

Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Monitoring

Im Test

**ManageEngine
OpManager 9.0**

14

Im Test

WhatsUp Gold 15

18

Workshop

**Windows Server-Protokolle
erfassen und auswerten**

34

Systeme

Neuerungen in Windows Server 8

46

Know-how

**Zehn Tipps für
ein besseres Monitoring**

76

Vernetzen statt verzetteln.

Manche Systeme verlangen tatsächlich von Ihnen, dass Sie die Infrastruktur Ihres Netzwerks neu konfigurieren, damit sie den Anforderungen des Systems genügt. Das IBM BladeCenter® mit Intel® Xeon® Prozessoren ist anders: Es bietet ein breites Spektrum an Netzwerktechnologien und einige der modernsten Virtualisierungslösungen. So können Sie sich für die Lösung entscheiden, die am besten zu Ihrer Infrastruktur passt. Im Vergleich mit anderen Anbietern hilft IBM BladeCenter Ihnen außerdem, Ihre Netzwerkkosten um bis zu 40% zu senken¹.



Überzeugen Sie sich ... in nur 10 Minuten.

Unser Konsolidierungsrechner zeigt Ihnen, wie Sie Ihren ROI bereits drei Monate nach der Migration erzielen. Mehr erfahren unter **ibm.com/systems/de/blade**

¹Die Kostenersparnis von 40% basieren auf einem Vergleich der Anschaffungskosten für 10 für das HP-Rack der neuesten Generation optimierte Lösungen (d.h. DL380 G7 Proliant mit 10-Gigabit-Ethernet- und Fibre-Channel-Infrastruktur) mit 10 IBM BladeCenter- und HS22-Systemen der neuesten Generation mit Converged-Fabric-Lösungen von Brocade. Siehe www-03.ibm.com/systems/bladecenter/hardware/openfabric/coe.html. Die IBM Lösung umfasst eine Chassis-Infrastruktur. Die Preiskalkulation umfasst die öffentlich zugänglichen Anschaffungskosten pro Port für ToR-Ethernet- und FC-Switches mit Stand Januar 2011. Die Kostenersparnis für Netzwerk-Hardware von 40% ergeben sich aus dem Verzicht auf separate Ethernet- und Fibre-Channel-Karten und -Switches bei der Bereitstellung einer FCoE-Lösung von IBM BladeCenter für 10 Server und der damit verbundenen Hardware im Vergleich zur HP-Lösung. IBM, das IBM Logo, ibm.com und BladeCenter sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten und/oder anderen Ländern. Andere Namen von Firmen, Produkten und Dienstleistungen können Marken oder eingetragene Marken ihrer jeweiligen Inhaber sein. Eine aktuelle Liste der IBM Warenzeichen finden Sie im Internet unter www.ibm.com/legal/copytrade.shtml. Intel, das Intel Logo, Intel Inside, das Intel Inside Logo, Xeon und Xeon Inside sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den Vereinigten Staaten und/oder anderen Ländern. © 2011 IBM Corporation. Alle Rechte vorbehalten.



Auf die Plätze, Fertig, 8!

Liebe Leser,

es ist das Betriebssystem, das den Platzhirschen XP endlich in die Schranken weisen konnte: Windows 7. Was dem etwas zu üppig geratenen Windows Vista nicht gelang, scheint für den leicht verbesserten Nachfolger keine große Sache mehr zu sein. Immer mehr setzt sich das Gespann Windows 7 / Server 2008 R2 auch in Unternehmen durch. Für den Anbieter Microsoft, der Windows XP (und ältere Versionen) wohl lieber heute als morgen von der Bildfläche verschwinden sehen würde, keine schlechte Sache – nicht zuletzt aus Gründen der IT-Sicherheit. Doch droht die erfolgreiche 7 etwa zum nächsten Windows-Evergreen zu werden?



Im Moment scheint das durchaus möglich. Viele Firmen nutzen oder nutzten ihre regulären Hardware-Zyklen, um flächendeckend auf das neue Betriebssystem umzustellen. Windows 7 und Server 2008 R2 durchdringen so mehr und mehr Unternehmen. Da dürfte es für den Nachfolger erst einmal eng werden – auch wenn dieser bereits in den Startlöchern steht. Denn wer möchte schon kurz nach der Installation gleich wieder auf ein neues Betriebssystem umsatteln, besonders im professionellen Serverumfeld. Dabei hat Windows Server 8 durchaus Neuerungen zu bieten, die Admin-Herzen höher schlagen lassen. Auch das unseres Autors übrigens, der den neuen Server im Vorab-Release für Sie in Augenschein nahm.

Besonders unter der Haube hat Microsoft es denn auch richtig krachen lassen und viele Features verbessert oder eingeführt – so beispielsweise ein Active Directory, das sich nun problemlos klonen lässt. Mit Windows Server 2008 und Snapshots kein ganz ungefährliches Unterfangen. Auch zeigt sich das Betriebssystem nun deutlich flexibler, was die unterschiedlichen Betriebsmodi wie Server Core ohne und mit grafischer Oberfläche angeht. Gute Gründe also, über Windows Server 8 nachzudenken und einen Blick auf die Vorab-Versionen zu werfen. Ab Seite 46 lesen Sie, was der neue Server zu bieten hat.

Auch die Redaktion des IT-Administrators arbeitet laufend daran, das Heft für Sie zu optimieren. So haben wir nun eine kleine, aber nicht unbedeutende Änderung in den Workshop-Listings vorgenommen und setzen die Variablen künftig farbig ab. Bislang standen diese in geschweiften {Klammern}, was jedoch bei einigen Programmier- und Skriptsprachen für Verwirrung sorgen konnte. Jetzt sehen Sie noch besser auf einen Blick, welche Teile eines Befehls wortwörtlich einzugeben sind und welche Sie an Ihre individuelle Umgebung anpassen müssen.

Viel Spaß beim Lesen, Ihr

Daniel Richey
Stellv. Chefredakteur

Monitoring

Im Test: SSC-ServerInspector



Jeder Administrator hat diese Situation wohl schon einmal erlebt: Der Server läuft, er ist erreichbar, alle Dienste sind augenscheinlich in Betrieb und trotzdem arbeitet das System nicht korrekt. Schon geht die aufwändige Fehlersuche los. Der SSC-ServerInspector will hier einen Schritt weitergehen und überwacht sowohl Server als auch das Netzwerk auf funktionaler Ebene. IT-Administratoren wollten genauer wissen, wie gut und zuverlässig das Tool diese Aufgabe erfüllt.

Seite 22

Exchange Server-Logs verwalten



Es handelt sich um einen Klassiker im Support: Ein verzweifelter Mitarbeiter wendet sich an den IT-Service, weil er auf eine dringende, bereits an ihn versandte E-Mail wartet, er diese aber noch nicht erhalten hat. Nun obliegt es dem Exchange-Administrator, schnell Klarheit zu schaffen und festzustellen, was geschehen ist und ob überhaupt ein Problem vorliegt. Dieser Workshop stellt die wichtigsten Exchange-Logs vor, um Ihnen Ansatzpunkte für das schnelle Troubleshooting an die Hand zu geben.

Seite 40

AKTUELL

06 News

10 ITANet aktuell: IT-Administrator Workshop "Lotus Domino Deployment" am 22. März in Bielefeld

Mit Lotus Notes/Domino in Version 8.5.3 bescherte IBM den Anwendern eine ganze Palette neuer Features. Diese beleuchtet der IT-Administrator Workshop am 22. März ebenso wie die Wege zur Virtualisierung des Systems.

12 ITANet aktuell: IT-Administrator Training "Windows Server Best Practice" am 21. März/16. April in München und 15. Mai in Hamburg

Wie die Best Practices in Sachen Active Directory, Domänencontroller und Hyper-V aussehen, zeigt Windows-Experte Nils Kaczinski in unserem neuen Training.

PRODUKTE

14 Im Test: ManageEngine OpManager 9.0

Netzwerk-Monitoring-Produkte sind mittlerweile extrem leistungsfähig, da sie immer mehr Geräte und Prozesse detaillierter überwachen müssen. Ende 2011 hat ManageEngine eine rundumneuerte Version der Software OpManager veröffentlicht. Wir haben uns die neunte Generation genauer angesehen.

18 Im Test: Ipswitch WhatsUp Gold 15 Standard

Ipswitch ist mit seiner Software zur Netzwerküberwachung bereits mit Version 15 am Start. IT-Administratoren hat überprüft, ob, und wenn ja, welche neuen Funktionen einen Umstieg auf das neue Release rechtfertigen.

22 Im Test: SSC-ServerInspector

Der Server läuft, alle Dienste sind in Betrieb und trotzdem arbeitet das System nicht korrekt. Schon geht die aufwändige Fehlersuche los. SSC-ServerInspector will hier einen Schritt voraus sein und überwacht sowohl Server als auch das Netzwerk auf funktionaler Ebene.

28 Im Test: Blue Coat Web Security Cloud Service

Statt eigene Appliances für die Filterung der Webzugriffe einzusetzen, gibt es die Alternative, einen Online-Dienst wie den Blue Coat Cloud Service zu nutzen. IT-Administratoren hat untersucht, wie zuverlässig der Dienst funktioniert.

PRAXIS

34 Workshop: Ereignisprotokolle von Windows-Servern erfassen und auswerten

Es gibt zahlreiche kostenlose Möglichkeiten, die Ereignisanzeigen und Protokolle der Server an zentraler Stelle zu erfassen und zu analysieren. Wie Sie den Überblick über Ihre Logdateien behalten und welche Werkzeuge Ihnen weiterhelfen, erfahren Sie in diesem Workshop.

40 Workshop: Protokolle unter Exchange Server 2007 und 2010

Kommen E-Mails nicht an, obliegt es dem Exchange-Administrator, anhand der Log-Dateien schnell festzustellen, wo das Problem liegt. Unser Workshop stellt Ihnen die wichtigsten Exchange-Protokolle vor.

46 Systeme: Neuerungen in Windows Server 8

Unter der Haube des kommenden Windows Server 8 hat Microsoft ordentlich Funktionen optimiert und Technologie erneuert. IT-Administratoren hat einen ersten Blick auf die Developer-Preview geworfen.

52 Systeme: Microsoft System Center Configuration Manager 2012

Aktuell arbeitet Microsoft an der Version 2012 des System Center Configuration Manager. Wir stellen Ihnen auf Basis der Beta 2 vor, wie sich die Neuerungen in der Praxis auswirken.

56 Systeme: Security Information and Event Management

Nicht zuletzt wegen der stetig steigenden Compliance-Anforderungen wird "Security Information and Event Management" immer wichtiger. Unser Beitrag zeigt, was eigentlich hinter diesem Begriff steckt.

60 Systeme: Kostenlose Android-Apps für Administratoren

Für Administratoren stehen immer mehr Apps bereit, die ihm bei seiner Tätigkeit hilfreich sind. IT-Administrator stellt zehn nützliche und kostenlose Apps aus den Bereichen Monitoring und Fernwartung vor.

64 Workshop: Stresstest für Virens Scanner selbst gemacht

Virens Scanner gehören schon lange zur Grundausstattung im Bereich IT-Sicherheit. Dabei kann jedoch eine falsche Einstellung schnell eine Sicherheitslücke aufreißen. Wie Sie Ihre Antivirus-Software leicht selbst testen, zeigt unser Workshop.

68 Workshop: Exchange Server 2010

In der Regel prüfen Administratoren die diversen Einstellungen und Dienste eines Exchange Servers per Hand, wenn es Probleme gibt. Doch gibt es auch praktische Cmdlets, die mit einem Aufruf zahlreiche Mausklicks und Prüfungen abnehmen.

70 Tipps, Tricks & Tools

WISSEN

74 Recht: Datenschutzgerechte IT-Protokollierung

Neben zahlreichen technischen Anforderungen zur Protokollierung muss der Administrator auch rechtliche einhalten – ein nicht immer ganz leichter und vor allem riskanter Spagat.

76 Know-how: Zehn Tipps für ein besseres Monitoring

Der einzige Weg, um sich wirksam gegen Datendiebstahl und Malware-Angriffe abzusichern, ist es, alle Systeme, Komponenten und Daten rund um die Uhr im Auge zu behalten. Wir geben zehn Tipps, wie Sie dies am besten bewerkstelligen.

78 Know-how: Als Opa Admin war: GRiD Compass 1101

79 Buchbesprechung "BizTalk Server 2010" und "Java Security"

80 Website & Fachartikel online

RUBRIKEN

03 Editorial

04 Inhalt

81 Das letzte Wort

82 Vorschau, Impressum, Inserentenverzeichnis

iläNet

Workshop in Bielefeld

Lotus Domino Deployment
am 22. März 2012

Microsoft System Center Configuration Manager 2012



Aktuell arbeitet Microsoft an der Version 2012 des System Center Configuration Managers, die zahlreiche Neuheiten bietet, zum Beispiel bei der Smartphone-Verwaltung. Eine weitere Neuerung ist das ausgeklügelte Regelwerk, das auf Basis verschiedener Werte wie Arbeitszeit, Standort, Uhrzeit und Endgerät genau die Anwendungen auf den Clients zur Verfügung stellen kann, die der Situation am besten gerecht werden. Wir stellen Ihnen auf Basis der Beta 2 vor, wie sich die Neuerungen in der Praxis ausprägen.

Seite 52

Datenschutzgerechte IT-Protokollierung

Die Protokollierung aller Vorgänge im IT-Netz über ein zentralisiertes IT-Datenmanagement ist der ebenso pragmatische wie wirkungsvolle Weg gegen Datenmissbrauch und Angriffe von extern und intern. So lassen sich Angriffsversuche frühzeitig erkennen und abwehren. Auch ist der Datenmissbrauch mithilfe der Protokollinformationen in seinen Ausmaßen quantifizierbar. Neben technischen Anforderungen zur Protokollierung muss der Administrator allerdings auch rechtliche einhalten – ein nicht immer leichter Spagat.

Seite 74

Themenübersicht

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

Die Agenda:

13:00 Uhr: Begrüßung

13.15 Uhr: Lotus Domino und Lotus Notes 8.5.3

Ein Überblick über die Neuerungen und Verbesserungen in der aktuellen Version.

Lotus Domino und Lotus Notes virtualisieren

- Beleuchten der Möglichkeiten, sowohl Server als auch Client in virtuellen Umgebungen zu betreiben. Welche Optionen bestehen, welche Virtualisierer werden unterstützt?
- Praxisbeispiel, wie Sie einen aktuellen Notes Client auf XenApp 6 für User zur Verfügung stellen.

15:00 Uhr: Kaffeepause

Lotus Notes Verteilung und Aktualisierung

- Zentrale und einheitliche Installation von Clientgeräten mit Lotus Notes.
- Möglichkeiten, die Installation zu vereinfachen und die Notes-Infrastruktur zu aktualisieren.

17:30 Uhr: Ende der Veranstaltung

Dozenten: Roland Joeriskes und Torben Volkmann, acocon GmbH

Ort:

acocon GmbH,
August-Schroeder-Straße 4, 33602 Bielefeld

ITANet Workshop-Partner:



Uhrzeit: 13.00 bis 17.30 Uhr

Teilnahmegebühren:

Für IT-Administrator-Abonnenten kostenlos.

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

Anmeldeschluss:

12. März 2012

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

Das kleine Schwarze

Mit dem **StorCenter ix2** gibt **Iomega** den Startschuss für die nächste Generation seiner **Netzwerkspeicher für kleinere Unternehmen**. Das NAS verfügt über zwei Laufwerksschächte für 3,5-Zoll-Festplatten und ermöglicht somit einen maximalen Gesamtspeicher von 6 TByte. Die Verwendung von RAID 1 verringert diese Bruttokapazität zwar um die Hälfte, sorgt im Rahmen einer Platten-Spiegelung aber für die Redundanz der Daten. Der Einsatz als iSCSI-Target mit Block-Level-Zugriff soll eine effiziente Nutzung des freien Speicherplatzes gewährleisten. Außerdem ist der Storage-Würfel für VMware- sowie XenServer-Umgebungen zertifiziert und unterstützt die Einbindung in ein Active Directory. Als besonders geeignet sieht der Hersteller sein Produkt auch für die Videoüberwachung: StorCenter ix2 verfügt über eingebaute Unterstützung für den Betrieb von bis zu fünf UPnP-Netzwerkcameras von Axis, Bosch oder Panasonic. Die angeschlossenen IP-Kameras erfassen und speichern

als MPEG-4 kodierte Videos direkt auf dem NAS-System, ohne dass ein dedizierter PC benötigt wird. Nutzer können die gespeicherten Video-Dateien so einstellen, dass sie nach einer bestimmten Zeit oder bei einer bestimmten Dateigröße gelöscht werden. Der Preis für das StorCenter ix2 ohne Festplatten beträgt rund 150 Euro. (ln)

Iomega: www.iomega.com



Neben den üblichen NAS-Funktionen fungiert das StorCenter ix2 von Iomega auch als Speicherzentrale für bis zu fünf IP-Überwachungskameras

IP-Kameras mit Tag- und Nachtsicht

D-Link baut sein Portfolio im Bereich **IP-Überwachung** weiter aus. Die **Full HD-Kamera DCS-6112** sowie die **Tag-/Nacht Kamera DCS-6113** eignen sich für professionelle Live-Videoaufzeichnungen sowie die Fernüberwachung via Internet. Sie arbeiten sowohl bei starkem Gegenlicht als auch bei völliger Dunkelheit. Der Live-Stream lässt sich zudem in drei Formaten abrufen. Die Kamera DCS-6113 von D-Link arbeitet auch bei völliger Dunkelheit. Die DCS-6112- und die DCS-6113-Kameras sind mit einem progressiven CMOS-Sensor ausgestattet, der für sehr genaue Aufnahmen sorgen soll. Im Vergleich zu

herkömmlichen IP-Netzwerkcameras gleichen die Kameras mit Hilfe dieser Sensortechnologie laut Hersteller dabei auch hohe Helligkeitskontraste aus. So würde beispielsweise in Räumen mit großen Fens-

tern auch bei direkt einfallendem Sonnenlicht eine im Gegenlicht stehende Person oder ein Gegenstand erkannt und überwacht. Beide Kameras verfügen außerdem über Infrarot-LEDs, womit sie sich auch für den Indoor-Überwachungseinsatz rund um die Uhr eignen sollen. Als Tag-/Nacht Kamera liefere die DCS-6113 selbst bei Dunkelheit detaillierte Aufnahmen. Ein weiteres Merkmal der neuen Kameras ist die integrierte ePTZ Funktion: Damit seien scharfe Nahaufnahmen jederzeit möglich – ohne die Kamera bewegen zu müssen. Auch die komfortable Weiterverwendung der Aufzeichnungen will der Anbieter gewährleisten. So können die Daten mit einem kompatiblen Endgerät in drei unterschiedlichen Formaten (H.264, MPEG-4 und MJPEG) über das Internet live abgerufen werden. Mit der mitgelieferten Management Software D-ViewCam Professional-Version DCS-220 lassen sich zudem bis zu 32 Geräte gleichzeitig über einen einzigen Bildschirm verwalten. Verfügbar ist das Modell DCS-6112 für 436 Euro, die Variante DCS-6113 für 503 Euro. (dr)

D-Link: www.dlink.de



Die Kamera DCS-6113 von D-Link arbeitet auch bei völliger Dunkelheit

Verbesserte Datenhaltung

LaCie bringt **Version 2.2** seines **NAS-Betriebssystems NAS OS** heraus. Es soll verbesserte Backup-Optionen und einfache Fernzugriffsfunktionen für LaCie Network 2-Produkte bieten. Diese aktualisierten Funktionen ermöglichen laut Hersteller sichere Backups und Datenfreigabe, auch von unterwegs. Die Unterstützung von NAS-zu-NAS-Backup ermögliche die Sicherung eines anderen kompatiblen NAS-Systems mit dem LaCie-NAS. Auch die Sicherung des LaCie-NAS mit einem anderen NAS-System, entweder über das gleiche Netzwerk oder über das Internet, soll möglich sein. Diese Funktion sei besonders nützlich für die Erstellung eines Offsite-Backups zum Schutz von Daten gegen Diebstahl oder Feuer, Überschwemmungen und andere Naturkatastrophen. Erweiterte Optionen ermöglichen dem Nutzer das Verschlüsseln oder Komprimieren von Daten sowie die Ausführung Speicherplatz sparender inkrementeller Backups. Das NAS OS 2-Update wird von allen Network 2-Produkten unterstützt und soll zudem vollständig kompatibel zu Windows 7, Windows XP und Mac OS 10.5, 10.6 und 10.7 (Lion) sein. Bestandskunden können das Update kostenlos herunterladen. (dr)

LaCie: www.lacie.com

Leider hat in der Januar-Ausgabe der Fehlerteufel zugeschlagen. So bezieht sich der Preis der in den News vorgestellten Appliance SRA EX9000 von SonicWALL nicht auf Euro, sondern 37.800 US-Dollar.

Im Beitrag "Windows-Laufwerke mit BitLocker und TPM-Chip verschlüsseln" aus der Ausgabe 12/2011 des IT-Administrator findet sich zudem eine ungenaue Formulierung, die unter Umständen zu einer nicht optimalen Konfiguration der Sicherheitseinstellungen führen kann. In dem Workshop ab Seite 56 beschreiben wir das gemeinsame Auswahlfeld für die Einstellungen der BitLocker-Verschlüsselung. Dabei ist die Einstellung "mit Diffuser" zu bevorzugen. Im ursprünglichen Artikel kann der Eindruck entstehen, wir würden empfehlen, diese Option ausgeschaltet zu lassen.

So stimmt's

Kühle Brise im Rechenzentrum

Der IT-Hersteller **Eduard Lehmann** bringt das **RearCool-Rack** auf den Markt – einen Serverschrank, der sich durch eine besonders **hohe Kühleffizienz** auszeichnen soll. Hierfür kombiniert das System zwei Kühlmethoden: die direkte Rack-kühlung sowie die Raumkühlung. Das Kühlwasser des primären Wasserkreislaufs wird der CDU (Cabinet Distribution Unit) zugeführt. Von dort aus werden im sekundären Wasserkreislauf die RearCool-Racks mit Kühlwasser versorgt. Alle Bauteile der CDU sind dabei redundant ausgelegt. Die Server saugen im Betrieb frontseitig Luft an und blasen rückwärtig die auf 35 bis 50 Grad Celsius erwärmte Luft durch das in der Rücktür verbaute Microchannel-Kühlregister aus, das eine hohe Luftdurchlässigkeit bieten soll. Durch diesen Kühlprozess würde neutral kühle Luft mit rund 23 Grad Celsius Temperatur in den Rechenzentrumsraum ausgeblasen. Die RearCool-Racks arbeiten zudem kondensatfrei, weil hohe Wasservorlauftemperaturen von 18 Grad gefährlich werden könnten. Dadurch könne bereits ab 16 Grad Außentemperatur



Das RearCool-Rack von Lehmann soll sich durch besonders hohe Effizienz bei der Kühlung auszeichnen

die Kälteerzeugung auf freie Kühlung umgestellt werden. Die Wassermenge pro Rücktür im RearCool-Rack betrage zwei Liter, in der CDU 32 Liter. Das komplette System ist zudem mit einem Leckageband versehen, um Schutz vor auslaufendem Wasser zu bieten. Für rund 2.900 Euro ist das System zu haben. (dr)

Lehmann: www.rearcool-rack.de

Schlanker Begleiter

Dell stellt mit dem **XPS 13** sein erstes **Ultrabook** vor. Mit einer Höhe zwischen sechs und 18 Millimeter ist es deutlich schlanker als bisherige Notebook-Modelle von Dell. Durch ein rahmenloses 33,8-cm-Display (13,3 Zoll) ist es dabei so kompakt, dass es die gleichen Abmessungen wie ein gängiges 11-Zoll-Notebook besitzt. Das Ultrabook wiegt in seiner leichtesten Ausführung weniger als 1,4 Kilogramm und besteht aus Aluminium und Kohlefaser, was es besonders widerstandsfähig machen soll. Mit einer Akkuladung hält das Gerät laut Dell bis zu knapp neun Stunden durch. Im Inneren bietet das XPS 13 Intel-Technologien wie "Rapid Start" und "Smart Connect". Mit Rapid Start lässt sich das Notebook in wenigen Sekunden hochfahren. Als eines der ersten Ultrabooks hat das XPS 13 außerdem die Funktion Smart Connect integriert. Damit erwacht es automatisch regelmäßig aus dem Ruhemodus, um sich mit bekannten Netzwerken zu verbinden und Kalendereinträge sowie den E-Mailaccount zu synchronisieren. An Prozessoren greift Dell auf Intels Core-i-Chips zurück. Je nach

Modell stehen die Varianten i5 oder i7 zur Verfügung. Das WLED-Breitbild-Display mit gehärtetem Gorilla-Glas bietet eine Lichtausbeute von 300 cd/m². Als Datenspeicher steht ein Solid-State-Laufwerk mit wahlweise 128 oder 256 GByte Kapazität zur Verfügung. Ferner bietet der Rechner Sicherheits- und Service-Optionen wie die Standard-Trusted-Platform-Module für die BitLocker-Datenverschlüsselung, einen optionalen ProSupport sowie einen Konfigurationservice. Für 1.099 Euro ist die Flunder ab Mitte März verfügbar. (dr)

Dell: www.dell.de



Das XPS 13 ist das erste Ultrabook von Dell und bietet 256 GByte SSD-Speicherplatz

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

Doctor Web geht mit einer neuen **Scan-Engine** gegen Malware vor. Als wesentlichen Vorteil der neuen Software nennt der Hersteller die erhöhte Scan-Geschwindigkeit. Möglich wurde dies laut Doctor Web durch ein neues Virendatenbank-Format und einen verbesserten Scan-Algorithmus. Benchmarks unter Laborbedingungen sollen eine vierfache Erhöhung des Scan-Tempos gezeigt haben. Die Engine unterstützt nun dynamische Ressourcennutzung – je nach Systemzustand erhält die Antiviren-Software eine unterschiedliche Rechenleistung zugeteilt. Eine Erweiterung erfuhr auch die heuristische Analyse: Die ScriptHeuristic-Technologie soll Schadcode in HTML- und PDF-Dokumenten noch schneller aufspüren. Das Update ist für Nutzer der Schutz-Programme des Herstellers kostenlos und wird automatisch heruntergeladen und installiert. (In) www.drweb-online.com

O&O Software bietet ab sofort mit **O&O AutoBackup** ein Werkzeug an, das automatisch ausgewählte Dateien und Ordner mit einem externen Sicherungsmedium synchronisiert. So kann der Nutzer mit dem Programm beispielsweise eine Sicherheitskopie eines bestimmten Dokumenten-Ordners auf einem USB-Stick erstellen und konfigurieren, dass in Zukunft Änderungen an den Originaldaten automatisch für die Sicherheitskopie übernommen werden. Beim Sichern der Informationen sind drei Optionen möglich: Ein vollständiges Backup, ein Schreiben lediglich der Änderungen oder eine vollständige Synchronisation, bei der das Utility im Originalverzeichnis gelöschte Dateien auch auf dem externen Medium entfernt. (In) www.oo-software.com

Ab sofort unterstützen **Rangee Thin Clients** auf Basis von **Windows Embedded** den Multimedia-Beschleuniger **RemoteFX**. Auch Geräte mit Rangee Linux können die Grafikfunktionen von RemoteFX dank eines Software-Moduls von FreeRDP nutzen. FreeRDP ermöglicht zudem mit einem Rangee Linux-basierten Thin Client, einen zweiten Bildschirm als erweitertes Display in einer Windows-Session zu nutzen. Für die Nutzung von RemoteFX ist zum einen eine Virtualisierung mittels Hyper-V erforderlich. Zum anderen setzt die Technologie eine leistungsstarke Grafikkarte auf Server-Seite voraus. (dr) www.rangee.com

Red Hat hat **Red Hat Enterprise Virtualization 3.0 (RHEV)** vorgestellt, dessen Hauptprodukt **RHEV für Server** bildet. Dies liefert den Hypervisor RHEV-H und einer Management-Software (RHEV-M), die auch Systeme verwaltet, bei denen statt RHEV Red Hat Enterprise Linux (RHEL) als Host verwendet wird. Ergänzt wird das Paket durch **RHEV für Desktops**, mit dem sich eine Virtual Desktop Infrastructure (VDI) aufsetzen lässt. Wie bisher nutzt der RHEV-Hypervisor zur Virtualisierung KVM (Kernel-based Virtual Machine) und setzt viele Kernkomponenten von RHEL ein, die im neuen RHEV 3 aus der aktuellen RHEL-Version 6.2 stammen und nicht mehr wie beim Vorgänger von RHEL 5. So bringt der neue RHEV-H viele Verbesserungen: Gastsysteme können nun bis zu 64 virtuelle CPU-Kerne und bis zu 2 TByte Arbeitsspeicher nutzen. Techniken wie vhost-net, Transparent huge pages (THP), x2apic und KSM (Kernel Shared Memory) sollen die Performance verbessern und die Effizienz steigern. RHEV für Server ist ab 499 US-Dollar pro Socket und Jahr mit Standard-Support verfügbar. (jp) www.redhat.com/rhev

Lifestyle-Rechner für KMUs

Lenovo kündigt mit der Reihe **ThinkPad Edge E530** neue Notebooks für kleine und mittlere Unternehmen (KMUs) an. Die Rechner richten sich an Nutzer, die **sowohl mit ihnen arbeiten als sie auch privat etwa für Entertainment-Zwecke** nach Feierabend nutzen möchten. Da-



Die neuen Lenovo-Notebooks sollen sowohl Unternehmens- als auch Entertainment-Ansprüchen genügen

bei können die Anwender entscheiden, wie leistungsstark ihr Notebook sein soll. Hierfür haben sie die Auswahl zwischen aktuellen Intel Core-Prozessoren oder AMD Fusion-APUs (bei den Modellen E535) sowie zwischen integrierter oder dedizierter Grafik. Zudem fahren die Notebooks

laut Hersteller besonders zügig hoch, bieten bis zu 1 TByte Speicherplatz, der mit SSD-Speicher kombiniert werden kann, USB 3.0-Anschlüsse und zudem eine hochauflösende Webcam. Modelle mit Intel Core-Prozessoren sind darüber hinaus mit dem Lenovo Solution Center ausgestattet, das durch Intel Small Business Advantage (SBA) unterstützt wird. Die Modelle ThinkPad Edge E530/535 sollen ab Mai 2012 zu einem Preis ab 429

Euro verfügbar sein. (dr)

Lenovo: www.lenovo.com/de

Neue Tricks für ZyWALL

ZyXEL bietet die **Firmware-Version 3.0** für **ZyWALL** an. Die neue Version soll mehr Leistung bieten und unterstützt **IPv6**. ZLD v3.0 ermöglicht zudem einen **Malware-Schutz** und eine **Easy-VPN-Funktion** erlaubt das einfache Einrichten eines ZyWALL IPSec-Clients. Dank eines einfachen Deployments ermöglicht die IPSec-Software einen ähnlichen Prozess wie der SSL-SecuExtender und soll so für eine stressfreie Auto-Provisionierung sorgen. Mit der 3.0-Firmware startet ZyXEL in die erste Phase der IPv6-Implementierung, mit Schwerpunkt auf Dual-Stack, 6rd- und 6-to-4-Transition sowie Host-, Router und Firewall-Funktionalitäten. ZyXEL konzentriert sich bewusst auf diese Bereiche, weil Serviceprovider (SP) bei größeren Phase-1-Deployments für ihre Investitionssicherheit 6rd-Technologien benötigen, neues SP-Equipment

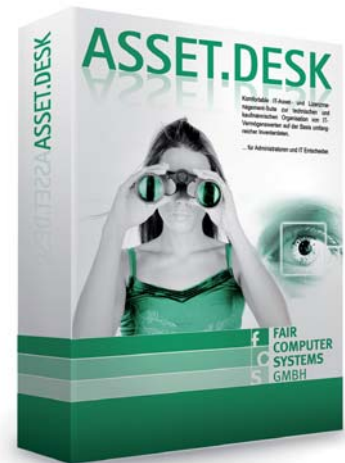
hingegen Dual-Stack-Unterstützung bedarf. Da IPv6 keinen NAT-Schutz bietet, ist zudem eine Firewall erforderlich. In den Phasen 2 und 3 im Laufe des Jahres werden weitere Funktionen wie Dynamic-Routing, IPSec, IDP oder IKEv2 integriert. Neu werden neben den bestehenden ZyXEL Services ein zusätzlicher Content-Filter- sowie Anti-Spam-Dienst der Firma Commtouch angeboten. Die neuen UTM-Services sind als Ein- oder Zweijahreslizenz für alle ZyWALL USG Firewalls verfügbar. Diese kann auch dann angewendet werden, wenn auf dem Gerät bereits der ZyXEL Bluecoat Content-Filter genutzt wird. Kunden können beide Dienste gleichzeitig aktivieren und vom einen zum anderen wechseln; dabei ist aber jeweils nur einer davon in Betrieb. Die Version 3.0 ist kostenlos verfügbar. (dr)

ZyXEL: www.zyxel.de

Das Wichtigste auf einen Blick

Fair Computer Systems startet mit einer neuen Version seiner **Software zum IT-Asset-Management** in das Jahr 2012. **Asset.Desk 5.0** erlaubt im jüngsten Release nun unter anderem die Individualisierung von Inventardaten. So kann der Nutzer selbst definieren, welche Daten das Werkzeug zu einem Gerät auf dessen Übersichtsseite anzeigt. Nicht benötigte Felder lassen sich mit einem grafischen Editor aus der Darstellung entfernen, notwendige hinzufügen. Ebenfalls neu ist die automatische Erkennung von virtualisierten Systemen. Diese werden durch ein eigenes Icon im Übersichts-Baum ersichtlich gemacht und lassen sich ihrem jeweiligen Hostsystem zuordnen. Beim Thema Lizenzmanagement will der Hersteller ebenfalls einen großen Schritt in Richtung Automatisierung gemacht haben. Über die einmalige Definition von Filtern kann der Benutzer neu installierte Software ohne manuellen Eingriff sofort der entsprechenden Katalogsoftware zuordnen. Mit der Einführung von Buchungskreisen soll es die Lösung zudem ermöglichen einzelne Firmen, zum Beispiel innerhalb eines Unternehmensverbunds, zu unterscheiden. Außerdem verfügt das Programm mit Hilfe von teilweise optional erhältlichen Scannern nun über die Funktion, auch Mac-Rechner sowie Android-Smartphones im Unternehmensnetzwerk zu erfassen. Der Preis von Asset.Desk 5.0 richtet sich nach der Anzahl der damit verwalteten Clients. In der Staffel bis 199 Clients beispielsweise kostet das Tool in der Basisversion 20 Euro pro Client. (ln)

Fair Computer Systems: www.fair-computer.de



Mit Asset.Desk 5.0 kann sich der Nutzer nur die Daten zu einem Gerät anzeigen lassen, die er auch wirklich benötigt

WLAN für unterwegs

ZTE bietet den **MF60 Mobile Hotspot** an. Bei dem Gerät handelt es sich um einen **mobil einsetzbaren Hotspot**, der eine Übertragungsgeschwindigkeit von bis zu 21,6 MBit/s ermöglichen soll. Der Hotspot bietet Anwendern so einen mobilen Internetzugang für bis zu acht WLAN-fähige Endgeräte. Geschäftliche Anwender können damit unterwegs oder bei Meetings effizient auf Informationen zugreifen, da der Hotspot einen Internetzugang sowohl über UMTS- als auch über HSPA+-Netze erlaubt. Das Gerät bietet

eine Reichweite von bis zu 40 Metern und unterstützt die WLAN-Standards 802.11b/g. Dabei sei ein mobiler Breitbandzugang für acht WLAN-fähige Geräte über HSPA+ mit einer Übertragungsrate bis zu 21,6 MBit/s möglich. Bis zu vier Stunden soll der Access Point dabei im Batteriebetrieb ohne externe Stromversorgung durchhalten. Eine webbasierte Benutzeroberfläche erlaubt die Einstellung der Parameter, während ein OLED-Display den



Der MF60 Mobile Hotspot bindet acht WLAN-Geräte via Mobilfunk ans Internet an

aktuellen Betriebszustand anzeigen. Für rund 50 Euro ist das Gerät erhältlich. (dr)

ZTE: www.zte-deutschland.de

Astaro goes Amazon

Astaro veröffentlicht das **Astaro Security Gateway in Version 8.3**. Mit der neuen Version lassen sich Astaros UTM-Funktionen nun auch in die **Amazon-Cloud** verlegen und lokale Astaro-Installationen mit einer Amazon Virtual Private Cloud verbinden. Dank der Unterstützung offizieller Amazon Machine Images (AMIs) können Anwender dabei laut Anbieter in Minutenschnelle eine vollständige virtuelle Astaro UTM-Appliance in ihrer eige-

nen Amazon-Cloud aufsetzen. In Version 8.3 ist zudem ein spezieller Connector für die Amazon Virtual Private Cloud (VPC) enthalten. Dieser ermöglicht es Kunden, ihre Serverinfrastruktur in eine sichere, skalierbare Amazon Cloud-Umgebung auszulagern und diese über den neuen Connector sicher mit ihrem Astaro Security Gateway und ihrem Unternehmensnetz zu verbinden. Die Einführung von BGP4 Routing in ASG 8.3 erlaubt Unternehmen und

Netzbetreibern zudem eine Reihe neuer Routing-Funktionalitäten, die die vorhandenen Routing-Tools deutlich erweitern und umfangreichere Einsatzszenarien und komplexe Routing-Umgebungen in Enterprise-Installationen ermöglichen. Des Weiteren beinhaltet Version 8.3 die Unterstützung für den neuen Sophos Access Point AP50, der seit Januar verfügbar ist. Der Einstiegspreis liegt bei 595 Euro. (dr)

Astaro: www.astaro.com

Einstiegs-NAS mit ZFS

Infotrend baut sein Portfolio an **NAS-Systemen für den SOHO- und KMU-Bereich** um weitere Modelle aus. Die neue Serie **EonNAS Pro** ist ein **Tower-System**, das sich laut Hersteller in weniger als 15 Minuten einrichten lässt und Platz für bis zu 24 TByte an Daten bietet. Verfügbare Modelle sind das EonNAS Pro 200, 500 und 800 mit zwei, fünf und acht Laufwerkschächten für 3,5-Zoll-SATA-Festplatten sowie EonNAS Pro 850 mit acht Laufwerkschächten und einem Dual Core 3,3 GHz-Prozessor für eine noch höhere Leistung – die zuerst genannten Varianten sind mit einer Intel-CPU mit 1,8 GHz ausgestattet. Das 850er-Modell ist in drei Variationen auf dem Markt, die sich in der Art

des Netzwerkanschlusses unterscheiden. So ist das Gerät entweder mit zwei oder sechs GBit-LAN-Ports zu haben, zudem ist es auch mit je zwei GBit- und 10 GBit-Ethernet-Anschlüssen erhältlich. Alle Modelle außer der 200er-Version sind an der Frontseite mit einem kleinen LCD-Display ausgestattet, über das sich zum Beispiel eine Schnell-Initialisierung durchführen lässt. Mit ZFS als internem Dateisystem will Infotrend für Datenintegrität sorgen und durch einen hierarchischen Prüfsummen-Mechanismus gerade das Phänomen der schleichenden Datenkorruption aus der Welt schaffen. Ferner sollen natürlich auch die verschiedensten RAID-Modi die Redundanz der Daten beziehungsweise schnel-

le Zugriffszeiten gewährleisten. Die Speicherwürfel unterstützen virtualisierte Umgebungen, IPv6, Port-Trunking, Deduplizierung und das Erstellen von Snapshots. Die Backup-Software FarStone Total Recovery Pro 7 ist im Lieferumfang enthalten. Die Produktreihe **EonNAS 1000** kann weitgehend den gleichen Funktionsumfang sowie die gleiche Software-Ausstattung vorweisen, ist mit einer Höheneinheit jedoch für den **Einbau in 19-Zoll-Racks** gedacht. In dieser Serie lieferbar ist derzeit das Modell 1100, das über vier Laufwerkschächte für 3,5-Zoll-Festplatten verfügt und so auf eine maximale Speicherkapazität von 12 TByte kommt. Außerdem kann der Nutzer des NAS-Geräts auf zwei GBit-Anschlüsse sowie fünf USB-Ports zurückgreifen. Während die Tower-Modelle der EonNAS Pro-Reihe ab 640 US-Dollar erhältlich sind, schlägt die Rack-Variante EonNAS 1000 mit mindestens 1.280 US-Dollar zu Buche. (In)

Infotrend: www.infotrend.com/de



Infotrend setzt beim EonNAS 1000 auf das Dateisystem ZFS und will damit eine hohe Datenintegrität garantieren

IT-Administrator Workshop "Lotus Domino Deployment" am 22. März in Bielefeld

Lotus Tuning

von John Pardey

Im November 2011 veröffentlichte IBM Lotus Notes/Domino in der Version 8.5.3 und bescherte den Anwendern eine ganze Palette neuer Features. Diese beleuchtet der IT-Administrator Workshop am 22. März ebenso im Detail wie Wege zur Virtualisierung des Systems. Außerdem erfahren die Teilnehmer, wie sich die Bereitstellung vereinfachen lässt.

Im harten Wettstreit der führenden kommerziellen Messaging- und Groupware-Systeme legt IBM für sein "Pferdchen im Rennen" Ende des vergangenen Jahres ein Update vor, das die Arbeit sowohl der Anwender als auch der Administratoren vereinfachen soll. Dazu gehören Verbesserungen beim Umgang mit E-Mails ebenso wie der Support für Virtualisierung mit KVM.

Wichtige Neuerungen

Im Rahmen unseres Workshops werden die Dozenten Torben Volkmann und Roland Joeriskes, Lotus Notes/Domino-Spezialisten des Systemhauses acocon, zunächst die wichtigsten Neuerungen im System vorstellen und darauf eingehen, wie sich diese Änderungen auf die tägliche Arbeit, aber auch auf die Optimierung des Systems auswirken.

So stehen Notes-seitig für den Anwender umfangreiche Neuerungen im E-Mailmanagement bereit, insbesondere bei der Suche. Auch lassen sich jetzt E-Mails mit unterschiedlichen Signaturen versenden. Ebenso erfuhr der Kalender und die Besprechungsplanung einige spannende Updates. Und auch mobile Anwender profitieren nunmehr stärker, etwa durch die Unterstützung für Android 3.0-Geräte.

Server-seitig können IT-Verantwortliche nunmehr mit Support für Kernel-based Virtual Machines auf Red Hat Enterprise Linux und SuSE Linux Enterprise Server rechnen. Welche Möglichkeiten dies in der

Praxis ermöglicht, erfahren die Teilnehmer ebenso wie beispielsweise neue Features bei der Verwaltung von Dokumenten.

Virtualisieren und einfach installieren

Wie fast überall in der modernen IT kommen IT-Verantwortliche auch beim Thema Lotus Domino und Lotus Notes nicht an der Virtualisierung vorbei. Unser Workshop beleuchtet die Möglichkeiten, sowohl Server als auch Client in virtuellen Umgebungen zu betreiben. Hier erfahren die Teilnehmer im Detail, welche Möglichkeiten der Virtualisierung bestehen und welche Virtualisierer Lotus Notes/Domino unterstützt. Dabei werden Joeriskes und Volkmann zeigen, wie sich ein aktueller Notes-Client auf XenApp 6 für User zur Verfügung stellen lässt.

Aber auch die unkomplizierte Bereitstellung betrachten die Dozenten: Zum Thema "Lotus Notes-Verteilung und -Aktualisierung" erfahren die Teilnehmer, wie eine zentrale und einheitliche Installation von Clientgeräten mit Lotus Notes zu realisieren ist. Wir zeigen den Teilnehmern zudem Möglichkeiten, die Installation zu vereinfachen und die Notes-Infrastruktur zu aktualisieren.

Alle Informationen zur Anmeldung und Details zum Workshop finden Sie im Kasten "Workshop Lotus Domino Deployment". Die Anmeldung ist bis eine Woche vor dem Termin möglich. Wir würden uns freuen, Sie in Bielefeld begrüßen zu dürfen. 

Agenda

13:00 Uhr: Begrüßung

13.15 Uhr: Lotus Domino und Lotus Notes 8.5.3

Ein Überblick über die Neuerungen und Verbesserungen in der aktuellen Version.

Lotus Domino und Lotus Notes virtualisieren

- Beleuchten der Möglichkeiten, sowohl Server als auch Client in virtuellen Umgebungen zu betreiben. Welche Optionen bestehen, welche Virtualisierer werden unterstützt?
- Praxisbeispiel, wie Sie einen aktuellen Notes Client auf XenApp 6 für User zur Verfügung stellen.

15:00 Uhr: Kaffeepause

Lotus Notes Verteilung und Aktualisierung

- Zentrale und einheitliche Installation von Clientgeräten mit Lotus Notes.
- Möglichkeiten, die Installation zu vereinfachen und die Notes-Infrastruktur zu aktualisieren.

17:30 Uhr: Ende der Veranstaltung

Termin & Ort

22. März 2012

acocon GmbH, August-Schroeder-Straße 4, 33602 Bielefeld

Referenten

Roland Joeriskes leitet den Geschäftsbereich Software Solutions der acocon GmbH und blickt auf eine langjährige Erfahrung im Bereich der Softwaretechnik zurück. Er beschäftigt sich mit der Planung und Realisierung von individuellen Softwarelösungen in internationalen Kundenprojekten. Einer seiner Tätigkeitsschwerpunkte liegt auf der Umsetzung browsergestützter, betrieblicher Anwendungssysteme unter Einsatz moderner Webtechnologien. Zudem ist er ein gefragter Spezialist für Anwendungen auf Basis von Lotus Notes/Domino und deren Integration in betriebliche Abläufe. Des Weiteren wirkt er als Referent auf verschiedenen Konferenzen und ist als Autor diverser Artikel für die Fachpresse tätig.

Torben Volkmann blickt auf eine langjährige Erfahrung im Bereich der Lotus Notes / Lotus Domino Administration zurück und ist bei der acocon GmbH im Geschäftsbereich Systems&Services tätig. Seine Tätigkeitsschwerpunkte liegen in der Konzeption und Realisierung von Collaboration- und Information Management-Lösungen auf Basis Lotus Domino sowie der Anbindung von mobilen Endgeräten im internationalen Projektumfeld.

ITANet Workshop-Partner:



Teilnahmegebühren

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 Euro 75,- (zzgl. 19% MwSt.) pro zusätzlichem Teilnehmer. Für Nicht-Abonnenten wird eine Schutzgebühr von Euro 145,- (zzgl. 19% MwSt.) fällig.

Workshop

"Lotus Domino Deployment"



1&1 SERVER NEXT GENERATION



WELTNEUHEIT EXKLUSIV BEI 1&1:

2 x 16 CORE
AMD OPTERON™ PROZESSOR 6272

DAS NEUE 1&1 DEDICATED SERVER PORTFOLIO:

NEU: 1&1 SERVER MIT
INTEL-PROZESSOREN!

**SERVER
4i**



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

79,99
€/Monat*

AKTION NOCH BIS 29.02.!

**SERVER
XL 6**



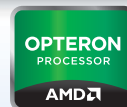
- AMD Hexa-Core Prozessor
- 6 Cores bis zu 3,3 GHz
- 16 GB ECC RAM
- 1.000 GB RAID 1 mit 2 x 1.000 SATA HDD

JETZT: 3 MONATE
FÜR 0,- €*

99,99
€/Monat*

EXKLUSIV BEI 1&1: DER WELT-
SCHNELLSTE HOSTING-SERVER!

**SERVER XXL
32 CORE**



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

499,99
€/Monat*

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

Weitere 1&1 Server
im Internet

1&1



Jetzt informieren
und bestellen:



0 26 02 / 96 91
0800 / 100 668

www.1und1.info

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

IT-Administrator Training "Windows Server Best Practice"
am 21. März/16. April in München und 15. Mai in Hamburg

Bestes Öl für das Windows-Getriebe

von John Pardey



Achtung!

Nur noch wenige Restplätze
 am 21. März in München.
Zusatztermin 16. April!

Von Generation zu Generation sind die Windows-Server robuster geworden und verrichten ihre Dienste, ohne ständig und grundlos in den Blue Screen-Modus zu verfallen. Doch der Administrator sollte dahinter keine Fehlertoleranz vermuten, die es ihm gestattet, nach

Belieben mit den Einstellungen seiner produktiven Server zu experimentieren. Vielmehr sollte der IT-Verantwortliche gerade in zwei zentralen Anwendungen aktueller Windows Server – den Domänendiensten mit dem Active Directory und dem Betrieb als Virtualisierungs-Host – auf bewährte Best Practices vertrauen. Wie diese in Sachen Active Directory, Domänencontroller und Hyper-V aussehen, zeigt Windows-Experte Nils Kaczinski in unserem neuen Training ebenso wie die Umsetzung der Best Practices in der Unternehmens-Infrastruktur. Und auch ein Blick auf kommende Versionen von Active Directory und Hyper-V fehlt nicht.

Einen Domänencontroller unter Windows zu installieren, ist wahrlich keine Kunst. Dieser Vorgang kostet heute auch ungeübte Personen nur wenige Klicks und noch weniger Zeit. Doch eine stabile Infrastruktur ist damit natürlich noch lange nicht etabliert und schon gar nicht ein abgesichertes Active Directory, das auch im Schadensfall schnell wieder online ist.

Das neue Training des IT-Administrator widmet sich daher bewährten Pfaden der Windows-Administration, die sich für komplexe Aufgaben wie die Virtualisierung von Domänencontrollern, die Active Directory-Replikation oder die Sicherheit bewährt haben. Dabei ist die Teilnehmerzahl pro Termin trotz des günstigen Preises von nur 145 Euro für Abonnenten streng begrenzt.

Das Active Directory optimieren

Mit seiner Erfahrung aus mehr als einem Dutzend Jahren Windows- und Active Directory-Administration zeigt unser Trainer Nils Kaczinski typische Stolperfallen und benennt Best Practices für das Active Directory.

Dazu betrachtet Kaczinski gemeinsam mit den Teilnehmern zunächst Fragestellungen hinsichtlich der optimalen Konfiguration von DNS und Active Directory. Anschließend stehen Themen wie Replikation und Sicherheit auf dem Programm. Und bevor Kaczinski "Lieblingsfehler" von Administratoren analysiert, wirft er einen Blick auf das korrekte Vorgehen bei der Virtualisierung eines Domänencontrollers. Und am Ende des ersten Themenblocks des Trainings steht ein Ausblick auf die Neuerungen im Active Directory unter Windows Server 8.

Disaster Recovery für das Active Directory

Doch selbst die besten Methoden der Windows-Administration helfen nicht immer, Fehler oder Datenverluste im Active Directory zu vermeiden. Denn auch wenn der Admin fehlerlos seinen Job verrichtet, wäre er auf ebensolche Hardware angewiesen, um einen reibungslosen Betrieb sicherzustellen.

Zudem kann es vorkommen, dass andere Personen mit schreibendem Zugriff auf

das Active Directory Fehler produzieren. Da sich beides und auch andere Fehlerfälle nicht komplett ausschließen lassen, ist es unverzichtbar, auf ein solides Notfall-Know-how zugreifen zu können.

Dazu startet unser Training mit einer Bestandsaufnahme im Active Directory und der Frage: Was kann eigentlich kaputtgehen? Ist dies geklärt, wird auch schnell offensichtlich, welche Backup-Methoden einzusetzen sind und welche Limitationen diese hinsichtlich des Active Directory aufweisen. Und anhand von Live-Demos zeigt Kaczinski, dass Restore mehr ist als Backup.

Hyper-V sicher und sauber

Ähnlich weitreichend und kritisch wie Fehler im Windows-Verzeichnisdienst sind ohne Frage Probleme beim Betrieb von Hyper-V als Host in der eigenen Virtualisierungsinfrastruktur. Wer aktuell oder zukünftig auf Hyper-V setzt, sollte auch hierfür einige Best Practices beachten. Im Rahmen des Trainings betrachten wir hierzu unter anderem die Sicherheit und das Sizing einer solchen

Infrastruktur. Und auch hier blicken wir zum Abschluss in die Zukunft und schauen uns Hyper-V im kommenden Windows Server 8 an.

Alle Informationen zur Anmeldung und Details der Veranstaltungen finden Sie im Kasten "IT-Administrator Training Windows Server Best Practice". Die Anmeldung ist bis zwei Wochen vor dem jeweiligen Termin möglich – die Teilnehmerzahl ist allerdings streng begrenzt. Wir würden uns freuen, Sie 2012 bei einem unserer Trainings begrüßen zu dürfen. 

Agenda

10:00 Uhr: Begrüßung

So läuft's rund im Active Directory

- Active Directory und DNS
- Virtuelle Domänencontroller
- Replikation
- Sicherheit
- Lieblingsfehler
- Ausblick: Neuerungen im Active Directory unter Windows Server 8

13:00 Uhr: Mittagspause

Wiederbelebung: Disaster Recovery für das Active Directory

- Was kann kaputtgehen?
- Backup-Methoden: Was geht und was nicht?
- Restore ist mehr als Backup: Praxisdemos

Hyper-V sicher und sauber

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

17:30 Uhr: Ende der Veranstaltung

Ort

21. März 2012 sowie Zusatztermin am 16. April 2012:

ExpertTeach Training Center München/Zentrum, Wredestr. 11, 80335 München

15. Mai 2012:

ExpertTeach Training Center Hamburg/Zentrum, Esplanade 6, 20354 Hamburg

Referent

Nils Kaczinski verfügt über mehr als 20 Jahre IT-Erfahrung. Seit Mitte der Neunzigerjahre ist er als Consultant für Windows-Netzwerke tätig und berät Firmen und Administratoren in technischen und strategischen Fragen. Für sein Engagement in Online-Communities ist er seit 2003 von Microsoft regelmäßig als Most Valuable Professional (MVP) in der Sparte "Directory Services" ausgezeichnet worden. Er wohnt mit seiner Familie in Hannover und leitet das Consulting und den Support bei einem mittelständischen Systemhaus. Seine Schwerpunkte sind Active Directory, Windows Server, Exchange, SQL, Scripting und Verfügbarkeit. Neben seiner beruflichen Tätigkeit ist er als Fachautor für Windows-Themen bekannt geworden.

