsetzen
- "Read-Only Domänencontroller" sind abgesicherte Server für Außenstellen

Windows Server 2008 R2

- Aus dem "AD-Papierkorb" lassen sich gelöschte Objekte ohne aufwändiges Recovery wiederherstellen
- "Managed Service Accounts" übernehmen die automatische Kennwortverwaltung für Dienstkonten

Windows Server 2012

- Das Active Directory unterstützt Snapshots von virtuellen Domänencontrollern
- Virtuelle Domänencontroller lassen sich klonen
- Mit "Claims-Based Access Control" lassen sich flexible Berechtigungsstrukturen aufbauen

Abhängigkeiten vom AD ermitteln

Um einen Eindruck zu bekommen, welche Anwendungen und Dienste des produktiven Netzwerks "AD-Konsumenten" sind, sollten Sie gemeinsam mit den Geschäftsbereichen des Unternehmens eine Bestandsanalyse der Applikationslandschaft durchführen. Welche Abhängigkeiten gibt es vom Active Directory (Protokolle, Dienstkonten, Datenquellen und so weiter) und wer ist verantwortlich für die Anwendungen und Dienste?

Zusätzlich ist die Information wertvoll, ob es bereits Testmatrizen für die Funktionen einer Anwendung gibt. Hier kommt es auf die Kernfunktionen der Applikation insbesondere beim Zugriff auf AD an, die anhand eines Testplans Schritt für Schritt oder besser noch automatisiert im Testlabor abgearbeitet werden. Häufig stellt sich in diesem Kontext dann auch die Frage, ob bestimmte Anwendungen überhaupt noch erforderlich sind. Außerdem ist es ratsam, die eigenen Programme und Prozesse zur AD-Administration mit in die Vorbetrachtung aufzunehmen:

- Sind zum Beispiel die Werkzeuge von Drittherstellern mit der neuen Active Directory-Version kompatibel?
- Ergeben sich durch das Upgrade auch Änderungen in den Microsoft-Werkzeugen zur AD-Verwaltung?
- Gibt es unter Umständen Abhängigkeiten von bestimmten Skripten?
- Ist ein Monitoring der AD-Dienste vorhanden und sind die jeweiligen Management Packs für die neuen Systeme verfügbar und getestet?

Auch können sich Programme komplett verändert haben – Beispiele hierfür sind die Windows-eigenen Backup-Programme in Windows Server 2003 und Windows Server 2008 (NTBackup vs. Windows Server Backup). Die Datensicherung mit Bordmitteln muss der Admin in diesem Fall neu aufbauen, die alten Mittel funktionieren nicht mehr.

Gesundheit des AD prüfen

Sind die organisatorischen Fragen geklärt, geht es im Projektplan mit der technischen Umsetzung weiter. Vor jeder Migration sollten Sie sich fragen, wie gesund

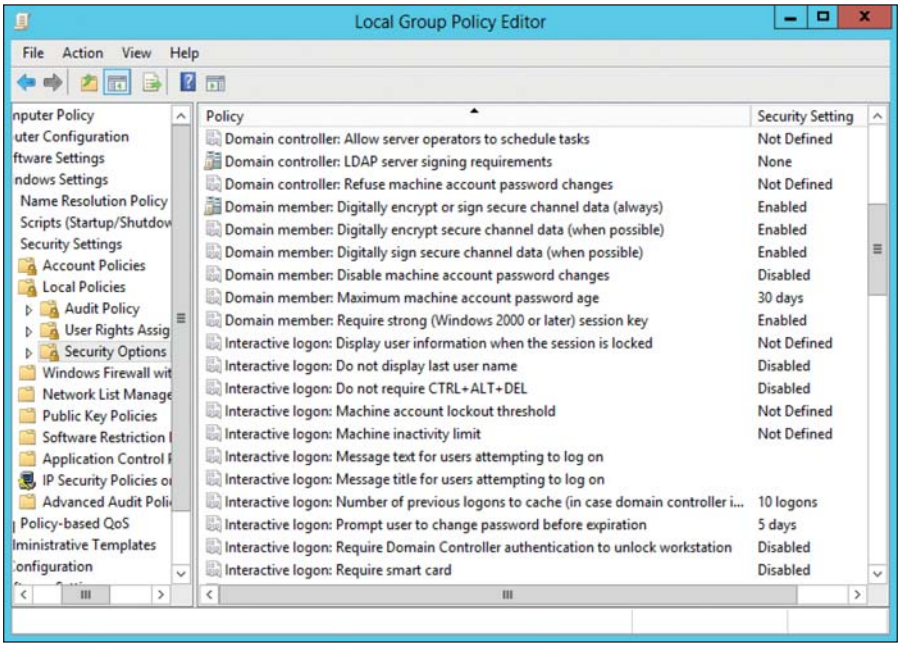


Bild 2: Die Domänen-Sicherheit lässt sich per Gruppenrichtlinie gezielt einstellen. Im Zuge der AD-Analyse vor dem Update empfiehlt sich eine Kontrolle, ob die Vorgaben noch dem Bedarf entsprechen.

Ihre Active Directory-Umgebung ist. Diese Frage sollten Sie sich eigentlich nicht erst vor einer Migration stellen – jedoch ist dieser Zeitpunkt günstig, noch einmal ganz genau auf das AD zu schauen.

Windows-Bordmittel wie "DCDiag", "Repadmin" und die Ereignisprotokolle sind Quellen erster Wahl für eine Bestandsanalyse, genauso wie zusätzliche Programme wie "Ultrasound" [4] zur Überwachung des File Replication Service (FRS) oder das "Active Directory Replication Status Tool" [5]. In der Königsklasse finden sich dann Lösungen wie der "System Center Operations Manager" von Microsoft oder ähnliche Dienste, die tiefgreifende Analysefunktionen bieten. Zusätzlich ist eine Dokumentation der AD-Umgebung empfehlenswert, beispielsweise mit den beiden Skript-Werkzeugen "José" [6] und "Borg" [7]. Auch wenn es selbstverständlich ist: Fehler in der Umgebung müssen Sie vor einer Migration beheben!

Neuen Domänencontroller planen

Als Nächstes steht die Definition der Basisinstallation für die neuen Domänencontroller an. Diese Festlegung von Details zu Partitionierung, Installationsverfahren, Konfigurationen, Treiberständen, Patchlevel, installierten (Dienst-)Programmen et cetera dient der Standardisierung der neuen Systeme. Standardisierung ist nicht nur ein Schlagwort – vielmehr ist es der Weg hin zu einer stabilisierten Umgebung, Automatisierung als auch vereinfachtem Troubleshooting. Welche Komponenten eine solche Basiskonfiguration enthält, orientiert sich an den vorab ermittelten Anforderungen. Dabei sollte die Definition langfristigen Bestand haben und nicht einfach wieder aufgeweicht werden.

Im Zuge der Basiskonfiguration ist es notwendig zu prüfen, ob Zusatzprodukte für die Domänencontroller mit dem neuen Betriebssystem kompatibel sind und vom Hersteller unterstützt werden. So gibt es häufig beispielweise mit Anti-Viren-Scannern oder anderer Filtertreibersoftware Probleme. Apropos AV-Scanner: Die Scan-Ausschlussliste [8] für Windows-Betriebssysteme ist einen Blick wert – sie gibt an, welche Dateien der Scan auslassen sollte. Wichtig ist hier, zuerst zu prüfen, ob Ausschlüsse überhaupt notwendig sind. Die Hersteller der AV-Lösungen sollten solche Fragen beantworten können. Wenn es jedoch notwendig wird, Ausschlüsse vorzunehmen, sollte dies immer nur auf Dateibasis erfolgen, nie auf Verzeichnisbasis. Letzteres öffnet Schadsoftware Tür und Tor.

Vorgehen bei der DC-Migration

Um den ersten DC mit einem neuen Betriebssystem in die Domäne beziehungsweise den Forest einzubinden, sind einige

Vorbereitungen nötig. Das betrifft vor allem das AD-Schema, also die Definition der Datenbank für neue Objektklassen und Attribute, denn jede neue Windows-Version erweitert die Möglichkeiten des AD. Daneben sind einige weitere Anpassungen notwendig. Diese Vorgänge sind unabhängig davon, ob Sie als ersten "neuen" DC einen vorhandenen Server aktualisieren oder eine neue Maschine aufsetzen.

Bereits seit Windows Server 2003 ist für diese Änderungen das Dienstprogramm *adprep.exe* zuständig, das auf der jeweils aktuellen Windows-Server-DVD enthalten ist. Kopieren Sie das Verzeichnis stets auf den Server, auf dem Sie das Tool ausführen wollen, um DVD-Lesefehler zu vermeiden. Das Schema-Update muss auf dem Schema-Master des Forests stattfinden, den Sie mit folgendem Kommando identifizieren:

```
netdom /query fsmo
```

Im Web finden sich oft Hinweise, dass Sie vor dem Schema-Update den Schema-Master isolieren sollen. Davon ist allerdings abzuraten, denn diese scheinbare Vorsichtsmaßnahme führt eher zu Problemen. Zwar kann Adprep auf Fehler laufen, doch die lassen sich stets beheben.

Melden Sie sich mit einem Konto an, das Mitglied der Gruppe Schema-Admins ist. Sollte der Schema-Master noch mit einer 32 Bit-Version von Windows laufen, dann nutzen Sie im Folgenden das Kommando *adprep32.exe*, bei 64 Bit-Servern hingegen *adprep.exe*. Das erste Kommando lautet:

```
adprep.exe /forestprep
```

Es führt die Schema-Erweiterungen aus, was ein paar Minuten dauern kann. Die folgenden Kommandos führen Sie dann einzeln in jeder Domäne des Forests aus, falls es mehrere gibt.

```
adprep.exe /domainprep /gpprep
adprep.exe /rodcprep
```

Je nachdem, in welchem Zustand sich die Domänen befinden, sind nicht alle Kommandos notwendig, es führt aber nicht zu Fehlern, wenn Sie sie dennoch aufrufen. Eine Besonderheit: In Windows Server 2012 ist Adprep in den Server-Manager integriert, der es bei Bedarf von selbst ausführt. Die 32 Bit-Variante ist hingegen dort gar nicht mehr vorhanden.

Sicherheitseinstellungen neuer Domänencontroller

Microsoft hat schrittweise mit neuen Betriebssystemen die Sicherheitsvorgaben verschärft, was sich natürlich auch auf die Kompatibilität vorhandener Clients und Applikationen auswirkt. Die folgende Auswahl nennt einige Beispiele; eine umfangreichere Liste finden Sie unter [2]:

- Kerberos DES-Verschlüsselung standardmäßig deaktiviert, wodurch Kerberos-aktivierte Dienste Probleme beim Zugriff auf Tickets bekommen können.
- NT4Crypto standardmäßig deaktiviert, so dass NT-Rechner oder ältere Samba-Systeme keinen SMB/CIFS-Zugriff mehr erhalten.
- Verschlüsselung des Secure Channel verschärft, wodurch NT-Rechner oder alte Samba-Domänen keine Vertrauensstellung zu Windows Server 2008 R2 mehr aufbauen können.
- Dynamischer Port-Bereich für RPC verändert, was Änderungen in der Firewall erfordern kann.

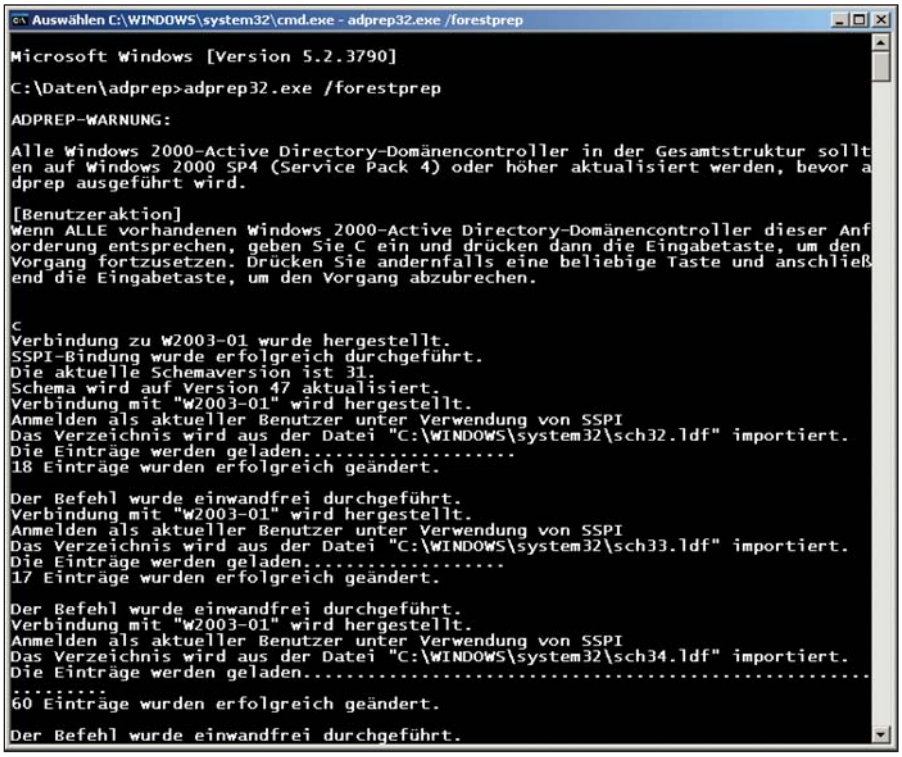


Bild 3: Bevor der Admin einen Domänencontroller mit einer neuen Windows-Version einrichtet, muss er im Forest das AD-Schema erweitern und einige weitere Vorbereitungen treffen

Erst nachdem diese Schritte abgeschlossen sind, stufen Sie den ersten neuen Server mit *dcpromo.exe* (bei Windows Server 2012 über den Server-Manager) zum zusätzlichen Domänencontroller der jeweiligen Domäne hoch. In Forests mit mehreren Domänen beginnen Sie bei der Wurzel-Domäne. Weitere neue DCs können Sie dann nach Bedarf hinzufügen.

Anschließend empfiehlt es sich, möglichst bald die Betriebsmaster-Rollen auf einen der neuen DCs zu übertragen, denn erst in diesem Moment schaltet Windows einige neue AD-Funktionen frei und erzeugt gegebenenfalls fehlende Objekte. Ist auch dies geschehen, können Sie Schritt für Schritt die älteren DCs per *dcpromo* herunterstufen und gegebenenfalls entfernen [9].

Sind die DCs auf dem neuen Stand, stufen Sie den Domänen- und Forest-Betriebsmodus auf die aktuellste Fassung hoch. Dies betrifft nur die Domänencontroller selbst und hat keine Auswirkungen auf die Clients und Mitgliedsserver der Domäne [10].

Neuer DC mit altem Namen

Administratoren fragen sich oft, ob sie einen neuen DC mit dem Namen und der IP-Adresse eines vorhandenen Servers installieren können, um diesen zu ersetzen. Grund dafür sind Abhängigkeiten in Applikationen, etwa wenn dort der Name oder die IP-Adresse eines Anmeldeservers fest konfiguriert ist. Hier sollten Sie prüfen, ob sich diese Abhängigkeit nicht lösen lässt: Viele Applikationen erlauben es etwa, beliebige DCs anzusprechen. In anderen Fällen lässt sich statt des Servernamens der Namen der Domäne angeben, denn DNS gibt dann von selbst die IP-Adressen gültiger DCs zurück.

Bleiben trotzdem Anwendungen oder Skripte übrig, die einen bestimmten Namen oder eine bestimmte IP-Adresse benötigen, können Sie tatsächlich dem neuen DC die Identität des alten geben. Dies erfordert aber einiges an Sorgfalt und geht nicht ohne Unterbrechungen.

Zunächst installieren Sie den neuen Server unter anderem Namen und mit einer eigenen IP-Adresse. Dann stufen Sie ihn als zusätzlichen DC hoch, sodass er parallel zum Altsystem läuft. Als Nächstes müssen Sie alle Client-Verbindungen zum alten Server beenden und ihn dann per *dcpromo* herunterstufen. In diesem Moment beginnt die Downtime für die Anwender. Den alten Server entfernen Sie nun oder Sie geben ihm einen neuen Namen und eine neue IP-Adresse.

Bevor Sie nun den Namen und die IP-Konfiguration auf den neuen Server übertragen, sollten Sie prüfen, dass der ehemalige DC in der AD-Konfiguration nicht mehr auftaucht. Anschließend sind die Verweise auf den Server in DNS zu entfernen, was manchmal nur manuell geht. Netzwerke mit mehreren AD-Standorten benötigen nun unter Umständen einige Zeit für die Replikation. Erst wenn dies abgeschlossen ist, tragen Sie die IP-Adresse beim neuen DC ein und ändern über die Systemsteuerung den Servernamen. Nach einem Neustart sollte der neue DC nun korrekt mit dem "alten" Namen und der passenden IP-Adresse ansprechbar sein. Erst dann endet die Downtime für die abhängigen Applikationen.

Sanfte Migration mit DNS-Magie

In großen Umgebungen fällt es oft schwer, alle Applikationen gegen die neuen Betriebssysteme beziehungsweise ihre Konfiguration zu testen (etwa Produktionsstraßen oder undokumentierte Applikationen). In

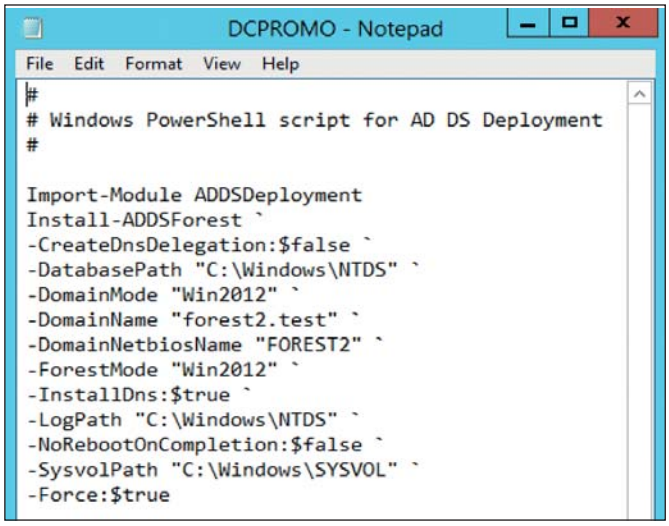


Bild 4: Seit Windows Server 2008 R2 generiert "DCPROMO" Antwortdateien als PowerShell-Befehle. So lassen sich die Schritte besser automatisieren, vereinheitlichen und auch gleichzeitig dokumentieren.

solchen Fällen ist es ratsam, die neuen Domänencontroller nicht direkt in den Produktionsstatus zu heben, sondern zunächst eine isolierte Pilotierung auszuführen.

Hierzu können Sie die "DNS Mnemonics" nutzen: Eigentlich gedacht, um die DNS-Einträge der DCs innerhalb ihrer Standorte zu optimieren, kann die Funktion auch einen neu eingebrachten DC "verstecken". Hierfür erzeugen Sie vorübergehend einen eigenen AD-Standort, beispielsweise mit dem Namen "Migration" und einem eigens dafür zugewiesenen IP-Subnetz. Nun weist eine Gruppenrichtlinie den NETLOGON-Dienst der neuen DCs per "DNS Mnemonics" an, die DNS-SRV-Einträge für den neuen DC ausschließlich in diesem AD-Standort durchzuführen. Die erforderlichen GPO-Einstellungen, verlinkt auf die OU "Domain Controllers" [11], sehen wie folgt aus: "Computer Configuration / Policies / Administrative Templates / System / Netlogon / DCLocator DNS Records / DC Locator DNS records not registered by the DCs: Mnemonics: Ldap LdapIpAddress DcByGuid Kdc Dc Rfc1510Kdc Rfc1510 UdpKdc Rfc1510Kpwd Rfc1510Udp Kpwd Gc GcIpAddress GenericGc".

Diese Gruppenrichtlinie geben Sie noch vor dem Verlinken per WMI-Filter nur für die neu einzuführenden Systeme frei. Der folgende WMI-Filter schränkt die Anwendung des GPO auf Domänencontroller ("ProductType=2") ab Windows Server 2008 ("Version>=6") ein:

```
Root\CIMV2;SELECT producttype,
  version FROM Win32_OperatingSystem
  WHERE producttype='2' AND
  version>='6'
```

Während des DCPROMO-Vorgangs müssen sich die DCs logisch im Standort "Migration" befinden – seit Windows Server 2008 erkennt ein DC seinen Standort anhand der IP-Konfiguration. Sobald *dcpromo* für einen oder mehrere DCs mit neuem Betriebssystem abgeschlossen ist und die DNS-SRV-Einträge in der AD-Site "Migration" registriert sind (und nur dort!), können Sie testweise Produktionsclients durch Änderung des IP-Subnetzes in diesen Test-Standort verschieben. So können Applikationen, die per DCLocator den zuständigen DC suchen, ab sofort die DCs in dem temporären AD-Standort finden und nutzen. Zeigen sich Probleme, setzt das Troubleshooting gezielt bei den Test-Clients an. Durch eine simple Subnetzänderung des Clients kann dieser jedoch bei Bedarf zurück in den normalen Produktionsbetrieb gelangen. Gleiches gilt für Server, die testweise die neuen DCs nutzen sollen. Gegebenenfalls sollten Sie die autorativen DNS-Nameserver-Einträge für die Zone "_msdcs" und die Domänen-Zonen ebenfalls entfernen, damit keine DNS-Anfragen bei diesen abgeschotteten DCs landen. Sofern es nach ausgiebigen Prüfungen zu keinen Problemen kommt, können die neuen DCs schrittweise per Subnetzänderung, Verschieben an ihren AD-Zielstandort und Entfernen der DNS-Mnemonics-Gruppenrichtlinie (alternativ: deren Sicherheitsfilterung) in die Produktion gelangen.

Genau anders herum dient das Vorgehen übrigens auch für das später erfolgende Entfernen der alten DCs: Da nicht immer klar ist, ob vielleicht Applikationen "hart" auf einen Domänencontroller zeigen (etwa per IP-Adresse oder Name), können Sie

1. Die alten DCs in den logischen AD-Migrations-Standort verschieben.
2. Dann wenden Sie die "DNS Mnemonics"-Gruppenrichtlinie auf diese DCs an.
3. Entfernen Sie nun DNS-SRV-Einträge in den anderen AD-Standorten. Dies erledigen Sie etwa mittels des Befehls *NLTEST.exe /DSDEREGDNS:DC_name.domain.tld*
4. Durch die Auswertung von Fehlerprotokollen oder Netzwerk-Traces prüfen Sie, welche Systeme dennoch auf diese DCs zeigen.

Da per DNS-Abfrage diese alten DCs nicht mehr sichtbar sind, können nur "hart verdrahtete" Anfragen auf diese DCs gehen, und die Übeltäter sind schnell identifiziert. Auch hier müssen Sie unter Umständen die autorativen DNS-Nameserver Einträge der DCs auf den jeweiligen DNS-Zonen entfernen.

Fazit

Erfahrungsgemäß ist ein AD-Upgrade ohne große Probleme durchzuführen, und wenn doch einmal etwas während des Updates nicht korrekt läuft, lässt es sich in der Regel sicher beheben. Die technischen Prozesse sind ausgiebig getestet und millionenfach bewährt. Trotzdem dürfen Sie ein solches Vorhaben nicht auf die leichte Schulter nehmen, denn natürlich ist das Active Directory das Rückgrat der Windows-Umgebung und es gibt viele Abhängigkeiten im Netzwerk.

Ein umfassender Migrationsplan und sorgfältiges Testen helfen, das Risiko zu minimieren. In kleineren Umgebungen ist dafür gar nicht viel Aufwand nötig und die Aktualisierung selbst lässt sich dort meist in wenigen Stunden abschließen. Je größer und komplexer das Netzwerk ist, desto intensiver sollte aber auch die Vorbereitung sein. Vorsicht übrigens bei Wochenend-Aktionen, zu denen Administratoren sich bei solchen Vorhaben oft gezwungen sehen: Am Wochenende fällt es im Notfall schwer, externe Hilfe zu bekommen. Schon aus diesem Grund ist es oft besser, die Aktualisierung während der Arbeitszeiten vorzunehmen, zumal nach guter Vorarbeit Ausfälle kaum zu befürchten sind. *(jp)*

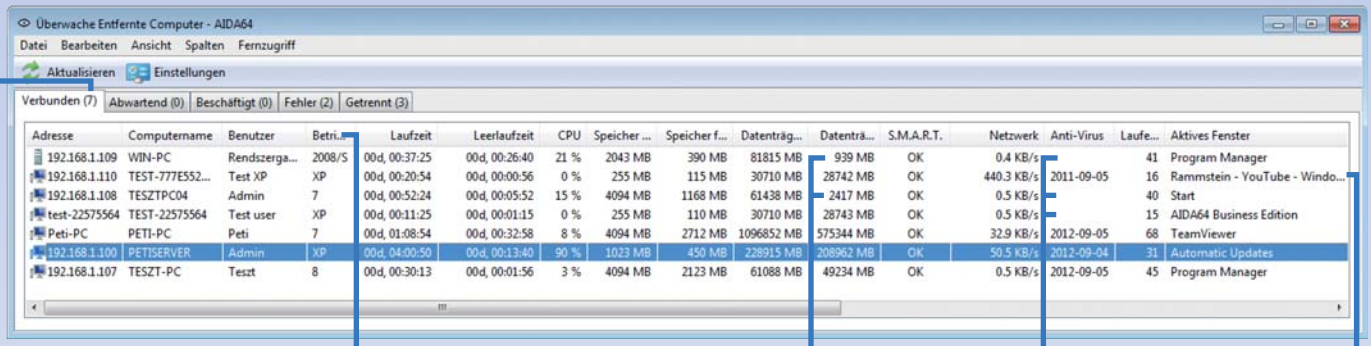
Link-Codes

[1] Welches Domänenmodell ist das beste für Active Directory? COP61
[2] Ergänzende Informationen der Autoren COP62
[3] Group Policy Management Console Sample Script COP63
[4] Ultrasound - Monitoring and Troubleshooting Tool for File Replication Service (FRS) COP64
[5] Active Directory Replication Status Tool COP65
[6] AD-Dokumentation mit José 3.2 COP66
[7] AD-Standorte mit Borg dokumentieren COP67
[8] Empfehlungen zum Virenscan auf Unternehmenscomputern COP68
[9] Was muss ich tun, um den ersten DC zu deinstallieren? COP69
[10] Was muss ich beim Anheben des AD-Betriebsmodus beachten? COP60
[11] How to optimize the location of a domain controller or global catalog that resides outside of a client's site COP6A

AIDA64 Business Edition – Neue Version!

