3 | 15

Kostenlose Werkzeuge für Exchange

Raumüberwachung mit dem Raspberry Pi

Neu von TeamViewer: Monitis

ISSN 1614-2888
€ 12,60
Österreich € 14,50
Luxemburg € 14,50
Schweiz CHF 20,50

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Monitoring:

Überwachung von Exchange 2013

Durchblick mit Bordmitteln

Maximale Performance

SSD-RAIDs optimal betreiben

Container-Management

Docker mit Kubernetes administrieren

Im Test

VMware vRealize Hyperic

www.it-administrator.de

SERVERMEILE ENTERPRISE SOLUTIONS

Best Offer – Performance meets Capacity

NEW Intel® Server System **R2312WTTYS**, 2HE Rackserver
NEW Intel® Server Board S2600WT mit Intel® C612 Chipset
NEW 2x Intel® Xeon® Processor E5–2640 v3, 20MB Smart Cache
NEW 128GB DDR4 registered–ECC 2133Mhz (max. 3072GB)
NEW Intel® Integrated RAID Module RMS3CC040 – 4x SAS 12Gb/s – 1GB RAM
NEW Intel® RAID Controller RS3DC080 – 8x SAS 12Gb/s – 1GB RAM
NEW 2 x Intel® RAID Maintenance Free Backup Unit
NEW 720GB SSD RAID–5 – 4x 240GB SM843T Datacenter Performance SSD
28TB RAID–5 SAS Storage – 8x Seagate SAS Enterprise Capacity 4TB
NEW **2x 10Gbit/s Netzwerkadapter**
5 Jahre SLA Enterprise Vor–Ort–Service

EUR 11.229 zzgl.19% Ust.

High SAS I/O Performance Tower

NEW Intel® Server System **P4304XXMUXX**,
NEW 750W redundantes Server Netzteil 80+ Platin Effizienz
NEW Intel® Server Board S2600CW mit Intel® C610 Chipset
NEW 2x Intel® Xeon® Processor E5–2620 v3 – 6x 2.4Ghz, 15MB Smart Cache
NEW 64GB DDR4 registered–ECC 2133Mhz (max. 2048GB)
NEW Intel® Integrated RAID Controller RS3DC040 –
NEW 4x SAS 12Gb/s – 1GB RAM
Intel® RAID Maintenance Free Backup Unit
NEW 1.2TB RAID–5 Storage – 3x 600GB 12Gb/s Seagate Enterprise Performance 15K SAS 128 MB Cache mit 120GB Enterprise **SSD Fast–Path I/O Optimierung**
2x 1Gbit/s Netzwerkadapter
3 Jahre SLA Enterprise Vor–Ort–Service

EUR 6.799 zzgl.19% Ust.

1HE Enterprise Server

NEW Intel® Server System **R1304WT2**, 1 HE Rackserver
NEW 750W redundantes Server Netzteil 80+ Platin Effizienz
NEW Intel® Server Board S2600WT mit Intel® C612 Chipset
NEW 2x Intel® Xeon® Processor E5–2650 v3 – 10 x 2.3Ghz 25MB Smart Cache – 9,6GT/s QPI, Turbo–Frequency 3.0 Ghz
NEW 64 GB DDR4 registered – ECC 2133 Mhz
2x Intel® i350 Gigabit LAN Adapter

EUR 4.699 zzgl.19% Ust.

Storage Server mit 20 Gbit/s Network I/O

NEW Intel® Server System **R2224WTTYS**, 2HE Rackserver
NEW Intel® Server Board S2600WT mit Intel® C612 Chipset
NEW 2x Intel® Xeon® Processor E5–2607 v3 – 6x 1.9Ghz, 15MB Smart Cache
NEW 32GB DDR4 registered–ECC 2133Mhz (max. 3072GB)
NEW Intel® Integrated RAID Module RMS3CC080 – 8x SAS 12Gb/s – 1GB RAM
NEW Intel® RAID Maintenance Free Backup Unit
22TB RAID–6 SAS Speicher – 24x Seagate 2,5 SAS Server Festplatte 1TB
KVM over IP mit separatem LAN–Port
NEW **2x 10Gbit/s Netzwerkadapter**

EUR 9.249 zzgl.19% Ust.

IT - CONSULTING

- Analyse und Beratung von bestehenden IT–Infrastrukturen
- Begleitung von zeitkritischen Serverumzügen für Windowsserver
- Aufbau von hochverfügbaren Clustersystemen
- Einführung und Überwachung von komplexen Backupstrategien
- **Über 20 Jahre Erfahrung mit IT–Infrastrukturen**

RECHENZENTRUM IN BERLIN

- Unterbringung von Serversystemen im Rechenzentrum in klimatisierten 19“ Rackschränken
- 100% Naturstrom mit USV–Absicherung
- Internetanbindung über Premium IP–Carrier Level3
- managed Server Leistungen wie VPN, Firewalls, Backup, etc

SERVER MEILE

DIE SERVER-FERTIGUNG

NetApp Silver Partner

Servermeile GmbH

Mittelbuschweg 6
12055 Berlin

Tel.: 030 - 2000 50 - 500
Fax: 030 - 2000 50 - 555

Email: info@servermeile.com
http://www.servermeile.com

intel Technology Provider Gold 2015

Advanced Partner LANCOM Systems

EDITORIAL

Das Böse ist immer und überall

Liebe Leser,

bestimmt erinnern Sie sich an den Ohrwurm "Ba-Ba-Banküberfall" der Ersten Allgemeinen Verunsicherung. Gesungen zu Zeiten, als Bankräuber noch mit Strumpfmasken in eine Filiale stürmten, während ihr Komplize im geklauten Fluchtwagen mit laufendem Motor wartete. Die durchschnittliche Beute: mehrere Zehntausend Euro. Um bis zu eine Milliarde US-Dollar soll die Cybergang "Carbanak" Finanzinstitute weltweit erleichtert haben. Eine Milliarde.

Ihren Weg in die Bankennetze fand sie über Angestelltenrechner, die sie per Spear-Phishing übernahm. Anschließend arbeitete sie sich in die Videoüberwachungssysteme vor, um die Bildschirme der für Geldtransfers zuständigen Mitarbeiter auszuspähen. Der Rest ist Geschichte. Aufgedeckt wurde das Komplott unter anderem von Interpol, Europol und Kaspersky Lab. Nach zwei Jahren.

Vergleichen wir diesen Fall mit ähnlichen Online-Einbrüchen, zeigt sich, dass derart motivierte Angreifer Zeit haben und jede Lücke für sich auszunutzen wissen. Dabei legen oft weder Unternehmen noch IT-Hersteller die Hürde überhaupt besonders hoch. Aktuelles Beispiel: MongoDB. In ihrer – offenbar gern genutzten – Standardkonfiguration ließ sich die Datenbank von jedermann abfragen und bearbeiten, auch im Internet. Millionen Kundendaten lagen offen, ganz ohne APTs und Zero-Day-Exploits. Oder der kürzlich gehackte US-Krankenversicherer Anthem, dessen Daten von 80 Millionen Kunden unverschlüsselt auf dem Präsentierteller lagen. Ein Eldorado für Cyberkriminelle.

Natürlich ist kein Produkt fehlerfrei und jedes Sicherheitskonzept lässt sich mit genügend Ausdauer und Raffinesse aushebeln. Vermeidbare Schwachstellen jedoch machen ein Unternehmen zur unnötig leichten Beute. Über 90 Prozent der webbasierten Angriffe lassen sich nach einer Untersuchung der Dennis Technology Labs bereits durch ein aktuelles System abwenden. Ebenfalls eine entscheidende Rolle spielt in dem Zusammenhang das frühzeitige Erkennen von Einbrüchen.

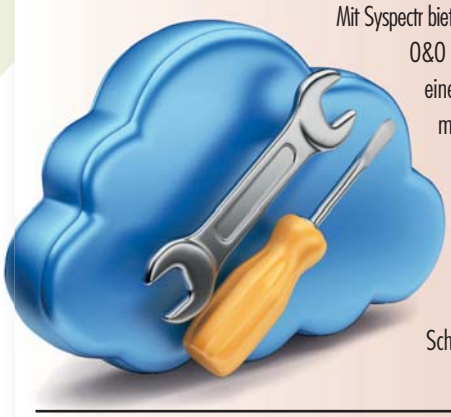
Um einen Beitrag für mehr Sicherheit in Ihrer IT-Umgebung zu leisten, zeigen wir Ihnen in dieser Ausgabe, wie Sie Ihre Active Directory-Verbunddienste im Auge behalten (Seite 74) und Logdateien unter Linux (Seite 78) auswerten. Außerdem erfahren Sie ab Seite 99, auf welche Aspekte es beim organisationsweiten Security-Monitoring ankommt – denn das Böse ist immer und überall!

Viel Spaß beim Lesen und einen sicheren Frühling wünscht

Daniel Richey,
Stellv. Chefredakteur

Monitoring

Im Test: O&O Syspectr



Mit Syspectr bietet das Berliner Unternehmen O&O Software seit gut einem Jahr einen Cloud-Dienst an, der Administratoren das Verwalten von Desktop-Systemen und Servern erleichtern soll. IT-Administrator hat sich den Dienst und dessen Möglichkeiten wie auch Schwächen näher angesehen.

Seite 30

Hochverfügbarkeit mit der Oracle Standard-Edition

Ausfallsicherheit ist für eine produktive Datenbank nahezu unverzichtbar. Strebt jedoch der IT-Verantwortliche dieses Ziel mit seiner Oracle-Datenbank an, scheint die Standard-Edition dafür ungeeignet und nur der tiefe Griff in Portemonnaie zum Erwerb der entsprechenden Lizenz hilft weiter. Der Workshop berichtet von Projekterfahrungen bei der Nutzung der Standard-Edition für HA-Aufgaben und gibt Hinweise zur eigenen Umsetzung.

Seite 44

AKTUELL

TESTS

PRAXIS

SCHWERPUNKT

WISSEN

Open Source-Tools zum Log-Management unter Linux

Schon in kleinen Netzen spucken die laufenden Dienste zahlreiche Log-Daten aus. Administratoren laufen dann nicht nur Gefahr, eine Fehlermeldung zu übersehen: Einem Problem auf die Spur zu kommen, ähnelt dann auch der Suche nach einer Nadel im Heuhaufen. Die Informationsflut bändigen wollen Fluentd, Graylog2, Logstash und Octopussy.

Seite 78

Aufbau und Betrieb von organisationsweitem Security-Monitoring

Täglich entstehen im IT-Betrieb unzählige Daten, in denen sich sicherheitsrelevante Informationen verbergen. Doch händisch ist diesem Datenmeer keine sinnvolle Information abzuringen. Security Information & Event Management-Systeme sollen helfen, die organisationsweite Sicherheitslage der IT abzubilden. Dies kann jedoch nur funktionieren, wenn IT-Verantwortliche beim Design der SIEM- und Sensorarchitektur einige wichtige Grundregeln beachten. Wir stellen die wichtigsten Eckpunkte vor, die bei der Auswahl eines SIEM-Systems und beim Design des Zusammenspiels mit Datenquellen und nachgeordneten Systemen zu berücksichtigen sind.

Seite 99

Themenübersicht


Server- und Systemmanagement


Sicherheit


Weiterbildung


Clientmanagement


Messaging


Virtualisierung


Storage


Netzwerkmanagement

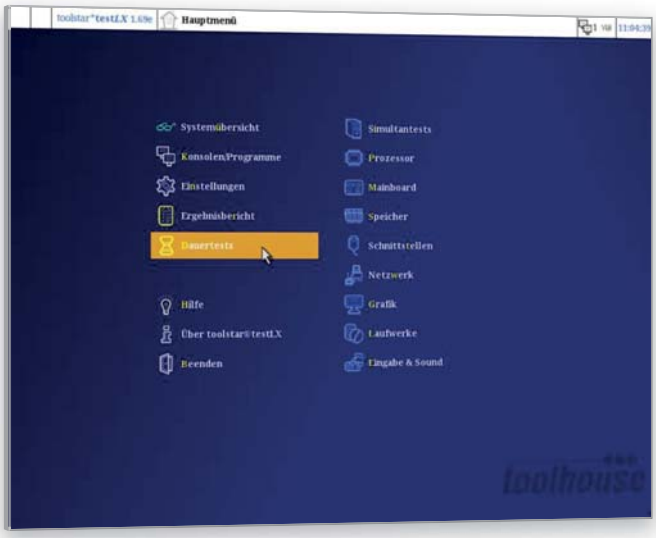

Recht

RUBRIKEN

Treffsicher testen

Mit der **Version 2.01 seiner PC-Testsoftware toolstar*testLX** bietet toolhaus Supportern zahlreiche neue Features. Dazu zählen vollständig erneuerte Speichertests, die mit **direkteren Zugriffen auf das RAM** eine bessere Quote der Fehlererkennung bieten sollen. Neu in toolstar*testLX ist die **Akku-Analyse für Notebooks**, die Daten wie Hersteller, Modell, Seriennummer, Typ, aktuelle Spannung und mehr ermittelt. Auch lässt sich die Software jetzt direkt mit aktivem SecureBoot booten – UEFI-SecureBoot muss nicht deaktiviert werden. Bei der Datenverwaltung bringt die Version 2.01 einerseits ein verbessertes Löschen von Daten, indem es **Shreddern auch in ansonsten unzugänglichen Sektoren** wie zum Beispiel Reserve-Sektoren bei SSDs ermöglicht. Anderseits lassen sich nunmehr mehrere Festplatten im Dauertest gleichzeitig testen oder shreddern. In den Testumfang der Software hat der Hersteller die neuesten Mainboards, Chipsätze, CPUs, Controller sowie LAN-, Grafik-Devices integriert. *(jp)*

toolhouse: www.toolhouse.de



Die Version 2.01 von toolstar*testLX erlaubt jetzt den parallelen Dauertest mehrerer Festplatten.