Teilnahmegebühren

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

Anmeldeschluss

7. März (München, Zusatztermin 2. April) beziehungsweise 2. Mai (Hamburg)

IT-Administrator Training
"Windows Server Best Practice"



EXPERTTeach

IT & TK Training



Security-Ausbildung

EXPERTTeach
Networking

Technologie-Know-how

Security in IP-Netzen

Sicherheitslücken erkennen und schließen (4 Tage)

IPv6 und Security

Netze und Endgeräte richtig absichern (2 Tage)

Security für VoIP

Verschlüsselung, Authentisierung und Firewalls (3 Tage)



Original Cisco Zertifizierungen

CCNA Security

Kurs IINS (5 Tage)

CCNP Security

Kurse SECURE, FIREWALL, IPSv7, VPN (4 x 5 Tage)

... und alles mit garantierten Kursterminen! 



Fordern Sie unseren
aktuellen Trainingskatalog an!
Tel. 06074 4868-0



Im Test: ManageEngine OpManager 9.0

Beste Fernsicht

von Sandro Lucifora



Quelle: Scot Maxwell – Fotolia.com

Netzwerk-Monitoring-Produkte sind mittlerweile extrem leistungsfähig, da sie immer mehr Geräte und Prozesse detailliert überwachen müssen. Unser Testkandidat OpManager zeichnet sich unter anderem dadurch aus, dass er für Unternehmen jeder Größe erschwinglich ist. So sind zwei Versionen erhältlich, die jeweils auf KMUs oder große Netzwerkstrukturen ausgerichtet sind. Ende 2011 hat ManageEngine eine runderneuerte Version der Software OpManager zur Überwachung großer Netzwerkumgebungen veröffentlicht. Wir haben uns die neunte Generation genauer angesehen.

Für unseren Test entschieden wir uns für die Standalone-Variante des OpManager 9 (OPM), ideal für das Monitoring in einem geschlossenen Netzwerk. Die Software installierten wir auf einem Windows Server 2008 R2. Im Netzwerk liefen zusätzlich ein Windows Server 2003 und ein Server unter Ubuntu-Linux 11.10 sowie einige Windows-Clients. Der Hersteller liefert native Applikationen für Linux und Windows, die als 32 und 64 Bit-Version erhältlich sind, aus.

Unkomplizierte Installation trotz Einschränkungen bei der Datenbank

Während der Installation mussten wir einige Einstellungen vornehmen und bestimmten den Port, auf dem die Webkonsole von OPM zu erreichen ist, da wir auf unserem Server bereits die IIS mit Port 80 betrieben. Zur Auswahl standen als Datenbank MS SQL sowie MySQL. Bei MS SQL Server ist der IT-Verantwortliche in der Lage, auf einen bereits im Netzwerk installierten Server zurückzugreifen; MS SQL Express wird nicht unterstützt. Alternativ installiert das Setup eine MySQL 5-Datenbank.

Hier hätten wir uns gewünscht, genau wie bei MS SQL Servern auf einen bestehenden MySQL-Server zurückgreifen zu können. In unserem Test haben wir uns für die gebündelte MySQL-Version entschieden. Ein Reboot war nicht notwendig, was die Installation im laufenden Betrieb ermöglicht.

Solide Leistung beim Erkennen der Netzgeräte

Nun mussten wir OpManager 9 konfigurieren und riefen dazu die Webkonsole per Browser auf. Nach dem ersten Login erschien ein Wizard, der uns bei der ersten Erkennung der Netzwerkgeräte behilflich war. Weitere Geräte, etwa solche, die sich nicht im gescannten Netzwerk befinden, ließen sich später noch manuell hinzufügen.

Zunächst mussten wir aber einige Berechtigungen hinterlegen, mit denen OpManager später die benötigten Informationen auf den Geräten abfragt. Damit kommt die Software auch ohne Agents auf den Clients aus. Wir haben sowohl die Berechtigung eines Domänen-Admins als auch für den SSH-Login auf dem Linux-Gerät hinterlegt.

Leider ist es hier nicht möglich, eine Login-Prozedur zu definieren, die nach dem User-Login ein “-su” und somit den Wechsel zu root ermöglicht.

Im nächsten Schritt legten wir fest, nach welchen Standard-Netzwerkdiensten OPM während des Erkennungsprozesses sucht. Neben dem vorgeschlagenen DNS, MS- und MySQL, Oracle, SMTP und Web fügten wir noch FTP und POP3 hinzu. Diese Überwachungen werden, sofern möglich, automatisch für die Geräte gesetzt.

Windows (32 Bit und 64 Bit)

7, 2008 R2, 2003 Server, Vista, XP Pro and 2000 Professional SP4

Linux

RedHat 4.x, Debian 3.0, Suse, Fedora and Mandrake

Datenbank

MS SQL 2000, 2005, 2008 oder MySQL v5.0

Hardware

Je nach Anzahl der zu überwachenden Dienste ab 2 GHz-CPU, 4 GByte Hauptspeicher, 20 GByte freier Festplattenplatz.

Systemvoraussetzungen



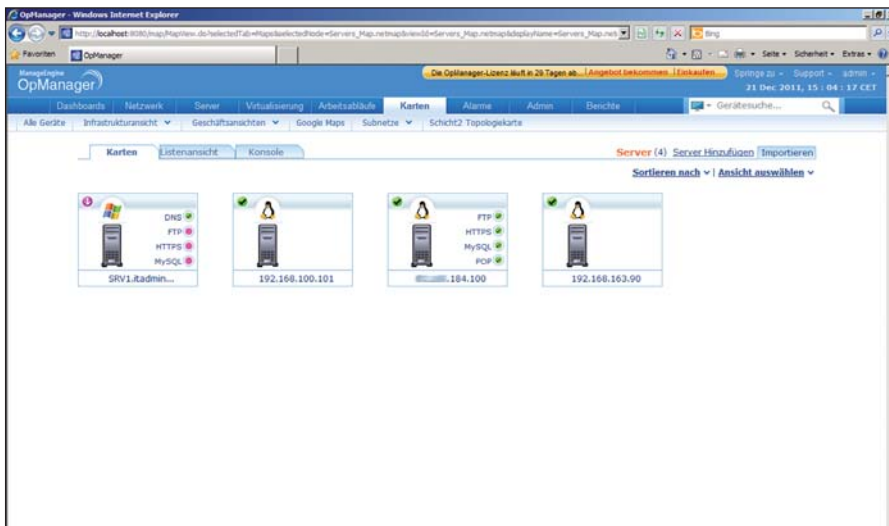


Bild 1: Übersichtliche Statusmeldungen helfen dem IT-Verantwortlichen, den Zustand seiner IT schnell zu überblicken

Schritt vier war die Definition des zu scannenden Adressbereichs. Wahlweise konnten wir hier einen festen IP-Raum wie auch CIDR (Classless Inter-Domain Routing) nutzen. Der Erkennungs-Assistent begann seine Arbeit und listete die Geräte auf, die im beschriebenen Adressraum angebunden waren und mit den zuvor hinterlegten Berechtigungen ausgelesen werden konnten. Nach dem Import der gefundenen Geräte starteten wir den Assistenten erneut, in diesem Fall jedoch mit einem anderen Subnetz, das über eine zweite Netzwerkkarte mit dem Server verbunden war. Auch hier listete uns der Assistent die gefundenen Geräte auf und fügte sie dem Pool hinzu. Geräte außerhalb der gescannten Netzwerke, wie zum Beispiel einen im WAN befindlichen Web-Server, fügten wir dem Überwachungspool nachträglich hinzu.

Schnelle Konfiguration der Überwachung dank Gruppen

Sind die Geräte im Überwachungspool, gilt es, jede Hardware manuell zu gruppieren und die einzelnen Monitore hinzuzufügen. Als Erstes riefen wir unseren Windows-Server über das Dashboard auf und wählten als "Lieferant" "Windows" aus. Danach mussten wir die Kategorie festlegen – hier "Server" – und welche Version installiert ist. Jetzt war es uns möglich, die für das Gerät – also einen Windows Server 2008 R2 – spezifizierten Monitore zu aktivieren. Der Schnellkonfigurations-Assistent half uns, die Überwachung für

mehrere gleichartige Geräte festzulegen. Da uns die Liste der allgemeinen Windows-Dienste und -Prozesse nicht ausreichte, ließen wir uns eine Übersicht der auf dem Gerät laufenden Dienste und Prozesse anzeigen. Leider konnten wir hier nicht – idealerweise mit wenigen Mausklicks – die Monitore für alle laufenden Dienste und Prozesse aktivieren. Vielmehr mussten wir jeden gewünschten Eintrag unkomfortabel einzeln anwählen.

Wird ein Lieferant nicht unterstützt – wie ein exotischer Hardware-Hersteller oder spezielle Linux-Distributionen –, lassen sich keine spezifischen Dienste und Prozesse überwachen. Hier beschränkt sich die Überwachung lediglich auf die Netzwerk-Erreichbarkeit und die über SNMP ermittelbaren Angaben.

Sehr hilfreich und auch notwendig ist die Konfiguration der Abhängigkeiten, die auch vererbt werden. Zum Beispiel lässt sich eine Gruppe von Netzwerkgeräten über VPN in einer Filiale überwachen. Die entfernten Geräte sind an einem Switch angeschlossen. Wir definierten somit die Abhängigkeit des Filialservers mit dem Switch und des Switches mit dem Router. Fällt die Verbindung zur Filiale aus, sind auch die daran angeschlossenen Geräte, Switches und Server nicht erreichbar und OPM meldet Alarm. Durch die Abhängigkeiten meldet das System jedoch "nur" den Ausfall des Routers und nicht auch des Switches und der daran angeschlossenen Geräte.

Detaillierte Überwachung durch herstellernahe Monitore

Wie schon beschrieben, steht dem IT-Verantwortlichen eine Geräte-abhängige Auswahl an Monitoren zur Verfügung, die sich in mehrere Klassen aufteilt. Wird ein Gerät per SNMP überwacht, so werden auch auf Basis des CLI-Protokolls (Command Line Interface) zum Beispiel die CPU-Auslastung, der freie und belegte Festplattenplatz und die Speichernutzung abgefragt.

Dell PowerEdge-Monitore erweitern die Überwachung per SNMP auf die Dell-spezifischen Sensoren wie die Spannung und Temperatur der Hardware. In dieser Form gibt es noch weitere herstellernahe Sensoren für HP Proliant Server und IBM Blade Center, softwareseitig bietet ManageEngine noch SNMP-Sensoren zur Überwachung von Lotus Notes. Hiermit werden der MTA, die Speicherauslastung und andere Details mit insgesamt 31 Monitoren überwacht.

Für die Überwachung eines Windows-basierten Servers gibt es wiederum andere Konfigurationsmöglichkeiten. Auf Basis des Windows-Dienste-Monitors sind wir so über die Betriebsbereitschaft zum Beispiel des DHCP- oder DNS-Servers, des IIS und natürlich der vielfältigen Exchange-Funktionen informiert.

Dateiprüfung mit zahlreichen Parametern

Je nach Client kann das Monitoring auch bis auf Datei- und Ordner-Ebene erfolgen. Bei Dateien konnten wir auf deren Fehlen oder Existieren prüfen. Das funktionierte in Verbindung mit Schwellenwerten bei Dateigröße und Alter als auch Änderung. Mit dem Dateimonitor überwachen wir im Test die Größe und das Alter einer über eine Web-Applikation erstellten Log-Datei. Wurde sie zu groß oder für mehr als 24 Stunden nicht verändert, meldete OPM dies zuverlässig.

Der Ordnermonitor erlaubt, auf das Vorhandensein oder Fehlen sowie die Größe von Ordnern und das Fehlen oder Vorhandensein von definierten Dateien zu prüfen. Die möglichen Logiken sind hier sehr umfangreich und miteinander kombinierbar.

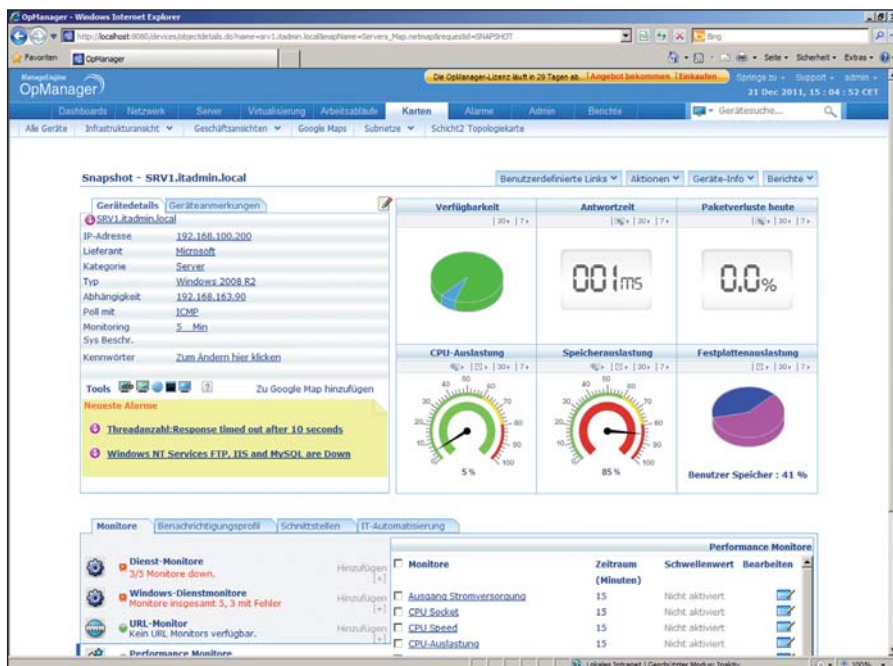


Bild 2: Die Daten aus den Monitoren fasst OpManager grafisch übersichtlich zusammen

Flexibler Nachrichtendienst für die Alarmierung

Natürlich wollten wir auch informiert sein, wenn ein von uns definiertes Ereignis eintritt. Dazu richteten wir einige Benachrichtigungsprofile ein. Um eine klassische E-Mailnachricht zu erhalten, mussten wir zunächst die Mailserver-Konfiguration durchführen. Hier lässt sich auch ein redundanter E-Mailserver festlegen, falls der erste nicht erreichbar oder ausgefallen ist. Für das E-Mail-Benachrichtigungsprofil definierten wir anhand von Variablen, welche Informationen in der Nachricht enthalten sind.

Für SMS-Meldungen wird zwischen E-Mail-basierten und Modem-basierten SMS unterschieden. Hier ist neben der Empfangsart auch die Nachrichtengröße

spezifisch berücksichtigt. Weitere Profilgruppen sind das Ausführen von Systembefehlen oder Programmen als auch das Anzeigen als Webalarm.

In jeder Gruppe legten wir mehrere unterschiedliche Profile an, die je nach Ereignis und Gerät zugewiesen wurden. Zurück beim überwachten Gerät definierten wir, für welches Ereignis und wahlweise auch in welchem Zeitraum ein zuvor definiertes Benachrichtigungsprofil angesprochen wird. So haben wir in Abhängigkeit der Zuständigkeiten für verschiedene Geräte und sogar für unterschiedliche Service-Level und Zeiten Benachrichtigungen an die verschiedenen Personen und Gruppen ausgelöst.

Geografisches Reporting schafft Übersicht

Je nach Netzwerkgröße ist die visuelle Übersicht über die Zustände sehr hilfreich. Dazu bietet OPM verschiedene Möglichkeiten. Zum einen lassen sich Geräte auf einer Google Map positionieren. Dazu benötigt die Software einen Google Map-API-Key. Eine ebenso umfangreiche wie aussagekräftige Übersicht erhielten wir über die Schicht-2-Topologiekarte.

Nachdem wir alle Geräte eingerichtet und ihnen Gruppen wie Router, Switch, Ser-

ver und so weiter zugewiesen hatten, konnte OPM eine Layer 2/Layer 3-Topologiekarte automatisch rendern. Dazu legten wir unseren Kern-Netzwerkknoten beziehungsweise einen Switch als Ausgangspunkt fest. Nach kurzer Zeit zeigte uns die Software eine Topologiekarte mit den Geräte-Status an.

Echtzeitberichte wie auch im Intervall erstellte und per E-Mail als PDF oder XLS versendete Berichte hielten uns immer auf dem Laufenden.

SBS vs. Enterprise

Wie erwähnt, steht der OpManager 9 in zwei Versionen zur Verfügung – für Small & Medium und für Large Enterprises. Der Unterschied bezieht sich dabei auf die strukturelle Anwendung.

Die OpManager Standalone-Edition ist für den Einsatz im Monitoring von bis zu 1.000 Geräten oder 10.000 Diensten ideal. Wichtig dabei ist, dass der Server auf alle zu überwachenden Geräte einen direkten Netzwerkzugriff hat, sei es über LAN oder WAN.

Sind Geräte geografisch verteilt und befinden sich Netzwerke hinter einer Firewall beziehungsweise einem Proxy, kommt die Large Enterprise-Version zum Einsatz. Hier sind die Managementkonsole und die Probes (Sonden) getrennt. Damit werden die Überwachungssensoren dezentral und geografisch unabhängig verteilt und autark betrieben. Über VPN oder das Internet sind diese mit dem CentralServer verbunden, der die Daten auswertet und entsprechend den Regeln reagiert.

Fazit

OpManager 9 von ManageEngine überwacht Netzwerke, Systeme, Datenbanken und Applikationen, darunter Server, Router, Switches und Drucker. Mit übergeordnetem Fehler- und Performance-Management, umfangreichen Berichten sowie CPU-, Speicher-, Disk- und Interface-Statistiken sind alle Informationen gut aufbereitet.

Die neue Version bietet neben einem erweiterten User Interface auch zahl-

Auch der OpManager 9 hat, trotz seines großen Funktionsumfangs, immer noch Lücken bei spezifischen Überwachungen. Um diese zu schließen, unterstützt die aktuelle Version auch die Skriptüberwachung. Damit haben wir im Test jeweils mit einem VBScript als auch einem PowerShell-Skript die Anzahl der Instanzen beziehungsweise die Threadanzahl eines Prozesses überwacht. Durch dieses mächtige Werkzeug sind der Überwachung kaum mehr Grenzen gesetzt – vorausgesetzt der Administrator kann entsprechende Skripte erstellen.

Unbegrenzte Möglichkeiten dank Scripting



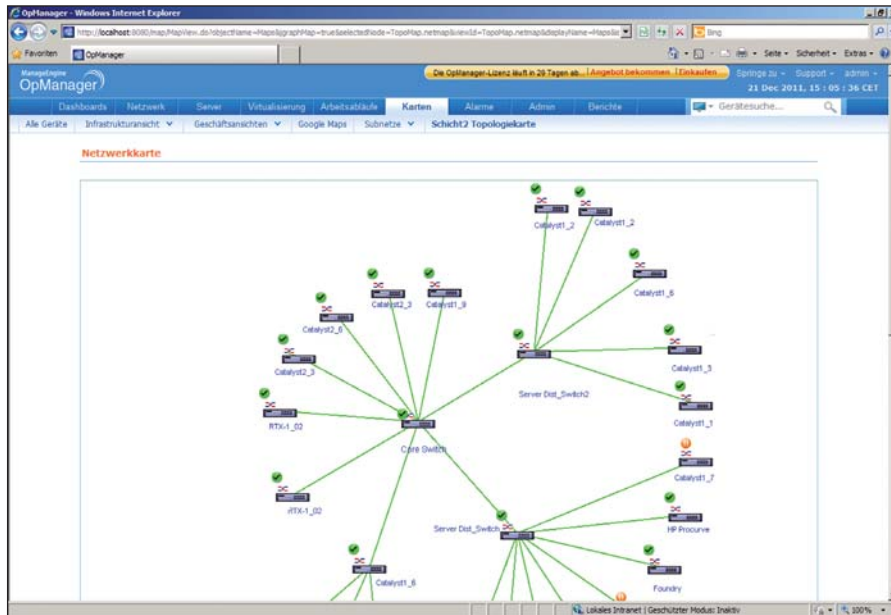


Bild 3: Die Topologiekarte hilft, den räumlichen Überblick über die eigene IT zu behalten

reiche neue Funktionen. So lassen sich jetzt IT-Workflows automatisieren. Zudem verfügt die Lösung über zusätzliche Dienste zur Überwachung virtualisierter Umgebungen unter VMware und Hyper-V. Über die REST-API, eine Programmierschnittstelle, lässt sich der OpManager in bestehende Systeme einbinden. Mit der Erstellung eigener Skripte lassen sich Netzwerke noch individueller überwachen.

Die Konfiguration hat sich, gerade bei großen Netzwerken, als sehr aufwändig herausgestellt. Zwar hilft der Schnellkonfigurator dabei, identische Einstellungen an mehreren Geräten vorzunehmen, doch bleibt es dem Administrator nicht erspart, die meisten Überwachungen manuell einzustellen. Hier hätten wir uns einen Assistenten gewünscht, der das Netzwerkgerät scannt und uns eine Grundausswahl von Monitoren anbietet – quasi eine halbautomatische Start-Konfiguration, wie wir es schon bei anderen Monitoring-Lösungen genutzt haben.

Ansonsten erwies sich OPM als sehr stabil und zuverlässig. Wurden erst einmal alle Einstellungen vorgenommen und Abhängigkeiten und Schwellenwerte eingerichtet, ist der OpManager 9 eine sehr zuverlässige Hilfe dabei, Probleme vorab zu erkennen oder Ursachen mit geringer Auswirkung auf die Erreichbarkeit zu beseitigen. (jp)

Produkt

Software zur Überwachung von Netzwerkkomponenten und -geräten sowie Dateien.

Hersteller

Zoho Corporation
www.manageengine.de

Preis

1.500 Euro in der SBS-Version.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Konfiguration	5
Anzahl an Monitoren	8
Erstellen eigener Monitore	8
Skalierbarkeit	7
Visualisierung und Berichte	6

Dieses Produkt eignet sich

optimal für dezentrale und lokale Netzwerke ab zehn zu überwachenden Geräten.

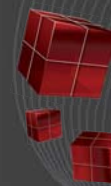
bedingt beim Einsatz von Windows SBS und wenigen Arbeitsplätzen.

nicht für die Überwachung eines Netzwerkes ohne Server.

ManageEngine OpManager 9

www.mypackage.de

Das Portal für
sofort verfügbare
Softwarepakete
zum Festpreis!



- ✓ einfach und wizardgesteuert
- ✓ individuell konfigurierbar
- ✓ dokumentierte Konfiguration
- ✓ mehrfach qualitätsgesichert
- ✓ softwareverteilungsunabhängig
- ✓ jedes Paket für nur 299,- Euro



get your package – now!

Unser **CeBIT-Special:**

Sichern Sie sich Ihren **freien Eintritt** und ein **gratis Softwarepaket** unter **www.mypackage.de**

Code **5j4gIA**

Besuchen Sie uns:

**Halle 6,
Stand G16**

und nehmen Sie an der Verlosung teil!

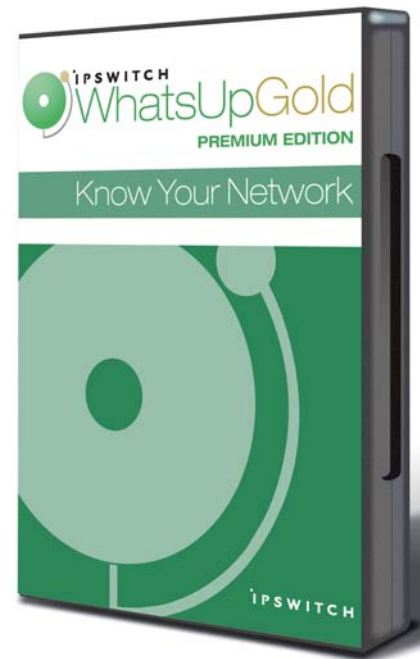


**Im Test: Ipswitch WhatsUp Gold 15 Standard**

Das Netz im Blick

von Thomas Bär

Es ist kaum ein Jahr vergangen, seit Ipswitch seine Netzwerküberwachung WhatsUp Gold in der vierzehnten Version auf den Markt brachte. Jetzt folgt bereits Nummer 15 – da liegt der Verdacht nahe, dass mit der heißen Nadel lediglich kosmetische Neuerungen umgesetzt wurden. IT-Administrator hat deshalb überprüft, ob, und wenn ja, welche neuen Funktionen einen Umstieg auf das neue Release rechtfertigen.



WhatsUp Gold des US-amerikanischen Herstellers Ipswitch ist ein Urgestein im Segment Netzwerkmanagement. Ausgehend von einem durchschnittlichen Release-Intervall von zehn bis zwölf Monaten zeigt die aktuelle Version 15 ganz deutlich, wie viele Jahre die Überwachungssoftware auf dem Buckel hat. Im Gegensatz zu anderen Programmen ist mit WhatsUp Gold eine Überwachung in Netzwerken möglich, ohne eine Client-Software auf die zu überwachenden Server und Geräte aufspielen zu müssen. Angesichts der kostenlosen Konkurrenz aus dem Open Source-Bereich, insbesondere Nagios, muss sich der Hersteller etwas einfallen lassen, um den Kunden bei der Stange zu halten. So ist WhatsUp Gold schnell eingerichtet, erklärt sich an vielen Stellen von selbst und bietet "out of the box" das, was die meisten Administratoren in Unternehmen benötigen. Das Ziel, und das haben die Entwickler von Ipswitch mit der komplett in Web-Technologie überarbeiteten Oberfläche noch einmal deutlich unterstrichen, ist eine einfache und gleichzeitig leistungsfähige Netzwerküberwachung.

Hersteller setzt auf Standards

Der Nutzer installiert WhatsUp Gold ganz klassisch auf einer Workstation- oder Server-Variante von Windows. Die Installation beginnt mit dem Download der knapp 300 MByte großen Installationsdatei über das Internet. Eine Retail-Fassung mit Packung

und Handbuch gibt es schon seit geraumer Zeit nicht mehr. Ipswitch bietet gegen Bekanntgabe einiger persönlicher Informationen eine 30-Tage-Evaluationsversion für Interessenten an. Der Installer prüft während der Einrichtung, ob alle benötigten Komponenten vorhanden sind. Ist dem nicht so, installiert der Assistent die fehlenden Voraussetzungen nach, beispielsweise das .NET Framework 4.

Die benötigte Datenbank, einen aktuellen Microsoft SQL-Server, installiert der Einrichtungs-Assistent in der 2005er Express Edition auf Wunsch gleich mit. Ansonsten steht es dem Systembetreuer frei, einen bereits vorhandenen, höchstwahrscheinlich leistungsfähigeren SQL-Server im Unternehmen einzubinden. Eine Bedingung knüpft der Hersteller jedoch an den Datenbankserver: WhatsUp unterstützt nur englischsprachige SQL-Server. Soll die Software auf einer virtuellen Maschine laufen, muss der Administrator zudem sicherstellen, dass die MAC-Adresse statisch vergeben ist, um Lizenzprobleme zu umgehen. Die restliche Installation beschränkte sich auf die Bestätigung einiger Pfadangaben und die Eingabe der benötigten Passwörter. Ansonsten verlief die Testinstallation ohne besondere Ereignisse.

Im Vergleich zu den Vorgängerversionen spielt das Monitoring-Werkzeug keinen zusätzlichen Webserver mehr auf – WhatsUp Gold 15 verwendet den in Mi-

crosoft Windows integrierten Internet Information Server (IIS). Dies hat den Vorteil, dass der Administrator der Betriebssicherheit des Webservers keine verstärkte Aufmerksamkeit widmen muss, da dieser über den klassischen Microsoft Update-Dienst oder über einen im lokalen Netzwerk betriebenen WSUS automatisch gepatcht wird. Generell baut das Kernsystem von WhatsUp zunehmend auf typischen Microsoft-Komponenten auf. Da der Hersteller auf einen aktiven Agent auf den zu überwachenden Zielsystemen komplett verzichtet, ist das Tool auf die bereits etablierten Standardschnittstellen angewiesen. Dies sind SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation) und andere Klassiker wie TCP/IP, ICMP-Ping und SSH.

Erstkontakt mit vielen Zugriffsdaten

Nach der rund 45 Minuten in Anspruch nehmenden Installation von WhatsUp

Aktuelle PC-Hardware mit Windows Server 2003 SP1 oder neuer, Windows Vista in den Editionen Business oder Ultimate, Windows Server 2008 und höher, Windows 7. Windows XP wird in der Version 15 nicht mehr als Plattform für die Installation unterstützt. Alle benötigten Komponenten installiert die Software bei Bedarf automatisch nach. Mindestens 2 GByte Arbeitsspeicher sind für den Betrieb erforderlich.

Systemvoraussetzungen



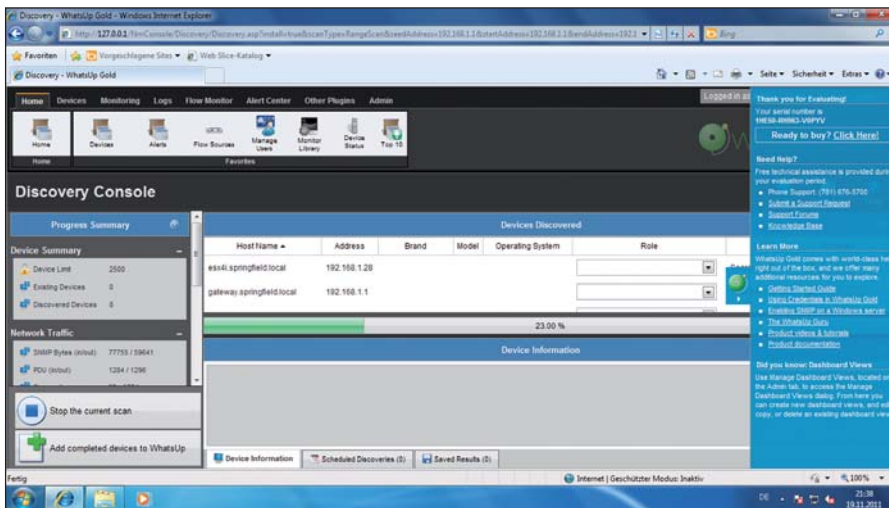


Bild 1: WhatsUp Gold ist in Version 15 nun komplett auf Webtechnik umgestellt – dennoch reicht der Platz immer noch nicht aus, um alle Informationen sinnvoll darzustellen

Gold wird der Administrator in einem Browser-Fenster aufgefordert, sich mit dem Admin-Konto anzumelden und ein Kennwort festzulegen. Von nun an heißt es, sich mit sattelfestem IT-Englisch durch die Dialoge zu arbeiten.

Der Einrichtungsassistent bietet seine Hilfe bei der Suche nach Aktivkomponenten im lokalen Netzwerk an. Je nachdem, ob der Benutzer alle SNMP-Zugriffsinformationen kennt, kann der erste Scan gleich detaillierter verlaufen. Wie auf Windows-Maschinen SNMP zu aktivieren ist, zeigt ein Lehrvideo von knapp sieben Minuten Länge, das im Browserdialog eingebettet ist. Über SNMP kann der Administrator aus Windows-Maschinen die wichtigsten Eckdaten wie den freien Festplattenspeicher oder CPU- und Netzwerkauslastung auslesen.

Im nächsten Schritt ist das E-Mailkonto der IT-Abteilung zu hinterlegen, damit das Überwachungs-Werkzeug im Fehlerfall die IT-Verantwortlichen informieren kann. Es gibt noch verschiedene andere Kommunikationswege. Beim Einstellen der Benachrichtigungen gilt es natürlich, die Kommunikationswege mit Augenmerk auf die Sicherheit auszulegen: Fällt beispielsweise der einzige Exchange-Server eines Standorts aus, so bekommt niemand mehr eine E-Mailnachricht, auch nicht von WhatsUp. Ausfälle des primären Mailservers sollten also durch weitere Benachrichtigungsmöglichkeiten ergänzt werden.

Erst in diesem Schritt fordert die Software die Eingabe der verschiedenen Zugriffsdaten. Im Auswahlfenster entdeckt der Benutzer neben SNMP v1 bis v3, Windows, ADO, Telnet und SSH auch VMware-Credentials. Dem Nutzer steht es frei, mehrere Zugriffsdatentypen mit unterschiedlichen Zugriffsdaten einzurichten. So legt der Administrator beispielsweise für SNMP die gängigen Standard-Kombinationen wie "public/private" oder "public/cisco" an. Die in diesem Dialog eingegebenen Informationen fügt die Software automatisch in die Datenbank ein.

Automatisierter Scan erspart Handarbeit

Der Administrator nimmt die Suche im Netzwerk entweder traditionell über einen IP-Bereich vor oder entscheidet sich für den sogenannten "SNMP Smart Scan". Bei dieser etwas eleganteren Methode handelt sich die Software über die SNMP-Zugriffsdaten von Router zu Router und findet so alle aktiven Geräte im Netzwerk. Die automatische Suche nach Komponenten, unabhängig von der gewählten Methode, erspart dem Benutzer das mühselige manuelle Eintragen. Trotz der komplett neu überarbeiteten Oberfläche, die insgesamt modern und ansprechend gehalten ist, hat sich ein Kritikpunkt der Vorgängerversion gehalten: Die Ausnutzung des Fensters zur Anzeige der Daten aus dem Scan ist miserabel. Das ist insbesondere für diejenigen Administratoren sehr ärgerlich, die auf einem Laptop mit schwacher Bildschirmauflösung arbeiten.

Das Scan-Ergebnis lag im Test nach wenigen Minuten vor und selbst in komplexeren Umgebungen mit mehreren hundert Geräten ist das erste Ergebnis üblicherweise in weniger als 15 Minuten sichtbar. Die von der Software vorgeschlagene Funktion eines Geräts im Netzwerk mussten wir in vielen Fällen nachbearbeiten, insbesondere wenn WhatsUp aufgrund mangelnder SNMP-Unterstützung nur anhand der angebotenen Services versucht, Rückschlüsse

Ipswitch liefert WhatsUp Gold in drei unterschiedlichen Ausbaustufen mit entsprechend unterschiedlichem Preismodell. Allen Editionen ist gemein, dass sie über die Weboberfläche gesteuert werden, eine SQL-Datenbank verwenden, die Netzwerküberwachung mit frei definierbaren Schwellenwerten über "Performance-Monitore" abwickeln und beliebige Skript-Jobs als Antwort auf einen erkannten Missstand bieten. In der Edition **WhatsUp Gold Standard** für kleinere und mittelständische Unternehmen steht die reine Netzwerküberwachung im Vordergrund. Die Variante **Premium** ermöglicht WMI-Überwachung, SSH-Aktionen für Unix- und Linux-Systeme, vorgefertigte Überwachungs-Vorlagen, Transaktions-Monitoring für HTTP/HTTPS und FTP sowie zusätzliche Echtzeitüberwachungen mit grafischer Auswertung.

In der dritten Version, der **WhatsUp Gold Distributed**, erweitert sich die Überwachungsfähigkeit in Bezug auf verteilte Netzwerke. Was die Premium-Edition kann, vollbringt auch die Distributed-Variante. Letztere bietet alle Funktionen, die für das Monitoring von Netzwerken, Servern und Anwendungen in komplexen, standortübergreifenden Netzwerken erforderlich sind. Sie eignet sich dabei sowohl für Zentral- als auch Remote-Installationen. Somit ist eine Überwachung des lokalen Standorts wie mit den beiden einfacheren Editionen möglich, aber eben auch die zentrale Steuerung der Außeninstallationen. So gesehen ist die Distributed-Variante eine Erweiterung von WhatsUp Gold Premium, da sie eine sichere Konnektivität zwischen einem zentralen Network Operation Center (NOC) und beliebig vielen Remote-Standorten herstellt.

Als **zusätzliche Erweiterungen** bietet Ipswitch die Module **Flow Monitor & Flow Publisher**, um die Netzwerkauslastung auf Applikationsebene feiner darzustellen. **Whats Configured** ist eine Konfigurations- und Change-Management-Software für Aktivkomponenten im Netzwerk, **Whats Connected** liefert eine detaillierte Suche und Überwachung von OSI-Layer 2/3-Geräten. Mit **Whats Virtual** möchte der Hersteller die Überwachung von virtueller Infrastruktur feiner abbilden und der **VoIP Monitor** stellt die Netzqualität der IP-Telefonie sicher. Alle diese Plug-In-Module sind kostenpflichtige, optionale Erweiterungen, die sich in jede Edition integrieren lassen.

Editionen und Module



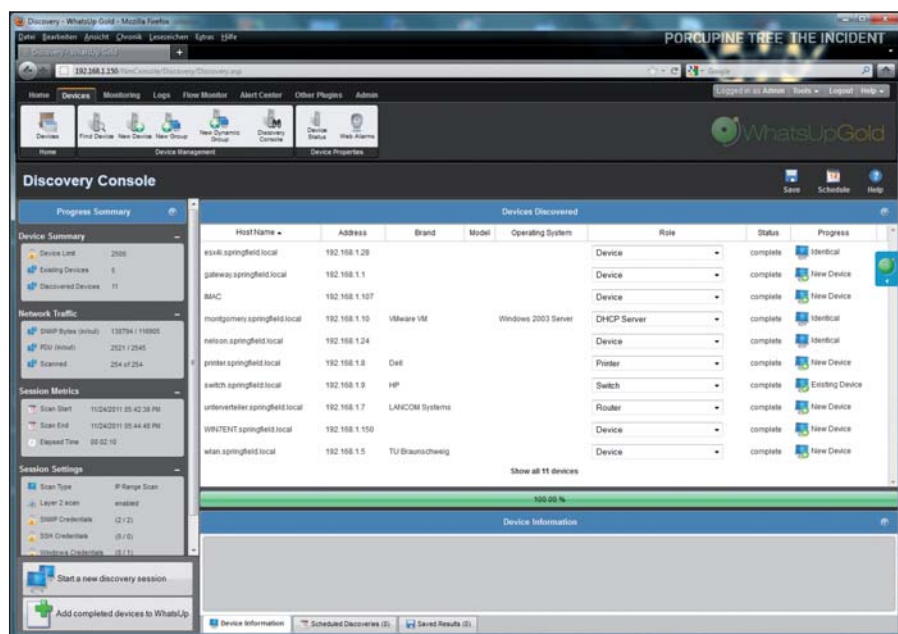


Bild 2: Dank der Suchfunktion ermittelt die Software auf Wunsch automatisch neue Netzwerkgeräte

zu ziehen. Rollen wären beispielsweise Router, Webserver oder Mailserver.

Wurde noch in der Vorgängerversion ein Cisco/Linksys WAP54G-Access Point zu einem Webserver, so ist es in der aktuellen Fassung ein schlichtes "Device". Die Fehlinterpretation, dass es sich hierbei um ein Gerät des Herstellers "Technische Universität Braunschweig" handelt, ist jedoch noch vorhanden. Ansonsten liefert die Software exakte Ergebnisse zu Routern und Switches von Lancom, Cisco oder HP und Windows-Servern. Bei unserem allerersten Scan des Netzwerks im Test konnten die Ergebnisse jedoch nicht gespeichert werden, wie uns ein Timeout-Fehler zeigte. Wir starteten die virtuelle Maschine, in der WhatsUp Gold lief, einmal durch und der Fehler trat nie wieder auf – möglicherweise bedarf die Software nach der Installation also einfach noch eines Reboots.

Die simple Suche im IP-Bereich hat den Nachteil, dass alle in diesem Segment betriebenen PCs in der Liste auftauchen. Dies hat zur Folge, dass der Administrator mit Meldungen zum Status-Wechsel überschüttet wird. Ob jedoch der Computer aus dem Empfangsbereich nun ein- oder ausgeschaltet ist, dürfte kaum einen Administrator wirklich interessieren. Der über das Netzwerk angebundene Laserdrucker indes bedarf der regelmäßigen

Prüfung, insbesondere dann, wenn sich mehrere Mitarbeiter im Unternehmen das Gerät als Arbeitsgruppendrucker teilen. Ob sich die automatische Suche mit dem Assistenten in der Praxis lohnt oder nicht, muss der Anwender im Einzelfall selbst entscheiden. Wiederholende Suchvorgänge helfen zumindest, das Netzwerk genauer im Blick zu behalten. Ob ein Device schon vor dem aktuellen Scan eingetragen war oder nicht, sieht der Administrator in der Zusammenfassung des Suchergebnisses.

Mit der Netzwerkkarte ans Ziel

Die grafisch orientierte Ansicht des Netzwerks, die "Map", darf natürlich auch in der neuesten Version nicht fehlen. Der Nutzer kann hier verschiedene Gerätegruppen zusammenstellen und sich so einen einfacheren Überblick verschaffen. Neben den logischen Verbindungen ist der Administrator so in der Lage, ebenso die physikalische Verkabelung der Geräte in Karten nachzuahmen.

Das Anlegen einer Karte ging im Praxis-test recht leicht von der Hand. Die Hauptschwierigkeit besteht in erster Linie darin, betriebsentscheidende Komponenten so in der Karte abzubilden, dass ein möglichst exaktes Bild entsteht. Sofern alle hinterlegten Geräte aktiv sind und alle zu überwachenden Dienste korrekt antworten, wird dies in einem selbstsprechenden

Farbmodell dargestellt. Fehlerhafte Systeme sind mit einem Blick zu erkennen: Der Hintergrund des Symbols erscheint nicht mehr in Grün, sondern wechselt in Abstufungen bis Rot.

Das Kontextmenü vereint verschiedene Befehle, die in der täglichen Administration häufig zum Einsatz kommen. Für den Zugriff auf Windows-Server ist hier der Remote Desktop zu nennen und für die meisten Netzwerkgeräte die Verbindung per Telnet oder auf die Weboberfläche. Welche Befehle angezeigt und genutzt werden können, bestimmt der Administrator in den Stammdaten der Software selbst. Die Integration von VMware ESX geht soweit, dass sich über das Kontextmenü ein Gastsystem direkt aus WhatsUp heraus neu starten lässt.

Ist erst einmal die komplette Netzwerklanschaft abgebildet, so beginnt das Programm in der Standardeinstellung damit, jedes Device im Takt von einer Minute abzufragen und die Leistungsdaten zu sammeln. Veränderungen, beispielsweise in der Laufzeit von ICMP-Pings, sind so statistisch auswertbar. Allein die Reaktionszeit von Ping-Kommandos bietet auf lange Sicht eine gute Grundlage, um Veränderungen in der Funktionalität des Netzwerks zu identifizieren.

Ob passiv oder aktiv – alle Geräte stets im Blick

Grundsätzlich unterscheidet die Software zwischen zwei verschiedenen Überwachungsarten: Diese werden als passive beziehungsweise aktive Monitore bezeichnet. Bei der aktiven Überwachung wird die Reaktion eines Netzwerkgeräts, klassischerweise das Rücksenden der Ping-Anfrage oder der Ausfall eines Dienstes, geprüft. Als aktive Monitore bietet WhatsUp DNS, Echo, FTP, HTTP, HTTPS, IMAP4, Interface, NNTP, Ping, Printer, POP3, Radius, SMTP, SNMP, Telnet oder Time als Protokoll beziehungsweise Funktion. Das im Windows-Umfeld gebräuchliche WMI nutzt WhatsUp Gold nur in den größeren Editionen. Beispielsweise ließe sich die Speicherauslastung eines Servers mit wenigen Mausklicks kontinuierlich überwachen oder die Anzahl von gesendeten Nachrichten eines Microsoft Exchange-Servers.



Die passive Überwachung prüft über die so genannten "Listener"-Meldungen, die von Geräten ausgesendet werden. Dies wäre beispielsweise der Eintrag der Antivirusssoftware in die Windows-Ereignisanzeige oder die SNMP-Meldung eines Switches, dass ein Netzwerkinterface den Status verändert hat. Weiterhin bieten sich SYSLOG-Ausgaben als passiver Monitor in WhatsUp Gold an.

Durchdachte Automatisierung

Die beste Überwachungssoftware nutzt nichts, wenn im Fehlerfall niemand in Kenntnis gesetzt wird. Im besten Fall leitet das Monitoring-Werkzeug sogar selbst automatisch Gegenmaßnahmen ein. Im Zweig "Admin" des im modernen Ribbon-Look gehaltenen Menüs legt der Systembetreuer unter "Actions" mögliche Maßnahmen fest. Die Bandbreite reicht von Benachrichtigungs-E-Mails über SMS-Aktionen, Syslog-Einträge, Programm-Aktionen bis hin zu "Text to Speech", sofern die Zusatzkomponente eingerichtet ist. Im letzten Fall könnte die Software einem Menschen bei Erreichen eines definierten Werts eine gesprochene Nachricht über das Telefon senden. Insgesamt umfasst der Aktionskatalog 19 verschiedene Möglichkeiten der Reaktion und Benachrichtigung.

Die klassische Benachrichtigung über den Ausfall ist sicherlich die E-Mail an

die Systemadministration. Den Textinhalt passt der Administrator gemäß den eigenen Wünschen an. Werte, die WhatsUp Gold liefert, wie beispielsweise IP-Adresse oder Gerätenamen, bietet die Software über Variablen an. Dank der bereits hinterlegten Vorlagen ist die Suche nach der passenden Variable nicht schwer. Die Fleißarbeit für den Administrator bei der Anpassung bleibt jedoch. Vor allem ist es mit dem Text allein nicht getan – die Hauptarbeit besteht darin, die für die Anlage passenden Eckwerte zu finden. Es gibt Geräte, die auch einmal drei Minuten in Folge nicht reagieren können, ohne dass gleich die IT mit einem Großeinsatz ausrücken muss.

Nach welchen Mustern Administratoren die Mischung aus Benachrichtigung und Monitoring auch stricken werden: Es ist und bleibt höchst individuell. Ab welchem Zeitwert oder Intervall eine Nachricht ausgeschickt wird, oder ob andere von dieser Überwachung abhängige Services oder Geräte ebenfalls Alarm schlagen sollen, ist ohne Blick in die englischsprachige Online-Doku zügig eingerichtet. Das Verfahren gleicht hierbei weitgehend den Vorgängerversionen.

Fazit

Die neue Oberfläche ist den Entwicklern von Ipswitch sehr gut gelungen. So gut wie alle modernen Elemente, etwa frei verschiebbare Ansichten im

Dashboard, beherrscht WhatsUp Gold in der Version 15. War bisher immer der Rückgriff auf die EXE-Datei notwendig, so ist die Software nun eine echte Web-Applikation.

Dank optionaler und kostenpflichtiger Erweiterung passt sich das intuitiv zu bedienende WhatsUp Gold – im einfachen Handling liegt einer der Hauptvorteile gegenüber dem freien Nagios – den gewünschten Anforderungen im Unternehmen an. Features wie die bessere VMware-Integration zeigen zudem, dass nicht nur an der Oberfläche gefeilt wurde. Gerade für Betreiber von (verteilten) virtualisierten Umgebungen dürfte sich ein Umstieg auf das aktuelle Release lohnen. (In) 

Produkt

Programm zur Überwachung von Netzwerkkomponenten in lokalen und verteilten Umgebungen.

Hersteller

Ipswitch
www.whatsupgold.com/de

Preis

Rund 1.500 Euro für 100 zu überwachende Devices.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Erkennung von Netzwerkkomponenten	8
Darstellung	8
Umfang der Monitoring-Features	8
Überwachung	8
Benachrichtigungsoptionen	7

Dieses Produkt eignet sich

optimal für Unternehmen, die in heterogenen und verteilten Netzwerken ein zügiges und sicheres Monitoring benötigen.

bedingt für kleinere und eher stabile Umgebungen.

nicht für Unternehmen, in denen keinerlei Aktivkomponenten vorhanden sind und Serverdienste extern bezogen werden.

Ipswitch WhatsUp Gold 15 Standard

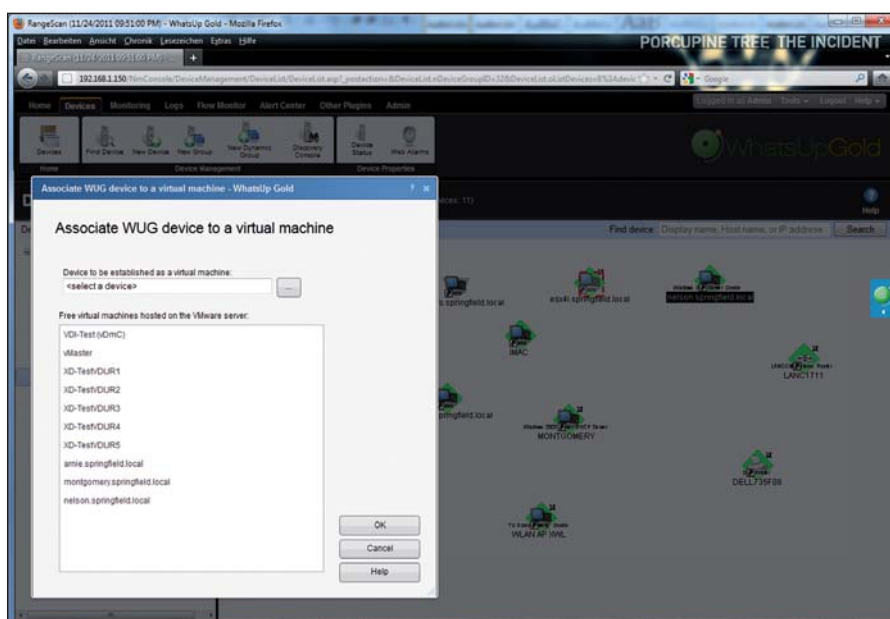


Bild 3: In der Version 15 ist WhatsUp Gold dazu in der Lage, direkt auf VMware ESX-Systeme zuzugreifen



24-Stunden-Diagnose

von Jürgen Heyer



Jeder Administrator hat diese Situation wohl schon einmal erlebt: Der Server läuft, er ist erreichbar, alle Dienste sind augenscheinlich in Betrieb und trotzdem arbeitet das System nicht korrekt. Schon geht die aufwändige Fehlersuche los. Der SSC-ServerInspector will hier einen Schritt voraus sein und überwacht sowohl Server als auch das Netzwerk auf funktionaler Ebene. IT-Administratoren wollten genauer wissen, wie gut und zuverlässig das Tool diese Aufgabe erfüllt.

Beim SSC-ServerInspector handelt es sich um ein Werkzeug für die Server- und Netzwerküberwachung aus der kleinen Software-Schmiede SSC-Software. Zielgruppe sind in erster Linie sehr kleine bis mittelgroße Unternehmen, die sowohl ihre Server als auch die betriebenen Dienste im Netzwerk nicht nur auf Verfügbarkeit, sondern auch auf Funktionalität hin prüfen möchten. Normalerweise sind solche Produkte zur Prüfung einer Applikationsverfügbarkeit zum einen recht teuer und zum anderen ziemlich aufwändig in der Bedienung. Dass es auch anders geht, hat ServerInspector im Test eindeutig bewiesen. Die Nutzung ist für einen Administrator beileibe kein Vollzeitjob, vielmehr dürfte das Tool nach der Einrichtung weitgehend unbeaufsichtigt laufen, nur abgesetzte Meldungen sind auszuwerten.

Rasche Installation auf Server oder Workstation

Das rund 33 MByte große Softwarepaket ist in wenigen Sekunden installiert. Dies kann auf einem Server, aber auch auf einer Workstation erfolgen. Dabei werden nur der Installationspfad und die Anmeldeinformationen für einen Domänenadministrator abgefragt. Es ist aber auch möglich, den Dienst des ServerInspectors unter dem lokalen Systemaccount laufen zu lassen. Dann sind allerdings bei Zugriffen auf andere Server entsprechende Anmeldeinformationen einzugeben – was auch bei allen Aktionen möglich ist.

Die gesamte Bedienung und Konfiguration erfolgt über eine zentrale Konsole. Im Anschluss an die Installation sind hier diverse Grundeinstellungen zu setzen, die in einer Rubrik zusammengefasst sind. So muss der Administrator die Benachrichtigungsempfänger angeben. ServerInspector besitzt hierzu eine eigene Benutzerverwaltung mit einer Gruppierungsmöglichkeit. Eine Anbindung an ein vorhandenes Active Directory ist nicht vorgesehen, was erfahrungsgemäß in kleineren Umgebungen noch nicht so tragisch sein dürfte, in

größeren Netzwerken aber auf jeden Fall wünschenswert wäre.