Netzwerk-Software für höchste Ansprüche

Kenner kennen AIDA64! Und für immer mehr Experten ist AIDA64 Business Edition die Software für ein komfortables und zuverlässiges Netzwerk-Management auf höchstem Niveau. Mit der neuesten Version v2.60 setzt AIDA64 noch einmal neue Maßstäbe!



SIEBEN GERÄTE SIND IN BETRIEB
Von 10 überwachten Computern sind 7 angemeldet. Wo sind die anderen 3 Kollegen verblieben?

3 x XP, 2 x WINDOWS 7, 1 x WINDOWS 8 und 1 x WINDOWS Server 2008
Ein Blick genügt, und man kann sofort erkennen, wie es um die Aktualisierung der Betriebssysteme steht.

1 BZW. 2,4 GB LEERER SPEICHERPLATZ
Bei 2 PCs wird der HDD-Speicherplatz gefährlich weniger, da lohnt es sofort einzugreifen!

VIRUS GEFAHR!
AIDA64 hat insgesamt auf 4 Geräten Virusschutz gefunden, auf 3 PCs gibt es keinen Schutz!

ARBEIT UND YouTube?
Es gibt wenig Stellenbeschreibungen, wo dies drinsteht.

Ab sofort ist die neueste Version v2.60 der AIDA64 Business Edition auf dem Markt. AIDA64 Business Edition: die intelligente Management-Lösung für alle 32- oder 64bit-Windows-Netzwerke. Ob 5 oder über 100 PC's - AIDA64 Business Edition hilft bei der Installation, Optimierung und lückenlosen Überwachung Ihres Netzwerkes und warnt Sie automatisch, wenn Risiken oder Sicherheitsmängel drohen.

Die neue Version von AIDA64 unterstützt vollständig Microsoft Windows 8 und Windows Server 2012 sowie die neuesten nVIDIA GeForce GTX Grafikkarten. Die 64bit-Geschwindigkeitsmessung und der Stabilitätstest wurden mit der Optimierung der AMD „Trinity" APU und VIA VX11 Plattform erweitert und nochmals verbessert. Die neuesten Feature auf einen Blick:

64bit optimierte Geschwindigkeitsmessung auf AMD „Trinity" APU

Das AIDA64 CPUID Panel, der Beschleunigungsspeicher- und das Speicher-Geschwindigkeitstest-Panel, der Systemstabilitätstest und jeder Speicher sowie der Prozessorgeschwindigkeitstest haben eine komplette FMA4 und XOP Optimierung für die AMD A4, A6, A8 und A10 „Trinity" Desktop und mobilen APU's bekommen.

Detaillierte Chipsatz-Information zu den AMD A55, A60M, A68, A68M, A70M, A75, A85X „Hudson" Fusion Controller Hub's. Vorläufige Unterstützung der AMD „Vishera" Prozessoren und AMD Memory Profiles DDR3-Speichermodule.

Microsoft Windows 8 RTM und Windows Server 2012 RTM Unterstützung

Betriebssystem- und Sicherheitssoftware-Informationen, Auflistung der installierten Programme bei der Microsoft Windows 8 und Windows Server 2012. Optimierte ACPI Abfrage- und Temperaturmessmodul; Antivirus- und Anti-Spyware Software-Information zur neuen Generation von Microsoft Windows Defender. Fehlerbehebung zur neuesten Windows Version: CPU-Taktmessung mit APIC Timing; Dekodierung vom Windows Produkt Schlüssel; Statusabfrage der Windows Produktaktivierung.

OpenGL 4.3, APP SDK 2.7, CUDA 5.0 Unterstützung

OpenGL Grafikkarte Information, Auflistung der OpenGL Erweiterungen, OpenGL 4.3 Anforderungstest. Zu den Direct3D Computer Shader, AMD Stream, nVIDA CUDA und OpenCL Tools stehen mit der Unterstützung von APP SDK 2.7, CUDA 5.0 und OpenCL Schnittstellen, GPGPU Informationen zur Verfügung.

Handling der neuesten Hardware

Grafikprozessor, OpenGL und GPGU Informationen, Temperatur- und Kühlventilator-Beobachtung zu den neuesten GPU-s: nVIDIA GeForce 620M, GeForce GTX 650, GeForce GTX 650M, GeForce GTX 660, GeForce GTX 660 Ti, GeForce GTX 680M, Quadro K Serie, Tesla K10, AMD FirePro V Serie. Weiterentwickelte Unterstützung der von Marvell 88SS9174 gesteuerten SSD's. Verbesserte Zusammenfassung der RAID-Komponenten und RAID SMART Unterstützung auf Intel RAID Steuerungen.

Sicherheit weiterhin im Vordergrund!

Selbstverständlich steht die Netzwerk-Sicherheit bei AIDA64 weiterhin im Vordergrund. Unter dem Menü-Punkt „Sicherheit" bietet Ihnen AIDA64 folgende Module an:

- **Windows-Sicherheit**. Hier gibt Ihnen AIDA64 einen Überblick über den Zustand Ihres Betriebssystems: UAC-Status, Version des Service Packs, logon shell. Auf Wunsch können Sie für die logon shell, die besonders häufig von Angriffen durch Viren und anderen Schädlinge betroffen ist, eine Alarmfunktion aktivieren, die Sie bei jeder Veränderung sofort informiert.
- **Windows-Update.** Mit diesem Modul erhalten Sie die völlige, aktive Kontrolle über die Updates des Betriebssystems.
- **Antivirus.** Egal, welche Antiviren-Software Sie benutzen. AIDA64 sagt Ihnen, welche Version installiert ist und wie aktuell die Viren-Datenbank ist. Hier können Sie einen Alarm einstellen, der sie nach einem von Ihnen definierten Zeitraum auffordert, die Datenbank zu aktualisieren.
- **Firewall. Anti-Spyware. Anti-Trojaner.** Mit diesen Modulen behalten Sie den genauen Überblick über sämtliche diesbezüglich installierte Software.
- **System-Files.** Kompletter Überblick und Kontrolle über so Viren-gefährdete Dateien wie system.ini, win.ini, hosts und lmhosts.sam.

Damit Sie aber Ihr Netzwerk nicht ständig selber aktiv überwachen und kontrollieren müssen, gibt es bei AIDA64 Business Edition noch eine ganze Reihe weiterer Überwachungsfunktionen, die Sie automatisch warnen.

Dabei können Sie den Zeitabstand der Alarme beliebig einstellen und bestimmen, ob AIDA64 Sie per Warnfenster oder auf andere Weise benachrichtigen soll.

Weitere Infos unter www.aida64.de

AIDA64

NETZWERK-MANAGEMENT AT ITS BEST!

AIDA64

DIE LÖSUNG FÜR IHR NETZWERK-MANAGEMENT

HARDWARE-DIAGNOSE

AIDA64 hat die präzisesten Erkennungsfähigkeiten seiner Klasse und erstellt blitzschnell und lückenlos einen Überblick über die gesamte Hardware jedes PC und damit des gesamten Netzwerks. Streßtests warnen rechtzeitig vor Problemen.

SOFTWARE-ANALYSE

AIDA64 bietet einen Überblick über alle installierten Programme, Software-Lizenzen, die Sicherheit von Anwendungen und Windows-Einstellungen. Dazu eine Liste aller gestarteten Prozesse, Dienste, DL-Dateien, Autostarts und besuchte Web-Sites.

ÜBERWACHUNG

AIDA64 sammelt Informationen über Hard und Software der vernetzten Computer über Kommandozeilen-Automatisierung und speichert die Daten in CSV-, XML-Dateien oder in einer SQL-Datenbank. Dabei meldet AIDA64 jede Veränderung an Hard- und Software.

(FERN-)WARTUNG

Mit der AIDA64-Fernverwaltung überwachen Sie jeden Computer Ihres Netzwerks, egal wo dieser steht. Dabei bietet AIDA64 die volle Kontrolle über den ferngesteuerten PC, um administrative Aufgaben durchzuführen oder Dateien zu übertragen.

DIE NEUE VERSION V2.60 DER AIDA64 BUSINESS EDITION IST AB SOFORT IM HANDEL. AIDA64 BUSINESS EDITION UNTERSTÜTZT ALLE 32- UND 64BITWINDOWS-BETRIEBSSYSTEME INKLUSIVE WINDOWS 8 UND WINDOWS SERVER 2012. AIDA64 BUSINESS EDITION - MEHR KOMFORT FÜR IHE NETZWERK-MANAGEMENT GEHT NICHT! WEITERE INFORMATIONEN UNTER WWW.AIDA64.DE

Hochverfügbarkeit für Hyper-V in Windows Server 2012 (2)

VM auf Wanderschaft

von Thomas Joos

Im abschließenden Teil unserer Workshopserie arbeiten wir weiter an einer hochverfügbaren Hyper-V-Umgebung. Dazu stellt Microsoft unter Windows Server 2012 für Hyper-V zusätzliche Features bereit, die die Hochverfügbarkeit auch kleinen und mittleren Unternehmen zu überschaubaren Kosten ermöglicht. Auf diesen Features lag das Augenmerk des ersten Teils unserer Workshopserie, im zweiten Teil richten wir nun Hyper-V im Cluster ein und konfigurieren die Livemigration.

Quelle: alexokokok – 123.RF

Die Livemigration ist dabei nicht nur ein Feature der Hochverfügbarkeit. Sehr interessant ist diese auch, um Wartungsfenster optimal zu nutzen oder um Wartungen am Host durchzuführen, ohne dass die Anwender auf ihre Applikationen verzichten müssen.

Hyper-V im Cluster und Livemigration

Sie können natürlich auch in Windows Server 2012 weiterhin Hyper-V im Cluster betreiben und virtuelle Server als Clusterressourcen nutzen. Unternehmen, die Server mit Hyper-V virtualisieren und eine Hochverfügbarkeit sicherstellen wollen, setzen auf die Livemigration im Cluster. Betreiben Sie Hyper-V in einem Cluster, können Sie sicherstellen, dass beim Ausfall eines physischen Hosts alle virtuellen Server durch einen weiteren Host automatisch übernommen werden. Dazu betreiben Sie die virtuellen Server als Clusterressourcen.

Um Hyper-V in einem Cluster zu betreiben, installieren Sie zunächst einen herkömmlichen Cluster mit Windows Server 2012. Das geht jetzt mit der Standard-Edition oder auch mit der kostenlosen Serverversion Hyper-V Server 2012. Die Dateien der virtuellen Server sind auf dem gemeinsamen Datenträger des Clusters gespeichert. Fällt der aktive Knoten aus, kann der passive Knoten die virtuellen Server übernehmen. Auf dem gemeinsamen Datenträger sind auch die virtuellen Festplatten der virtuellen Server gespeichert.

Grundlage für Livemigration mit Hyper-V oder den generellen Betrieb von Hyper-V im Cluster ist zunächst ein normaler Cluster mit Windows Server 2012. Jeder Knoten des Clusters erhält ein Computerkonto in derselben Domäne im Active Directory. Jeder physikalische Knoten benötigt eine IP-Adresse. Der Cluster erhält eine IP-Adresse, jeder virtuelle Server und die Netzwerkkarten für die private Kommunikation des Clusters erhalten eine IP-Adresse in einem getrennten Subnetz.

Setzen Sie in den Einstellungen der Netzwerkverbindung auf der Registerkarte "WINS" in den erweiterten Einstellungen für IPv4 die Option "NetBIOS über TCP/IP deaktivieren", da NetBIOS die interne Kommunikation eines Clusters stören kann. Ändern Sie die Bindungsreihenfolge so ab, dass die Netzwerk-Verbindung ins herkömmliche Netzwerk ganz oben ist. Die Einstellungen für den internen Clusterverkehr ordnen Sie danach ein.

In den erweiterten Eigenschaften der Windows-Firewall sollten Sie auf der Registerkarte "Erweitert" die Firewall für das private Clusternetz und für das Netzwerk zum Datenspeicher deaktivieren. Clustering installieren Sie auch in Windows Server 2012 als Feature über den Server-Manager. Während der Installation nehmen Sie keine Einstellungen vor. Achten Sie darauf, dass die gemeinsamen Datenträger auf allen Knoten verbunden und mit dem gleichen Laufwerksbuchstaben versehen sind.

Um die notwendigen Features für einen Hyper-V-Cluster zu installieren, können Sie auch die PowerShell verwenden. Geben Sie die folgenden CMDlets ein:

```
Add-WindowsFeature Hyper-V
Add-WindowsFeature Failover-
  Clustering
Add-WindowsFeature Multipath-IO
```

Starten Sie dann auf dem ersten Knoten die Failover-Clusterverwaltung über die Eingabe von *cluster* im Startbildschirm. Dann klicken Sie auf den Link "Konfiguration überprüfen". Nachdem der Assistent alle wichtigen Punkte getestet hat, erstellen Sie den Cluster. Dies ist auch in der PowerShell möglich, die Syntax dazu lautet

```
New-Cluster -Name Clustername
  -StaticAddress IP-Adresse des
  Clusters -Node Knoten 1, Knoten 2
```

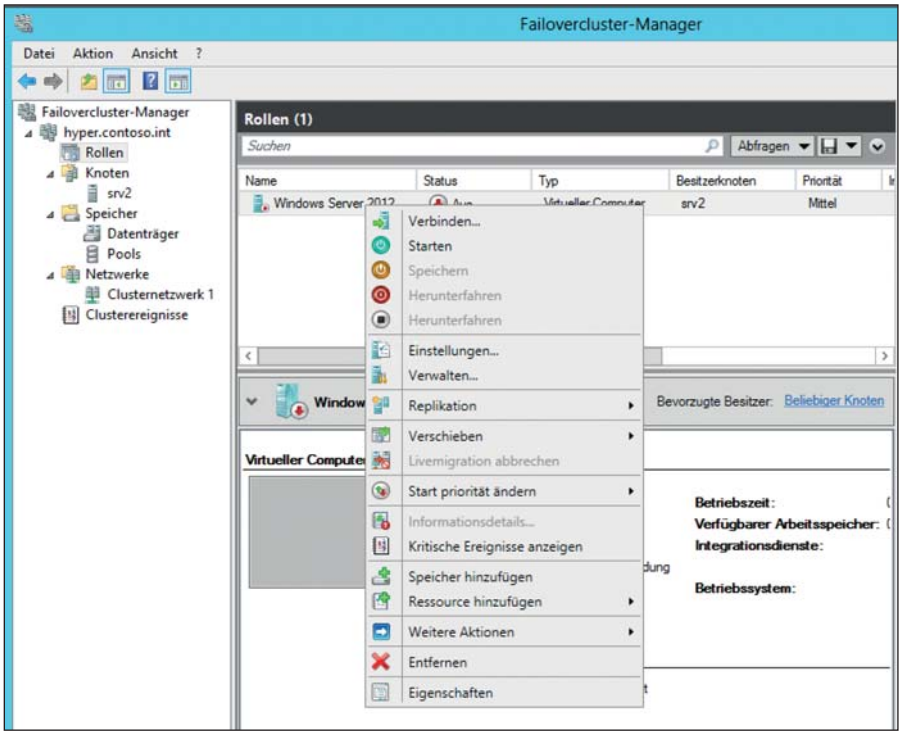


Bild 1: Virtuelle Computer lassen sich im Failovercluster-Manager vollständig verwalten

Setzen Sie Hyper-V im Cluster ein, müssen Sie bei der Datensicherung und der Erstellung von Snapshots einige wichtige Punkte beachten. Sie sollten es möglichst vermeiden, Snapshots von laufenden virtuellen Maschinen in Clustern zu erstellen. Setzen Sie einen solchen Snapshot zurück, setzt dieser nicht nur den Inhalt der virtuellen Festplatte zurück, sondern auch den des Arbeitsspeichers der VM. Dieser Umstand macht vor allem im Zusammenhang mit der Livemigration Probleme. Wenn Sie also Snapshots von VMs in einem Cluster durchführen wollen, fahren Sie die VM herunter. Auch wenn Sie einen Snapshot auf eine VM anwenden wollen, sollten Sie die Maschine vorher herunterfahren.

Gemeinsame Datenträger mit CSV

Ein wichtiger Punkt für die Livemigration sind die Cluster Shared Volumes (CSV). Diese ermöglichen es, dass mehrere Server gleichzeitig auf einen gemeinsamen Datenträger zugreifen können. Neben einem automatischen Failover lassen sich virtuelle Server auch manuell übertragen. Der Start einer Livemigration kann entweder über die Clusterkonsole erfolgen, per Skript (auch PowerShell) oder über den System Center Virtual Machine Manager. Die Livemigration setzt voraus, dass der Clusterknoten, der die VM hostet, noch läuft, liest den Arbeitsspeicher des virtuellen Servers aus und überträgt ihn zum Zielserver. Alle Systeme, die mit Hyper-V laufen, lassen sich mit der Livemigration absichern. Dies betrifft auch Linux oder ältere Windows Server.

Um Hyper-V mit Livemigration in einem Cluster zu betreiben, aktivieren Sie die CSV für den Cluster, nachdem Sie den Cluster erstellt haben. Windows legt dann auf der Betriebssystempartition im Verzeichnis "ClusterStorage" Daten ab. Diese liegen aber nicht tatsächlich auf der Festplatte C: des Knotens, sondern auf dem gemeinsamen Datenträger, dessen Abruf auf das Verzeichnis "C:\ClusterStorage" umgeleitet ist. Die VHD(X)-Dateien der VMs liegen in diesem Verzeichnis und sind daher von allen Knoten gleichzeitig zugreifbar. Fällt eine Netzwerkverbindung zum SAN von einem Knoten aus, verwendet der Knoten alternative Strecken über andere Knoten. Die virtuellen Maschinen, deren Dateien im CSV liegen, laufen uneingeschränkt weiter. Um CSV für einen Cluster zu aktivieren, starten Sie das Verwaltungsprogramm für den Failovercluster. Dort klicken Sie mit der rechten Maustaste im Bereich "Speicher / Datenträger" auf den Datenträger, den Sie für Hyper-V nutzen wollen, und wählen "Zu freigegebenen Clustervolumes hinzufügen".

Cluster in Windows Server 2012 beherrschen Dynamic I/O. Wenn die Datenverbindung eines Knotens ausfällt, kann der Cluster den Datenverkehr, der für die Kommunikation zu den virtuellen Computern im SAN notwendig ist, automatisch über die Leitungen des zweiten Knotens routen, ohne dazu ein Failover durchführen zu müssen. Sie können einen Cluster so konfigurieren, dass die Clusterknoten den Netzwerkverkehr zwischen den Knoten und zu den CSV priorisieren. Damit Sie die Livemigration nutzen können, müssen Sie als Nächstes auf allen Clusterknoten Hyper-V installieren, ge-

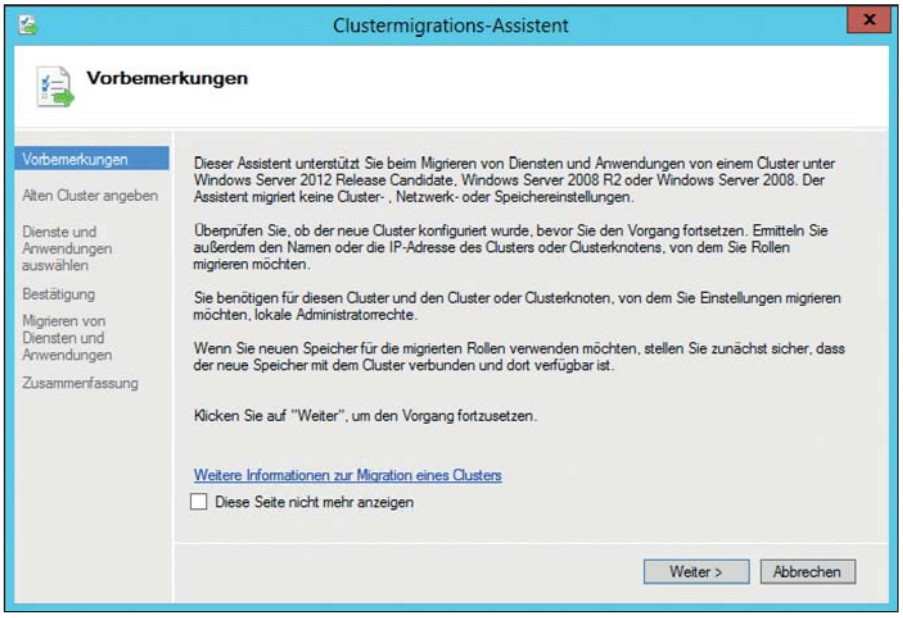


Bild 2: Die Migration von Clustern zu Windows Server 2012 erledigt der Administrator schnell und unkompliziert mit einem Assistenten

nauso wie auf herkömmlichen Servern, auf denen Sie Hyper-V betreiben wollen.

Um eine virtuelle Maschine in einem Cluster zu erstellen, verwenden Sie den Failovercluster-Manager:

1. Klicken Sie mit der rechten Maustaste auf "Rollen / Virtueller Computer / Neuer virtueller Computer" und starten Sie den Assistenten.
2. Wählen Sie den Clusterknoten, auf dem Sie diesen Server bereitstellen wollen.
3. Schließen Sie die Erstellung des virtuellen Servers ab. Der Assistent konfiguriert ihn automatisch für den Cluster.

Klicken Sie mit der rechten Maustaste auf den virtuellen Computer, sehen Sie, dass im Failovercluster-Manager auch die Steuerung der virtuellen Maschinen hinterlegt ist. Sie können über diesen Weg den virtuellen Server komplett verwalten. Wählen Sie "Virtuelle Computer starten" aus, wird die Ressource online geschaltet und die virtuelle Maschine startet. Über das Kontextmenü können Sie sich jetzt mit dem virtuellen Computer verbinden und das Betriebssystem installieren.

Standardmäßig kann die Livemigration nach der Installation eines Clusters und der Integration von virtuellen Computern verwendet werden. Wollen Sie eine Livemigration durchführen, klicken Sie den virtuellen Computer mit der rechten Maustaste an, rufen im Kontextmenü den Eintrag "Verschieben / Livemigration" auf und wählen den Knoten aus.

MAC-Adressen im Cluster konfigurieren

Wichtig sind die Einstellungen für virtuelle MAC-Adressen in den Einstellungen der virtuellen Netzwerkkarten. Hier müssen Sie bezüglich der Livemigration, beim Betrieb von Hyper-V im Cluster und vor allem der Aktivierung des Betriebssystems von virtuellen Servern Einstellungen vornehmen, da Sie ansonsten ständig die Server neu aktivieren müssen. Außerdem spielen diese Einstellungen auch in NLB-Clustern mit Exchange Server 2010 eine Rolle.

Verschieben Sie einen virtuellen Server mit aktivierten dynamischen MAC-Adressen im Cluster auf einen anderen Host durch die Livemigration, ändert sich dessen MAC-Adresse beim nächsten Start dieser virtuellen Maschine [1]. Jeder Hyper-V-Host hat einen eigenen Pool aus dynamischen MAC-Adressen. Welcher das ist, sehen Sie im Hyper-V-Manager über den Manager für virtuelle Netzwerke im Bereich "MAC-Adressbereich". Microsoft beschreibt die Zusammenhänge auf der Webseite [2] noch genauer. Aus diesem Grund ist es empfehlenswert, die statische Zuordnung von MAC-Adressen für virtuelle Server zu aktivieren. Sie finden diese Einstellung im Bereich "Netzwerkkarte" der einzelnen virtuellen Server im Hyper-V-Manager. In diesen Einstellungen steuern Sie auch das Spoofing für Netzwerkkarten. Hyper-V kann genau unterscheiden, welche Netzwerkdaten zu den einzelnen Servern gesendet werden sollen und verwendet dazu die MAC-Adresse des virtuellen Servers. Das heißt, virtuelle Server empfangen nur die Daten, die für ihre MAC-Adresse gedacht sind.

Migration zu einem Windows Server 2012-Cluster

Setzen Sie Hyper-V bereits in einem Windows Server 2008 R2-Cluster ein, können Sie diesen auch zu Windows Server 2012 aktualisieren. Dazu entfernen Sie Knoten vom Cluster, die aktuell keine Ressourcen hosten. Den Server können Sie jetzt direkt zu Windows Server 2012 aktualisieren oder auf Wunsch auch neu installieren. Anschließend erstellen Sie mit dem neuen Server einen neuen Cluster mit Windows Server 2012.