Neue Software-Zentrale

Aagon präsentiert die **Client-Management-Suite ACMP** in **Version 5.0**. Eine komplett **überarbeitete Oberfläche** samt neuen Icons und Überschriften soll die Bedienung der Suite erleichtern. **Verbesserte Performance-Einstellungen** erhöhen laut Aagon zudem die Stabilität, während die neue Version eine deutlich höhere Arbeitsgeschwindigkeit mitbringen soll. Ebenso wurden die **Automatisierungsmöglichkeiten für administrative Aufgaben** erweitert. Zu den wesentlichen Neuerungen von ACMP 5.0 gehört das **OS Deployment**, das ein einfaches Betriebssystem-Rollout – inklusive des neuen Windows 10 – direkt aus ACMP heraus ermöglicht. Die Antwortdateien samt den Installationsdetails der Clients verwaltet ACMP unabhängig vom Betriebssystem. Für die Software-Verteilung sind keine Microsoft-Bereitstellungs-Tools oder Windows-Deployment-Services (WDS) erforderlich. Die Software-Verteilung lässt sich dabei per **Timing** steuern. Auch hat der Hersteller eine **Lizenz-Key-Verwaltung** integriert, die jederzeit ersichtlich macht, wie viele PCs die Lizenzen aktuell nutzen. Der Datenaustausch beziehungsweise die **Verschlüsselung** zwischen ACMP-Agent, Server und der Konsole findet nun durchgehend **Ende-zu Ende** statt. Auch die Übertragung per Internet ist per SSL verschlüsselt. ACMP 5.0 ist ab sofort verfügbar und unterstützt neben Windows 10, Windows 8.1 und 8 / 7 auch MacOS X ab Leopard sowie alle gängigen Linux-Distributionen mit Python 2.6 oder höher. Die Preise für die Lizenzen richten sich nach der Zahl der Arbeitsstationen und sind unabhängig von der Betriebssystem-Plattform. ACMP Desktop Automation kostet für 100 Clients beispielsweise 30,12 Euro pro Lizenz zuzüglich ein Jahr Wartung für 6,93 Euro pro Lizenz. *(dr)*

Aagon: www.aagon.de

MongoDB 3.0 veröffentlicht

Mit dem Release 3.0 ist nach Aussagen der MongoDB-Entwickler ein neuer **Meilenstein in der Geschichte der NoSQL-Datenbank** erreicht. So bringt **MongoDB 3.0** gleichzeitig bessere Performance und mehr Flexibilität. Letzteres wird durch eine Architektur erreicht, die es erlaubt, unterschiedliche Storage-Backends zu verwenden. Davon macht die im aktuellen Release enthaltene **Storage-Engine WiredTiger** Gebrauch, die durch den Einkauf der gleichnamigen Firma in den Besitz von MongoDB gekommen ist. Die originale Storage-Engine, die jetzt den Namen MMAPv1 erhalten hat, wurde dahingehend verbessert, dass sie gleichzeitige Zugriffe auf der Ebene von Collections erlaubt und **effizienteres Journaling** bietet. WiredTiger implementiert die Kontrolle für gleichzeitige Zugriffe auf der Ebene von Dokumenten und reduziert durch die Verwendung transparenter Komprimierung den Speicherplatz um bis zu 80 Prozent. Zum besseren Management enthält MongoDB 3.0 eine neue Software-Komponente namens **Ops Manager**, die viele der bisher verwendeten Tools für Provisioning und Automatisierung ablösen soll. Gleichzeitig bietet der Ops Manager eine API, über die er sich in bestehende Management-Umgebungen integrieren lässt. *(of)*

MongoDB: www.mongodb.com

Mozilla-Projekt startet Tor-Relays

Wie im Zuge des Polaris-Projekts angekündigt, hat die Mozilla-Initiative **Relay-Knoten zum Tor-Netzwerk** beigesteuert, das **anonymisierten Internet-Zugang** bietet. Dafür setzt sie ausgemusterte Rechner in einem redundanten Setup ein. Es handelt sich um zwei Juniper-Switches EX4200 und drei HP-Server mit je 48 GByte RAM, zwei Xeon-Prozessoren und zwei GBit-Ethernet-Karten. Ans Internet angebunden sind die Tor-Relays über zwei 10 GBit-Leitungen. Dank des redundanten Setups arbeitet das Relay weiter, wenn ein Knoten ausfällt, bietet aber dann nur noch 50 Prozent der Kapazität. In dem Blog-Beitrag, der das neue Relay ankündigt, erläutert ein Administrator die grundlegenden Überlegungen, Einschränkungen und die dahinter liegende Software-Infrastruktur. So ist es aus Sicherheitsgründen im Rahmen des Tor-Projekts gar nicht erlaubt, dass sich mehr als zwei Tor-Knoten eine IP-Adresse teilen. Andernfalls könnten Angreifer eine Vielzahl von Fake Nodes starten, um die Anonymisierung auszuhebeln. Außerdem dauere es **bis zu zwei Monate, bis ein neu gestartetes Relay seine volle Bandbreite ausschöpfen könne**. Man wolle deshalb die Auslastung genau beobachten und sei gespannt, ob auch der Mozilla Tor Node diesem Muster folge. Zum Konfigurationsmanagement verwenden die Mozilla-Admins das **Ansible**-Tool, für das es bereits ein "ansible-tor"-Profil gibt, auf das sie zurückgreifen konnten. Ihre eigene Ansible-Konfiguration stellen sie auf Github zur Verfügung. Fürs Monitoring und die Visualisierung des Ressourcenverbrauchs setzen die Mozilla-Admins auf das **Observium**-Paket. Die Mozilla-Administratoren haben eine Reihe von Maßnahmen ergriffen, um ihr Tor-Relay abzusichern. Neben strikten Firewall-Regeln und der Basis-Härtung durch das Abschalten überflüssiger Services ist dies ein gesonderter Schutz der Management-Interfaces durch Paketfilter.

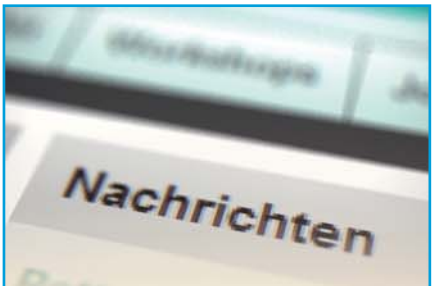
Deploying Tor Relays:
https://blog.mozilla.org/it/2015/01/28/deploying-tor-relays/

Management aus der Box

Dell präsentiert die neueste Version seiner **System-Management-Appliance KACE K1000**. Neue und verbesserte Funktionen sollen Anwendern helfen, **Rechner in Multi-Plattform-Umgebungen** zu identifizieren, zu konfigurieren, zu sichern und zu verwalten. So sollen Anwender von einer neuen, **agentenlosen Inventarisierung** von Windows-Servern und -PCs profitieren und mehr Kontrolle über die vorhandenen Systeme erhalten. Die Appliance bietet zudem eine optionale **Integration von Server-Monitoring-Protokollen und Warnmeldungen** für Windows, Linux und Unix-Server. Die Version 6.3 unterstützt dabei auch Chromebook. Die neue Version vereinfacht zudem das Patch-Management durch **Echtzeit- und Roll-up-Status-Reporting**. Weitere Verbesserungen umfassen laut Dell den Service-Desk, die bessere Integration mit dem herstellereigenen Enterprise Mobility Management über Single Sign-On und ein erweitertes Software-Asset-Management für die Unterstützung unterschiedlicher Lizenztypen sowie die Bestandsaufnahme von Anwendungen, die mit Microsoft App-V installiert wurden. Dell KACE K1000 in Version 6.3 steht ab sofort als physische, virtuelle oder gehostete Appliance zur Verfügung. Die Preise beginnen bei 7.140 Euro für die physische und virtuelle Appliance mit 100 verwalteten Systemen – Computer oder Server. K1000-as-a-Service ist für monatlich 5 Euro pro verwalteten Computer erhältlich. *(dr)*

Dell: www.dell.com/kace

Die Dell KACE K1000 unterstützt nun auch Chromebook.



Good Technology stellt gemeinsam mit Samsung **Good for Samsung Knox** vor. Die Lösung kombiniert Goods App-Container und App-Ökosystem mit Samsungs KNOX-Plattform. Dies funktioniert so, dass ein von Good abgesicherten Bereich innerhalb einer Android-Installation mit Samsung KNOX erzeugt wird. Hier lassen sich dann sämtliche Good-Apps, mit Good abgesicherte Apps oder maßgeschneiderte Apps nutzen, die durch die Good Dynamics Secure Mobility-Plattform gesichert werden. Good will zudem umfassenden Support für das Mobile Device Management-API-Set von KNOX bieten. *(ln)*

Link-Code: F3A11

SolarWinds gibt den Startschuss für Version 11.5 seines **Network Performance Monitor**. Das Tool zur Netzwerküberwachung verfügt nun über spezielle Karten zur Drahtlosabdeckung, mit denen sich die Signalstärke entsprechend den Grundrissen anzeigen lässt. Eine Funktion zur Client-Standortnachverfolgung erlaubt es dem Administrator, nach Drahtlosgeräten im Netzwerk zu suchen und Endbenutzer und Rogue-Geräte visuell aufzuspüren. Außerdem bietet das Werkzeug dem Nutzer eine Kapazitätsprognose zur Planung der Netzwerkanforderungen. *(ln)*

Link-Code: F3A12

Cisco hat sein Managed-IT-Werkzeug **Meraki** erweitert. Die Cloud-basierten Services dienen nun nicht mehr nur zum Management von drahtlosen, mobilen Netzwerken, sondern auch von Switches und Sicherheitsfunktionen. So zählt zu den Neuerungen unter anderem ein umfassendes Unified Threat Management zur Identifikation und Abwehr von Bedrohungen, basierend auf der integrierten Sourcefire-Technologie. Auf Basis von MX Security Appliances will Cisco zudem die WAN-Funktionalität bei Public und Hybrid Clouds verbessert haben. *(ln)*

Link-Code: F3A13

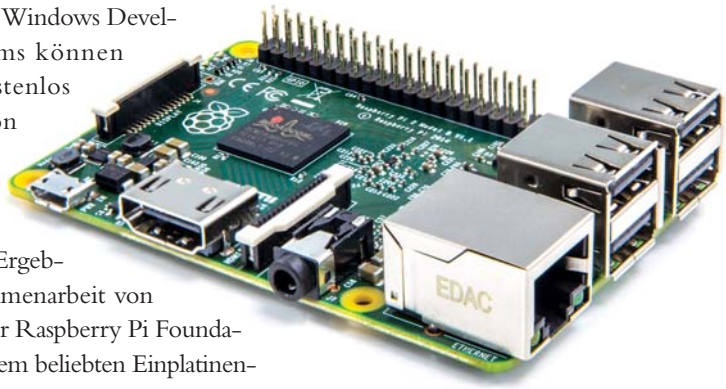
Mit Version 8.3 der Firewall **genugate** will **genua** für mehr Sicherheit bei Web-Diensten sorgen, die auf Basis des verbreiteten Service Oriented Architecture Protocol (SOAP) via Internet angeboten werden. Zu diesem Zweck hat der Hersteller das neueste Release mit einer speziellen Prüf-Software ausgestattet. Diese analysiert alle Anfragen und Antworten umfassend, bis hin zur Inhaltskontrolle. Dabei wird unter anderem geprüft, ob die Anfrage berechtigt ist, ob sie den Vorgaben entspricht und ob in den Formularfeldern ausschließlich zulässige Zeichen und Werte stehen. *(ln)*