Die abgefragten Benutzerangaben sind konsequent auf den Bedarf der Software zugeschnitten. So sind für den Empfang von Benachrichtigungen E-Mailadresse und Telefonnummer des Handys anzugeben. Dann lassen sich die Arbeitszeiten festlegen, um in einem weiteren Register anzugeben, ob E-Mail- und SMS-Benachrichtigungen des Programms nur während der Arbeitszeit oder auch außerhalb zugestellt werden sollen. Einstel-

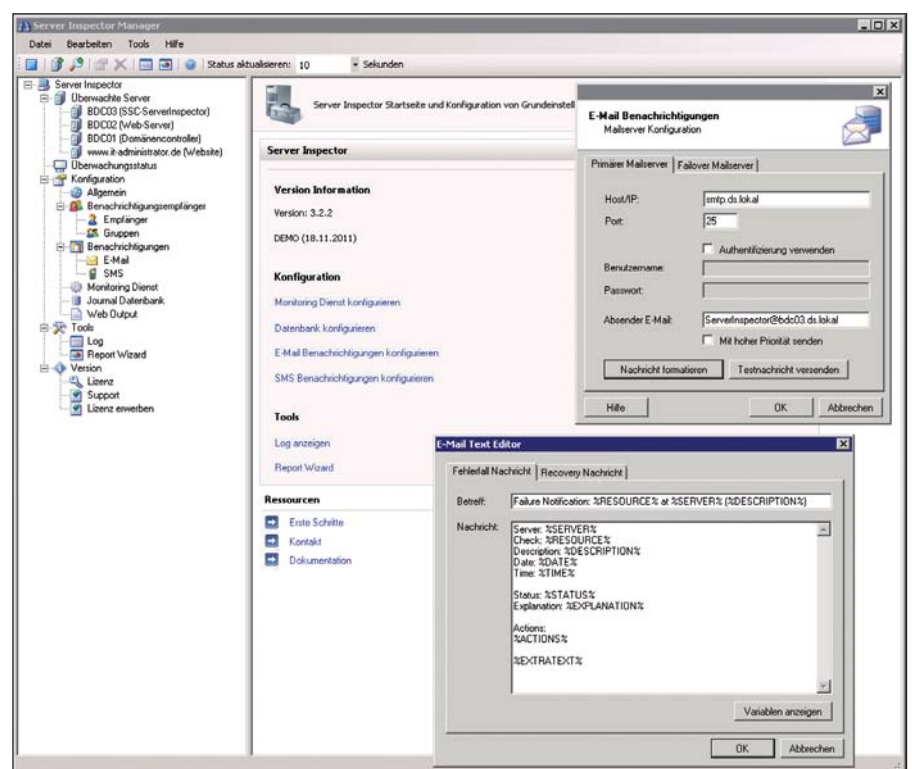


Bild 1: ServerInspector verschickt bei Fehlern E-Mails, die sich hinsichtlich des Inhalts genau konfigurieren lassen



Bild 2: Benachrichtigungen per SMS können wahlweise über ein GSM-Modem oder einen SMS-Dienst im Internet verschickt werden

len lässt sich beispielsweise auch, dass während der Arbeitszeit E-Mails und außerhalb SMS gesendet werden. Um die Zuweisung von Benutzern und Gruppen zu Überwachungen zu vereinfachen, lässt sich pro Benutzer und Gruppe angeben, ob das Objekt bei jeder neu angelegten Überwachung automatisch als Empfänger hinzugefügt werden soll.

Benachrichtigung auf mehreren Wegen

Benachrichtigungen können als E-Mail oder per SMS verschickt werden, auf Wunsch auch parallel. Neben einem primären Mailserver wird ein Failover-Mailserver unterstützt. SMS lassen sich über den Anbieter Clickatell oder ein GSM-Modem versenden, auch steht ein Failover-Pfad zur Verfügung. Eine Weitergabe von Meldungen per SNMP ist hingegen nicht vorgesehen. Allerdings ermöglicht ServerInspector neben der aktiven Benachrichtigung auch eine Bereitstellung des Status im HTML- und XML-Format.

In diesem Fall erzeugt das Programm in festen Abständen eine Status-Seite im HTML- und/oder XML-Format, die entweder in ein bestimmtes Verzeichnis kopiert oder als FTP-Upload an einen vorgegebenen Ort übertragen wird. Betreibt nun ein Unternehmen einen eigenen Webserver, so kann ServerInspector seine Statusseite in dessen Struktur regelmäßig aktualisieren. Bei Bedarf greift ein Administrator darauf zu, um beispielsweise bei einer Benachrichtigung besser zu erkennen, was alles betroffen ist. Unserer Meinung nach ist diese Möglichkeit eine gute Ergänzung zu den aktiven Be-

nachrichtigungen, die zudem mit wenigen Mitteln erfreulich einfach zu konfigurieren ist.

Auch innerhalb der Konsole des ServerInspectors gibt es eine komprimierte Ansicht "Überwachungsstatus". Hier sind alle Überwachungen nach Systemen geordnet mit Status, Typ, Beschreibung, Intervall und Fehlerzähler aufgelistet. In der Statusspalte wird mit farbigen Einträgen gearbeitet, so dass rot markierte Fehler sofort zu erkennen sind. Der Administrator kann zudem sortieren lassen, wobei aber die Trennung nach den Servern beibehalten wird. Es stehen dann nur alle fehlerhaften Überwachungen jeweils oben in der Liste.

Während bei der Benachrichtigung an redundante Wege gedacht wurde, ist hinsichtlich eines Ausfalls des ServerInspectors selbst nichts explizit vorgesehen. Wir sehen hier zwei vom Tool unabhängige Lösungsansätze. Der eine besteht darin, das darunterliegende System möglichst hochverfügbar zu machen, indem beispielsweise eine virtuelle Maschine verwendet wird, die sich bei Bedarf verschieben lässt. In etwas größeren Umgebungen könnte ServerInspector auch zweimal installiert werden, um die Überwachungen aufzuteilen und damit sich die beiden Systeme einfach gegenseitig kontrollieren.

Kommunikation ohne Agenten

Um nun einen Server zu überwachen, ist dieser zuerst mit seinem Namen oder der IP-Adresse zu erfassen. Dann können Anmeldeparameter übergeben werden. Inwiefern diese benötigt werden, hängt davon ab, ob Aktionen ausgeführt werden sollen, die eine Anmeldung erfor-

dern. Wurde bei der Grundkonfiguration des Tools ein Domänenadministrator angegeben, der auch für dieses System zur Anmeldung verwendet werden kann, so kann eine erneute Eingabe entfallen. Ein Agent muss auf den zu überwachenden Systemen nicht installiert werden, denn eventuell benötigte Kenngrößen fragt die Software per WMI ab. Das erleichtert die Einrichtung und Pflege enorm, da sich diese somit allein auf ServerInspector selbst beschränken. Es ist nur darauf zu achten, dass bei Nutzung der Windows-Firewall die benötigten Ports geöffnet sind.

Zu jedem Server können feste Wartungszeiten hinterlegt werden, in denen die Überwachung ausgesetzt wird, also auch keine Meldungen verschickt werden. Standardmäßig werden die Wartungszeiten auf die zugeordneten Überwachungen vererbt, es lassen sich hier aber auch andere Zeiten festlegen. Ist nun ein System in ServerInspector erfasst, folgt als nächster Schritt das Eintragen von Überwachungsaufträgen. Bei jedem Auftrag öffnet sich ein Fenster mit fünf Registern. Im ersten Register "Allgemein" ist die Beschreibung einzutragen sowie das Überwachungsintervall. In ein Zusatztext-Feld können beliebige Hinweise hinterlegt werden, die auch in einer Benachrichtigungsmail erscheinen.

Im Register "Benachrichtigungen" sind die angelegten Benutzer und Gruppen zu sehen, um daraus die gewünschten Empfänger auszuwählen. Wie schon erwähnt, kann der Administrator Standardempfänger vorgeben, die automatisch bei jedem Überwachungsauftrag hinzugefügt wer-

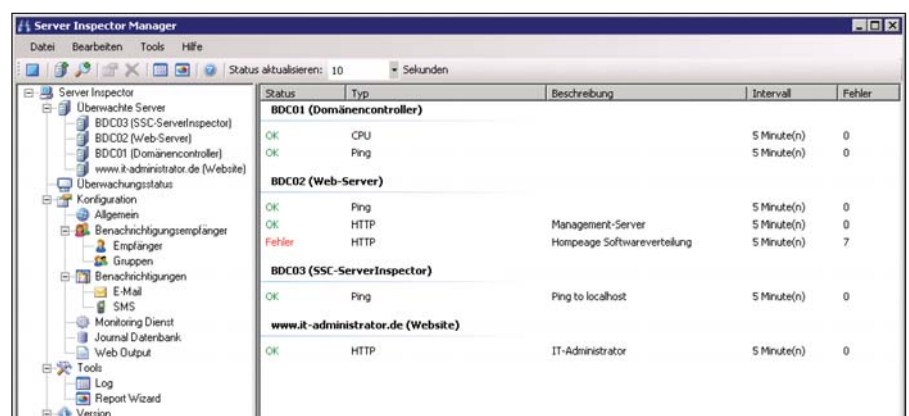


Bild 3: Eine Statusseite liefert nach Servern geordnet das aktuelle Ergebnis für alle laufenden Überwachungen

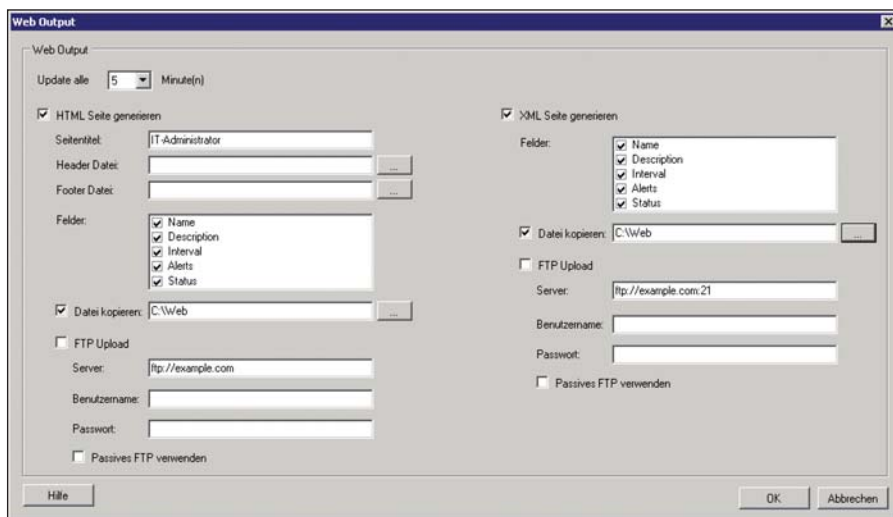


Bild 4: ServerInspector erzeugt für eine aktuelle Statusanzeige regelmäßig eine Seite im HTML- und/oder XML-Format, die sich einfach in einen Webauftritt einbinden lässt

den. Als sehr sinnvoll empfanden wir im Test die Möglichkeit, anzugeben, ob eine Benachrichtigung nur einmal oder wiederholt verschickt werden soll, solange das Problem besteht. Gut ist auch, dass sich vorgeben lässt, dass nur alle x Überprüfungen benachrichtigt werden soll. Wird also im Fünf-Minuten-Takt geprüft und dann eingestellt, dass nur alle zwölf Überprüfungen benachrichtigt werden soll, so erhalten die Empfänger stündlich eine Mail. Das hat uns recht gut gefallen, denn so besteht weder die Gefahr, dass ein Problem wegen einer nur einmaligen Benachrichtigung vergessen wird, noch dass ein Empfänger von der Häufigkeit einer Meldung genervt wird und womöglich in der ständigen Meldungsflut eine andere wichtige übersieht. Sinnvoll ist auch, dass ServerInspector auf Wunsch eine Benachrichtigung verschickt, wenn eine Überprüfung nach Fehlern wieder ein positives Resultat liefert. Über das Register "Wartung" können andere Wartungszeiten hinterlegt werden, wenn die globalen Vorgaben für den Server nicht übernommen werden sollen.

Zahlreiche Überwachungsvarianten an Bord

Inhalt und Aufbau des Registers "Konfiguration" orientieren sich an den Detailinformationen, die für die jeweilige Überwachung benötigt werden. ServerInspector kennt insgesamt 24 unterschiedliche Überwachungsarten, die in vier Rubriken unterteilt sind – Datenbank, Netzwerk/Internet, Windows Betriebssystem und

Sonstiges. Lässt sich das Gewünschte mit keiner der 24 Arten abbilden, so besteht noch die Möglichkeit, ein eigenes Skript in C# oder VB.Net-Syntax zu hinterlegen. Ein kurzes Beispiel wird mitgeliefert, darüber hinaus leistet auch OptCon Support.

Bei der Datenbanküberwachung unterstützt ServerInspector Microsoft SQL, MySQL, Oracle sowie eine allgemeine ODBC-Datenquelle. Dabei prüft das Tool nicht nur die Verbindung, sondern führt auf Wunsch auch einen Abfragebefehl aus, sofern einer hinterlegt wurde, und wartet auf ein gültiges Ergebnis. Wird kein Ergebnis zurückgegeben, ist dies das Zeichen für eine Fehlfunktion.

In der Rubrik Netzwerk/Internet kann ServerInspector eine Prüfung von FTP, HTTP/HTTPS, IMAP, Ping, POP3, SMTP und SNMP vornehmen, weiterhin eine Portüberwachung durchführen und eine komplette E-Mail-Route testen. Bei Letzterem verschickt das Tool eine Testmail per SMTP, prüft dann wahlweise den Eingang im Postfach per POP3 oder IMAP und löscht die Nachricht optional

nach erfolgreicher Übertragung. Weniger umfangreich ist der FTP-Check, der aus einem einfachen Verbindungstest besteht. Bei der SNMP-Prüfung können Objekt-IDs auf ihren Inhalt hin abgefragt werden.

Umfangreicher ist wiederum die HTTP/HTTPS-Prüfung. Hier testet ServerInspector auf jeden Fall die Verfügbarkeit der Webseite, überprüft aber optional noch den Inhalt dahingehend, ob ein bestimmter Text enthalten ist, beziehungsweise als Ausschluss, dass ein bestimmter Text nicht enthalten sein darf. Sollte die Webseite eine Authentisierung verlangen, so kann das Tool auch damit umgehen. Im Fall einer E-Mailbenachrichtigung wird auf Wunsch gleich ein Screenshot mitgeschickt, so dass der Administrator das Prüfergebnis auch optisch kontrollieren kann.

Übrigens lassen sich die Überwachungen in dieser Rubrik nicht nur auf eigene Server anwenden, sondern auch unabhängig davon. Logischerweise lässt sich eine E-Mail-Route ebenso prüfen, wenn Server und Postfach bei einem Provider im Internet liegen. Um zu sehen, wie gut die HTTP-Prüfung funktioniert, trugen wir unsere eigene Webseite www.it-administrator.de ein und prüften auf einige typische Worte auf dieser Seite, was problemlos klappte.



Bild 5: Umfangreiche Eingabemasken helfen bei der Definition genauer Prüfaufträge



Liefertermin:
Ende März 2012

Bestellen Sie jetzt das IT-Administrator Sonderheft I/2012!

180 Seiten Praxis-Know-how rund um das Thema

Exchange 2010 Migration, Betrieb und Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft I/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/



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

☐ **Ja**, ich bin IT-Administrator Abonnent mit der Abonummer (falls zur Hand) _____ und bestelle das IT-Administrator Sonderheft I/2012 zum **Abonnenten-Vorzugspreis** von nur **€ 24,90** inkl. Versand und 7% MwSt.

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____

BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

So erreichen Sie unseren Vertrieb, Abo- und Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252

leserservice@it-administrator.de

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



Heinemann Verlag

Leopoldstraße 85

D-80802 München

Tel: 089-4445408-0

Fax: 089-4445408-99

Geschäftsführung:

Anne Kathrin Heinemann

Matthias Heinemann

Amtsgericht München HRB 151585

ITA 0112



Bei den betriebssystemnahen Überwachungen kennt ServerInspector die Arten CPU, Datei, Dienst, Drucker, Event-Log, Laufwerk, Prozess, RAM, Verzeichnis und Kommandozeilenprogramm-Ausgabe. Bei einer Dateiprüfung kann es je nach Vorgabe zu einem Alarm kommen, wenn eine Datei existiert, nicht existiert, der Inhalt geändert wurde oder bestimmte Zeichenketten enthalten sind. Die Event-Log-Überwachung sucht in den verschiedenen Logs gezielt nach bestimmten Einträgen, auf Wunsch auch nur nach den Ereignissen, die im Laufe der letzten Minuten aufgetreten sind.

Recht detailliert ist auch die Verzeichnisprüfung auf Inhalt, Alter, Anzahl oder Größe der Dateien. Für einen Test richteten wir eine Prüfung auf Dateianzahl ein und bekamen prompt eine Nachricht, als wir Dateien hineinkopierten und die vorgegebene Menge überschritten wurde. Auf Wunsch werden übrigens auch Unterverzeichnisse mit durchsucht. Bei der Laufwerksüberwachung prüft ServerInspector auf freien Platz. Allerdings ist für jedes Laufwerk die Regel einzeln einzutragen und es lässt sich kein prozentualer, sondern nur ein absoluter Wert vorgeben.

In der Rubrik "Sonstiges" findet sich die Möglichkeit, für Prüfungen Skripte in C# und VB.Net aufzurufen. Weiterhin ist, sofern ein entsprechender Sensor angeschlossen ist, eine Prüfung auf maximale Temperatur und Luftfeuchtigkeit möglich. Dies geschieht mit einem USB-Sensor, der bei OptCon erhältlich ist.

Wie schon erwähnt, haben wir einige Überwachungen im Test eingerichtet, was durchwegs gut und schnell klappte. Allerdings fiel uns auf, dass das Einrichten von vielen Überwachungen doch recht zeitintensiv ist. So besitzt ServerInspector keinerlei Gruppierungsfunktion oder die Möglichkeit, so etwas wie Standard-Sets

anzulegen, um beispielsweise bei allen überwachten Servern die CPU-Last, RAM-Belegung und freie Plattenkapazität zu prüfen. Vielmehr ist jeder Eintrag einzeln vorzunehmen. Hier wäre es aus unserer Sicht sinnvoll, zusätzliche Funktionen einzubauen, die die Verwaltung bei vielen Überwachungen vereinfacht. Eine Nachfrage beim Hersteller ergab, dass eine derartige Erweiterung bereits in Planung ist. Auch lassen sich die überwachten Server in der Ansicht nicht gruppieren, sondern sie erscheinen alphabetisch geordnet als lange Liste.

Passende Reaktionen auf Ereignisse

Bei der Beschreibung der Überwachungsaufträge haben wir das Register "Aktion" noch nicht angesprochen. Dahinter verbirgt sich die Möglichkeit von ServerInspector, bei der Überwachung nicht nur mit Benachrichtigungen zu reagieren, sondern auch eigenständig eine Aktion zu starten, um ein Problem wenn möglich in Eigenregie ohne Eingriff des Administrators zu beheben.

Verfügbar sind sechs Aktionen: "Dienst", "Programm ausführen", "VB Script ausführen", "Computer neu starten oder herunterfahren", "Event Log Eintrag" und "URL aufrufen". Die Bezeichnungen sind schon fast selbst erklärend. So kann ein Dienst wahlweise gestoppt, gestartet oder neu gestartet werden. Handelt es sich um einen Dienst auf einem entfernten System, so können die notwendigen Anmeldeparameter mit eingetragen werden.

Weiterhin lässt sich ein Programm aufrufen, wobei die Routine optional vorher prüft, ob der Prozess nicht schon



Bild 6: Die HTTP-Überwachung prüft nicht nur die Erreichbarkeit einer Webseite, sondern auf Wunsch auch den Inhalt anhand einer Textstelle

läuft, um mehrfache Ausführungen zu vermeiden. Über die Option "Event Log Eintrag" ergänzt ServerInspector einen Ereignis-Log-Eintrag, wobei der Administrator genau vorgeben kann, in welches Log (Anwendungen, Sicherheit, System) und welcher Event-Typ es sein soll inklusive eines eigenen Textes, einer Event-ID, -Quelle und -Kategorie.

Reporting mit Historie

Für ein Reporting schreibt ServerInspector alle Vorfälle und deren Dauer in eine Datenbank. Standardmäßig handelt es sich hier um eine lokale Jet-Datenbank. Der Hersteller empfiehlt aus Performancegründen bei mehr als 30 Überwachungen die Verwendung einer SQL-Datenbank (MS SQL oder MySQL).

Ein Report-Assistent bereitet den Inhalt auf und ermöglicht die Ausgabe von Detailberichten oder Zusammenfassungen. Der Administrator muss dazu den gewünschten Zeitraum eingeben und kann einzelne Überwachungen herausgreifen oder alle selektieren. Allerdings ist das Auswahlfenster mit nur acht Zeilen etwas klein geraten. Bei vielen gleichzeitigen Überwachungen erschwert das eine gezielte Auswahl. Das Ergebnis wird wahlweise als HTML- oder TXT-Datei ausgegeben.

Windows XP, Vista, 7, Windows Server 2003/2008 (R2), 32 und 64 Bit, .Net Framework 2.0 oder höher

Systemvoraussetzungen



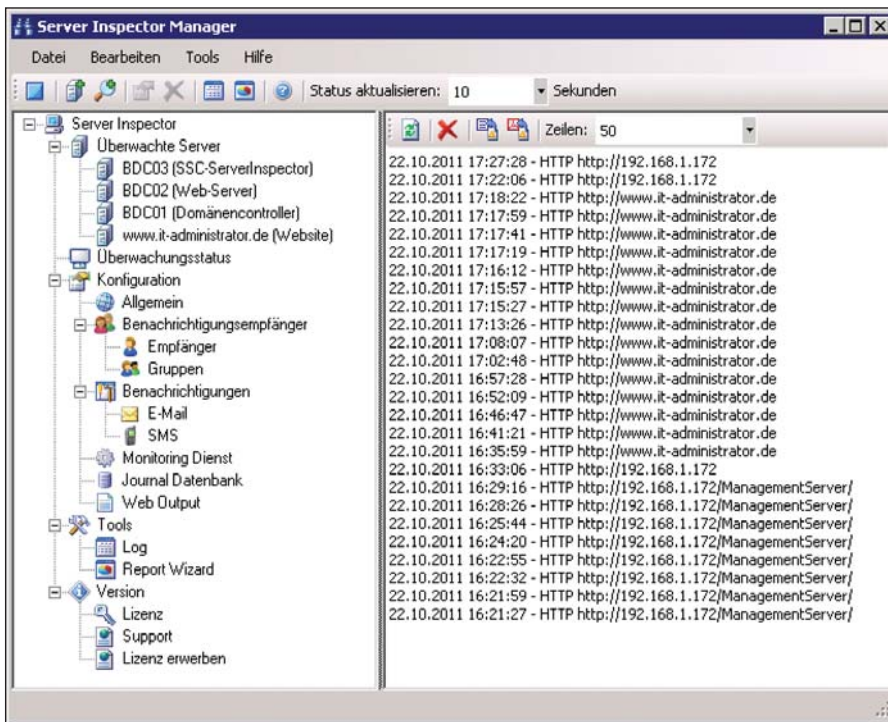


Bild 7: Die Konsole liefert unter anderem eine chronologische Liste aller fehlerhaften Überwachungen

Weiterhin gibt es in der Konsolenansicht ein fortlaufendes Log aller Fehler mit Datum, Uhrzeit und Überwachungsart, das sich wahlweise in eine TXT- oder PDF-Datei exportieren lässt. Sofern nur der aktuelle Status interessiert und nicht die Vergangenheit, kann der Administrator die bereits erwähnte Komplettübersicht über den Überwachungstatus in der Konsole oder die aktuellen Auswertungen im HTML- und XML-Format nutzen.

Fazit

Der SSC-ServerInspector beweist, dass es problemlos möglich ist, mit einfachen Mitteln eine praxisnahe Software zur Server- und Netzwerküberwachung bereitzustellen, die sich mit wenig Aufwand einrichten lässt und praktisch sofort einsetzbar ist. Gefallen hat uns die übersichtliche, intuitive Bedienung, so dass für den Basisbetrieb keine umfangreiche Einarbeitung erforderlich ist. Erst wenn mit eigenen Skripten gearbeitet werden soll, steigt der Aufwand. Von Vorteil ist, dass typische Überwachungsaufgaben bereits vorbereitet und nur die entsprechenden Zielparameter einzugeben sind.

Der größte Nutzen lässt sich unserer Meinung nach daraus ziehen, dass Ser-

verInspector neben einigen Standardüberwachungen in der Lage ist, Verfügbarkeiten auch auf funktionaler Ebene zu prüfen. Dazu kann er beispielsweise explizit testen, ob eine Datenbankabfrage ein Resultat liefert, der Aufruf einer Webseite ein entsprechendes Ergebnis und ob der Mailversand sowie -empfang zu einer Gegenstelle tatsächlich funktionieren.

Durch die Scripting-Möglichkeit lassen sich auch komplexe individuelle Anforderungen abdecken. Gut ist, dass neben Benachrichtigungen per E-Mail und SMS auch Aktionen gestartet werden können, um die Fehlfunktion möglichst in Eigenregie zu beseitigen.

Der Test hat allerdings ebenso gezeigt, dass es noch genügend Optimierungspotential gibt, wenn es darum geht, das Werkzeug in größeren Umgebungen einzusetzen. Hier vermissten wir eine Anbindung der Benutzerverwaltung an das Active Directory sowie die Möglichkeit, den Administrationsaufwand bei häufig benötigten Überwachungsaufgaben durch Gruppierungsmöglichkeiten zu vereinfachen. Noch ist jede Überwachung einzeln einzutragen und zu pflegen. Diesbezüglich sind aber Erweiterungen in Planung, weiterhin sol-

len sich zukünftig auch Linux-Systeme überwachen lassen und es ist neben der Konsole auf dem Server eine Web-GUI zur Bedienung in Entwicklung, um den ServerInspector netzwerkweit konfigurieren zu können. Unserer Meinung nach eignet sich ServerInspector auch als gutes Add-on zu bestehenden Monitoring-Werkzeugen, mit speziellem Fokus auf die funktionalen Prüfungen. Interessierte Administratoren können eine 30-tägige, voll funktionsfähige Trialversion herunterladen. (dr)

Produkt

Programm zur Serverüberwachung und zum Netzwerkmonitoring.

Hersteller

SSC Software Solution Creators
www.ssc-software.com

Preis

ServerInspector kostet pro Installation 690 Euro, pro überwachtem Client sind 150 Euro zu bezahlen. Hinsichtlich der Clients gibt es Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Benutzerverwaltung	5
Serverüberwachung	8
Funktionsprüfung	9
Benachrichtigung	7
Reporting	8

Dieses Produkt eignet sich

optimal für sehr kleine bis hin zu mittelgroßen Umgebungen sowohl zur Überwachung der Server als auch der Kommunikation im Netzwerk.

bedingt für große Umgebungen, da es keine AD-Integration für die Benutzerverwaltung gibt und keine Gruppierungsmöglichkeiten für die zu überwachenden Systeme. Bei vielen Systemen und Überwachungen wird das Tool unserer Meinung nach unübersichtlich.

nicht für Umgebungen, die nicht auf Windows aufsetzen. Die Überwachung von Linux-Systemen ist aber in Arbeit.

SSC-ServerInspector

**Im Test: Blue Coat Web Security Cloud Service**

Auffangnetz in der Cloud

von Jürgen Heyer



Quelle: 123RF

Um die gesamte Bandbreite des Bedarfs abzudecken und für jeden Geldbeutel etwas bereitzustellen, bietet Blue Coat neben den Hardware-Appliances neuerdings einen Cloud-basierten Web-Security-Dienst mit der Produktbezeichnung "Blue Coat Cloud Service Web Security Module" an. Der Dienst basiert auf dem "Threatpulse Security Service". Für einen Administrator entfällt hier ein Teil des Aufwands, da er sich nicht mehr um die Hardware kümmern muss, sondern nur noch um die Regeldefinition. Statt hoher Investitionskosten am Anfang für die Anschaffung ist jährlich auf Benutzerbasis für den Dienst zu zahlen.

Deutlich einfacher wird es für den Administrator auch bei der Berücksichtigung von Außenstellen und Heimarbeitsplätzen. Indem sich deren Datenverkehr recht einfach über den Dienst leiten lässt, wird alles auf gleichem Niveau abgesichert. Dem Administrator reicht dabei stets eine zentrale Konsole,

um alle Webaktivitäten der Nutzer zu steuern und zu beobachten. Der angebotene Dienst beinhaltet fünf funktionale Bereiche: Malware Scanning, Policy Management, Content Filtering, Reporting und Web 2.0 Application Controls.

Vier Betriebsarten zur Auswahl

Der Cloud Service ist flexibel einsetzbar in Organisationen unterschiedlicher Größe, wobei er sich leicht an die Gegebenheiten anpassen lässt. Dazu unterstützt der Dienst vier Arten der Anbindung. Die erste ist IPsec-VPN, wobei der Datenverkehr transparent von einer Firewall zum Cloud Service weitergeleitet wird. Dazu ist die Firewall so zu konfigurieren, dass sie den gesamten Verkehr ins Internet über die Ports 80 und 443 über eine Site-to-Site-VPN-Verbindung zum Threatpulse Web Security Service weiterleitet. Die Verschlüsselung auf diesem Weg erfolgt über 256 Bit AES. Während der Konfiguration wird ein Shared Key definiert. Über einen Connector Agenten zum Active Directory ist es möglich, die Datenströme den Anwendern zuzuordnen. Die Konfiguration

in Verbindung mit verbreiteten Firewall-Typen (Check Point, Cisco 1941, Cisco ASA, Juniper SSG20) ist im Handbuch eingehend beschrieben.

Die zweite Variante nennt sich Proxy Chaining oder Proxy Forwarding und kommt dann in Frage, wenn im Unternehmen bereits ein Secure Gateway Proxy, ein Squid oder ein ISA-Server vorhanden ist. Auch hier finden sich im Handbuch detaillierte Konfigurationsbeschreibungen für die ProxySG Appliance, Forefront TMG und den Microsoft ISA Server. Eine optionale Identifizierung der Datenströme nach Benutzern ist auch hier durch Installation eines Connector-Agenten zum Active Directory möglich.

Die dritte Möglichkeit nennt sich Explicit Proxy und basiert darauf, dass der Standort unter einer festen IP-Adresse erreichbar ist, die beim Cloud Service einzutragen ist. Auf der Benutzerseite ist im Webbrowser ein Proxy zu konfigurieren.

Die dritte Möglichkeit nennt sich Explicit Proxy und basiert darauf, dass der Standort unter einer festen IP-Adresse erreichbar ist, die beim Cloud Service einzutragen ist. Auf der Benutzerseite ist im Webbrowser ein Proxy zu konfigurieren.

Client Connector: Windows XP SP3 (32 Bit), Windows Vista (32 Bit) und Windows 7 (32 oder 64 Bit), Mac OS X 10.6 (Snow Leopard), 10.7 (Lion)

Systemvoraussetzungen

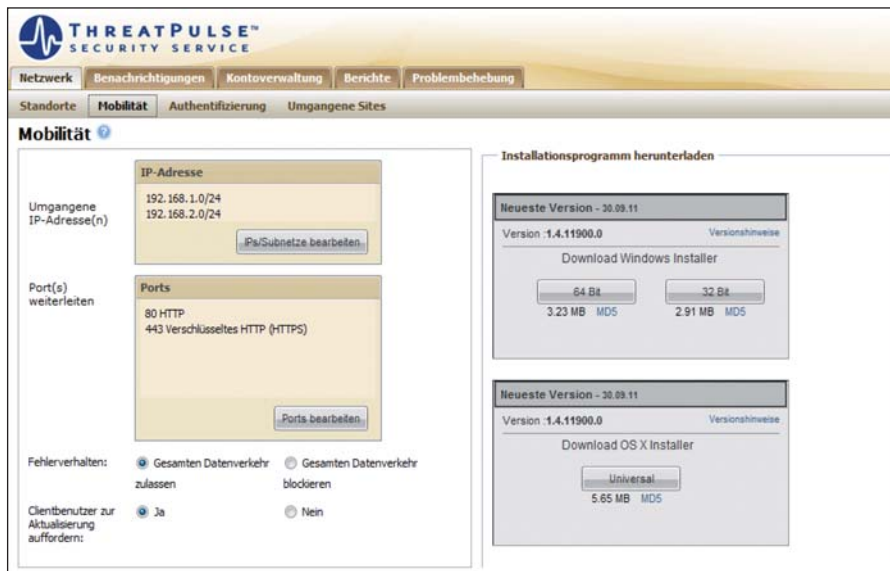


Bild 1: Der mobile Client wird auf einer Webseite konfiguriert und lässt sich dort herunterladen

rieren, der Einfachheit halber mittels Link auf eine PAC-Datei (Proxy Auto-Config). Hierzu ist im Handbuch genau beschrieben, wie die verbreiteten Browser zu konfigurieren sind. Letztendlich gestaltet sich dies in allen Fällen sehr einfach, da nur an einer Stelle die URL zur PAC-Datei einzutragen ist. Zu beachten ist allerdings, dass diese Methode primär für Demonstrationszwecke und für Standorte ohne Anforderung an eine granulare Filterung gedacht ist, da keine Benutzer- und gruppenbasierten Policies unterstützt werden.

Die vierte und letzte Variante ist für mobile Endgeräte gedacht und basiert auf einem Client Connector, einem kleinen Agenten, der die Daten zum Cloud Service weiterleitet. Dieser wird in der Administrationskonsole zum Download bereitgestellt und ist so vorbereitet, dass bei dessen Installation keine weiteren Abfragen zu beantworten sind. Es ist aber möglich, bei einer Kommandozeilen-basierten Installation ein Passwort mitzugeben, ohne dessen Eingabe sich der Agent nicht wieder deinstallieren lässt. Auch erkennt der Agent, wenn jemand versucht, einen anderen Proxy zu nutzen, um die Schutzmechanismen zu umgehen und verweigert dann den Zugriff. Dies lässt sich im Rahmen der Installation bei Bedarf deaktivieren. Für den Test haben wir mit den beiden letzten Varianten gearbeitet und den Zugang für mehrere Systeme konfiguriert.

Konfiguration der Standorte und mobilen Clients

Um den Cloud Service überhaupt nutzen zu können, ist zuerst auf einer Webseite ein Account mit Credentials anzulegen. Darüber erfolgt dann die Anmeldung auf einer web-basierten Benutzeroberfläche als Administrationskonsole. Über eine Erstkonfiguration erfolgt unter anderem die Festlegung der Sprache, wodurch die GUI weitgehend angepasst wird. Sie ist inhaltlich in die Bereiche "Dienst" und "Lösungen" geteilt, wobei beide durch unterschiedliche Farbschema (braun und blau) gut identifizierbar sind. Im Bereich "Dienst" findet die gesamte Grundkonfiguration des Cloud Service statt. So kann der Administrator hier noch weitere Benutzer hinzufügen, wahlweise ebenfalls als Administrator oder nur als Berichtsbenu- tzer, der das Reporting nutzen kann. Hinsichtlich des Abrufs von Berichten lassen sich wiederum Filtergruppen bilden, so

dass nicht jeder Berichtsbenu- tzer alle Auswertungen einsehen kann.

Der wohl wichtigste Konfigurationsschritt ist das Eintragen des eigenen Standorts mit der IP-Adresse und Auswahl einer der genannten Zugriffsmethoden (Explicit Proxy, Firewall/VPN, Proxy Forwarding). Bei Nutzung der Firewall- und VPN-Methode ist ergänzend noch ein Authentifizierungsschlüssel anzugeben. Der Client Connector für mobile Geräte ist unabhängig von der gewählten Methode zusätzlich nutzbar.

Sofern es im Unternehmen Subnetze gibt, deren Datenverkehr nicht vom Threatpulse-Dienst geprüft werden soll – so genannte umgangene IPs/Subnetze –, lassen sich diese hinterlegen. Um eine Zuordnung des Datenverkehrs zu Benutzern durchführen zu können, wird eine Anbindung an das Active Directory unterstützt. Hierzu kann über eine Webseite ein sogenannter Auth Connector heruntergeladen werden. Sobald ein Benutzer versucht, eine Seite oder einen Dienst aufzurufen, der gesperrt ist, sieht er stattdessen eine Hinweisseite, deren Design der Administrator festlegen kann. Dabei erhält der Anwender einen Grund für die Sperre und optional auch Informationen zum Helpdesk, an den er sich bei Rückfragen wenden kann.

Zusätzliche Konfigurationsschritte sind für den Client Connector notwendig. Dieser ist bei mobilen Systemen zu verwenden, die von einer Lokation ohne feste IP-Adresse kommen. Dies sind in der Regel Notebooks im Außendienst sowie PCs im Home Office, können aber auch Arbeits-



Bild 2: Damit der interne Netzverkehr nicht fälschlicherweise zum Threatpulse-Service geschickt wird, lassen sich einzelne IP-Adressen und Subnetze ausklammern



plätze in sehr kleinen Außenstellen mit einfachem DSL-Anschluss sein. Standardmäßig wird der Verkehr über die Ports 80 und 443 zum Threatpulse Server geleitet, es lassen sich aber noch weitere Ports eintragen. Auch kann der Administrator festlegen, wie sich der Client verhält, sollte der Dienst einmal nicht verfügbar sein. Entweder wird dann der Datenverkehr ungeprüft weitergegeben oder komplett gesperrt. Weiterhin lässt sich festlegen, ob die Anwender zum Update aufgefordert werden, wenn Blue Coat eine neue Client-Version bereitstellt, oder nicht.

Sofern beispielsweise ein Notebook sowohl in einem beliebigen Netz als auch innerhalb einer bereits durch eine der drei anderen Optionen geschützten Site betrieben wird, schaltet sich der Client innerhalb der Site in einen passiven Modus. Blue Coat nennt diese Erkennung "Location Awareness". Eine zweite Prüfung, die "Tamper Protection", verhindert, dass Anwender den Schutz des Connectors umgehen können, indem sie einen nicht überprüften Port für die Kommunikation verwenden. Letzteres lässt sich allerdings bei der Clientinstallation deaktivieren, da es Konstellationen geben kann, in denen einem Anwender die Änderung der Proxy-Einstellungen gestattet sein soll.

Individuelles Filtern des Datenverkehrs

Der Bereich "Lösungen" in der Web-GUI beschäftigt sich mit der eigentlichen Nutzung der Funktionen des Cloud Ser-

vices. Er ist wiederum in die vier Rubriken "Übersicht", "Inhaltsfilterung", "Schutz vor Bedrohungen" und "Einstellungen für Webanwendungen" unterteilt. Jede Rubrik hat nochmals drei Unterrubriken "Dashboard", "Berichtszentrale" und "Richtlinie". Beim ersten Durchklicken fühlten wir uns geradezu erschlagen angesichts der vielen bereits angebotenen Berichte und Einstellmöglichkeiten. Insofern empfiehlt es sich, mit Systematik an die individuelle Parametrisierung heranzugehen. Immerhin kommt der Cloud Service mit Standardeinstellungen und kann ohne weitere Anpassung in diesem Bereich sofort genutzt werden. So ist das Malware Scanning etwa grundsätzlich aktiviert.

Für eine weitergehende individuelle Konfiguration sind zuerst die jeweiligen Richtlinien-Unterrubriken von Interesse. So kann der Administrator bei der Inhaltsfilterung gezielt zugelassene Quellen und Ziele sowie blockierte Ziele einzeln eingeben. Während sich dies aber als mitunter arbeitsintensiv erweist, bietet sich die Möglichkeit an, nach Kategorien zu filtern. Die Unterteilung erfolgt in 82 Kategorien in den Gruppen "Business", "Legalität", "Unproduktiv" und "Sicherheit". Einige Kategorien wie Kinderpornografie, Phishing oder Spam sind grundsätzlich gesperrt, für einige weitere ist eine Sperre vorgegeben, die der Administrator jedoch entfernen kann. Wie gut das funktioniert, ließ sich im Test leicht prüfen: Nach Sperren der Kategorie "Pornografie" funk-

tierte beispielsweise der Zugriff auf die Playboy-Seite nicht mehr und nach Sperren von "Alkohol" konnten wir nicht mehr auf die Webseiten bekannter Spirituosenhersteller zugreifen.

Wem die einfache Inhaltsfilterung nicht reicht, kann in die fortgeschrittene Konfiguration wechseln und individuelle Regeln definieren. Dies ist nicht nur global möglich, sondern auch auf Benutzergruppen bezogen, die über den bereits erwähnten Connector aus dem AD importiert wurden.

Bei den Einstellungen für Webanwendungen (Web 2.0) findet der Administrator eine Vielzahl an verbreiteten Angeboten (unter anderem Facebook, Gmail, Windows Live Messenger, YouTube, Flickr, Digg und Amazon Cloud Drive) in mehreren Rubriken vor. Im Gegensatz zur Inhaltsfilterung, die übrigens Vorrang hat, können die Anwendungen nicht nur komplett erlaubt oder gesperrt, sondern auch funktional beschränkt werden. So kann der Administrator wohl das Lesen per E-Mail zulassen, aber den Up- und Download von Anhängen sperren. Gerade bei den sozialen Netzwerken geht es besonders granular zu – bei Facebook etwa mit dem Erlauben oder Beschränken von Games, Post Messages, Chat sowie dem Hochladen von Attachments, Videos und Bildern. Möglich ist auch eine zeitabhängige Steuerung, um den Mitarbeitern beispielsweise in der Mittagspause gewisse Dienste zu erlauben, die während der restlichen Arbeitszeit blockiert sind. Statt hier beim Greifen einer Regel nur den erwähnten Hinweis einzublenden, kann der Administrator den Anwender auch gezielt auf eine Seite im Intranet umleiten, wo er beispielsweise die Unternehmensvorgaben zur Internetnutzung nachlesen kann. Als weiteres Feature unterstützt der Cloud Service für die großen Suchmaschinen eine sichere Suche (Safe Search), also das Ausfiltern von Links zu Seiten mit nicht jugendfreien Inhalten. Die Suche nach bestimmten Begriffen wie "Porno" liefert dann keine oder nur entsprechend gefilterte Ergebnisse.

Bei genauerer Betrachtung der unterstützten Webanwendungen fiel uns im Test auf,

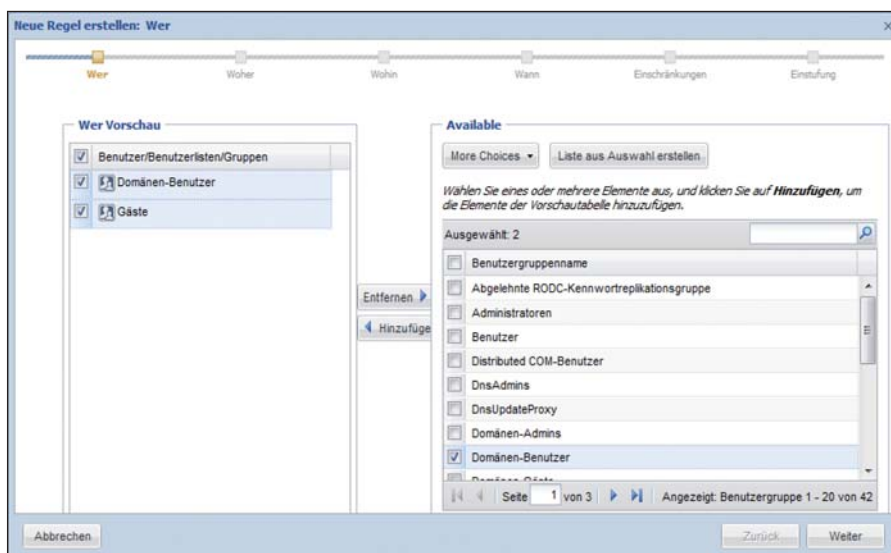


Bild 3: Beim Erstellen neuer Regeln ist eine Filterung auch nach AD-Gruppen möglich



Bild 4: Versucht ein Anwender einen Zugriff auf eine verbotene Seite, sieht er einen Sperrhinweis mit kurzer Begründung und optional mit Helpdesk-Kontakt

dass abgesehen von den weltweit agierenden sozialen Netzwerken und den Suchmaschinen der Fokus mehr auf in den USA verbreiteten Diensten lag, etwa bei den Webmail-Anbietern Yahoo, Hotmail, Gmail, Comcast Mail oder AOL Mail. Auf Nachfrage beim Hersteller erfuhren wir jedoch, dass einige für den deutschsprachigen

Raum relevante Applikationen wie Web.de, GMX, Vkontakte, Xing, studiVZ und meinVZ zum Testzeitpunkt kurz vor der Umsetzung stünden.

Von der prinzipiellen Vorgehensweise her ist es am besten, zuerst über die Inhaltsfilterung kategoriebasierte Sperren zu aktivieren und anschließend gezielte Freigaben, gegebenenfalls auch abteilungsbezogen, einzurichten, so dass beispielsweise nur die Abteilungen für Presse und Marketing YouTube-Videos hochladen dürfen.

Zum Test konfigurierten wir unter anderem eine Konstellation, bei der wir über die Inhaltsfilterung die Nutzung von Suchmaschinen untersagten, dann

aber Google, Yahoo sowie Bing erlaubten und wiederum die sichere Suche aktivierten. Derartige Szenarien lassen sich mit wenigen Eingaben realisieren und bei einer korrekten Konfiguration haben die Anwender praktisch keine Möglichkeit, auszuweichen.

Hinsichtlich der Performance machten wir übrigens nur gute Erfahrungen im Test. So waren bei den Webzugriffen trotz der Umleitung des Datenverkehrs über den Cloud Service inklusive der dortigen Analyse keine störenden Verzögerungen festzustellen.

Berichte in Hülle und Fülle

In jeder der genannten Rubriken ist bereits eine Vielzahl an Berichten vorbereitet. Weiterhin lassen sich sehr detaillierte eigene Berichte definieren und mit entsprechenden Filtern nach Zeit, IP-Adressen, Gruppen und Benutzern versehen. Berichte können im Archiv gespeichert oder per E-Mail verschickt werden. Außerdem lässt sich die Berichtserstellung mittels Zeitplaner au-

WHD.global 2012

20. – 23. März 2012

Europa-Park Rust

Das größte Hosting-Event der Welt – Jetzt anmelden!

WHD 2012
Get connected!

IT-Administrator ist Mediapartner
der WHD.global 2012.
Kostenlose Teilnahme für Leser:
Promo Code: MX14IN89
www.worldhostingdays.com



tomatisieren. Insgesamt haben uns die Möglichkeiten hier sehr gut gefallen und es lassen sich erfreulich einfach aussagekräftige Reports mit Zahlen und Grafiken erstellen. Indem auch die Reportdefinitionen gespeichert werden, sind die Berichte jederzeit erneut erstell- beziehungsweise abrufbar.

Neben der Berichtserstellung kann der Administrator für jede Rubrik die dazugehörige Dashboard-Seite inhaltlich weitgehend frei gestalten. Alle Seiten sind bereits gefüllt und lassen sich beliebig anpassen. Sie enthalten in so genannten Portlets ebenfalls Berichte mit der Ergebnisdarstellung als Raster, Diagramm oder beides. Die Anordnung erfolgt in drei Spalten und die einzelnen Portlets lassen sich mit einem Klick auf- und zuklappen. Indem der Administrator auf den Dashboard-Seiten die für ihn wichtigsten Informationen zusammenfasst, bekommt er mit wenigen Klicks einen schnellen Überblick über den Gesamtstatus. Insgesamt macht die Darstellung einen sehr ausgereiften Eindruck.

Als ausgesprochen übersichtlich erweisen sich übrigens auch die Online-Handbücher. Zeichnungen stellen die möglichen Verbindungen sowie Beziehungen anschaulich dar und praxisnahe Beispiele zeigen, wie sich diverse Konfigurationsanforderungen am besten umsetzen lassen.

Fazit

Der Blue Coat Cloud Service ist unserer Meinung nach vor allem für kleinere Firmen und Unternehmen mit vielen Außenstellen eine interessante Alternative zum Betrieb eigener Web Security Appliances. Blue Coat rundet hiermit sein Angebotsportfolio nach unten hin ab. Der Dienst übernimmt das Malware Scanning, erlaubt eine Inhaltsfilterung durch Sperren von Webseiten oder bestimmten Inhalten und ermöglicht die Kontrolle moderner Web 2.0-Applikationen (Soziale Netzwerke, Webmail und sichere Websuche).

Die Lösung lässt sich problemlos in unterschiedliche Umgebungen mit bereits vorhandenen Firewalls und Proxies integrieren. Interessant erscheint uns hier auch der zusätzliche Client Connector für ein Roaming (Zugriff von einer Lokation mit beliebiger IP-Adresse), der es beispielsweise erlaubt, dass auch Nutzer von unterwegs sowie aus dem Home Office den gleichen Schutz genießen wie beim Webzugriff innerhalb der Firma.

Von Vorteil ist, dass sich die Lösung problemlos an veränderte Nutzerzahlen anpassen lässt – was auch hilft, die Kosten zu begrenzen. Der Administrator muss sich in erster Linie mit der Definition der gewünschten Regeln beschäftigen, wird aber von der Beaufsichtigung der

Hardware entlastet. Übrigens ist auch eine Kombination möglich, indem der Firmenstandort mit einer Hardware-Lösung geschützt wird und der Cloud Service nur für mobile Nutzer sowie beim Zugriff aus dem Home Office oder einer sehr kleinen Außenstelle zum Einsatz kommt. Interessierte Administratoren können einen Account beantragen und den Dienst 30 Tage lang testen. (dr) 

Produkt

Online-Dienst für Web-Security.

Hersteller

Blue Coat
www.bluecoat.com

Preis

Je nach Anzahl der Abonnenten jährlich zwischen 20 und 50 US-Dollar pro Benutzer.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleinere Firmen und Unternehmen mit vielen Außenstellen oder Mitarbeitern im Home Office, um alle über einen zentralen Dienst für Web Security auf gleichem Niveau absichern zu können.

bedingt für mittlere und größere Unternehmen mit wenigen Standorten. Hier ist eine Abschätzung erforderlich, ob nicht der Betrieb eigener Web Security Appliances interessanter ist oder ob sich eine Kombination mit einer eigenen Appliance am Firmensitz und Nutzung des Cloud Service für mobile Anwender empfiehlt.

nicht für Unternehmen, die bereits eigene Web Security Appliances betreiben und keine mobilen Nutzer schützen müssen.

Blue Coat Web Security Cloud Service

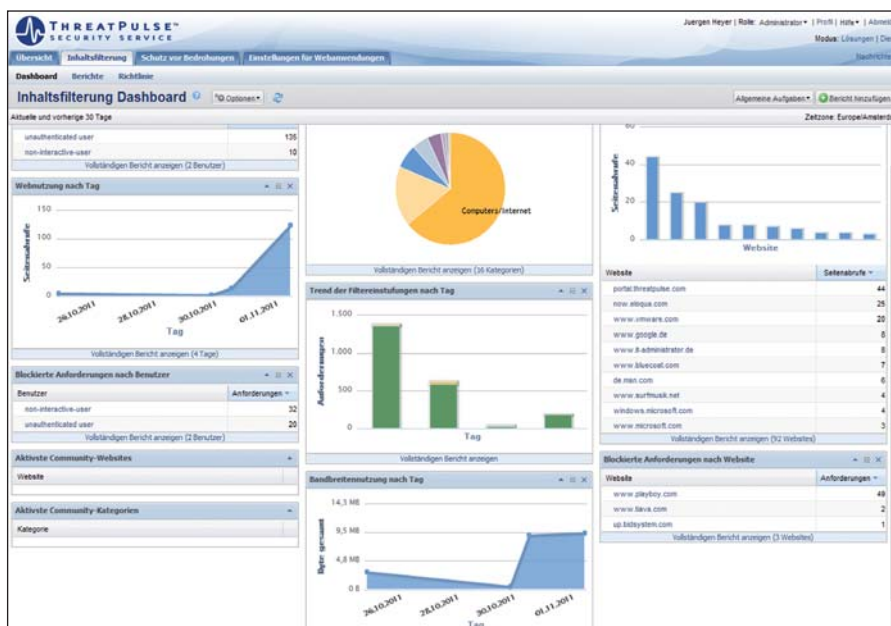


Bild 5: Die Inhalte der Dashboard-Ansichten lassen sich frei anhand der verfügbaren Berichte zusammenstellen und enthalten die Informationen wahlweise als Grafik sowie als Liste

Training Windows Server Best-Practice

München, 21. März/16. April 2012 – Hamburg, 15. Mai 2012



Themen des Trainings:



Active Directory: So läuft's rund. Praxis aus 12 Jahren

- Active Directory und DNS - Virtuelle DCs
- Replikation - Sicherheit - Lieblingsfehler
- Ausblick: Neuerungen im Active Directory unter Windows Server 8



Wiederbelebung: Disaster Recovery für das Active Directory

- Was kann denn kaputtgehen?
- Backup-Methoden: Was geht und was nicht?
- Restore ist mehr als Backup: Praxisdemos



Hyper-V sicher und sauber

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

Referent: Nils Kaczinski

Termin: 21. März 2012 (Achtung nur noch Restplätze!)
16. April 2012 (Zusatztermin)

Ort: ExperTech Training Center München,
Wredestr. 11, 80335 München

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 7. März 2012 bzw.
2. April 2012 (Zusatztermin)

Termin: 15. Mai 2012

Ort: ExperTech Training Center Hamburg,
Esplanade 6, 20354 Hamburg

Uhrzeit: 10.00 bis ca. 17.30 Uhr

Anmeldeschluss: 2. Mai 2012

Trainings-Partner:



EXPERTeach

Teilnahmegebühren:

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

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





Ereignisprotokolle von Windows-Servern erfassen und auswerten Auf dem Laufenden

von Thomas Joos



Es gibt zahlreiche kostenlose Möglichkeiten, die Ereignisanzeigen und Protokolle der Server an zentraler Stelle zu erfassen und zu analysieren. Zunächst bietet Windows Server 2008 mit sogenannten Abonnements die Möglichkeit, Ereignisse von Servern im Netzwerk einzusammeln. Darüber hinaus gibt es Freeware-Tools, die ebenfalls Ereignisse in den Protokollen von Windows-Servern erfassen und Administratoren zentral zur Verfügung stellen. Wie Sie den Überblick über Ihre Logdateien behalten und welche Werkzeuge Ihnen weiterhelfen, erfahren Sie in diesem Workshop.