Danach migrieren Sie die virtuellen Server einzeln zum neuen Server und installieren dann den noch verbliebenen Clusterknoten mit Windows Server 2012 und nehmen ihn in den neuen Cluster mit auf. Die virtuellen Server übernehmen Sie am besten mit System Center Virtual Machine Manager 2012. Allerdings muss das Service Pack 1 für SCVMM 2012 installiert sein, damit sich Server mit Windows Server 2012 verwalten lassen. Alternativ übernehmen Sie die virtuellen Maschinen vom alten Cluster auf den neuen Windows Server 2012-Cluster mit dem Windows Server 2012 Cluster Migration Wizard [3]. Den Migrations-Assistenten starten Sie über den Link "Rollen migrieren" im Bereich "Konfigurieren" des Failovercluster-Managers [4]. *(jp)*

[1] Hyper-V and Dynamic MAC Address Regeneration
BOS3N

[2] Windows Server 2008 Hyper-V virtual machines generate a stop error when NLB is configured
BOS3P

[3] Aktualisieren von Failoverclustern
C9P11

[4] How to Move Highly Available (Clustered) VMs to Windows Server 2012
C9P12

Link-Codes

Wichtige Neuerungen in IPCop 2.0

Patrouille im Netzwerk

von Dr. Holger Reibold

Hendri Nguriana – 123RF

Wenn Sie Ihr lokales Netzwerk vor Attacken von außen schützen wollen, muss eine leistungsfähige und zuverlässige Firewall her. Unter Administratoren genießt IPCop einen ausgezeichneten Ruf. Mit der Einführung von IPCop 2.0 hat das Entwicklerteam noch einmal nachgelegt. Wir erklären in diesem Workshop, wie Sie mit den wichtigsten Neuerungen umgehen und was Sie tun müssen, um sowohl den integrierten DHCP-Server als auch die Firewall selbst optimal zu konfigurieren.

IPCop [1] hat mit übe so manche Höhen und Tiefen durchgemacht. Mit der Ende September 2011 veröffentlichten Version 2.0 haben die Entwickler eine ohnehin schon vorbildliche Lösung weiter verfeinert. Bei IPCop handelt es sich um eine spezielle Linux-Distribution, die sich auf die Kernfunktionen Router und Firewall konzentriert. Die Vorgängerversion 1.4 kommt heute in Tausenden Netzwerken zum Einsatz. Administratoren schätzen nicht nur ihre Solidität und Funktionalität, sondern auch die einfache Verwaltung über die webbasierte Schnittstelle. IPCop 2.0 knüpft nahtlos an dieser Tradition an und bietet eine Fülle von Detailverbesserungen.

Die wichtigen Neuerungen im Überblick

Nach jahrelanger Entwicklungsarbeit bietet IPCop 2.0 verschiedene wesentliche Verbesserungen. Es gibt jedoch leider keinen Update-Mechanismus, mit dem Sie einfach von Version 1.x auf 2.x umsteigen könnten. Lediglich Updates von 1.9.9 auf höhere Versionen sind über die integrierte Update-Funktion möglich.

Jetzt mit VPN

Zu unterscheiden ist zwischen technologischen und optischen Neuerungen. Auf technischer Seite verwendet IPCop 2.0 in der aktuellen Fassung den Linux-Kernel 2.6.32 und bietet in Sachen Hardware-Unterstützung mehr Einsatzmöglichkeiten. So ist das Werkzeug nun auch auf Cobalt-, Sparc- und PPC-Plattformen einsetzbar.

Der neu gestaltete Installer erlaubt es, die Linux-Distribution, die seit Version 1.4 auf Linux from Scratch (LFS) basiert, auf Flash-Medien und Festplatten zu installieren. Sie können bereits während der Installation die Netzwerkkarten auswählen, um diese den entsprechenden Netzwerken zuzuordnen. Änderungen gibt es auch beim Zugriff auf die Web-Schnittstelle. In der neuen IPCop-Version ist der Zugriff auf alle Seiten der Weboberfläche passwortgeschützt. Eine weitere Modifikation: Der Port für sichere HTTPS-Verbindungen wurde auf 8443 geändert. Außerdem funktionieren die Weiterleitungen der Ports 81 und 445 nicht mehr.

Die herausragende technische Neuerung stellt die Integration von OpenVPN dar. Die VPN-Lösung ersetzt die bisherige, komplex zu konfigurierende IPSec-Komponente und erlaubt es IPCop-Administratoren, ein eigenes virtuelles privates Netz zu betreiben. Auf der anderen Seite haben sich die Entwickler dafür entschieden, bei IPCop 2.0 das Intrusion Detection System "Snort" wegzulassen. Es soll jedoch in Zukunft als Add-on verfügbar sein.

Umbauten gab es ferner bei der Update-Funktion, mit der Sie Ihre Firewall-Installation per Knopfdruck auf verfügbare Aktualisierungen prüfen können. Standardmäßig führt das System mit der aktivierten Option "Nach Verbindung auf Updates überprüfen" einen Update-Check durch. Dieses Feature wird auch als Phone Home-Funktion bezeichnet und lässt sich in IPCop 2.0 deaktivieren. Wenn Sie die Prüfung deaktivieren, sollten Sie sich zumindest über die Mailingliste "ipcop-announce" über verfügbare Aktualisierungen informieren.

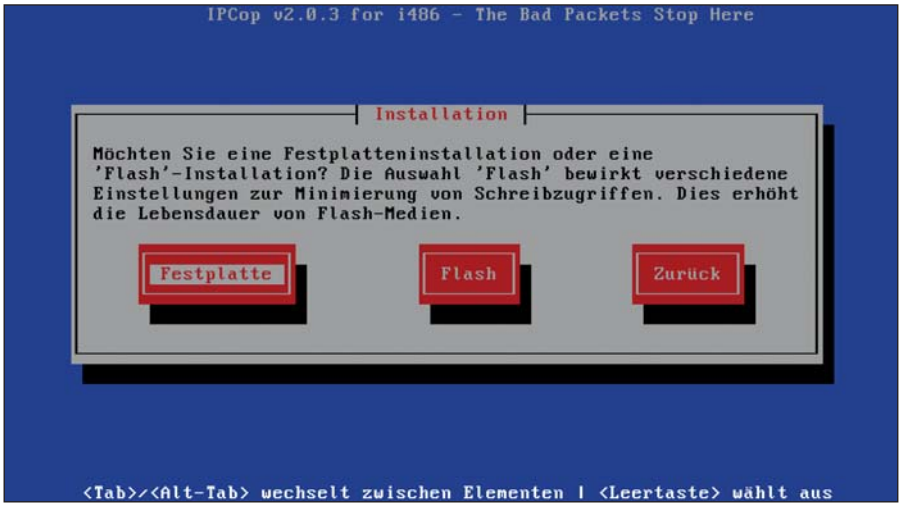


Bild 1: Der überarbeitete Installer erlaubt sowohl die Festplatten- als auch die Flash-Installation

Mehr Komfort in der GUI

Auch optisch hat IPCop 2.0 einige interessante Neuerungen zu bieten. Die neu gestaltete Benutzeroberfläche verfügt beispielsweise im System-Menü über eine neue Scheduler-Seite, auf der Sie verschiedene Ereignisse planen können. Im Status-Menü finden Sie zusätzliche Seiten, die Ihnen Details zur Systeminfo, Traffic-Erfassung und iptables präsentieren. Zusätzlich wurde die Seite für Verbindungen vollständig überholt. Im aktualisierten Web-Proxy-Menü greifen Sie auf verschiedene neue oder erweiterte Einstellmöglichkeiten zu.

In IPCop 2.0 haben die Entwickler außerdem die DHCP-Server-Konfiguration vereinfacht. Das hängt nicht zuletzt damit zusammen, dass dhcpd durch dnsmasq als DCHP-Server ersetzt wurde. Auch der Umgang mit der Zeitserver-Seite gestaltet sich nun einfacher. Die Firewall-Umgebung verwendet jetzt ntpd vollständig. Und last but not least haben die IPCop-Macher das gesamte Firewall-Menü überholt. In Version 2.0 werden Schlupflöcher und Port-Weiterleitungen durch Firewall-Regeln gesteuert.

Das Auswahlmenü "Aktion" umfasst nun folgende Befehle: Wiederverbinden, Verbinden, Trennen, Neustart, Herunterfahren, DynDNS-Update erzwingen, auf Updates überprüfen und zum Einwahlprofil wechseln. Beachten Sie, dass Sie bei der Profilwechsel-Aktion alternative Profile anlegen müssen. Dazu verwenden Sie die Funktionen auf der Seite "Einwahl".

Das Status-Menü versorgt Sie mit Informationen und Statistiken zur Ausführung des IPCop-Servers. Besonders ausführlich sind die Informationen zum Systemstatus. Diesem Menü können Sie die aktuell laufenden Dienste und deren Speicherverbrauch entnehmen, die Verwendung des Speichers und der Auslagerungsdatei, den gesamten, verwendeten und freien Speicherplatz auf den einzelnen Festplatten-Partitionen sowie die Inodes der Partitionen. Das Untermenü "Uptime und Benutzer" gibt das Ergebnis des w-Kommandos aus, das die Laufzeit und Informationen über aktuell angemeldete IPCop-Benutzer ausgibt.

Webzugriff und Scheduler konfigurieren

Bei der Einrichtung der IPCop-Umgebung weisen Sie mit Hilfe des Installationsassistenten für den Root-, den Backup- und den Web-Zugriff jeweils ein Passwort zu. Das Web-GUI lässt sich über einen Browser starten und ist über die IP-Adresse der grünen Schnittstelle beziehungsweise den Host-Namen der IPCop-Installation erreichbar. Beachten Sie, dass HTTP-Verbindungen ab IPCop 2.0.0 nicht mehr auf Port 81 umgeleitet werden. Wie bereits erwähnt, finden sowohl Port 81 als auch Port 445 keine Unterstützung mehr. Der Aufruf des Web-Interfaces erfolgt nun zusammen mit der Port-Nummer 8443 mit der Eingabe von *https://ipcop:8443* oder etwa *https://192.168.1.1:8443*.

Sollte Ihnen diese Standardkonfiguration nicht zusagen, können Sie den HTTPS-Port ändern. Hierfür steht Ihnen das Kommandozeilenprogramm "setreservedports" zur Verfügung. Um den HTTPS-Port zu modifizieren, verwenden Sie die Option "--gui". Um den Port auf 5445 zu setzen, verwenden Sie folgenden Befehl:

```
$ /usr/local/bin/setreservedports.pl
  -gui 5445
```

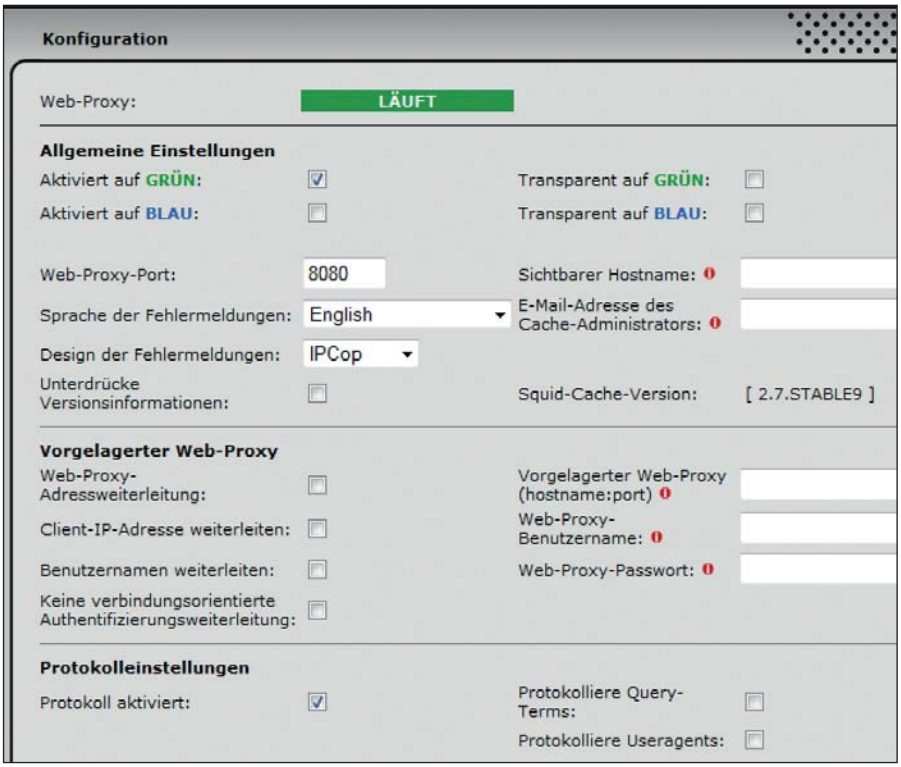


Bild 2: Das Web-Proxy-Menü wurde grundlegend überarbeitet und bündelt die wichtigsten Funktionen auf einen Blick

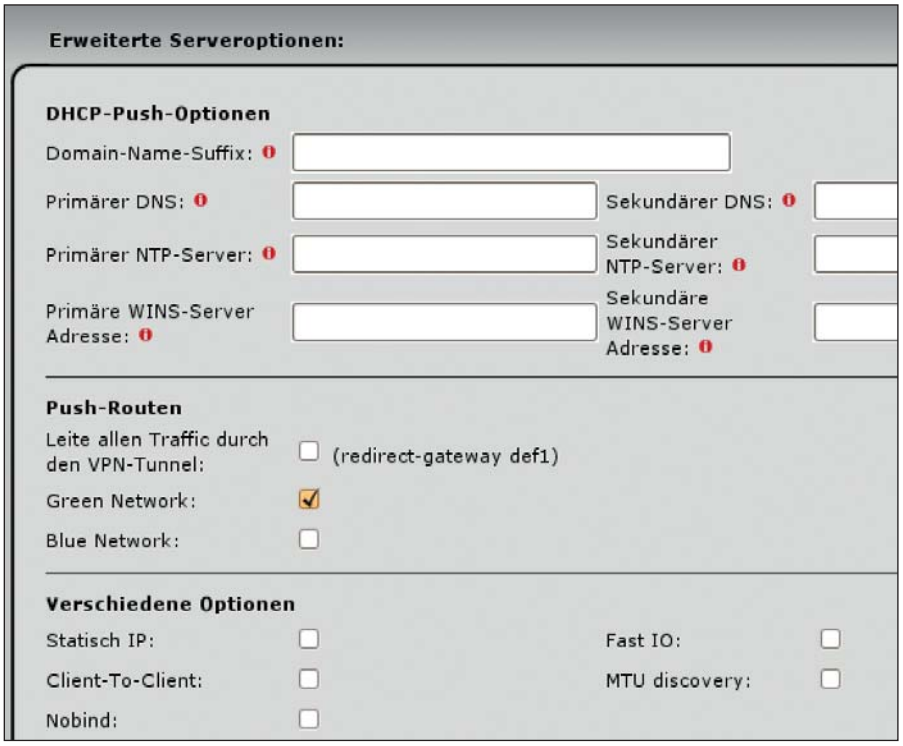


Bild 3: Die erweiterten Einstellungen des OpenVPN-Servers stellen diverse Push-Funktionen zur Verfügung

Das IPCop-Team schlägt diesen Port als Alternative vor, aber Sie können jeden beliebigen anderen Port zwischen 1 und 65536 verwenden, solange er nicht mit einem anderen Dienst kollidiert.

Mit der neuen Scheduler-Seite ist es einfach, bestimmte Aktionen per Zeitsteuerung auszuführen. Sie finden den Scheduler im System-Menü. Er weist zwei Bereiche auf: Im ersten Dialog legen Sie die geplante Aktion an, im zweiten bestimmen Sie die durchzuführende Aktion. Bestimmen Sie im Scheduler-Dialog zunächst die auszuführende Aktion, dann die Uhrzeit und den Tag. Klicken Sie dann auf die Schaltfläche "Hinzufügen", um die neue Aktion im Scheduler einzureihen.

Runderneuerte Web-Proxy- und DHCP-Konfiguration

Über das Dienste-Menü ist der aktualisierte und erweiterte Web-Proxy verfügbar. Er dient dem Cachen von Web-Seiten, wobei Netzwerk-Clients bevorzugt mit Daten aus dem Zwischenspeicher versorgt werden. In den allgemeinen Einstellungen bestimmen Sie, für welche Netze (grün für privat und/oder blau für wireless) der Proxy Client-Requests verarbeitet. Hier aktivieren Sie auch den transparenten Modus, in dem der Proxy umgangen wird.

Der Proxy bietet eine Fülle von interessanten Anwendungs- und Konfigurationsmöglichkeiten. Sie können ihn beispielsweise einfach als vorgelagerten Proxy einsetzen. Er bietet zudem die Möglichkeit der Zugriffskontrolle. Wenn Sie nur über eine beschränkte Bandbreite verfügen, können Sie mithilfe der Downloadbandbreite diese pro Schnittstelle und/oder pro Host beschränken. Ebenso ist die Limitierung auf bestimmte Inhaltstypen möglich.

Durch den Wechsel des DHCP-Servers ergeben sich in IPCop 2.0 gegenüber der Vorgängerversion Änderungen in der DHCP-Konfiguration. Auch dieser Server ist über das Dienste-Menü verfügbar. Die Server-Konfiguration erlaubt Ihnen die Verwendung des DHCP-Dienstes für die Schnittstelle Grün und/oder Blau. Wie es sich für einen professionellen DHCP-Server gehört, gestattet dieser die fixe und dynamische Adressenvergabe.

Nicht alle DHCP-Servereinstellungen sind jedoch über die Web-Schnittstelle zugänglich. Für verschiedene spezielle Parameter müssen Sie die Datei */var/ipcop/dhcp/dnsmasq.local* editieren (siehe Kasten "Individuelle Anpassungen"). Damit etwaige Änderungen greifen, bedarf es eines

Neustarts des DHCP-Servers über die Web-Schnittstelle oder auf der Konsole mit *restartdhcp*.

Firewall-Kernfunktion beherrschen

Im Firewall-Menü finden Sie die Hauptfunktionen der IPCop-Umgebung, mit denen Sie den Datenverkehr über die Firewall steuern. Die Firewall-Funktionen haben einige grundlegenden Änderungen in IPCop 2.0 erfahren. In der neuen Version akzeptiert die Firewall-Umgebung nicht mehr alle Pakete, die von internen Schnittstellen gesendet werden. Sie nimmt nur noch Pakete von Diensten entgegen, die IPCop kennt, also von DHCP, DNS, NTP, Proxy und OpenVPN.

Die Port-Weiterleitungen kontrollieren Sie in IPCop 2.0 im Firewall-Menü über die Seite "Firewall-Regeln". Das gilt ebenso für den externen Zugriff: Auch dieser wird jetzt über die Seite Firewall-Regeln gesteuert. Eine Änderung betrifft den Zugriff auf das blaue Netzwerk: Hierfür ist das Menü "Adressfilter" zuständig. Sie können den Filter über das Menü "Firewall-Einstellungen" deaktivieren und das Verhalten durch Ändern der Schnittstellenrichtlinie und Einrichten von Firewall-Regeln manipulieren.

Schließlich wurde die Firewall um eine Option erleichtert: Die Möglichkeit, Ping-Antworten von bestimmten Schnittstellen zu deaktivieren, ist nicht mehr gegeben. Wollen Sie dennoch Ping-Responses unterdrücken, legen Sie einfach eine Firewall-Regel mit der Aktion "DROP" an. Das Erstellen von Firewall-Regeln ist dabei besonders simpel. IPCop stellt Ihnen im Dialog "Neue Regel hinzufügen" folgende Optionen zur Auswahl:

- Ausgehender Traffic
- Zugriff auf IPCop
- Internet Traffic
- Port-Weiterleitung
- Zugriff von extern auf IPCop

Die angelegten Regeln stellt IPCop in Form einer Tabelle im zweiten Abschnitt dar. Hier können Sie sie einfach aktivieren und deaktivieren. Auch die Verarbeitungsreihenfolge lässt sich hier anpassen.

So gelingt die OpenVPN-Integration

Die herausragende Neuerung von IPCop 2.0 ist die Integration von OpenVPN. Mit IPCop können Sie einen sicheren Übertragungskanal zwischen zwei oder mehreren Netzwerken über ein anderes Netzwerk erzeugen. Die OpenVPN-Funktionen sind über das VPN-Menü verfügbar. Bevor Sie jedoch den OpenVPN-Server einsetzen können, müssen Sie mit dem Menübefehl "VPN / CA" eine Zertifizierungsstelle anlegen. In den globalen Einstellungen verrät Ihnen IPCop zunächst, ob der OpenVPN-Server gestartet oder angehalten wurde.

Mit den nun folgenden beiden Kontrollkästchen aktivieren Sie die Verwendung der roten und blauen Schnittstelle. Die blaue ist nur dann verfügbar, wenn Sie eine solche konfiguriert haben. Unter "Lokaler VPN-Hostname/IP" geben Sie jetzt den vollqualifizierenden Domänennamen beziehungsweise die öffentliche IP-Adresse der roten Schnittstelle an. Sollten Sie einen dynamischen DNS-Service verwenden, geben Sie den dynamischen DNS-Namen an. Das Menü "Protokoll" stellt Ihnen die beiden Protokolle UDP (Standardkonfiguration) und TCP zur Wahl. OpenVPN ist von Haus aus optimal für die Verwendung mit UDP ausgelegt – wo dieses Protokoll aber nicht zum Einsatz kommt, können Sie mit TCP arbeiten.

In den erweiterten OpenVPN-Einstellungen bearbeiten Sie verschiedene DHCP-Push-Optionen, Push-Routen, Protokollierungsoptionen und RADIUS-Servereinstellungen. Das OpenVPN-Modul stellt Ihnen außerdem Funktionen für den Verbindungsstatus und die -kontrolle zur Verfügung.

Fazit

IPCop ist in Version 2.0 noch einen Tick besser als sein Vorgänger geworden. Allein schon wegen der Integration des OpenVPN-Servers und den vielen Detailverbesserungen lohnt sich ein Umstieg. Dank der vorbildlichen Dokumentation – sie ist überwiegend auch in deutscher Sprache verfügbar – fällt die Einarbeitung leicht. Die deutsche Community trifft sich in einem eigenen IPCop-Forum [3]. *(ln)*

Individuelle Anpassungen

IPCop kommt mit einigen Skripten daher, die es Ihnen erlauben, das Werkzeug an Ihre Bedürfnisse anzupassen. Sie müssen nur wissen, wo Sie diese finden und wie Sie sie einsetzen. Um die Skripte zu bearbeiten, benötigen Sie einen entsprechenden Editor wie "vi" und Root-Rechte auf der Konsolenebene.

Bei jedem Boot- und Herunterfahrenvorgang wird das Shell-Skript */etc/rc.d/rc.event.local* aufgerufen, das die Datei */etc/rc.d/rc.local* von früheren Versionen ersetzt – auch beim Starten oder Stoppen der Netzwerkschnittstellen (rote ausgenommen). Sie können das Skript um weitere Optionen ergänzen. Der Aufruf beim Boot-Vorgang sieht wie folgt aus:

```
/etc/rc.d/rc.event.local system up
```

Mit dem ersten Parameter geben Sie das Ereignis (system, network, red) an, mit dem zweiten den Wert (up, down).

IPCop verfügt über einen eigenen Sicherungsmechanismus. Wenn Sie Dateien gezielt aus der Datensicherung ausschließen wollen, bearbeiten Sie die Datei */var/ipcop/backup/exclude.user*. Sie wird von offiziellen Updates nicht überschrieben und ist Bestandteil der Datensicherung. In */var/ipcop/backup/include.system* ist die genaue Syntax dokumentiert. Sie können aber nicht nur Dateien ausschließen, sondern diese auch explizit einbinden. Dazu passen Sie */var/ipcop/backup/include.user* an.

Die erweiterten Funktionen des DHCP-Servers sind durch Editieren der Datei */var/ipcop/dhcp/dnsmasq.local* verfügbar. Um dem System beispielsweise mit zwei Schnittstellen (Ethernet-Anschluss und eingebaute WLAN-Karte) eine fixe Adresse zuzuweisen, fügen Sie folgende Zeile hinzu:

```
dhcp-host=XX:XX:XX:XX:XX:XX,YY:YY:YY:YY:YY:YY,
    192.168.1.100
```

Sie können zudem eine Liste mit zu blockenden Domänen einbinden. Dazu erweitern Sie die Datei um folgende Zeile:

```
conf-file=/path-to-your/blocklist
```

Wichtig ist, dass die Block-Liste das Format "address=/domain-name/127.0.0.1" besitzt. Nachdem Sie Änderungen am DHCP-Server vorgenommen haben, müssen Sie diesen neu starten, damit diese Änderungen ins Netzwerk verteilt werden. Weitere Informationen zu den Konfigurationsmöglichkeiten des DHCP-Servers finden Sie unter [2].

Link-Codes

[1] Projektseite IPCop
COP51

[2] Konfiguration des DHCP-Servers von IPCop
COP52

[3] Deutsches IPCop-Forum
COP53

Nürnberg, Germany 16. – 18.10.2012

it sa 2012

Die IT-Security Messe
The IT-Security Expo

Drei Tage – ein Thema: Sicherheit

Seien Sie sicher vor Cybercrime und Hacking-angriffen! Schützen Sie Ihre Daten und Ihr Unternehmen!

Damit Ihre Daten auch Ihre Daten bleiben:
Europas IT-Security Messe Nr. 1

Jetzt neu: mit Kongress

Erstmals in 2012 werden im Rahmen der it-sa in hochkarätigen Fachvorträgen aktuelle IT-Security-Themen beleuchtet.