Link-Code: F3A14

Online vorgestellt

Windows 10 auf Raspberry Pi 2 portiert

Im Rahmen des Windows Developer Programms können Entwickler kostenlos eine Version von **Windows 10 für Raspberry Pi 2** herunterladen. Das ist das Ergebnis einer Zusammenarbeit von Microsoft mit der Raspberry Pi Foundation, die hinter dem beliebten Einplatinenrechner mit ARM-Prozessor steht. Im Februar wurde die **neue Baureihe Raspberry Pi** 2 vorgestellt, die über einen **ARM Cortex A7 mit vier Cores und 900 MHz sowie 1 GByte RAM** verfügt. Ansonsten ist der Raspberry Pi 2 mit dem aktualisierten Vormodell identisch. Er besitzt eine erweiterte GPIO-Schnittstelle, vier USB-2.0-Ports, einen 100-MBit-Ethernet-Port und eine HDMI-Schnittstelle. Preislich beläuft sich der Raspberry Pi 2 auf 35 Euro. Mit Windows 10 für Raspberry Pi 2 will Microsoft seine Aktivitäten im Bereich **Internet of Things (IoT)** weiter ausbauen. Vorher gab es bereits eine Windows-Version für das Galileo-Board von Intel. Bislang wird der Raspberry Pi vor allem mit **Linux-Distributionen** betrieben, etwa mit einer speziellen Debian-Distribution namens Raspbian. *(of)*



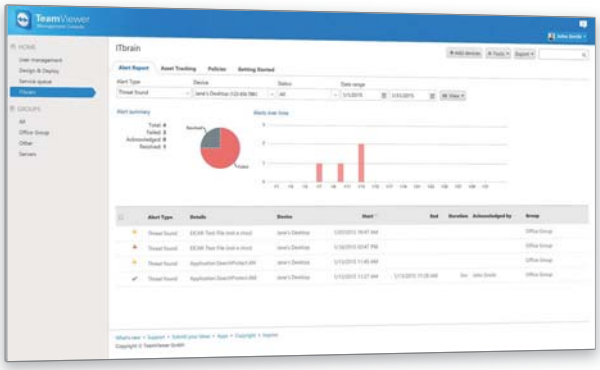
Die neue Generation des Raspberry Pi ist gegenüber dem Vorgänger bis zu sechsmal schneller.

Raspberry Pi 2: www.raspberrypi.org/raspberry-pi-2-on-sale/

Gefahrenabwehr mit Hirn

Aus dem Hause **TeamViewer** kommt mit **ITbrain Anti-Malware** ein **webbasierter Gefahren-Schutz** für kleine und mittelständische Unternehmen auf den Markt. Über eine **cloudbasierte Management-Konsole** können Firmen alle Endpunkte in Echtzeit zentral überwachen, unabhängig vom Mix an eingesetzten Windows-Desktops und -Servern. Ein Dashboard bietet dabei eine **Status-Momentaufnahme aller verwalteten Clients in Echtzeit**. Während Administratoren alle wesentlichen Rechte besitzen, haben Angestellte keinen Zugriff auf übergreifende Sicherheitsregeln und Einstellungen. Mehrmals am Tag aktualisiert sich das Werkzeug selbst, wobei die neuesten Signaturen heruntergeladen werden. Entdeckte **schädliche Dateien werden automatisch in Quarantäne verschoben**, ohne dass Mitarbeiter dafür aktiv werden müssen. Bei Bedarf kann der Anwender diese Dateien auch wiederherstellen. Unternehmen können Umfang und Spezifizierung der Scans zentral festlegen und anstoßen. So lässt sich etwa bestimmen, wann vollständige Scans zur Gewährleistung maximaler Sicherheit durchzuführen sind und wann schnelle Scans während der Arbeitszeit. Auch die Intervalle – ob täglich, wöchentlich oder selbstdefiniert – sind hier konfigurierbar. Laut TeamViewer basiert die Technologie hinter ITbrain auf einem bekannten Anti-Malware-Werkzeug, das bereits tausende von Unternehmen einsetzen. Pro Endpunkt werden im Abo-Modell rund 2,50 Euro pro Monat fällig. *(ln)*

ITbrain: www.itbrain.com/de/



Die TeamViewer-Management-Konsole bringt alle von ITbrain entdecken Bedrohungen übersichtlich auf den Schirm.

Auf in neue Sphären

VMware kündigt mit **VMware vSphere 6** die neueste Version seines Hypervisors an. Laut Herstellerangaben verbergen sich in dem Major Release mehr als **650 neue Features**. VMware vSphere 6 wird ergänzt durch die neuesten Versionen von VMware vCloud Suite 6, VMware vSphere with Operations Management 6 und VMware Virtual SAN 6. Zu den neuen Funktionen und Features von vSphere 6 zählen unter anderem die **breite Anwendungsunterstützung** durch verbesserte Skalierung, Performance und Verfügbarkeit. Somit soll vSphere 6 als Plattform für die **Virtualisierung von Anwendungen wie SAP HANA**, Hadoop, Microsoft SQL Server, Oracle Database und SAP ERP dienen. Neu ist auch die **Long-Distance Live Migration,** womit die Live-Migration über große Entfernungen hinweg möglich ist. Ein weiteres Novum ist die Multi-Prozessor-Fehlertoleranz, mit der Anwender von der **kontinuierlichen Verfügbarkeit von großen virtuellen Maschinen** mit bis zu vier virtuellen CPUs profitieren. Darüber hinaus ermöglicht die Instant Clone Technologie das rasche Kopieren und Bereitstellen von tausenden Container-Instanzen und virtuellen Maschinen. Diese werden **mit Instant Clone im Arbeitsspeicher geklont** und stellen so eine neue virtuelle Infrastruktur in kurzer Zeit bereit. Mit VMware vSphere Virtual Volumes soll zudem die native Virtual Machine-Awareness für eine Vielzahl von Storage-Systemen von Drittanbietern ermöglicht und so die Software-definierte Speichersteuerungsebene von VMware erweitert werden. Darüber hinaus erhöht VMware die Maximalwerte für vCPUs und RAM pro Host und VM, steigert die Anzahl möglicher Hosts in einem Cluster auf 64 und erhöht weitere Leistungsindikatoren mindestens um den Faktor zwei. VMware vSphere 6 ist im Laufe des ersten Quartals 2015 erhältlich. Die Preise für vSphere 6 beginnen bei 995 US-Dollar pro CPU. *(jp)*

VMware: www.vmware.de

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.

Testen Sie jetzt sechs Ausgaben zum Preis von drei!

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

shop.heinemann-verlag.de

Meine erste Firewall

Clavister will mit der **Firewall-Appliance W20** sein Portfolio um ein **kostengünstiges Einstiegs-Gateway** erweitern. Das Gerät erscheint in **zwei Varianten**, die sich im Leistungsumfang unterscheiden. Während das Standardmodell etwa auf eine Firewall-Performance von 3 GBit/s und eine VPN-Geschwindigkeit von 250 MBit/s kommt, kann die **Pro-Version 6 GBit/s und 300 MBit/s vorweisen**. Auch bei der Anzahl der gleichzeitig möglichen Verbindungen (250.000 versus 500.000) sowie der Menge gleichzeitiger VPN-Tunnel (250 versus 500, sowohl IPsec als auch SSL ist hier möglich) weisen die Geräte unterschiedliche Leistungsmerkmale auf. Beide Varianten laufen unter dem Betriebssystem Clavister cOS, verfügen über **sechs GBit-Ethernet-Anschlüsse** und messen im 19 Zoll-Rack-Format eine Höheneinheit. Punkten will der Hersteller auch mit einem leicht nachzuvollziehenden Security Service-Abonnement, das alle Software-Upgrades und Next Generation Firewall- und Unified-Threat-Management-Funktionen wie True Application Control zur Identifikation und Kontrolle von mehr als 2.300 Anwendungen beinhaltet. Der Listenpreis für die Standard-Variante der W20 beträgt 2.030 Euro. Ohne zusätzliche Lizenzkosten enthalten ist die Hochverfügbarkeits-Funktion – beim Kauf einer zweiten W20 lassen sich beide Geräte als Cluster betreiben. *(ln)*

Clavister: www.clavister.com

Mittels Clavister InControl lässt sich die W20-Firewall von zentraler Stelle aus managen.

Amazon mit neuem E-Mail-Dienst

Unter dem Namen WorkMail hat Amazon einen neuen Cloud-Dienst vorgestellt, der den **E-Mail- und Kalenderdienst für Firmen** übernehmen kann. Damit können Unternehmen auf die Installation eines eigenen Diensts verzichten und stattdessen den von Amazon bereitgestellten Dienst für ihre Zwecke konfigurieren. Sicherheit und Datenschutz werden dabei nach Angaben von Amazon groß geschrieben: Die **gespeicherten Daten werden mit Keys verschlüsselt**, die der WorkMail-Administrator über den AWS Key Management Service verwaltet. Zudem können Kunden das zur Speicherung verwendete Data Center auswählen – seit kurzem betreibt Amazon beispielsweise auch in Frankfurt ein Rechenzentrum. Derzeit bietet Amazon den Dienst als Preview aber nur in den Data Centern Virginia (USA) und Irland an. Amazon WorkMail ist insbesondere als **Exchange-Ersatz** konzipiert und unterstützt beispielsweise die wichtigsten Microsoft-Mailclients wie Outlook 2007, 2010, 2013 auf Windows. Außerdem ist WorkMail kompatibel zu Outlook 2011 auf OS X und Mailclients auf Mobilgeräten. Wer seine User in einem **Active Directory** verwaltet, kann es mit WorkMail verbinden, sodass Anwender mit ihren Login-Daten Zugriff auf den Amazon-Maildienst haben. Amazon bietet selbst als Mail-Frontend einen einfachen webbasierten Client. Auch **Spam- und Virenschutz** ist in dem Paket enthalten. Security-Policys für Mobilgeräte verteilt WorkMail mit dem ActiveSync-Protokoll. Für den Dienst berechnet Amazon 4 US-Dollar pro User und Monat, bei einer maximalen Mailbox-Größe von 50 GByte. Eine 30 Tage gültige Testsubskription ist auf 25 Anwender beschränkt. *(of)*

Amazon Workmail: http://aws.amazon.com/de/workmail/

Jetzt wird's schmutzig

bintec elmeg gibt mit Modell **bintec WI1003n** den Startschuss für einen neuen **Access Point**, der speziell für den Einsatz in industriellen Produktionsstätten und die **Maschine-zu-Maschine-Kommunikation** konzipiert ist. Das Gerät besitzt die Schutzklasse IP40 und trotzt somit auch rauen und verschmutzten Umgebungen sowie extremen Temperaturen – der Hersteller nennt hier einen Bereich zwischen -20 und +50 Grad Celsius. Der Neuzugang verfügt über ein **Funkmodul nach 802.11abgn** mit MIMO 2x2-Technik und ermöglicht Bruttodatenraten bis zu 300 MBit/s. Das Funkmodul lässt sich **wahlweise für den 2,4-GHz- oder für den 5-GHz-Bereich** einsetzen. Neben dem Access Point-Betrieb ist es möglich, die Netzwerkkomponente als WLAN Client und als Bridgelink-Gerät zum Aufbau drahtloser Funkbrücken einzusetzen. Als WLAN Client soll das neue Modell eine einfache Anbindung von Maschinen an das Unternehmensnetz erlauben. Durch Scannen der relevanten Funkkanäle im Hintergrund kann das Gerät laut Hersteller nahezu unterbrechungsfrei zum nächsten AP wechseln, falls die Maschine sich aus dem Bereich des jeweiligen Access Points bewegt. Der Access Point lässt sich durch den zentralen bintec WLAN Controller managen. Für kleine WLAN-Netze bis sechs APs kann die Neuvorstellung selbst die Rolle des WLAN Controllers übernehmen. Das Aluminiumgehäuse ist konventionell an die Wand oder mit DIN-Hutschienenadapter in eine Schalttafel montierbar. Als Preis nennt bintec elmeg rund 500 Euro. *(ln)*

bintec elmeg: www.bintec-elmeg.com/de/

Für den Einsatz in beweglichen Geräten bietet der bintec WI1003n im Client Mode einen Fast-Roaming-Modus.