Windows Server 2008 R2 kann bereits mit Bordmitteln die Ereignisanzeigen verschiedener Server im Netzwerk zusammentragen und anzeigen. Diese Funktion trägt die Bezeichnung "Abonnements" und lässt sich direkt in der Ereignisanzeige einrichten. Basis ist der Windows-Ereignissammeldienst. Dieser muss auf dem Server gestartet sein, der die verschiedenen Ereignisse sammeln soll, sowie auf allen beteiligten Servern. Damit die Sammlung von Ereignisanzeigen funktioniert, müssen Sie die beteiligten Computer vorbereiten, das Abonnement erstellen und dann in der Ereignisanzeige die Fehler der entsprechenden Server anzeigen.

Log-Sammlung in Ereignisanzeige einrichten

Die Sammlung von Ereignisanzeigen basiert auf zwei Grundlagen. Es gibt einen Server, der die Daten sammelt (Sammlungsserver), und Server, die an diesem Sammlungsserver angebunden sind (Quellcomputer). Die Sammlung von Ereignisanzeigen führen Sie am besten auf Servern durch, die in einer gemeinsamen Active Directory-Gesamtstruktur positioniert sind. Im ersten Schritt müssen Sie die Remoteverwaltung auf den einzelnen

Servern aktivieren. Dazu führen Sie auf jedem Quellcomputer und dem Sammlungscomputer in einer Befehlszeile mit Administratorrechten (über das Kontextmenü gestartet) den Befehl `winrm quickconfig` aus. Im nächsten Schritt geben Sie noch den Befehl `wecutil qc` ein. Das Tool konfiguriert das Weiterleiten von Ereignissen über das Netzwerk zu einem Sammlungscomputer. Nehmen Sie anschließend das Computerkonto des Sammlungscomputers, auf dem Sie die Ereignisse aller angebundenen Server anzeigen wollen, in die lokalen Administratorgruppen der einzelnen Server auf. Die lokale Benutzerverwaltung starten Sie am schnellsten durch die Eingabe von `lusrmgr.msc` im Suchfeld des Startmenüs. Rufen Sie die Eigenschaften der lokalen Administratorgruppe auf und klicken Sie auf "Objekttypen", um auch Computerkonten in die Gruppe aufzunehmen.

Möchten Sie Ereignisabonnements in Arbeitsgruppen erstellen, müssen Sie manuell eine Ausnahme für die Windows-Firewall für "Remote-Ereignisprotokollverwaltung" auf jedem Quellcomputer hinzufügen. Das Konto, mit dem Sie die Ereignisse auf den Quellcomputer sammeln, hinterlegen Sie

anschließend bei der Einrichtung des Abonnements. Zusätzlich geben Sie auf dem Sammlungscomputer den Befehl

```
winrm set winrm/config/client
@{TrustedHosts="Alle Quellcomputer, durch Komma getrennt"}
```

ein. Die Sammlung nehmen Sie am besten mit einem Konto vor, das über Administratorrechte in der Domäne verfügt. Möchten Sie ein eigenes Konto dafür anlegen, müssen Sie dieses in die lokale Administratorgruppe auf allen Quellcomputern aufnehmen. Normalerweise reicht es aus, wenn nur das Computerkonto des Sammlungscomputers Mitglied der Administratorgruppe auf den Quellcomputern ist.

Erstellen eines neuen Abonnements

Haben Sie alle Vorbereitungen getroffen, starten Sie auf dem Sammlungscomputer die Ereignisanzeige und klicken auf "Abonnements". Ist der Systemdienst "Windows-Ereignissammlungsdienst" nicht gestartet, erhalten Sie eine entsprechende Meldung. Lassen Sie in diesem Fall den Dienst starten. Anschließend klicken Sie mit der rechten Maustaste auf "Abonnements" und



```

Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>winrm quickconfig
WinRM ist bereits zum Empfangen von Anforderungen auf diesen Computer konfiguriert.
WinRM wurde nicht für Verwaltungsremotenzugriff auf diesen Computer konfiguriert.
Folgende Änderungen müssen durchgeführt werden:
Erstellen Sie einen WinRM-Listener auf HTTP://*, um die WS-Verwaltungsanforderungen an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Aktivieren Sie die WinRM-Firewallausnahme.
Diese Änderungen durchführen [y/n]? y
WinRM wurde für die Remoteverwaltung aktualisiert.
Auf HTTP://* wurde ein WinRM-Listener erstellt, um die WS-Verwaltungsanforderungen an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Die WinRM-Firewallausnahme ist aktiviert.
C:\Windows\system32>wevtutil qc
Der Startmodus für den Dienst wird in den Modus für verzögerten Start geändert.
Möchten Sie den Vorgang fortsetzen (J- ja oder N- nein)? j
Der Windows-Ereignissammeldienst wurde erfolgreich konfiguriert.
C:\Windows\system32>_

```

Bild 1: Konfigurieren der Remoteverwaltung und des Windows-Ereignissammeldienstes in Windows Server 2008 R2

dann auf "Abonnement erstellen". Klicken Sie im Menü "Aktionen" auf "Abonnement erstellen". Im neuen Fenster konfigurieren Sie jetzt das Abonnement. Bei "Abonnementname" geben Sie einen Namen ein. Sie haben auch die Möglichkeit, eine Beschreibung einzugeben. Bei "Zielprotokoll" wählen Sie schließlich aus, wo auf dem Sammlungsserver die Ereignisse der Quellcomputer gesammelt werden sollen. Standardmäßig ist hier das Protokoll "Weitergeleitete Ereignisse" ausgewählt.

Anschließend bestimmen Sie die Art des Abonnements. Wählen Sie hier "Sammlungsinitiiert" und dann "Computer auswählen". Anschließend legen Sie die Quellcomputer fest, die das Abonnement erfassen soll. Sie sollten für jeden Computer, den Sie hinzufügen, die Schaltfläche "Testen" anklicken, um sicherzustellen, dass der Sammlungscomputer eine Verbindung aufbauen kann.

Über die Schaltfläche "Ereignisse auswählen" legen Sie nun neue Filter an, über die Sie festlegen, welche Ereignisse auf den Quellcomputern der Sammlungscomputer anzeigen soll. Grundsätzlich wählen Sie aus, welche Ereignisse von welchen Protokollen erfasst werden sollen. Haben Sie den Filter erstellt, klicken Sie auf "OK". Bevor Sie weitere Einstellungen vornehmen, klicken Sie erneut auf "OK", um das Abonnement zu überprüfen. Nach der Erstellung muss das Abonnement als "Aktiv" gekennzeichnet sein. Auf diesem Weg erstellen Sie auch mehrere Abonnements, die verschiedene Computer mit verschiedenen

Abfragefiltern erfassen. Mit einem Doppelklick auf das Abonnement passen Sie dieses jederzeit wieder an.

Anschließend können Sie die Ereignisse im ausgewählten Protokoll anzeigen. Haben Sie das Standardprotokoll "Weitergeleitete Ereignisse" ausgewählt, finden Sie dieses im Bereich "Windows-Protokolle". Bis die ersten Ereignisse eintreffen, kann es allerdings eine Weile dauern. Von welchem Server die Ereignisse stammen, sehen Sie in der Spalte "Computer".

Erweiterte Einstellungen für Abonnements

Neben den Standardeinstellungen für Abonnements können Sie über die Schaltfläche "Erweitert" in den Eigenschaften des Abonnements einige Einstellungen ändern. Sie legen an dieser Stelle zum Beispiel fest, dass die Abfrage der Ereignisse nicht durch das Computerkonto des Servers erfolgt, sondern mit einem speziellen Benutzerkonto, dessen Daten Sie in den erweiterten Einstellungen des Abonnements hinterlegen. Achten Sie aber darauf, dieses Konto in die lokale Administratorengruppe der Quellcomputer aufzunehmen. Außerdem können Sie in den erweiterten Einstellungen festlegen, wie der Sammlungscomputer die Daten abrufen soll. Hier stehen die drei Optionen "Normal", "Bandbreite minimieren" und "Wartezeit minimieren" zur Verfügung.

Bei der Standardeinstellung "Normal" verwendet das Abonnement den Pull-Zustellmodus. Dabei fasst das Abo immer fünf

Elemente zusammen und überträgt diese vom entsprechenden Quellcomputer auf den Sammlungsserver. Die Option "Bandbreite minimieren" begrenzt die Bandbreite, die dem Abo zur Verfügung steht. "Wartezeit minimieren" stellt dagegen sicher, dass Ereignisse möglichst schnell auf dem Sammlungsserver zur Verfügung stehen. In den erweiterten Einstellungen legen Sie auch den Port und die Übertragungsart fest. Wenn Sie diese ändern, müssen Sie in den Firewall-Einstellungen der Quellcomputer ebenfalls entsprechende Regeln definieren. In Active Directory-Umgebungen können Sie dazu auch Gruppenrichtlinien verwenden, um Regeln auf den Servern zu erstellen.

Ereignisprotokolle im Netzwerk verwenden

Neben den Abonnements können Sie natürlich auch mit der Standard-Ereignisanzeige problemlos Ereignisanzeigen von Computern im Netzwerk abrufen. Verwenden Sie dazu die Ereignisanzeige selbst oder das Befehlszeilentool "wevtutil", um Ereignisprotokolle auf einem Remotecomputer zu verwalten. Starten Sie die Ereignisanzeige und klicken Sie mit der rechten Maustaste auf "Ereignisanzeige (Lokal)". Anschließend öffnen Sie durch Auswahl von "Verbindung mit einem anderen Computer herstellen" die Ereignisanzeige beliebiger Server. Möchten Sie auf diesem Weg eine Verbindung mit mehreren Servern aufbauen, müssen Sie eine neue Managementkonsole erstellen und das Snap-In der Ereignisanzeige mehrmals integrieren. Möchten Sie eine Verbindung mit einem anderen Benutzerkonto aufbauen, aktivieren Sie noch die Option "Verbindung unter anderem Benutzerkonto herstellen" und wählen das entsprechende Konto aus. Sie können nun Benutzernamen und Kennwort für die Verbindung festlegen.

Sie können die Ereignisanzeige eines Servers auch direkt durch Eingabe des folgenden Befehls öffnen:

```
eventvwr Computername
```

Zudem bauen Sie in der Befehlszeile eine Verbindung zur Ereignisanzeige eines anderen Servers auf, indem Sie den Befehl

wevtutil Option **/r:Computername**
/u:Benutzername /p:Kennwort

eingeben. Verwenden Sie die Optionen “/u” und “/p” nicht, verbindet Sie wevtutil mit dem Benutzer, mit dem Sie angemeldet sind. Welche Optionen zur Verfügung stehen, sehen Sie bei der Eingabe von *wevtutil*. Das Tool dient nicht dazu, die Ereignisanzeige über das Netzwerk zu öffnen, sondern Einstellungen vorzunehmen oder das Protokoll zu löschen. Mit *wevtutil el /r:sbs.contoso.local* lassen Sie sich zum Beispiel alle verfügbaren Protokolle auf dem Remotecomputer anzeigen. Sie können mit wevtutil auch Ereignisanzeigen ohne Rücksprache löschen lassen. Dazu verwenden Sie den Befehl *wevtutil cl Name des Protokolls*. Der Befehl *wevtutil cl System /r:sbs* löscht zum Beispiel das System-Protokoll auf dem Server “SBS” ohne weitere Rücksprache. Natürlich können Sie mit dem Tool auch Protokolle über das Netzwerk auf den lokalen Computer in *.evtx-Dateien exportieren. Dazu verwenden Sie den Befehl *wevtutil epl*.

Andere Windows-Protokolle überprüfen

Neben der Ereignisanzeige bietet Windows Server 2008 R2 noch verschiedene Protokolle auf Textbasis an, zum Beispiel von den Internetinformationsdiensten (IIS) sowie Routing- und RAS-Diensten. Die meisten Dateien tragen die Endung .log. Viele Logdateien befinden sich in den Verzeichnissen %Systemroot%\Debug, %Systemroot%\System32\Config und %Systemroot%\System32. Die Logdateien von

IIS finden Sie im Inetpub-Verzeichnis. Im Debug-Verzeichnis befinden sich etwa die Logdateien *depro.mou.log* und *depro.mou.log*, die während der Heraufstufung zum Domänencontroller erzeugt werden.

Viele Serverprodukte erstellen zudem eigene Protokolle, so zum Beispiel SharePoint und Exchange. Um deren Inhalte zu überprüfen, öffnen Sie die Protokolle direkt. Bricht zum Beispiel bei SharePoint 2010 die Installation mit einem Fehler ab, sollten Sie die Logdateien mit der Bezeichnung “PSCDiagnostics” im Verzeichnis *C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS* überprüfen. Hier finden Sie verschiedene Protokolldateien, die auf den Fehler hinweisen können. Öffnen Sie solche Logdateien mit dem Windows-Editor und suchen Sie nach “Warnung” sowie “Error” oder verwenden Sie Zusatztools. Da die Logdateien von SharePoint extrem umfangreich sind, bietet es sich in diesem Fall an, für das Öffnen nicht den Windows-Editor zu verwenden, sondern spezielle Tools, die Logdateien besser auslesen können. Microsoft stellt etwa über das MSDN die Freeware ULSViewer [1] als EXE-Datei zur Verfügung. Sie müssen es daher nicht installieren. Starten Sie das Tool und öffnen Sie die entsprechenden Logdateien. Anschließend sehen Sie die Spalten in einer Tabelle sortiert, wodurch



Bild 3: Ein erfolgreich erstelltes Abonnement taucht in der Ereignisanzeige auf

sich die Überprüfung und Fehlersuche wesentlich effizienter gestaltet. Außerdem können Sie mehrere Protokolldateien parallel öffnen. Das Tool zeigt jede Datei in einer eigenen Registerkarte an.

Sie können in den Protokolldateien Fehler filtern oder leichter nach Inhalten suchen. ULS-

Viewer funktioniert auf 32 Bit-Computern genauso wie auf 64 Bit-Rechnern, auch unter Windows 7 und Windows Server 2008 R2. Treten bereits während der Installation Fehler auf, starten Sie den Windows-Explorer und geben als Verzeichnis %temp% ein. Es öffnet sich das Temp-Verzeichnis des Benutzerkontos, mit dem Sie SharePoint installiert haben. Die Logdateien der Installation finden Sie im Verzeichnis 1 oder 2 des Temp-Verzeichnisses. Dort finden Sie die Datei *SharePoint Server Setup Zeitstempel.log*. In ihr sehen Sie eventuelle Fehler, nach denen Sie im Internet suchen können. In den meisten Fällen finden Sie so die Lösung. Führen Sie eine Installation über die PowerShell durch, finden Sie im Verzeichnis %COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\LOGS Protokolldateien mit der Bezeichnung *PowerShell_ConfigurationDiagnostics.log*.

Auch Exchange führt solche Dateien. In manchen Situationen bricht die Installation von Servern ab oder es gibt Probleme bei der Installation von Patches. Die Installationsroutine von Exchange Server 2010 führt eine eigene Logdatei, in der alle Informationen der Installation gespeichert sind. Diese Datei trägt die Bezeichnung *ExchangeSetup.log* und befindet sich im Verzeichnis *C:\ExchangeSetupLogs*. In ihr werden alle Informationen abgelegt, die während der Installation oder bei der Aktualisierung durch Patches anfallen. Untersuchen Sie Probleme während der Installation von Exchange Server 2010 oder der Installation von Patches, sollten Sie diese Datei nutzen, da sie mehr Informationen enthält, nach denen Sie auch im Internet suchen können, wenn Probleme auftreten. Kommt es während der Installation zu Problemen, haben Sie die größte Chance, in dieser Logdatei den Fehler zu finden. In der Datei *Exchange-*

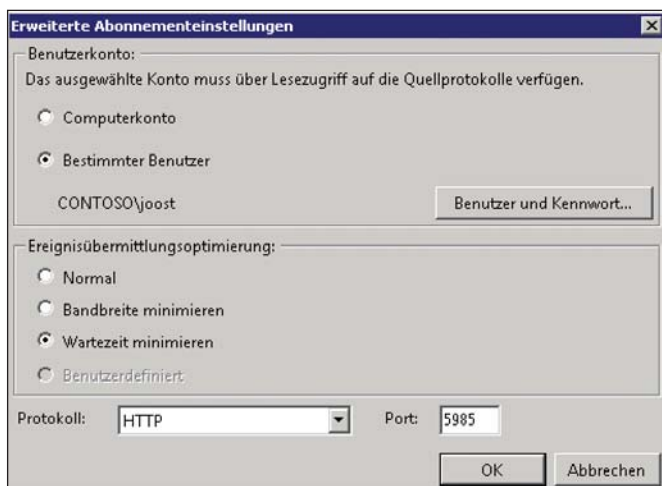


Bild 2: Die erweiterten Einstellungen für Abonnements erlauben die Auswahl zwischen “Bandbreite minimieren” und “Wartezeit minimieren”



Setup.msilog sind die Informationen gespeichert, die der Windows Installer während der Extraktion der Exchange Server-Installationsdateien protokolliert.

Sie können diese Datei auch während der Installation aufrufen, wenn Sie das Gefühl haben, dass die Installation einer Rolle zu lange dauert. Tritt ein Fehler während der Installation auf, wartet das Setup-Programm häufig nach verschiedenen Intervallen und hält den Fehler auch in der Logdatei fest. So können Sie bereits nach dem Fehler suchen, während Exchange noch versucht den Server zu installieren. Entsprechende Fehler sehen Sie dann am Ende der Datei.

Über die Nachrichtenverfolgung in Exchange Server 2010 haben Sie die Möglichkeit, sich die zugestellten E-Mails und deren Informationen anzeigen zu lassen. Die Nachrichtenverfolgung greift auf Logdateien zu, in denen das Versenden und der interne Transport der Nachrichten protokolliert sind. Diese Dateien finden Sie auf Hub-Transport-, Edge-Transport- und Mailboxservern im Verzeichnis `C:\Programme\Microsoft\Exchange Server\14\TransportRoles\Logs\MessageTracking`. Die Bezeichnung der Protokolldateien ist auf Servern mit unterschiedlichen Exchange-Rollen unterschiedlich. Auf Hub-Transport- und Edge-Transport-Servern sind die Protokolldateien nach dem Format "MSGTRKyyyyymmdd.log" bezeichnet, auf Mailboxservern nach dem Format "MSGTRKMyyyyyymmdd.log".

Hat eine Protokolldatei ihre maximale Größe erreicht, wird eine neue mit fortlaufender Nummerierung angelegt. Abgespeichert sind die Protokolldateien im Textformat, die einzelnen Werte durch Komma voneinander getrennt (CSV). Im Protokoll ist nicht der Text der E-Mails gespeichert, sondern nur der Betreff und der Zeitpunkt des Sendens und der Zustellung sowie weitere Informationen. Bei Exchange Server 2010 ist die Nachrichtenverfolgung auf allen Servern mit den Rollen Hub-Transport, Edge-Transport und Mailbox bereits standardmäßig aktiviert. Sie finden die Einstellungen der Nachrichtenverfolgung in den Eigenschaften des Servers in der Exchange-Verwaltungskonsolle. Klicken Sie auf "Serverkonfiguration / Hub-Transport"

Time	Server	Process	Thread	Product	Category	EventID	Level	Correlation	Message
03.09.2010 16:15:32.09	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Health	8tu6	High		Registering the
03.09.2010 16:15:32.57	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Monito...	b4ly	High		Leaving Monito
03.09.2010 16:15:32.87	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:32.87	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Health	8tu6	High		Registering the
03.09.2010 16:15:33.34	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Monito...	b4ly	High		Leaving Monito
03.09.2010 16:15:33.71	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:33.71	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Health	8tu6	High		Registering the
03.09.2010 16:15:34.29	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Monito...	b4ly	High		Leaving Monito
03.09.2010 16:15:34.67	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.70	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.70	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Monito...	b4ly	High		Leaving Monito
03.09.2010 16:15:34.70	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Monito...	b4ly	High		Leaving Monito
03.09.2010 16:15:34.70	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.70	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.73	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.78	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.78	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:34.79	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE
03.09.2010 16:15:35.01	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Upgrade	tbv7	Medium		[psconfig] [SF
03.09.2010 16:15:35.01	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Upgrade	tbv7	Medium		[psconfig] [SF
03.09.2010 16:15:35.01	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Upgrade	tbv7	Medium		[psconfig] [SF
03.09.2010 16:15:36.20	SPS...	PSConfigUI.exe [0x09...	0x060C	Share...	Topolo...	8xq2	Medium		Updating SPPE

Bild 4: Protokolldateien zeigt ULSViewer übersichtlicher an

und rufen Sie die Eigenschaften des Servers auf. Auf der Registerkarte "Protokolleinstellungen" finden Sie die Konfiguration der Nachrichtenverfolgung.

Echtzeitüberwachung mit EventSentry

Bei EventSentry [2] handelt es sich um eine Monitoring-Software zur Erfassung, Analyse und Anzeige von Systemereignissen. Um auch unterwegs auf dem Laufenden zu bleiben, besteht die Möglichkeit, Informationen per E-Mail zu versenden, wenn bestimmte Ereignismeldungen in den Protokollen der Server auftauchen. In der E-Mail ist die auslösende Ereignismeldung mit allen Daten enthalten. Eine Lizenz der Anwendung kostet 85 US-Dollar. Es gibt auch eine komplett kostenlose, aber etwas eingeschränkte Light-Variante von EventSentry. Diese kann ebenfalls Ereignisanzeigen überwachen und E-Mails versenden, aber nicht so umfassend laufende Dienste überwachen oder Protokolldateien auf Servern. Die genauen Unterschiede finden Sie auf der Seite des Herstellers unter [3]. In vielen Fällen reichen die Funktionen der kostenlosen Light-Edition aber aus.

Der größte Vorteil von EventSentry liegt darin, dass Sie die Ereignisanzeigen aller Ih-

rer Server in Echtzeit überwachen können. Abhängig von Fehlermeldungen, die in den verschiedenen Ereignisanzeigen auftreten, lassen sich Aktionen durchführen, zum Beispiel E-Mails an Administratoren verschicken, die den Inhalt der Ereignismeldung enthalten. Mit diesem Tool erkennen Sie somit Fehler und drohende Ausfälle in Ihrem Netzwerk relativ früh. Zur Überwachung installieren Sie auf den zu überwachenden Servern das Tool mit den entsprechenden Agenten zur Überwachung. Auf einem Computer im Netzwerk installieren Sie die Verwaltungsoberfläche, auf jedem Server, den Sie überwachen wollen, den entsprechenden Agenten. Die entsprechende Auswahl nehmen Sie im Setup-Assistenten vor. Nach dem Start erscheint ein Agent, der Sie bei der Einrichtung der Anwendung unterstützt.

Im Rahmen der Einrichtung legen Sie fest, auf welche Arten von Ereignissen in den Ereignisanzeigen das Tool achten soll. In der Verwaltungsoberfläche können Sie direkt die Ereignisanzeigen "Application", "Security" und "System" auf dem angeordneten Server öffnen. Im Bereich "Packages / Event Log Packages / Default" bestimmen Sie, welche Ereignisse das Tool auf den Servern überwachen soll, auf denen der Agent installiert ist. Auf diesem Weg



können Sie auch gezielt nach einzelnen IDs oder nach Ereignisquellen filtern lassen. Im Bereich "Actions" wählen Sie aus, welche Aufgaben das Tool durchführen soll, wenn Ereignisse auftreten, die den konfigurierten Filtern entsprechen. Die einzelnen Aktionen wiederum, zum Beispiel die Konfiguration der Warn-E-Mails, nehmen Sie im Bereich "Actions" im linken Bereich der Verwaltungsoberfläche vor. Nach der Einrichtung sollten Sie eine Test-E-Mail versenden lassen, um sicherzustellen, dass der E-Mailfluss funktioniert. Nach der Installation blendet EventSentry auch ein Informationsfenster ein, sobald ein Fehler auf dem Server auftaucht.

Ereignisanzeigen mit PsLoglist sammeln

Mit PsLoglist aus der PsTools-Sammlung von Sysinternals [4] können Sie über die Befehlszeile die Ereignisanzeigen verschiedener Computer einsammeln, anzeigen und vergleichen. Rufen Sie das Tool ohne Optionen auf, zeigt PsLoglist alle Einträge des lokalen Systemereignisprotokolls an. Das Programm hat darüber hinaus zahlreiche Optionen [5], welche beim Abfragen der Ereignisanzeigen viele verschiedene Vergleichsmöglichkeiten bieten:

```
psloglist [\Computer[, Computer
[,...]] | @Datei [-u Benutzername
[-p Kennwort]] [-s [-t delimi-
ter]] [-m #|-n #|-h #|-d #|-w]
[-c][-x][-r][-a mm/dd/yy]
[-b mm/dd/yy][-f filter] [-i
ID[,ID[,...]] | -e ID[,ID[,...]]]
[-o event source[,event sour-
ce][,...]] [-q event source[,event
source][,...]] [-l event log file]
Eventlog
```

Geben Sie zum Beispiel den Befehl *psloglist system* ein, listet das Tool in der Befehlszeile alle Ereignisse des Systemereignisprotokolls auf. Der Befehl *psloglist application* zeigt das Anwendungsprotokoll an. Wollen Sie nur die aktuellsten fünf Einträge sehen, verwenden Sie den Befehl *psloglist system -n 5*. Die fünf ältesten Einträge zeigen Sie mit *psloglist system -r -n 5* an.

Um effizient Daten anzuzeigen, sollten Sie die Anzeige filtern, da ansonsten zu

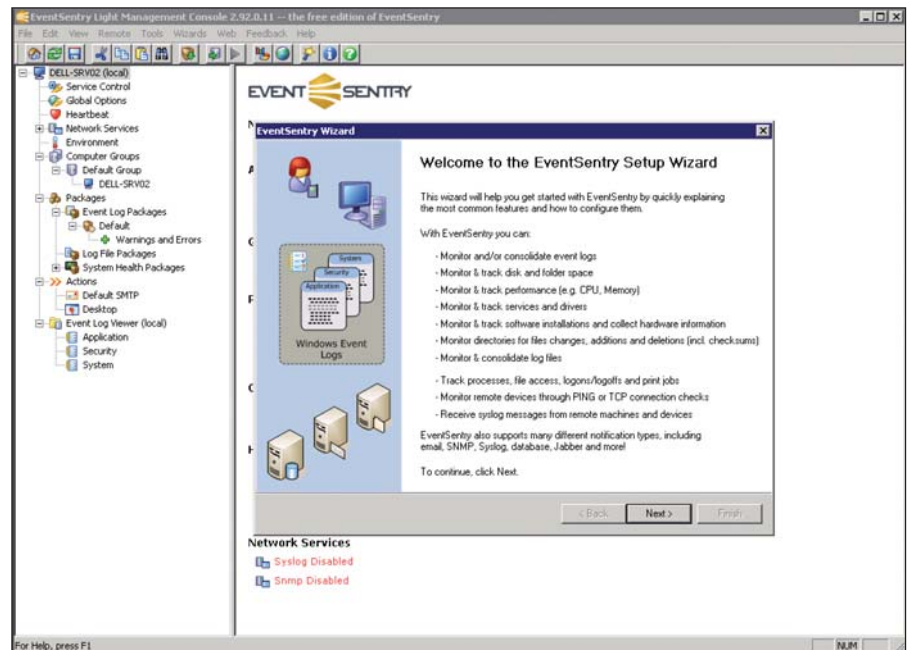


Bild 5: Server lassen sich mit EventSentry zentral überwachen

viele Informationen auf dem Bildschirm erscheinen. Dazu verwenden Sie die Option "-f". Möchten Sie zum Beispiel nur Fehlermeldungen erfassen, geben Sie den Befehl *psloglist system -f e* ein. Fehler und Warnungen erhalten Sie mit der Option "-f ew" angezeigt. Um nur Meldungen einer bestimmten ID anzuzeigen, verwenden Sie "-i", gefolgt von einer kommasetrennten Liste der IDs, die Sie anzeigen wollen. Eine weitere Möglichkeit ist das Exportieren der Ausgabe in eine .evt-Datei, die Sie wiederum mit der Ereignisanzeige in Windows öffnen können. Dazu verwenden Sie zusätzlich die Option "-g .\evt-Datei". Mit PsLoglist lesen Sie auch die Ereignisanzeigen von Computern im Netzwerk aus. Dazu nutzen Sie zunächst die Option *psloglist \Computer* und dann die verschiedenen Optionen des Tools, um die Anzeige zu aktivieren. Dabei gehen Sie genauso vor wie bei der Abfrage lokaler Ereignisanzeigen.

Performance Analysis of Logs

Unter [6] erhalten Sie die Freeware "Performance Analysis of Logs" (PAL), die bei der Auswertung von Leistungsberichten eine gute Hilfe sein kann. Das Tool ist allerdings nur dann geeignet, wenn Sie einen englischen Server betreiben und eine ausführliche Analyse von Logdateien durchführen wollen, die über die normalen Möglichkeiten hinausgeht. Grund-

sätzlich sollten Sie das Tool nur auf Testservern installieren, nicht auf produktiven Servern. Auf der Seite finden Sie die Software und weiterführende Hilfe und Dokumentationen zum Thema Leistungsüberwachung von Servern. Sie benötigen für das Tool zusätzlich noch die ebenfalls frei erhältlichen Zusatzprogramme Log Parser 2.2 [7], Microsoft Chart Controls für Microsoft .NET Framework 3.5 [8] und das Office 2003-Add-In Office Web Components [9]. (dr)

- [1] Microsoft ULSViewer C2P11
- [2] EventSentry C2P12
- [3] EventSentry Light vs. Full C2P13
- [4] Sysinternals C2P14
- [5] PsLoglist-Optionen C2P15
- [6] Freeware Performance Analysis of Logs C2P16
- [7] Log Parser 2.2 C2P17
- [8] Microsoft Chart Controls für Microsoft .NET Framework 3.5 C2P18
- [9] Office Web Components C2P19

Link-Codes



Bleiben Sie in Verbindung!



Folgen Sie uns auf Twitter

twitter.com/ita_blog



Werden Sie ein Fan auf Facebook

www.facebook.de/itanet



Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet



Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

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

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



Protokolle unter Exchange 2007 und 2010

Logs in Reih und Glied

von Christian Weihs

Es handelt sich um einen Klassiker im Support: Ein verzweifelter Mitarbeiter wendet sich an den IT-Service, weil er auf eine dringende, bereits an ihn versandte E-Mail wartet, er diese aber noch nicht erhalten hat. Nun obliegt es dem Exchange-Administrator, schnell Klarheit zu schaffen und festzustellen, was geschehen ist und ob überhaupt ein Problem vorliegt. Dieser Workshop soll die wichtigsten Exchange-Logs vorstellen, um Ihnen Ansatzpunkte für das schnelle Troubleshooting im Umfeld von Microsofts Mailserver an die Hand zu geben.



Quelle: 123RF

ten Zeile taucht die "Version" auf, gefolgt vom "Datum", an dem das Log-File generiert wurde. Exchange ergänzt den Header noch um die Zeile "Logtype", die den Ursprung der Meldung präzisiert (RCA Protocol Logs oder Message Tracking Log). Abgeschlossen wird der Header über die Zeile "Fields", die als Spaltenname zu verstehen ist (date-time, client-ip, client-hostname et cetera). Durch dieses einfache Format lassen sich die Daten sehr gut weiternutzen, egal ob über Excel, Access oder einen SQL-Server.

Protokoll zur Nachrichtenverfolgung

Die erste Anlaufstelle für die Nachrichtenverfolgung ist das Nachrichtenverfolgungsprotokoll. Dieses Übertragungsprotokoll sammelt Informationen darüber, wer wem welche E-Mail gesendet hat und wie diese intern verarbeitet wurde. Dieses Protokoll aktivieren Sie in den Eigenschaften des Servers bei "Serverkonfiguration / HUB-Transport" auf der Registerkarte "Protokolleinstellungen". Alternativ ist dies über die PowerShell mit dem Befehl `Set-Mailboxserver/Set-Transportserver -MessageTrackingLogEnabled $true` möglich. An dieser Stelle definieren Sie auch den Pfad zu den Log-Files.

Parameter anpassen

Die weitere Konfiguration für die maximale Protokollgröße, die maximale Protokolldateigröße sowie das maximale Alter nehmen Sie mit dem Kommando `Set-Mailboxserver/Set-Transportserver` in der PowerShell vor (MessageTrackingLog-MaxDirectorySize, MessageTrackingLog-

Protokolle sind eine der wichtigsten Anlaufstellen, um mögliche Probleme zu identifizieren und diese nachzuvollziehen. Zudem lässt sich mit Hilfe der Log-Dateien erkennen, ob eingeleitete Lösungsversuche Erfolg versprechen und auch in Zukunft einsetzbar sind. Letztendlich sind Protokolle natürlich ein wichtiger Lieferant für Statistiken und Statusinformationen. Bevor wir uns mit den Details der verschiedenen Protokolle auseinandersetzen, wollen wir zunächst einen Überblick über die verschiedenen Logs geben. Denn je nachdem, ob die Nachrichtenübermittlung über einen externen Server per SMTP erfolgt oder ob die Kommunikation eines Clients über RPCoverHTTPS stattfindet, sind die Log-Files an verschiedenen Stellen zu finden. Die entsprechenden Verzeichnisse entnehmen Sie der Tabelle "Speicherpfade der wichtigsten Exchange-Protokolle".

Grundvoraussetzungen schaffen

Wichtig für eine Log-Auswertung ist natürlich, dass die Protokollaufzeichnung auch aktiviert sein muss. Daneben sind immer die Aufbewahrungszeiten und die maximale Größe der Logs zu berücksichtigen – ist die maximale Größe erreicht, werden die ältesten Protokolle überschrieben. Gerade bei Protokollen, die viele Daten mitschreiben, ist das Standard-Limit eventuell innerhalb weniger Stunden erreicht. Eine detaillierte Auswertung ist dann nicht mehr möglich. Es ist also wichtig, eine für das Unternehmen passende Größe zu finden.

Die Protokolle liegen als Text-Datei vor und sind vom Aufbau her nahezu identisch. Die ersten drei Zeilen führen unter "Software" den Ursprung auf (Microsoft Internet Information Services 7.5 oder Microsoft Exchange Server). In der nächs-



Speicherpfade der wichtigsten Exchange-Protokolle

Protokoll	Beschreibung	Standardpfad in Exchange 2007 – Anpassung für 2010 in Klammern
Nachrichtenverfolgung	Verlauf der Nachrichten	\Exchange Server\<V14>\TransportRoles\Logs\MessageTracking
SMTP Send	Überwacht die ausgehende Kommunikation	\Exchange Server\<V14>\TransportRoles\Logs\ProtocolLog\SmtpSend
SMTP Receive	Überwacht die eingehende Kommunikation	\Exchange Server\<V14>\TransportRoles\Logs\ProtocolLog\SmtpReceive
RPC Client Access	Zugriffslog der MAPI-Clients inklusive OAB	nur Exchange 2010: \Exchange Server\Logging\RPC Client Access
Connectivity	Verbindungsüberwachung zwischen Servern, Informationen zur DNS-Auflösung und Verbindungsfehlern	\Exchange Server\<V14>\TransportRoles\Logs\Connectivity
IIS Logs	Überwacht die HTTP/HTTPS-Verbindungen	Server 2003: \Windows\System32\LogFiles\W3SVC1 Server 2008 (R2): \inetpub\Logs\LogFiles\W3SVC1
Agent Logs	Überwacht Ereignisse aus den Anti-Spam-Agents	\Exchange Server\<V14>\TransportRoles\Logs\AgentLog
POP3/IMAP Logs	Protokolliert die Kommunikation über POP3/IMAP	\Exchange Server\Logging\IMAP\POP3

MaxFileSize, MessageTrackingLogMaxAge). Abgelegt werden die Protokolle im Verzeichnis *MessageTracking* unter “Exchange Server\<V14>\TransportRoles\Logs\”. Das Protokoll hält die wichtigsten Informationen zu den einzelnen Schritten bei der Nachrichtenübermittlung fest.

Die Verarbeitung einer E-Mail stellt sich wie folgt dar: Eine Nachricht kommt über den Event “RECEIVE” mit der Quelle “STOREDRIVER” (MAPI-Client) oder über SMTP zum Exchange-Server und wird über den Event “DELIVER” mit der Quelle “STOREDRIVER” im Postfach abgelegt. Sollte es sich um eine intern versandte E-Mail handeln, können Sie das Ablegen der E-Mail in den gesendeten Objekten des Senders über “SUBMIT/ STOREDRIVER” weiter beobachten. Weiterhin ist das Aufbrechen eines Verteilers über “EXPAND” leicht nachzuvollziehen. Eine ausführliche Definition der Felder und ihrer Bedeutung ist in der Tabelle “Felder zur Klassifizierung einzelner Nachrichtenverfolgungsereignisse” zu finden.

Auswertung über Konsole oder Shell

Die Auswertung der Log-Files kann über verschiedene Wege erfolgen. Die erste Anlaufstelle ist die Toolbox der Exchange Management Console (EMC). Dort arbeiten Sie mit einem Assistenten zur Nachrichtenverfolgung (Exchange 2007) beziehungsweise dem Verfolgungsprotokoll-Explorer (Exchange 2010).

Über Kriterien wie Sender, Empfänger, Betreff et cetera grenzen Sie die Nachrichten hier weiter ein. Haben Sie eine E-Mail in der Liste markiert und klicken Sie auf “Weiter”, erweitert sich die Suche auf die Nachrichten-ID. Auf diese Weise lässt sich der Verlauf einer E-Mail gezielt nachvollziehen.

Als zweites Werkzeug bei der Log-Auswertung ist die Exchange Management Shell (EMS) zu nennen. Durch die unzähligen Möglichkeiten der Verknüpfung von Befehlen und das Erstellen ganzer Skripte werden Sie die Logs nach Belieben mit den Filtern von “Get-MessageTrackingLog” aus.

Ein letzter Weg, der speziell für den Anwender eingerichtet wurde, ist in den Optionen von Outlook Web Access (OWA) versteckt. Diese Methode bietet dem Nutzer ab Exchange 2010 die Möglichkeit, selbstständig den Verlauf eigener Mails zu prüfen und nachzu-

vollziehen. Die Daten werden für den Anwender leserfreundlich aufgewertet und auskommentiert.

Das Microsoft Exchange-Team nutzt das Log auf seine eigene Weise und hat das Script “ProcessTrackingLog” veröffentlicht. Dieses übernimmt die Auswertung selbstständig und bereitet die wichtigsten Kennzahlen wie die Anzahl gesendeter E-Mails oder die häufigsten Fehler auf und speichert sie als CSV-Datei.

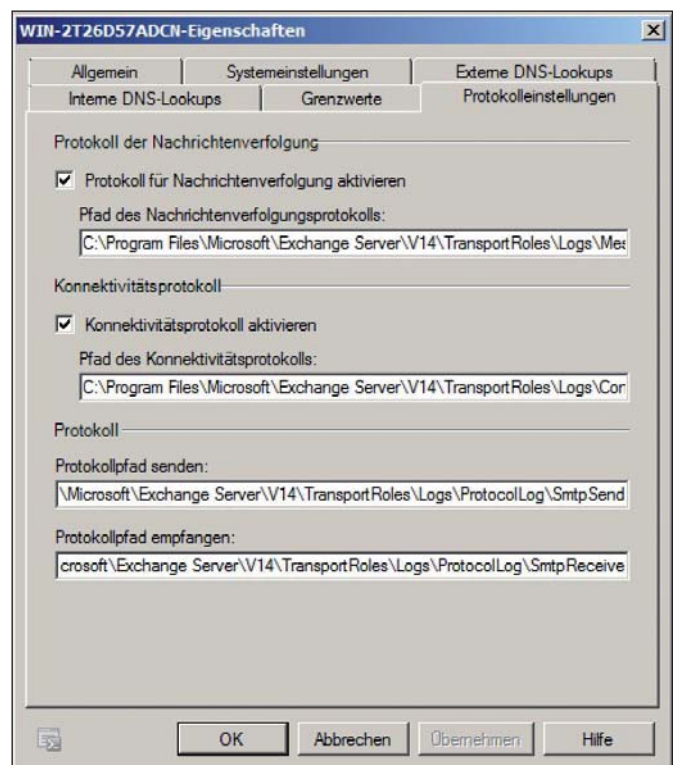


Bild 1: Die Aktivierung des Protokolls zur Nachrichtenverfolgung findet in der Serverkonfiguration statt



Felder zur Klassifizierung einzelner Nachrichtenverfolgungsereignisse

Feld	Beschreibung
date-time	Datum/Uhrzeit des Nachrichtenverfolgungsereignisses im UTC-Format, das im ISO-8601-Format dargestellt wird. Der Wert ist formatiert als yyyy-mm-ddThh:mm:ss.fffZ, mit yyyy = Jahr, mm = Monat, dd = Tag, hh = Stunde, mm = Minute, ss = Sekunde, fff = Bruchteile einer Sekunde und Z = Zulu (eine weitere Möglichkeit zur Angabe von UTC).
client-ip	Die TCP/IP-Adresse des Messagingsservers oder -clients, der die Nachricht übermittelt hat.
client-hostname	Der Name des Messagingsservers oder -clients, der die Nachricht übermittelt hat.
server-ip	Die TCP/IP-Adresse des Exchange-Quellservers oder -Zielservers.
server-hostname	Der Name des Zielservers.
source-context	Zusätzliche Informationen, die zum Quellfeld gehören.
connector-id	Der Name des Sende-Connectors oder Empfangs-Connectors am Quell- oder Zielstandort.
source	Die für das Nachrichtenverfolgungsereignis zuständige Exchange-Transportkomponente. Die möglichen Werte für dieses Feld lauten wie folgt: ADMIN für die Übermittlung durch das Wiedergabeverzeichnis, AGENT, DSN, GATEWAY für die Übermittlung durch fremde Connectoren, PICKUP, ROUTING, SMTP und STOREDRIVER für MAPI-Übermittlung.
event-id	Der Nachrichtenereignistyp. Mögliche Werte sind BADMAIL, DEFER, DELIVER, DSN, EXPAND, FAIL, POISONMESSAGE, RECEIVE, REDIRECT, RESOLVE, SEND, SUBMIT und TRANSFER.
internal-message-id	Eine Nachrichten-ID, die derjenige Exchange 2007-Server zuweist, der die Nachricht aktuell verarbeitet. Der Wert einer bestimmten Nachricht ist im Nachrichtenverfolgungsprotokoll jedes Servercomputers mit Exchange 2007, der an der Zustellung der Nachricht beteiligt ist, unterschiedlich.
Nachrichten-ID	Der Wert des Felds "Message-Id.", das sich in den Kopfzeilenfeldern einer Nachricht befindet. Wenn das Kopfzeilenfeld "Message-Id." nicht vorhanden ist, wird ein beliebiger Wert zugewiesen. Dieser Wert ist für die Lebensdauer der Nachricht konstant.
recipient-address	Die E-Mailadressen der Nachrichtenempfänger. Mehrere E-Mailadressen sind durch ein Semikolon getrennt.
recipient-status	Dieses Feld gibt ein SEND- oder FAIL-Ereignis an.
total-bytes	Die Größe der Nachricht, die Anlagen enthält, in Bytes.
recipient-count	Die Gesamtzahl der Empfänger in der Nachricht.
related-recipient-address	Dieses Feld arbeitet mit EXPAND-, REDIRECT- und RESOLVE-Ereignissen, um die E-Mailadressen weiterer Empfänger anzuzeigen, die dieser Nachricht zugeordnet sind.
reference	Das Feld enthält zusätzliche Informationen für bestimmte Ereignistypen: DSN: Das Feld "reference" enthält den Wert Internet-Message-Id der Nachricht, die die Benachrichtigung über den Übermittlungsstatus verursacht hat. SEND: Das Feld "reference" enthält den Wert Internet-Message-Id einer Benachrichtigung über den Übermittlungsstatus. TRANSFER: Das Feld "reference" enthält den Wert Internet-Message-Id der Nachricht, die verzweigt wird. Für alle anderen Ereignistypen ist das Feld "reference" leer.
message-subject	Der Nachrichtenbetreff aus dem Kopfzeilenfeld "Subject:". Die Nachrichtenbetreffverfolgung wird durch den Parameter <i>MessageTrackingLogSubjectLoggingEnabled</i> im Cmdlet <i>Set-TransportServer</i> (Hub-Transport-Server und Edge-Transport-Server) oder im Cmdlet <i>Set-MailboxServer</i> (Postfachserver) gesteuert. Die Nachrichtenbetreffverfolgung ist in der Standardeinstellung aktiviert. Die Nachrichtenbetreffverfolgung lässt sich deaktivieren, indem der Parameter <i>MessageTrackingLogSubjectLoggingEnabled</i> auf "false" gesetzt wird.
sender-address	Die E-Mailadresse, die im Kopfzeilenfeld "Sender:" oder "From:" angegeben ist (falls "Sender:" nicht vorhanden ist).
return-path	Die E-Mailadresse des Absenders, die unter "MAIL FROM:" im Nachrichtenumschlag angegeben ist. Zwar ist dieses Feld niemals leer, es kann jedoch den Absenderadresswert Null enthalten, der durch <> dargestellt wird.

SMTP-Protokollierung

Erreicht eine E-Mail den Exchange-Server erst gar nicht, müssen Sie die Connectoren und damit die SMTP-Übermittlung näher betrachten. Diese Protokollierung ist allerdings standardmäßig deaktiviert. Schalten Sie sie über die EMC oder mit dem Befehl *Set-SendConnector -ProtocolLoggingLevel Verbose* beziehungsweise mit *Set-ReceiveConnector -ProtocolLoggingLevel Verbose* über die EMS ein. Damit auch dieses Log nicht zu viel Speicherplatz auf der Festplatte belegt, setzen Sie die maximale Größe mit diesem Kommando fest:

```
Set-TransportServer -Identity Exchange-Server -SendProtocolLogMaxDirectorySize 10240MB -ReceiveProtocolLogMaxDirectorySize 10240MB.
```

Das System legt die Protokolle unter der Rolle Hub-Transport im Verzeichnis "\\Exchange Server\[V14]\TransportRoles\Log\ProtocolLog\" ab. Mit Hilfe dieser Protokolle überprüfen Sie die einzelnen Schritte einer Übermittlung. Angefangen von einer Begrüßung über "HELO" beziehungsweise "EHLO", um zu bestimmen, ob Standard-SMTP oder

das erweiterte SMTP (ESMTP) zum Einsatz kommt und ob sich beide Systeme in Startposition befinden, über Empfänger und Sender bis zur Beendigung über "QUIT".

Beim Logging des eingehenden SMTP-Verkehrs ist ferner sehr aufschlussreich, welcher Connector genutzt und mit welchen Rechten die Verbindung ausgestattet wurde. Sie sehen hier zum Beispiel, ob alle Absender (Ms-Exch-SMTP-Accept-Any-Sender) beziehungsweise Empfänger zugelassen sind (Ms-Exch-SMTP-

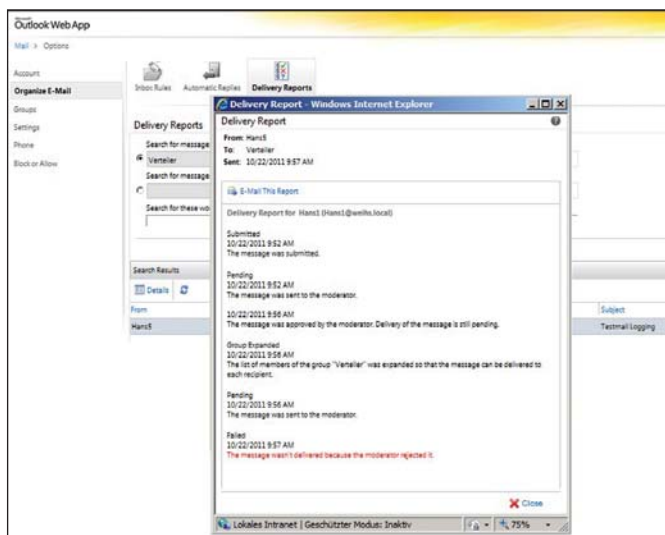


Bild 2: Outlook Web Access versorgt den Nutzer mit einem übersichtlichen Delivery Report

Accept-Any-Recipient) und ob es eventuell zu einer Umgehung des SPAM-Filters kommt (ms-Exch-Bypass-Anti-Spam). Eine Übersicht zum Transportberechtigungsmodell gibt es unter [1]. Die häufigsten SMTP-Statusmeldungen sind unter [2] zu finden. Diese werden über den Unzustellbarkeitsbericht auch an den Sender weitergeleitet und lassen in den meisten Fällen Rückschlüsse auf die Ursache zu, so dass ein Fehler schnell auszumachen ist. Eine Übersicht über die Fehlermeldungen erzeugt zum Beispiel das ProcessTrackingLog (Nachrichtenverfolgungsprotokolle).

Verbindungsprotokoll für abgehende Verbindungen

Ein weiteres Protokoll, das nicht ganz so tief in die SMTP-Übermittlung schaut, aber die ausgehende Übermittlung dennoch im Blick hat, ist das Verbindungsprotokoll. In diesem Log geht es nicht um die Protokollierung einzelner Nachrichten, sondern um die Verbindung zwischen den Servern. Es gibt Aufschluss über die Zielsever, die DNS-Auflösung, Verbindungsfehler sowie über die Anzahl der übertragenen Nachrichten. Das Protokoll lässt sich wie das Nachrichtenverfolgungsprotokoll über die EMC oder die EMS mit *Set-TransportServer* und der Ergänzung *ConnectivityLogEnabled \$true* aktivieren. Das Log ist standardmäßig im Ordner "Exchange Server \ TransportRoles \ Logs \ Connectivity" zu finden.

Diagnoseprotokoll individuell konfigurierbar

Eine weitere wichtige Anlaufstelle ist das Windows EventLog. Exchange schreibt von Hause aus sehr viele Informationen in das Anwendungsprotokoll – manchmal aber nicht genug. Aus diesem Grund gibt es die Möglichkeit, das Logging für bestimmte Exchange-Dienste zu erhöhen, um detailliertere Informationen oder Fehlermeldungen zu erhalten. Aktivieren können Sie es in der EMC am Server in der Serverkonfiguration oder über die Powershell mit dem Befehl *Set-EventLogLevel * -Level high*. Da die Dienste-Namen doch etwas länger sind und mehrere Dienste infrage kommen, empfiehlt es sich, die Ergebnisse einer Suche zu pipen, um das Level gleich hochzusetzen. Mit dem

Bestellen Sie jetzt das IT-Administrator Sonderheft II/2011!



180 Seiten Praxis-Know-how rund um das Thema

SharePoint 2010 für Administratoren

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Mehr Informationen und ein
Onlinebestellformular finden Sie auch hier

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

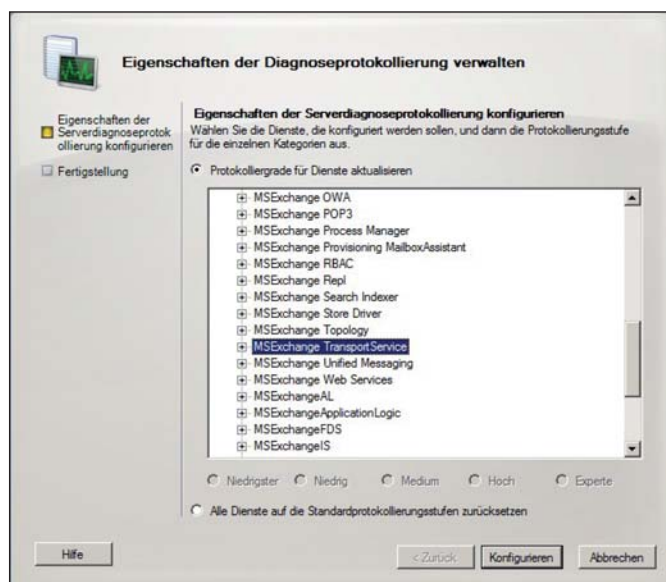


Bild 3: In den Eigenschaften der Diagnoseprotokollierung lässt sich der Protokolliergrad je nach Bedarf festsetzen

folgenden Beispiel erhöhen Sie das Logging für den SMTP-Dienst und Sie kommen zum Beispiel Verbindungsproblemen einfacher auf die Schliche:

```
Get-EventLogLevel *SMTP* | Set-EventLogLevel -Level high
```

Mit der Zeichenfolge

```
Get-EventLogLevel | ft Identity,EventLevel -AutoSize
```

ermitteln Sie die aktuellen Einstellungen aller Dienste mit den dazugehörigen Log-Level. Sollte es in einem Bereich des Servers zu Problemen kommen (OAB-Generierung), erhöhen sie für diesen Bereich das Logging und suchen im EventLog nach weiteren Fehlern. Aufgrund der Vielzahl an Informationen sollten Sie die Diagnoseprotokollierung aber nicht ständig detailliert mitlaufen lassen, sondern nach der Fehlersuche wieder auf ein Minimum stellen. Andernfalls ist Exchange äußerst mitteilungsbedürftig.