- **Sicheres Cloud Computing**
  – Gefahren, Planung, Praxis
- **Mobile Security**
  – Mit Vollgas auf der Bremse
- **„Bring your own Device"**
  – Rechtliche Vorgaben und technische Umsetzung
- **Industrielle IT-Sicherheit**
  – Neue Angriffsziele, alte Konzepte?
- **Datacenter Expert Summit**
  – Safety, Security & Strategy

Powered by eco Verband der deutschen Internetwirtschaft e.V.

Jetzt informieren und anmelden:
it-sa.de/congress

Kontakt:
Tel +49 (0) 9 11. 86 06-49 26
besucherservice@nuernbergmesse.de

it-sa.de

Kongress-Sponsor Platin:
ROHDE&SCHWARZ

Kongress-Sponsor Classic:
axway business. in motion.

Mit Unterstützung von:
ITSECURITY Bavarian IT Security & Safety Cluster

NÜRNBERG MESSE

Microsoft System Center 2012 (1)

Schaltzentrale in den Wolken

von Thomas Joos

Die neue Version 2012 von Microsoft System Center konzentriert sich vor allem auf die Verwaltung von Private Clouds. Dabei hat Microsoft die PowerShell-Integration deutlich verbessert. Das soll das Scripten erleichtern und eine Automatisierung von Verwaltungsaufgaben ermöglichen. Auch die Lizenzierung hat Microsoft vereinfacht und Editionen zusammengefasst. Lesen Sie in unserer dreiteiligen Workshopserie, was das neue System Center 2012 zu bieten hat. Zunächst geben wir Ihnen einen Überblick und zeigen, wie Sie die Microsoft-Suite optimal austesten.

Das neue System Center 2012 [1] ist nur noch als Paket erhältlich und soll die Server-Verwaltung im Unternehmen wesentlich verbessern. Die Produkte lassen sich nicht mehr einzeln erwerben, mit Ausnahme des Virenschutzes Endpoint Protection 2012. Für Unternehmen, die Vorprodukte eingesetzt haben, wie zum Beispiel System Center Virtual Machine Manager, kann sich durchaus eine Verteuerung ergeben, und zwar eine deutliche. Um Unternehmen den Einstieg zu ermöglichen, gibt es zwei Editionen von System Center 2012. Die Lizenzierung erfolgt auf Basis der verwalteten Endgeräte.

Produkte in System Center 2012 im Überblick

System Center 2012 besteht hauptsächlich aus acht Produkten:

- Der **System Center Configuration Manager 2012** (SCCM) dient vor allem der Verwaltung von Endgeräten und der installierten Anwendungen. Die neue Version hat vor allem die Anwender selbst und deren wechselnden Geräte im Fokus. Auch Smartphones lassen sich mit der neuen Version verwalten.
- Der **System Center Operations Manager 2012** (SCOM) hat vor allem die Überwachung der mit SCCM installierten Server und Netzwerkgeräte zum Schwerpunkt und ergänzt den SCCM.
- Der **System Center Data Protection Manager 2012** (SCDPM) stellt die Datensicherungslösung im System Center dar. Die Lösung kann alle Server im Netzwerk sichern und die Sicherungen zentral verwalten.
- Der Fokus des **System Center Service Manager 2012** ist die Anbindung als zentrale Verwaltungsoberfläche und Knotenpunkt für alle System Center-Produkte im Unternehmen sowie die Bildung von Schnittstellen und deren Verknüpfung und Automatisierung.
- Der **System Center Virtual Machine Manager 2012** (SCVMM) dient der Verwaltung der virtuellen Server im Netzwerk. Hier lassen sich neben Hyper-V auch andere Virtualisierungslösungen wie vSphere anbinden. Viele Unternehmen haben SCVMM außerhalb von System Center lizenziert und müssen in der neuen Version deutlich tiefer in die Tasche greifen.
- Der **System Center Orchestrator 2012** automatisiert IT-Prozesse. Microsoft hat das zugekaufte Produkt Opalis in SCO umbenannt und in der neuen Version für die Verwaltung mit der PowerShell erweitert. Wie Service Manager auch findet das Produkt derzeit nur wenig Anklang.
- Der **System Center App Controller 2012** soll dabei helfen, Anwendungen im Unternehmen zentral zu verwalten, und zwar in einer Private Cloud oder der Cloud eines Herstellers. Das Tool stellt Vorlagen für Anwendungen bereit, die sich über andere System Center-Produkte bereitstellen lassen.
- Bei **System Center Endpoint Protection 2012** handelt es sich um einen Virenschutz, der sich mit SCCM verwalten und verteilen lässt.

Neuerungen im System Center Configuration Manager 2012

Der "System Center Configuration Manager 2012" ist das wichtigste Produkt im neuen System Center. Microsoft integriert die Funktionen des bisherigen System Center Mobile Device Manager 2008 komplett in SCCM. Dieser bietet jetzt die Möglichkeit, Windows Phone 7/7.5-Geräte und andere Systeme zu verwalten. SCCM 2012 konzentriert sich im Gegensatz zu seinen Vorgängerversionen nicht auf die PCs der einzelnen Anwender, sondern auf die Anwender und die benötigten Applikationen selbst. Microsoft spricht dabei von einer benutzerorientierten Verwaltung (User Centric Management, UCM) im SCCM 2012.

Die Definition eines primären Gerätes hilft bei der Verteilung von Anwendungen. Umgekehrt können Sie auch einem Gerät mehrere Anwender zuweisen. Ferner lassen

Bild 1: Die Verwaltungsoberfläche von System Center Configuration Manager 2012 zeigt im Überblick den Navigationsindex

sich Geräten auch primäre Anwender zuweisen, die dann wiederum im System ihre Arbeitszeit hinterlegen können. Auf Basis dieser Daten entscheidet SCCM 2012 dann, welche Anwendungen mit den unterschiedlichen Technologien angebunden werden. Auf seinem primären Rechner erhält der Anwender zum Beispiel eine lokale Installation seiner benötigten Anwendungen. Arbeitet er an einem anderen Computer, erhält er Zugriff über App-V oder einen Remotedesktop.

Im Zuge dessen können Sie auch Abhängigkeiten zwischen Anwendungen konfigurieren, sodass immer die notwendigen Tools und Anwendungspakete auf den PCs installiert sind. SCCM kann Anwendungen auch wieder von PCs entfernen und deinstallieren. Die Installation von Anwendungen kann automatisiert erfolgen oder Anwender installieren die zugeordneten Programme über das neue Webinterface selbst auf ihrem Endgerät. Im Portal sehen Anwender dann alle Programme, die sie aktuell auf dem entsprechenden Gerät verwenden dürfen.

Rechnern, die Unternehmen im Schichtbetrieb einsetzen, können Administratoren auch mehrere primäre Anwender zuteilen. Über diesen Weg lässt sich die IT-Infrastruktur also sehr detailliert darstellen. Dazu nutzen Sie den Menüpunkt "Administration / Hierarchy Configuration / Discovery Methods". Über das Kontextmenü von "Active Directory User Configuration" lassen sich die Eigenschaften des Dienstes aufrufen. Der Assistent erlaubt auch die Anbindung mehrerer Filter zur Benutzerkonfiguration.

Automatische Suche nach Benutzern

Über die Registerkarte "Polling Schedule" legen Sie fest, wann und wie oft der Assistent nach neuen Benutzern sucht. Um primäre Geräte zuzuweisen, verwenden Sie in der Konsole den Bereich "Assets and Compliance / User Collections". Durch Klicken auf eine Sammlung lassen sich über das Menüband die Mitglieder der entsprechenden Sammlung anzeigen. Mit der Auswahl eines Benutzers über die rechte Maustaste lässt sich das primäre Gerät festlegen, mit dem der Benutzer arbeitet. Administratoren können Sie in SCCM verschiedene Regeln und Wege einrichten, über die eine Anwendung zur Verfügung steht. Das kann eine Installation sein, die Bereitstellung als virtuelles App-V-Paket oder als Remotedesktop. Auch Apps für mobile Endgeräte verwalten Sie auf diese Weise. Neben diesen Möglichkeiten lassen sich Anwendungen auch in Abhängigkeit zueinander setzen. Soll auf einem Computer zum Beispiel die Anwendung A installiert werden, die von B abhängig ist, dann installiert SCCM erst Anwendung B und anschließend Anwendung A.

Geräte, die an SCCM 2012 angebunden sind, wie etwa Windows 7-Rechner, verfügen in der Systemsteuerung über den neuen Bereich "Configuration Manager". Hierüber lassen sich verschiedene Einstellungen vorgeben und anzeigen, die die Geräte mit der System Center-Infrastruktur anbinden. SCCM hilft übrigens auch bei der Bereitstellung von Betriebssystemen im Unternehmen. Linux und Unix lassen sich mit SCCM 2012 besser verwalten als mit den Vorgängerversionen. Optimal unterstützt werden AIX, HP-UX, Red Hat Enterprise Linux, Solaris und Suse Linux Enterprise Server.

Auch die Aufteilung der Sites hat Microsoft überarbeitet. Die oberste Ebene einer SCCM 2012-Infrastruktur ist die "Central Administration Site" (CAS). Mit dieser lassen sich alle Standorte anbinden und verwalten. Der CAS sind keine Clients zugeordnet, sondern sie dient nur der zentralen Verwaltung aller Server und Sites. Einer CAS lassen sich daher mehrere primäre Sites zuordnen und zentral verwalten. Die CAS behält dazu Kontrolle über die Datenbank, die zentrale Konfiguration der SCCM-Infrastruktur und kann auch Berichte erstellen. Sekundäre Sites lassen sich zu Distribution Points herabstufen, primäre Sites lassen sich nicht mehr anpassen. Auf diese Weise ist die Verwaltung wesentlich einfacher als noch in den Vorgängerversionen. Ebenfalls neu ist die Funktion "Active Directory Forest Discovery". Damit erkennt und verwaltet SCCM 2012 mehrere Active Directory-Gesamtstrukturen. Die Verwaltungsoberfläche hat Microsoft ebenfalls komplett überarbeitet.

Rollenbasierte Rechtevergabe

SCCM 2012 arbeitet mit einer rollenbasierten Zugriffsberechtigung (RBAC), ähnlich wie Exchange Server 2010. Administratoren können die Verwaltung verschiedener Aufgaben an Benutzer delegieren. Dazu bietet das System Center bereits vorgefertigte Verwaltungsrollen an, zum Beispiel zur Verwaltung von Endpoint Protection.

Natürlich lassen sich auch eigene Rollen mit entsprechenden Rechten anlegen. Zur Verwaltung hinterlegen Administratoren zunächst die Benutzerkonten, die Verwaltungszugriff haben sollen, in der Management-Konsole des System Center. Dabei kann das System Center natürlich auch auf Benutzer aus dem Active Directory zugreifen. Die Benutzer lassen sich dann entsprechenden Verwaltungsrollen zuweisen und erhalten dadurch Verwaltungsrechte. Die Verwaltung der Rollen basiert zusätzlich zu den zugewiesenen Rollen noch auf Security Scopes. Dabei handelt es sich um Sammlungen von Geräten, die an das Sys-

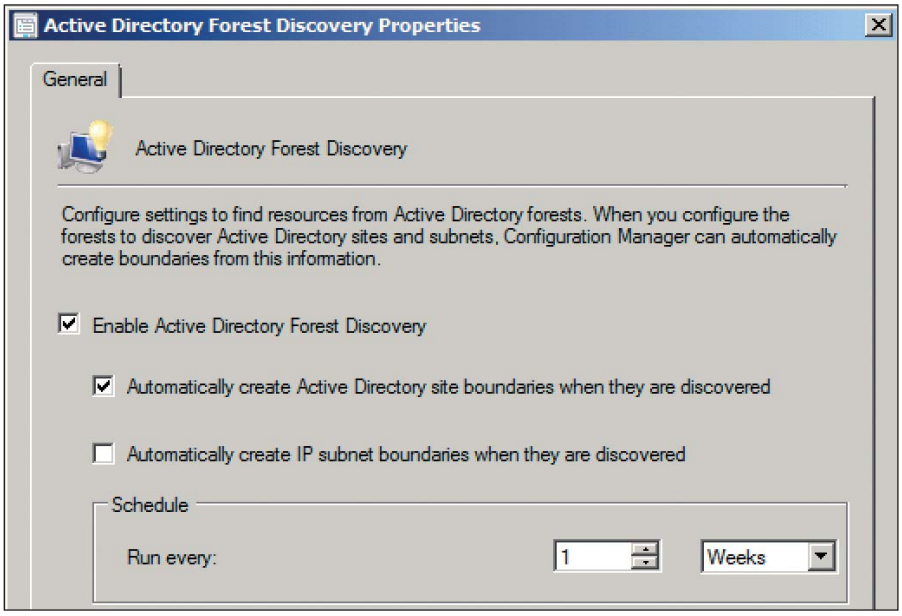


Bild 2: Das Durchsuchen des Active Directory zur Anbindung von Benutzern ist dank Scheduler in regelmäßigen Abständen möglich

tem Center angebunden sind. Security Scopes können zum Beispiel Computer einer Niederlassung sein, die nur bestimmte Administratoren verwalten dürfen.

Ebenfalls integriert ist das User State Migration Tool (USMT) 4.0, um Benutzereinstellungen zu übernehmen. Der PXE-Boot über das Netzwerk funktioniert wesentlich zuverlässiger und einfacher. Installationen von Anwendungen und Patches lassen sich in Offline-Bereitstellungen von WIM-Images integrieren und an angebundene Clients verteilen. Auch hier arbeitet SCCM 2012 wesentlich stabiler als die Vorgängerversionen.

Anbinden lässt sich noch Exchange Server 2010 für die Verwendung des Exchange Server-Connectors. Über diesen Connector liest SCCM 2012 ActiveSync-Richtlinien ein und leitet diese an die angebundenen Endgeräte weiter. SCCM 2007 unterstützt ältere Windows Mobile-Versionen mit eigenen Verwaltungsfunktionen. Diese überschneiden sich allerdings mit den ActiveSync-Richtlinien. Daher geht SCCM 2012 einen anderen Weg und bindet die Exchange ActiveSync-Richtlinien direkt von den Exchange-Servern ein. Hierbei handelt es sich um eine Technologie, die SCCM 2012 vom System Center Device Manager 2008 übernommen hat. Die entsprechenden Einstellungen dazu nehmen Sie direkt in den Eigenschaften des Exchange Server-Connectors vor. Über diesen Connector können Administratoren die angebundenen Endgeräte auch über das Internet löschen (Remote Wipe). Der Connector kann aber nicht nur Richtlinien von Exchange an die Clients weiterleiten, sondern auch Inventuren bei sämtlichen angebundenen Geräten durchführen.

Editionen und Lizenzen im Vergleich

Mit der Standard Edition sollen Unternehmen lokal installierte Server verwalten können – das gilt auch für virtuelle Server. Große Unternehmen lizenzieren die Datacenter Edition. Beide Pakete umfassen alle System Center-Produkte sowie die notwendigen Lizenzen für die Installation einer SQL Server-Datenbank. Der wesentliche Unterschied zwischen beiden Editionen besteht in den installierbaren Betriebssystemen. Die Standard Edition erlaubt zwei Betriebssysteme auf einem Server. Im Falle eines Hyper-V-Hosts also den Host selbst und einen virtuellen Server. Auch wenn Microsoft die Lizenzierung [2] vereinfacht hat, stecken noch viele Fallstricke im Detail. Allerdings müssen, was die Anzahl an installierten Betriebssystemen angeht, nur die verwalteten Systeme einbezogen werden. Verwaltungs-Server und Datenbankserver selbst zählen nicht mit.

Dann müssen Sie noch die Prozessoren der angebundenen Clientsysteme zählen. Auf dieser Basis ist dann eine Entscheidung notwendig, ob mehrere Standard Edition-Lizenzen günstiger sind als weniger Datacenter Editionen. Hinzu kommen noch die verschiedenen Verträge, die Unternehmen mit Microsoft eingehen können. Im Schnitt kostet die Datacenter Edition knapp das Dreifache der Standardedition (3.600 US-Dollar anstatt 1.300 Dollar). Die Datacenter Edition erlaubt allerdings auch eine unbegrenzte Anzahl an Systemen. Dabei werden pro Lizenz bei beiden Editionen wiederum nur zwei Prozessoren berücksichtigt. Die Anzahl der Kerne dieser CPUs spielt keine Rolle. Ein Server mit

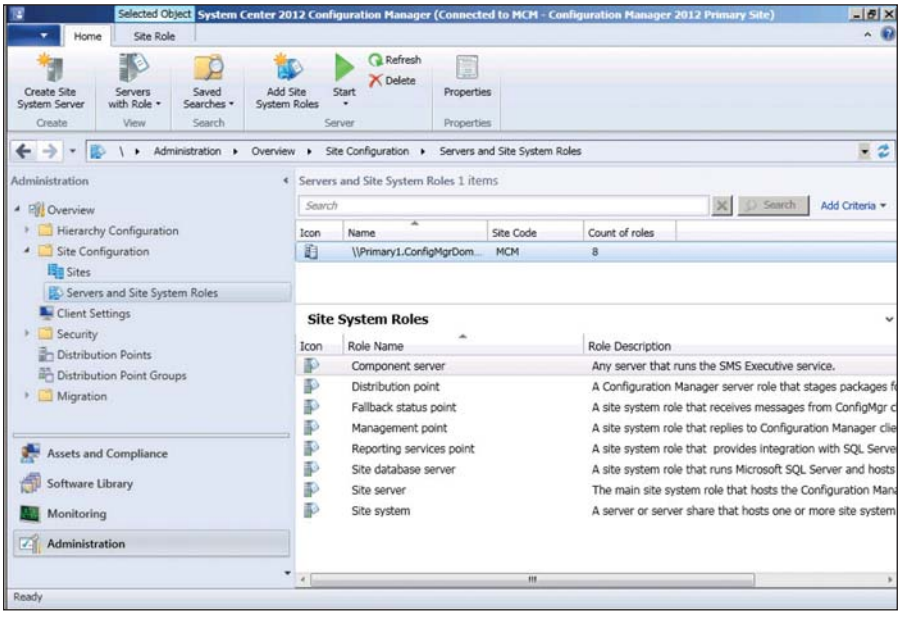


Bild 3: Das Verwalten einer System Center Configuration Manager-Infrastruktur ist über Site System Roles möglich

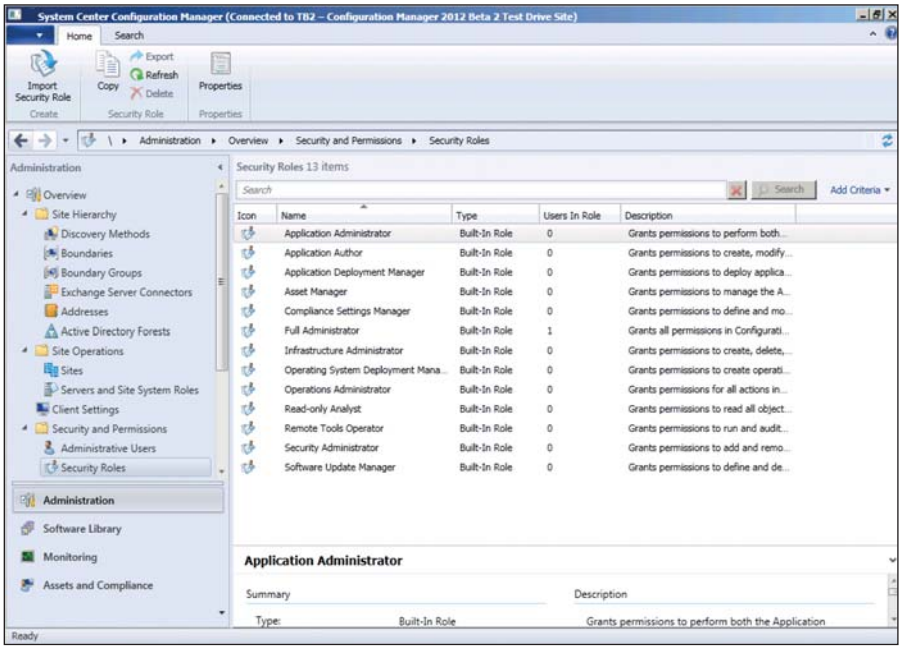


Bild 4: Die Administration der Berechtigungen in SCCM 2012 läuft über Security Roles ab und lässt sich so auch delegieren

vier Prozessoren benötigt daher zwei Lizenzen. Wer die Software einsetzen will, kommt daher um eine ausführliche Lizenzberatung nicht herum. Die Lizenzierung ist zwar simpler geworden, aber nicht wirklich einfach. Über ein Whitepaper [3] lassen sich die häufigsten Fragen beantworten.

Software-Verwaltung in System Center 2012

Um in System Center 2012 mit System Center Configuration Manager 2012 Anwendungen zur Verfügung zu stellen, definieren Sie zunächst ein primäres Gerät für den Anwender. Hierbei handelt es sich um den standardmäßigen Arbeitsplatz. Anwender können Programme, die sie benötigen, auch selbst aus dem Software-Katalog des SCCM 2012 auswählen und installieren. Dazu lassen sich über den Menüpunkt "Administration" in der Verwaltungskonsole für die einzelnen Sites in der Konfiguration Einstellungen vornehmen. Als Administrator müssen Sie für einzelne Sites den Server vorgeben, der den Katalog verwalten soll. Dazu ist es notwendig, die entsprechende Systemrolle auf einem Server in der Site zu installieren.

Die Installation erfolgt in der Verwaltungskonsole über "Servers and Site System Roles" auf der Registerkarte "Home". Neue Rollen installieren Sie über den Menüpunkt "Add Site System Roles". Starten Sie den Assistenten zur Installation von neuen Systemrollen, lassen sich der entsprechende Server und anschließend die Rolle auswählen, die auf dem Server installiert werden soll. Damit Anwender selbst Programme über den Anwendungskatalog auswählen können, sind in der Site die Rollen "Application Catalog Web Service Point" und "Application Catalog Website Point" notwendig.

Heterogene Netzwerke überwachen

In Microsoft System Center Operations Manager 2012 gibt es keinen Root Management Server (RMS) mehr, denn alle Verwaltungsserver arbeiten nun gleichberechtigt. Fällt ein Management-Server aus, übernehmen andere Server dessen Aufgaben. In Vorgängerversionen bis SCOM 2007 R2 musste in Umgebungen mit hochverfügbaren Servern der RMS-Server geclustert sein, um einen Ausfall zu verhindern. Management-Server in SCOM 2012 lassen sich nicht mehr clustern, sondern nur noch zu Gruppen zusammenfassen.

Anwendungen und Netzwerkhardware wie Switches, Firewalls oder Router können Sie mit SCOM 2012 effizienter überwachen. In diesem Bereich kann der Operations Manager die Leistung und Verfügbarkeit der Komponenten nun besser beurteilen und darstellen. Die neue Version erkennt zum Beispiel, an welchem Port eines Switches ein überwachter Server angeschlossen ist und überwacht diesen speziell. Auch für die Darstellung der Infrastruktur ist das sinnvoll. Für die bessere Überwachung einzelner Anwendungen im Netzwerk unterstützt SCOM 2012 Java JEE-Webanwendungen wie WebSphere 6.1/7, WebLogic 10 und 11, JBOSS und Tomcat. Sie haben dabei die Möglichkeit, SCOM 2012 auch über eine Webkonsole zu verwalten, wobei Ihnen Webparts für die Einbindung in das eigene Intranet etwa über SharePoint zur Verfügung stehen. Eigens zusammengestellte Dashboards bieten ferner alle wesentlichen Informationen auf einen Blick. Die Microsoft-Entwickler gehen in ihrem Blog unter [4] auf die Dashboards und deren Möglichkeiten genauer ein. Zusätzlich bietet die neue Version eine bessere Verwaltung über die PowerShell an.