Turbo-Restore dank SSD

Unitrends lüftet den Vorhang für die nächste Generation seiner **Backup-Appliances** der Recovery Series. Das erweiterte Portfolio umfasst Modelle mit **Speicherkapazitäten zwischen 1 und 97 TByte**. Mit Hilfe von **SSDs für Tiered Flash Storage** will der Hersteller neue Maßstäbe bei der Backup- und Recovery-Performance setzen. Nutzer können Richtlinien zur Flash Cache-Nutzung einrichten, um die Performance bei wachsenden Datenmengen zu optimieren. Zu den Merkmalen der überarbeiteten Appliances zählen Verbesserungen bei der CPU (je nach Modell kommen zwischen zwei und 16 Prozessorkerne zum Einsatz), bei den Memory- und RAID-Funktionen sowie den Kompressionsmöglichkeiten. Über Unitrends Bridge ist es zudem möglich, gesicherte **physische Server als virtuelle Maschine wiederherzustellen**. Über das optionale Network Data Management Protocol (NDMO) sollen sich NAS-Speicher von EMC und NetApp besonders einfach sichern und wiederherstellen lassen. Die neuen Appliances erlauben weiterhin ein Backup in die Cloud, was sowohl mit einem herstellereigenen Angebot als auch mit den entsprechenden Diensten von Amazon, Google oder Dropbox funktioniert. Für Unternehmen mit kleinem IT-Budget eignen sich die Recovery-602- oder Recovery-603-Varianten mit einer Höheneinheit, die ab 3.400 Euro beziehungsweise ab 5.100 Euro erhältlich sind. Unternehmen mit hohen Speicheranforderungen haben die Wahl zwischen zwei neuen 3 HE-Modellen – die Recovery-933S mit einer Brutto-Kapazität von 37 TByte oder die Recovery-936S mit einem Brutto-Fassungsvermögen von 73 TByte – oder der 943S-Appliance mit vier Höheneinheiten und einer Kapazität von 97 TByte. *(ln)*

Unitrends: www.unitrends.com

Für jeden etwas: Die neuen Appliances der Recovery-Serie von Unitrends erscheinen in verschiedenen Modellvarianten.

Startschuss für Xen 4.5

Mit dem Mitte Januar vorgestellten **Release 4.5** haben die Entwickler die XM-Management-Tools aus der **Hypervisor-Distribution Xen** entfernt. In vielen Fällen sind die jetzt aktuellen XL-Tools kompatibel mit dem Vorgänger, aber sie bieten keine Möglichkeit zur Netzwerkkonfiguration. Dies muss der Administrator künftig mit den betriebssystemeigenen Tools erledigen. Das neue Xen-Release bietet für Windows-VMs einen Virtual machine generation identifier (VM Generation ID), der es ermöglicht, **Domain Controller mit Windows 2012 oder neuer zu migrieren**. Außerdem ist jetzt die Remus-Technologie unterstützt, die **kontinuierliche Live-Migration und darauf aufbauende Hochverfügbarkeits-Set-ups** ermöglicht. Bei der Integration in die Virtualisierungs-Abstraktions-Bibliothek Libvirt gibt es diverse Verbesserungen, etwa Support für PCI/SR-IOV (Single Root I/O), der auch Hotplug unterstützt. Auch die Migration von VMs ist mit der Libvirt möglich. *(of)*

Xen 4.5: http://wiki.xenproject.org/wiki/Xen_Project_4.5_Feature_List

NAS mit Notizfunktion

Zuwachs in der NAS-Familie von **QNAP** gibt es mit der neuen **Turbo NAS-Serie TS-x31+**. Die Tower-Modelle verfügen über **zwei (TS-231+) oder vier (TS-431+) Festplatteneinschübe** und einen 1,4 GHz ARM Cortex-A15-Doppelkernprozessor. Dank neuer VFPv4-Gleitkomma-Einheit und 1 GByte DDR3-RAM mit systemeigener Unterstützung für 6 GBit/s-SATA-Laufwerke sorgt die Reihe für einen maximalen **Durchsatz von bis zu 200 MByte/s**. Dank **Hardware-beschleunigter Verschlüsselung** sollen die Geräte auch mit AES 256 Bit-Full-NAS-Volume-Verschlüsselung noch auf Übertragungsgeschwindigkeiten von über 150 MByte/s kommen. Mit zwei GBit-LAN-Anschlüssen bieten die Netzwerkspeicher zudem zwei IP-Einstellungen und Modi zur Portbündelung. Damit ermöglichen sie Nutzern die Einrichtung einer Fehlertoleranz und Link-Aggregation für erhöhten Datendurchsatz. Drei USB 3.0-Ports komplettieren die Anschlussmöglichkeiten. Mit Apps wie der neuen **Notes Station 2.0** erstellen Anwender digitale Notizen in ihrer privaten Cloud, die sie zur gemeinsamen Nutzung an ausgewählte Kontakte weiterleiten können. Die App unterstützt den Import /Export von PDF-Dateien, RSS-Live-Feeds sowie Snapshots für die Versionskontrolle. Anwender erhalten eine Online-Vorschau auf beigefügte Multimedia-Dateien, AES 256 Bit-Verschlüsselung für Notizen und die Möglichkeit, in Evernote aufgezeichnete Notizen zu sichern und zu modifizieren. Das QNAP TS-231+ ist ab sofort für rund 240 Euro, das TS-431+ für 330 Euro erhältlich. *(ln)*

QNAP: www.qnap.com/i/de/

Wie bei NAS-Geräten üblich, lassen sich die Festplatten auch beim QNAP TS-431+ im laufenden Betrieb wechseln.

IT-Administrator Training

Open Source-Monitoring

Zusätzlich zu den beliebten Windows-Seminaren bietet IT-Administrator auch dieses Jahr eine Reihe von Trainings zu Open Source-Monitoring mit Check_MK an. An zwei Terminen finden die Seminare in München und Dietzenbach statt.

Wer mit Open-Source-Software seine Systemlandschaft überwachen möchte, sieht sich einer großen Auswahl an potenziellen Lösungen gegenüber. Alleine vom bekannten Monitoring-System Nagios gibt es diverse Ableger, aber auch Forks wie Shinken und Icinga, die mit den Altlasten des Systems aufräumen möchten. Als Nagios-Modul ist auch die Neu-Entwicklung Check_MK entstanden, die sich mittlerweile als eigenständige Lösung etabliert hat, die sich besonders leicht mit der Open Source Monitoring Distribution in Betrieb nehmen lässt.

In unserem Training erfahren Sie, wie Sie mit Check_MK ein professionelles Monitoring aufbauen können, um Netzwerk, Server, Betriebssystem und Anwendungen im Blick zu behalten. Dabei benötigen Sie explizit keine Linuxkenntnisse. Die Arbeit auf der Kommandozeile wird bei Check_MK auf ein Minimum reduziert, da mit WATO ein mächtiges webbasiertes Konfigurationsmodul vorhanden ist mit dem Sie problemlos auch große und komplexe Installationen meistern.

In diesem Training verwenden wir als Unterbau die Open Monitoring Distribution (OMD), die Installation und Update des Monitoring-Systems vereinfachen. Darin enthalten sind viele beliebte Addons wie NagVis (grafische Visualisierung) und PNP4Nagios (Langzeitaufzeichnung von Messwerten).

Im Rahmen des Workshops wird mittels OMD eine vollständige Monitoring-Umgebung installiert, die nicht nur Check_MK, sondern auch viele weitere nützliche Addons enthält. Anschließend richten wir Schritt für Schritt ein Monitoring von Netzwerkgeräten, Linux- und Windowsservern, Netzwerkdiensten und Anwendungen ein. Dabei erfahren Sie, wie Check_MK funktioniert, zum Beispiel Acknowledgements und Downtimes, wie man Benachrichtigungen konfiguriert, Hosts und Services Benutzern zuweist und vieles mehr.

Unser Training wendet sich an Linux-, Windows- und Unix-Administratoren, die mit Open Source-Software ihre Umgebung überwachen möchten. Die Teilnehmer bekommen dabei einen Einblick in die Installation und Konfiguration von Check_MK. Zu jedem der beiden Trainingstermine stehen 25 Plätze zur Verfügung, die erfahrungsgemäß schnell vergeben sein werden. Alle Details zur Anmeldung finden Sie im Kasten auf dieser Seite. IT

Die Inhalte des Trainings

- Von Nagios zu Check_MK
- Monitoring modular
- Automatische Erkennung und Einrichtung von Checks
- Monitoring von Linux, Windows und SNMP-Geräten
- Alarme, Acknowledgement und Downtimes
- Verteiltes Monitoring

Termin & Ort

Dietzenbach: Dienstag, 09. Juni 2015
ExperTeach Training Center Frankfurt, Waldstraße 94, 63128 Dietzenbach

München: Mittwoch, 10. Juni 2015
ExperTeach Training Center München, Wredestr. 11, 80335 München

Teilnahmegebühren

IT-Administrator Abonnenten zahlen 195,90 Euro inklusive 19% Mehrwertsteuer. Für Nicht-Abonnenten wird eine Gebühr von 254,90 Euro (inklusive 19% MwSt.) fällig. Die Teilnahmegebühr umfasst das Training inklusive Dokumentation und das Mittagessen sowie Kaffeepausen am Trainingstag.

Open Source-Monitoring

Dozent

Karl Deutsch ist freiberuflicher Linux-Berater und Trainer. Für Mathias Kettner ist er seit mittlerweile sechs Jahren als Dozent in Deutschland, Österreich und der Schweiz tätig. Er leitet unter anderem die fünftägige Schulung "Systemmonitoring mit Nagios und Check_MK".

Fachliche Leitung

Mathias Kettner ist Gründer der gleichnamigen Firma, die Schulungen und Beratung rund um Linux und Open Source anbietet. Ein Schwerpunkt ist dabei Monitoring, für das die Firma die Lösung Check_MK entwickelt hat, die als Open-Source-Software unter der GPL-Lizenz zur Verfügung steht.

Neben dem Open Source-Training bietet der IT-Administrator noch Seminare zu **Windows-Client-Management**, **vSphere-Tuning und -Monitoring** sowie **Best Practices für Hyper-V** an. Das Anmeldeformular und ausführliche Inhalte zu allen Trainings finden Sie unter www.it-administrator.de/workshops

Weitere Seminare

MONITORING **EXPO**

10. JUNI 2015 · MAINZ

NETWORKS · INFRASTRUCTURE · DATA-CENTER

Jetzt anmelden!

Network Monitoring & DCIM

IT Infrastrukturen wachsen stetig und durchdringen alle Bereiche der Wirtschaft sowie des täglichen Lebens. IT Infrastrukturen, egal ob gross oder klein, sind heute Lebensadern von Unternehmen und Organisationen und somit kritische Funktionseinheiten, die mit höchster Priorität gemanagt werden müssen. Ohne spezialisierte Produkte und Konzepte ist es fast unmöglich die Anforderungen an Sicherheit und Service zu erfüllen. Genau hier liefert die MONITORING EXPO das benötigte Expertenwissen um als IT Verantwortlicher seine Organisation weiter zu entwickeln.

Die EXPO

Die MONITORING EXPO bietet erstmals eine umfassende Plattform zur Information rund um das Thema IT Monitoring und zum Austausch mit den Spezialisten der Branche. Schwerpunkt ist die Vermittlung von Information und Wissen als Entscheidungsbasis für IT Verantwortliche. Entsprechend der Konferenzidee „Inform – Inspire – Interact“ gibt es Sessions mit Experten zu allen wichtigen Schwerpunkten und der direkte Austausch mit den führenden Herstellern. Die Konferenz garantiert jedem Teilnehmer einzigartiges Expertenwissen „Komm als Spezialist gehe als Experte“.

Aussteller

- Network Monitoring
- Infrastructure Monitoring
- DCIM Data Center Information Management
- Environmental Monitoring
- Monitoring „Internet of Things“
- Open Source Monitoring
- Monitoring of Things - Industrie 4.0

Media Partner

eco

IT Administrator – Das Magazin für professionelle System- und Netzwerkadministration

funkschau – Kommunikationstechnik für Profis

LANline – IT ▪ Netze ▪ Infrastruktur

GRASS CONSULTING

monitoring-expo.com

Im Test: iQSol PowerApp 2.1

Unter Strom

Quelle: neyro2008 – 123RF

von Jürgen Heyer

Zu einer professionell betriebenen IT-Umgebung gehören auch eine oder mehrere USVs zur Notstromversorgung, um bei einem Stromausfall nicht im Dunkeln zu stehen. Dies wiederum setzt eine zuverlässige Steuerung voraus, denn nur durch gezieltes Herunterfahren lässt sich die Beschädigung von Geräten vermeiden und Datenverlust vorbeugen. Genau hier setzt PowerApp an, das sogar rechenzentrumsübergreifend einsetzbar ist.

In kleineren Umgebungen mit wenigen Servern und USVs lassen sich diese meist direkt miteinander koppeln, um einen koordinierten Shutdown bei einem Stromausfall zu realisieren. Sobald es aber etwas komplexer wird und Abhängigkeiten zu berücksichtigen sind, bedarf es einer zentralen Steuerung aller Aktionen durch ein Tool wie PowerApp von der österreichischen Programmschmiede iQSol. Hierbei handelt es sich um eine Lösung in Form einer physischen oder virtuellen Appliance, die die Zustände der USVs sowie gegebenenfalls weitere Umgebungssensoren überwacht und auf dieser Basis die angeschlossenen Server herunterfährt oder auch virtuelle Maschinen in ein anderes Rechenzentrum verschiebt.