Clients und Postfächer überwachen

Seit Exchange 2010 ist die CAS-Rolle auch für den MAPI-Zugriff zentraler Dreh- und Angelpunkt. Um hier den Überblick zu behalten, gibt es das "RPC Client Access"-Log. Dieses ist standardmäßig aktiv und die Protokolle sind im Verzeichnis "Exchange Server \ Logging \

RPC Client Access\" zu finden. Das Aktivieren und Deaktivieren sowie die Konfiguration (Aufbewahrungszeit, Log-Größe) erfolgt über die Datei *Microsoft.Exchange.RpcClientAccess.Service.exe.config* im Bin-Verzeichnis von Exchange. Neben interessanten Informationen zum Client (IP, Benutzername, Version, Cache) werden auch Zugriffe auf andere Postfächer und das Archiv mitgeschritten. Daneben existiert noch ein eigenes Log, das die Zugriffe auf das Outlook-Adressbuch mitschreibt. Dieses liegt im Verzeichnis *Addressbook Service* im Ordner "Exchange Server \ Logging\". Die Konfiguration erfolgt über die Datei *Microsoft.Exchange.RpcClientAccess.Service.exe.config*.

Seitdem Outlook Anywhere und mobile Geräte immer stärkere Verbreitung finden, rückt das IIS-Protokoll zunehmend in den Fokus des Administrators. Sei es, um Problemen beim Zugriff über Outlook oder beim Autodiscover auf den Grund zu gehen oder Verbindungsschwierigkeiten von mobilen Geräten zu analysieren. Das IIS-Protokoll loggt alle Zugriffe auf die virtuellen Exchange-Verzeichnisse. Neben wichtigen Informationen zu Client-IP, Nutzer und Agent (Browser,

Device) lässt sich am Status erkennen, ob der Zugriff erfolgreich war (200) oder ob der Zugriff verweigert wurde (401). Sie konfigurieren und starten das Protokoll über den IIS-Manager.

Spam im Blick dank Agent-Protokollierung

Sofern Sie im Unternehmen die Anti-Spam-Funktion des Exchange-Servers nutzen, ist das Agent-Log interessant. Es nimmt Informationen zu den Verbindungs-, Inhalts-, Empfänger- und Absenderfiltern auf und bietet eine Anlaufstelle, um Ereignisse in diesem Bereich näher zu betrachten. Sie richten das Logging über die Datei *EdgeTransport.exe.config* im Bin-Verzeichnis ein. Hier definieren Sie zudem Größe und Aufbewahrungszeitraum. Abgelegt wird das Protokoll dann im Verzeichnis "Exchange Server \ TransportRoles \ Logs \ Agent-Log". Auch dieses Log können Sie mit einfachen Mitteln weiter auswerten – Exchange bringt hierfür bereits einfache Powershell-Skripte mit. *Get-AntispamFilteringReport.ps1* und *Get-AntispamSCLHistogram.ps1* sind nur zwei Skripte unter vielen, die im Ordner "Exchange Server \ Scripts" zu finden sind und mit *Get-Antispam* beginnen.

IMAP/POP3-Protokollierung

Als letztes Log seien noch die Protokolle für POP3 und IMAP aufgeführt. Oft spielen sie nur noch eine untergeordnete Rolle. Geht es aber um die Auswertung der Kommunikation zwischen Client und Server, sind sie die erste Adresse. In dem Protokoll finden Sie neben Client-IP und Nutzer ausführliche Informationen zur Aktualisierung von Ordnern und

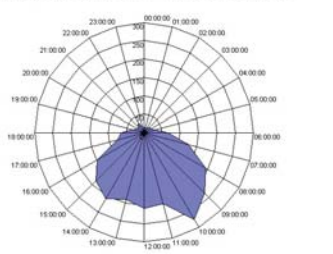


Bild 4: Die IIS-Protokollierung lässt sich im IIS-Manager aktivieren und konfigurieren



```
Logparser "SELECT
QUANTIZE(TO_TIMESTAMP(EXTRACT_PREFIX(TO_STRING(
EXTRACT_SUFFIX([#Fields: date-
time],0,'T')),0,'.'), 'hh:mm:ss'),3600) AS
Hour, COUNT(*) AS Hits INTO radar_traffic2.gif
FROM 'REC\20111206*.log' WHERE event='+' GROUP
BY Hour ORDER BY Hour ASC" -i:CSV -nSkipLines:4
-o:CHART -charttype:RadarLineFilled -charttit-
le:"Eingehende SMTP-Verbindungen"
```

Eingehende SMTP-Verbindungen



Grafische Ausgabe von Logparser



zur Anmeldung, wodurch Sie ein Fehlverhalten schnell lokalisieren können.

Unter Exchange 2007 erfolgt die Konfiguration noch über die Datei *Microsoft.Exchange.Pop3.exe.config* beziehungsweise *Microsoft.Exchange.IMAP4.exe.config* in dem Verzeichnis "Exchange Server \ Clientaccess \ PopImap". An dieser Stelle nehmen Sie die Aktivierung/Deaktivierung genauso wie die Anpassung zur Größe der Logs und zur Aufbewahrungszeit vor. In Exchange 2010 wurde die Konfiguration in die Shell verschoben und die Einrichtung findet über *Set-IMAPSettings* beziehungsweise *Set-POPSettings* statt. Das Cmdlet gab es bereits unter Exchange 2007, die Erweiterungen *ProtocolLogEnable*, *LogFileRollOverSettings* sowie *LogPerFileSizeQuota* und *LogFileLocation* sind aber neu hinzugekommen.

Auswertung der Logs mit Logparser

Bis hierhin haben wir lediglich die verschiedenen Protokolle vorgestellt und erläutert, welche Informationen in welchem Protokoll zu finden sind. Durch die Unmengen an Dateien und enthaltenen Zeilen ist die Auswertung der Log-Files über Notepad und andere Editoren manchmal aber nur schwer möglich. Als Alternative bietet sich das von Microsoft bereitgestellte Tool Logparser an, das Daten aus verschiedensten Quellen (IIS-Logs, EventLog et cetera) analysieren kann. Nach der Installation des Werkzeugs sollten Sie den Pfad zu *Logparser.exe* in den Systemvariablen

hinterlegen, damit sich die Software direkt aus den Logverzeichnissen öffnen lässt.

Logparser nutzt über SELECT, FROM, WHERE, GROUP BY et cetera die SQL-Syntax, weshalb SQL-Grundkenntnisse für die Nutzung hilfreich sind. Über SELECT wählen Sie die einzelnen Felder aus, die zurückgegeben werden sollen. Der Bereich FROM bestimmt das Log. Durch das Datum im Log-Namen schränken Sie die Suche sehr schnell auf einen Zeitraum ein. Eine gezielte Filterung des Logs erfolgt dann im Bereich WHERE.

Neben der reinen Abfrage definieren Sie bei Logparser noch das Ein- und Ausgabeformat. Standardmäßig können Sie das Format CSV für Exchange-Logs nutzen, wobei Sie in diesem Fall die ersten Informationszeilen im Protokoll über *nSkipLines* ausblenden müssen. Handelt es sich um das IIS-Log, kennt Logparser das Format und kann es über IISW3C direkt einbinden. Als Standardausgabe nutzen wir die GUI-Ausgabe über DATAGRID, die etwas übersichtlicher ist als die Anzeige in der Konsole über NAT.

Eine einfache Auflistung sämtlicher Zeilen aus dem IIS-Log ist über Logparser mit folgendem Kommando möglich:

```
"SELECT * FROM *.log" -i:IISW3C
-o:DATAGRID
```

Im Folgenden führen wir zur Verdeutlichung einige Beispielabfragen auf. Die Anzahl der gesendeten E-Mails je Connector beispielsweise im Monat November (SMTP-SendLog) lassen Sie sich mit diesem Befehl anzeigen:

```
Logparser "SELECT Connector-ID,
COUNT(*) AS Total FROM
*201111*.log WHERE DATA LIKE
'Quit' GROUP BY remote-endpoint,
connector-id WITH Rollup" -i:CSV
-nSkipLines:4 -o:DATAGRID
```

Alle fehlerhaften Übermittlungen gibt das Werkzeug mit folgender Zeichenfolge aus (SMTP-SendLog):

```
Logparser "SELECT * FROM *.log WHERE
TO_INT( SUBSTR(DATA,0,3)) > 500
```

```
AND event = '>' -i:CSV -nSkipLi-
nes:4 -o:DATAGRID
```

Die Anzahl der eingehenden Verbindungen pro Host (SMTP-ReceiveLog) bringen Sie mit diesem Befehl auf den Schirm:

```
Logparser "SELECT reversedns
(extract_prefix(remote-
endpoint,0,':')) AS Remote,
COUNT(*) AS Hits FROM *.log WHERE
data like 'Quit' GROUP BY Remote
ORDER BY Hits desc" -i:CSV -nSkip-
Lines:4 -o:DATAGRID
```

Die OWA-Nutzungsstatistik eines User (IIS-Log) erfahren Sie mit diesem Kommando:

```
Logparser "select * from C:\inet-
pub\logs\LogFiles\W3SVC1\u_ex11*.
log WHERE cs-uri-stem LIKE '%OWA%'
AND cs-username like '%USER%' AND
cs-uri-stem LIKE '%form%' ORDER BY
date,time DESC" -i:w3c -o:DATAGRID
```

Die Ergebnisse der Abfragen lassen sich auch direkt als Grafiken ausgeben. Hierfür müssen Sie die Office 2003 Web Components inklusive SP1 installieren. Als Ausgabebetyp wählen Sie "CHART" und über "CHART-TYPE" und "CHARTTITLE" legen Sie Diagrammtyp und Titel fest. Über das Listing "Grafische Ausgabe von Logparser" stellen Sie etwa die Verteilung der eingehenden E-Mails an einem Tag sehr ansprechend dar.

Fazit

Dieser Workshop hat die wichtigsten Protokolle und ihren Nutzen kurz vorgestellt. Es sollte im Sinne jedes Administrators sein, den Inhalt der verschiedenen Protokolle zu kennen. Über diese lassen sich Fehler schnell lokalisieren und weiterführende Informationen herausfiltern. Auch können Sie auf diesem Weg sehr schnell Statistiken zu OWA oder zum E-Mailverhalten generieren, die tiefere Einblicke in die Nutzung der Exchange-Umgebung bieten. (In) 

[1] Exchange 2007-Transport-Berechtigungsmodell
C2P31

[2] Understanding Non-Delivery Reports
C2P32

Link-Codes



Neuerungen in Windows Server 8

Server mit Köpfchen

von Ulf B. Simon-Weidner

So nach und nach findet das Gespann Windows 7 und Windows Server 2008 R2 seinen Weg in die Unternehmensnetze. Da steht bereits der Nachfolgeserver in den Startlöchern: Windows Server "8". Unter der Haube hat Microsoft ordentlich Funktionen optimiert und Technologie erneuert. Vieles im Anfang 2013 erwarteten Server dürfte Admin-Herzen dabei höherschlagen lassen. Dazu zählen etwa die Möglichkeiten, ein Active Directory zu klonen oder Netzwerkkarten über Windows Server direkt zusammenzuschalten. IT-Administrator hat einen ersten Blick auf die Developer-Preview geworfen – und ist positiv überrascht.

Rein optisch betrachtet wirkt der erste Blick auf Windows 8 eher ernüchternd. Das "Metro-Style"-Startmenü mit seinen Kacheln und klaren Farben erinnert an die modernen Würfelhäuser im Bauhausstil und wirft gleich zu Beginn die Frage auf, ob eine Windows Phone- oder iPad-Benutzeroberfläche auf einem Server zeitgemäß ist. Auf der anderen Seite: Warum erwarten Administratoren einen leeren Bildschirm mit einem kleinen Startknopf und einem Startmenü, in dem sich der Nutzer mühsam durch mehrere Instanzen arbeiten muss, nachdem er sich am System angemeldet hat?

Der Server für die Cloud

Windows Server 8 wird von Microsoft als der Server für die Cloud schlechthin dargestellt. Damit stellt sich die Frage, ob er überhaupt interessant für Unternehmen ist, die keine Cloud-Ambitionen haben? Und was bedeutet es, wenn ein Server für die Cloud geschaffen wurde? Zunächst ist es bei Cloud Computing wichtig, mandantenfähig zu sein. Mandantenfähig heißt bei Microsoft "Multi-Tenant" und bedeutet, dass Systeme unterschiedlicher Kunden völlig isoliert voneinander parallel laufen können, vielleicht sogar auf dem gleichen Virtualisierungshost, während die Systeme des gleichen Mandanten miteinander kommunizieren können. Das ist Voraussetzung für eine Cloud, unterstützt den Administrator aber auch bei der Erfüllung von Anforderungen wie Entwicklungssysteme in separaten Netzen oder Vor-Produktionssystemen.



Bild 1: Das Startmenü im Metro-Style verbirgt sich hinter dem Start-Knopf. Durch kurzes Warten unten links gelangt der Administrator auch in die Suche oder Einstellungen.

Es sollten sich außerdem möglichst viele virtuelle Maschinen auf einen Host packen lassen. Hierfür bietet Microsoft einige Verbesserungen: Die Limits an unterstützten Prozessoren und RAM sind signifikant gestiegen, die Installationen lassen sich stark verschlanken und sogar offline warten. Verschieben lassen sich virtuelle Maschinen wahlweise wie bisher im Cluster mit gemeinsamem Plattenspeicher oder sogar nur über das Netzwerk – natürlich auch hier im laufenden Betrieb. Nicht zuletzt unterstützt nun auch der Client Hyper-V. Und damit das Netzwerk weder Single Point of Failure noch Flaschenhals

ist, wird das Zusammenschalten von Netzwerkkarten direkt vom Betriebssystem unterstützt. Alles Möglichkeiten, die auch im Rechenzentrum ohne Cloud-Pläne interessant sind.

Ein weiterer wichtiger Punkt ist die Verwaltung. Hier setzt Microsoft weiterhin auf die PowerShell, bietet aber mit dem Servermanager auch eine grafische Benutzeroberfläche an, die nicht nur einzelne Maschinen lokal oder remote verwalten kann – der Administrator hat nun auch die Möglichkeit, Servergruppen einzurichten und mehrere Systeme auf einmal

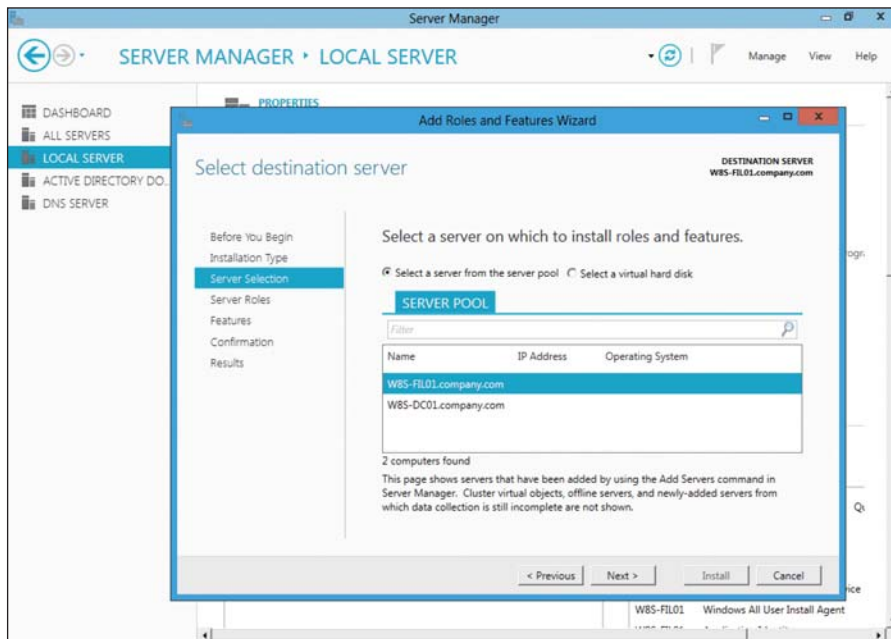


Bild 2: Der Servermanager erlaubt die Verwaltung von entfernten Systemen und virtuellen Festplatten

zu verwalten. Ein Muss in der Cloud, aber auch für diejenigen interessant, die mehr als einen Server mit ähnlichen Diensten verwalten müssen. Dass die Verwaltbarkeit über mehrere Systeme hinweg wichtig ist, hat Microsoft offensichtlich verstanden und gleich noch eine neue Möglichkeit geschaffen, um DNS- und DHCP-Server zentral zu administrieren. Außerdem unterstützt der Servermanager die Offline-Wartung von virtuellen Festplatten, die als Alternative zu laufenden Servern als Administrationsziel dienen.

Hochverfügbarkeit von Diensten erhalten Administratoren mit dem Cluster, der mit Cluster-shared Volumes (CSV) die Verbindung von mehreren Clusterknoten auf die gleiche Partition erlaubt. Dies war im letzten Release Hyper-V vorbehalten. In der neuen Version ist es möglich, zahlreiche Server mit dem gleichen Dienst zu betreiben, zum Beispiel Dateiserver. Durch das CSV ist es nicht notwendig, dass nur ein Server den Dienst zur Verfügung stellt und die anderen darauf warten, dass er ausfällt. Im Gegenteil: Über jedes der Systeme kann auf die Informationen zugegriffen werden und der Cluster kümmert sich darum, dass die Shares identisch sind und wer gerade Änderungen durchführt.

Mit diesen neuen Möglichkeiten im Clusterumfeld können Dateien knotenübergreifend angeboten werden. Einen Failover

gibt es damit so gut wie nicht, die gleichen Daten stehen über unterschiedliche Knoten identisch zur Verfügung. Über Single-Instance-Storage kann sichergestellt werden, dass jede Datei nur einmal abgelegt wird. Dies ist auch unter dem Begriff "Deduplication" geläufig und war bisher den Benutzern des Windows Storage Servers vorbehalten. Und einen Durchbruch im Thema Dateisystemberechtigungen gibt es auch mit "Flexible Access to Files", das Lö-

sungen für zahlreiche Problemfälle in diesem Bereich mitbringt.

Vereinfachtes Management

Die Installation verläuft unspektakulär und basiert auf den Windows-Images, die seit Windows Vista zum Einsatz kommen. Dadurch geht die Installation sehr zügig vonstatten. Der Administrator hat hier auch weiterhin nicht viel Auswahl, abgesehen von der Wahl der Serverversion: Server Core, Server Core mit Server GUI oder voller Installation. Nach der Anmeldung am System kommt die erste große Änderung. Das Startmenü ist nicht mehr ein klassisches Menü, vielmehr öffnet sich eine bildschirmfüllende Ansicht unterschiedlicher Kacheln. Microsoft nennt diese Benutzeroberfläche "Metro" – vor allem mit dem Client wird es Anwendungen geben, die speziell für diese Benutzeroberfläche geschrieben sind und im Vollbildmodus ausgeführt werden. Aber auch klassische Anwendungen laufen weiterhin. Im Startmenü verbirgt sich die Suche. Der Nutzer muss lediglich anfangen zu tippen, und die Suche zeigt sowohl passende Anwendungen wie auch sonstige Dokumente.

Den Servermanager hat Microsoft signifikant überarbeitet. Endlich lassen sich damit nicht nur einzelne Systeme verwalten, son-

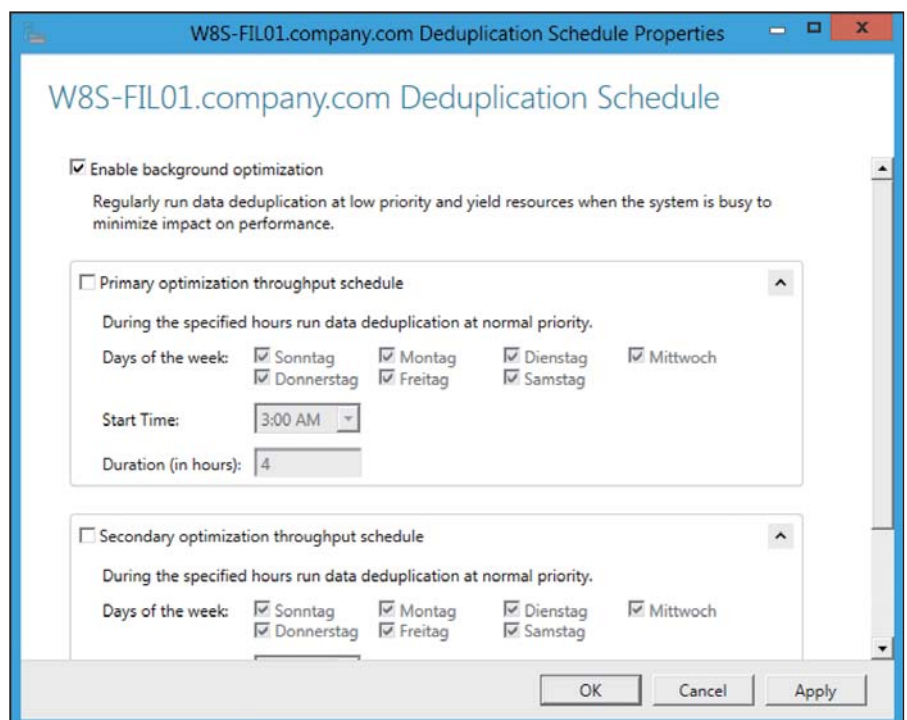


Bild 3: Die Deduplication stellt sicher, dass jede Datei nur einmal vorgehalten wird – interessant für Home- und Gruppenlaufwerke

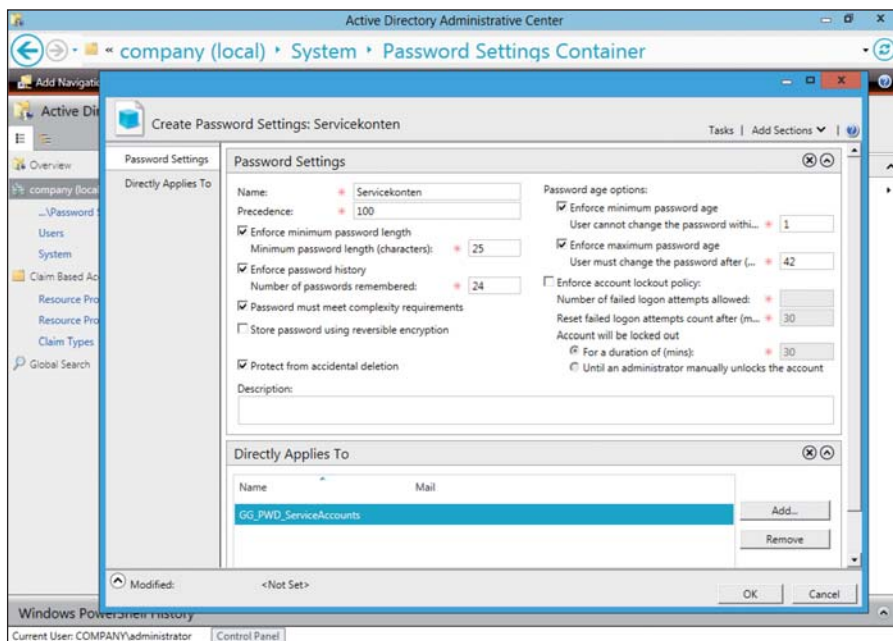


Bild 4: Fine Grained Password Policies: Seit Windows Server 2008 vorhanden, gibt es die grafische Administrationsoberfläche auch beim Windows Server 8

dem der Administrator kann auch Gruppen von Systemen auf einmal überblicken (Eventlogs, Performance, Best Practices Analyzer) und ausgewählte Operationen über mehrere Systeme hinweg ausführen. Wird auf einem Server eine neue Windows Rolle wie DHCP, Active Directory, Fileserver oder Webserver installiert, zeigt der Servermanager automatisch eine neue Gruppe an. Für eigene Anwendungen lassen sich auch selbst Gruppen definieren, so dass der Administrator alle Systeme, die einem ähnlichen Zweck dienen, gemeinsam überwachen kann. Ob eine neue Rolle dem lokalen oder einem entfernten Server zugewiesen wird, spielt dabei keine Rolle.

PowerShell noch leistungsfähiger

Die PowerShell ist jetzt überall. So verwundert es nicht, dass sich vom Servermanager aus direkt ein PowerShell-Fenster starten lässt, mit rechtem Mausklick auf einen anderen Server sogar remote. Die PowerShell wurde denn auch kräftig erweitert. Während in Windows Server 2008 die PowerShell noch nicht standardmäßig zum Lieferumfang gehörte, lieferte die in Windows Server 2008 R2 integrierte Skriptsprache bereits rund 230 Befehle (Cmdlets). Bei Windows Server 8 sind es über 1.400.

Ebenfalls positiv: In den letzten Jahren sind einige Features rausgekommen, die nur durch die PowerShell unterstützt werden.

Zum Beispiel im Bereich Active Directory gab es mit Windows Server 2008 die "Fine Grained Password Policies", die sich der Administrator zu Hilfe nehmen konnte, um unterschiedliche Passwortanforderungen für Benutzer, Administratoren, Dienstkonten oder sonstige frei definierbare Gruppen zu vergeben. Hierzu gab es ab 2008 R2 dann PowerShell-Kommandos, die diese Richtlinien unterstützt haben, die grafische Benutzeroberfläche (GUI) hatte aber nicht mitgezogen.

Ein anderes Beispiel ist der in 2008 R2 eingeführte Papierkorb für das Active Directory, der ein Wiederherstellen von Benutzerkonten unterstützt – allerdings nur über die PowerShell oder mit Drittanbieter-Tools. In Windows Server 8 finden sich auch diese Features mit einer entsprechenden grafischen Benutzeroberfläche. Die Administration wurde in das Active Directory Administrative Center, die Active Directory-Verwaltungskonsolle, integriert. Und nicht nur die alten Features, die bisher noch nicht in der GUI unterstützt wurden, finden hier Unterstützung. Auch neue Funktionen wie "Flexible Access to Files" oder "Claim-based Access to Files" – derzeit stehen unterschiedliche Namen für das gleiche Feature im Raum – werden bereits in der grafischen Benutzeroberfläche unterstützt. Und noch einen Schritt weiter geht die neue Active Directory-Verwaltungskonsolle: Am unteren Fensterrand befindet sich die "Windows PowerShell History". Die Konsole führt alles über die PowerShell durch und der Administrator kann sich einfach über die Kommandos informieren, um diese dann in eigenen Skripten zu verwenden.

Gleiches gilt auch für die Assistenten des Servermanagers. Führt etwa der Administrator die Konfigurationsschritte durch, um eine neue Rolle einzurichten, erhält er auf der Zusammenfassungsseite das An-

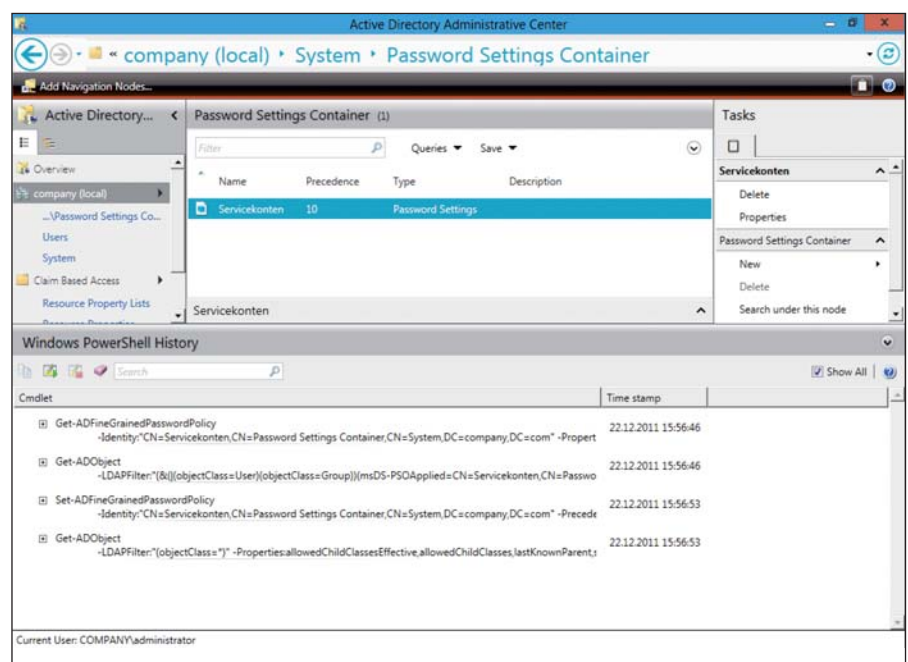


Bild 5: Das Active Directory Administrative Center führt alle Aktionen über die PowerShell durch und loggt mit, so dass sich der Administrator über die Befehle informieren kann

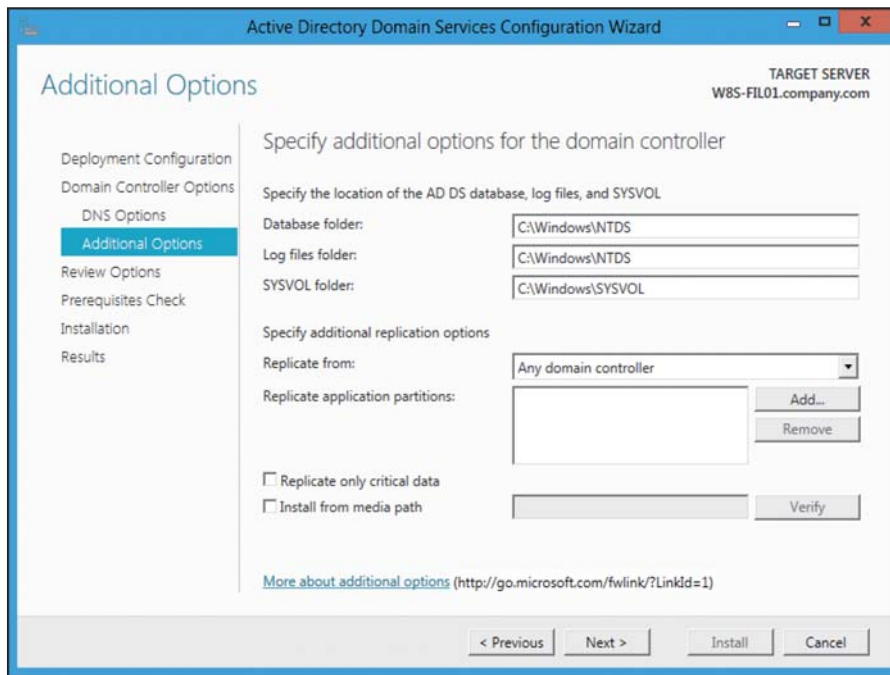


Bild 6: Statt einer Vielzahl einzelner Seiten beschränken sich die neuen Assistenten und bieten mehr Funktionalität auf einer Seite an

gebot, die Konfigurationsschritte auch als PowerShell-Kommando zu exportieren.

Neues im Netzwerk

Auch im Bereich der Netzwerkverwaltung hat Microsoft einige Neuerungen parat: Der DHCP-Server kann nun seine Scopes mit anderen DHCP-Servern replizieren. Hierbei hat der Administrator die Wahl, ob er eine Lastverteilung oder einen Hot Standby nutzen möchte. Die hierfür eingerichteten DHCP-Scopes replizieren dann zwischen den Servern und entweder teilen sich die Server die Arbeit oder der eine lauscht, ob der andere seine Arbeit verrichtet und springt ein, falls notwendig. Um das Netzwerk besser verwalten zu können, gibt es schließlich noch das "IP Address Management", eine zentrale Administrationskonsole für die bisher jeweils lokalen Konsolen.

Flexibler Server Core

Manchmal heißt es, Microsoft mache es erst mit dem dritten Release richtig. Das mag etwa bei Hyper-V stimmen, aber auch beim Server Core. Diese Option, einen Server gänzlich ohne grafische Benutzeroberfläche zu installieren, ist sowohl bei der Virtualisierung wie auch im Datacenter interessant. Bei der Virtualisierung liegt klar der Vorteil auf der Hand, mehr Maschinen auf die gleiche Hardware pa-

cken zu können. Des Weiteren verringert eine kleinere Installation die Notwendigkeit, zu patchen (ohne den Internet Explorer sind die Patches hierfür beispielsweise nicht notwendig), und auch die Angriffsfläche ist mit weniger Komponenten reduziert.

Beim Server Core hat sich denn auch einiges getan. Standardmäßig gibt es jetzt drei Modi: Den komplett reduzierten Server Core ohne grafische Benutzeroberfläche, einen Server Core mit Server-Benutzeroberfläche und den vollen Server. Der Erste kommt wie gesagt komplett ohne Benutzeroberfläche daher. Lediglich die Kommandozeile und die PowerShell sind vorhanden. Der Anmeldeschirm bleibt weiterhin grafisch. Die zweite Option hat einige grafische Verwaltungsinstrumente mit an Bord, dennoch fehlen hier viele Komponenten wie der Internet Explorer oder der Windows Explorer.

Interessant dabei ist: Server Core ist nicht mehr nur eine Installationsoption. Bei bisherigen Versionen musste sich der Administrator bereits bei der Installation entscheiden, welche Variante er nutzen wollte. Hat er es sich später anders überlegt, musste er den Server komplett neu installieren. Stattdessen ist Server Core tatsächlich optional geworden, so dass je-

derzeit die grafische Benutzeroberfläche komplett mit oder ohne Serververwaltung deinstalliert und installiert werden kann. Herstellern von Serversoftware wird daher nahegelegt, sich für diese neuen Optionen zu rüsten und die Kompatibilität ihrer Anwendungen mit den Server Core-Optionen sicherzustellen.

Ein weiterer wichtiger Punkt: Seit Windows Vista hat eine Installation immer sämtliche Installationsdateien zur Verfügung, um auch ohne Produkt-DVD zum Beispiel einen DNS-Server nachzuinstallieren. Beim Windows Server 8 ist dies auch der Fall, der Administrator kann aber nicht nur ein Feature – wie die grafische Benutzeroberfläche – deinstallieren, er kann auch angeben, dass die Installationsdaten des Features von der Festplatte entfernt werden. Dadurch schrumpft der von der Installation benötigte Plattenplatz deutlich, was Virtualisierung und damit auch Cloud Computing zugute kommt. Der neue Purismus von Microsoft wirkt sich also auch hier aus. Sollte es sich der Administrator hinterher doch einmal anders überlegen, kann er das Feature immer noch installieren. Hierfür muss er nur ein Windows-Installationsimage oder Windows-Update beim Aktivieren des Features in der PowerShell mit angeben. Insgesamt bietet Windows Server 8 rund 300 Features an, die der Administrator installieren, deinstallieren oder sogar deren Installationsdateien entfernen kann.

Dateiberechtigungen leicht gemacht

Das Windows-Sicherheitsmodell ist etwas in die Jahre gekommen, aber aufgrund der Abwärtskompatibilität zu unterschiedlichen Betriebssystemversionen, Anwendungen oder Dateisystemen nur schwer zu ersetzen. Dabei ist NTFS bereits deutlich sicherer und mächtiger als viele andere Dateisysteme. Kunden haben sich in den vergangenen Jahren besonders mehr Flexibilität gewünscht. Darunter etwa der Wunsch nach abfragenbasierten Sicherheitsgruppen, wie bei den dynamischen Verteilerlisten von Exchange. Da sich die Berechtigungen unter Windows aber bei der Erstellung des Tokens, also beim Logon, entscheiden, ist es etwas schwieriger, eine angemessene Flexibilität



zu bieten. Dann gab es immer wieder den Wunsch, Berechtigungen kombinieren zu können, etwa mit den Bedingungen "ist in diesem Team und ist Manager, dann Schreibzugriff".

Was die genannten Tokens betrifft, gibt es ein mitunter einschränkendes Limit, da selbst mit zusätzlicher Konfiguration ein Anwender nur in maximal rund 1.015 Gruppen Mitglied sein kann. Da hierzu auch indirekte, rekursive Mitgliedschaften zählen, gibt es zahlreiche Unternehmen, die diesen Wert schnell erreichen. Einziger Workaround ist eine Änderung der Berechtigungsstruktur oder sogar eine separate Gesamtstruktur, damit der Token in bestimmten Bereichen neu generiert wird. Windows Server 8 hat ein neues Feature an Bord, genannt "Flexible Access to Files", "Claim-based File Access" oder auch "Dynamic Access Control". Der bisherige Token bleibt erhalten, jedoch kann er durch sogenannte "Claims" ergänzt werden. Claims gibt es schon länger bei den Federation Services. Die Ergänzung des Tokens hat keine Auswirkungen auf die bisherigen Berechtigungen oder die Tokengröße und der Claim muss auch nicht verpflichtend beim Logon ergänzt werden.

Damit bietet Microsoft neue Möglichkeiten zur Lösung der Token-Size Problematik. Über die neuen Berechtigungen ist vieles möglich: Der Administrator definiert in einer Art Abfrage, wie der Zugriff auf Dateien aussehen soll: "Wenn der Zugreifende Mitglied des Bereiches xyz ist, und er Manager ist, aber nicht Mitglied der Unterabteilung abc, dann soll er Zugriff erhalten". Dieser Ansatz ist sehr mächtig. Es lassen sich aber nicht nur Berechtigungen aufgrund von Benutzerinformationen steuern, sondern der Administrator kann auch definieren, dass bestimmte Dateien nur geöffnet werden können, wenn der Anwender von einem domänenintegrierten Arbeitsplatz aus zugreift – oder wenn er eine Zertifikatsbasierte Anmeldung etwa mit Smartcards durchgeführt hat.

Es stehen also vielfältige Möglichkeiten zur Berechtigung ins Haus. Doch wäre es nicht schöner, wenn der Ersteller eines Dokuments von vornherein die Berechtigungen mitsteuert? Hier kommen wir zu einem

zweiten Vorteil dieses neuen Features: Es hilft beim Identifizieren und Klassifizieren der Daten. Dies kann über unterschiedliche Methoden erfolgen: Beim Erstellen einer Freigabe legt der Administrator fest, ob es sich um eine Freigabe für einzelne Benutzer, Gruppen oder eine organisationsweite Freigabe handelt. Zusätzlich kann die Anwendung, die die Datei erstellt, mit berücksichtigt werden. Außerdem können noch sogenannte "Tags" benutzt werden. Der Anwender wird dabei angewiesen, bei seinen Dokumenten eine Vertraulichkeitsstufe festzulegen (etwa "Öffentlich", "Firmenintern", "Projektintern", "Vertraulich innerhalb der Firma").

Auf Basis dieser Tags erfolgt dann eine Klassifizierung automatisch, so dass zum Beispiel bei einem entsprechenden Dokument ein externer Mitarbeiter in der Firma keinen Zugriff erhält – völlig automatisch, weil das Dokument vom Ersteller entsprechend klassifiziert wurde. Zusätzlich ist der Dialog anpassbar, wenn der Zugriff verweigert wird. Hier kann auf eine URL im Intranet mit den Policies verlinkt oder eine E-Mail versendet werden, in der der Anwender den Zugriff erbitten kann. Zusätzlich werden die "neuen Berechtigungen" auch für die Überwachungsrichtlinien (Auditing) verwendet: Der Administrator überwacht damit an den richtigen Stellen und wird nicht von Ereignismeldungen überhäuft, sondern kann sich auf die relevanten Zugriffe konzentrieren – zum Beispiel, ob Externe versucht haben, auf als vertraulich markierte Dokumente zuzugreifen. Das neue Feature kann auch mit dem "Rights Management Server" zusammenarbeiten, so dass Dateien sogar verschlüsselt oder Ablaufzeiten für bestimmte Berechtigungen festgelegt werden können.

Dynamic Access Control wird über das Active Directory gesteuert und vieles auch im AD konfiguriert, so dass die zentralen Policies auch über alle Fileserver im Unternehmen hinweg gelten können. Natürlich können die neuen Berechtigungen auch individuell gesetzt werden, aber insbesondere über die automatische Klassifizierung von Dokumenten weitreichende Berechtigungen zu steuern, macht dieses Feature so interessant.

Um Dynamic Access Control nutzen zu können, reicht nach derzeitigem Stand aus, einen Domänencontroller auf Basis von Windows Server 8 sowie die Dateiserver, die die zu schützenden Daten enthalten, zu migrieren. Ein Client-Rollout ist hierfür nicht notwendig – wenn der Client keinen Token mit dem "Claim-Anteil" präsentieren kann, kümmert sich der Dateiserver darum, diesen zu erhalten.

Mehr Virtualisierung und Netzwerkfähigkeiten

Die erwähnte Mandantenfähigkeit im Netzwerkbereich wird durch neue Private Virtuelle Netzwerke (PVLAN) sowie den erweiterbaren Switch in Hyper-V 3.0 unterstützt. Virtualisierungshosts müssen skalierbar sein und möglichst viele Server gleichzeitig betreiben können. Windows Server 8 unterstützt ganze 640 logische Prozessoren und 4 TByte RAM, der Virtualisierungshost Hyper-V kann bis zu 160 logische Prozessoren (und bis zu 32 virtuelle Prozessoren pro virtueller Maschine) und 2 TByte RAM (bis zu 512 GByte pro virtueller Maschine) unterstützen. Virtuelle Systeme lassen sich einfach verschieben, dies geht wie bisher im Cluster, neu aber auch einfach über das Netzwerk – auch hier im laufenden Betrieb. Die Virtualisierungshosts müssen sich also gar nicht die Festplatten in einem Cluster teilen, im Extremfall soll es sogar möglich sein, eine virtuelle Maschine auf einen Windows 8-Client zu schieben, da auf diesem neuerdings auch Hyper-V läuft.

Das alles stellt natürlich Ansprüche an das Netzwerk. Doch auch hier hat sich einiges getan. Viele Administratoren kennen die Problematik, dass die Netzwerkkarte als Single Point of Failure nur durch das Zusammenschalten mehrerer identischer Netzwerkkarten umgangen werden kann. Zusätzlich bietet dies eine Erhöhung der Übertragungskapazität. Dies erforderte bislang jedoch stets spezielle Treiber der Hersteller. Wenn Admins im Server-Support bei Microsoft anfragten, war häufig eine der ersten Fragen, ob Teaming zum Einsatz kommt, und wenn ja, die Aufforderung, dies abzuschalten und zu überprüfen, ob der Fehler dann immer noch vorliegt. Und oft war Teaming in der Tat schuld an Fehlermeldungen. Im neuen Windows wird

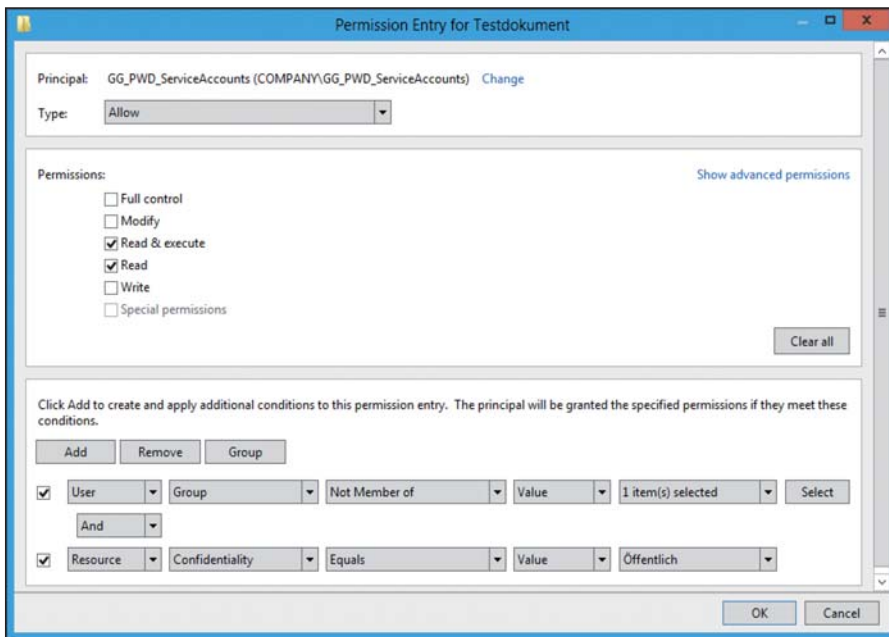


Bild 7: In Windows Server 8 sind kombinierte Berechtigungen möglich, die sich in Abhängigkeit von Benutzer, Gruppen und Ressourceinformationen verknüpfen lassen

Teaming standardmäßig vom Betriebssystem unterstützt. In einer Demonstration auf der BUILD-Konferenz im September 2011 hat Microsoft sogar gezeigt, wie eine weitere Netzwerkkarte in einen Hot Plug-fähigen Server gesteckt werden kann, um die Netzwerkkapazität mal eben zu erhöhen. Kaum war die Karte verbunden, hat sie eine bestehende Kopieroperation sogar gleich mit beschleunigt, indem sie ihre Kapazitäten zur Verfügung gestellt hat. Das NIC-Teaming unterstützt bis zu 32 Netzwerkkarten und kann für die Neuerungen im Cluster-Bereich sogar Server-übergreifend eingerichtet werden.

Um dies alles zu ermöglichen, ist ein schnelles und flexibles Netzwerk notwendig. An dieser Stelle entsteht angesichts der Vielzahl an Änderungen fast der Eindruck, dass der Netzwerkstack komplett umgeschrieben wurde. Das SMB-Protokoll wurde erweitert, SMB2-Direct unterstützt Remote Direct Memory Access (RDMA) und kann damit Daten schnell über das Netzwerk ohne großen Protokoll-Overhead schieben. Hierbei wird die Netzwerkkarte deutlich mehr gefordert, die CPU hingegen wesentlich weniger für Netzwerktransfers belastet. Datacenter TCP ermöglicht besseren Durchsatz und weniger Overhead bei Applikationsservern innerhalb des Rechenzentrums, und Datacenter Bridging kann sich darum küm-

mern, dass Daten zwischen Datacentern mit einer besseren Priorität und Qualität übertragen werden.

Besonders bei der Nutzung von Remote DMA scheint es fast so, als ob die Dateien auf lokalen Laufwerken und nicht im Netz liegen. Dies ist insbesondere dem schnellen Zugriff zu verdanken. In einer Demonstration erreichte die neue Technologie eine Transferrate von 2 GByte/s. Die CPU war dabei mit weniger als einem Prozent ausgelastet. Zusätzlich hat sich Microsoft auch dafür eingesetzt, dass Netzwerkports besser identifizierbar sind: Das Betriebssystem versucht demnach, den Karten aussagekräftigere Namen zu geben, die bereits durch das BIOS vorgeprägt sind. Mit zahlreichen Herstellern wurden Vereinbarungen darüber getroffen, diese Namen auch auf die Gehäuse zu drucken. Damit ist ein Netzwerkport für den Administrator sowohl im Betriebssystem wie auch physikalisch klar erkennbar – das irrtümlicherweise falsche abgezogene Netzkabel soll der Vergehenheit angehören.

Active Directory-Klone

Active Directory Domänencontroller können nun auch geklont werden, ohne irreparable Schäden im AD [2] zu verursachen. Damit sind Snapshot-Technologien bei Datensicherungen möglich, die bisher zu meist ein absolutes Tabu sind und häufig

zu der Empfehlung geführt haben, diese Technologien komplett abzuschalten, wenn DCs virtualisiert werden. Bei der Installation des Active Directory muss sich der Administrator nicht mehr mit Vorbereitungen wie Schemaerweiterungen auseinandersetzen. Der neue Installationsassistent kümmert sich selbst darum – natürlich erst, nachdem er die Voraussetzungen für die Installation des Domänencontrollers geprüft hat. Managed Service Konten, die ihre Passwörter selber verwalten, hat Microsoft zudem überarbeitet. Sie können jetzt Maschinen-übergreifend eingesetzt werden. Die Produktaktivierung mit dem Key Management Server ist in Active Directory integriert worden, so dass IT-Abteilungen sich einfacher davor schützen können, dass ein mitgebrachtes Gerät einfach so mit dem Unternehmensschlüssel aktiviert wird.

Fazit

In unserem Artikel haben wir einen ersten Blick auf einige der Technologien in der kommenden Version des Windows Servers geworfen. Ob der neue Server dann Windows Server 8, 2012 oder 2013 heißt, bleibt abzuwarten – genauso, welche Features es tatsächlich in das finale Produkt schaffen. Auf alle Fälle verspricht bereits die Developer Preview des kommenden Windows Server viel Interessantes. Dazu gehören auch Technologien, die stark überarbeitet wurden oder endlich ihren Weg in den Server gefunden haben. Welche Funktionen Microsoft dabei in einem Server-Release vereint, ist durchaus beeindruckend. Die Arbeit mit dem neuen Startmenü ist zwar zunächst gewöhnungsbedürftig, doch ein Admin dürfte sich schnell zurechtfinden. Und für den Administrator, der auch schon jetzt einen Blick auf den neuen Server geworfen hat und auf die nächste Beta wartet: Der neue Server lässt sich ausschalten, indem der Nutzer den Mauscursor links unten verweilen lässt, dann auf "Settings" geht, das Stromsymbol wählt und hier die Option zum Herunterfahren findet. (dr) 

[1] Präsentationen der Microsoft BUILD-Konferenz C2P41

[2] IT-Administrator Sonderheft II / 2010 "Active Directory"

Link-Codes



Microsoft System Center Configuration Manager 2012

Der Mensch im Mittelpunkt

von Thomas Joos



Aktuell arbeitet Microsoft an der Version 2012 des System Center Configuration Manager, die zahlreiche Neuerungen bietet, zum Beispiel bei der Smartphone-Verwaltung. Eine weitere Neuerung ist das ausgeklügelte Regelwerk, das auf Basis verschiedener Werte wie Arbeitszeit, Standort, Uhrzeit und Endgerät genau die Anwendungen auf den Clients zur Verfügung stellen kann, die der Situation am besten gerecht werden. Wir stellen Ihnen auf Basis der Beta 2 vor, wie sich die Neuerungen in der Praxis ausprägen.

System Center Configuration Manager 2012 (SCCM) konzentriert sich nicht auf die PCs der einzelnen Anwender, sondern auf die Anwender und die benötigten Applikationen selbst. Diese Änderung des Fokus soll Administratoren die Arbeit erleichtern. In einer SCCM 2012-Infrastruktur können Anwender mit mehreren Endgeräten, aber den gleichen Anwendungen arbeiten. Die Definition eines primären Gerätes hilft bei der Verteilung von Anwendungen. Umgekehrt können Sie auch einem Gerät mehrere Anwender zuweisen, wenn Sie mit wechselnden PCs arbeiten. Geräten lassen sich auch primäre Anwender zuweisen, die dann wiederum im System ihre Arbeitszeit hinterlegen können.

Anwenderorientierte Verwaltung

Auf Basis dieser Daten kann SCCM 2012 dann entscheiden, welche Anwendungen mit den unterschiedlichen Technologien angebunden werden. Auf seinem primären Gerät erhält der Anwender zum Beispiel eine lokale Installation seiner benötigten Programme. Arbeitet er an einem anderen Gerät, erhält er Zugriff über App-V oder einen Remotedesktop.

Auf Basis der hinterlegten Regeln kann SCCM 2012 also automatisiert genau die Anwendungen auf den angebundenen Endgeräten zur Verfügung stellen, die die An-

wender benötigen. Dabei lassen sich auch virtualisierte Anwendungen auf Basis von App-V oder Remotedesktops mit lokalen Installationen mischen. Einer Applikation lassen sich in der neuen Version mehrere Verteilungswege zuweisen und Regeln zuordnen, Deployment Type genannt. Die Vorgängerversionen konnten pro Paket immer nur einen Verteilungsweg verwenden. Meldet sich der Anwender an einem Arbeitsplatz an, der über eine schmalbandige Verbindung zum internen Netzwerk angebunden ist, bekommt dieser zum Beispiel Zugriff auf

den Remotedesktop zur Anwendung. Im Firmennetzwerk installiert SCCM dann das Programm ganz normal auf dem Computer oder virtualisiert es über App-V.

Außerdem lassen sich Abhängigkeiten zwischen Anwendungen konfigurieren, so dass immer die notwendigen Tools und Anwendungspakete auf den PCs installiert sind. SCCM 2012 erkennt Abhängigkeiten und kopiert voneinander abhängige Pakete in einen gemeinsamen "Distribution Point". Auf diese Weise stehen die Anwendungen

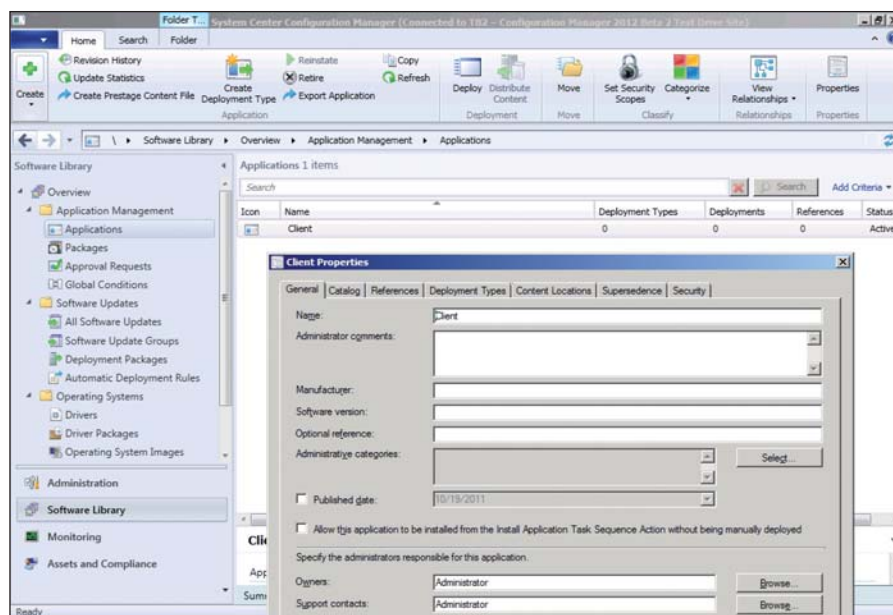


Bild 1: Aus der neuen Verwaltungsoberfläche des SCCM 2012 ist ein Client zur weiteren Bearbeitung ausgewählt



immer zur Verfügung. Dieses Kopieren können Administratoren aber einschränken oder für einzelne Inhalte auch deaktivieren. Selbstverständlich kann SCCM Anwendungen auch wieder von PCs entfernen und deinstallieren. Die Installation von Applikationen kann automatisiert erfolgen, oder Anwender installieren die zugeordneten Programme über das neue Webinterface selbst auf dem Endgerät.