Umfassende Linux-Unterstützung

SCOM 2012 arbeitet mit dem Sicherheitsmodell von Linux zusammen und erfordert nicht immer vollständige Root-Rechte. Nur wenn ein bestimmter Überwachungsprozess erweiterte Rechte benötigt, erhält dieser auch unter Linux mehr Rechte. Für eine effiziente Serverüberwachung müssen Sie prinzipiell einen Agenten von SCOM 2012 installieren. Dieser lässt sich auf den meisten Windows-Systemen einrichten; auch Linux-/Unix-Server überwacht das System mit eigenen Agents. Offiziell unterstützt Microsoft die folgenden Linux/Unix-Systeme:

- HP-UX 11i v2 und v3 (PA-RISC und IA64)
- Oracle Solaris 9 (SPARC) und Solaris 10 (SPARC und x86)

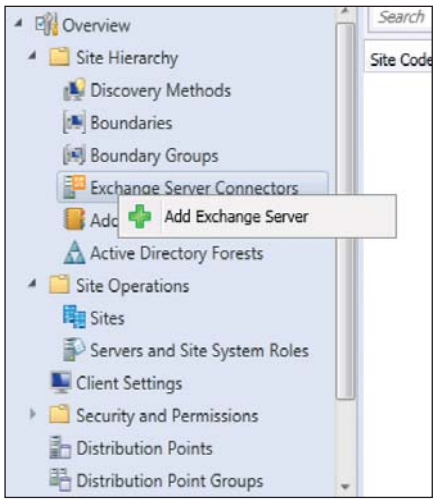


Bild 5: Per Mausklick lassen sich Exchange Server an SCCM 2012 anbinden

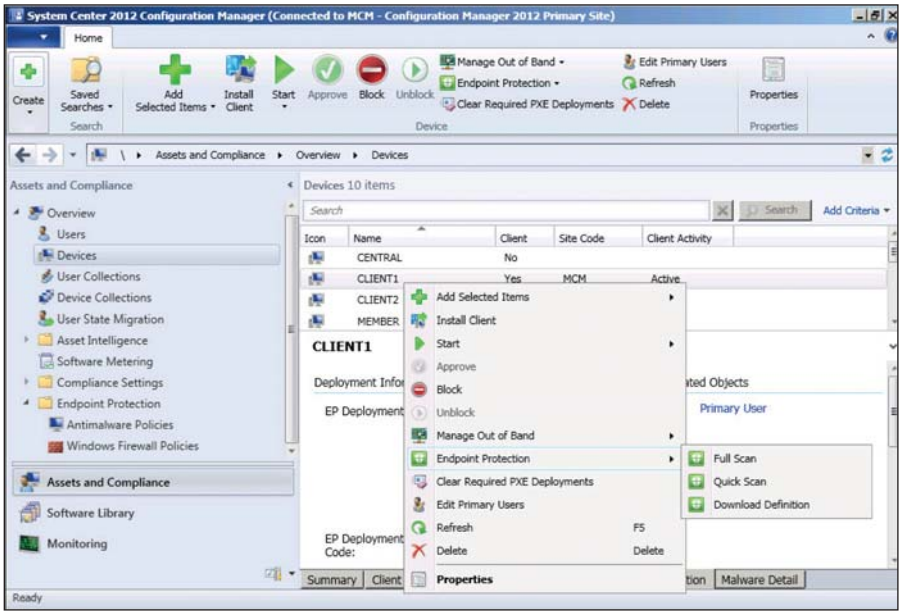


Bild 6: Die Clients überwachen Sie in der System Center-Verwaltungskonsole und starten von hier Virenscans

- Red Hat Enterprise Linux 4, 5 und 6 (x86/x64)
- Novell SUSE Linux Enterprise Server 9 (x86), 10 SP1 (x86/x64) und 11 (x86/x64)
- IBM AIX 5.3, AIX 6.1 (POWER) und AIX 7.1 (POWER)

Microsoft bietet noch das "UNIX/Linux Shell Command Template Management Pack" zum Download an. Mit diesem lassen sich in der Verwaltungskonsole von OPS 2012 Regeln erstellen, die Unix/Linux-Shell-Befehle zur Überwachung nutzen. Um solche Regeln einzubinden, ist allerdings einiges an Linux-Wissen notwendig. Unter [5] finden Sie einige Anleitungen zu diesem Thema.

Testumgebung mit System Center aufbauen

Testumgebungen mit System Center 2012 einzurichten, gestaltet sich meist ziemlich kompliziert. Um sich einen Überblick über System Center 2012 und die einzelnen Produkte zu verschaffen, verwenden Sie am besten eines der verschiedenen TechNet Virtual Labs [6]. Diese bieten verschiedene Bereiche des System Centers zum Testen an. Die Verbindung erfolgt dazu per Remotedesktop auf einen Testserver bei Microsoft. In zwei Webcasts [7] zeigt Microsoft die Neuerungen der neuen Version an. Administratoren mit TechNet-Abonnement können sich die neuen Versionen herunterladen [8].

Die Serverkomponenten von SCOM 2012 sollten Sie auf Servern mit Windows Server 2008 SP2 oder besser Windows Server 2008 R2 SP1 installieren. Die einzelnen Verwaltungsserver lassen sich nicht clustern. In vielen Fällen erscheint bei der Installation eine Fehlermeldung, dass sich SCOM 2012 nicht mit der Datenbank verbinden kann. In diesem Fall hilft auf dem SQL-Server der Befehl

```
mofcomp.exe "C:\Program Files
  (x86)\Microsoft SQL Server\100\
  Shared\sqlmgmproviderxpsp2up.mof"
```

Um die Webkonsole zu testen, müssen Sie auf dem Server zunächst die Rolle "Webserver (IIS)" über den Server-Manager installieren und anschließend das .NET Framework 4.0 [9]. Fehlen Komponenten, erscheinen entsprechende Meldungen bei der Installation des RC. Allerdings kann der Installationsassistent diese nicht beheben, ähnlich wie bei der Installation von SharePoint 2010.

Wurde das .NET-Framework 4 vor dem IIS installiert, hilft der Befehl

```
%WINDIR%\Microsoft.NET\Framework64\
  v4.0.30319\aspnet_regiis.exe -r
```

Dieser muss in einer Eingabeaufforderung mit Administratorrechten gestartet werden. Um die Webkonsole auf einem Server zu installieren, müssen außerdem noch ISAPI- und CGI-Einschränkungen konfiguriert werden, bevor die Installation von SCOM 2012 losgeht:

1. Starten Sie den IIS-Manager und klicken Sie auf den Namen des Servers.
2. Klicken Sie in der Mitte im Bereich IIS doppelt auf "ISAP- und CGI-Einschränkungen".
3. Klicken Sie mit der rechten Maustaste auf "ASP.NET v4.0" und wählen Sie "Zulassen" für beide Zeilen.

Anschließend lässt sich die Webkonsole auf dem Server installieren, wenn alle notwendigen Komponenten des IIS installiert sind. Fehlen Funktionen, können Sie diese über den Server-Manager nachinstallieren. Damit SCOM 2012 auf den SQL-Server zugreifen darf, sind unter Umständen noch Einstellungen auf dem SQL-Server notwendig. Zusätzlich müssen Sie auf dem SQL-Server eine neue Firewall-Regel erstellen, da die Firewall die beiden TCP Ports 1433 und 1434 blockiert:

Link-Codes

[1] System Center 2012
COP21

[2] System Center-Lizenzierung
COP22

[3] Lizenz-Whitepaper
COP23

[4] Blog zu Dashboards
COP24

[5] Contoso.se-Blog zu Linux-Einbindung
COP25

[6] TechNet Virtual Labs
COP26

[7] Webcasts zu System Center-Neuerungen
COP27

[8] System Center-Download in TechNet
COP28

[9] .NET Framework 4.0-Download
COP29

[10] Konfiguration der Windows-Firewall auf SQL-Servern
COP20

[11] TechNet-Artikel zu SQL-Überwachung
COP2A

[12] Vollständige Dokumentation zu Operations Manager
COP2B

1. Geben Sie dazu auf dem SQL-Server im Suchfeld des Startmenüs *wf.msc* ein.
2. Klicken Sie auf "Eingehende Regeln".
3. Klicken Sie rechts auf "Neue Regel".
4. Aktivieren Sie auf der ersten Seite des Assistenten zum Erstellen von neuen Firewall-Regeln die Option "Port".
5. Aktivieren Sie auf der nächsten Seite die Optionen "TCP" und "Bestimmte lokale Ports".
6. Geben Sie im Feld neben der Option "Bestimmte lokale Ports" den Wert "1433-1434" ein.
7. Aktivieren Sie auf der nächsten Seite die Option "Verbindung zulassen" sowie auf der folgenden Seite alle Profile. In sicheren Umgebungen genügt es, wenn Sie nur das Domänenprofil aktivieren.
8. Weisen Sie abschließend der Regel einen passenden Namen zu und bestätigen Sie die Erstellung.
9. Sollten immer noch Fehler erscheinen, schalten Sie über die Standardeinstellung der Firewall in der Systemsteuerung noch die Remoteverwaltung des Servers frei.

Auf der Seite [10] finden Sie ausführliche Hinweise zur Konfiguration der Windows-Firewall auf SQL-Servern. Funktioniert die Verbindung zum SQL-Server noch nicht, öffnen Sie auf dem SQL-Server den SQL Server Configuration Manager. Klicken Sie dann auf SQL-Server-Netzwerkkonfiguration und stellen Sie sicher, dass TCP/IP und Named Pipes aktiviert sind. Für den Zugriff über das Netzwerk ist vor allem TCP/IP notwendig, Named Pipes steuert den Zugriff auf dem lokalen Server. Diese Konfigurationen sind auch notwendig, wenn SharePoint 2010 auf einen SQL-Server zugreifen soll. Wie viele Server notwendig sind, um das Netzwerk zu überwachen, lesen Sie direkt im TechNet [11]. Eine vollständige Dokumentation der aktuellen Möglichkeiten stellt Microsoft ebenfalls im TechNet zur Verfügung [12].

Fazit

System Center 2012 bringt zahlreiche Neuerungen mit. Unternehmen, die allerdings bisher nur einzelne Microsoft-Produkte gekauft und lizenziert haben, müssen in System Center 2012 auch alle anderen Produkte lizenzieren. Das kostet mehr als vorher, teilweise deutlich mehr. Ob sich die zusätzlichen Produkte lohnen, lässt sich für jedes Unternehmen nur nach einer sorgfältigen Analyse festlegen. Aber in den seltensten Fällen sind alle Produkte im System Center notwendig.

Beabsichtigt ein Unternehmen aber ohnehin, neue Sicherungslösungen und einen Virenschutz zu erwerben, kann sich System Center 2012 lohnen. Die einzelnen Produkte sind ausgereift und bieten einen echten Mehrwert. Allerdings erweist sich die Verwaltung als sehr komplex, weshalb das Unternehmen mit Schulungskosten rechnen muss. Da Windows Server 2012 vor der Tür steht, gilt auch hier zu beachten, wie das neue Betriebssystem mit System Center 2012 zusammenarbeitet. Firmen, die bereits ein Produkt aus der System Center-Reihe einsetzen und planen auf Windows 8 und Windows Server 2012 zu migrieren, sollten mit einer Aktualisierung zu System Center 2012 deshalb besser warten. *(dr)*

Quelle: Yael Weiss – 123RF

Best Practices für Windows Server 2012

Voller Erfahrungen

von Ulf B. Simon-Weidner

Über die Jahre hinweg hat Microsoft Windows Server immer unternehmenstauglicher gemacht. Aber gerade wenn eine Installation zunächst besonders einfach erscheint, stellt sich die Frage, ob die zahlreichen Komponenten denn auch korrekt konfiguriert sind. Beim neuen Server 2012 bringt das Produkt selbst bereits viele Erfahrungen mit. Wir zeigen in diesem Workshop, wie Sie sich die Eigenintelligenz des Betriebssystems zu Nutze machen und die Software optimal für den produktiven Betrieb einrichten.

Installiert sind die Microsoft-Betriebssysteme ja immer recht einfach und mittlerweile auch schnell. Auch Rollen und Funktionen lassen sich flott hinzufügen. Aber wie sieht es mit den Best Practices aus, also denjenigen Erfahrungen, die sich seit Jahren angesammelt haben und Empfehlungen darstellen?

Gerade in diesem Bereich hat das Server-Betriebssystem aus Redmond über die Zeit einiges mitbekommen. Hat sich ein Internet Information Server unter Windows 2000 noch mit fast allen Diensten, Protokollen und Erweiterungen installiert, wurde dies über die Jahre geändert und der Administrator muss sich im Detail damit auseinandersetzen, welche Unterkomponenten die Webanwendung benötigt. Waren der Domänencontroller installiert und die Standard-Vorgaben akzeptiert, sah Microsoft bis Windows Server 2003 R2 nur einen Server für den wichtigen Globalen Katalog vor. Und im DNS waren die Standard-Installationseinstellungen für Domänen unter Windows 2000 nicht wirklich tauglich für Unternehmen mit mehreren Domänen.

Um aktuelle Best Practices in jedem Unternehmen zu etablieren, geht Microsoft verschiedene Wege:

- Anfragen bei dem Microsoft Support werden analysiert und die häufigsten Fehlerursachen dahingehend untersucht, ob eine Änderung der standardmäßigen Installation der Komponenten dazu führen kann, solche Fehler bei der überwiegenden Zahl an Kunden zu vermeiden.
- Die Installation des Betriebssystems beziehungsweise dessen Komponenten wird dahingehend optimiert, standardmäßig für die meisten Unternehmen optimal eingestellt zu sein.
- Ein Best Practice Analyzer wurde in das Betriebssystem mit eingebaut.

In den vergangenen Jahren hat Microsoft immer wieder Sicherheitshürden als neue Standards in sein Betriebssystem eingebaut. Hierbei ging es weniger darum, Unternehmen dazu zu zwingen, veraltete Technologien abzuschalten, sondern vielmehr bekannt gewordene und potentielle Sicherheitslücken zu schließen, um vor möglichen Gefahren zu schützen. Häufig sind diese Anpassungen aber nur bei Neuinstallationen zu finden – wenn ein Unternehmen seine Server-Infrastruktur von einem Betriebssystem auf die nächste oder übernächste Generation aktualisiert, werden häufig die Sicherheitseinstellungen übernommen, um eine Funktionalität des Gesamtsystems nicht zu gefährden. Daraus ergibt sich aber, dass migrierte Infrastrukturen einen höheren Bedarf an der Analyse von Sicherheitsmängeln und sonstigen Best Practices haben. Aber gehen wir zunächst auf einen anderen Punkt ein, die von Anfang an geänderten standardmäßigen Optionen von Betriebssystem und Komponenten.

Schlanke Rollendienste

Installieren Sie einen Internet Information Server, dann erfolgt dies zunächst nur mit minimalen Rollendiensten. Alles Weitere müssen Sie explizit anfordern. Bei der Installation eines Active Directory mit DNS-Server werden die Zonen so eingerichtet, wie es für Unternehmen mit mehreren Domänen und Standorten passt, ohne dabei die Firmen zu schädigen, die nur eine Domäne in einem Standort haben. Und der Assistent zur Inbetriebnahme eines Domänencontrollers macht mittlerweile jeden DC zum globalen Katalogserver, anstatt sich darauf zu verlassen, dass der Administrator hieran nach dem Starten der Komponente denkt.

Ein weiterer Schlüsselaspekt der Sicherheit und für Best Practices ist das Anwenden von Sicherheitsupdates. Dies ist in vielen Unternehmen in den vergangenen Jahren, insbesondere durch Dienste wie den Windows Software Update Service oder

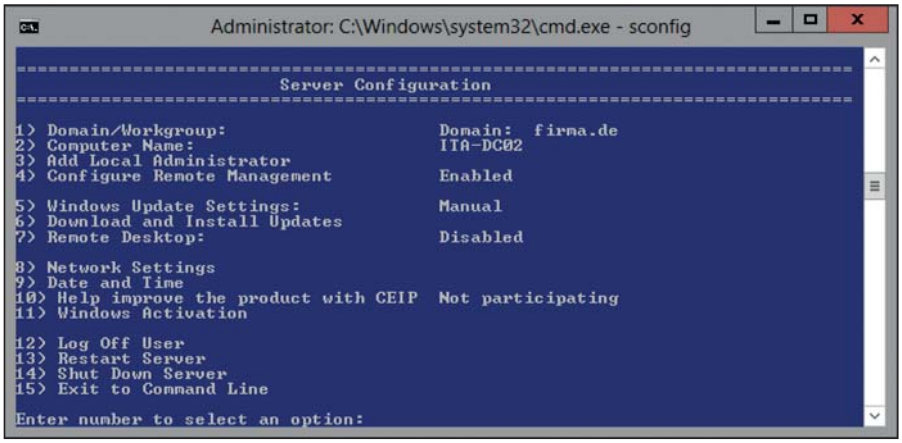


Bild 1: Wie in MS DOS-Zeiten: Für die Verwaltung des Server Core gibt es mit *sconfig.exe* jetzt ein aufwändiges, menüartiges Konfigurationstool

System Center Configuration Manager, deutlich besser geworden.

Server Core jetzt Standard

Um die Angriffsfläche und die damit zu aktualisierenden Komponenten zu reduzieren, hat Microsoft mit dem Windows Server 2008 den Server Core eingeführt. Ein Serverbetriebssystem, das vollständig auf Internet Explorer, Media Player, ja sogar auf Startmenü, Windows Explorer, Taskleiste und die meisten grafischen Komponenten verzichtet, aber dennoch in der Lage ist, viele Rollendienste zur Verfügung zu stellen. Sie mussten sich als Administrator aber bereits bei der Installation entscheiden, ob Sie einen vollen Server bevorzugen oder den reduzierten (und dadurch performanteren) Server Core. Entschieden Sie sich später um, mussten Sie bisher den Server neu installieren.

Hier ist Microsoft mit Windows Server 2012 ein Generationswechsel gelungen. Zum einen ist Server Core die standardmäßig vorgeschlagene Installationsoption und wird somit als Best Practice empfohlen. Er unterstützt auch die PowerShell, lässt sich über Verwaltungskonsolen auf anderen Systemen verwalten und bringt den Konfigurationsassistenten *sconfig.exe* für allgemeine Aufgaben mit. Aber insbesondere müssen Sie sich nicht schon bei der Installation final entscheiden, welche Option die richtige für Ihren Server ist.

Auf Wunsch: Reduzierte Management-Oberfläche

Zudem gibt es einen weiteren Modus: Der Server mit Management-Oberfläche verzichtet weiterhin auf den Windows Explorer, Internet Explorer und die meisten Komponenten der grafischen Benutzeroberfläche, jedoch steht der Server Manager wie viele weitere Verwaltungskonsolen für die Rollen in gewohnter Oberfläche zur Verfügung.

Besonders zu erwähnen gilt, dass Sie jetzt zwischen den Modi wechseln können. Durch die Installation weiterer Komponenten machen Sie aus einem Server Core einen Server mit Verwaltungsoberfläche oder einen vollen Server, und das Gleiche geht auch anders herum. So ist es zum Beispiel denkbar, dass Sie den Server zunächst mit voller Funktionalität oder der reduzierten, grafischen Verwaltungsoberfläche einrichten, um danach auf Server Core zu wechseln. Oder Sie installieren einen Server Core, um dann festzustellen, dass Applikationen auf dem Server die volle Installation benötigen. In diesem Fall installieren Sie einfach die weiteren Komponenten nach.

Vollständiges Löschen der Installationspakete

Eine weitere Option besteht darin, vom Server Komponenten nicht nur zu deinstallieren, sondern zu löschen. Seit Windows Server 2008 und Vista haben die Betriebssysteme aufgehört nach der CD/DVD zu fragen, wenn weitere Komponenten installiert werden sollten. Die Dateien dafür sind immer komprimiert auf jedem System. Um einen möglichst abgespeckten Server Core bieten zu können, können Sie nicht benötigte Komponenten jetzt aber komplett entfernen – auch die gepackten Installationsimages. Dies geschieht, indem Sie dem PowerShell-Cmdlet "disable-WindowsOptionalFeatue" den Parameter "-remove" hinzufügen.

Auch der umgekehrte Weg ist deutlich einfacher geworden: Standardmäßig werden Komponenten, deren Installationsdaten von der Festplatte entfernt wurden, diese Informationen von Windows Update aus dem Internet beziehen. Sie haben aber die Möglichkeit, eine Windows Server-Installation im Netzwerk als Datenquelle anzugeben oder können mit wenigen Schritten sogar die Installationsquelle von DVD verwenden.

Pakete von DVD nachladen

Um gelöschte Installationsdaten wieder von einer DVD nachzuladen, sind ein paar Zwischenschritte notwendig: Zunächst müssen Sie sich entscheiden, welche Quelle aus dem Installationsimage auf der DVD die Komponenten enthält. Dies ist entweder die Edition "Enterprise" oder "Datacenter" ohne die Core-Option (Windows Server

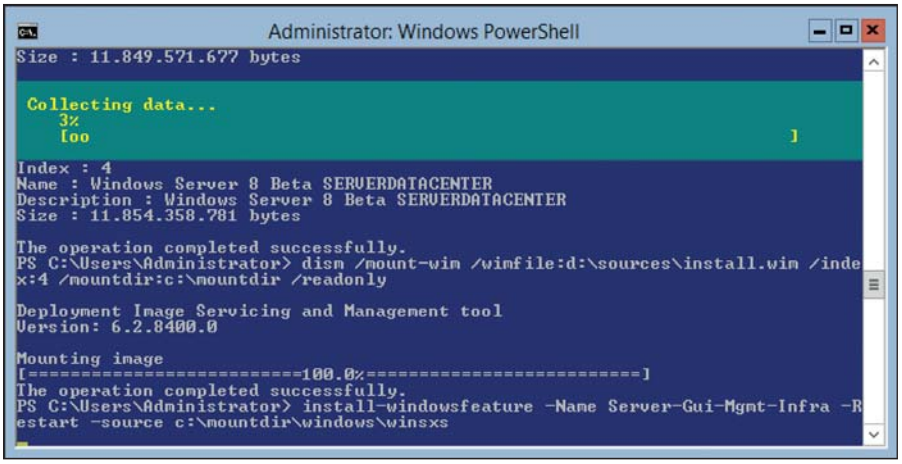


Bild 2: Sie können auf einem Server Core jederzeit die grafische Benutzeroberfläche nachinstallieren, sei es nur für die Verwaltung oder sogar vollständig mit Windows Explorer und Taskbar

gibt es nur noch in diesen zwei Varianten, die außer der Lizenzierung für virtuelle Maschinen keine technischen Unterschiede haben). Hiervon benötigen Sie den Index der Installationsoption in *install.wim*, die Sie mit dem folgenden Kommando ermitteln:

```
Dism /get-wiminfo /wimfile:DVD-
  Pfad:\sources\install.wim
```

Als Nächstes erstellen Sie einen Ordner, in den das Installationsimage gemounted werden kann:

```
Mkdir c:\installwim
```

Danach mounten Sie das Installationsimage in den Ordner:

```
Dism /mount-wim /wimfile:DVD-
  Pfad:\sources\install.wim
  /index:Indexnummer
  /mountdir:c:\installwim /readonly
```

Mit der PowerShell zur GUI

Im Anschluss richten Sie die Rollen und Features ein. Wollen Sie von Server Core auf den Server mit der Verwaltungsoberfläche wechseln, geschieht das über das folgende Kommando:

```
Powershell.exe
Install-WindowsFeature Sever-Gui-
  Mgmt-Infra -Restart -Source c:\
  installwim\windows\winsxs /readonly
```

Für den vollen Server geben Sie das Feature mit "Server-Gui-Mgmt-Infra,Server-Gui-Shell" an. Nachdem Sie die Installation durchgeführt haben, können Sie mit

```
dism /unmount-wim /mountdir:c:\
  installwim /discard
```

das Mounten des Images wieder aufheben und den Ordner "installwim" löschen.

Nicht ohne den Best Practice Analyzer

Beim Erstellen einer neuen Domäne greifen zahlreiche Änderungen in der Sicherheit. Verschlüsselungsoptionen werden eingeschaltet, anonyme Zugriffe verweigert – alles Einstellungen, die sicherer sind und mit denen Windows gut zurechtkommt. Aber was ist, wenn die Infrastruktur heterogen ist? Um heterogene Infrastrukturen oder auch Unternehmensnetzwerke mit zahlreichen Anwendungen bei einer Migration zu unterstützen, finden die neuen Sicherheitseinstellungen bei einer Migration häufig keine Anwendung: Sie müssen selbst wissen, was die neuen Best Practices sind, die relevanten Anwendungen und Systeme dahingehend prüfen und die Konfigurationsoptionen im Nachgang aktivieren. Ein schwieriges Unterfangen.

Hier hilft der Best Practice Analyzer (BPA). Diese Komponente ist fest in den Server Manager, die standardmäßige Verwaltungsoberfläche unter Windows Server 2012, integriert. Der Servermanager ist in der Lage, viele Server gleichzeitig zu verwalten und fasst diese nach den installierten Rollen zusammen. Sie können natürlich auch eigene Servergruppen bilden. Diese verwalten Sie dann einfach so wie nur einen Server, egal ob Sie ein weiteres Feature aktivieren wollen oder ob Sie Eventlogs von allen Servern einlesen wollen. Auch der BPA wird über alle Systeme hinweg ausgelesen und gibt Empfehlungen, was anzupassen ist.

Server Manager als Zentrale

Standardmäßig warnt der Server Manager, wenn er keine BPA-Ergebnisse der verbundenen Server finden kann. Dies liegt zunächst einfach daran, dass der BPA nicht automatisch läuft. Sie müssen diesen initiieren oder als Scheduled Task einrichten. Wenn im Server Manager weitere Server hinzugefügt wurden, können Sie den BPA gleich auf mehreren Servern gleichzeitig starten. Windows Server 2012 lassen sich standardmäßig hinzufügen, da bei diesen das Remote Management bereits aktiviert ist. Wollen Sie es deaktivieren oder haben Sie es versehentlich deaktiviert und möchten dies rückgängig machen, ist dies im Bereich "Lokaler Server" des Server Managers möglich. Für den Server Core lässt sich dies über *sconfig.exe* erledigen.

Regelsätze schaffen Klarheit

Der BPA untersucht verschiedene Kategorien an Regelsätzen, die sich aus Erfahrungen und Anfragen bei den Support Services zusammensetzen sowie den Erkenntnissen neuer Betriebssysteme, die bei einer Migration nicht berücksichtigt werden. Diese sind:

- Sicherheitsregeln, die entweder zu Datenverlust oder Schaden führen können oder nicht autorisierten Personen Einsicht in vertrauliche Daten ermöglichen.
- Leistungsregeln, bei denen Server dem Risiko ausgesetzt sind, nicht performant zu laufen.
- Konfigurationsregeln, mit denen sichergestellt wird, dass die Konfiguration einer Rolle den bekannten Best Practices entspricht.
- Richtlinienregeln für Best Practices im Bereich der Gruppenrichtlinien.