Für unseren Test nutzten wir die virtuelle Appliance PowerApp VM, die funktional mit den physischen Appliances vergleichbar ist. Sie unterstützt die Kontrolle von bis zu 1.500 Servern. Die beiden physischen Modelle PowerApp 1000 und PowerApp 500 sind für bis zu 1.500 beziehungsweise 250 Server geeignet.

PowerApp arbeitet bei den Zugriffen auf die Server ohne Agenten und nutzt ausschließlich SNMP zur Abfrage der USVs. Die Lösung ist von bestimmten USV-Modellen unabhängig und damit universell einsetzbar. Sie steht im Mitbewerb zu diversen Überwachungstools, die die großen USV-Hersteller selbst im Portfolio haben und als Ergänzung anbieten. Sicher sind diese Tools jeweils in erster Linie auf die eigenen USVs zugeschnitten, unterstützen teilweise aber auch Fremdgeräte. Daher stellten wir uns die Frage, wie sich PowerApp von diesen Tools abgrenzt.

Installation mit kleineren Hürden

PowerApp VM kommt nicht als fertig vorbereitete Appliance für VMware, sondern als ISO-Datei. Ein Leitfaden zur Installation und Konfiguration beschreibt die notwendigen Schritte leider nur sehr grob. So erhält der Administrator den Hinweis, dass er eine leere VM auf Basis einer 64 Bit-Vorlage von Ubuntu erstellen muss. Es fehlen jedoch in diesem Leitfaden Hinweise zum genaueren Sizing. Diese fanden wir dann im umfangreicheren Benutzerhandbuch sowie auf der Hersteller-Webseite. Einmal angestoßen läuft die Installation voll geskriptet automatisch ab. Dabei werden die Sprache und die IP-Parameter (IP-Adresse, Subnetz, Gateway und DNS-Server) abgefragt. Für einige weitere Angaben wie die Zeitzone macht das Setup Vorschläge, die wir allesamt übernehmen konnten. Nach den Abfragen dauerte der weitere Ablauf einige Minuten mit Neustarts der VM, das Setup empfiehlt eine Kaffeepause.

Anschließend steht dem Administrator eine Web-GUI zur Verfügung, direkt auf der Konsole der VM sind keinerlei Eingaben zu machen, sie wird allenfalls im Supportfall von iQSol genutzt.

Betreuung mehrerer Rechenzentren inklusive

Für die weitere Konfiguration ist es notwendig, die Mandantenfähigkeit beziehungsweise das Client-Konzept von PowerApp zu verstehen. Auch dieses ist im erwähnten Installationsleitfaden nicht umfassend beschrieben, was uns den Einstieg erschwerte.

So ist nach der Installation nur eine Anmeldung als sogenannter Superadmin möglich, um globale Einstellungen vorzunehmen (Zeiteinstellungen, Änderung der Netzwerkparameter, SMTP-und LDAP-Konfiguration, Einspielen der Lizenzdatei). Außerdem kann der Superadmin Updates einspielen und muss als wichtigste Aufgabe Clients, also Mandanten, anlegen. Ein Client kann beispielsweise ein Rechenzentrum sein oder eine Außenstelle. Unter der Superadmin-Anmeldung ist eine Erfassung der genutzten USVs und Server nicht möglich, erst innerhalb eines Clients.

Da die Lizenzierung auf Basis der erfassten Server erfolgt, muss der Superadmin jedem Client aus dem Gesamtlizenzpool eine ge-

Systemvoraussetzungen

Eine virtuelle Maschine mit den Anforderungen Dual Core CPU, 4 GByte RAM, 60 GByte HDD.

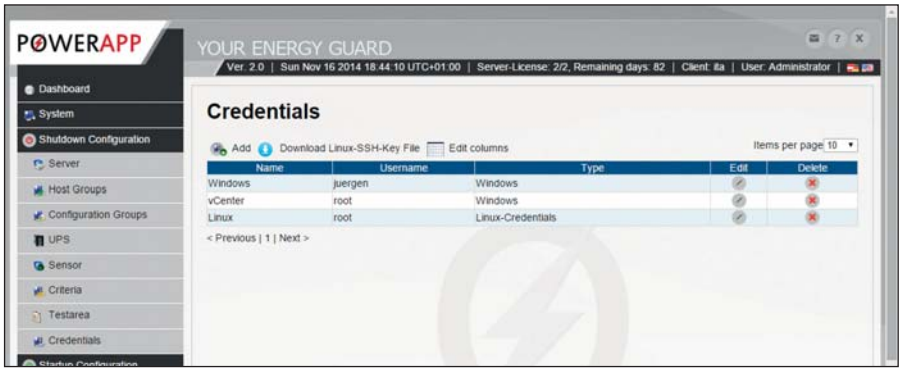


Bild 1: Für den agentenlosen Serverzugriff sind die Anmeldeinformationen für Linux und Windows getrennt zu hinterlegen.

wisse Anzahl an Lizenzen zuweisen. Die Verteilung kann er jederzeit ändern, sofern Lizenzen noch nicht genutzt sind. Jeder Client besitzt eine eigene Benutzerverwaltung, wobei bei der Anlage des Clients ein Admin-Benutzer erstellt wird. Für einzelne Außenstellen zuständige Administratoren können PowerApp dadurch praktisch eigenständig nutzen. Auch sind innerhalb jedes Clients wieder eigene SMTP- und LDAP-Einstellungen vorzunehmen, wobei wir uns wunderten, dass die globalen Einstellungen bei der Clientanlage nicht als Standard mit übernommen werden. Das könnte in den meisten Fällen diverse Mehrfacheingaben ersparen.

Neben der Nutzung eines LDAP-Verzeichnisses ist jeder Client wiederum mit einer eigenen lokalen Benutzerverwaltung ausgestattet. Über Gruppen können die Benutzer zusammengefasst und mit verschiedenen Rechten ausgestattet werden. Sofern eine Aufteilung der Umgebung in mehrere Clients nicht gewünscht ist, lässt sich natürlich alles unter einem Dach verwalten. Im Test legten wir mehrere Mandanten an, arbeiteten dann aber letztendlich mit einem.

Mühevolle Systemerfassung

Die Erfassung der zu überwachenden physischen Server erwies sich im Test als mühevoll, weil es keine Suchfunktion im Netzwerk gibt. Daher ist jedes System manuell einzutragen. Bevor jedoch der erste Server erfasst werden kann, sind zuerst Konfigurationsgruppen anzulegen. Pro Konfigurationsgruppe ist zu definieren, wie viele Minuten nach Auslösen eines Alarms die zu dieser Gruppe gehörigen Server die jeweils hinterlegte Aktion (Befehl ausführen, System herunterfahren, Wartungsmodus aktivieren) starten sollen.

Nachdem PowerApp ohne Agenten arbeitet, benötigt es Anmeldeinformationen für den Zugriff auf die Server und unterscheidet hier zwischen den Typen Windows- und Linux-Anmeldedaten sowie Nutzung eines Linux-SSH-Schlüssels. Positiv ist, dass sich die Server hinsichtlich der hinterlegten Anmeldeinformationen automatisch regelmäßig prüfen lassen, um zu erkennen, ob sich etwas geändert hat, was eine Steuerung durch PowerApp verhindert. Weiterhin kennt PowerApp Hostgruppen, um Server mit gleichen Eigenschaften und identischer Anmeldung zusammenzufassen.

Neben den Servern muss der Administrator die zu überwachenden USVs mit ihrer IP-Adresse erfassen. Die Kommunikation zwischen PowerApp und einer USV erfolgt grundsätzlich per SNMP, sodass PowerApp alle SNMP-fähigen USVs unterstützt, sofern die dazugehörige SNMP-MIB vorhanden ist und bei der Erfassung mit importiert wird. Das Einspielen der MIB ist erforderlich, da PowerApp von Haus aus keine USV-Modelle kennt. Vielmehr ist alles über SNMP-Objekte (SNMP-OID) zu definieren, wozu wir später noch kommen. Die agentenlose Arbeitsweise erlaubt es übrigens auch, beliebige andere Geräte wie Stromleisten und PDUs mit einzubinden, sofern eine Anmeldung möglich ist und eine Steuerung über Befehle unterstützt wird.

Kommunikation per SNMP-Polling

Bei der Kommunikation via SNMP verlässt sich PowerApp nicht auf Traps, sondern fragt die USVs per Polling mittels SNMP-Get ab. Das Abfrageintervall lässt sich einstellen und liegt standardmäßig bei 70 Sekunden. Sofern zusätzliche Sensoren wie Brandmelder oder Temperaturmesser eingebunden werden sollen, sind diese wie eine USV, jedoch in einer eigenen Rubrik, anzulegen. Auch ist die dazugehörige MIB nötig.

Der Administrator muss nun Kriterien definieren, die entsprechende Aktionen wie beispielsweise das Herunterfahren von Systemen auslösen. Dabei kann er verständlicherweise nur Informationen nutzen, die auch als SNMP-Objekt bereitgestellt werden, und er muss alles selbst entwickeln und testen, denn es sind keinerlei Abläufe vorbereitet.

Um das Festlegen von Kriterien für Aktionen zu vereinfachen, steht in PowerApp ein MIB-Browser zur Verfügung. Damit lassen sich die MIB analysieren, die relevanten SNMP-OIDs mit ihren Werten heraussuchen und Vergleichsregeln erstellen. Im Test hatten wir dies für die uns zur Verfügung stehende USV umgesetzt, mussten aber schnell erkennen, dass es recht mühevoll ist und intensiver Funktionstests bedarf. Gerade in einer heterogenen Umgebung mit mehreren USV-Modellen kann die Umsetzung langwierig und aufwändig werden.

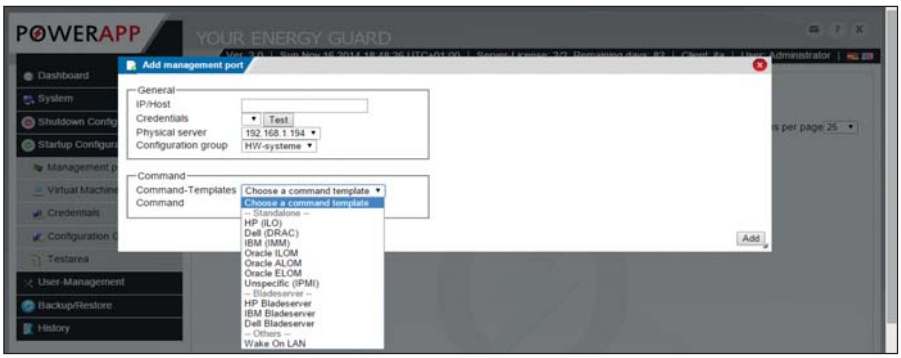


Bild 2: Zum Einschalten physischer Server unterstützt PowerApp die Fernsteuerzugänge verschiedener Hersteller.

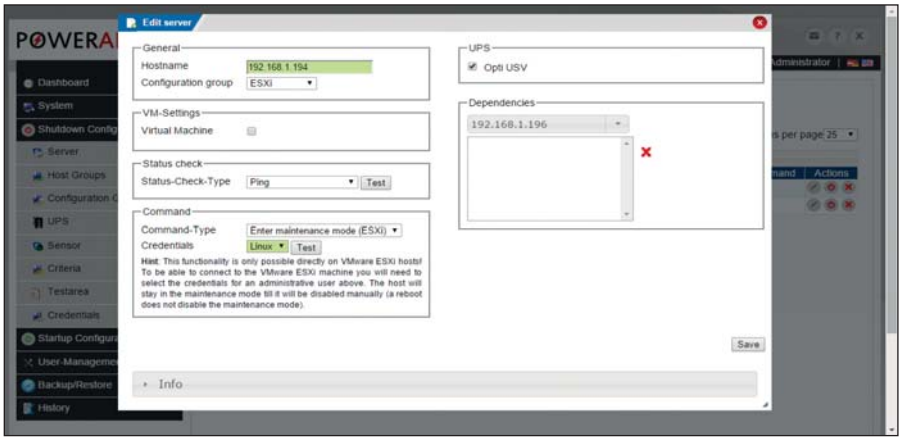


Bild 3: Bei der Aufnahme eines Servers sind diverse Eingaben notwendig, um den Anmeldetyp, die Aktion bei Ausfall und die Abhängigkeiten zu beschreiben.

Der Vorteil liegt aber in einer individuellen Programmierbarkeit. Prinzipiell lassen sich alle möglichen Ablaufszenarien realisieren, etwa ein zeitiger Lastabwurf durch das schnelle Herunterfahren weniger wichtiger Systeme und ein Abwarten für die wichtigen Server bis zu einer Restladung der USVs. Das Gelingen hängt allein davon ab, welche Informationen sich per SNMP abfragen lassen.