Im Portal sehen Anwender dann alle Programme, die Sie aktuell auf dem entsprechenden Gerät verwenden können. Welche Programme die Nutzer dort finden, legen Administratoren bei der Bereitstellung der Anwendung fest. Das heißt in SCCM 2012 erstellen Sie zunächst eine neue Anwendung und legen für diese die Deployment Types fest (normale Installation, Bereitstellung mit App-V oder Remotedesktop). Welchen Deployment-Typ die Anwendung dann für das entsprechende Endgerät verwendet, steuern Sie über Regeln. Und hier haben Sie zahlreiche Steuerungsmöglichkeiten wie Betriebssystem, Arbeitszeit, Endgerät, Abhängigkeiten und vieles mehr. Sie müssen also für eine Anwendung nicht mehrere Pakete erstellen und unterschiedliche Deployment Types zuweisen.

In SCCM 2012 lassen sich jetzt auch Wartungscenter für die Installation von Patches oder Anwendungen definieren. Jeder Anwender kann darüber hinaus selbst Wartungszeiten festlegen, indem er seine Arbeitszeit hinterlegt. Dadurch beeinträchtigen Wartungsvorgänge nicht die Arbeit der Benutzer. Auch hierfür dient das Webinterface für Anwender in SCCM 2012. Benötigt ein Nutzer eine Software, für die er nicht berechtigt ist, kann er im Webinterface auch eine Genehmigung anfordern. Alle Programme, die SCCM verwaltet, lassen sich im Portal darstellen, das im Netzwerk wie ein App Store funktioniert. Und bevor SCCM 2012 Anwendungen auf PCs bereitstellt, kann der Server über den Netzwerkzugriffsschutz in Windows Server 2008 R2 sicherstellen, dass das entsprechende Endgerät auch den Sicherheitsrichtlinien entspricht.

Betriebssysteme bereitstellen

SCCM hilft auch bei der Bereitstellung von Betriebssystemen im Unternehmen. Verbes-

sert hat Microsoft die Verwaltung und den Zugriff auf die Bootmedien sowie die Übernahme der Benutzerdaten und -profile. Dazu nutzt SCCM 2012 das User State Migration Tool (USMT) 4.0. Patches lassen sich in der neuen Version nicht nur an PCs verteilen, sondern auch direkt in die Installations-Images integrieren, mit denen Sie Rechner im Netzwerk installieren. Auf diese Weise sind auch neue Rechner sofort nach der Installation aktuell. Am besten lassen sich Betriebssysteme integrieren, die bereits über WIM-Images verfügen, wie Windows 7 oder Windows Server 2008 R2.

Linux und Unix lassen sich mit SCCM 2012 besser verwalten als mit den Vorgängerversionen. Testen lässt sich das allerdings erst mit der RTM-Version. Optimal unterstützt werden AIX, HP-UX, Red Hat Enterprise Linux, Solaris und Suse Linux Enterprise Server. Server lassen sich anbinden, inventarisieren und überwachen. Sinnvoll ist dies allerdings nur für Unternehmen, die hauptsächlich auf Windows-Server bauen und nur einige wenige Linux-Server im Netzwerk integrieren. Die RTM-Version unterstützt auch die Verwaltung der Smartphones besser. Durch die Integration des System Center Mobile Device Managers 2008 und der Weiterentwicklung für die Unterstützung von Windows Phone 7 können Unternehmen auch ihre mobilen Endgeräte verwalten. In welchem Umfang, bleibt abzuwarten.

Vor allem kann SCCM 2012 die Umsetzung und Weiterleitung von Exchange ActiveSync-Richtlinien überwachen und verwalten. SCCM 2012 arbeitet über einen Connector mit Exchange Server 2010 zusammen. Dieser kann ActiveSync-Richtlinien abrufen und an Clients verteilen. Die Richtlinien verwalten Sie nur noch in SCCM, nicht mehr in Exchange. Über den Connector können Administratoren End-

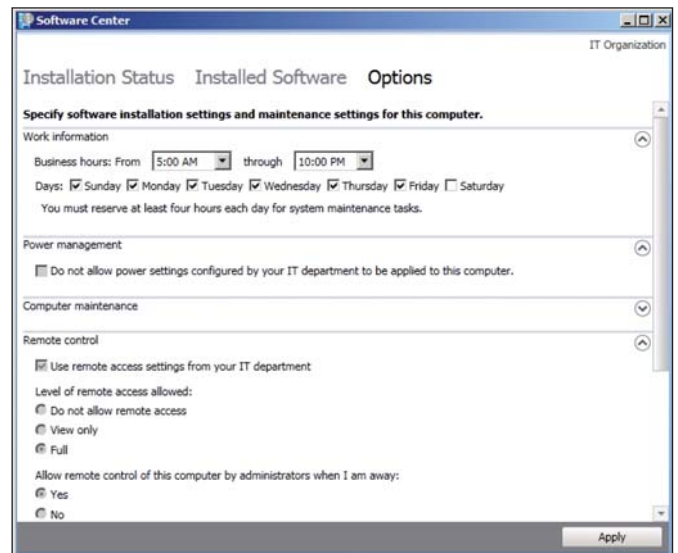


Bild 2: Der Anwender kann eigenständig Wartungsfenster für seinen Client festlegen, so dass der Support zu diesen Zeiten ungestört auf das System zugreifen kann

geräte auch über das Internet löschen (Remote Wipe) sowie Smartphones inventarisieren. Der Connector lässt sich für beliebige Geräte auch nur lesend konfigurieren. Auf diesem Weg kann SCCM 2012 zwar keine Änderungen an den Endgeräten durchführen, aber ein Inventar erstellen.

Verbesserte Verwaltung von Exchange und Active Directory

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.

Primäre Sites können bis zu 100.000 Clients anbinden und stellen keine Begrenzung mehr für Sicherheitseinstellungen, Rechte oder Einstellungen dar. Sekundäre Sites lassen sich zu "Distribution Points" herabstufen, primäre Sites lassen sich hingegen nicht mehr anpassen. Das heißt, primäre Sites können keine untergeordneten primären Sites anbinden, diese Aufgabe übernehmen die Central Administration Sites. Sekundäre Sites können aber weiterhin auch sekundäre Sites ent-

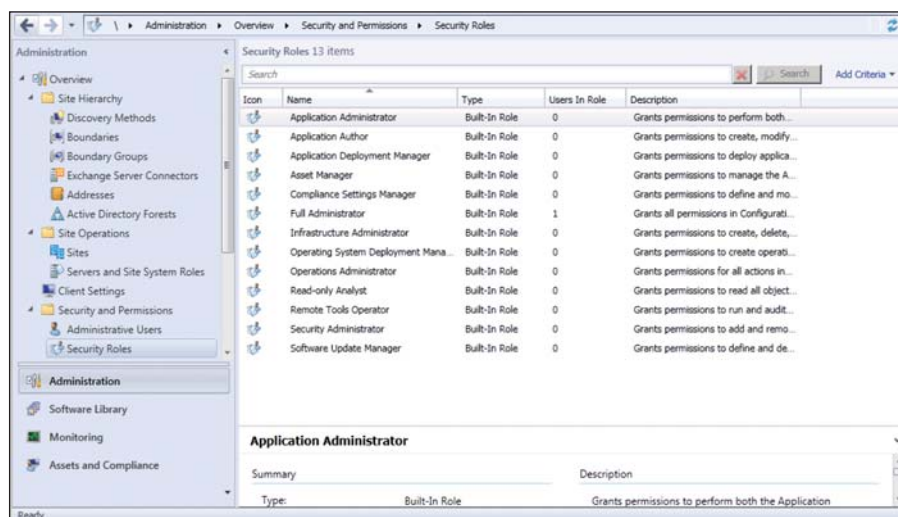


Bild 3: Durch die neuen Sicherheitsrollen in SCCM 2012 sehen Administratoren in der Oberfläche nur die Befehle, für die sie berechtigt sind

halten. Installieren können Sie sekundäre Sites nur über die Verwaltungskonsolle, nicht mehr über eine Setup-Option.

Ebenfalls neu ist die Active Directory Forest Discovery. Mit dieser Technik kann SCCM 2012 mehrere Active Directory-Gesamtstrukturen erkennen und verwalten. Auf diese Weise lassen sich Daten von Sites aus SCCM auch in verschiedenen Gesamtstrukturen zur Verfügung stellen.

Zentrales Client-Management

Clienteneinstellungen lassen sich in SCCM 2012 zentral vorgeben und durchsetzen, unabhängig an welchen Sites oder Standorten Clients angebunden sind. Für Sites lassen sich gemischte Anbindungen von Clients über HTTP oder HTTPS festlegen, abhängig davon, wo sich ein Client befindet. Über das Internet angebundene Clients erlauben zum Beispiel nur verschlüsselte HTTPS-Verbindungen, während Clients an der gleichen Site im internen Netzwerk über HTTP-Verbindung aufbauen dürfen.

Es gibt keinen native/mixed-Mode mehr für Sites. Stattdessen legen Sie über "Site System Roles" fest, welche Clients sich mit den verschiedenen Protokollen verbinden lassen. Generell verfügt SCCM 2012 über zahlreiche weitere Verbesserungen, um Clients über das Internet anzubinden. Benutzerrichtlinien lassen sich zum Beispiel jetzt auch für Clients im Internet umsetzen und die Verwaltung der Zertifikate wurde vereinfacht und verbes-

sert. Clientagenten für SCCM 2012 installieren Sie auf dem gleichen Weg wie bei SCCM 2007. Sie können Agenten auf die Clients pushen, über Gruppenrichtlinien oder manuell installieren, Anmeldeskripte verwenden oder den Agent in ein Image einbinden.

Patches, Softwarepakete und Betriebssystemimages können SCCM-Server untereinander replizieren. Dazu nutzt SCCM 2012 die BranchCache-Funktionalität von Windows Server 2008 R2 und Windows 7. Allerdings müssen in SCCM 2012 auch sekundäre Sites einen eigenen SQL-Server erhalten. Dieser ist für die SQL-Replikation mit der primären Site notwendig. Bei der Datenbank kann es sich aber auch um eine kostenlose Express Edition von SQL Server 2008 handeln. Über die SQL-Replikation gibt SCCM 2012 Änderungen an der Konfiguration und den Einstellungen der Server weiter. Pakete und Patches replizieren sich über das Dateisystem.

Rollenbasierte Admin-Berechtigungen

Die Verwaltungsoberfläche hat Microsoft ebenfalls komplett überarbeitet. SCCM 2012 arbeitet mit einer rollenbasierten Zugriffsberechtigung (RBAC), ähnlich wie Exchange Server 2010. Standardmäßig stehen schon Rollen zur Verfügung, Sie können aber auch benutzerdefinierte Rollen erstellen. Die Oberfläche hat Microsoft komplett überarbeitet und modernisiert. Die Administratoren der verschiedenen Sites sehen in

der Oberfläche nur die Befehle, für die sie berechtigt sind. Das heißt die neue Verwaltung ist wesentlich flexibler und intuitiver.

Die Rollen definieren Sie in der Verwaltungsoberfläche. Dazu hinterlegen Sie Benutzergruppen oder Anmeldenamen aus dem Active Directory in den Rollen. Der beste Weg ist, wenn Sie Benutzergruppen aus dem Active Directory den Verwaltungsrollen in SCCM zuordnen. Wollen Sie Benutzern administrative Rechte erteilen, müssen Sie deren Benutzerkonten nur im Active Directory in die entsprechende Gruppe aufnehmen. Sie haben über die rollenbasierte Zugriffsberechtigung keine Möglichkeit, explizit Zugriffe zu verweigern, sondern können nur Rechte erteilen. Hat ein Administrator auf einen Bereich keine Rechte, darf er diesen auch nicht verwalten.

Durch die komplexe Struktur in SCCM ist es aber durchaus möglich, dass solche Benutzer partiell Zugriff auf Bereiche haben, für die sie eigentlich nicht berechtigt sein sollen. Allerdings kommt dabei nie vor, dass Administratoren Änderungen vornehmen können, sondern sie erhalten dann lediglich lesenden Zugriff auf den entsprechenden Konfigurationsbereich. Der Benutzer, der den ersten SCCM 2012-Server installiert, erhält vollständigen administrativen Zugriff auf die SCCM 2012-Infrastruktur. Weitere Administratoren fügen Sie in der SCCM-Verwaltungskonsolle über die Rolle "Full Administrator" hinzu.

SCCM 2012 gibt es nur noch als 64 Bit-Version. Die Datenbank von SCCM 2012 muss auf einer 64 Bit-Datenbank liegen. Die Beta 2-Version des SCCM 2012 unterstützte weder das SP2 für SQL Server 2008 x64 noch SQL Server 2008 R2. An die Beta 2-Version konnten Sie die 32 Bit-Version von Windows XP Professional SP3 anbinden sowie Windows XP x64 mit SP2. Inzwischen hat Microsoft den Release Candidate veröffentlicht.

Windows Vista kann SCCM 2012 in den Editionen Business, Enterprise und Ultimate verwalten, Sie müssen aber das SP2 für Windows Vista installieren. Windows 7 lässt sich in den Editionen Enterprise und Ultimate anbinden. Welche Betriebssysteme in der finalen Version enthalten sein werden, ist aktuell noch nicht klar. Es ist aber zu erwarten, dass Microsoft bis Windows XP SP3 zurückgehen wird, da noch sehr viele Unternehmen auf Windows XP setzen, vor allem Unternehmen, die im Fokus von SCCM 2012 stehen.

Systemvoraussetzungen





Migration zu SCCM 2012

Sie können SCCM 2007 nicht direkt auf SCCM 2012 aktualisieren (In-Place-Update), sondern müssen die SCCM 2012-Server neu installieren und die Site-Struktur neu erstellen. Das ist notwendig, da Microsoft die Sites und deren Struktur stark überarbeitet hat. Client-Inventare aus der Vergangenheit lassen sich ebenfalls nicht übernehmen, werden aber bei der Anbindung von Clients neu aufgebaut. Wollen Sie ältere Inventarisierungsdaten behalten, sollten Sie eine SCCM 2007-Site im Netzwerk behalten. Mit dem SP2 für SCCM 2007 können Sie auch SCCM 2012 in die Infrastruktur einbinden. Das heißt, wenn Sie zu SCCM 2012 migrieren wollen, kommen Sie um eine Installation des SP2 nicht herum.

Softwarepakete bleiben bei einer Migration erhalten, müssen aber umgewandelt werden. Auch Sammlungen können Sie übernehmen, sowie die zu Grunde liegenden Regeln. Während der Migration können Sie in SCCM 2007 auch so genannte "Shared Distribution Points" konfigurieren. Die Daten dieser Distribution Points liegen auf den SCCM 2007-Servern und sind von den SCCM 2012-Clients aus zugreifbar. Während der Migration können Sie SCCM 2007 Distribution Points direkt zu SCCM 2012 Distribution Points aktualisieren und die Daten übernehmen. Auch sekundäre Sites können Sie zu SCCM 2012 Distribution Points migrieren. Bei der Migration der Daten bleiben diese aber in der SCCM 2007-Infrastruktur erhalten. SCCM 2012 kopiert die entsprechenden Dateien und verifiziert ihren Status. Löschen müssen Administratoren manuell die Daten in der SCCM 2007-Infrastruktur nach der Migration.

Sie haben auch die Möglichkeit, mehrere SCCM-Hierarchien zu einer einzelnen SCCM 2012-Hierarchie zu migrieren. Allerdings können Sie das nur nacheinander durchführen und die Hierarchien müssen natürlich verschiedene Site Codes aufweisen. Eine Schemaerweiterung von Active Directory ist bei einer Aktualisierung zu SCCM 2012 nicht notwendig, da SCCM 2012 mit dem gleichen Schema wie SCCM 2007 arbeitet. Dennoch ist die Migration zu SCCM 2012 eine komplexe Angelegenheit, da sehr viele Daten in Bewegung sind.

SCCM 2012 testen

Microsoft stellt mittlerweile den Release Candidate [1] zur Installation zur Verfügung und als VHD-Datei, die Sie in Hyper-V einbinden können. Um eine Testinstallation durchzuführen, benötigen Sie eine recht umfangreiche Anleitung [2]. Für eine Testumgebung ist der Weg über Hyper-V der schnellere. Allerdings müssen Sie die einzelnen Dateien der Umgebung manuell herunterladen, was oft fehlschlägt. Am besten verwenden Sie für den Download solcher großen Dateien einen Download Manager, zum Beispiel den kostenlosen Free Download Manager [3]. Sie müssen die Dateien nur in die Umgebung importieren und haben sofort eine lauffähige Testumgebung. Dazu laden Sie alle Dateien herunter und klicken auf die ausführbare Datei. Kopieren Sie anschließend das komplette Verzeichnis auf den Hyper-V-Server. Die virtuelle Maschine benötigt 4 GByte Arbeitsspeicher, das heißt der virtuelle Hyper-V-Host muss die entsprechende Leistung zur Verfügung stellen.

Fazit

Auch wenn SCCM 2012 aktuell nur als Release Candidate zur Verfügung steht, ist

schnell ersichtlich, wohin der Weg geht. Microsoft öffnet das Produkt für die Cloud und die Anbindung von Clients über das Internet sowie für Smartphones und andere Systeme wie Linux. Durch die Anbindung mehrerer Gesamtstrukturen und die Möglichkeit, mehrere Hierarchien der Vorgängerversionen zu einer gemeinsamen Hierarchie zusammenzufassen, zentralisiert sich die Verwaltung von Endgeräten im Unternehmen. Dass in der neuen Version der Benutzer im Zentrum steht, nicht mehr dessen Geräte, vereinfacht die Verwaltung. Das gilt auch für die Möglichkeit, Regeln für Anwendungen zu erstellen und mehrere Bereitstellungsarten zu hinterlegen. Dafür ist die Verwaltung und der Betrieb der Infrastruktur noch immer nicht sehr einfach.

Schade ist, dass in der betrachteten Beta 2 noch kein Test der Smartphone-Features möglich ist. Da immer mehr Unternehmen auch iOS-, Android- und andere Systeme anbinden und auch auf diesen Geräten Apps laufen, wäre eine zentralisierte Verwaltung dieser Systeme optimal. Viele Unternehmen greifen dazu noch zu zusätzlichen Verwaltungslösungen. Ob SCCM 2012 der große Sprung für Microsoft ist, wird sich zeigen. Unternehmen, die SCCM 2007 einsetzen, sollten einen Blick wagen, da sich die Verwaltung im Vergleich zum Vorgänger deutlich verbessert hat. (jip)



[1] Download SCCM RC
C1P31

[2] Aufbau einer Demoumgebung mit SCCM 2012 Beta 2
C1P32

[3] Free Download Manager
C1P33

Link-Codes



E-BOOK
SYSTEMS

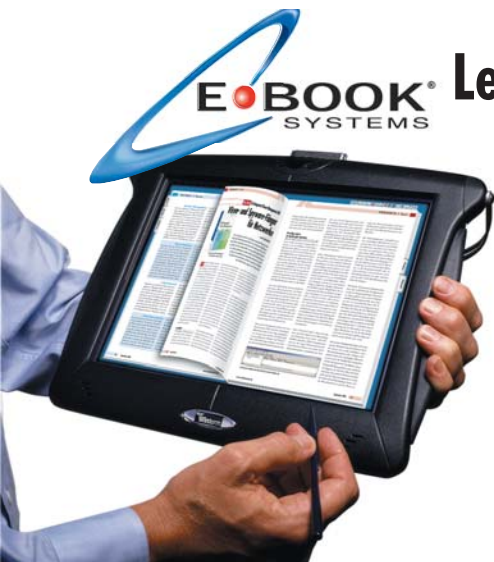
Lesen Sie den IT-Administrator als E-Paper

Testen Sie kostenlos und unverbindlich die elektronische IT-Administrator Leseprobe auf www.it-administrator.de.

Wann immer Sie möchten und wo immer Sie sich gerade befinden – Volltextsuche, Zoomfunktion und alle Verlinkungen inklusive. Klicken Sie sich ab heute mit dem IT-Administrator einfach von Seite zu Seite, von Rubrik zu Rubrik!

Infos zu E-Abos, E-Einzelheften und Kombiangeboten finden Sie auf:

www.it-administrator.de/magazin/epaper





Security Information and Event Management

Wissen ist Macht

von Martin Kuppinger

In den vergangenen Monaten ist der Markt für Produkte zum Security Information and Event Management – kurz SIEM – in Bewegung geraten. Nachdem HP mit ArcSight bereits vor einiger Zeit einen der Marktführer übernommen hatte, wurden nun Q1 Labs von IBM und NitroSecurity von McAfee aufgekauft. Die Akquisitionen zeigen: SIEM wird immer wichtiger. Dieser Beitrag erklärt dieses Konzept und zählt die nötigen Komponenten auf, damit SIEM auch das bringt, was sich der IT-Verantwortliche davon erhofft.



Quelle: 123RF

SIEM fasst also eine laufende Überwachung und Analyse von Ereignissen und die Benachrichtigung darüber mit der Sammlung historischer Daten zusammen. Eine Trennung zwischen SIM und SEM erfolgt heute in der Regel nicht mehr.

Zentralisierte IT-Sicherheit

SIEM-Lösungen kommen für zwei Einsatzbereiche in Frage. Ein Bereich ist die IT-Sicherheit. Hier spielen sowohl die Analysefunktionen als auch die längerfristige Sammlung von Informationen eine Rolle, wobei der Fokus typischerweise eher auf der laufenden Analyse von Ereignissen liegt.

Ein Vorteil von SIEM liegt unter anderem darin, dass der Sicherheitsverantwortliche nicht mehr die Protokolle und Ereignisse einzelner Systeme über jeweils proprietäre Schnittstellen und Werkzeuge verarbeiten muss, sondern eine Schnittstelle für alle IT-Anwendungen nutzen kann. Das unterstützte Spektrum reicht von Netzwerkgeräten wie Routern und Firewalls über Betriebssysteme, Netzwerkdienste und Datenbanken bis hin zu Anwendungen. Grundsätzlich lassen sich also alle relevanten Ereignisse auf allen Ebenen des Netzwerks zentralisieren und konsolidieren.

Der zweite wesentliche Vorteil liegt in der Korrelation von Ereignissen. Bedrohungen lassen sich oft früher oder einfacher erkennen, wenn Ereignisse auf verschiedenen Ebenen miteinander in Beziehung gesetzt werden. Angriffe von außen können sich bei der Firewall, auf Betriebssystemen und bei Datenbanken zeigen. Gerade mit Blick

S IEM steht für Security Information and Event Management. Der Begriff ist aus SIM und SEM entstanden, zwei ursprünglich getrennten Lösungsansätzen. Security Information Management zielt dabei auf die langfristige Archivierung und Analyse sowie auf die durch die gesammelten Daten erstellten Reporte von sicherheitsrelevanten Informationen ab, insbesondere von Log-Dateien und anderen Protokollen. Das schließt auch den Bereich des (Enterprise) Log Managements ein, also von Werkzeugen, die auf die Konsolidierung von Log-Dateien aus verschiedenen Systemen ausgerichtet sind.

Der zweite Bereich ist SEM, also das Security Event Management. Hier geht es um die Überwachung von Ereignissen in verschiedenen Systemen zur Laufzeit, also eine Real-Time-Analyse. Dazu gehört das Sammeln von Ereignissen, deren Korrelation auch über verschiedene Systeme hinweg, darauf basierenden Benachrichtigungen, Dashboards und anderen Formen der Anzeige. Diese Analyse basiert unter anderem auch wieder auf Informationen in Log-Dateien, aber auch auf Alerts und anderen Formen von Ereignisbenachrichtigungen, die von Systemen gesendet werden.

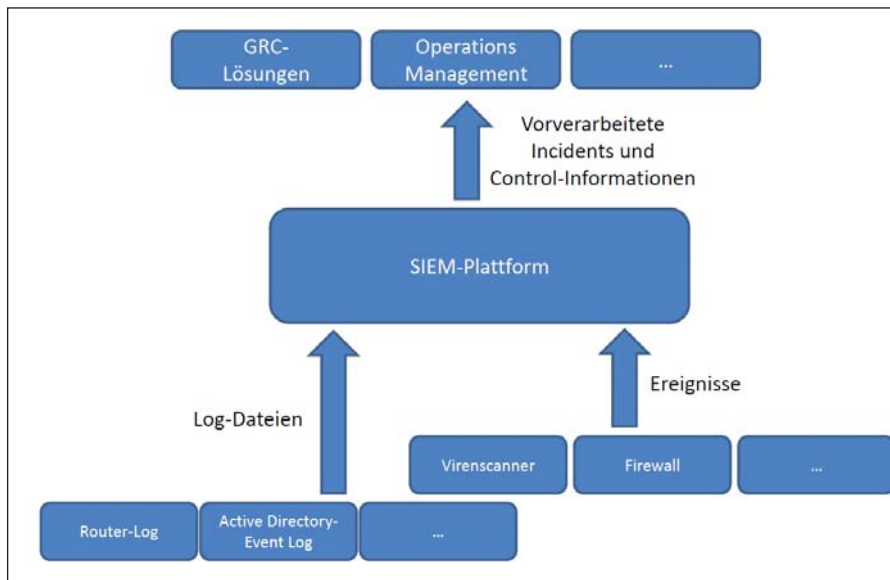


Bild 1: Die Entwicklung von SIEM aus SEM/SIM hin zu einer zentralen Schnittstelle für die Sammlung und Analyse von Ereignissen auch für andere Einsatzbereiche

auf die wachsende Bedrohung durch professionalisierte Angriffe, auch als APTs (Advanced Persistent Threats) bezeichnet, sind solche Korrelationen von Ereignissen von Bedeutung, um Angriffsmuster besser erkennen zu können.

SIEM-Werkzeuge sollen dabei helfen, kritische Situationen – und das umfasst nicht nur Angriffe, sondern auch Fehlfunktionen, Systemausfälle und dergleichen – zu erkennen und gezielt darauf zu reagieren. Das setzt eine entsprechende Konfiguration der Systeme voraus, was in Anbetracht der Vielzahl möglicher Ereignisse eine nicht zu unterschätzende Herausforderung darstellt. Darauf gehen wir weiter unten noch näher ein.

Forensik- und Compliance-Helfer

Die Datensammlung ist beim Sicherheitsmanagement oft nicht der primäre Fokus. Für die Ex-Post-Analyse von Vorfällen, also die Forensik, spielt sie aber auch hier eine nicht zu unterschätzende Rolle. So lassen sich über die archivierten Informationen beispielsweise Angriffe nachträglich nachvollziehen. Der IT-Verantwortliche kann aber auch erkennen, ob ein neu identifiziertes Angriffsmuster bereits früher vorgekommen ist. Insgesamt liegt der Schwerpunkt beim Einsatz von SIEM-Lösungen aus Gründen der IT-Sicherheit aber eher bei der ständigen Analyse von Ereignissen, um auf diese schnell und gezielt reagieren zu können.

Das zweite Haupteinsatzfeld liegt also eher bei der Archivierung von Informationen und darauf basierenden Reporten. Um Compliance-Anforderungen, also gesetzliche, aufsichtsbehördliche und auch unternehmensinterne Vorgaben, erfüllen zu können, sind die langfristige Aufbewahrung vieler sicherheitsrelevanter Informationen und gute Reporting-Funktionen erforderlich. Um bei Audits schnell Auskunft geben zu können, bedarf es leistungsfähiger Analyse- und Reporting-Funktionen. Diese müssen auch für vergangene Zeitpunkte Informationen liefern, also auf gespeicherte Daten zugreifen und diese effizient auswerten können.

Wichtiges Element des Risikomanagements

Die historische Analyse und die Unterstützung von Fragen von Prüfern ist allerdings nur ein Grund, warum SIEM-Lösungen in den vergangenen Jahren gerade auch durch den wachsenden Compliance-Druck populär geworden sind. Denn auch für umfassende GRC-Lösungen bedarf es einer laufenden Analyse von Ereignissen. GRC steht für Governance, Risk Management and Compliance und betrachtet die Erfüllung von Compliance-Anforderungen nur als einen Teil der Governance, also der korrekten Umsetzung der IT. Die Erkennung und Reduktion von Risiken ist ein zweiter Bereich. GRC arbeitet über die Definition von Controls als Steuerungselemente, deren Status regelmäßig manuell oder automatisch überprüft wird. Die Überschreitung von definierten Schwellenwerten ist als Incident (Vorfall) definiert und muss adressiert werden.

In solchen Modellen lassen sich für Sicherheitsrisiken Controls definieren, deren Status in definierten Intervallen oder permanent durch die SIEM-Lösungen aktualisiert wird. Ebenso können hier von SIEM-Systemen ausgelöste Ereignisse verarbeitet werden. SIEM ist damit eine wesentliche Quelle innerhalb von GRC-Modellen, um sicherheitsrelevante Ereignisse schnell und zuverlässig verarbeiten zu können. Die permanente Analyse ist damit

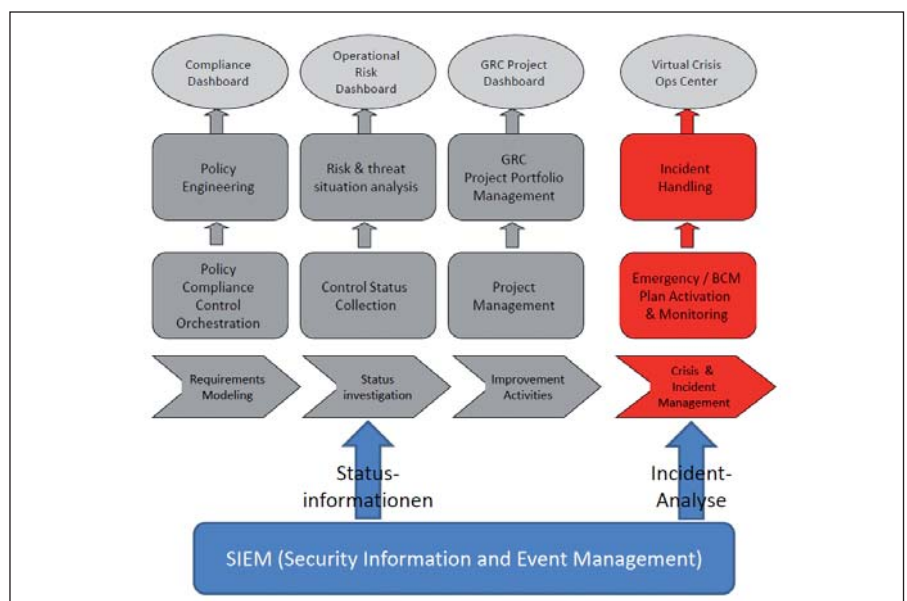


Bild 2: Innerhalb von GRC-Konzepten hat SIEM eine wichtige Bedeutung für die automatisierte Lieferung von Controls und die Identifikation von Incidents



auch für die Erfüllung von Compliance-Anforderungen und die Verringerung von Risiken von hoher Bedeutung.

Ergänzung zum Operations Management

Auch wenn die Produktkategorie die Bezeichnung SIEM trägt: Ihre Nutzung muss sich keineswegs auf den Bereich Sicherheit beschränken. Denn wer Log-Daten und Ereignisse einsammelt, korreliert und darauf basierend Ereignisse auslöst, kann dies natürlich auch für andere Informationen machen. SIEM-Lösungen stehen damit zumindest teilweise im Wettbewerb mit Lösungen für das Operations Management, die letztlich in genau der gleichen Weise arbeiten und dabei ja durchaus auch Sicherheitsereignisse verarbeiten können.

Allerdings sind Operations Management-Systeme im Gegensatz zu SIEM-Produkten für diesen Einsatzbereich mehr Lösung als nur reines Werkzeug. Schnittstellen zu vielen Produkten und den relevanten Protokolldateien sind vordefiniert. Zudem sind in Operations Management-Produkten Reaktionen auf bestimmte Ereignisse vorkonfiguriert und werden häufig auch durch eine ergänzende Wissensbasis unterstützt. Auch wenn die grundsätzliche Funktionalität von SIEM-Lösungen also der von Operations Management-Produkten entspricht, lassen sich mit spezialisierten Werkzeugen für das Operations Management in der Regel schnellere Ergebnisse erzielen. Die leistungsfähigen Korrelationsfunktionen führender SIEM-Produkte können auf der anderen Seite aber auch Möglichkeiten eröffnen, die sich in gängigen Operations Management-Lösungen, bei denen der Fokus eher auf einzelnen Ereignissen und einfachen Regeln für die Verknüpfung von Ereignissen liegt, so nicht eröffnen.

Werkzeug zur langfristigen Bedrohungsanalyse

Während sich der IT-Verantwortliche beim Operations Management heute genau überlegen muss, ob SIEM-Produkte die Anforderungen abdecken können oder doch spezialisierte Lösungen nötig sind, stellen APTs und verwandte, ausgefeilte Angriffsmodelle inzwischen einen der wichtigsten Gründe für viele Unterneh-

men dar, um in SIEM zu investieren. APT bezeichnet eine Gruppe von Angriffen auf Unternehmen sowie staatliche und nicht-staatliche Organisationen, die langfristig angelegt sind und mit einer Mischung unterschiedlicher Angriffstechniken und guter Planung darauf ausgelegt sind, längerfristige Ziele zu verfolgen.

Hinter solchen Angriffen stehen sowohl Staaten als auch terroristische und kriminelle Vereinigungen. Im Gegensatz zu klassischer Malware, die automatisiert und nur mit einem Konzept genutzt wird, lassen sich APTs häufig erst durch das kombinierte Auftreten verschiedener Vorfälle wirklich identifizieren. Hier kommen die systemübergreifenden, korrelierenden Funktionen von SIEM ins Spiel, weil sich damit auch komplexere Angriffsszenarien potenziell erkennen lassen.

Allerdings setzt dies voraus, dass die gesuchten Angriffe in ihrem Muster bekannt sind. Zudem reichen SIEM-Werkzeuge nicht unbedingt aus – es besteht davor gegebenenfalls Bedarf an weiteren Tools, von klassischen Signatur-basierten Virenskannern bis hin zu Systemen, die Angriffsmuster zu identifizieren versuchen, um basierend auf deren Ereignissen dann in einem SIEM-Werkzeug die Analyse durchführen zu können.

Herausforderung Konfiguration

Gerade der Umgang mit APTs ist ein Musterbeispiel für die größte Herausforderung beim Thema SIEM: SIEM ist nur ein Werkzeug. Und SIEM ist nur so gut wie das, was damit gemacht wird. Wer nicht weiß, nach was er suchen muss, findet auch nichts. Um beispielsweise APTs zu erkennen, ist ein sehr breites und tiefes Wissen darüber vonnöten, wie sich mögliche Angriffe in einer IT-Infrastruktur erkennen lassen und wie die verschiedenen Indizien zusammenhängen.

Die Kunst bei SIEM ist es also, möglichst genau die Ereignisse zu identifizieren, die kritisch sind. Letztlich stellen SIEM-Lösungen einen Filter zwischen der Gesamtmenge an Ereignissen und den manuell zu behandelnden Ereignissen dar. Daher ist zunächst Wichtiges von Unwichtigem zu trennen. Innerhalb der als wichtig identi-

fizierten Ereignisse richtet sich der Blick dann auf die Frage, welche davon automatisch behandelt werden können und welche eine manuelle Reaktion erfordern. Das Ziel muss sein, möglichst wenige, aber alle wesentlichen Ereignisse an die Experten zu übergeben, die sich mit diesem verbleibenden Rest beschäftigen müssen.

Die Herausforderung ist demnach, einerseits "false negatives" zu vermeiden, also sicherheitsrelevante Ereignisse auszufiltern. Andererseits sind auch die "false positives", also die als sicherheitsrelevant identifizierten Ereignisse, die das aber gar nicht sind, zu minimieren. Eine solche Konfiguration ist komplex und kann erfolgreich nur mit gutem Wissen zu den beteiligten Systemen, deren Events und möglichen Indikatoren für Sicherheitsbedrohungen erfolgen – und bei SIEM eben nicht nur mit Fokus auf ein System, sondern über eine heterogene, vielschichtige IT-Infrastruktur hinweg.

Die richtige Konfiguration und Nutzung von SIEM setzt in jedem Fall Experten voraus, die sich mit der IT-Sicherheit im Detail auskennen. Diese sind aber rar, denn dieses Wissen entsteht über Jahre hinweg und setzt Erfahrung voraus. Hinzu kommt, dass die Nachfrage nach solchen Experten derzeit sehr viel schneller wächst als das Angebot wachsen kann. Das führt zu zwei Ansätzen im Bereich SIEM: Managed Services und vorkonfigurierte Lösungen. Im ersten Fall erfolgen die Konfiguration und/oder Analyse durch externe Unternehmen und deren Experten. Im zweiten Fall werden Schnittstellen und Auswertungsregeln für verschiedene zu überwachende Systeme und die dort typischen Ansätze vorgegeben, um zumindest einen schnellen Einstieg und eine Art von "baseline security" zu ermöglichen.

SIEM boomt – und das hat gute Gründe. Die wachsenden Sicherheitsbedrohungen und immer mehr Compliance-Anforderungen führen dazu, dass eigentlich kein Weg an dem Werkzeug vorbeiführt. Allerdings ist SIEM noch längst keine Technologie, die sich einfach so nutzen lässt. Es braucht Expertise und ein hohes Maß an spezifischer Konfiguration. Zudem gilt es, SIEM-Lösungen richtig mit anderen

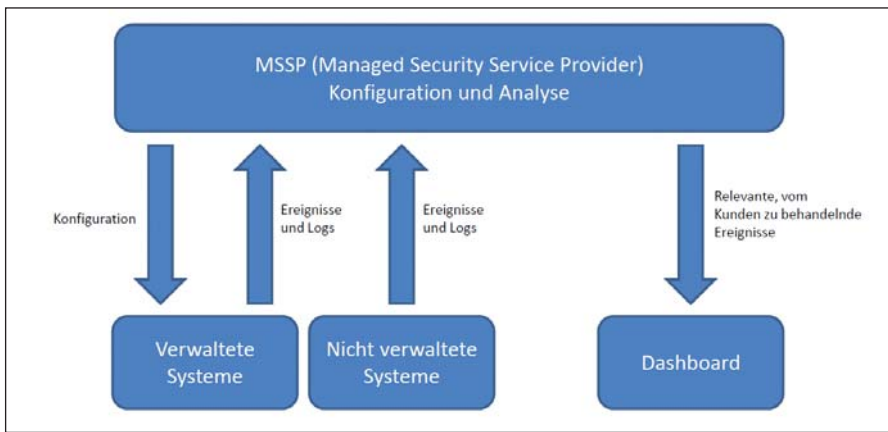


Bild 3: Managed Service-Modelle werden immer mehr an Bedeutung für effiziente SIEM-Ansätze gewinnen

Technologien im Unternehmen, von Firewalls und Virenscannern bis hin zu GRC-Lösungen, zu integrieren.

Die Zukunft von SIEM

Ein Indikator für den Status des Marktes ist die immer noch große Zahl von Herstellern. Derzeit gibt es deutlich mehr als 25 Anbieter von SIEM-Lösungen. Die Akquisitionen der letzten Monate zeigen dabei auch die in solchen Wachstumsmärkten typische Tendenz zur Konsolidierung. Immer mehr große Anbieter steigen in den Markt ein oder erweitern ihr Angebot. So hat IBM nach der Übernahme von Q1 Labs ein deutlich breiteres Lösungsangebot. McAfee ist durch den Kauf von NitroSecurity neu in den Markt eingestiegen, in dem sich mit Symantec bereits einer der direkten Wettbewerber des Unternehmens findet. Auch andere führende IT-Unternehmen wie HP, RSA oder Quest Software sind in diesem Marktsegment bereits unterwegs. Dennoch gibt es auch noch sehr viele Nischenanbieter und damit potenzielle Akquisitionsziele und spricht vieles dafür, dass sich der Markt in den kommenden zwei bis drei Jahren weiter konsolidieren wird. Zudem werden die Anbieter auch weiterhin intensiv in die Produktentwicklung investieren – gerade in einem so umkämpften Markt mit vielen kleinen und innovativen Anbietern entwickeln sich Produkte schnell weiter.

Darüber hinaus gibt es einige weitere Trends, die heute bereits absehbar sind. Einer ist die wachsende Bedeutung von Managed Services und Cloud-basierten Angeboten für SIEM. Immer mehr MSSP (Managed Security Service Provider) bie-

ten SIEM-Lösungen an, bei denen Experten die Konfiguration und Analyse übernehmen. Auch einige Hersteller haben bereits solche Angebote oder sind derzeit dabei, diese zu schaffen. Durch die Komplexität und die fehlende Verfügbarkeit von Experten wird auch die Nachfrage nach solchen Lösungsansätzen weiter zunehmen.

SIEM-Lösungen werden zunehmend mehr Integration erfahren. Die Integration mit GRC-Lösungen ist ein naheliegender Bereich, da SIEM wesentliche Informationen für automatisierte Controls liefert. Generell dürfte SIEM eine Entwicklung hin zu einer Drehscheibe für sicherheitsrelevante Ereignisse nehmen, bei der Informationen von einer wachsenden Zahl von Systemen – und gerade auch neuen Lösungen für die Erkennung bestimmter Bedrohungen – gesammelt und mit Log-Einträgen und anderen Informationen korreliert werden, um eine Gesamtsicht auch auf komplexe Bedrohungsszenarien zu erhalten – und gleichzeitig Daten an darüber liegende Anwendungen wie eben GRC-Frameworks oder auch Operations Management-Systeme zu liefern.

Ein dritter Bereich ist ein wachsendes Angebot an Anwendungslösungen auf Basis von SIEM-Technologien. So nutzt beispielsweise der deutsche Anbieter IT-Cube die Entwicklung von ArcSight für seine spezialisierte Lösung für das SAP-Umfeld. Genauso ist es vorstellbar, dass spezielle Operations Management-Lösungen auf Basis von SIEM-Technologien entstehen. Der Plattform-Charakter vieler SIEM-Lösungen ist eine gute Basis

für Szenarien, mit denen spezielle Anwendungsfälle abgedeckt werden.

Mit der wachsenden Bedeutung als zentrales Element in der Bedrohungsanalyse und für die Erfüllung von Compliance-Anforderungen werden SIEM-Lösungen allerdings auch immer mehr zu einem potenziellen Angriffsziel. Angreifer könnten diese Produkte attackieren, um Spuren zu verwischen. Deshalb, aber auch wegen der Sensitivität der darin enthaltenen Informationen, sind durchdachte Sicherheitskonzepte ein wesentliches Entscheidungskriterium bei der Auswahl von Produkten in diesem Marktsegment.

Fazit

Der Markt ist, wie erwähnt, kräftig am Wachsen. Durch die Vielzahl von Anbietern, die hohe Innovationsgeschwindigkeit und die Tendenz zu Übernahmen von Herstellern in diesem Segment ist die Auswahl von Lösungsanbietern allerdings mit einem nicht unerheblichen Risiko verbunden. Das lässt sich natürlich durch MSSPs abfedern, um einen bestimmten Service zu nutzen, dabei aber nicht selbst die Technologieentscheidung, deren Konfiguration und den Betrieb leisten zu müssen.

Viel wichtiger als das Tool ist aber, dieses auch richtig zu nutzen. Hier liegt die eigentliche Herausforderung bei SIEM. Denn das beste Werkzeug ist nichts wert, wenn es nicht richtig eingesetzt wird. SIEM kann vieles, bedarf aber eines hohen Maßes an Expertise. Wer wichtige sicherheitsrelevante Ereignisse nicht erkennt oder mit zu vielen tatsächlich unkritischen Ereignissen konfrontiert wird, für den liefern SIEM-Werkzeuge bestenfalls einen geringen Mehrwert. Die Expertise der Anbieter, Integratoren oder auch MSSPs muss daher eines der wichtigsten Elemente in Auswahlentscheidungen sein.

Dennoch wird kaum ein IT-Verantwortlicher auf Dauer an solchen Lösungen vorbeikommen. Denn sowohl die Sicherheits- als auch die Compliance-Anforderungen machen eine integrierte Sicht auf sicherheitsrelevante Ereignisse und leistungsfähige Analysefunktionen für historische Daten sowie deren korrekte, langfristige Speicherung zu einer Notwendigkeit. (In)

Kostenlose Android-Apps für Administratoren

Mini-Jobber

von Sandro Lucifora

Mittlerweile ist das Telefonieren mit einem Mobiltelefon nur noch eine von vielen Möglichkeiten, das Gerät zu nutzen. Vielmehr stehen immer mehr Apps bereit, die dem Administrator im Arbeitsalltag hilfreich sind. IT-Administrator stellt zehn nützliche und kostenlose Apps aus den Bereichen Monitoring und Fernwartung vor.

Das erste Kriterium unserer Übersicht ist der Nutzwert für den Administrator. Die von uns zusammengestellte Auswahl enthält ausschließlich kostenlose Apps, die die tägliche Arbeit erleichtern und den Einsatzort des IT-Spezialisten unabhängiger machen. Dabei haben wir uns zunächst auf Apps konzentriert, die im Android Market zum Download zur Verfügung stehen. Die Kurzvorstellungen ergänzen wir am Ende des Beitrags mit einer Übersicht der technischen Anforderungen der Apps – unserem Android-Steckbrief.

Netzmanagement mit LanDroid 1.2

Der Entwickler von LanDroid bezeichnet seine App als ein Schweizer Messer mit Netzwerktools. Die App kommt ohne Werbung aus und liefert eine Vielzahl von Informationen des Netzwerks, in das sich das Smartphone per WLAN einloggt. Weiterhin erhalten wir die Routinginforma-

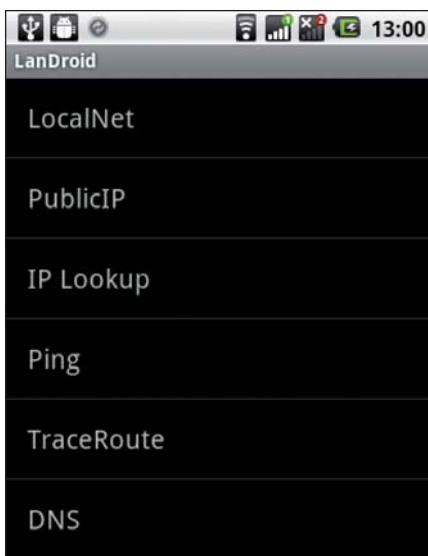


Bild 1: LanDroid bietet eine ganze Reihe bewährter Netz-Tools

tionen des lokalen Netzwerks und die öffentliche IP des Routers.

Mit IP-Lookup, DNS-Lookup und Whois erfahren Sie mehr über den Standort und den Eigentümer von beliebigen IPs und Domains. Ping und TraceRoute geben Informationen zur Zugriffszeit und dem Routing zu einem Netzwerkgerät aus. Für die Betreiber eines eigenen Mailservers ist die Überprüfung einer IP auf den SpamBlacklists sehr hilfreich. Lediglich den IPv6-Support vermissen wir (noch), den der Entwickler zugunsten der Performance nicht implementiert hat.

Netzanalyse mit Fing Network Tools 1.25

Fing prüft und scannt das lokale Netzwerk, so dass sich Probleme schnell erkennen und die Ursachen finden lassen. Nach dem Start und dem ersten Scan zeigt das Tool alle im Netzwerk angemeldeten Geräte an und listet Grundinformationen wie Adressraum, Gateway, ISP et cetera auf. Der Wechsel auf die Anzeige des Gerätes gibt wiederum Basisdaten zu dem Anschluss aus und erlaubt das weitere Scannen der offenen Ports. Anschlüsse wie SSH, Telnet, FTP, FTPS, SFTP, SCP, HTTP, HTTPS, SAMBA werden wiederum auf ihre Funktion getestet. Eine Wake-On-LAN-Funktion rundet die Möglichkeiten ab. Fing ist auch für Windows, Linux und Mac erhältlich.

Remote-Support mit TeamViewer 7.0

Neben RDP und VNC hat sich TeamViewer als Remote-Software etabliert. Mit der App lassen sich Clients von unterwegs aus fernsteuern. Der Vorteil ist, dass die Verbindung auch hinter jeder Firewall – über den



Bild 2: Mit Fing lassen sich unter anderem offene Ports scannen

Internet-Port 80 – aufgebaut wird. Dazu muss auf dem entfernten Computer der für den Privatgebrauch kostenlose TeamViewer-Client installiert sein.

Über die TeamViewer-ID und das generierte Kennwort oder die Partnerliste – in der sich Computer automatisch für die Fernwartung anmelden – greifen wir auf den Desktop zu. Die Bedienung ist nicht ganz so intuitiv, da der linke und rechte Mausklick sowie das Sliden des Bildschirms mit den Fingern umgesetzt werden. Die vollwertige Bildschirmtastatur sowie der Zugriff auf alle (virtuellen) Sondertasten und Tastenkombinationen ermöglichen einen Zugriff aus der Ferne. So lässt sich beispielsweise ein Server von unterwegs aus neu starten oder ein Kennwort neu setzen. Mit der TeamViewer-App muss nicht immer das Notebook dabei sein.



Bild 3: Das bekannte TeamViewer ist kostenlos als App zu haben

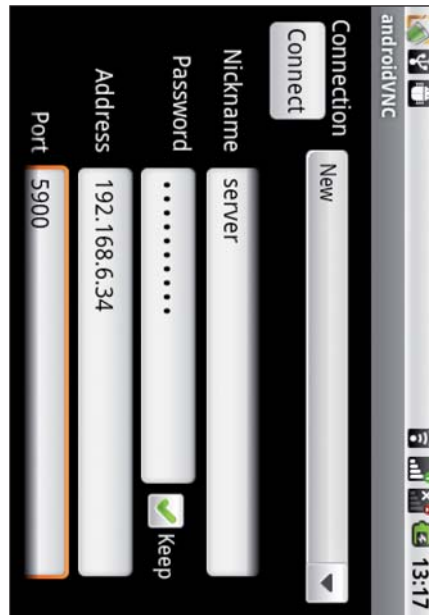


Bild 4: Wer Rechner remote über VNC verwalten möchte, sollte den android-vnc-viewer testen



Bild 5: Mit PC Monitor 2.7 lässt sich sogar das Active Directory überwachen

VNC-Fernzugriff mit android-vnc-viewer 0.5

Wer seine Computer und Server statt mit RDP oder TeamViewer über VNC fernsteuern möchte, findet mit dem android-vnc-viewer eine freie Alternative zu der kostenpflichtigen App von RealVNC. Nach der Installation verbindet sich die App zu den meisten bekannten VNC-Servern wie TightVNC und RealVNC unter Windows und Linux als auch mit dem Apple Remote Desktop.

Die Bedienung des entfernten Computers ist etwas gewöhnungsbedürftig aufgrund des Handlings mit der Maus und dem Verschieben des Bildschirms. Der Einsatz der virtuellen Tastatur ist auf dem Smartphone nur in der senkrechten Position sinnvoll, da sie fast den ganzen Bildschirm bedeckt. Uns hat die verhältnismäßig gute Darstellung und Zugriffszeit über UMTS gefallen sowie die flüssige Zoom-Funktion.

Umfassender Support dank PC Monitor 2.7

Ein Administrator sollte immer über den Zustand der von ihm zu wartenden Computer informiert sein. PC Monitor ist eine App, die auf dem Smartphone und dem Tablet eine umfangreiche Übersicht des Zustands aller registrierten Geräte liefert.

Zunächst ist auf den zu überwachenden Computern die Client-Software zu in-

stallieren und ein Account am PC Monitor-Server anzulegen. Darüber tauschen App und Client ihre Informationen aus. Mit der kostenlosen Version lassen sich bis zu drei Geräte anmelden und überwachen. Der gesamte Datenaustausch zwischen Windows-Computer, Server und App erfolgt dabei verschlüsselt.

Nach dem Start meldet sich die App ebenfalls am Server an und empfängt die bereitgestellten Informationen, etwa den Status und die Laufzeit des Computers als auch die Belastung der CPU und des Speichers. Die Zustände der lokalen Festplatten und des Netzwerkinterfaces sowie die Einsicht in die laufenden Prozesse und Hardware-Details sind weitere hilfreiche Auskünfte. Der IIS wird ebenso überwacht wie das Active Directory.

Für die schnelle Lösung von Problemen übertragen IT-Verantwortliche über die App auch direkt Befehle etwa zum Starten und Stoppen von Services als auch zum Beenden von Prozessen. Auch der Restart, Wake-on-LAN und andere Power-Aktionen helfen, von unterwegs etwaige Schwierigkeiten zu lösen.