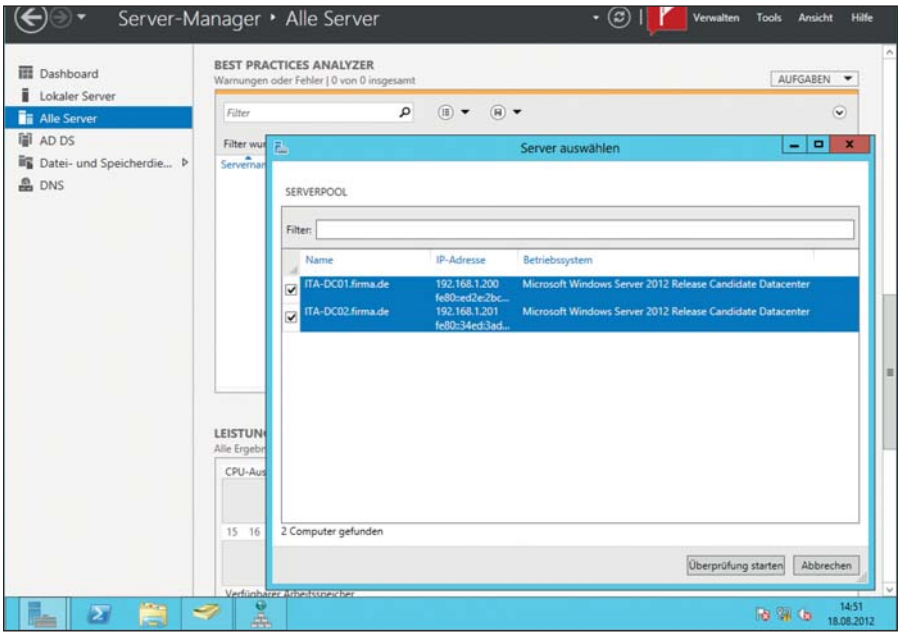


Bild 3: Der Best Practice Analyzer kann über den Server Manager bei mehreren Systemen gleichzeitig die Best Practices analysieren

- Vorgangsregeln, die zum Beispiel überprüfen, ob bestimmte administrative Rollen ihren zugedachten Tätigkeiten nachgehen können.
- Pre-Deployment-Regeln, mit Hilfe derer der Servermanager bei der Installation einer neuen Rolle überprüft, ob die Voraussetzungen für diese optimal geschaffen sind.
- Post-Deployment-Regeln, die überprüfen, ob eine kürzlich installierte Rolle korrekt funktionieren kann.
- Voraussetzungsregeln, mit denen sich feststellen lässt, ob der BPA selbst seine Dienste korrekt ausführen und überhaupt alle relevanten Daten erhalten kann.

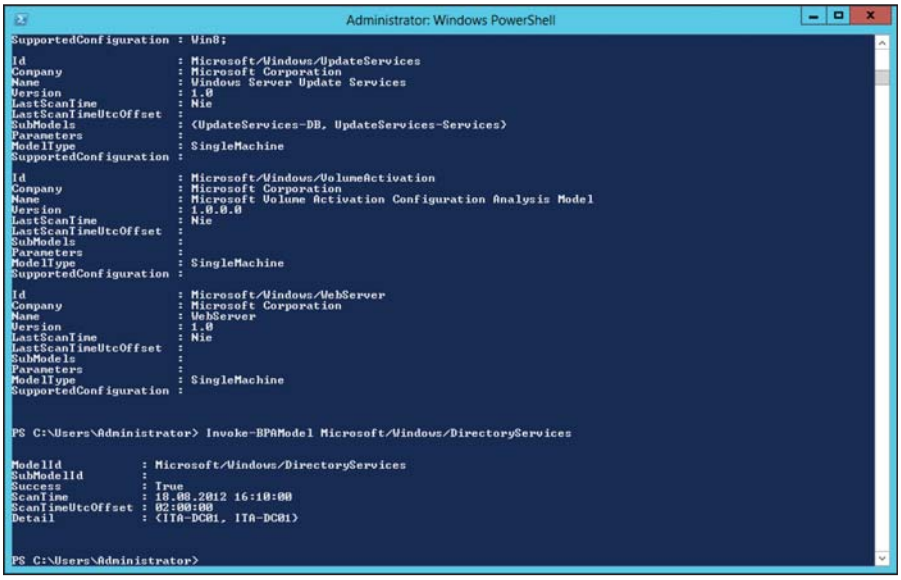
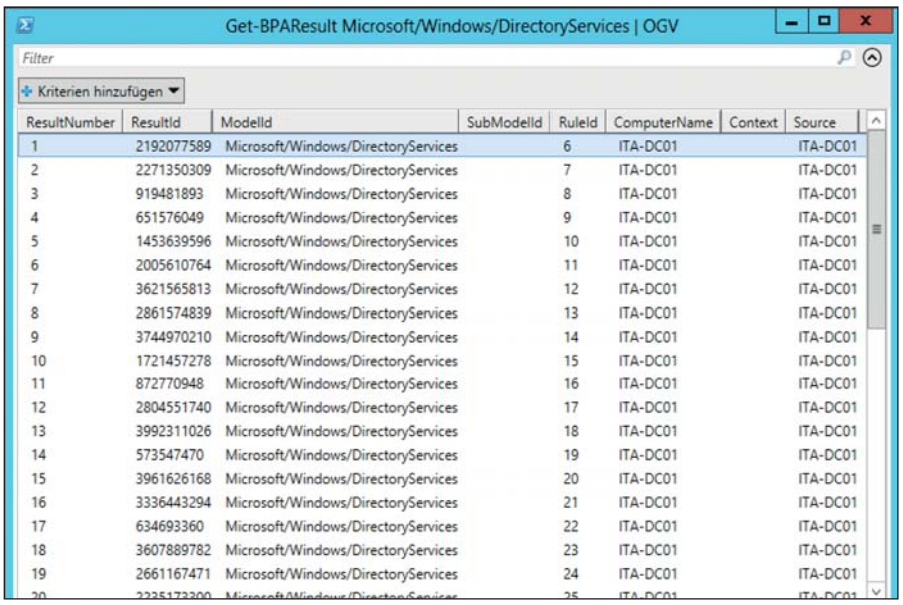


Bild 4: Best Practices lassen sich auch über die mächtige PowerShell 3.0 analysieren

Den BPA starten Sie direkt über den Servermanager. Hierzu wählen Sie entweder in der Gruppe "Alle Server" den Best Practice Analyzer aus und entscheiden sich im Menü "Aufgaben" für den Punkt "BPA-Überprüfung starten". Anschließend geben Sie dann an, für welche der angeschlossenen Server der BPA ausgeführt werden soll, oder Sie wählen den BPA direkt aus einer bereits installierten Rolle (zum Beispiel Domänendienste, Dateidienste), um explizit diesen Teil der Best Practices-Analyse zu starten.

BPA über die PowerShell

Alternativ können Sie die Analyse über die PowerShell ausführen oder als gespeicherte Aufgabe regelmäßig durchführen lassen. Gespeicherte Aufgaben richten Sie auch über Gruppenrichtlinien-Präferenzen ein, sodass Sie die Möglichkeit haben, diese Scans per GPO jedem Server in Auftrag zu geben. Dabei kommen die PowerShell-Kommandos "Get-BPAModel", "Invoke-BPAModel", "Get-BPAResult" und "Set-BPAResult" zum Einsatz.



ResultNumber	ResultId	ModelId	SubModelId	RuleId	ComputerName	Context	Source
1	2192077589	Microsoft/Windows/DirectoryServices		6	ITA-DC01		ITA-DC01
2	2271350309	Microsoft/Windows/DirectoryServices		7	ITA-DC01		ITA-DC01
3	919481893	Microsoft/Windows/DirectoryServices		8	ITA-DC01		ITA-DC01
4	651576049	Microsoft/Windows/DirectoryServices		9	ITA-DC01		ITA-DC01
5	1453639596	Microsoft/Windows/DirectoryServices		10	ITA-DC01		ITA-DC01
6	2005610764	Microsoft/Windows/DirectoryServices		11	ITA-DC01		ITA-DC01
7	3621565813	Microsoft/Windows/DirectoryServices		12	ITA-DC01		ITA-DC01
8	2861574839	Microsoft/Windows/DirectoryServices		13	ITA-DC01		ITA-DC01
9	3744970210	Microsoft/Windows/DirectoryServices		14	ITA-DC01		ITA-DC01
10	1721457278	Microsoft/Windows/DirectoryServices		15	ITA-DC01		ITA-DC01
11	872770948	Microsoft/Windows/DirectoryServices		16	ITA-DC01		ITA-DC01
12	2804551740	Microsoft/Windows/DirectoryServices		17	ITA-DC01		ITA-DC01
13	3992311026	Microsoft/Windows/DirectoryServices		18	ITA-DC01		ITA-DC01
14	573547470	Microsoft/Windows/DirectoryServices		19	ITA-DC01		ITA-DC01
15	3961626168	Microsoft/Windows/DirectoryServices		20	ITA-DC01		ITA-DC01
16	3336443294	Microsoft/Windows/DirectoryServices		21	ITA-DC01		ITA-DC01
17	634693360	Microsoft/Windows/DirectoryServices		22	ITA-DC01		ITA-DC01
18	3607889782	Microsoft/Windows/DirectoryServices		23	ITA-DC01		ITA-DC01
19	2661167471	Microsoft/Windows/DirectoryServices		24	ITA-DC01		ITA-DC01

Bild 5: In der PowerShell lässt sich die Ausgabe der BPA-Reporte formatieren: Außer der hier gezeigten filterbaren Tabellenansicht stehen HTML oder CSV zur Auswahl

Zunächst starten Sie die PowerShell 3.0 von einem Windows Server 2012. Hierbei müssen Sie keine Module mehr importieren – die PowerShell stellt automatisch fest, wenn Sie Kommandos ungeladener Module ausführen, und lädt diese selbstständig nach. Als Nächstes tippen Sie den Befehl *Get-BPAModel* ein. Sie erhalten dann alle "Model-IDs" von Komponenten, die im BPA verfügbar sind. Danach führen Sie den BPA-Scan mit dem Kommando *Invoke-BPAModel* aus, indem Sie die identifizierten Model-IDs, die Sie ausführen möchten, mit Kommas getrennt hinter den Befehl hängen.

Anzeigen der BPA-Daten

Nachdem der BPA durchgelaufen ist, können Sie dessen Ergebnisse einsehen. Sie finden sowohl im Bereich "Alle Server" des Server Managers die kritischen Fehler aller verbundenen Server wie auch Details zu den jeweiligen Diensten. Hierbei ist jeweils darauf zu achten, dass nur die Daten des Servers angezeigt werden, der im Bereich "Server" auf der jeweiligen Seite markiert ist. Wie in Windows üblich, können Sie mehrere Systeme gleichzeitig markieren und so die Ergebnisse verschiedener Server gleichzeitig auf den Bildschirm bringen.

Natürlich können Sie sich die Daten auch in der PowerShell ansehen. Hier sind besonders die Filter- und Exportmöglichkeiten interessant.

Indem Sie die Ergebnisse an den Online-GridViewer übertragen, können Sie die Ergebnisse in einer filterbaren Tabelle betrachten und auswerten:

```
Get-BPAResult Microsoft/Windows/
  DirectoryServices | OGV
```

Des Weiteren dürfte auch die Exportfunktion in eine HTML-Datei von Interesse sein:

```
Get-BPAResult Microsoft/Windows/
  DirectoryServices | ConvertTo-Html
  | Set-Content ($env:userprofile +
  "\Desktop\BPAResult.htm")
```

Finale Bewertung bleibt Admin-Sache

In unserer auf zwei Domänencontroller beschränkten Workshop-Umgebung fand der BPA nicht weniger als 43 Warnungen oder Fehler. Diese gingen wir Schritt für Schritt durch, wobei jedoch etwas Erfahrung notwendig war. Zum einen fanden sich viele Ergebnisse, die ganz einfach der Testumgebung geschuldet waren. Nachdem diese abgeschottet läuft, war etwa kein externer Zeitdienst eingerichtet. Auch war klar, dass die DNS-Auflösung ins Internet nicht funktioniert, was aber in diesem Fall so gewollt war.

Viele Ergebnisse stellen aber in der Regel tatsächlich Best Practices dar, die Sie implementieren sollten. So sind zum Beispiel nicht alle organisatorischen Einheiten vor versehentlichem Löschen geschützt – ironischerweise hat Microsoft selbst vergessen die OU "Domaincontrollers" vor versehentlichem Löschen zu schützen. Dies sollten Sie unbedingt nachholen.

Weitere Ergebnisse regen zum Nachdenken an: So wird angeregt, die 8.3-Namen im Dateisystem abzuschalten. Existieren noch alte Anwendungen wie DOS-Bootdisketten, die eigene Installationen durchführen, könnten diese zwar noch benötigt werden, dies ist aber eher unwahrscheinlich. In Industriebetrieben, wo gegebenenfalls Robotersysteme auf Dateidaten zugreifen, ist dies schon wieder nicht so undenkbar.

Haben Sie die Best Practice-Empfehlungen eingeholt, bleibt es Ihnen überlassen, diese Schritt für Schritt zu bewerten. Hierbei können Sie bestimmte Meldungen bei zukünftigen Scans ausschließen. Dies sollten Sie jedoch nur machen, wenn Sie sich sicher sind, dass diese keinen Ihrer Kollegen interessieren: Einmal ausgeschlossen, bleiben die Meldungen für alle unsichtbar. Möchten Sie sich hingegen nur auf bestimmte Meldungen konzentrieren und ein Kollege analysiert weitere Meldungen später, sollten Sie statt dem Ausschließen die Filtermöglichkeiten in der grafischen Benutzeroberfläche oder der PowerShell nutzen.

Fazit

Windows Server 2012 bietet mit der Installation der Rollen, mit den neuen Möglichkeiten im Bereich Server Core sowie dem Best Practice Analyzer vielfältige Wege, die Server-Infrastruktur im eigenen Unternehmen zu optimieren und von den Erfahrungen anderer zu profitieren. Der BPA wird immer wieder aktualisiert und angepasst, Meldungen lassen sich Server- und Rollen-übergreifend betrachten und gewollte "Missstände" von den Scans ausschließen.

Trotzdem sind nach wie vor Erfahrungen der Administratoren notwendig, da viele Meldungen auf dem Schirm erscheinen, die gegebenenfalls in diesem Szenario korrekt oder gewollt sind. Aber sowohl die weniger erfahrenen Administratoren wie auch die alten Hasen profitieren von den neuen Möglichkeiten und den guten Ratschlägen, ob Sie sie nun annehmen oder aus gutem Grund beiseitelegen. *(ln)*

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

Wie in der physikalischen werden ja auch **in der virtuellen Welt MAC-Adressen** für die Kommunikation im Netzwerk benötigt. Dazu stellt Hyper-V den virtuellen Maschinen meines Wissens nach den sogenannten **MAC Address Pool** zur Verfügung. Virtuelle Maschinen lassen sich **bei Hyper-V mit einer dynamischen oder einer statischen MAC-Adresse** konfigurieren. Können Sie kurz erklären, welche Variante unter welchen Voraussetzungen mehr Sinn macht und wie sich gerade Host-übergreifende **doppelte Vergaben vermeiden** lassen?

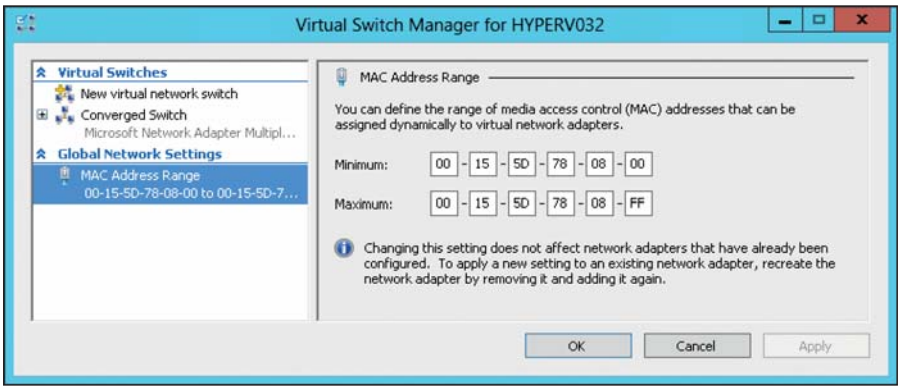
Eine statische Konfiguration ist vor allem dann sinnvoll, wenn eine spezielle Applikation oder Konfiguration dies erfordert. Ansonsten empfiehlt es sich, die Vergabe dynamisch respektive automatisch durch den Hypervisor vorzunehmen zu lassen. Hyper-V nutzt ein Algorithmus, um die Vergabe von doppelten MAC-Adressen auf einzelnen Hosts zu verhindern, allerdings funktioniert dies nicht Host-übergreifend. Jeder Hyper-V-Host verfügt über einen eigenen Bereich an MAC-Adressen. Die einzelnen Adressen bestehen jeweils aus zwei Teilen, dem OEM Identifier und dem Unique Value. Der OEM Identifier, die ersten drei Oktette, wurde speziell hierfür durch Microsoft registriert und ist auf sämtlichen Hyper-V-Hosts gleich (00-15-5d). Der Unique Value wird anhand der letzten zwei Oktette der IP Adresse generiert, die dem ersten Network Adapter zugewiesen wurde. Ein Hyper-V-Host kann somit über 256 MAC-Adressen bereitstellen, die sich für virtuelle Maschinen, aber auch für die Internal Virtual Adapters nutzen lassen. Besonders wegen dieser Adapter, die zum Einsatz kommen, um einen Virtual Switch mit dem Management-OS zu teilen, sollten Sie sicherstellen, dass kein Host MAC-Adressen aus der gleichen Range nutzt. Die Informationen zum MAC Address Pool findet sich beim Hyper-V-Host in der Registry unter "HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \ Virtualization". Setzen Sie "00" als "MinimumMacAddress" und "FF" als "MaximumMacAddress" ein, was die Default-Einstellung ist, stehen dem Host 256 unterschiedliche MAC-Adressen zur Verfügung. Am einfachsten können Sie diese Einstellung unter "Hyper-V Management Tools / Virtual Switch Manager" editieren. Mit Windows Server 2012 können Sie diese Anpassung nun auch mittels PowerShell vornehmen:

```
Set-VMHost -MacAddressMinimum "00-15-5D-78-80-00" -MacAddressMaximum "00-15-5D-78-8F-FF"
```

Dieses Beispiel erhöht den Pool von 256 auf 4.096 mögliche MAC-Adressen. Beachten Sie hierbei jedoch, dass bereits genutzte MAC-Adressen vom System nicht automatisch angepasst werden. Daher sollten Sie die Konfiguration bereits dann in Angriff nehmen, bevor Sie virtuelle Maschinen oder interne Netzwerkadapter erstellen. Achtung: Setzen Sie den System Center 2012 Virtual Machine Manager für das Deployment von virtuellen Maschinen ein, kommt allerdings ein ganz anderer Address Pool zum Einsatz. Dieser Pool gilt dann für alle Hosts und stellt sicher, dass keine doppelten MAC-Adressen vergeben werden. Die für SCVMM reservierte Range ist "00:1D:D8:B7:1C:00" bis "00:1D:D8:F4:1F:FF".

(Michel Lüscher/ln)

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



Mit dem Virtual Switch Manager passen Sie die MAC Address Range für virtuelle NICs an

Es gibt ja so gut wie kein Programm mehr, das keine **Verbindung zum Internet** aufbaut: Nicht nur Virenscanner, Internetbrowser oder Tools wie RSS-Feedreader arbeiten online, sondern auch die **übrigen Programme überprüfen auf den Herstellerseiten**, ob es neue Versionen gibt oder übertragen sogar Daten. Aber auch Viren und Trojaner kommunizieren ins Internet. Gibt es eine **einfache Methode, alle Anwendungen zu identifizieren, die so rege mit dem Web in Verbindung stehen?**

Um alle Daten austauschenden Applikationen zu identifizieren, öffnen Sie zunächst eine neue Befehlszeile und geben Sie in der Eingabeaufforderung den Befehl *netstat -o* ein. Wollen Sie die Ausgabe in eine Textdatei umleiten, nutzen Sie den Befehl *netstat -o >C:\netstat.txt*. Anschließend können Sie die Datei bearbeiten. Nun zeigt die Eingabeaufforderung alle laufenden Programme und deren aktuellen Verbindungszustand an. Im Feld "Remoteadresse" sehen Sie, zu welchem Server oder zu welcher Adresse im Internet das Tool eine Verbindung aufbaut. Möchten Sie eine bestimmte Verbindung nun genauer untersuchen, merken Sie sich deren Process-ID (PID) in der letzten Zeile. Rufen Sie anschließend den Taskmanager auf, etwa über den Befehl *taskmgr*. Wechseln Sie hier auf die Registerkarte "Prozesse". Wird die Spalte mit der PID nicht angezeigt, klicken Sie im Taskmanager auf den Menüpunkt "Ansicht / Spalten auswählen" und aktivieren Sie den Haken bei "PID". Anschließend zeigt Ihnen der Taskmanager für alle laufenden Prozesse deren PID an und Sie können den gewünschten Prozess genauer unter die Lupe nehmen. *(Thomas Joos/ln)*

Auf manchen Client-Systemen **dauert das Starten oder Beenden von Windows ungewöhnlich lange**, obwohl wir die entsprechenden Rechner erst vor kurzem unter Windows 7 neu installiert haben. Wir vermuten, dass die Verzögerung irgendwie mit Fehlern in Programmen oder **defekten Treibern** zusammenhängt, konnten die genauen Probleme aber noch nicht ausfindig machen. **Gibt es Windows-Bordmittel, mit denen sich der Fehler eingrenzen lässt?**

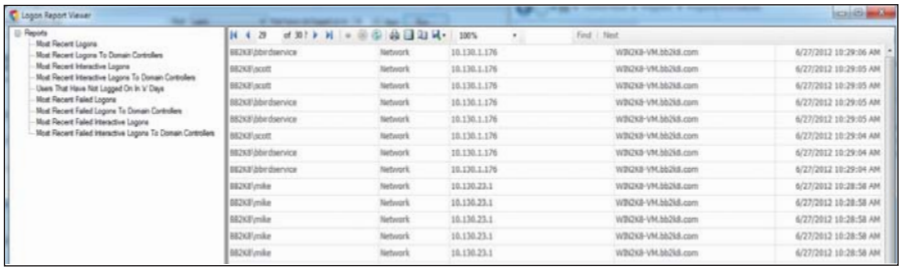
Sie können den Problemen mit Bordmitteln auf die Spur gehen – allerdings nur, wenn Windows diese erkennt. Gehen Sie dazu folgendermaßen vor: Öffnen Sie zunächst das Wartungscenter von Windows 7. Am schnellsten geht das, wenn Sie den Begriff "Wartungscenter" im Suchfeld des Startmenüs eingeben. Klicken Sie links im Fenster auf den Link "Leistungsinformationen anzeigen" und dann im neuen Fenster auf den Link "Weitere Tools". Im Bereich "Leistungsprobleme" ganz oben im Fenster stellt Windows Informationen darüber bereit, welche Programme den Computer bremsen oder wie Sie dessen Leistung verbessern können. *(Thomas Joos/ln)*

Damit 32 Bit-Clients auf Drucker zugreifen können, die wir in unserem Netzwerk unter Windows Server 2008 R2 oder Windows 7 freigegeben haben, muss ja **auf dem Server ein 32 Bit-Treiber zur Verfügung stehen**. Alternativ ließe sich auf den Clients natürlich **manuell ein Treiber für den Drucker installieren, dies würden wir aber gerne vermeiden**. Können Sie kurz schildern, was dabei zu beachten ist?

Zur Installation des Treibers muss dieser in ausgepackter Form vorliegen. Dazu müssen Sie den Treiber über die INF-Datei installieren lassen. Sie können das Druckermodell auch im Windows Update Katalog [Link-Code: C0PE4] suchen. Sie erhalten eine Liste aller Treiber, die zu dem gesuchten Modell passen und in der Datenbank vorhanden sind: Rufen Sie über "Geräte und Drucker" zunächst die Eigenschaftenseite des installierten Druckers auf und wählen Sie die "Druckereigenschaften" aus. Klicken Sie dann bei der Registerkarte "Freigabe" rechts unten auf "Zusätzliche Treiber". Hier besteht nun die Möglichkeit, Treiber für unterstützte Plattformen hinzuzufügen, indem Sie den Haken bei "x86" setzen. Anschließend erfolgt die Auswahl des Zielordners mit der INF-Datei des Treibers. Jetzt navigieren Sie in den X86-Ordner und wählen die dortige INF-Datei aus. Anschließend wird der Treiber installiert und steht zur Verfügung. Nun können Sie den Drucker über das Active Directory oder durch direkte Eingabe des Freigabenamens einrichten, ohne auf dem Client manuell Treiber installieren zu müssen. *(Thomas Joos/ln)*

Unlängst mussten wir schmerzhaft feststellen, dass **Windows 7 den Zugriff auf die versteckten System$-Freigaben wie C$ nicht mehr so einfach ermöglicht**, wie dies noch unter Windows XP der Fall war. Das liegt wohl vor allem daran, dass Windows 7 den **Zugriff auf administrative Freigaben über die Authentifizierung von lokalen Benutzerkonten blockiert**. Gibt es irgendeine Möglichkeit, um dieses Problem möglichst einfach zu umgehen?