Nachdem PowerApp nur SNMP-Get-Kommandos nutzt, erfolgt der Zugriff ausschließlich lesend und auch nur, um daraus auf die hinterlegten Kriterien zu prüfen. Bis auf eine Ampelanzeige zum Status der USVs liefert die Appliance keine weiteren Informationen. Für einen tieferen Einblick in eine USV ist der Administrator letztendlich auf die jeweils mitgelieferten Werkzeuge angewiesen.

VM-Support in Maßen

PowerApp unterstützt beim Management der Server auch virtuelle Umgebungen unter VMware und Hyper-V, sowohl über einzelne Hosts als auch über das vCenter oder den SCVMM. Zu diesem Zweck muss PowerApp die virtuellen Maschinen kennen, um beispielsweise vor dem Herunterfahren eines Hosts die darauf laufenden VMs in einen definierten Zustand zu bringen (Ausschalten, Suspend) oder auf einen anderen Host zu verschieben. Zu diesem Zweck lassen sich die VMs manuell importieren, was wir in unserer Testumgebung mit einem vCenter realisieren wollten.

Als etwas holprig erwies sich hier die Angabe des vCenter-Servers, bei dem PowerApp davon ausgeht, dass es sich um einen physischen Windows-Server handelt. Da wir in unserer Testumgebung die vCenter-Appliance nutzten, mussten wir etwas tricksen und die Appliance in PowerApp als physische Maschine definieren. Andernfalls ließ sie sich nicht als vCenter-Server auswählen. Laut Hersteller ist dies bewusst so realisiert, damit der vCenter-Server nicht durch eine Eingruppierung als VM bereits ganz am Anfang mit heruntergefahren wird und PowerApp so die Steuermöglichkeit für die ganze virtuelle Umgebung verliert.

Wichtig ist nun noch vor dem VM-Import, dass alle Hosts der Virtualisierungsfarm in PowerApp erfasst und der richtigen USV zugeordnet sind, damit bei einem Stromausfall eine korrekte VM-Host-Zuordnung stattfinden kann. So bekamen wir nach dem Starten der Importroutine für den vCenter-Server alle angelegten VMs zur Auswahl mit dem vCenter als hinterlegtem Host. Sollte nun eine USV auf Batteriebetrieb schalten, wird über das vCenter ermittelt, auf welchen Hosts die VMs gerade laufen. Ein Shutdown oder eine Migration erfolgen nur für die VMs, die auf einem Host laufen, dessen USV gerade auf Batterie läuft. Das stellt sicher, dass auch in dynamischen Umgebungen immer die richtigen VMs adressiert werden.

Ein erneuter Import ist immer dann erforderlich, wenn neue VMs erstellt wurden, die unter PowerApp zu berücksichtigen sind. Die Importroutine unterstützt dahingehend, dass sie optional nur neue VMs oder auch nur laufende Maschinen anzeigt. Damit ist es recht einfach, beispielsweise Test-VMs, die meist ausgeschaltet sind, aus Sicht von PowerApp auszuklammern. Eine Automatisierung des Imports per Scheduler ist laut Hersteller bereits in Arbeit. VMs, die nach einem Import über längere Zeit wieder nicht erreichbar sind, können automatisch aus der Serverliste gelöscht werden, wobei der Administrator dies individuell konfigurieren kann.

Was das bereits erwähnte Migrieren von VMs anbetrifft, lässt sich als Ziel ein anderer Host angeben. Sinnvoll ist dies, wenn es ein zweites Rechenzentrum mit eigener Stromversorgung gibt. In größeren Umgebungen mit Ressourcenpools, die mehrere Hosts enthalten, könnte es zwar durchaus mehrere mögliche Zielhosts für eine VM geben, was sich aber in PowerApp nicht in vollem Umfang abbilden lässt. Nicht vorhanden ist übrigens ein Plug-In für eine vCenter-Integration.

Um einmal erstellte Kriterien für einen Shutdown möglichst praxisnah zu testen, stehen zwei Optionen zu Verfügung: So kann sich der Administrator auflisten lassen, welche Aktionen beim Zutreffen eines Kriteriums ausgelöst werden.

Da diese Auflistung noch nicht garantiert, dass auch alles so klappt, beispielsweise aufgrund falscher Anmeldedaten, kann er das Herunterfahren auch komplett ausführen lassen. Das setzt natürlich ein Wartungsfenster voraus.

Getrennte Verwaltung von Shutdown und Startup

Die bisherige Beschreibung der Gruppen, Anmeldedaten und Kriterien bezieht sich auf das Herunterfahren der Systeme (Shutdown-Prozess), was PowerApp in der Web-GUI auch als eigenen Menüblock behandelt. Ein weiterer, insgesamt etwas kleinerer Bereich ist die Startup-Konfiguration, um die Systeme nach einem Shutdown wieder koordiniert in Betrieb nehmen zu können.

Für das Einschalten unterstützt PowerApp die bei den renommierten Servermodellen üblichen Fernsteuerkarten oder -anschlüsse

(HP iLO, Dell DRAC, IBM IMM, Oracle ILOM/ALOM/ELOM) sowie das universelle IPMI-Protokoll und Wake-on-LAN. Auch Bladeserver von HP, Dell und IBM lassen sich einschalten sowie andere Systeme, sofern sie eine SSH-Verbindung unterstützen wie beispielsweise Cisco UCS. Es ist nur erforderlich, den korrekten Startbefehl zu ermitteln und im Kommandofeld einzutragen.

Produkt

Virtuelle oder physische Appliance zur Überwachung der USVs per SNMP für einen geordneten Server-Shutdown.

Hersteller

iQSol
www.iqsol.biz

Preis

PowerApp VM für 25 Systeme inklusive einem Jahr Wartung kostet 4.560 Euro, die PowerApp 500 Appliance für 100 Systeme mit Erstjahreswartung 10.860 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Steuerung physischer Server	7
Integration in VM-Umgebungen	6
USV-Kommunikation	5
Mandantenfähigkeit	7
Dokumentation	5

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Umgebungen mittlerer Größe, wenn es für die verwendeten USVs keine geeigneten Steuerwerkzeuge vom Hersteller gibt, Agenten auf den Servern nicht gewünscht sind oder eine individuelle Steuerung benötigt wird.

bedingt für homogene Umgebungen mit einfachen Standardanforderungen an die Steuerung. Hier sollten die Tools der USV-Hersteller im Vergleich betrachtet werden.

nicht für kleine Umgebungen, in denen sich eine direkte Zuordnung zwischen Server und USV realisieren lässt, sowie sehr große Installationen, die einen Server-unabhängigen Dauerschutz bieten (Notstrom).

iQSol PowerApp 2.1

Ähnlich zur Shutdown-Konfiguration sind für den Startup Anmeldedaten zu hinterlegen und Konfigurationsgruppen für eine zeitliche Koordination zu definieren. Die Konfigurationsgruppen sind über eine Liste in die gewünschte zeitliche Reihenfolge zu bringen. Dass zuerst die physischen Server hochzufahren und erst anschließend die virtuellen Maschinen zu starten sind, versteht sich von selbst.

Bezüglich der VMs kann der Administrator hinterlegen, welche im Rahmen eines Startups gestartet werden sollen und ob Abhängigkeiten untereinander zu beachten sind. Standardmäßig ist der automatische Start deaktiviert und es ist sicher sinnvoll, diesen auf die wichtigen Systeme zu beschränken. Da die Einstellung statisch ist, sollte sie regelmäßig kontrolliert werden. Auch für den Startup gibt es einen Testbereich.

Fest in PowerApp integriert sind Funktionen zum Sichern und Wiederherstellen der Konfiguration der Appliance. Dabei lässt sich die Konfiguration lokal sowie auf eine CIFS-Freigabe sichern und von dort auch wieder laden. Bei einem Restore ist es möglich, selektiv Objekte auszuwählen, damit nicht zwingend die gesamte Konfiguration überschrieben wird.

Um auch im Nachhinein kontrollieren zu können, was PowerApp durchgeführt hat, werden drei Protokolle geschrieben. Das Audit-Protokoll enthält alle von Benutzern durchgeführten Aktionen, das SNMP-Geräte-Protokoll listet alle Statusinformationen zu den USVs und Sensoren auf und im Server-Protokoll werden alle Statusinformationen bezüglich der Server aufgezeichnet.

Fazit

Vom grundsätzlichen Ansatz her ist ein zentrales Mandanten-fähiges Managementwerkzeug für die Verwaltung der USVs in einem Unternehmen eine gute Idee. Hinsichtlich der Ausführung, Funktionalität und Bedienbarkeit dürfte es bei PowerApp jedoch unter den Administratoren sehr unterschiedliche Meinungen geben.

Wer eine komfortable GUI sucht, mit Agenten auf den Servern einverstanden ist, schnell ohne viel Programmierung sowie umfangreiche Tests zum Ziel kommen will und sich idealerweise für USVs von einem der großen Hersteller entschieden hat, kommt mit der dazu angebotenen Zusatzsoftware sicher schneller zum Ziel als mit PowerApp.

Wer jedoch den Anspruch erhebt, keine vorgefertigte Lösung zu nutzen, sondern alle Regelwerke inklusive Konzept selbst definieren will, der ist bei PowerApp richtig aufgehoben. Dann muss er aber bereit sein, auch wirklich von Grund auf zu beginnen. Generelles Optimierungspotenzial sehen wir bei PowerApp in der Dokumentation, die zwar die Funktionen grundlegend beschreibt, aber diverse Lücken aufweist. *(dr)*

NEXT GENERATION
1&1 CLOUD SERVER

Easy to use – ready to cloud.
Die neuen 1&1 Cloud Server bieten Ihnen die perfekte Kombination aus der Leistungsstärke dedizierter Hardware und der Flexibilität der Cloud!

FLEXIBEL & GÜNSTIG

Individuelle Konfiguration

- SSD, RAM und CPU sind unabhängig voneinander, flexibel einstellbar, und lassen sich so genau an Ihre Anforderungen anpassen

Kostentransparent

- **NEU:** Minutengenaue Abrechnung
- **NEU:** Gut strukturierte Kostenübersicht für effiziente Planung und Kontrolle

EINFACH & SICHER

1&1 Cloud Panel

- **NEU:** Die innovative, nutzerfreundliche Oberfläche – mit Smart-Administration – erleichtert die Verwaltung Ihres Servers

Sicherheit

- Die 1&1 Hochleistungs-Rechenzentren zählen zu den sichersten in Europa
- Backups und Snapshots vermeiden unbeabsichtigte Datenverluste
- Die integrierte Firewall wehrt Angriffe auf Ihren Server sicher ab

ALLES INKLUSIVE

Top-Performance

- **NEU:** Bereitstellung Ihres Cloud Servers in weniger als 1 Minute
- **NEU:** Premium SSD mit virtual unlimited Performance
- **NEU:** Private Netzwerke, professionelles API, Load Balancers, Firewalls und viele weitere Server Features einfach konfigurierbar
- **NEU:** Virtualisierung durch die führende Technologie von VMware
- **NEU:** Ready-to-use Applications inklusive: WordPress, Drupal, Magento
- Parallels® Plesk 12
- Unlimited Traffic

Internet made in Germany

DOMAINS | E-MAIL | HOSTING | SHOPS | **SERVER**

E-Mail-Adresse eingeben und direkt starten

JETZT 1 MONAT TESTEN!*

DE: 02602 / 9691
AT: 0800 / 100668

*1&1 Cloud Server 1 Monat kostenlos, ohne Angabe der Bankverbindung testen. Danach ab 15,84 €/Monat (Mindestkonfiguration). Keine Einrichtungsgebühr. Preise inkl. MwSt.
1&1 Internet AG, Elgendorfer Straße 57, 56410 Montabaur.

1&1

1und1.info

Im Test: Monitis

Online-Auge

von Sandro Lucifora


Quelle: bluedarkat – 123RF

Ständig über den Zustand der betreuten IT Bescheid zu wissen, ist die Erwartungshaltung an den Administrator. Um auch bei einem großen Fuhrpark unterschiedlicher Hardware für Überblick zu sorgen, buhlen zahlreiche Monitoring-Werkzeuge um die Gunst des Nutzers. Mit Monitis haben wir ein Cloud-basiertes Exemplar unter die Lupe genommen, das nicht jede Überwachungsanforderung umsetzen konnte.

Monitis gehört zur TeamViewer-Familie. Der Vorteil des auf Deutsch verfügbaren Tools ist, dass ein Unternehmen selbst keine IT zur Überwachung vorhalten muss. Der Dienst läuft vollständig auf der Serverfarm des Herstellers. Um herauszufinden, wie zuverlässig Monitis arbeitet, haben wir mit der Lösung über einen Zeitraum von mehr als einem Jahr reale Systeme in einer Produktivumgebung überwacht.