Gut gefällt an der App, dass Administratoren über sie auch Teile des Active Directory verwalten und beispielsweise User-Passwörter entsperren, aktivieren und neu setzen können. Das Management für Exchange-, Hy-

per-V und VMware-Server macht die App zum Allrounder, um schnelle Lösungen für Probleme von unterwegs zu schaffen. Wer am Arbeitsplatz auch alles im Blick haben will, nutzt auf seinem Desktop das PC Monitor Dashboard für Windows.

Overlook Whiz 1.3 testet Server-Verfügbarkeit

Overlook Whiz ist ein Widget für den Homescreen des Smartphones oder Tablets. Es zeigt die Erreichbarkeit eines Servers im Internet oder LAN an. Üblicherweise wird ein Webserver mit dem Tool überwacht, aber auch andere Dienste auf



Bild 6: In Grün signalisiert Overlook Whiz 1.3 die gegebene Erreichbarkeit definierter Dienste

jedem erreichbaren Port, wie SMTP und POP3, lassen sich monitoren.

Das kleine Tool erstellt für jede zu überwachende IP-Port-Kombination auf dem Homescreen ein Widget. Es zeigt die Erreichbarkeit in grün, gelb oder rot an. Ein Webserver lässt sich so nicht nur auf die Erreichbarkeit des Ports, sondern auch auf den Inhalt der Rückmeldung prüfen. Sehr hilfreich ist es, dass der Nutzer festlegen kann, ob ein Test nur mit einer bestimmten WLAN-Verbindung erfolgen soll – so werden zum Beispiel tagsüber im Unternehmens-LAN auch lokale Server in das Monitoring eingebunden.

Erreichbarkeits-Test mit Server Monitor 1.0

Auch Server Monitor ist eine App, die die Erreichbarkeit von Servern überwacht, jedoch mit einem anderen Konzept als Overlook Whiz arbeitet. Server Monitor zeigt auf dem Homescreen ein Widget, in dem die zuvor konfigurierten Hosts zusammengestellt und angezeigt werden, was übersichtlicher ist. Die Einstellungen beschränken sich jedoch auf den Anzeigenamen, die IP oder URL und die Art der Verbindung wie HTTP, TCP oder ECHO. Über die Einstellungen lässt sich noch die Refreshzeit



Bild 7: Kein optisches Wunderwerk, aber eine schlanke Diagnose-App ist Server Monitor

der Widgets festlegen. Ein Ping, Trace und nslookup auf das Netzwerkgerät ergänzen die Funktionen. Für einen reinen Erreichbarkeits-Test für Geräte im Internet ist das Tool eine schlanke Lösung.

Website-Diagnose mit WebCheck 1.7

Für mehr als nur einen Test auf Erreichbarkeit einer Webseite ist WebCheck



Bild 8: Für Webserver-Verantwortliche bietet die App WebCheck erstaunliche Überwachungsfunktionen

ausgelegt. Diese App prüft nicht die Verbindung, sondern den Inhalt einer Internetseite und schlägt beim Auslesen eines zuvor definierten Wortes Alarm. Die Möglichkeiten sind damit sehr vielfältig: So ist es beispielsweise möglich, in einem Shop-System den Inhalt einer Seite auf das Wort “MySQL” zu prüfen. Sobald die Verbindung zum Datenbankserver fehlschlägt, gibt das PHP-Skript

Übersicht Android-Apps

App	Lauffähig ab	Smartphone / Tablet	App auf SD-Karte	Notwendige Berechtigungen
LanDroid 1.2	Android 2.1	ja / ja	ja	Netzwerkstatus anzeigen
Fing 1.25	Android 2.1	ja / ja	ja	Uneingeschränkter Internetzugriff, Inhalt des USB-Speichers und der SD-Karte ändern/löschen, Standby-Modus deaktivieren
TeamViewer 7.0	Android 1.6	ja / ja	ja	Uneingeschränkter Internetzugriff, Telefonstatus lesen und identifizieren, WLAN-Status anzeigen, Standby-Modus deaktivieren
android-vnc-viewer 0.5	Android 1.5	ja / ja	nein	Uneingeschränkter Internetzugriff, Inhalt des USB-Speichers und der SD-Karte ändern/löschen
PC Monitor 2.7	Android 2.0	ja / ja	nein	Uneingeschränkter Internetzugriff, Telefonstatus lesen und identifizieren, Netzwerkstatus anzeigen
Overlook Whiz 1.3	Android 2.1	ja / ja	nein	Uneingeschränkter Internetzugriff, Telefonstatus lesen und identifizieren, Standby-Modus deaktivieren, WLAN-Status ändern, Vibrationsalarm steuern, Netzwerkstatus anzeigen, WLAN-Status anzeigen
Server Monitor 1.0	Android 2.1	ja / ja	nein	Uneingeschränkter Internetzugriff, Netzwerkstatus anzeigen
WebCheck 1.7	Android 2.1	ja / ja	nein	SMS senden, uneingeschränkter Internetzugriff, Inhalt des USB-Speichers und der SD-Karte ändern/löschen, Standby-Modus deaktivieren, Vibrationsalarm steuern, Lichtanzeige steuern, automatisch nach dem Booten starten
ConnectBot 1.7	Android 1.5	ja / ja	ja	Uneingeschränkter Internetzugriff, Inhalt des USB-Speichers und der SD-Karte ändern/löschen, Vibrationsalarm steuern, Netzwerkstatus anzeigen
Plesk Monitor 1.0	Android 2.0	ja / ja	nein	Uneingeschränkter Internetzugriff, Telefonstatus lesen und identifizieren, Netzwerkstatus anzeigen



Bild 9: Willkommen auf der Kommandozeile:
ConnectBot bietet SSH für die Linux-Konsole

eine Warnmeldung mit diesem Wort aus und WebCheck erkennt sofort den Fehler. Das lässt sich mit einem reinen Erreichbarkeits-Check nicht umsetzen.

Ebenso können Administratoren die Seite eines Internetauftritts mit dem Wort "Found" prüfen. Dieses ist Teil der Fehlermeldung "Not Found", die ausgegeben wird, sofern eine aufgerufene Seite nicht angezeigt werden kann. Alternativ wird der Alarm auch ausgelöst, wenn ein Wort nicht mehr zurückgemeldet wird.

Gut gefällt an der App, dass die Alarmmeldung über die Statusbar des Smartphones angezeigt wird und sich auch auf Wunsch mit einem Ton und dem Vibrieren bemerkbar macht. Das bietet keine der anderen Apps. Mit WebCheck können eine Webseite oder Foren und eCommerce-Lösungen sogar auf die richtige Funktion überwacht werden.

SSH mit ConnectBot 1.7

Neben dem Zugriff auf Windows- und Mac-Desktops stehen Administratoren auch immer wieder vor der Aufgabe, per SSH zum Beispiel eine Linux-Konsole zu bedienen. Um auch unterwegs beispielsweise einen cronjob zu administrieren oder neue Linux-User anzulegen, bietet sich die einfache, aber wirksame App ConnectBot an.

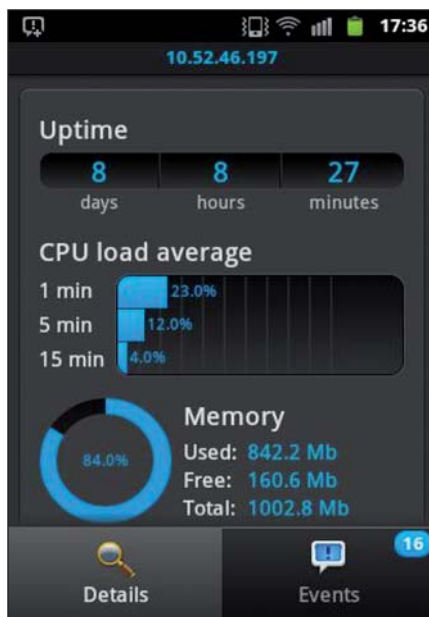


Bild 10: Optisch schick, doch funktional
noch ausbaufähig ist der Plesk Monitor

Sie ist in ihrer Einfachheit und ihrem Nutzen mit Putty auf Windows-Computern zu vergleichen. ConnectBot ist ein SSH-Client, der mehrere verschiedene SSH-Sitzungen verwalten und getunnelte Verbindungen herstellen und nutzen kann. Sind mehrere SSH-Verbindungen offen, lässt sich sogar bequem zwischen ihnen hin und her wechseln. Auf dem Smartphone ist die Anwendung wirklich nur im Notfall sinnvoll, auf dem Tablet hingegen lassen sich auch umfangreichere Server-Konfigurationen via SSH vornehmen.

Webserver-Administration mit Plesk Monitor 1.0

Sehr viele Hostler bieten die Administration ihrer Webserver über die Oberfläche Plesk von Parallels an. Wer einen solchen Server administriert, bekommt mit dem neuen Plesk Monitor eine hilfreiche App an die Hand. Ab der Plesk Panel Version 10.4 kann die App alle Statusinformationen des Servers abrufen und anzeigen.

Allerdings fehlt eine optische und akustische Meldung, wenn ein zuvor eingestelltes Ereignis eintritt – wie der Ausfall eines Dienstes oder der Ablauf einer Lizenz. Bisher hat die App noch wenig Inhalt, ist aber ein guter Anfang, dem hoffentlich noch viele Updates und Erweiterungen folgen werden. (jip)

Worüber Administratoren morgen reden

Sichern Sie sich den
E-Mail-Newsletter des
IT-Administrators und
erhalten Sie Woche für
Woche die

- neuesten TIPPS & TRICKS
- praktischsten TOOLS
- interessantesten WEBSITES
- unterhaltsamsten GOODIES

sowie einmal im Monat
die Vorschau auf die
kommende Ausgabe des
IT-Administrators!

Jetzt einfach und kostenlos
bestellen unter:



www.it-administrator.de/newsletter



Stresstest für Virens Scanner selbst gemacht

Leistungsnachweis

von Ralph Dombach



Quelle: Maksym Yemelyanov - Fotolia.com

Virens Scanner gehören schon lange zur Grundausstattung im Bereich IT-Sicherheit. Zu groß ist das Risiko, um auf diese Maßnahme zu verzichten. In den meisten Fällen wird die Schutzsoftware auf die Unternehmensrechner verteilt, ohne die einwandfreie Funktion im Nachhinein tatsächlich zu überprüfen. Dabei kann durch falsche Einstellungen oder fehlerhafte Software schnell eine Sicherheitslücke aufreißen oder wichtige und saubere Programme werden abgeschossen. Wie Sie Ihre Antivirus-Software leicht selbst testen, zeigt dieser Workshop.

In der Regel arbeiten die Viren-Wächter ohne Probleme und verrichten unauffällig ihren Dienst. Doch was passiert, wenn der Scanner anfängt, legitime Programme als gefährlich einzustufen oder Viren unter bestimmten Umständen gar nicht erst sucht? Mit einem einfachen Testszenario schauen Sie Ihrem Antivirus bei der Arbeit auf die Finger.

Aktuelle Erkennungsmethoden basieren unter anderem auf

- einer heuristischen Erkennung (Code ähnelt dem eines anderen Virus)
- einer Sandbox zur testweisen Ausführung von Programmen
- dem Ausführen einer Hash-Prüfung
- der Analyse des Programmverhaltens
- Bytemustern für bekannte Viren
- und/oder weiteren, herstellereigenen Verfahren.

Diese Detektionsmethoden sind technisch durchaus anspruchsvoll in der Umsetzung und auf hohen Datendurchsatz ausgelegt, denn der Virens Scanner soll die

Performance natürlich möglichst wenig beeinträchtigen. Zusammen mit täglich zigtausend neuen Virusdefinitionen ergibt sich so ein komplexes Gebilde, das leider auch fehleranfällig ist. Selten, aber immer wieder mal, rutschen Probleme unerkannt durch die Qualitätskontrollen der Antivirus-Hersteller.

Machbarer Testumfang

Sie könnten natürlich alles Mögliche testen und den Herstellern in ihrem eigenen Umfeld durchaus Konkurrenz machen. Doch das sollte professionellen Testinstituten wie AV-Test oder AV-Comparatives vorbehalten bleiben. Für das Unternehmen müssen Stichproben genügen, die mit überschaubaren Mitteln realisiert werden, aber trotzdem grobe Probleme entlarven. Typische Testszenarien sind

- korrektes Erkennen der Schadsoftware
- das Vermeiden von False Positives
- der Produkt-Selbsttest (funktioniert der On-Access- und On-Demand-Modus?)
- Fehler-Korrekturverfahren, wie das Rollback zu einer früheren Virus-Definitionsdatei

Prinzipiell gilt: Je mehr Schadsoftware erkannt wird, desto besser die Erkennungsqualität der eingesetzten Virenschutzsoftware. Allerdings ist von einem Test mit echten Computerviren aufgrund der damit verbundenen Sicherheitsrisiken abzuraten. Alternativ sollten Sie hier auf das harmlose Testvirus "EICAR" [1] zurückgreifen. Dabei handelt es sich um eine Datei, die keinen tatsächlichen Virus enthält, aber deren Signatur von quasi allen Antiviren-Herstellern zu Testzwecken erkannt wird.

Die Einschränkung dabei ist, dass mit dem EICAR-Testfile nur eine Art der Viruserkennung getestet werden kann – in der Regel die auf einem definierten Bytemuster basierende. Besser wäre es, weitere Testfiles zu nutzen, die andere Erkennungsmethoden ansprechen. Diese sind zumindest nach unserer Kenntnis nicht frei verfügbar. Doch auch mit dem EICAR-Testfile lässt sich ein guter Stresstest durchführen. Voraussetzung dafür ist, dass Sie den Überlegungen der Virenprogrammierer folgen und das Testfile jeweils in einer anderen Verpackung präsentieren. Im Download-Bereich der EICAR-Webseite wird das Testfile bereits in unterschiedlichen Verpackungen an-



Bild 1: Unter den Antivirus-Herstellern ist es fester Standard, den Zugriff auf die EICAR-Testdatei zu blockieren

geboten. Als klassisches COM-File, mit einer doppelten Erweiterung (.com.txt) und in einem ZIP-Archiv. Weitere Methoden, um das Testfile zu verpacken, wären beispielsweise die Nutzung anderer Komprimierungsprogramme, das Konvertieren in andere Formate oder das Einbinden in Dokumente oder Dateien. Der eigenen Kreativität sind hier kaum Grenzen gesetzt. Einzige Bedingung ist, dass die Datei auf einem Standard-PC ausführbar sein muss. Denn ohne Ausführung gibt es auch keine Aktion und/oder Ausbreitung. Die Verpackung sollte dabei effektiv und verlockend sein, darf aber den durchschnittlichen Anwender auch nicht übermäßig daran hindern, sein infiziertes File zu öffnen.

Keine False Positives

Ein False Positive liegt dann vor, wenn eine Datei fälschlicherweise als Schadsoftware identifiziert ist. Problematisch wird dies dann, wenn in der Virens Scanner-Konfiguration festgelegt ist, bei einem Virusbefund die Datei automatisch zu löschen oder in einen geschützten Quarantänebereich zu verschieben. Dies führt dann im Ereignisfall dazu, dass eine Anwendung nicht mehr lauffähig ist, weil auf einmal Komponenten fehlen oder der Zugriff darauf durch den Virens Scanner blockiert wird. Welche Auswirkungen dies für die Steuerung einer Fertigungsstraße oder ein Aktienhandels-System

hat, kann sich jeder selbst ausrechnen.

Die Hersteller führen umfangreiche Qualitätstests durch und nutzen verstärkt auch Cloud-Angebote, um die Mehrzahl der existierenden Dateien sicher zu erkennen. Doch viele selbstentwickelte und wenig bekannte Tools und Programme sind davon oft ausgeschlossen. Daher empfiehlt es sich, Nicht-Standardsoftware, die im eigenen Unternehmen genutzt wird,

im Stresstest auf False Positives zu testen. Analog zu den EICAR-Dateien kopieren Sie die entsprechenden Dateien in den Stresstest-Folder. Als Empfehlung gilt hier, zumindest die EXE- und DLL-Dateien zu kopieren. Falls weitere ausführbare Dateien (*.scr, *.com, *.shs etc.) vorhanden sind, sollten Sie diese auch kopieren. Nutzen Sie im Unternehmen eine veraltete Business-Software, so soll-

ten Sie diese auch für den Test heranziehen, da unter Umständen fünf Jahre alte Software bei den Qualitätstests der AV-Hersteller keine Rolle mehr spielt.

Sollte dann der Virens Scanner im Stresstest-Folder eine Schadsoftware entdecken, so liegt hier gegebenenfalls eine Falschmeldung vor. Zur Bestätigung empfiehlt es sich, die infizierte Dateien mit einem Multi-Produkttester wie VirusTotal [2] zu prüfen. Findet nur Ihr verwendetes AV-Produkt etwas, liegt vermutlich ein False Positive vor. In diesem Fall bietet es sich an, den Antivirus-Hersteller zu informieren und auf eine Behebung der Falschmeldung zu drängen. Bestätigen auch die anderen Antiviren-Programme den Fund, sollten Sie sich die entsprechende Datei in Zusammenarbeit mit dem AV-Hersteller näher ansehen.

Virenerkennung testen

Üblicherweise nutzen Antiviren-Scanner zwei unterschiedliche Arbeitsweisen: den On-Access- und den On-Demand-Scan. Bei einem On-Access-Scan (OAS) findet die Überprüfung einer Datei zu dem Zeitpunkt statt, zu dem ein Zugriff auf sie stattfindet. Also beispielsweise

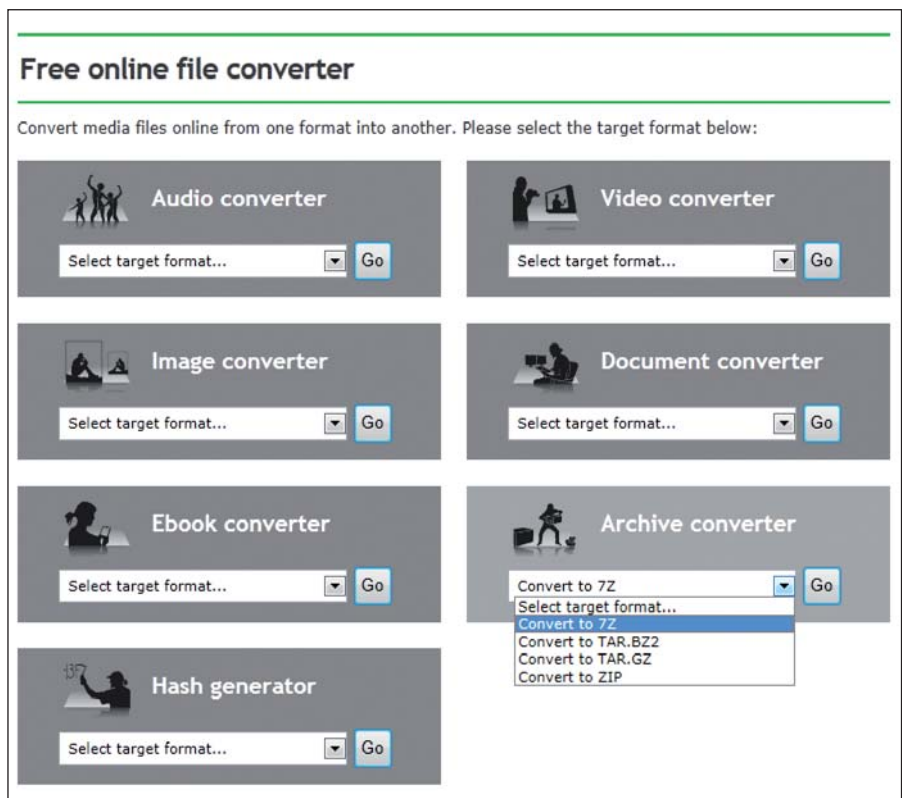


Bild 2: Mit Online-Konvertern können Sie ohne zusätzliche Software Dateien in neue Formate umwandeln



wenn die Datei geöffnet wird, um sie zu lesen, zu beschreiben oder zu kopieren. Der On-Demand-Scan (ODS) findet dagegen auf Anforderung oder nach einem definierten Zeitplan statt und überprüft in der Regel alle infizierbaren Dateien. Bei beiden Varianten gilt, dass der Virens Scanner die Dateitypen prüft, die als prüfenswert definiert sind: direkt oder indirekt ausführbare Dateien. Ein klassischer Fehler wäre es, bei der Virens Scanner-Konfiguration versehentlich EXE-Dateien von der Überprüfung auszuschließen. Denn dann könnte sich jede beliebige Malware, die auf EXE-Dateien basiert, ungehindert ausbreiten, da die Quelle und weitere Ziele nicht geprüft werden.

Im Rahmen eines Stresstests sind beide Arbeitsweisen zu testen. Für den On-Access-Scan müssen daher alle Dateien, die direkt ausführbar sind, aufgerufen werden. Dies lässt sich durch ein Skript einfach bewerkstelligen. Idealerweise werden auch die Komponenten berücksichtigt, die nicht direkt aufrufbar sind. Dies ist etwa bei einem Archiv der Fall, das per Aufruf entpackt wird. Funktioniert der OAS, wird der Scanner die entpackte Datei im Falle einer Infektion als Schadsoftware markieren. Für den ODS starten Sie das Antivirenprodukt und überprüfen den entsprechenden Stresstest-Folder auf Malware. Auch hier sollten alle Files untersucht werden, die direkt ausführbar sind. Je nach Qualität des Produktes werden aber auch Archive und andere Verpackungen unter die Lupe genommen.

Eigenes Testpaket schnüren

Für den schnellen Test in der eigenen Umgebung können Sie zehn Testfiles erstellen. Deaktivieren Sie den lokalen PC-Virens Scanner für den Zeitraum, in dem Sie die EICAR-Köderdateien erstellen und verpacken. Ebenso sollten Sie daran denken, den Windows Defender zu stoppen, falls dieser Schutz aktiviert ist. Sollte dies Ihre Security-Policy nicht erlauben, nutzen Sie alternativ einen virtuellen PC, der ohne Virens Scanner läuft. Denken Sie daran, nach Abschluss Ihrer Arbeiten den Scanner wieder zu aktivieren. Über die EICAR-

Name	Änderungsdatum	Typ	Größe
01_eicar	25.09.2011 11:49	MS-DOS-Anwend...	1 KB
02_eicar.com	25.09.2011 11:49	Textdokument	1 KB
03_eicar_com	25.09.2011 11:49	ZIP-komprimierte...	1 KB
04_eicarcom2	25.09.2011 11:50	ZIP-komprimierte...	1 KB
05_eicar.rd_	25.09.2011 11:49	RD_-Datei	1 KB
06_eicar.7z	25.09.2011 12:35	7Z-Datei	1 KB
07_eicar_2010-eingebettet	25.09.2011 12:23	Microsoft Word-D...	21 KB
08_eicar_2010-eingebettet	25.09.2011 12:24	Adobe Acrobat D...	127 KB
09_eicar_wo97-eingebettet	25.09.2011 12:24	Microsoft Word 9...	29 KB
10_eicar_rar.rar	25.09.2011 18:40	RAR-Datei	1 KB

Bild 3: Die zehn Files des Eicar-Testsets sind in gängige Formate eingebettet

Homepage erhalten Sie bereits vier Dateien, die Sie verwenden können: *ecar.com*, *ecar.com.txt*, *ecar_com.zip* und *ecarcom2.zip*.

Die fünfte Datei erstellen Sie, indem Sie das File Nummer 1 umbenennen von *ecar.com* auf *ecar.rd_* – also als Dateinamenserweiterung einen nicht genutzten String verwenden. Die sechste Datei legen Sie an, indem Sie eine der bestehenden Dateien in ein 7z-Archiv umwandeln. Diese Aufgabe erleichtern zuverlässig diverse Online-Tools [3] im Web. Embedded Dateien sollten auch zum Testset gehören. Die siebte Test-Datei erstellen Sie, indem Sie in ein Textdokument die Datei 1 einfügen. Um die achte Datei anzulegen, konvertieren Sie die Datei 7 beispielsweise in eine PDF-Datei. Dies erledigt in der Regel das Textsystem selbst oder alternativ ein Online-Tool. Sinnvoll ist es auch, alte Textformate zu testen. Für die neunte Datei kann die aktuelle Textdatei mit eingebettetem Inhalt in einer Vorgänger-Version abgespeichert werden. Schließlich nutzen Sie für die Datei Nummer 10 ein alternatives Archivformat. Dazu konvertieren Sie wiederum mit einem Online-Tool das ZIP-Archiv in ein RAR-File.

Resultate auswerten

Im bestmöglichen Fall werden alle EICAR-Köderdateien als solche erkannt und unternehmenseigene Tools und Anwendungen bleiben ohne Befund. Bei diesem Ergebnis können Sie die aktuelle Definitionsdatei freigeben und im Unternehmen verteilen. Wichtig ist, bei einem Stresstest darauf zu achten, dass dieser schnell ein Resultat liefert. Denn mit jeder Minute, die eine neue Virus-Definitionsdatei verzögert installiert wird,

steigt das potenzielle Risiko, Opfer einer Schadsoftware zu werden. Primär wird der erforderliche Zeitbedarf dabei von der Anzahl unternehmenseigener Tools und Anwendungen bestimmt. Je höher die Anzahl, desto länger benötigt der Virens Scanner zur Überprüfung und damit der Stresstest zur Abarbeitung. Ein akzeptabler Wert ist alles, was innerhalb einer Stunde erledigt werden kann. Genügt diese Zeit nicht, sollten Sie versuchen, den Stresstest auf mehrere Systeme zu verteilen oder den Testlauf durch optimierte Hardware und Software zu beschleunigen. Auf keinen Fall sollten Sie überlegen, unternehmenseigene Tools und Anwendungen aus dem Stresstest zu entfernen, wenn diese noch genutzt werden. Denn jede neue Virus-Definitionsdatei kann andere Ergebnisse liefern.

Mit diesen zehn Dateien haben Sie die Basis für Ihren eigenen Stresstest gelegt. Für Erweiterungen Ihres Testsets berücksichtigen Sie weitere Archive und Archive mit Passwort und Rekursion. Auch Laufzeitpacker und selbstextrahierende Archive sowie Embedded Files in anderen Dateien können für einige Virens Scanner knifflig werden. Schließlich bietet sich das Testen weiterer bekannter Namens-erweiterungen an. (dr)



- [1] EICAR-Testdateien
C2PA1
- [2] VirusTotal
C2PA2
- [3] Online-Konverter
C2PA3, C2PA4

Link-Codes



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



Exchange Server 2010 Statusprüfung über die Management Shell

von Robert Lindermeier

In der Regel prüfen Administratoren die diversen Einstellungen und Dienste eines Exchange Servers per Hand, wenn es Probleme gibt. Doch gibt es auch für diesen Bereich praktische Cmdlets, die mit einem Aufruf zahlreiche Mausklicks und Prüfungen ersetzen oder abnehmen. In diesem Workshop beleuchten wir die wichtigsten im Detail und zeigen deren Funktion auf.

Dienste prüfen mit Test-ServiceHealth

Das Cmdlet "test-servicehealth" prüft den Status der Exchange Server-Dienste und zeigt in der Ausgabe in Abhängigkeit der einzelnen installierten Exchange Server-Rollen die Dienste an, die für diese Rolle benötigt werden, und ob diese aktuell gestartet sind oder nicht. Läuft ein benötigter Dienst nicht, dann zeigt die Ausgabe diesen an. Das nachfolgende Beispiel zeigt einen einzelstehenden Exchange Server mit den zugehörigen Diensten:

test-ServiceHealth

Es gibt natürlich die Möglichkeit, die Ausgabe zu filtern und mit der entsprechenden Syntax nur die essenzielle Information anzeigen zu lassen. Das könnte beispielsweise die Frage sein, ob alle notwendigen Dienste gestartet sind:

```
test-ServiceHealth | ft role,
requiredservicesrunning -AutoSize
```

Sie können auch direkt weitere Exchange Server im Unternehmensverbund abfragen, indem Sie den Exchange Server über den Parameter "-Server" definieren:

```
test-ServiceHealth -Server
Servername | ft role,
requiredservicesrunning
-AutoSize
```

Jetzt haben wir aber durchaus Umgebungen mit mehreren Servern und möchten diese nun mit einem kleinen Skript abfragen:

```
$allserver = Get-ExchangeServer

foreach ($server in $allserver)
{Write-Host "Exchange Server: "
$server.Name Test-ServiceHealth
-Server $server | t role, requi-
redservicesrunning -Autosize}
```

Hier können Sie abschließend sich auf einem der Exchange Server einen kleinen täglichen Task einrichten, der über ein PS-Skript (*.ps1) dann die Abfrage ausführt und etwa per E-Mail an das Support-Postfach sendet.

Anbindung testen mit Test-MAPIConnectivity

Das Cmdlet "Test-MAPIConnectivity" prüft, ob der grundsätzliche MAPI-Zugriff auf ein bestimmtes Postfach oder einen Postfachspeicher möglich ist. Gibt es also Zugriffsprobleme mit einem oder mehreren Outlook-Clients, wäre das die erste Option, um serverseitige Probleme auszuschließen:

```
test-MAPIConnectivity Nutzernamen
```

Noch interessanter und hilfreicher ist das erweiterte Kommando, dessen Ausgabe den Rahmen unseres Workshops weit sprengen würde:

```
[PS] C:\Windows>test-MAPIConnecti-
vity Nutzernamen -MonitoringContext
$true
```

Es liefert sehr hilfreiche Informationen inklusive Performance Daten. (dr)

```
[PS] C:\Windows>test-servicehealth
```

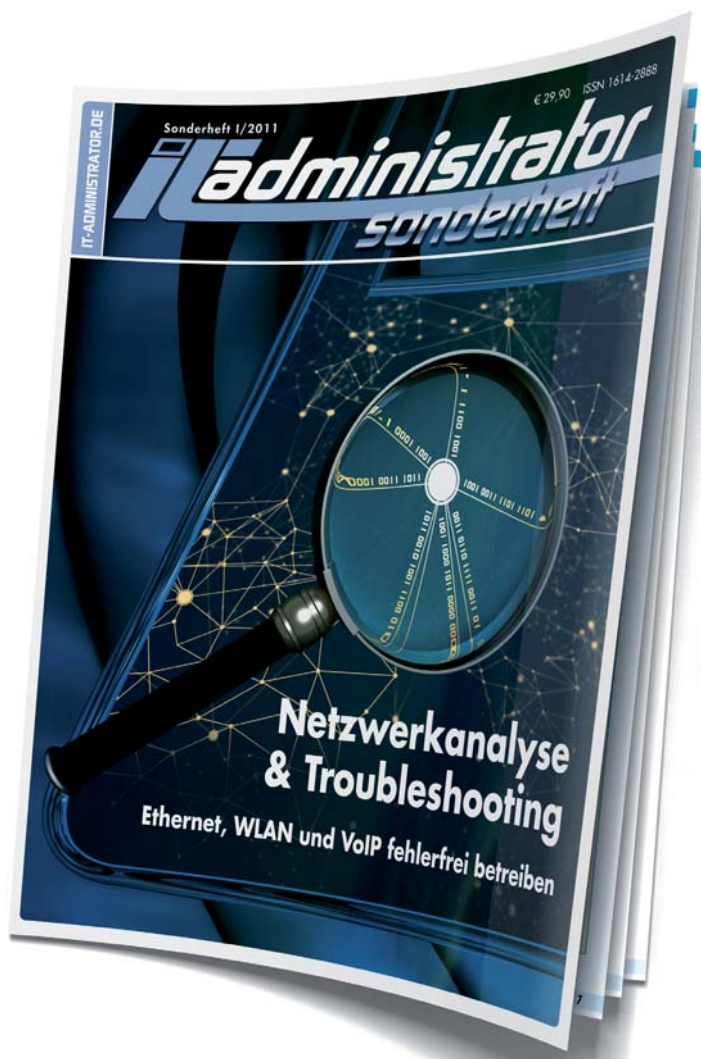
Role :	Mailbox-Serverrolle
RequiredServicesRunning :	True
ServicesRunning :	{IISAdmin, MSExchangeADTopology, MSExchangeIS, MSExchangeMailboxAssistants, MSExchangeMailSubmission, MSExchangeRepl, MSExchangeRPC, MSExchangeSA, MSExchangeSearch, MSExchangeServiceHost, MSExchangeThrottling, MSExchangeTransportLogSearch, W3Svc, WinRM}
ServicesNotRunning :	{}

Dienste prüfen mit Test-ServiceHealth

```
[PS] C:\Windows>test-ServiceHealth | ft role, requiredservicesrunning -AutoSize
```

Role	RequiredServicesRunning
Mailbox-Serverrolle	True
Clientzugriff-Serverrolle	True
Hub-Transport-Serverrolle	True

Test-ServiceHealth nach gestarteten Diensten filtern



Bestellen Sie jetzt das IT-Administrator Sonderheft I/2011!

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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



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

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

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

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

Ich zahle ☐ per Bankeinzug

Firma: _____

Geldinstitut: _____

Name, Vorname: _____

Kto.: _____

BLZ: _____

Straße: _____

oder ☐ per Rechnung

Land, PLZ, Ort: _____

Datum: _____

Tel: _____

Unterschrift: _____

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.

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

Leserservice IT-Administrator
vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville
Tel: 06123/9238-251
Fax: 06123/9238-252

leserservice@it-administrator.de

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



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

ITA 0911



Tipps & Tricks ohne Gewähr

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



Ein **Hyper-V-Cluster** ist in unserem Unternehmen das Mittel der Wahl, um die Verfügbarkeit der virtuellen Maschinen zu steigern. Wir haben jedoch das Problem, dass sich **nach einem Failover eine der Cluster-Disks nicht online** nehmen lässt. Wir erhalten eine Fehlermeldung mit dem Error Code 0x80071398, dass der **Umzug auf den alternativen Knoten gescheitert** sei. Als Grund führt das System an, dass der entsprechende Knoten weder "owner of the group" noch "possible owner of the group" sei. Was müssen wir hier ändern, um ein erfolgreiches Failover innerhalb des Clusters zu gewährleisten?

Hyper-V definiert für jede Cluster Resource, welche Cluster Nodes berechtigt sind, diese Resource zu betreiben. In einer speziellen Konstellation kann es nun dazu kommen, dass ein Cluster Node nicht in die Liste der "Possible Owners" mit aufgenommen wird – meist dann, wenn zum Zeitpunkt, wenn der Node dem Cluster hinzugefügt wird, Probleme mit dem Zoning bestehen. Hat der neue Cluster Node (noch) keinen Zugriff auf die Cluster Disk – also das Cluster Shared Volume (CSV) – würde dies einen "Redirected Access" verursachen. Neben der von Ihnen beschriebenen Fehlermeldung direkt beim Failover dokumentiert Hyper-V das Problem auch im Failover Cluster Validation Report. Der Konflikt taucht unter "Cluster Configuration / Resource Status" mit fol-

gender Beschreibung auf: "This resource does not have all the nodes of the cluster listed as 'Possible Owners'. The group that this resource is a member of will not be able to come online on any node that is not listed as a 'Possible Owner'". Bei virtuellen Maschinen oder normalen Cluster Disks können Sie die Selektion der "Possible Owners" in den Eigenschaften vornehmen. Dieser Weg bleibt Ihnen bei einem Cluster Shared Volume jedoch versperrt, da der Tab "Advanced Policies" fehlt. Sie müssen deshalb bei einem CSV auf die PowerShell zurückgreifen. Doch zunächst einmal sollten Sie die aktuelle Konfiguration auslesen. Dies führen Sie am besten mit folgendem Cmdlet durch: `Import-Module FailoverClusters`
`Get-ClusterSharedVolume |`
`Get-ClusterOwnerNode`

Im zweiten und entscheidenden Schritt fügen Sie nun die fehlenden Cluster Nodes als "Possible Owner" hinzu und kontrollieren die Änderungen:
`Set-ClusterOwnerNode -Owners`
`hyperv01, hyperv02, hyperv03`
`-Resource "Cluster Disk 2"`
`Get-ClusterSharedVolume |`
`Get-ClusterOwnerNode`

Das Problem mit dem Failover dieser Cluster Resource sollte danach behoben sein. Zur Sicherheit sollten Sie aber dennoch eine vollständige Cluster Validation durchführen. (Michel Lüscher/ln)



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

Das Verzeichnis **winsxs** existiert meines Wissens erst seit Windows Vista und enthält die **Installations- und Deinstallationsdateien von Programmen**. Laut Microsoft soll der Ordner ja auf keinen Fall einfach gelöscht werden. Allerdings weist er auf einem unserer Testsysteme mit 15 GByte freiem Speicherplatz auf der Systempartition bereits eine Größe von 5 GByte auf. Gerade auf Rechnern, die lediglich mit einer kleinen SSD ausgerüstet sind, ist jedes GByte kostbar. Gibt es denn keine **Möglichkeit, um den Speicherhunger des Verzeichnisses zu minimieren**?

Es gibt in Bezug auf den von Ihnen genannten Systemordner einen Weg über die Kommandozeile, um gerade unter Windows 7 Speicherplatz freizugeben. Öffnen Sie dazu mit Administrator-Rechten die Kommandozeile und geben Sie folgenden Befehl ein:

```
dism /online /cleanup-image  
/spsuperseded
```

Durch diesen dism-Befehl sollte einiges an zusätzlichem Speicherplatz wieder freigegeben werden – in Ihrem Fall ist wohl mit rund 3 GByte zu rechnen. (ln)

Um im Büro eines Kunden ein **WLAN aufzubauen**, das möglichst nicht mit anderen Funknetzen in der Nähe überlappt, würde ich mir gerne **alle benachbarten Netze samt Kanalbelegung und Stärke anzeigen** lassen. Gibt es außer Tools wie zum Beispiel Netstumbler eine Möglichkeit mit Windows-Bordmitteln, um sich einen Überblick über sämtliche aktiven Funknetzwerke zu verschaffen? Besonders interessant wäre für mich noch, wenn sich auch diejenigen

WLANs finden ließen, die die Aussendung ihrer SSID unterdrücken.

Seit Windows Vista haben Sie über die Kommandozeile diverse Optionen, um die WLAN-Settings zu ändern und sich benachbarte Funknetze anzeigen zu lassen. Dies funktioniert über den Befehl `netsh wlan`. Um selbst die eigentlich "versteckten" Funknetzwerke auf den Bildschirm zu bringen, geben Sie einfach folgendes Kommando ein:

```
netsh wlan show networks mode=bssid
```

Mit dem `netsh`-Befehl lassen sich noch diverse WLAN-Einstellungen schnell und simpel durchführen, etwa das Aufsetzen eines Adhoc-Webserver. Mit dem Einsatz von Skripten ist es zudem problemlos möglich, die WLAN-Settings eines Rechners in wenigen Schritten auf weitere PCs zu exportieren. Eine ausführliche Dokumentation zur Verwendung von `netsh wlan` finden Sie unter [Link-Code C2PE9] im TechNet. (In)



Wir haben in unserer VMware-Umgebung wiederholt das Problem, dass bei der **Migration von virtuellen Maschinen mit vMotion** der Vorgang bei zehn Prozent hängen bleibt und schließlich ganz abbricht. vCenter Server bringt daraufhin folgende Fehlermeldungen auf den Schirm: "Migration will cause the virtual machine's configuration to be modified to preserve the CPU feature requirements for its guest operating system – Operation timed out – A general system error occurred: Failed waiting for data. Error 16. Invalid argument". Ehrlich gesagt haben wir keine Ahnung, was die Ursache für diesen Fehler sein könnte. Haben Sie vielleicht eine Idee?

Mit der folgenden Anleitung diagnostizieren Sie, was den Ausfall von VMware vMotion bei zehn Prozent verursacht haben könnte. Gehen Sie Schritt für Schritt vor, um das Problem einzugrenzen und die richtige Lösung zu finden. Stellen Sie sicher, dass vMotion auf allen ESX-Hosts aktiviert ist. Loggen Sie sich dazu über den vSphere-Client in vCenter Server ein. Klicken Sie auf einen ESX-Host und navigieren Sie auf den Tab "Configuration". In der Rubrik "Hardware" wählen Sie den Punkt "Networking" aus. Klicken Sie

nun auf "Properties" bei demjenigen virtuellen Switch, an dem ein VMkernel-Port konfiguriert wurde. Nun öffnet sich eine Dialogbox, in der Sie im Tab "Ports" die Option "vmkernel" auswählen und auf "Edit" klicken. Aktivieren Sie danach bei "vMotion" einfach "Enabled" und klicken Sie auf "OK". Überprüfen Sie auf diesem Weg, ob ein Deaktivieren und anschließendes Reaktivieren der vMotion-Einstellung sowohl am Ursprungs- als auch am Zielhost das Problem beseitigt. Überprüfen Sie auch, ob eine VMkernel Netzwerk-Konnektivität vorhanden ist – öffnen Sie dazu eine ESX-Konsole oder eine Remote-Konsole und verwenden Sie den Befehl `VMKping`. Nähere Informationen zum Einsatz dieses Kommandos erhalten Sie in der Knowledge Base von VMware unter [Link-Code C2PE4]. Stellen Sie im Anschluss sicher, dass die virtuelle Maschine nicht etwa so konfiguriert ist, dass sie ein Gerät (wie zum Beispiel ein CD-ROM-Laufwerk) benutzt, das auf dem Zielhost nicht vorhanden ist. Deaktivieren Sie in diesem Fall das Gerät in der Konfiguration der VM und versuchen Sie, den vMotion-Vorgang erneut auszuführen. Wenn Jumbo Frames aktiviert sind (MTU von 9000), überprüfen Sie die Verbindung mit folgendem Befehl:

```
vmkping -s 8972 Ziel-IP-Adresse
```

Es könnten Probleme auftreten mit dem Trunk zwischen zwei physikalischen Switchen, die mit einer MTU von 1500 falsch konfiguriert wurden. Überprüfen Sie außerdem, ob die Namensauflösung auf ESX gültig ist. Wie das geht, erfahren Sie unter [Link-Code C2PE5]. Verifizieren Sie, ob aus dem Gast-Betriebssystem heraus eine Netzwerkverbindung besteht. Eine Anleitung zu diesem Schritt erhalten Sie unter [Link-Code C2PE6]. Testen Sie, ob das Umstecken von Netzwerkadaptern des ESXi/ESX-Hosts das Problem löst. Überprüfen Sie ferner, ob die Zeit über die gesamte Umgebung hinweg synchronisiert ist. Wie das geht, ist unter [Link-Code C2PE7] nachzulesen. Untersuchen Sie, ob die VM Ressourcen-Reservierungen aufweist, die am Zielhost nicht (mehr) zur Verfügung stehen. Kontrollieren Sie die Ressourcen-Einstellungen an der VM und ändern Sie diese gegebenenfalls. Auch hierzu erfahren Sie in der Knowledge Base unter [Link-Code C2PE8] Genaueres.

Wenn Sie all diese Schritte befolgt haben, sollte eine Migration mit vMotion reibungslos funktionieren. (VMware/In)



Hardware

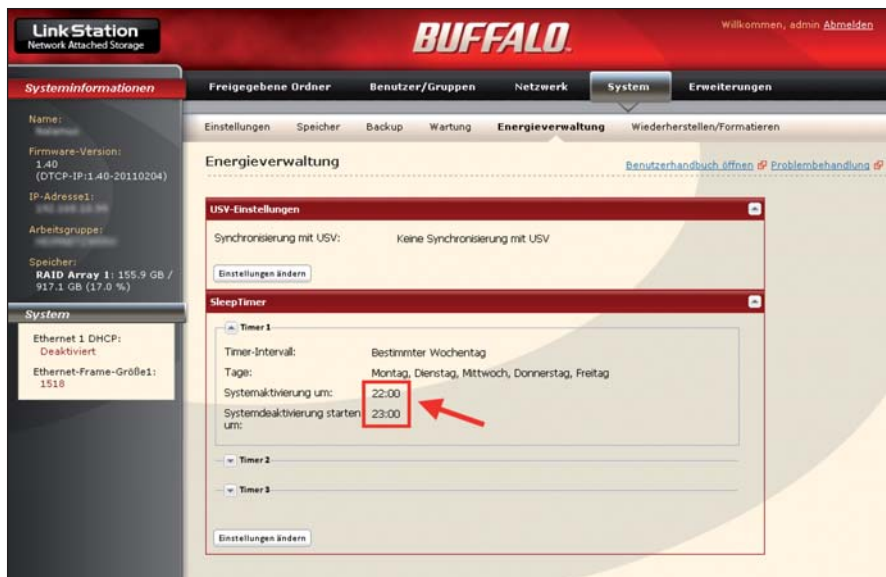
Im Showroom einer Niederlassung wollen wir Gästen unkompliziert den Netzwerkzugang per LAN-Kabel ermöglichen. Leider ist dieser Raum nicht verkabelt, so dass wir uns dazu entschlossen haben, das existierende **WLAN über den Wireless-N Ethernet Converter** von Buffalo Technology abzugreifen und über den im Gerät integrierten Switch zur Verfügung zu stellen. Die Einrichtung der Netzwerkkomponente hat wunderbar geklappt. Am Ende des Konfigurationsvorgangs über das Webinterface habe ich jedoch noch das Admin-Kennwort neu gesetzt – seitdem **kann ich mich nicht mehr einloggen**. Ich bin mir ganz sicher, mich nicht vertippt zu haben. Gibt es hier noch eine Login-Möglichkeit, ohne das Gerät komplett zurückzusetzen? Probleme habe ich leider auch mit einem NAS-Gerät des Herstellers, das dem erwähnten Showroom zugeordnet ist, aber nur am Nachmittag / Abend laufen soll. Die Einstellungen der schon etwas älteren LinkStation Duo von Buffalo erlauben einen Energiesparmodus, der das Starten und Herunterfahren des Netzwerkspeichers zu bestimmten Zeiten ermöglicht. Dies klappt beim Shutdown wunderbar, leider **startet das NAS jedoch entweder gar nicht automatisch oder nur zu gänzlich anderen als den angegebenen Zeiten**. Was kann hierfür die Ursache sein?

Beide Probleme beruhen auf einer fehlerhaften Firmware. Was den Wireless-N Ethernet Converter betrifft, so akzeptiert dieser lediglich Kennwörter, die maximal acht Zeichen lang sind. Dummerweise ist dies nirgendwo dokumentiert. Das einzige Indiz hierfür ist, dass das Konfigurationsmenü bei

Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Über 60.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator das praxisnahe Fachmagazin für Administratoren ist administrator.de die Internetplattform für alle System- und Netzwerkadministratoren.

www.administrator.de





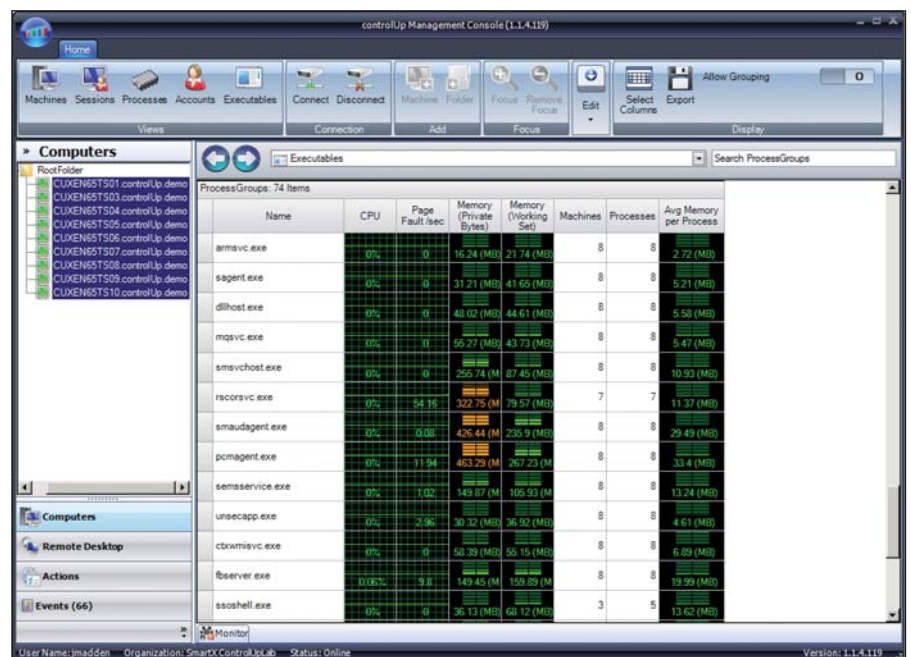
Das Buffalo-NAS richtet sich teilweise nach Tokio-Zeit: Die markierten Einstellungen bringen das NAS zwar um 23 Uhr zum Schlafen, wecken es aber nicht erst um 22 Uhr auf, sondern bereits um 14 Uhr.

der Eingabe von längeren Passwörtern nur acht Platzhalter anzeigt. Gerade bei einem neun oder zehn Zeichen langen Passwort fällt dies bei der Eingabe aber oft nicht auf und alle Zeichen ab der neunten Stelle fallen unter den Tisch. Mit den ersten acht Zeichen des von Ihnen gesetzten Passworts sollten Sie sich also einloggen können. Wenn nicht, hilft wirklich nur ein Zurücksetzen des Geräts. Was das NAS angeht, kommen zwei Fehlerursachen in Betracht. Stellen Sie zunächst sicher, dass der Netzschalter des Geräts auf "ON" und nicht auf "AUTO" steht. Nur im normalen Betriebsmodus greifen die Einstellungen des Energiesparmodus und eventuell gesetzte Ein- und Ausschaltzeiten. Ansonsten beruhen die seltsamen Startzeiten auf einem Bug der Firmware. Wenn Sie das NAS auf mitteleuropäische Zeit konfiguriert haben, richtet sich nur die Shutdown-Zeit im Menü "System / Energieverwaltung / SleepTimer" nach der eingestellten Zeitzone. Die Start-Zeit des NAS hingegen fußt auf japanischer Zeit – ein Zeitunterschied zur MEZ von acht Stunden. Wenn Sie also beispielsweise den Netzwerkspeicher von 14 bis 23 Uhr online haben wollen, müssen Sie bei Startzeit 22 Uhr eintragen, während bei Shutdown-Zeit ganz regulär 23 Uhr zu setzen ist. (In)

schen Teufel und Beelzebub: Kostenlose Programme bereiten oft nur sowieso in den Systemen vorhandene Daten grafisch neu auf oder sind so komplex, dass Einarbeitung und Fehlbedienung mehr Kosten verursachen als die Anschaffung einer kommerziellen Lösung. Wenn in diesem Umfeld dann ein freies Werkzeug erscheint, das nicht nur einen eigenen technologischen Ansatz zum Monitoring mit sich bringt und dabei auch neue Technologie wie die Desktop-Virtualisierung berücksichtigt, lohnt sich ein genauer Blick darauf.

Die Firma Smart-X bietet mit **ControlUp** ein kostenloses Tool für das zentrale Ma-

nagement von Windows-Maschinen, insbesondere, aber nicht ausschließlich für Terminalserver-Farmen und virtualisierte Desktops. Neben den **umfassenden Monitoring-Funktionen**, die zahlreiche Daten über Server, Sessions oder Prozesse für den Admin übersichtlich aufbereiten, erlaubt das Werkzeug, auch diverse Aktionen remote auf den verwalteten Maschinen auszuführen. Dazu zählt etwa das Kopieren und Löschen von Dateien, das Starten und Beenden von Prozessen oder das Editieren der Registry. Zentraler Aspekt von ControlUp sind **tabellarische Sichten auf Performance-Daten**, die definierte Merkmale für eine Vielzahl von Rechnern zusammenfassen. Beispielsweise erhält der Admin einen Überblick aller aktiven Sessions inklusive administrativem Zugriff darauf. Ähnliches gilt für Prozesse oder angemeldete Benutzer, die maschinenübergreifend angezeigt, gefiltert und bearbeitet werden können. Die verschiedenen Sichten auf die Systemparameter liefern Ansatzpunkte, um **Engpässe aufzuspüren und zu beseitigen**. Darüber hinaus erlaubt ControlUp den **Fernzugriff auf Registry und Windows-Dienste**. Speziell für die Terminaldienste bietet das Tool eine Nachrichtenfunktion, mit der ein Administrator Meldungen inklusive Grafiken an alle User von ausgewählten Servern schicken kann. ControlUp ist eine portable Anwendung, die das .NET-Framework 3.5 voraussetzt. Der Einsatz der Software bedarf



Unkompliziert, mächtig und trotzdem kostenlos: ControlUp ist eine neue Generation freier Monitoring-Werkzeuge



Tools

Bei Werkzeugen zum Monitoring der IT-Infrastruktur hat der IT-Verantwortliche oft nur die Wahl zwi-

der Installation eines Agenten auf allen Zielrechnern. Dieser lässt sich komfortabel von der ControlUp-Konsole aus verteilen. Die Konsole lässt sich nur auf PCs ausführen, die Mitglied in einer Domäne sind, und der Benutzer muss auf allen verwalteten Rechnern Administrationsrechte besitzen. ControlUp kann Computer unter Windows ab XP/Server 2003 verwalten. Eine Besonderheit stellt die Registrierung für die kostenlose Software dar: Der Anwender muss sich erst im Rahmen der Installation in Form eines Online-Accounts beim Hersteller registrieren. Zudem lässt sich das Tool – als Anforderung des Herstellers – nur mit einer permanenten Internetverbindung nutzen. (jp)

Link-Code:C2PE1

Administratoren, die für VMware-Infrastrukturen verantwortlich zeichnen, kennen das Problem des **Partition Misalignment**, das zu deutlichen Leistungseinbußen führt. Zwar spielt dieses Problem auch bei einzelnen physikalischen Servern eine Rolle, doch gravierend sind die Auswirkungen in größeren virtuellen Infrastrukturen durch die große Anzahl virtueller Maschinen einer LUN oder eines NFS Datastores. Dort führt dieser Effekt zu einer **deutlichen Belastung des Storage**. Freie Tools, die bei diesem Problem weiterhelfen, stammen oft von den Storage-Herstellern und eignen sich daher nur für deren eigene Produkte. Auf der anderen Seite stellt sich bei kostenpflichtigen Werkzeugen zur Behebung des Misalignments die Frage nach Kosten und Nutzen, insbesondere wenn sich der Performance-Verlust durch diese Storage-Problematik nicht so ohne weiteres beziffern lässt.