Ein Workaround für das besagte Problem besteht darin, dass Sie Freigaben manuell erstellen. Das Gleiche gilt auch für ganze Festplatten. Wichtig an dieser Stelle ist, dass Sie der Gruppe "Jeder" entsprechenden Zugriff gewähren oder ein Benutzerkonto auf dem Computer anlegen, mit dem sich Benutzer bei der Netzwerkanmeldung authentifizieren können. Alternativ können Sie das Sperren der lokalen Anmeldung für administrative Freigaben in der Registry deaktivieren. Gehen Sie dazu folgendermaßen vor: Geben Sie *regedit* im Suchfeld des Startmenüs ein. Öffnen Sie den Schlüssel "HKEY_LOCAL_ MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ System". Erstellen Sie hier einen neuen DWORD-Wert mit der Bezeichnung "LocalAccountTokenFilterPolicy". Geben Sie den Wert "1" ein und starten Sie den Computer neu. Danach sollte die lokale Freigabe kein Problem darstellen. *(Thomas Joos/ln)*



Mit einer Reihe vordefinierter Berichte im Identity Auditor, die zentral alle Anmeldevorgänge im Unternehmen listen, erkennt der IT-Verantwortliche schnell Zugriffe eines bestimmten Anwenders

Der Desktop Viewer ist offiziell ein Teil von XenDesktop-Umgebungen und wird bei der initialen Installation des Webinterfaces auf einem XenDesktop Controller (DDC) automatisch konfiguriert. Mit ihm lassen sich Bildschirmeinstellungen bequem aufrufen oder schnell zwischen verschiedenen virtuellen Desktops wechseln. Sollte dies nicht der Fall sein, weil eine bereits vorhandene Webinterfacesite genutzt wird, können Sie dies aber mit einer kleinen Anpassung der Konfigurationsdatei *WebInterface.conf* auf dem Web Interface Server für XenApp und XenDesktop ICA-Sessions freischalten. Hierzu müssen Sie lediglich den Parameter "ShowDesktopViewer" der Datei auf den Wert "on" setzen. Dazu gehen Sie einfach wie folgt vor: Melden Sie sich am Server, der das Web Interface hostet, mit Administrator-Rechten an. Öffnen Sie dort das Verzeichnis "C:\ Inetpub \ wwwroot \ Citrix \ *Name der Webinterfacesite* \ conf" für die Web Interface-Verbindungen beziehungsweise "C:\ Inetpub \ wwwroot \ Citrix \ *Name der PNAgent-Site* \ conf" für die PNAgent-Verbindungen. Bearbeiten Sie in beiden Verzeichnissen jeweils die Datei *WebInterface.conf*. Dazu entfernen Sie das Zeichen "#" am Anfang der Zeile mit dem Parameter "ShowDesktopViewer", falls dieses gesetzt war, und setzen den Wert auf "On". Speichern Sie die Datei und rufen das Webinterface erneut auf. Beim nächsten Start Ihres virtuellen Desktops wird die Desktop Viewer Bar am oberen Rand der Session angezeigt. *(Citrix/ln)*

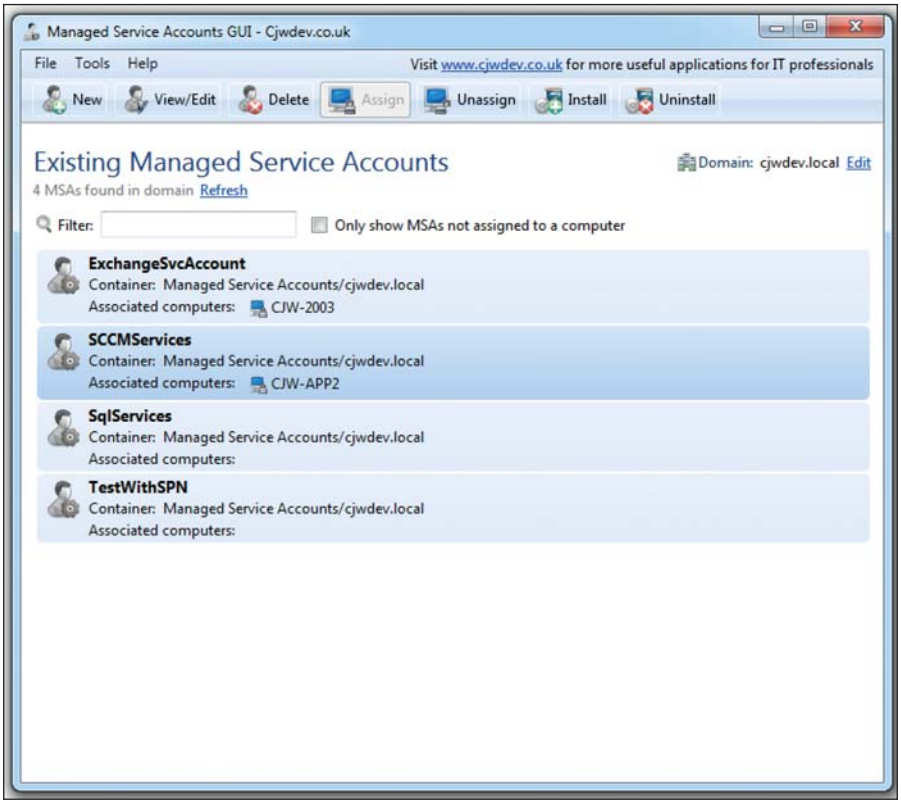
Tools

Wenn der Chef mal wieder hinter dem Administrator steht und unbedingt sofort Informationen zu den **letzten Log-ons eines Anwenders** benötigt, kann dieser leicht ins Schwitzen geraten. Als Windows-Admin öffnet er den **Event Viewer**, verbindet sich auf einen Domänencontroller und filtert nach dem gesuchten User. Dort lassen sich einige Einträge finden, aber vielleicht gibt es auf dem anderen DC noch mehr? Währenddessen dürfte sich der Chef so langsam fragen, warum so viel Zeit verstreicht, bis diese triviale Information vorliegt.

Damit der Chef nicht ewig warten muss, bietet sich der Einsatz des kostenlosen **Blackbird Privilege Identity Auditor** an, der dem Administrator das Leben auch vereinfacht, wenn der Vorgesetzte gerade kein dringendes Anliegen hat. Das kleine Tool **sammelt zentral alle Anmeldeinformationen von Domänencontrollern** und anderen sensitiven Rechnern. Diese Daten bereitet die Software für den Administrator in Berichten auf, die zu den Bereichen

- letzte Log-ons (für Domänencontroller, Mitgliedsserver oder Desktops)
- interaktive Log-ons
- inaktive User
- gescheiterte Log-ons
- gescheiterte interaktive Log-ons

zur Verfügung stehen. Jeder dieser Berichte **listet den fraglichen Account, die Art des Log-ons, den PC, von dem das Log-on versucht wurde, sowie den authentifizierenden Server auf**. Die Installation der Software sollte dabei keinen Administrator vor unüberwindliche Hindernisse stellen, die meiste Zeit dürfte der Download in Anspruch nehmen. Dieser ist allerdings erst nach einer kurzen Registrierung beim Hersteller möglich, der daraufhin per E-Mail einen Link zur Installationsdatei versendet. Voraussetzungen für eine erfolgreiche Installation sind das NET-Framework 3.5, der Microsoft Report Viewer und SQL Server 2008 Express oder höher. Die letzteren beiden Produkte stellt der Identity Auditor aber auch im Rahmen der Installation zur Verfügung. Nach der Installation benötigt die Software noch einen Service Account und der Anwen-



Das Tool "Managed Service Accounts GUI" listet alle im Netz vorhandenen Managed Service Accounts

Das Dashboard des Projektmanagement-Tools Rike zeigt den aktuellen Projekt-Status auf einen Blick

der muss festlegen, welche Maschinen überwacht werden sollen. Schon hat der IT-Verantwortliche die Gewissheit, auch in hektischen Situationen **schnell Audit-Infos zur Hand zu haben**. Zudem erlaubt das Tool auch weit komplexere Abfragen und Analysen, die die IT langfristig unterstützen. *(jp)*

Link-Code: C0PE1

Mit Windows Server 2008 R2 führte Microsoft die äußerst nützlichen **Managed Service Accounts** (MSA) ein. Zwar sind diese erst einsatzbereit, wenn das Forest- und Domänen-Schema auf den Stand 2008 R2 gehoben wurde, bieten jedoch mit ihrem automatischen Passwortwechseln durch das Active Directory viele Vorteile für die Sicherheit der IT. Allerdings hat Microsoft vor den Einsatz der Managed Service Accounts die Hürde PowerShell gesetzt: Nur durch die Verwendung von drei unterschiedlichen Cmdlets lassen sich Managed Service Accounts erzeugen, konfigurieren, zuweisen und installieren.

Damit war Chris Wright, dessen Tool für Domänen-Passwörter wir schon in der September-Ausgabe vorstellten, nicht zufrieden und erstellte das kostenlose **Managed Service Account GUI**. Damit ist der Administrator für die Verwaltung der Managed Service Accounts nicht mehr auf die PowerShell angewiesen, sondern erledigt dies in einer **intuitiven grafischen Oberfläche**. Dahinter erledigt das Tool alles, wofür der IT-Verantwortliche sonst auf die PowerShell zurückgreifen müsste, und fügt sogar noch Features wie die **Verwaltung der MSA-Gruppenmitgliedschaften** hinzu. Außerdem erlaubt es die Software, MSAs auf entfernten Rechnern zu installieren oder zu entfernen. Voraussetzung für den Einsatz ist allerdings ein installiertes Active Directory-PowerShell-Modul. *(jp)*

Link-Code: C0PE2

Öfter als ihm vielleicht lieb ist, findet sich der Administrator verantwortlich im **Projektmanagement** wieder. Wiederum ist dieser Zustand in vielen IT-Abteilungen nicht so regelmäßig, dass es sich lohnen würde, eine Projektmanagement-Software zur Unterstützung zu erwerben. Zwar wird der aufmerksame Leser des IT-Administrator aus unseren beiden großen Serien zum Projektmanagement wissen, dass die entscheidenden Faktoren für den Projekterfolg eher die zwischenmenschlichen sind, aber schaden kann ein Projektmangement-Tool auch wieder nicht.

Vor allem dann nicht, wenn es als Open Source-Software kostenlos zur Verfügung steht – in diesem Fall **Rike** aus dem Hause arago. Dieses IT-Systemhaus entwickelte das Projekt-Werkzeug für den internen Einsatz und stellt es nach zwei Jahren Programmierung als freie Software allen Interessierten zur Verfügung. Die Besonderheit an Rike: Das Projektmanagement-Tool baut auf dem **Kanban-Prinzip** auf und berücksichtigt gleichzeitig Elemente anderer agiler Methoden. Die Kanban-Methode setzt ein aktives Engagement der Mitarbeiter voraus: Statt des klassischen Push-Prinzips, bei dem abgeschlossene To-Dos automatisch an den nächsten Mitarbeiter weitergegeben werden, baut Kanban auf ein Pull-Prinzip. **Die Projektbeteiligten holen sich ihre Aufgaben selbst ab**, sobald sie die entsprechenden Kapazitäten dazu haben. Zuvor können alle Team-Mitglieder einzelne Tätigkeiten in Rike einstellen und mit verschiedenen Merkmalen wie Priorität, geschätzter Dauer, prognostizierter Größe, Schwierigkeitsgrad et cetera kategorisieren. Auf Basis der im System eingestellten Aufgaben wählen die Mitarbeiter dann die Jobs aus, die sie erledigen möchten und können. Das führt zu einer Steigerung der Motivation und Zufriedenheit im Team, da nichts delegiert wird. Rike sieht vor, dass jeder Mitarbeiter maximal drei Tätigkeiten gleichzeitig bearbeitet, um so die Produktivität zu steigern und auch beispielsweise im Krankheitsfall keine große Projektverzögerung zu verursachen. Um das Projektmanagement möglichst schlank und übersichtlich zu halten, werden einzelne To-Dos in Rike mittels URLs eingetragen, hinter denen sich die eigentlichen Informationen über die Aufgaben verbergen. Anhand der Historie zu den Projekten lassen sich außerdem Performance-Daten errechnen, die ein Optimierungspotenzial für zukünftige Arbeitsabläufe liefern. Rike wurde mit der Open Source-Portal-Software Liferay 6, Java 1.6 sowie Portlets entwickelt. *(jp)*

Link-Code: C0PE3

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

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

Aufbau eines hochverfügbaren Datennetzwerks beim Hessischen Rundfunk

Auf Sendung!

von Dr.-Ing. Tarik Erdemir

Beim Hessischen Rundfunk fungiert ein hochverfügbares Datennetzwerk als zentrale Infrastruktur und unterstützt die Rundfunkanstalt beim reibungslosen Betrieb aller IT- und Sendesysteme. Für höchste Performance und Sicherheit im neuen Netzwerk sorgen MPLS-Technologie sowie ein intelligentes Zonenkonzept. Lesen Sie in unserer Reportage, wie sich diese Umgebung realisieren ließ.

Als landesweiter Rundfunksender ist der Hessische Rundfunk (hr) in allen Geschäftsbereichen auf eine hochverfügbare und leistungsfähige IT-Infrastruktur angewiesen: Der hr produziert mehr und mehr Inhalte für Hörfunk und Fernsehen bandlos und überträgt immer häufiger Audio- und Videomaterial filebasiert via IP. Auch die komplexe Studio-, Produktions- und Gebäudeleittechnik benötigt ein hochperformantes Netzwerk für Kommunikation und Datenübertragung.

Im Netzwerk des hr stand 2009 der End-of-Live-Austausch einer Reihe Ethernet Switches bevor. Im Zuge dessen entschloss sich der Sender, seine bestehende IT-Infrastruktur zu erneuern, um den Anforderungen nach höheren Übertragungskapazitäten zur Produktion medialer Inhalte in Verbindung mit HD Rechnung zu tragen und rund um die Uhr einen reibungslosen Sendebetrieb zu gewährleisten.

Interdisziplinäres Projektteam

In der IT-Infrastruktur des Hessischen Rundfunks greifen herkömmliche Netzwerktechnik sowie Fernseh- und Rundfunktechnik des Senders eng ineinander. Deshalb stellte der hr ein interdisziplinäres Projektteam für Netzwerkaufbau und -migration zusammen. Darin arbeiteten Spezialisten aus den Bereichen Hörfunk, Fernsehen und Betriebstechnik mit der IT zusammen. Die Leitung und Projektverantwortung übernahm Jürgen Senft, Leitung IT-Infrastruktur beim hr.

Die neue Infrastruktur vereint Kommunikations- und Produktionsnetz in einer physikalischen Plattform und ermöglicht es, den Datenverkehr logisch voneinander zu separieren. Um alle Systeme und Außenstellen mit höchster Datenrate an die IT-Infrastruktur anzubinden und so höchste Übertragungsqualität zu erreichen, entschieden sich der hr und der Dienstleister Controlware, das neue Hochleistungsnetzwerk MPLS-basiert (Multi Protocol Label Switching) aufzusetzen.

Mit MPLS lassen sich selbst hochsensible Fernseh- und Produktionssysteme, beispielsweise Schnittplätze, unabhängig von ihrer Lokation in das Netzwerk einbinden. "Mithilfe der MPLS-Technologie können wir alle Daten für Hörfunk, Fernsehen und die Verwaltung über ein einziges Netzwerk bereitstellen", erläutert Senft. "Über die QoS-Klassen stellen wir sicher, dass echtzeitkritische Hörfunk- und Fernsehdaten vorrangig behandelt werden."

Fit für neue Technologien

Mit der Erneuerung des IT-Netzwerkes setzte das Projektteam folgende Ziele um:

- Aufbau einer effizienten und zukunftssicheren MPLS-Umgebung mit Bandbreiten von 10 GBit/s im Backbone und zur Server-Anbindung sowie GBit-Ethernet an den Arbeitsplätzen.
- Implementierung einer hochverfügbaren und fehlertoleranten Netzwerkstruktur, die sich zentral managen lässt.
- Erhöhte Sicherheit durch logische Segmentierung des Netzwerkes.
- Flächendeckende Bereitstellung von Power-over-Ethernet in den Büros.
- Optimale Unterstützung von Technologien wie Voice-over-IP, Audio-over-IP und zukünftig IP-TV.
- Hochperformante Übertragung hochauflösender Videodaten sowie Video Streaming in Echtzeit.

Auf Grundlage dieser Ziele erarbeitete Controlware ein technisches Konzept für die neue IT-Infrastruktur. Zur Vorbereitung der Migration und Inbetriebnahme wurden die Mitglieder der Projektgruppe und die

Systemadministratoren von Trainern eines Controlware-Tochterunternehmens geschult. Die Trainer vermittelten die nötigen netzwerktechnischen Grundlagen für eine erfolgreiche Umsetzung des Projektes.

MPLS-fähige Hardware als Basis

Um das hr Netzwerk MPLS-fähig und hochsicher zu konzipieren, fiel die Wahl auf folgende Produkte:

- Die modularen Cisco Catalyst 6509-Switches sorgen für höchste Ausfallsicherheit und Flexibilität im Backbone.
- Die Data Center-Switches Cisco Nexus 7000 bieten eine hochskalierbare und ausfallsichere Plattform für 10 GBit-Ethernet-Netzwerke.
- Die Access Switches (überwiegend Cisco Catalyst 3750) integrieren Büroetagen und Einzelnetze zuverlässig und hochsicher in die IT-Infrastruktur.
- Die Check Point Power-1 Appliance 11085 verbindet die verschiedenen Netzwerkzonen (MPLS-VPNs).
- Die Infoblox IPAM-Appliances stellen Netzwerkdienste wie DNS, DHCP und NTP bereit.
- Zur Inventarisierung der Netzwerkkomponenten wird der REALTECH NetworkManager eingesetzt.
- Die Software FNT Command findet Verwendung zur Dokumentation der LWL-Infrastruktur und der dort angeschlossenen Systeme.
- Für Netzwerkzugangskontrollen kommt der Cisco ACS 5.1 Server zum Einsatz.

Ausgehend von den Projektzielen erarbeiteten die Spezialisten die finale Konfiguration für alle Switches, Appliances und das Firewall-System.

Zonenkonzept schafft Sicherheit

Das neue Firewall-Cluster gliedert das Netzwerk in verschiedene Zonen und steuert den Datenverkehr zwischen den einzelnen Segmenten mit einem granularen Regelwerk. "Das Regelwerk legt fest, welche Datenquellen mit welchen Datensenken kommunizieren dürfen und über welche Ports und Protokolle der Austausch stattfindet", erläutert Jens Caspary, Verkaufsleiter der Geschäftsstelle Mitte bei Controlware. "Die 802.1x Port- und MAC-basierte Zugangskontrolle schafft zusätzliche Sicherheit", so Caspary, "und genügt selbst den höchsten Sicherheitsanforderungen."

Die räumliche und funktionelle Segmentierung des Netzwerkes – zum Beispiel in Büro-, Gast- und Produktionsnetze – ließ sich mithilfe der MPLS-Technologie mit höchsten Sicherheitsstandards und minimalen Latenzzeiten realisieren. Zusätzlich können mit den Netzwerkzonen eventuell auftretende Störungen räumlich eingeordnet und die Ausbreitung in andere Zonen verhindert werden.

Migration bei laufendem Sendebetrieb

Nachdem die neue IT-Landschaft implementiert und parallel zum bestehenden Netzwerk in Betrieb genommen wurde, folgte im April und Mai 2011 die nächste Herausforderung: Alle zentralen und dezentralen Systeme des Hessischen Rundfunks mussten bei laufendem Betrieb und ohne Sendeausfall in die neue Netzwerkstruktur überführt werden. Die Migration betraf neben den produktionsrelevanten und sendekritischen Systemen auch die Gebäudeleittechnik. Deshalb fanden die Migrationsarbeiten überwiegend nachts zwischen 20 Uhr und 6 Uhr und an Wochenenden statt. Insgesamt migrierte der Dienstleister gemeinsam mit 130 Spezialisten vom hr rund 5.500 dezentrale Systeme, überwiegend PCs, Notebooks, Netzwerkdrucker, sowie circa 1.400 Server und weitere zentrale Systeme.

Um den reibungslosen Ablauf der Umstellung sicherzustellen, richtete der hr eine zentrale Anlaufstelle ein. Von dort aus koordinierten die Verantwortlichen die Migration der Systeme in die neuen IP-Netze und bereiteten die notwendigen Firewall-Regeln vor. Dabei wurden die Abhängigkeiten der Systeme untereinander in sinnvollen Paketen zusammengefasst und ein Zeitplan für die Migration erstellt.

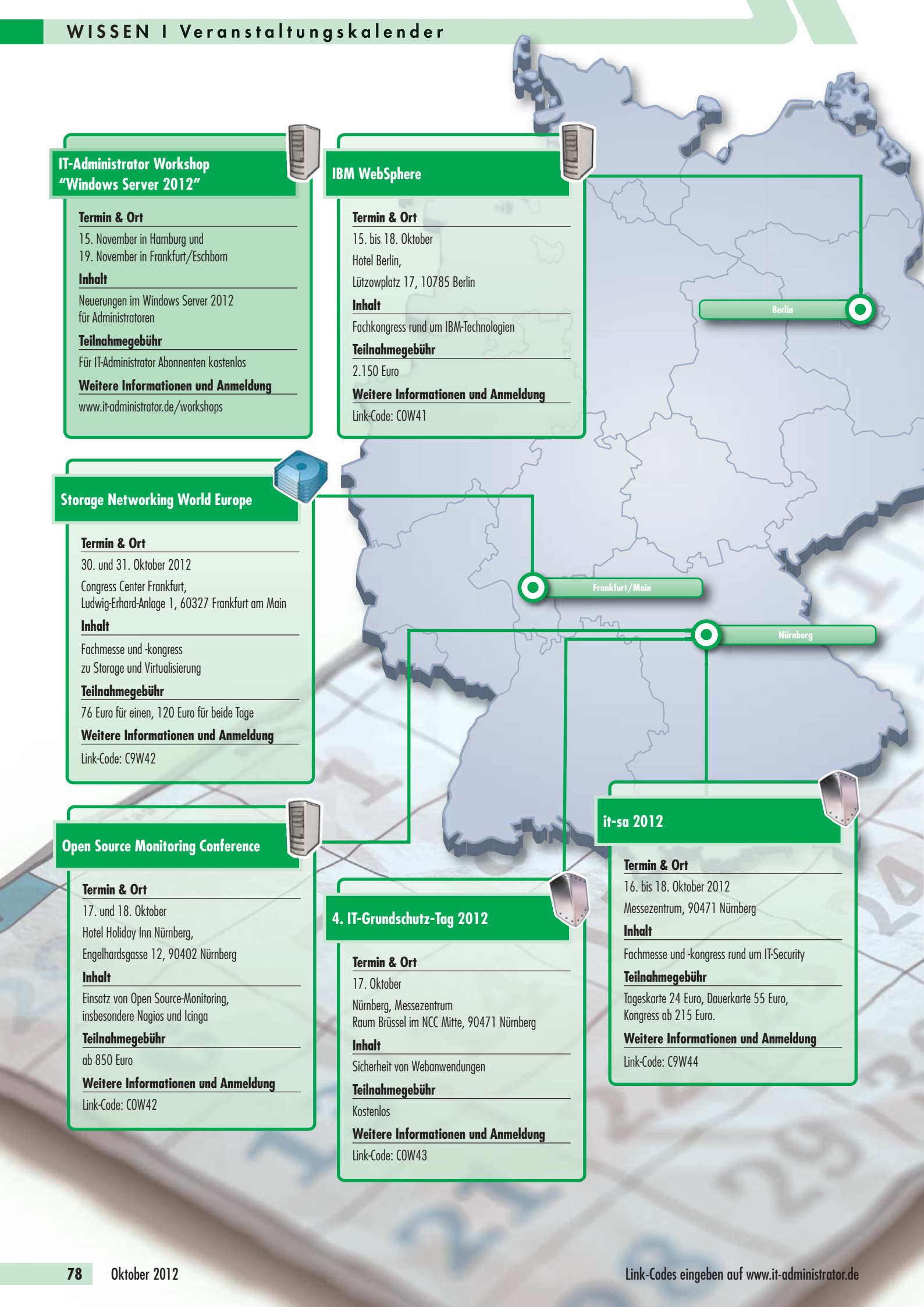
"Dank des ausgefeilten Migrationskonzeptes verlief der Austausch der Infrastruktur für alle Anwender störungs- und stressfrei", resümiert Reiner Othmer, Planungsingenieur und Projektverantwortlicher beim Hessischen Rundfunk. "Durch die exakte Abstimmung mit unserem Change Management-Team gab es keine Überschneidungen, etwa durch Wartungsarbeiten, im Regelbetrieb." Controlware Projektleiter Dirk Hamann zeigt sich mit dem reibungslosen Projektablauf hochzufrieden: "Die enge Verzahnung der IT mit der Hörfunk- und Fernsehtechnik war sowohl organisatorisch als auch technisch eine echte Herausforderung. Doch dank der exzellenten Zusammenarbeit und Kommunikation innerhalb des Projektteams und mit den Entscheidern und Führungskräften des hr konnten wir jede Hürde schnell und mühelos meistern."