Um die Überwachungen einzurichten, loggten wir uns nach einer Registrierung auf der Webseite des Herstellers ein. Die Frontpage ist in Dashboards unterteilt, die sich individuell zusammenstellen lassen. Um die Übersicht zu behalten, generierten wir mehrere Dashboards, die als Registerkarten angeordnet sind. Das Menü ist übersichtlich und unterteilt sich in Monitore, Warnungen, Statusansichten, Berichte, Extras und Hilfe. Monitis unterscheidet zwischen internen und externen Überwachungen. Die internen beziehen sich auf Informationen, die das System durch einen auf dem zu überwachenden Server installierten Agenten erhält. Externe Überwachungen sind solche, die über das Internet die Verfügbarkeit von Diensten prüfen.

Unkomplizierte Agenten-Installation

Wir installierten Agenten sowohl unter Linux als auch auf Windows 2012-Servern. Unter Linux loggten wir uns auf der Konsole ein und luden den Agenten mittels wget herunter. Danach entpackten wir das tar.gz-Archiv im Ordner *opt*. Bevor wir den Agenten konfigurierten, stellten wir sicher, dass die Bibliotheken libssl, libc und libxml2 installiert waren. Ebenso öffneten wir in der Firewall den ausgehenden Port 443 für Monitis. Danach starteten wir die Konfiguration mittels *./monits.sh conf,* worauf uns das Skript neben den Credentials nach einer Bezeichnung für den Server fragte, die später in der Weboberfläche zu sehen war. Der Start über *./monits.sh start* verlief problemlos.

Ein Agent war jedoch selbst nach einiger Zeit nicht im Dashboard zu sehen. Daher überprüften wir mit *./monits.sh log* die entsprechenden Einträge und stellten fest, dass das System unser Kennwort nicht akzeptiert hatte. Um dieses noch einmal einzutragen, starteten wir die Konfiguration erneut, bestätigten alle Angaben und trugen nur das Kennwort neu ein. Danach war auch dieser Agent angemeldet.

Unter Windows verlief die Installation problemlos. Nachdem das Setup die Software installiert hatte, öffnete sich das Programm-Fenster, in dem wir wieder unsere E-Mail-Adresse, unser Kennwort und den Namen für den Agenten festlegten. Danach klickten wir auf "Start Monitoring" und nach kurzer Zeit stand dieser Server in der Liste aktiver Agenten.

Schnelles Einrichten einer Überwachung

Als Nächstes legten wir interne Überwachungen an. Dazu greift Monitis auf die zuvor installierten Agenten zurück und fragt bei diesen die gewünschten Informationen über den Server ab. Das hat den Vorteil, dass auch mehrere überwachte Server per NAT und einer IP-Adresse mit dem Internet verbunden sein können. Zudem müssen nicht alle möglichen Ports für die Abfragen geöffnet sein. Die Kommunikation zwischen Monitis und dem Agenten erfolgt über eine sichere SSL-Verbindung und den Port 443.

Wir riefen über das Menü "Monitore" den Punkt "Server/Geräteüberwachung" auf und erhielten eine Liste allgemeiner Überwachungen. Darunter die Einträge CPU, Arbeitsspeicher, Laufwerk, Linux-Auslastung, Datenträger E/A, Bandbreite, SNMP-Objekt, Ping sowie HTTP und HTTPS. Um unter Linux definierte Pro-

Systemvoraussetzungen

Über einen der verbreiteten Browser lässt sich Monitis von nahezu jedem Computer nutzen. Die zur Server-Überwachung benötigten Agenten liefert der Hersteller für die Linux-Distributionen Debian, Ubuntu, Red Hat, SuSE, Fedora und CentOS sowie für Windows ab XP. Für OS X sind keine Agenten erhältlich und laut Hersteller auch nicht geplant.

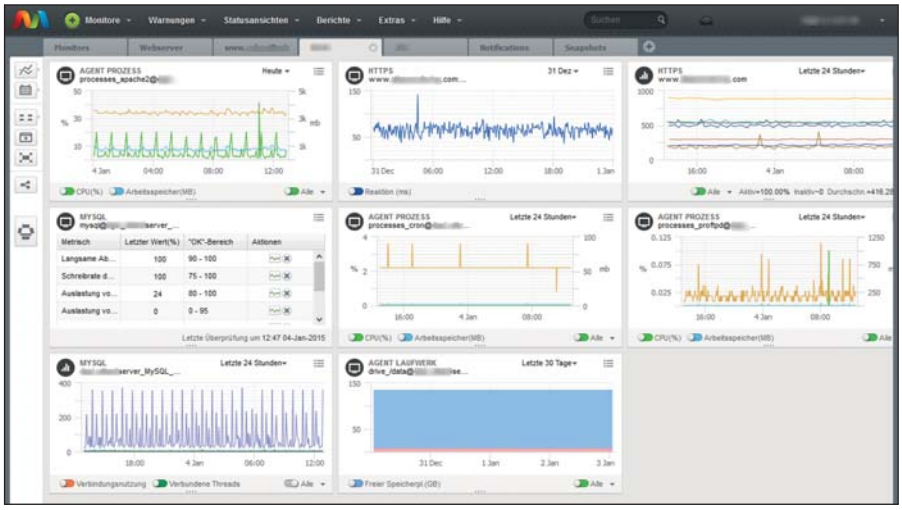


Bild 1: Das Dashboard von Monitis ist klar strukturiert und übersichtlich.

zesse und unter Windows spezielle Dienste abzufragen, gibt es noch die jeweils gleichnamigen Punkte zur Auswahl.

Als Erstes wählten wir den Eintrag CPU, worauf sich ein Fenster mit der Liste aller angemeldeten Agenten öffnete, aus denen wir einen auswählten. Im nachfolgenden Fenster trugen wir Grenz- und Warnwerte ein. Danach konnten wir auch direkt weitere Überwachungen hinzufügen und mussten dazu nicht wieder über das Menü gehen. Weiterhin gaben wir ein, zu welcher Warngruppe die Überwachungen gehören. Unter einer Warngruppe versteht der Hersteller die Konfiguration, wie und an wen Warnmeldungen zu versenden sind. Darauf kommen wir noch im Detail zurück.

Nach der Bestätigung fragte ein Dialog, an wen die Warnungen zu versenden sind. Dabei standen zur Auswahl "Alle aktiven Kontakte", "Benutzerdefinierte Auswahl" und "Keine Warnungen senden". Wir entschieden uns für den ersten Punkt, da wir die Warnungen selber in der Warngruppe festlegten. Danach definierten wir die Warnregeln beziehungsweise wählten eine bereits hinterlegte aus. Damit gaben wir an, an welche Kontaktgruppe und in welchen Fällen zu warnen ist.

Dashboard nicht nur übersichtlich

Nach diesem Dialog erschien das neue Widget der gerade erstellten Überwachung auf dem Dashboard. Beim Widget konnten wir zwischen Listenansicht, in der die erfassten Werte als Tabelle zu sehen waren, und einem Liniendiagramm auswählen. Kann eine Überwachung mehrere Werte anzeigen, wie zum Beispiel die CPU-Last in Prozent und den verwendeten Arbeitsspeicher in MByte, so zeigt das Liniendiagramm beide Werte an. Über Schalter konnten wir die Ansicht einzelner Werte ein- und ausschalten. Ebenso wählten wir aus, für welchen Zeitraum wir die Werte sehen wollten. Neben voreingestellten Zeitspannen konnten wir auch ein spezielles Datum zur Anzeige auswählen. Dies ist sehr hilfreich, um im Nachhinein die Daten eines Überwachungszeitraumes gezielt zu überprüfen.

Je nachdem, wie viele Überwachungen auf einem Register angeordnet sind, wird die Ansicht schnell unübersichtlich. Daher erlaubt Monitis das Anordnen der Überwachungen per Drag & Drop. Auch die Anpassung des Layouts eines jeden Registers ist möglich. Dabei standen das Raster für die Höhe sowie die Anzahl der Spalten der dargestellten Überwachungen zur Verfügung. Wir hätten uns gewünscht, dass die Einstellung pro Spalte möglich wäre, was bei bestimmten Werten sinnvoll ist.

Solide Erreichbarkeits- und Anwendungsüberwachung

Unter dem Menüpunkt "Betriebszeitüberwachung" hat der Hersteller die Überwachungen zusammengefasst, die Online-Dienste auf Erreichbarkeit prüfen, darunter HTTP und HTTPS sowie Ping, DNS, FTP, TCP, SSH, SIP und UDP. Mailserver prüft das System über die Dienste SMTP, POP3 und IMAP. Zudem gibt es noch Überwachungen für MySQL nach dem SOAP-Protokoll.

Im Regelfall prüfen die Überwachungen nur, ob die Dienste antworten. Das heißt, sie fragen die jeweiligen Ports ab und testen, ob diese erreichbar sind. Ein Funktionstest, wie zum Beispiel das Einloggen auf einem POP3-Konto oder das Login über FTP oder SSH, erfolgt nicht. Lediglich die Überwachung eines DNS-Servers erwartet bei der Einrichtung neben der URL auch den erwarteten Rückgabewert sowie den abzufragenden Nameserver. Mit diesen Daten überprüft Monitis nicht nur, ob ein DNS-Server erreichbar ist, sondern ob er für eine konkrete Domain die richtigen Daten zurückliefert.

Um die korrekte Funktion zu prüfen, gibt es auf Basis von Agenten die Anwendungsüberwachungen. Diese beschränken sich leider nur auf die klassischen Internet-Dienste wie Tomcat, Java, Oracle und MySQL. Neu hinzugekommen sind Anwendungsüberwachungen für node.js und die E-Mail-Übertragung. Gerade Windows-Services wie Exchange, MSSQL oder SharePoint lassen sich aber nicht mit dieser Funktion im Auge behalten.

Für den Test richteten wir eine Anwendungsüberwachung für MySQL ein. Dazu riefen wir den entsprechenden Monitor auf und wählten den Agenten aus. Im Dialog trugen wir die IP-Adresse des MySQL-Servers ein sowie den Port und gaben neben Nutzernamen und Kennwort auch eine abzufragende Datenbank an. Die Webseite prüfte die Angaben und nach erfolgreicher Verbindung sahen wir das Überwachungs-Widget auf dem Dashboard. Als Informationen erhielten wir nun die Zugriffszeit einer Standardabfrage durch den Agenten.

E-Mail-Überwachung per Weiterleitung

Ein spezieller Anwendungsmonitor ist die Überwachung für E-Mail-Übermittlungen. Er überwacht den gesamten E-Mail-Prozess, um sicherzustellen, dass die eingehenden und ausgehenden E-Mails ordnungsgemäß transportiert werden. Dabei prüft das System die gesamte Übermittlungskette, indem es eine E-Mail an eine definierte Adresse schickt. Um sicherzustellen, dass diese auch wirklich angekommen ist und vor allem wie lange

es gedauert hat, muss der Mailserver diese E-Mail an Monitis weiterleiten. So kommt die versendete E-Mail an Monitis zurück und der Monitor kann messen, wie lange die Übertragung dauerte.

Um diese Überwachung einzurichten, erwartete der Dialog die Eingabe der Test-E-Mail-Adresse. Diese richteten wir auf unserem E-Mail-Server ein und aktivierten die Weiterleitung von E-Mails an die vorgegebene Monitis-Adresse. Auch hier erschien nach der Bestätigung das Widget auf dem Dashboard. In der Überwachung des E-Mail-Roundtrips stellten wir die maximal erlaubte Zeit ein, die vom Versenden bis zum Empfangen der Test-E-Mail erlaubt ist. Da der Versand derzeit ausschließlich aus den USA erfolgt, hat dieser Weg bei uns zwischen 35 und 42 Sekunden gedauert. Das Prüfintervall lässt sich relativ frei einstellen.

Schnell zur eigenen Webseiten-Statistik

In der Gruppe "Endbenutzerüberwachungen" gibt es neben der Ladezeitüberwachung auch einen Transaktionsmonitor sowie den Real User Monitor (RUM). Dieser erlaubt es, die Besucherströme auf einer Internetseite zu erfassen und auszuwerten. Um diesen Monitor einzurichten, benötigten wir Zugang zum Quellcode der zu überwachenden Internetseite. Neben dem Domain-Namen wählten wir die zugehörige Überwachungsgruppe aus. Nun erstellte Monitis einen neuen Reiter mit einem vollflächigen Widget. Danach fügten wir ein vom System vorgegebenen Java-Skript-Aufruf in die Seiten ein, die wir mit RUM erfassen wollten.

Für Seitenbetreiber, die keinen Zugriff auf den Quellcode haben, aber mit einem CMS wie Wordpress, Joomal! oder Drupal arbeiten, stellt Monitis ein Plug-In zur Verfügung, das im jeweiligen Backend zu installieren und um die Tracking-ID zu ergänzen ist. Dieses fügt dann über das CMS den Aufruf beziehungsweise den notwendigen Quellcode in die Seiten ein.