Doch mit **UBERAlign** steht nunmehr ein kostenloses Werkzeug zur Verfügung, das es mit seiner kommerziellen Konkurrenz aufnehmen kann. UBERAlign adressiert das Problem des Partition Misalignment in VMware-Umgebungen. Mit diesem Ziel startete Nicholas Weaver seine Entwicklung für die Community, nur um dabei festzustellen, dass dieses Problem zahlreiche Aspekte aufweist, die seine Software berücksichtigen muss (etwa Windows Boot Disks, verlorene Laufwerks-Mappings, NTFS-Metadata). So wurde, wie Weaver selbst schreibt, aus einem einfachen Schneeball eine ausgewachsene Lawine in Form seiner Soft-



UBERAlign beseitigt das Problem des Partition Misalignments in VMware-Umgebungen

ware. So ist die Liste an Features, die das nunmehr fertige UBERAlign bietet, derartig lang, dass wir an dieser Stelle auf unseren Link-Code verweisen, der einerseits zum Download der beiden benötigten Komponenten (Console und vAligner) führt und andererseits die Leistungsmerkmale detailliert aufführt. Die Software arbeitet mit Windows 2000/XP/2003/2008 (NTFS) und Linux (EXT2/EXT3/EXT4) zusammen und ist für vSphere 4.1 und 5 geeignet. Und wie erwähnt besteht UBERAlign aus zwei Komponenten: Die "UBERAlign Console" ist das grafische Interface für den Admin (Windows XP/7 oder Server ab 2003 mit .NET 4.0 oder neuer), während "UBERAlign vAligner" als vApppliance die notwendige Ergänzung für die vSphere-Umgebung darstellt. (jp)

Link-Code:C2PE2

Besonders in **Storage-Infrastrukturen** beziehungsweise SANs, die als Plattform für Virtualisierung genutzt werden, ist die **Performance** von entscheidender Bedeutung. Die verbreitesten **Flaschenhälse und Problemzonen** im Storage sind dabei die Front-Ports des Storage, die Storage-Controller und die Festplatten selbst. Die Herausforderung für den IT-Verantwortlichen liegt darin, die genauen Ursachen für zu hohe Latenzzeiten des Storage zu identifizieren.

Mit dem freien **Storage Response Time Monitor** bietet Solarwinds ein interessantes Tool, um derartigen Problemen auf die Spur zu kommen. Das Tool

ist spezialisiert auf die Analyse virtualisierter IT-Landschaften. Es **überwacht die Antwortzeiten auf der komplette Strecke zwischen Host und Storage**. Die Monitoring-Ergebnisse bekommt der Administrator mit Hinweisen auf die Teile der Infrastruktur präsentiert, die für die höchsten Latenzen verantwortlich sind. Dies hilft dabei, die Leistung der Virtualisierungs-Infrastruktur sicherzustellen, die sich durch Besonderheiten wie beispielsweise Überprovisionierung von Speicherplatz auszeichnet. Zudem spart das Tool Zeit bei der Suche nach der Bremse im System, da diese in solchen komplexen Systemen oft der sprichwörtlichen Suche nach der Nadel im Heuhaufen gleicht. Nach der kurzen, vom Hersteller geforderten Registrierung steht der Storage Response Time Monitor zum Download bereit. (jp)

Link-Code:C1PE3





Datenschutzgerechte IT-Protokollierung

Schwieriger Balanceakt

von Matthias Maier

Die Protokollierung aller Vorgänge im IT-Netz über ein zentralisiertes IT-Datenmanagement ist der ebenso pragmatische wie wirkungsvolle Weg gegen Datenmissbrauch und Angriffe von extern und intern. So lassen sich Angriffsversuche frühzeitig erkennen und abwehren. Auch ist der Datenmissbrauch mithilfe der Protokollinformationen in seinen Ausmaßen quantifizierbar. Neben technischen Anforderungen zur Protokollierung muss der Administrator allerdings auch rechtliche einhalten – ein nicht immer ganz leichter Spagat.

Es ist die rechtliche Komponente beim IT-Datenmanagement, die nicht selten von Administratoren außer Acht gelassen wird. Sowohl die Datenschutzgesetze der Länder als auch das Bundesdatenschutzgesetz (BDSG) enthalten Regelungen, aus denen sich die Pflicht zur Protokollierung von IT- und Logdaten ergibt. Die Brisanz dieser Vorschriften zeigt sich an einem Beispiel: Der Europäische Gerichtshof für Menschenrechte hat in einem Urteil aus dem Jahr 2008 (ECHR Application NO. 20511/03) im Zusammenhang mit Zugriffen auf medizinische Daten eines Krankenhausinformationssystems entschieden, dass in der fehlenden Protokollierung von (lesenden) Zugriffen auf medizinische Daten ein Verstoß gegen Artikel 8 der Europäischen Menschenrechtskonvention liegt.

Protokollpflichten und Datenschutzgrenzen

Die rechtliche Verpflichtung der IT-Datenprotokollierung ist mit strikten Regelungen im Umgang damit verbunden – und darin liegt eine wesentliche Herausforderung für das Unternehmensmanagement und die eingesetzten Lösungen: In den Datenschutzgesetzen ist als oberste Priorität die Zweckbindung von Protokolldaten festgehalten. Die Protokollierung soll rein zur Aufrechterhaltung und Überwachung der Systeme

und des Datenschutzes dienen. Eine Auswertung zur Verhaltens- und Leistungskontrolle von Mitarbeitern darf nicht durchgeführt werden. Es muss sichergestellt sein, dass nur autorisierte Personen Zugriff auf die entsprechenden Auswertungstools und dabei nur auf die für sie relevanten Logdaten haben. Dafür ist ein strukturiertes Rollenkonzept erforderlich, sowohl technisch als auch organisatorisch.

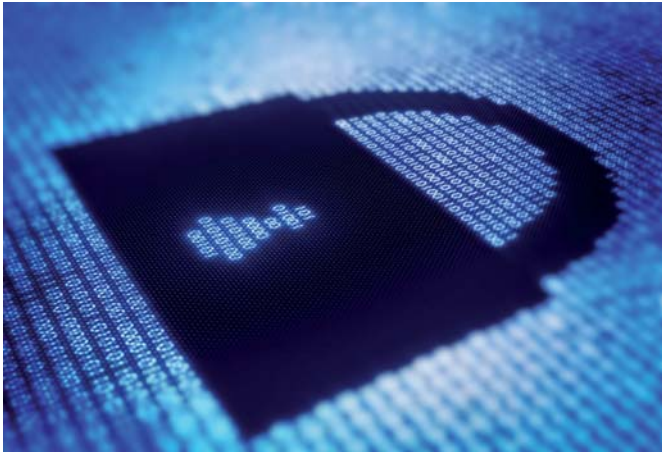
Darüber hinaus müssen sämtliche Abfragen, Suchaufträge, Systemänderungen und Reports im verwendeten Log Management-System aufgezeichnet und regelmäßig kontrolliert werden. Diese rechtlich vorgeschriebene Zweckbindung ist die Konsequenz aus dem Umstand, dass Protokollierungsdaten einen umfassenden und damit datenschutzrechtlich sensiblen Einblick in die Tätigkeiten von Administratoren und Anwendern ermöglichen, sie aber gleichzeitig für die genannten Kontrollzwecke erforderlich sind.

Datenaufbewahrungspflichten und Zeitgrenzen

Generell gilt für die Protokollierung die Datensparsamkeit und Datenvermeidung – was in der Praxis häufig in einem Spagat zwischen den Interessen resultiert. Schließlich sollen im Falle eines möglichen Da-

tenmissbrauchs die zumeist vermeintlich “autorisierten” Schritte potenzieller Eindringlinge nachverfolgbar sein. Aber auch eine Protokollierung der erfolgreichen lesenden Zugriffe ist aufgrund der datenschutzrechtlichen Revisionsicherheit erforderlich. Eine Anforderung an das IT-Datenmanagement ist daher, unterschiedliche Datenvorhaltungszeiten für Log-Messages zu planen. So empfiehlt beispielsweise der Landesbeauftragte für den Datenschutz Rheinland Pfalz, administrative Logs länger vorzuhalten als die nicht-administrativen. Eine Orientierung für die Aufbewahrungszeit administrativer Logs können die internen IT-Anträge sein. Wird zum Beispiel ein Antrag zur Löschung eines Benutzer-Accounts gestellt, sollte das zugehörige Log für den Löschvorgang als Beweis entsprechend lange vorgehalten werden. In diesem Zusammenhang ist ebenso eine zeitnahe Prüfung von Interesse, ob der Benutzer-Account eines Mitarbeiters, der das Unternehmen verlassen hat, erneut verwendet wurde.

Die Aufbewahrungsdauer ist im Datenschutz nach der “Erforderlichkeit der Aufgabenerfüllung” beschrieben. Daten müssen gelöscht werden, wenn es keinen zwingenden Grund für ein weiteres Vorhalten gibt. Der PCI-Standard der Kre-



Die Analyse von Logdateien muss innerhalb der Datenschutzgrenzen erfolgen

ditkartenanbieter gibt hierzu eine detaillierte und klare Aussage: Alle Protokollierungsdaten müssen ein Jahr aufgehoben werden. Die Leitlinie zur Protokollierung bei gesetzlichen Krankenversicherungen empfiehlt den gleichen Zeitraum, administrative Zugriffe sollen nach dem Arbeitskreis Gesundheit und Soziales über zwölf Monate hinaus aufbewahrt werden. Schließlich zeigt die Praxis aus den aktuellen Hacking-Vorfällen, dass sich das Ausspähen bis hin zur Veröffentlichung oder einer entsprechenden Drohung von Hackern meist über einen längeren Zeitraum erstreckte. Wurden die IT-Daten der Verbindungen bis dahin gelöscht, kann beispielsweise nicht mehr entgegenwirkend bewiesen werden, dass es zu keinem Datenverlust kam. Auch eine Nachverfolgung ist dann zu spät. Für die Verwendung im IT-Betrieb genügt die Vorhaltung der Daten meist für wenige Wochen. Für den forensischen Ansatz wünschen sich viele Verantwortliche allerdings einen deutlich langfristigeren Ansatz.

Datenanonymisierung für rechtskonforme Kontrollmaßnahmen

Wichtig für Unternehmen in Europa ist, dass Lösungen für das Aufbewahren von personenbezogenen Protokollierungsinformationen die Anonymisierung von Logdaten erlauben. Dieser Prozess ermöglicht es, auch datenschutzrechtlich kritische Log-Nachrichten auszuwerten, da sie nur auf kontrollierte Weise durch ein Vier-Augenprinzip vollständig angezeigt werden. So können neben personenbezogenen Daten in Unternehmen oder Krankenhäusern auch Transaktionsdaten bei Banken oder entsprechenden Zahlungsterminals ohne

rechtliche Probleme gespeichert und verarbeitet werden.

In allen Fällen gilt: Für ein ganzheitliches und richtiges Bild von Vorfällen ist es wichtig, dass Logdaten lückenlos vorliegen. Schon bei der Sammlung muss sichergestellt werden, dass keine Logdaten verloren ge-

hen. So sollte etwa eine Übertragung mit einem verbindungslosen Protokoll (UDP) vermieden werden, denn insbesondere über WAN-Strecken verlieren sich in der Praxis so immer wieder Logs – mit der Folge, dass sich falsche oder unklare Sachverhalte bilden. Des Weiteren müssen die abgespeicherten Protokollierungsdaten vor Manipulationen geschützt sein. Nur so sind sie vor Gericht im Ernstfall verwendbar. Daher empfiehlt sich der Einsatz von Hashes zur Prüfung der Integrität, wobei hier dem bereits als unsicher eingestuften MD5 ein SHA256-Hash vorzuziehen ist.

Die rechtliche Anforderung führt auch zu der Konsequenz, dass Protokolldaten als relevante Informationsbasis nicht auf Produktionssystemen aufbewahrt werden sollten oder auf Systemen, die selbst überwacht werden. Sinnvoll ist ein externes, unabhängiges System, das keine administrativen Zugriffe durch die zu überwachenden Abteilungen erlaubt.

Protokollierung zum Schutz privilegierter Anwender

Das Bundesdatenschutzgesetz fordert, dass alle Ereignisse und Tätigkeiten protokolliert werden, die die Funktionsweise der informationstechnischen Geräte verändern. Diese Form der Kontrolle dient insbesondere zum Schutz und zur Entlastung der Administratoren vor unberechtigten Vorwürfen hinsichtlich eines möglichen Missbrauchs ihrer erweiterten Rechte. Üblicherweise werden dafür alle Authentifizierungs- und Autorisierungsvorgänge, Dateneingaben und -Veränderungen, Dateneinsicht, Datenübermittlung und Datenlöschung erfasst. Ohne eine solche Protokollierung von pri-

vilegierten Zugriffsrechten können Vorwürfe etwa gegen Administrationspersonal nicht nachhaltig entkräftet werden. Hilfreich ist dabei auch die Verwendung von personalisierten Administrationskennungen, wie es das Bundesamt für Sicherheit in der Informationstechnik (BSI) und auch der Datenschutz fordern.

Eine Erfassung von Daten macht nur Sinn, wenn diese auch in regelmäßigen Abständen überprüft werden – wirtschaftlich und effektiv mit Auswertungssystemen, welche die Daten aggregiert (gruppiert) zum Beispiel nach Message-ID ausgeben. Empfehlungen zu Kontroll-Szenarien gibt die Norm ISO 27002.

Fazit

Aufgrund seiner strategischen, rechtlichen und wirtschaftlichen Bedeutung hat sich IT-Datenmanagement zur Aufgabe der Unternehmensführung entwickelt. In der Konsequenz fordert das Thema professionelle Lösungen, die hoch automatisiert und systemübergreifend ansetzen. Nur dann ist der strategische Vorteil einer lückenlosen Sicht auf alle Vorgänge im IT-Netz mit effizienter Analyse und Rechtssicherheit auch realisierbar. Manuelle Prozesse oder die Silohaltung von IT-Daten sind hier kaum akzeptabel – schon allein aufgrund des dafür nötigen Personalaufwands und der Zeitverzögerung. Nicht zu unterschätzen ist zudem der Kostenfaktor Speicherung: Moderne IT-Datenmanagement-Lösungen sorgen für eine hohe Kompression der typischerweise T-Bytes an IT-Daten, die ansonsten schnell bestehende Speicherkapazitäten sprengen könnten. Weiterführende Informationen zum Thema Protokollierung stehen beim Bundesbeauftragten für Datenschutz und Informationsfreiheit [1] unter dem Stichwort "Orientierungshilfe Protokollierung" zur Verfügung. (dr)

Matthias Maier ist System Engineer - CEUR, CISSP bei LogLogic Deutschland.

[1] Bundesbeauftragter für Datenschutz und Informationsfreiheit
C2W21

Link-Codes





Zehn Tipps für ein besseres Monitoring Netzwerk unter Beobachtung

von Ingolf Hahn

Anonymous, LulzSec und ihre Aktionen belegen, dass Hacker immer professioneller vorgehen und jede noch so kleine Sicherheitslücke ausnutzen. Der einzige Weg, um sich wirksam gegen Datendiebe und Malware-Attacken abzusichern, ist es, alle Systeme, Komponenten und Daten rund um die Uhr im Auge zu behalten. Für diese anspruchsvolle Aufgabe gibt es mittlerweile wesentlich mehr Hilfsmittel als das klassische Rot-Grün-Monitoring. Lesen Sie in diesem Beitrag zehn Tipps, wie Sie Ihr Monitoring so auslegen, dass dabei gerade Sicherheitsaspekte nicht zu kurz kommen.

Für Unternehmen, die ihre Netzwerksicherheit mit intelligenten Monitoring-Tools effizient und nachhaltig erhöhen möchten, bietet der aktuelle Markt viele interessante Lösungen. Innovative Monitoring-Software sollte automatisch Angriffsmuster und Schwachstellen erkennen und Konfigurationen mit Compliance-Richtlinien und anderen Vorgaben abgleichen. Aber unabhängig von der Performance des Monitoring-Tools sollten Sie stets die folgenden zehn Regeln im Kopf haben.

1. Behalten Sie den Überblick

Das A und O des Monitorings ist das Netzwerk-Monitoring. Setzen Sie eine Monitoring-Appliance oder -Software ein, um sofort zu wissen, wann und wo in Ihrem Netz ein Server durch einen DoS-Angriff ausfällt, ein Netzwerksegment von Viren befallen ist oder ein Router keine Signale weiterleitet. Damit gelingt es Ihnen, die Verfügbarkeit Ihres gesamten Netzwerks ständig zu überwachen. Einziger Nachteil: Als Präventivmaßnahme eignet sich das Netzwerk-Monitoring nicht. Netzwerk-Monitoring-Lösungen sind jedoch der perfekte Einstieg in die Systemüberwachung und lassen sich später sehr gut mit anderen Monitoring-, Management- und Security-Tools kombinieren.

2. Stoppen Sie Angriffe auf Ihre Non-IP-Komponenten

Der Wurm Stuxnet markiert den bisher spektakulärsten Angriff auf Non-IP-Systeme. Seitdem werden Strom- und Steuerungssysteme immer häufiger zur Zielscheibe Cyber-Krimineller. Umgekehrt nutzen Hacker mittlerweile auch abgelegene Trafo-Häuschen, um sich von dort aus unbemerkt ins Unternehmensnetzwerk vorzuarbeiten. Wenn Sie komplexe Strom-, Mess- und Steuerungstechnik im Einsatz haben, sollten Sie Ihre gesamte Infrastruktur lückenlos im Blick behalten. Mit einem Non-IP-Monitoring können Sie Attacken auf derartige Strukturen frühzeitig erkennen und abblocken.

3. Schützen Sie Smartphones, Notebooks & Co.

Implementieren Sie ein Endpoint-Monitoring, damit Sie dem Smartphone- und App-Wildwuchs in Ihrem Unternehmen gelassen entgegensetzen können. Besonders, wenn Sie ein Bring-Your-Own-Device-Konzept verfolgen oder Ihre Mitarbeiter Firmengeräte auch privat nutzen. Mit Endpoint-Monitoring erfassen Sie alle Endpoints in Ihrem Unternehmen zentral – vom Desktop-PC bis zum Smartphone. So wissen Sie jederzeit, welche Mitarbeiter mit welchen Geräten auf das Unternehmensnetzwerk zugreifen.

Sobald ein Mitarbeiter den Verlust eines Smartphones meldet, lässt sich das Gerät umgehend lokalisieren und alle sensiblen Daten zentral löschen. Achten Sie bei der Wahl Ihres Endpoint-Monitorings auf zusätzliche Management-Features, um Updates oder Sicherheitsanpassungen zentral zu steuern.

4. Verhindern Sie unerlaubte Zugriffe auf Ihre Datenbanken

Egal, ob Sie brisante Informationen oder sensible Kundendaten in Ihren Datenbanken gespeichert haben oder datenbankbasierte Web-Applikationen zum Einsatz kommen: Datenbank-Monitoring lohnt sich. Zudem schreiben immer mehr Compliance-Richtlinien vor, dass Zugriffe auf Datenbanken genauestens dokumentiert werden müssen. Achten Sie bei der Wahl des richtigen Datenbank-Monitoring-Tools darauf, dass das Werkzeug alle gängigen Datenbank-Plattformen unterstützt. Eine integrierte Black- und White-Listing-Funktion erlaubt es Ihnen, die Zugriffe auf Ihre Datenbanken individuell zu kategorisieren und unautorisierte Aktionen zielsicher zu erkennen.

5. So bleiben Ihre Firewalls effektiv

In gewachsenen Firewall-Regelwerken schleichen sich immer wieder Sicherheitslücken ein. Mit einer Firewall-Mo-

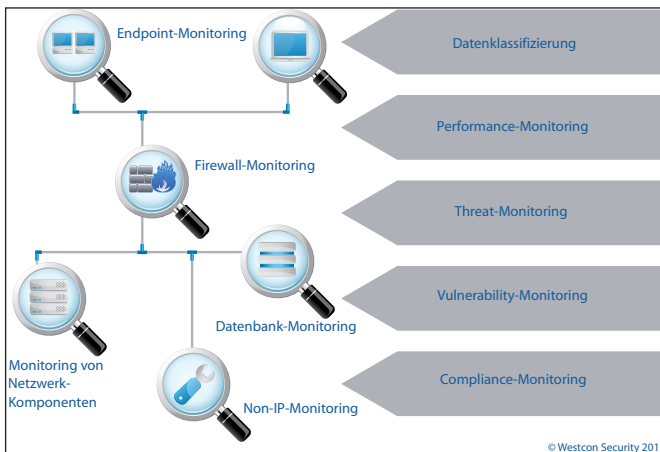


Bild 1: Monitoring-Werkzeuge überwachen verschiedenste Sicherheitsbereiche im Unternehmen und bilden bei Bedarf sogar Nicht-IP-Umgebungen ab

monitoring-Lösung wissen Sie jederzeit, welche Regeln Sie auf welchen Firewalls implementiert haben und welche Firewalls ein Update nötig haben. Das Monitoring-Tool meldet Ihnen widersprüchliche und redundante Regeln automatisch. Die systematische Überwachung Ihrer Firewalls lohnt sich für Sie besonders, wenn Sie verschiedene Firewall-Modelle in Ihren Netzwerken einsetzen. Achten Sie bei der Auswahl Ihrer Monitoring-Lösung unbedingt darauf, dass die Lösung mit allen Ihren Firewalls kompatibel ist.

6. Identifizieren Sie sensible Daten auf Knopfdruck

Um Ihre sensiblen Unternehmensdaten zu schützen, müssen Sie zuallererst definieren, welche Daten sensibel sind. Am einfachsten und genauesten funktioniert das mit einem Werkzeug zur Datenklassifizierung. Die Monitoring-Software sollte alle alten und aktuellen Versionen wichtiger Dateien mit einbeziehen. Automatisierte Lösungen klassifizieren Ihre Daten und ermitteln, welche Dateien in Kopie auf Servern, lokalen Desktops oder in E-Mails vorhanden sind. Den größten Nutzen bieten Datenklassifizierungstools, die Daten sowohl nach Dokumenteigenschaften als auch kontextbezogen klassifizieren.

7. So erkennen Sie frühzeitig Überlastungs-Angriffe

Mit Performance-Monitoring kontrollieren Sie die Auslastung Ihrer Netzwerke in Echtzeit und stellen durch Regelwerke sicher, dass kritische Anwendungen stets verfügbar sind. So erkennen Sie automa-

auslastung können Sie leistungsstarke Echtzeit-Firewalls und umfangreiche Monitoring-Lösungen betreiben, ohne dass dadurch Ihre geschäftskritischen Anwendungen in Stoßzeiten langsamer laufen. Performance-Monitoring schafft auch ideale Voraussetzungen, um virtuelle Umgebungen rundum abzusichern und hochverfügbar bereitzustellen.

8. So dokumentieren Sie alle Cyber-Attacken

Viele Hacker-Angriffe bleiben unbemerkt, da sie von Firewalls erfolgreich abgewehrt werden oder keinen erkennbaren Schaden im Netz anrichten. Dennoch lohnt es sich, Security-Logs Ihrer Router, Firewalls et cetera zu sammeln und auszuwerten. Mit dem richtigen Threat-Monitoring entdecken Sie Angriffsmuster und können sich optimal gegen wiederkehrende Attacken zur Wehr setzen. Intelligente Threat-Management-Tools analysieren und erkennen ungewöhnliche und bedrohliche Verhaltensmuster und stoppen diese, bevor sie Schaden in Ihren Netzwerken anrichten können. Damit schützen Sie Ihre IT-Umgebung auch optimal vor Advanced Persistent Threats.

9. Erkennen Sie Ihre Schwachstellen

Ein ungepatchter Mailserver oder ein veralteter PDF-Reader auf einem Ihrer Unternehmensrechner öffnet ein Einfallstor für Exploits und Malware. Um solche Schwachstellen lückenlos zu erkennen und effektiv abzuschirmen, empfiehlt sich ein Vulnerability-Monitoring. Das Vulnerability-Management unter-

tisch, wenn DoS- und Buffer-Overflow-Attacken Ihre Ressourcen in die Knie zwingen und können gleichzeitig genügend Bandbreite für wirksame Security-Lösungen reservieren. Performance-Monitoring hilft zudem, wenn Sie Ihre Security-

Lösungen aufrüsten wollen: Dank optimaler Bandbreiten-

stützt Sie bei der Planung und Erfolgskontrolle Ihrer Security-Maßnahmen. Intelligente Vulnerability-Management-Tools stufen die entdeckten Schwachstellen zudem nach ihrer Wichtigkeit ein und simulieren, welcher Schaden durch einen Angriff in Ihrem Netzwerk entstehen kann. Viele Vulnerability-Management-Tools überprüfen auch, ob Sicherheitsrichtlinien eingehalten werden.

10. Sichern Sie hohe Security-Standards

Wenn Ihr Unternehmen Compliance-Richtlinien erfüllen muss, bieten intelligente Compliance-Monitoring-Tools optimale Unterstützung. Diese Produkte sorgen für eine lückenlose Dokumentation und warnen, sobald eine der Vorgaben nicht oder nicht mehr eingehalten wird. Das schafft nicht nur Rechtssicherheit, sondern hilft Ihnen ferner dabei, Sicherheitsstandards konsequent auf hohem Niveau zu halten. Viele automatisierte Compliance-Monitoring-Lösungen übernehmen auch die Anpassung von Konfigurationen und Regelwerken an die Compliance-Richtlinien und liefern in regelmäßigen Abständen Compliance-Audits.

Fazit

Monitoring-Lösungen tragen enorm dazu bei, die Sicherheit im Unternehmensnetzwerk zu erhöhen. Ob Sie mehr von einer speziellen oder eher umfassenden Lösung profitieren, hängt von mehreren Gesichtspunkten ab: Wollen Sie gezielt neuralgische Punkte – wie Datenbanken mit Kreditkartendaten oder die E-Mail-Accounts der Chefetage – überwachen, liegt dort auch der ideale Ansatzpunkt für eine Monitoring-Lösung. Benötigen Sie erst einmal einen Überblick über Ihr Netzwerk und möchten den Bedarf an weiteren Sicherheitsmaßnahmen ermitteln, beginnen Sie am besten mit klassischem Netzwerk-Monitoring. Setzen Sie mehrere Monitoring-Tools in Ihrem Unternehmen ein, lohnt es sich eventuell, ein herstellerübergreifendes, zentrales Management zu implementieren. (In)



Ingolf Hahn ist Director Professional Services bei Westcon Security in Deutschland sowie Managing Director von Westcon Security in der Schweiz.

Als Opa Admin war: GRiD Compass 1101 Es kommt Bewegung in den PC-Markt

von John Pardey



Gegen Ende der 1970er-Jahre war die Miniaturisierung der Computertechnologie so weit fortgeschritten, dass portable Rechner gebaut werden konnten. Denn die Vorteile eines mobilen Computers beispielsweise für die Forschung waren den frühen Hardwareentwicklern ebenso präsent wie uns heute, wo ein leistungsstarker Rechner so gut wie jedermann rund um die Uhr begleitet. Doch die ersten "Portables" wurden mit einem Gewicht im zweistelligen Kilogramm-Bereich eher ihrem Spitznamen "Schleppable" gerecht. Und doch war es nur eine Frage der Zeit, bis der Form- und natürlich der Gewichtungsfaktor soweit optimiert wurden, dass der erste Laptop das Licht der Welt erblickte.

Form follows function

Und obwohl es eine ganze Reihe früher mobiler Rechner gab, ist es weitestgehend unstrittig, dass der GRiD Compass 1101 der Erstgeborene in der Laptopfamilie ist. Dies liegt unzweifelhaft an seinem Design, das sich prinzipiell bis heute in jedem Laptop widerspiegelt – ein hochklappbarer Monitor, der eine darunterliegende Tastatur freigibt ("Clamshell"). Verantwortlich dafür zeichnete Industriedesigner Bill

Moggridge, der jedoch "nur" das Design des GRiD Compass 1101 entwickelte, nicht jedoch dessen IT-Komponenten.

Doch ganz perfekt war das Design des ersten Laptops noch nicht. So betrieb der Anwender seinen GRiD Compass 1101 nicht mit Akkus oder Batterien, sondern über ein Netzkabel. Ein Feature, das die Mobilität ohne Frage ein Stück weit behinderte. Auch durfte der Nutzer nie vergessen, den Fuß auf der Unterseite auszuklappen (leider in unserem Bild auf dieser Seite nicht zu sehen – so wie dort aufgebaut, war der Compass nicht betriebsbereit), denn ansonsten mangelte es an Luftzirkulation zur Kühlung und der Rechner überhitzte.

Mobilität ist nicht ganz günstig

Als der GRiD Compass 1101 1982 auf den Markt kam, waren seine leichten fünf Kilogramm ein absoluter Spitzenwert. Aber auch die Rechenleistung konnte sich durchaus sehen lassen: Für einen Preis zwischen 8.000 und 20.000 US-Dollar (je nach Ausbaustufe von Speicher und Software der teuerste PC seiner Zeit) erhielt der glückliche Besitzer einen Intel 8086-Prozessor, der auf 256 KByte DRAM zugreifen konnte. Ein Elektrolumineszenz-Display mit 320 x 240 Pixeln meisterte alles, was ein Display damals können musste, mit Bravur.

Beim Massenspeicher setzte der Hersteller jedoch auf eine Technologie, die 1982 eigentlich schon auf dem absteigenden Ast war und bald von den Festplatten ausbootet werden sollte: Magnetblasenspeicher (ein dünner Film eines magnetisierbaren Materials, in dem sich kleine magnetische Bereiche, die sogenannten Blasen befinden, die jeweils ein Bit Daten speicherten). Über

384 KByte dieses Speichermediums verfügte der digitale Begleiter.

Erweitern ließ sich der Massenspeicher über den "General Purpose Instrumentation Bus". Dieser erlaubte es, externe Festplatten beziehungsweise Floppy Disk-Laufwerke anzuschließen. Auf diese Weise war es auch möglich, mehrere 1101er zusammenzuschließen.

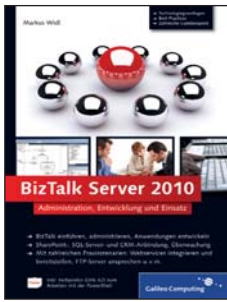
Griff nach den Sternen

Ein Großteil des Kaufpreises entfiel auf das Betriebssystem GRiD-OS. Stolz 10.000 US-Dollar wurden in der größten Ausbaustufe fällig. Doch wie so viele Computer Anfang der 80er Jahre, die nicht von IBM produziert wurden, war auch der Compass nicht IBM-kompatibel. Zwar legte der Hersteller später die MS-DOS-Kompatibilität nach, doch das teure und sehr spezialisierte GRiD-OS verhinderte eine weite Verbreitung. Und doch war die Verarbeitung des Geräts ebenso wie die Funktionalität seiner Hard- und Software so robust, dass die NASA ihren Astronauten einen GRiD Compass 1101 als Begleiter angedieh. 1985 flog der erste Laptop mit dem Space Shuttle in den Weltraum.



Vom frühen GRiD Compass 1101 sind leider keine druckfähigen Bilder verfügbar, daher hier das äußerlich baugleiche 1530-Modell

BizTalk Server 2010



Der BizTalk Server zählt zur Produktfamilie der Microsoft Application Platform und fungiert dort als eine Schlüsselkomponente. Die Plattform soll Integrations- und Geschäftsmanagement-

Prozesse verschmelzen, was bedeutet, dass Systeme und Daten miteinander gekoppelt werden. Daraus folgt, dass der BizTalk Server mit anderen MS-Server-Produkten wie Windows Server, Visual Studio und SQL Server zusammenspielt. Zur Kostensenkung wird Hyper-V unterstützt, das virtualisierte Instanzen in unlimitierter Zahl gestattet.

Markus Widl hat sich mit seinem Buch der Umsetzung in der Praxis angenommen und liefert eine Veröffentlichung jenseits der Internetdokumentation von Microsoft. Dabei ist der Einstieg in die Materie ansprechend gestaltet und erzeugt die Neu-

gier, sich mit dem BizTalk Server detaillierter auseinanderzusetzen. Dazu widmet sich der Autor Beispielen aus der Praxis, die direkt einsetzbar sind. Zunächst beschreibt er die Rolle des BizTalk Servers und die verschiedenen Editionen, bevor er im Folgekapitel die notwendigen Techniken und Komponenten (zum Beispiel Flatfiles) für die Entwicklung einer BizTalk-Anwendung vorstellt.

Anwendungsintern kommt XML zum Einsatz. Mit diesem Hintergrundwissen widmet sich der Autor der Konfiguration des Nachrichtenflusses und der beteiligten Komponenten. Das Kapitel endet mit der Beschreibung der Verteilung fertiger Anwendungen auf verschiedenen Servern. Detailreich wird es im praktischen Abschnitt "BizTalk im Einsatz". Dabei geht der Autor auf die Arbeit mit Dateien ebenso ein wie auf den Zugriff auf SQL-Datenbanken oder das Ansprechen von FTP-Adaptoren. Hinzu kommen die Arbeit mit E-Mails und das Platzieren von Webservices sowie die Anbindung von SharePoint (sowohl mit und ohne InfoPath) und einer CRM-Lösung.

Fazit

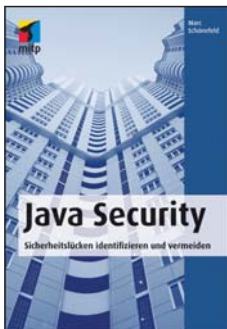
Das komplexe Produkt BizTalk Server 2010 wird in dieser Publikation sowohl für Administratoren als auch Entwickler von Beginn an bestens erläutert. Zielgruppe sind Personen, denen dieses Produkt der MS-Serverfamilie bisher fremd war und die die Möglichkeiten kennenlernen und mit der Arbeitsweise vertraut werden möchten. Vielzählige Schritt-für-Schritt-Anleitungen, untermauert mit Screenshots, helfen den Lesern, raschen Zugang zu finden. Die leicht nachvollziehbare Schreibweise des Autors garantiert einen raschen Einstieg. Die übersichtliche und ansprechende Strukturierung erfreuen Augen und steigern die Aufmerksamkeitsdauer.

Frank Große

Autor	Markus Widl
Verlag	Galileo Computing
Preis	59,90 Euro
ISBN	978-3836215459

Bewertung (max. 10 Punkte) **10**

Java Security



Bei der Einführung von Java lagen die Vorteile in puncto Sicherheit gegenüber bis dato bekannten und in der professionellen Software-Entwicklung eingesetzten Programmiersprachen primär in der automatischen

Speicherverwaltung und dem Sandbox-Modell. Doch die mittlerweile große Verbreitung und damit verbundene regelmäßige Aktualisierungen sorgen für Interesse am Aufspüren von Sicherheitslücken und entsprechendes Angriffspotenzial. Diesem Thema widmet sich Marc Schönefeld mit seinem Buch "Java Security".

Der Aufbau der Publikation erfolgt logisch. Zunächst beschreibt der Autor detailliert die Grundlagen der Java-(Sicherheits)-Archi-

tektur. Dabei liegt das Augenmerk auf dem Sicherheitsmanager, der zur Abwehr unautorisierter Angriffe dient, aber in vielen Installationen nicht zum Einsatz gelangt. Über Programmierwerkzeuge und Grundlagen der sicheren Java-Programmierung wird der Leser zu möglichen Angriffszielen geführt. Eine umfangreiche Anzahl an Beispielen zeigt anhand von abstrakten Schwachstellen mögliche Leaks auf. Bei diesen Ausführungen konzentriert sich der Autor auf häufig auftretende Schwachstellen und deren grundsätzliche Entgegnung.

Große Sorgenfalten können vorgefertigte Malware-Pakete bereiten, die im nächsten Kapitel besprochen werden. Diesen Abschnitt dürften Administratoren im Desktop- und Softwarebereich mit Interesse lesen. Der Autor widmet sich der Analyse der aktiven Fehlersuche mit Fuzzing und zeigt dessen praktischen Einsatz auf, bevor er sich den Schwächen von Java Enterprise widmet. Die Erkenntnis: Zeitgemäße Java-Applikationen setzen sich aus vielen Kompo-

nenten zusammen und eigenständige Konfigurations- und Designeigenschaften können Hintertüren öffnen, die im Gesamtkontext einer Enterprise-Applikation Schwachstellen ermöglichen.

Fazit

Softwareentwickler dürften von diesem Buch am meisten profitieren, da der akademische Ansatz der vorgestellten Ausführungen sich auf die prototypische Demonstration von potentiellen Angriffen (inklusive Code-Schnipsel) konzentriert. Administratoren, die im Bereich der Software-Sicherheit agieren, finden die nötigen Anregungen für die Suche nach Lücken.

Frank Große

Autoren	Marc Schönefeld
Verlag	mitp
Preis	39,95 Euro
ISBN	978-3826691058

Bewertung (max. 10 Punkte) **8**

www.securitymonitoringblog.de

Mit Sicherheit durchblicken

Es ist kein großes Geheimnis, dass die IT trotz vieler technologischer Fortschritte eher komplexer wird als übersichtlicher. Dies hat weniger damit zu tun, dass die Informationstechnologie keine Fortschritte macht, als dass sich die IT in immer mehr Felder der Arbeitswelt bewegt und immer mehr Aufgaben übernimmt. Dem folgt eine zunehmende Spezialisierung der Aufgaben und natürlich auch des notwendigen Know-hows. Vor diesem Hintergrund stellen wir Ihnen in diesem Monat die recht junge Website securitymonitoringblog.de vor. In diesem Blog betrachtet Florian Roth Aspekte des Monitorings sicherheitsrelevanter Bereiche der IT. Dies macht natürlich viel Sinn, denn Sicherheit – in diesem Fall die der eigenen IT – beruht einerseits auf gezielten Maßnahmen zur Erhöhung des Securityniveaus, andererseits natürlich auf einem möglichst aktuellen Stand des eigenen Wissens rund um die Vorgänge im Netz. Und diese lassen sich eben nur über geeignete Monitoringansätze feststellen.

Roth ist neben seiner Tätigkeit als Blogger IT Security Consultant und be-

schäftigt sich beruflich mit zahlreichen Aspekten der Informationssicherheit wie etwa Intrusion Detection, Web Application Security, Penetration Testing oder Firewall Audits. Zudem ist er langjähriger Autor einer Zeitschrift seines Fachgebiets. Gleichzeitig betont er jedoch, den Blog eher "locker und formlos" gestalten zu wollen, um ihn von seiner regulären Arbeit abzugrenzen. Und doch verspricht er seinen Lesern "Unterstützung bei diversen Problemen bieten" zu wollen und ihnen neue Werkzeuge vorzustellen.

Da Roths Blog erst ein knappes halbes Jahr online ist, wäre es zweifellos vermessen, von einem umfassenden Know-how-Schatz oder vergleichbarem zu sprechen. Dennoch greift Roth in seinen Blogeinträgen sehr praxisnahe Themen auf, etwa die zentrale Zusammenführung der Logs der Windows-Firewall aller Clients, die Auswertung von Event-IDs oder auch das gezielte Aufspüren von Conficker (der auch drei Jahre nach seinem ersten Erscheinen immer noch Rechnersysteme infiziert). Und seine Kategorien zeigen auch, wohin sich der Blog entwickeln soll: Skripte, Videos und Tutorials finden sich dort. Geben Sie diesem jungen Blog doch einfach eine Chance und abonnieren den RSS-Feed. (jp)

Skript Auswertung Windows Eventlog nach User und Event ID

	A	B	C	D	E
1 User	ID 529	ID 577	ID 4662	ID 4667	
2 a.mueller		12		45680	
3 h.meister		2450	8650		
4 k.keller		1267	1800	23809	345

Mit folgendem Skript lassen sich Windows Eventlog Protokolle an Hand der Benutzer ID und der von diesem Benutzer verursachten Event IDs analysieren. Es erzeugt einen CSV Output, der dann wieder vielfältig weiterverwendet werden kann.

[Continue Reading](#)

Lang laufende Prozesse finden

by Venom
in Command Line
Comments (0)

KATEGORIEN

- Allgemein (1)
- Command Line (6)
- Logdatensammlung (3)
- Malware (2)
- Netzwerk (4)
- Neuigkeiten (1)
- Skripte (3)
- Tools (5)
- Tutorial (3)
- Video (3)
- Wissen (2)

LINKS

- BSK Consulting GmbH
- Neos Ubuntu Tipps und Tricks

THEMEN

In Florian Roths Blog finden IT-Security und Monitoring ein gemeinsames Zuhause

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

Netzwerk-Monitoring garantiert Webseiten-Performance

Vor mehr als 20 Jahren ging die erste Webseite online, die das HTTP-Protokoll nutzte. Heute zählt der Online-Auftritt für viele Unternehmen längst zu den wichtigsten Business-Motoren. Umso ärgerlicher ist es, wenn zu hoher Traffic die Seite zusammenbrechen lässt oder defekte Links den Nutzer in eine Sackgasse führen. Ratsam ist daher ein permanentes Monitoring. In unserem Beitrag im Web zeigen wir, welche Vorsichtsmaßnahmen effektiv sind und was das Internet-Geschäft sogar dann aufrechterhält, wenn Fehler auftreten.

Link-Code: C2W51

So vermeiden Sie Social Media-Datenlecks

Die steigende Social Media-Nutzung in Unternehmen erhöht das Risiko hinsichtlich Malware-Infektionen und Datenlecks. Antivirus-Software kann das Malware-Risiko zwar im Zaum halten, doch Datenlecks bleiben offen. Auch betriebliche Nutzungsrichtlinien helfen nur bedingt, da sie häufig unterlaufen werden. Wir erklären auf unserer Webseite, wie Sie mit einer Data Leak Prevention-Software der Weitergabe sensibler Unternehmensdaten über Datenlecks effektiv einen Riegel vorschieben.

Link-Code: C2W52

Die fünf größten Herausforderungen beim Netzwerk-Monitoring

Die Aufgaben von Servern in Organisationen haben sich beträchtlich verändert – Nutzung, Anforderung und Komplexität sind in den letzten Jahren erheblich gestiegen. Viele der herkömmlichen Tools und Techniken, die in der Vergangenheit noch ausreichten, genügen heute nicht mehr. Folglich stellt die Überwachung von Servern in heutigen anspruchsvollen Umgebungen IT-Verantwortliche vor besondere Aufgaben. Unser Fachartikel im Internet erläutert die wichtigsten Herausforderungen, mit denen sich IT-Administratoren auseinandersetzen müssen, um eine optimale Server-Leistung sicherzustellen.

Link-Code: C2W53

Smartphones aus Sicht der Informationssicherheit

Bring your own device – nicht erst seit der zunehmenden Akzeptanz dieses Credo halten Smartphones rasant Einzug in der Unternehmens-IT. Was die Sicherheit der mobilen Geräte und damit auch die des gesamten Netzwerkes betrifft, tun sich dabei aber viele Lücken auf. In unserem Online-Fachartikel diskutieren wir, wie sich die Risiken beim Verlust eines Smartphones minimieren lassen. Außerdem beleuchten wir, wie Sie die Verbreitung schadhafter Apps durch den Einsatz eines IRM-Systems verhindern können.

Link-Code: C2W54

Besser informiert: Fachartikel auf der Website des IT-Administrator

»Die vielseitige Arbeit im Team macht mir viel Spaß«

Frank Wohowsky (33) ist als Teamleiter für den reibungslosen Systembetrieb der Conergy AG Solarmodule Frankfurt (Oder) verantwortlich. Das Unternehmen ist ein internationaler Anbieter von Systemen zur Erzeugung und Nutzung von erneuerbaren Energien. Dabei produziert Conergy alle für eine Solaranlage erforderlichen Komponenten unter einem Dach.

Warum sind Sie IT-Administrator geworden?

Eigentlich habe ich mein Hobby zum Beruf gemacht. Computertechnik hat mich schon immer sehr interessiert und außerdem macht es mir Spaß, Verantwortung zu übernehmen.

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

Weil es einer der besten und vielseitigsten Berufe ist. Von der Elektrotechnik bis hin zu Menschenkenntnis ist alles dabei.

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

Die Planung von Projekten sowie die Verantwortung, die mein Beruf mit sich bringt, gefallen mir sehr. Ich habe Spaß an der Arbeit im Team und am Schreiben von Skripten. Es gibt eigentlich nichts, was mir nicht Spaß macht – sonst würde ich den Job wechseln.

Welches Netzwerk- und Systemmanagement nutzen Sie?

Unser Leadsystem für die Netzwerküberwachung ist die Überwachungssoftware Nagios. Weiterhin nutzen wir selbst geschriebene Shell-Skripte basierend auf PHP (Hypertext Preprocessor) und in Verbindung mit SNMP (Standard Network Management Protocol) für die Auswertung von den Ereignissen im Netzwerk.

Mit welchen Werkzeugen überwachen Sie Ihre Server?

Wir arbeiten mit Nagios und den zugehörigen Tools.

Nutzen Sie ein Logmanagement?

Ja, hier nutzen wir selbst geschriebene Skripte für das Reporting.

Welche Aspekte vermissen Sie beim Monitoring in Ihrer Umgebung?

Keine. Wir haben eine Erhebung, die verschiedene Aspekte durchgeht und diese in das Reporting umsetzt.

Auf welche Bereiche werfen Sie ein besonderes Auge?

Die Dokumentation der IT-Infrastruktur und deren Prozesse sowie die Netzwerksicherheit und der Virenschutz sind mir

besonders wichtig. Wert lege ich vor allem auch auf die Vereinfachung der Standardabläufe.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir erstellen derzeit eine neue Datenbankbasis.

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

Das kann ich nicht generell beantworten. Das kommt auf den jeweiligen Unternehmenshintergrund an, da tauchen dann in speziellen Situationen auch entsprechende Wünsche auf.

Wie denken Sie, wird ein IT-Administrator in zehn Jahren arbeiten?

Hoffentlich hauptsächlich nach dem ITIL-Standard.

Und als was möchten Sie in zehn Jahren arbeiten?

Als "Head of IT" in einem mittelständischen Unternehmen.

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

Momentan fällt mir hier nichts ein, alles läuft gut.

Welches ist der dümme Anwenderfehler, der Ihnen untergekommen ist?

Wirklich dumme Anwenderfehler gibt es ja nicht. Die meisten können nur die Technologie nicht richtig bedienen. Das kann man aber lernen und dafür gibt es uns Administratoren.

Wie finden Sie den nötigen Ausgleich zu Ihrer Arbeit?

Beim Sport sowie beim Zusammensein mit meiner Familie.

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

Ja, und das leider viel zu oft.

Inwieweit hat Ihr Beruf Ihre Hobbys geprägt?

Im Grunde nur sehr wenig. Aber natürlich übernimmt man Ansprüche an bestimmte technische Standards und auch das antrainierte Zeitmanagement.

Wie sieht die IT im Privatleben in zehn Jahren aus?

Das soziale Leben wird sich meiner Einschätzung nach noch mehr ins Netz ver-



Geburstag: 08.02.1978
Admin seit: 12 Jahren
Hobbys: Reiten, Schwimmen, Skaten, Volleyball

Frank Wohowsky, IT-Administrator

Ausbildung und Tätigkeit

- Ausbildung zum Automatisierungs- und Computertechniker
- Zurzeit als Teamleiter Systemadministration tätig

Betreute Umgebung

- Infrastruktur im Bereich erneuerbare Energien
- Schwerpunkt Cisco Netzwerktechnik und Oracle Datenbanken

lagern. Man wird sich auch als Online-Person weitergehend etablieren müssen, um alle sozialen und beruflichen Kontaktmöglichkeiten nutzen zu können. Aus meiner Sicht wird auch die Zahl der Internetsüchtigen zunehmen. Alltagsmedien wie das Fernsehen werden komplett verschwinden und durch Internet-Streams und Downloads ersetzt werden. Im Freizeitbereich werden die Computerspiele sicherlich auch noch viel realistischer und die 3D-Technik standardisiert werden. Außerdem dürfte der Alltagsbereich auch im Privaten noch weiter automatisiert und technisiert werden, sobald die Kosten für entsprechende Anwendungen sinken.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 3/12 erscheint am 28. Februar 2012

Schwerpunktthema:

Netzwerkmanagement

Im Test: System Management-Appliance Dell KACE

Im Test: Network Ressource Manager v3.0

Workshop: Neuerungen und Betrieb von OSSIM 2.3

Workshop: Netzwerkdokumentation mit Network Notepad

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

Die Ausgabe im **April** befasst sich mit dem Thema **Backup & Verfügbarkeit**. In unserer Test-Rubrik nehmen wir unter anderem Nova Backup 12.5 und Veeam Backup & Replication v6 genauer unter die Lupe. In unserer Praxisrubrik lesen Sie, wie Sie Load Balancing mit Exchange Server betreiben.

Als Schwerpunkt im **Mai** geht es dann um das Thema **Desktop-Virtualisierung**.

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

Netzwerkmanagement

IMPRESSUM

Redaktion

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

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

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

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

Autoren dieser Ausgabe

Petra Adamik, Thomas Bär, Ralph Dombach,
Frank Große, Ingolf Hahn, Jürgen Heyer, Thomas Joas,
Martin Kuppinger, Robert Lindermeier, Sandra Lucifora,
Matthias Maier, Ulf B. Simon-Weidner, Christian Weihs

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-Hohstadt

Vertrieb

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

Abo- und Leserservice

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

Vertriebsbetreuung

SI special interest Pressevertrieb GmbH,
www.specialinterest.com

Erscheinungsweise

monatlich

Bezugspreise

Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-

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

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

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 85
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des
Amtsgerichts München unter
HRB 151585.

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

ISSN

1614-2888

Urheberrecht

Alle in IT-Administrator erschienenen Beiträge sind
urheberrechtlich geschützt. Alle Rechte, einschließlich
Übersetzung, Zweitverwertung, Lizenzierung vorbe-
halten. Reproduktionen und Verbreitung, gleich wel-
cher Art, ob auf digitalen oder analogen Medien, nur
mit schriftlicher Genehmigung des Verlags. Aus der
Veröffentlichung kann nicht geschlossen werden, dass
die beschriebenen Lösungen oder verwendeten Be-
zeichnungen frei von gewerblichen Schutzrechten sind.

Haftung

Für den Fall, dass in IT-Administrator unzutreffende
Informationen oder in veröffentlichten Programmen,
Zeichnungen, Plänen oder Diagrammen Fehler en-
thalten sein sollten, kommt eine Haftung nur bei
grober Fahrlässigkeit des Verlags oder seiner Mit-
arbeiter in Betracht. Für unverlangt eingesandte
Manuskripte, Produkte oder sonstige Waren über-
nimmt der Verlag keine Haftung.

Manuskripteinsendungen

Die Redaktion nimmt gerne Manuskripte an. Diese
müssen frei von Rechten Dritter sein. Mit der Ein-
sendung gibt der Verfasser die Zustimmung zur Ver-
wertung durch die Heinemann Verlag GmbH. Sollten
die Manuskripte Dritten ebenfalls zur Verwertung
angeboten worden sein, so ist dies anzugeben.
Die Redaktion behält sich vor, die Manuskripte
nach eigenem Ermessen zu bearbeiten. Honorare
nach Vereinbarung.

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

1 und I S. 11
CebiCon S. 17
ExperTeach S. 13

IBM S. 02
Strato S. 84
WHD. global 2012 S. 31

INSERTENTENVERZEICHNIS

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator
Jahresabo All-Inclusive** mit allen Monats-
ausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes
Sonderheft nur Euro 19,90 – und müssen
keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März
und Oktober jeden Jahres das jeweilige
IT-Administrator Sonderheft und mit
Ihrer Dezemberausgabe die jeweilige
Jahres-CD mit allen Monatsausgaben
des Jahres im PDF-Format zugestellt.



Als bestehender Jahresabonnent
können Sie hier upgraden:

[www.it-administrator.de/
abonnements/aboupgrade/](http://www.it-administrator.de/abonnements/aboupgrade/)

Oder Sie sind Neukunde? Hier können Sie bestellen:

[www.it-administrator.de/
abonnements/jahresabo/](http://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

www. .de

Martin Hummelt
STRATO Hosting-Kunde
www.freshpepper.de

Power Hosting

schon ab **5,90** €/Mon.*

**Jetzt starten und 6 Monate
die Grundgebühr sparen!**

**STRATO bietet Ihnen alles was Sie brauchen,
um Ihre Idee erfolgreich ins Internet zu bringen.**

- Bis zu 12 Domains, unlimited Traffic und 30 MySQL-Datenbanken
- Mehr Leistung: Bis zu 20.000 MB Speicher und 2 GB E-Mailspace
- Profi-Features: PHP, Perl, Python, Ruby und 1-Klick-Installationen
- **NEU!** Günstige Partnerangebote für individuelle Text- und Designkreation