Der Leiter IT-Infrastruktur des hr, Jürgen Senft, vor einer zentralen Komponente des neuen hochverfügbaren Netzwerks – dem Data Center-Switch Cisco Nexus 7000

Fazit

Die neue MPLS-Infrastruktur hat sich seit der Implementierung als tragfähiges Fundament für die vielfältigen Arbeitsprozesse des Hessischen Rundfunks bewährt. Die hochsichere IT-Umgebung läuft selbst in Stoßzeiten stabil und bietet Wachstumskapazitäten für die zunehmende Nutzung von Voice- und Audio-over-IP sowie für die filebasierte Produktion, etwa im Bereich HDTV. Auf Basis eines weiteren MPLS-VPNs soll eine stärkere Trennung von externen Nutzern und internen Mitarbeitern in Form eines Gastnetzes für die zusätzliche Erhöhung der Sicherheitsstandards sorgen. *(ln)*

Dr.-Ing. Tarik Erdemir ist Head of Network Solutions & UCC, Business Development bei Controlware.



IT-Administrator Workshop "Windows Server 2012"

Termin & Ort

15. November in Hamburg und
19. November in Frankfurt/Eschborn

Inhalt

Neuerungen im Windows Server 2012 für Administratoren

Teilnahmegebühr

Für IT-Administrator Abonnenten kostenlos

Weitere Informationen und Anmeldung

www.it-administrator.de/workshops

IBM WebSphere

Termin & Ort

15. bis 18. Oktober
Hotel Berlin,
Lützowplatz 17, 10785 Berlin

Inhalt

Fachkongress rund um IBM-Technologien

Teilnahmegebühr

2.150 Euro

Weitere Informationen und Anmeldung

Link-Code: C0W41

Storage Networking World Europe

Termin & Ort

30. und 31. Oktober 2012
Congress Center Frankfurt,
Ludwig-Erhard-Anlage 1, 60327 Frankfurt am Main

Inhalt

Fachmesse und -kongress zu Storage und Virtualisierung

Teilnahmegebühr

76 Euro für einen, 120 Euro für beide Tage

Weitere Informationen und Anmeldung

Link-Code: C9W42

Open Source Monitoring Conference

Termin & Ort

17. und 18. Oktober
Hotel Holiday Inn Nürnberg,
Engelhardsgasse 12, 90402 Nürnberg

Inhalt

Einsatz von Open Source-Monitoring, insbesondere Nagios und Icinga

Teilnahmegebühr

ab 850 Euro

Weitere Informationen und Anmeldung

Link-Code: C0W42

4. IT-Grundschutz-Tag 2012

Termin & Ort

17. Oktober
Nürnberg, Messezentrum
Raum Brüssel im NCC Mitte, 90471 Nürnberg

Inhalt

Sicherheit von Webanwendungen

Teilnahmegebühr

Kostenlos

Weitere Informationen und Anmeldung

Link-Code: C0W43

it-sa 2012

Termin & Ort

16. bis 18. Oktober 2012
Messezentrum, 90471 Nürnberg

Inhalt

Fachmesse und -kongress rund um IT-Security

Teilnahmegebühr

Tageskarte 24 Euro, Dauerkarte 55 Euro,
Kongress ab 215 Euro.

Weitere Informationen und Anmeldung

Link-Code: C9W44

Computernetzwerke, 4. Auflage

Die Welt der Netzwerke hat sich seit den ersten Tagen intensiv in verschiedene Richtungen weiterentwickelt. So beinhaltet "Computernetzwerke" in der 4. Auflage neben Überarbeitungen die thematischen Neuerungen seit der letzten Neuauflage vor drei Jahren. Den Einstieg bietet die Historie der Netzwerke mit einer Definition und der Übersicht über das OSI-Modell.

Hiernach werden die für Netzwerker interessanten Layer 1 bis 4 des OSI-Modells sehr ausführlich beschrieben: physikalische Schicht, Sicherungsschicht, Vermittlungsschicht und Transportschicht. Virtuelle Netze (VLANs) und virtuelle private Netzwerke (VPNs) sind die nächsten zwei Schwerpunktthemen des Buchs. Beide Abschnitte gehen jedoch nicht über Grundlagenwissen hinaus. Dennoch werden sowohl Trunks, Grenzen wie auch Erweiterungen von VLAN-Umgebungen aufgeführt. Die VPN-Tunnel betrachtet der Autor Rüdiger Schreiner von der theoretischen Seite – auch die Verschlüsselung reißt er nur kurz an. Die mobilen Netzwerke (WLAN, Funk und Voice) sind vom Autor in dieser Ausgabe komplett überarbeitet worden und befinden sich auf dem aktuellen Stand. Dies wird ergänzt durch die Szenarien von Netzzugängen, wie zum Beispiel WiMAX oder Gebäudeverbindungen via Richtfunk und Richtlaser. Die Inhalte hier verlieren sich nicht im Detail oder in Produktbeschreibungen.

IPv6 hat Schreiner neu aufgenommen und behandelt das Protokoll auf knapp zwanzig Seiten. Hardware-lastig und erfreulicherweise mit gut erkennbaren Fotos hinterlegt ist der Abschnitt der Steckertypen. Über das Buch sind vertiefende Beispielszenarien (auch Fehleranalysen) verstreut, die durch typische Netzwerkgrafiken unterstrichen werden. Additional gibt es ein Repetitorium, Verständnisfragen und Praxisübungen, die die Theorie des Gelesenen proben lassen.

Fazit

Was passiert zwischen den Kabeln der Netzwerke? Für einen Unbedarften sind die Vorgänge eine Black Box. Mit dem vorliegenden Grundlagenwerk kann zumindest Einsteigern Abhilfe geschaffen werden. Erfreulich, dass der Autor sich bei seinen Beschreibungen nicht im Detail verliert und somit eine übersichtliche Publikation erstellt hat. Die logische Struktur und der Aufbau erlauben es, das Buch auch als Nachschlagewerk zu verwenden.

Frank Große

Autor	Rüdiger Schreiner
Verlag	Hanser
Preis	24,90 Euro
ISBN	978-3446431171
Bewertung *(max. 10 Punkte)*	**9**

LPIC-1, 3. Auflage

Für viele große Hard- und Software-Lösungen gibt es Zertifizierungen jenseits beruflicher und akademischer Abschlüsse. So zertifiziert etwa das "Linux Professional Institute" (LPI) Linux-Experten. Das vorliegende Buch soll die Leser auf die Prüfungen 101 und 102 vorbereiten, was dem Niveau eines Junior Level Linux-Zertifikats (LPIC-1) entspricht. Die LPI-Prüfungsklassifikation dient als Vorlage für die Aufteilung im Buch. Zunächst vermittelt der Autor Harald Maaßen die Inhalte kompakt, aber mit der nötigen Detailtiefe. Für die Prüfung 101 findet sich der Leser im Prozess der Installation und Paketverwaltung wieder, nachdem die Systemarchitektur nahegelegt wurde. Kernbestandteile sind GNU/Unix-Kommandos, Geräte und Dateisysteme. Die Prüfung 102 soll Anwender dann dazu in die Lage versetzen, ihr Linux-System zu beherrschen. So finden sich Themen wie Shell, Datenverwaltung, Desktops und grundlegende Systemdienste wieder. Aber auch administrative Aufgaben, Netz-Grundlagen und Sicherheit haben ihren Platz gefunden.

Der Autor empfiehlt für das praktische Üben mindestens zwei verschiedene Distributionen in einer virtuellen Maschine zu erstellen – was bekräftigt werden kann, da sich die Inhalte auf die Vermittlung von Wissen konzentrieren und das Buch ohne Screenshots auskommt. Beide Teile enthalten Prüfungsfragen (120 für die Prüfung 101 und 112 für die Prüfung 102), die zumeist im Multiple Choice-Verfahren aufgebaut sind. Damit kann der Leser das erworbene Wissen überprüfen. Dabei hat das LPI die Gewichtung nicht außer Acht gelassen. Dieser Teil ist besonders gelungen, da die Antworten ausführlich begründet dargelegt werden und sich der Autor nicht nur mit der Nennung der richtigen Lösung begnügt. Der übersichtliche Index listet neben Schlagworten auch Befehle et cetera auf.

Fazit

Die Inhalte zu LPI 101 und 102 sind topaktuell und entsprechen dem LPI-Stand zum Sommer 2012. Unabhängig davon, ob der Leser das Zertifikat im Rahmen seiner Aus- oder Weiterbildung abschließen möchte, wird er mit den Inhalten bestens vorbereitet. Übungsfragen und der auf der DVD mitgelieferte Prüfungssimulator ergänzen den vermittelten Stoff prima. Der didaktisch ansprechende Aufbau eignet sich bestens zum Selbststudium. Mit entsprechendem Fleiß bei der Durcharbeitung der Inhalte des Buches sollten die Prüfungen kein Problem darstellen. Der ein oder andere Screenshot oder Schaubilder hätten dem Buch jedoch sicher nicht geschadet.

Frank Große

Autor	Harald Maaßen
Verlag	Galileo Computing
Preis	34,90 Euro
ISBN	978-3836217804
Bewertung *(max. 10 Punkte)*	**9**

https://openhpi.de/

Gratis, nicht umsonst

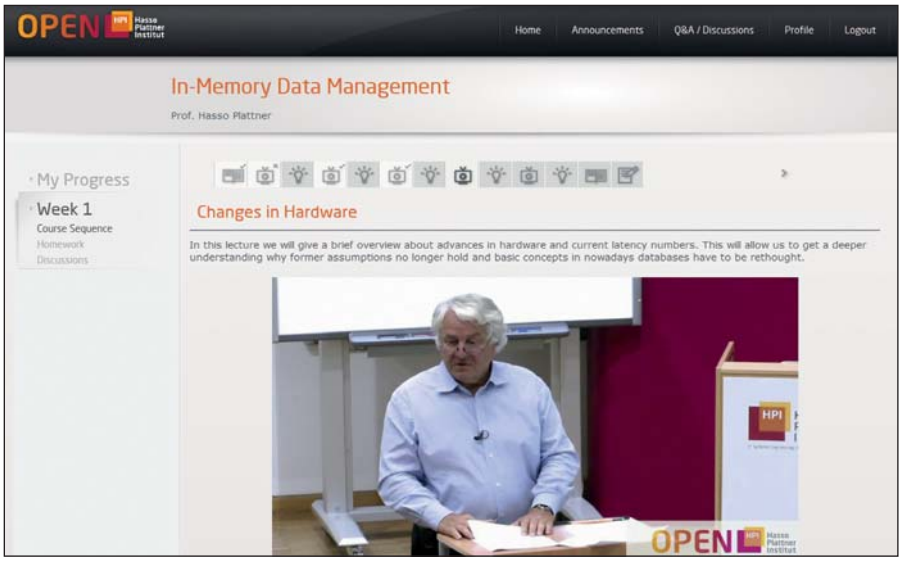
Fortbildung ist einer der Kompetenz-Eckpfeiler eines IT-Verantwortlichen. Denn gerade in der IT ist die ständige Weiterbildung im Angesicht rasant fortschreitender Technik Pflicht. Doch traditionelle Weiterbildung ist für den Administrator oft nicht optimal: Die Lektüre eines Buches nach Feierabend frisst nicht nur kostbare Freizeit, sie ist oft auch zu theoretisch und der Austausch mit gleichgesinnten Lernenden fehlt völlig. Hingegen kostet ein praxisnahes Seminar mit vielen Gelegenheiten zu Kollegengesprächen nicht nur eine oft happige Gebühr, sondern bedeutet auch, dass der Admin in diesem Zeitraum nicht im Unternehmen weilt. Für viele Firmen ist dies leider mittlerweile ein K.O.-Kriterium.

Sozusagen zwischen diesen beiden Fortbildungsformen positionieren sich die webbasierten Lernplattformen. Und diese werden von großen Unternehmen zunehmend auch kostenlos angeboten, wie etwa Microsofts "Virtual Academy", die wir Ihnen hier vor einigen Monaten vorstellten. In diese Reihe reiht sich nun auch unsere Website des Monats ein: Mit "openHPI" bietet das Hasso-Plattner-Institut kostenlose Fortbildung.

Zulassungsbeschränkungen für die in ein soziales Lernnetzwerk eingebetteten Online-Kurse gibt es bei openHPI nicht. Geleitet werden die Kurse von den Informatikprofessoren des HPI. Jeder der kostenlosen Kurse widmet sich einem spezifischen Thema und dauert rund zwei Monate. Die Kursmaterialien umfassen Lernvideos, Selbsttests, wöchentliche Hausarbeiten und eine abschließende Prüfung. Bei erfolgreicher Teilnahme an einem Kurs erhalten die Teilnehmer ein Zertifikat. Aktuell kann der Interessierte jedoch auf dem Portal nur einen Kurs absolvieren, ein zweiter ist angekündigt. Zudem hat openHPI sein Versprechen, auch Kurse in deutscher Sprache anzubieten, bisher nicht eingelöst.

Die Aufbereitung und der Ablauf der Kurse zeigen jedoch, dass es dem Anbieter um qualitativ hochwertige und nachhaltige Wissensvermittlung geht. Im Vergleich zu Microsofts Angebot zeigt sich openHPI frei von Schnickschnack aus dem Web 2.0-Umfeld. Und doch nutzt die Website Internettechnologie intelligent, etwa für wöchentliche Video-Antworten mit Vertiefungen zu den wichtigsten und spannendsten zwischen Studenten und den Kursbetreuern durchdiskutierten Fragen.

Aktuell ist openHPI ganz sicher einen ersten Blick wert, auch wenn das Kursangebot sehr überschaubar ist. Doch das Konzept wirkt durchdacht und das Know-how der hinter der Website stehenden Organisation lässt kaum Zweifel daran, dass dort eine beispielhafte kostenlose Lernplattform entstehen soll. *(jp)*



Hasso Plattner leitet persönlich durch den ersten verfügbaren Online-Kurs auf openHPI

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

WLAN-Virtualisierung als Alternative zur Mikrozellen-Struktur

Unternehmen binden immer mehr Geräte mittels Funk ins Netzwerk ein. Dabei kommt die WLAN-Virtualisierung ins Spiel, die von einer effektiveren Nutzung der Access Points (APs) geprägt ist. Die Technologie arbeitet mit virtuellen Zellen und Ports. Eine virtuelle Zelle umschließt dabei alle APs und macht ein Roaming unnötig. Unser Fachartikel im Web fokussiert die Vorteile der Technik und erklärt etwa, warum es anders als bei der Mikrozellen-Struktur keine sich überlappenden Kanäle gibt.
Link-Code: COW51

Die Private Cloud und das Unternehmensnetzwerk

Die Cloud ist in der Realität angekommen – IT-Profis müssen Konzepte für ihre Nutzung vorlegen. Das bevorzugte Modell ist dabei die Private Cloud, da hier die Hoheit über Anwendungen und Daten im Unternehmen verbleibt. Zentrale Ressource für die Cloud ist das Unternehmensnetzwerk. Der Online-Fachartikel umreißt die Anforderungen an das zugrundeliegende Netzwerk, beschreibt die Vorteile einer intelligenten Infrastruktur und wie sich diese – auch auf vorhandenen Umgebungen – effizient aufbauen lässt.
Link-Code: COW52

BYOD: Herausforderungen für die IT-Abteilung

"Verändere dich, verändere die Welt!" passt als Leitspruch zur aufkeimenden IT-Anarchie durch private Smartphones und Tablets im Unternehmen. Das Ziel für IT-Verantwortliche ist fest im Auge: Ungehinderter, aber zugleich sicherer Zugang zum Unternehmensnetzwerk von persönlichen Geräten aus. Unser Fachbeitrag im Web zeigt, wie Sie sich durch Device Fingerprinting, die automatische Erkennung von Geräte-Typen und Zuweisungen von Sicherheitsprofilen bis hin zu Mitarbeiter-Selbst-Registrierungsportalen dem BYOD-Trend stellen.
Link-Code: COW53

Sicherheitskonzepte für virtualisierte Server

Auf virtuellen Servern liegen unzählige vertrauliche Daten, die nicht in falsche Hände geraten sollten. In Zeiten von Cloud Computing und BYOD wird die Gewährleistung der Sicherheit jedoch immer komplizierter. Die Sicherung von virtuellen Servern stellt deshalb eine schwierige Aufgabe für die IT-Abteilung dar. Das Angebot an Sicherungs-Lösungen ist groß, aber unübersichtlich. Unser Online-Beitrag stellt verschiedene Sicherheitskonzepte vor und wägt Chancen und Risiken der einzelnen Angebote ab.
Link-Code: COW54

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

»Server ohne Firewall zu betreiben ist fahrlässig«

Die bremen online services GmbH & Co. KG (bos KG) ist im Technologiepark Bremen angesiedelt und hat rund 100 Mitarbeiter. Für deutsche und europäische Kunden aus den Bereichen E-Government, E-Justice und E-Business bietet das Unternehmen IT-Lösungen für die sichere und rechtsverbindliche Datenübermittlung, elektronische Signaturen und Kryptografie. Andreas Bücking (43) ist bei bos sowie der Konzerntochter Governikus verantwortlich für das System-Engineering und betreut mit einem Team von sechs Administratoren die gesamte IT-Infrastruktur.

Warum sind Sie IT-Administrator geworden?

Während meines Elektrotechnikstudiums hat mich die IT, speziell Rechnernetze, am meisten begeistert. 1996 steckte das Internet noch in den Kinderschuhen und Serveradministration war im Vergleich zu heute eine echte Herausforderung. Das Berufsbild traf meine Interessen und ich konnte mich hier am besten verwirklichen.

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

Spaß machen mir die täglich neuen Herausforderungen, neue Technologien sowie der Kontakt mit Kollegen und Kunden. Weniger spaßig sind Routinearbeiten, beispielsweise die Erstellung von Dokumentationen. Aber auch die gehören zum Handwerk und müssen erledigt werden.

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

Für technisch interessierte Menschen gibt es meiner Ansicht nach wenig Jobs, die eine größere Abwechslung bringen.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Auf Basis der in unserem Haus entwickelten Lösung zur Nutzung der eID-Funktion des neuen Personalausweises bieten wir unseren Kunden einen eID-Service an. Im Zuge stetiger Verbesserungen bauen wir derzeit eine georedundante HA Systemumgebung auf.

Welches IT-Problem oder Produkt ließ Sie in letzter Zeit verzweifeln und warum?

Der Aufbau eines Datenbankclusters in einer VMware Umgebung mit Zugriff auf ein gemeinsames RAW Device war eine echte Herausforderung.

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

Das wäre ein Tool, das sämtliche Einzel-Tools wie Überwachung, Patchmanagement, Deployment, Client- und Serveradministration betriebssystemübergreifend zur Verfügung stellt. Das würde manches erleichtern.

Worin sehen Sie die größte Gefahr für Ihre Server?

Ein Verlust wichtiger Daten ist, denke ich, die größte Gefahr für ein Unternehmen. Das kann sowohl durch Bedienfehler, aber auch durch einen Totalausfall des Systems hervorgerufen werden.

Welche Technologien nutzen Sie zur Server-Absicherung?

Server, die ohne Firewall im Netz stehen, sind schon sehr fahrlässig. Das Gleiche gilt für eine fehlende Backupstrategie. Für unser Firmennetz setzen wir eine Hardware-Firewall ein, die in Zukunft auch das IDS übernehmen wird. Als Antimalware setzen wir auf eine Mischung von MS Forefront Protection und aktuelle Virenscanner. MS SCCM nutzen wir für das Patchmanagement. Als Backupstrategie setzen wir auf eine Mischung aus Bandroboter und Backups sowie auf ein separates SAN. Kundendaten sind bei uns grundsätzlich verschlüsselt, das gilt natürlich auch für die Verbindungen zum Server.

Nutzen Sie Hochverfügbarkeit in Ihrer Umgebung?

Die meisten unserer Serversysteme, primär die virtualisierten, sind hochverfügbar installiert. Für einige kritische Systeme setzten wir auf Kundenwunsch auch eine georedundante Hochverfügbarkeit ein. Wir arbeiten dafür mit mehreren Rechenzentren zusammen.

Welche Rolle spielt Open Source bei der Sicherheit?

Open Source und Sicherheit ist ein schwieriges Thema. Fehler im Sourcecode können von der Community schneller gefunden werden. Dies kann sowohl eine große Gefahr als auch eine große Chance sein, beispielsweise um Bugs schnellstens zu lösen. Nüchtern betrachtet würde ich für kritische Systeme im Bereich Security wie Firewalls oder Virenscanner den Einsatz von Open Source nicht empfehlen.

Woraus leiten sich für Sie die Security-Anforderungen ab?

Unsere Software ist nach den Common Criteria Richtlinien vom BSI zertifiziert. Aufgrund dieser Richtlinien sind uns im Bereich der Security hohe Anforderungen gestellt. Hinzu kommen einige gesetzliche Anforderungen, speziell im Bereich des Datenschutzes. Grundsätzlich hängt im Mutterkonzern bos als auch bei Governikus die Latte für IT-Sicherheit sehr hoch.

Das Interview führte Petra Adamik.

Geburtstag:	13.06.1969
Admin seit:	14 Jahren
Hobbys:	Reisen, Sport

Andreas Bücking, IT-Administrator

Ausbildung und Tätigkeit

- Ausbildung zum Fernmeldehandwerker mit anschließendem Studium zum Diplom-Ingenieur (FH) Elektrotechnik/Informationstechnik.
- Heute Head of Systems Engineering mit einem Team von sechs Admins, das sowohl die interne Administration für zwei Unternehmen (bos und Governikus) als auch Unterstützungsleistungen bei Kunden erbringt.

Betreute Umgebung

- Heterogene Systemumgebung, bestehend aus Windows 7-Clients sowie Linux- und Windows 2003/2008-Servern. Rund 80 Prozent der Server sind mit VMware oder Hyper-V-Systemen virtualisiert.

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 11/12 erscheint am 29. Oktober 2012

Schwerpunktthema:

Storage & Cloud

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

Im **Dezember** befasst sich IT-Administrator mit dem Schwerpunkt **Server-based Computing**. In unseren Tests nehmen wir unter anderem H+H Netman 5 und 2X App-Server unter die Lupe. In der Praxisrubrik erfahren Sie außerdem, was die Remotedesktopdienste im Windows Server 2012 zu bieten haben und wie Sie App-V 5 optimal nutzen. Nicht zuletzt werfen wir einen Blick auf das Thema Application Performance Monitoring.

Als Schwerpunkt im **Januar** geht es dann um **Client-Sicherheit**.

***Im Test:* Netgear ReadyDATA 5200**

***Im Test:* Quantum vmPRO 3.0**

***Workshop:* Windows Server 2012 Online-Sicherung in der Cloud**

***Workshop:* Neuerungen in Samba 4**

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 und CvD*
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, Dr.-Ing. Tarik Erdemir, Thomas Gronenwald, Frank Große, Jürgen Heyer, Thomas Joos, Nils Kaczenski, Ulrich Lenz, Sandro Lucifora, Fabian Müller, Dr. Holger Reibold, Ulf B. Simon-Weidner

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

Es gilt die Anzeigenpreisliste Nr. 9 vom 01.01.2012

LAC/2011

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

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

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

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

Vertriebsbetreuung
SI special interest Pressevertrieb GmbH,
www.special-interest.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
(incl. E-Paper Monatsausgaben, 2 Sonderheften und 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: € 8,99
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
80802 München

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

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

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

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

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

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

INSERENTENVERZEICHNIS

Das IT-Administrator Komplettprogramm!!!

NEU! Jetzt auch inklusive E-Paper!

Sichern Sie sich jetzt das **IT-Administrator Jahresabo All-Inclusive** mit allen Monatsausgaben im Print- und E-Paper-Format, zwei Sonderheften pro Jahr und der Jahres-CD.

Automatisch bekommen Sie im März und Oktober jeweils das IT-Administrator Sonderheft und im Dezember die Jahres-CD mit allen Monatsausgaben im PDF-Format zugestellt. Ihre Abonummer wird zum Login für die E-Paper-Monatsausgabe – jetzt auch mit App fürs iPad!

Als bestehender Jahresabonnent können Sie hier upgraden:

www.it-administrator.de/abonnements/aboupgrade/

Oder Sie sind Neukunde? Hier können Sie bestellen:

www.it-administrator.de/abonnements/jahresabo/

www.it-administrator.de

Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

Tel: 0049-89-4445408-0
Fax: 0049-89-4445408-99
info@heinemann-verlag.de

Vertrieb, Abo- und Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

Tel: 06123/9238-251
Fax: 06123/9238-252
leserservice@it-administrator.de

LANCOM. Connecting your business.

LANCOM Systems

NEU **SMART. SCHNELL. INNOVATIV.**

Die neue LANCOM Smart Access Point Serie für High-Performance WLAN.

Noch mehr Speed für Ihr Enterprise WLAN!

- Bis zu 900 MBit/s brutto Datendurchsatz
- Mehr Leistung im WLAN – über 430 MBit/s netto Datendurchsatz (TCP)

- Höherer Datendurchsatz dank Band Steering (automatische Entlastung des 2,4 GHz Bandes – flexibel konfigurierbar)
- Paralleler Funkbetrieb in 2,4 und 5 GHz für heterogene Clientumgebungen

- STBC und beste Funkverbindung
- Verbesserte WLAN-Performance im Randbereich einer Funkzelle

- Spectral Scan für mehr Netzwerkübersicht
- Identifikation von WLAN-Störquellen (z. B. Bluetooth-Geräte) für ein effizientes Netzwerk-Troubleshooting

WLAN-Lösungen von LANCOM:

Kabellos glücklich.

Smart WLAN Technology

- **Sichere Integration** von Tablets, Smartphones und Notebooks in Unternehmensnetze
- **Optimaler Durchsatz** dank Smart WLAN Controlling
- **Perfekte Sicherheit** durch hohen Verschlüsselungsstandard und überwachte Sicherheitspolicies

Informieren Sie sich jetzt unter:
www.lancom.de/smartwlan