Im Ergebnis sahen wir nach einiger Zeit im Überblick sowohl die Anzahl der Seitenaufrufe als auch die mittlere, minimale oder maximale Ladezeit. Weiter erfuhren wir die verwendeten Browser und Gerätetypen. Eine weitere Darstellung listete die geographische Zuordnung der Besucher-IP-Adressen auf. All diese Angaben konnten wir uns im Detail in Zusatzregistern ansehen. Zudem ließen sich alle Werte in eine Excel-Tabelle exportieren.

Bild 2: Die iOS-App erlaubt das Hinzufügen externer Überwachungen.

Vermisst haben wir die Möglichkeit, Zugriffe in den Statistiken herauszufiltern. Zum Beispiel ist es sinnvoll, Zugriffe aus dem eigenen Unternehmen aus der Statistik herauszunehmen, um so nur die wirklichen Kundenbesuche zu erfassen. Ebenso ist es hier nicht möglich, Warnmeldungen zu verschicken, beispielsweise wenn die maximale Ladezeit überschritten wird oder die Seitenzugriffe überproportional wachsen – etwa bei einem DDoS-Angriff.

Webapplikationen und Dienste im Auge behalten

Der Transaktions-Monitor ist für Webapplikationen interessant, um deren Funktionsweise zu überwachen, etwa bei E-Commerce-Lösungen oder Frontends wie Outlook Web Access. Hierzu benötigt Monitis ein Skript. Während der Einrichtung des Monitors konnten wir eine der wenigen vordefinierten Vorlagen auswählen oder ein eigenes Skript erstellen. Im Test gab es drei Vorlagen: Anmelden an Dropbox, an Office365 oder an Zendesk. Diese Muster dienen mehr der Veranschaulichung der Funktionsweise. Über ein Firefox-Plug-In nahmen wir eine Eingabesequenz auf, aus der dann ein Skript entstand. Dies luden wir in unseren Monitis-Account und wählten es für die Überwachung aus. Wieder legten wir fest, von welchen Orten der Zugriff zu testen ist und welche Benutzer im Fehlerfall zu benachrichtigen sind. Als Option bietet dieser Monitor lediglich "funktioniert nicht" an. Das heißt, läuft das Skript bis zum Ende durch, ist alles ok. Bricht es zwischendurch ab, erfolgt eine Warnmeldung. Wir hätten uns gewünscht, bereits hier auch Verzögerungen zu erkennen, die in der Regel auf eine hohe Auslastung eines Systems zurückzuführen sind.

Server-Überwachung top, Peripherie-Monitoring flop

Da sich die bisherigen Überwachungen auf Webseiten und -applikationen fokussierten, testeten wir noch die Prozess- und

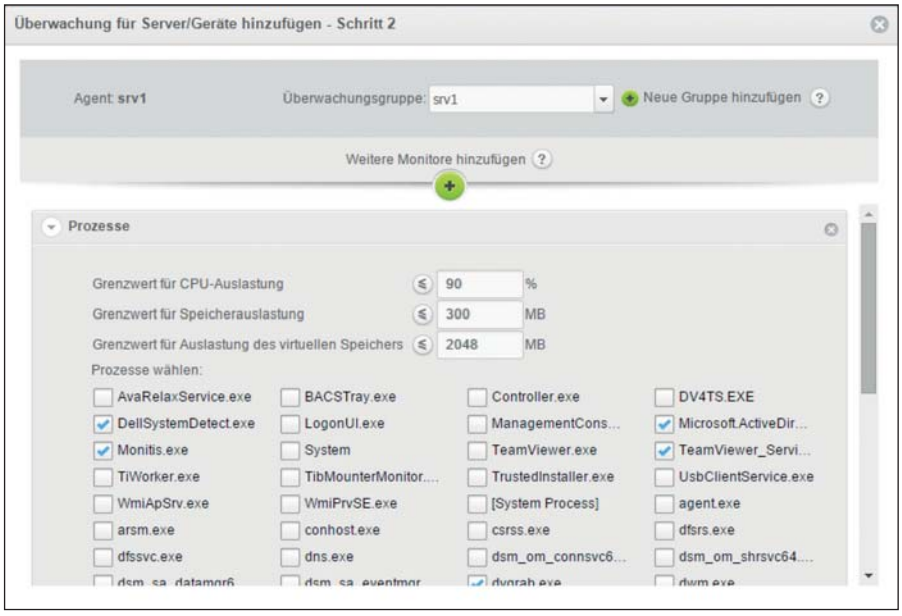


Bild 3: Dienste und Prozesse lassen sich auch im Bulk hinzufügen.

Dienste-Überwachung. Monitis unterscheidet dabei den Monitor für Linux, der Prozesse, und für Windows, der Dienste überwacht. Damit war es uns möglich zu prüfen, ob eben ein Prozess oder ein Dienst auf einem Server lief. Konkrete Funktionsweisen, wie die eines Exchange-Servers, ermittelte das System dabei nicht. Dieser Monitor ist für die Dienste und Prozesse gedacht, die sonst keine Überprüfung über die IP-Adresse und einen Port erlauben.

Auch hier riefen wir die Monitoreinrichtung auf und wählten den gewünschten Agenten aus. Danach fragte Monitis die auf dem Server laufenden Dienste ab und zeigte sie uns zur Auswahl an. Nun trugen wir Grenz- und Alarmwerte ein und gaben wiederum an, wer bei einem Ausfall zu benachrichtigen ist. Unter Windows überwachten wir auf diesem Wege unter anderem Dienste für Exchange, Acronis Backup und MSSQL-Server. Unter Linux prüften wir, ob Prozesse wie Cron, FTP, Postfix und Apache liefen.

Gänzlich vermissten wir eine Möglichkeit, im Unternehmen laufende und nicht aus dem Internet erreichbare Peripherie zu überwachen. So wollten wir zum Beispiel per SNMP einen Drucker abfragen und uns benachrichtigen lassen, sobald der Toner eine Füllstandmenge unterschreitet. Dies war nur möglich, wenn wir den Zugriff auf den Drucker per NAT und einer eigenen externen IP-Adresse ermöglichten. Andere Monitoring-Lösungen bieten für einen solchen Fall eine Software als internen Datensammler an, die innerhalb des Netzwerkes installiert ist, die Daten sammelt und an die Überwachungslösung sendet.

Benachrichtigungswege mit unflexibler Zeitplanung

Während des Einrichtens der Überwachungen trafen wir immer wieder auf die Auswahl der Monitor-Gruppe. Wie eingangs erwähnt, handelt es sich dabei um eine Konfiguration der Alarmeinstellungen, die Ansicht der Widgets und mehr. Diese Gruppen konfigurierten wir im Laufe der Testphase, sodass wir separate Alarmmeldungen erhielten.

Apps für iOS und Android

Zu den erwähnten Kontakten bietet der Hersteller in den jeweiligen Stores noch Apps an. Nach der Installation auf dem mobilen Gerät meldeten wir uns mit unserem Account an. Danach zeigte uns Monitis das mobile Gerät als zusätzlichen Kontakt an, dessen Warnmeldungen wir wie bei den zuvor beschriebenen Kontakten konfigurierten. Sobald eine Warnung vorlag und wir mit dem Tablet oder Smartphone online waren, erhielten wir eine Systembenachrichtigung. Weiter hatten wir die Möglichkeit, uns den Status der Überwachungen anzuschauen und externe Monitore hinzuzufügen. Die App ist demnach keine vollwertige Benutzeroberfläche, sondern dient lediglich dem schnellen Blick von unterwegs und dem Empfang von Warnungen.

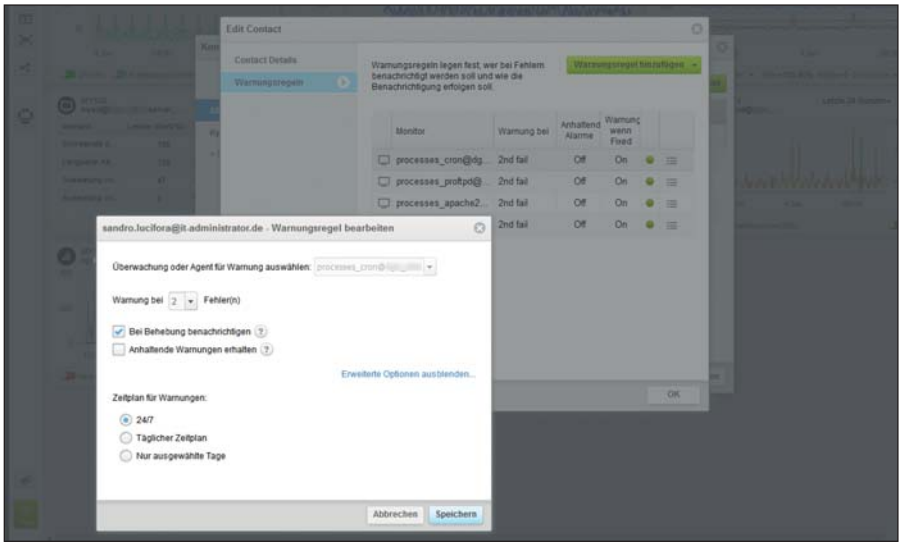


Bild 4: Jeder Kontakt erhält individuelle Einstellungen der Warnregeln.

Dazu richteten wir Kontakte ein, die wir der jeweiligen Gruppe zuordneten. Dabei definierten wir bei einem Kontakt neben dem Vor- und Zunamen auch die Art der Kontaktaufnahme. Zur Auswahl standen E-Mail, SMS und Telefonanruf. Weiterhin bietet Monitis die Benachrichtigung via Google Chat und Twitter an. Es war ferner möglich, eine URL mit Parametern im JSON-Format aufzurufen, um so zum Beispiel Daten in eine externe Datenbank zu schreiben oder über einen externen Dienste-Anbieter SMS zu versenden. Nicht zuletzt verfügt Monitis noch über Schnittstellen zu PagerDuty und VictorOps, beides freie Benachrichtigungsdienste.

Im nächsten Schritt stellten wir für jeden Kontakt Warnregeln ein. Für schon vorhandene Monitore bearbeiteten wir die Warnregeln. Dazu klickten wir auf "Bearbeiten" und definierten, bei wie vielen erkannten Fehlern wir eine Meldung wünschten. Das ist einstellbar, da gerade bei Online-Systemen Verbindungsprobleme auftreten können, die sich nach einer Weile von selbst erledigt haben. Dann legten wir fest, ob der Kontakt auch bei einer Behebung zu benachrichtigen ist und ob Monitis Meldungen bei anhaltenden Warnungen verschicken soll – sogenannte Reminder.

In den erweiterten Meldungen legten wir den Zeitplan für die Warnmeldungen fest. Neben 24/7 hatten wir zur Auswahl einen täglichen Zeitplan, zum Beispiel von 7 bis 22 Uhr, und einen für ausgewählte Tage. Leider sind beide Zeitpläne relativ unflexibel, da sich zum Beispiel nicht mehrere Perioden an einem Tag einstellen lassen. Auch der Zeitplan an ausgewählten Tagen erlaubt es lediglich, aufeinander folgende Tage auszuwählen – zum Beispiel von Dienstag bis Freitag von 8 bis 15 Uhr. Einzelne Tage und unterschiedliche Zeiten konnten wir nicht einrichten.

Fazit

Um im Testverlauf die Überwachungsfunktionen zu überprüfen, führten wir gezielte Überlastungen auf den überwachten Systemen durch oder stoppten Dienste und Services. Insgesamt konnten wir feststellen, dass Monitis alle Fehler im Rahmen der Zeitintervalle erkannte und die Warnmeldungen verschickte. Zu Anfang des Tests erreichten uns vermeintliche Fehlalarme, da wir Schwellenwerte oftmals zu niedrig eingestellt hatten. Im Laufe der Zeit passten wir die Überwachungen auf den jeweiligen Systemen an und konfigurierten die verschiedenen Gruppen so, dass wir möglichst perfekte Warnmeldungen erhielten.

Dabei stellten wir fest, dass uns vor allem die Funktion fehlte, Überwachungen in Abhängigkeit zu bringen. Meldet ein interner Monitor zum Beispiel, dass der Service Apache nicht läuft, reicht eine Warnmeldung, und weitere Monitore, die zum Beispiel die Ladezeit auf dem Server überwachen, müssten nicht auch einen Ausfall melden. Ebenso kristallisierte sich im Test heraus, dass sich die angebotenen Überwachungen zum größeren Teil auf Online-Server fokussieren. Auf Unternehmensservern konnten wir mittels Agenten nur den Status eines Dienstes ermitteln, nicht aber die richtige Funktionsweise der Anwendung prüfen.

Der Eindruck von Monitis ist je nach Anforderung gemischt. Wer das System für die Überwachung von Windows- oder interner Unternehmenshardware nutzen möchte, sollte sich vorher sehr intensiv die Möglichkeiten der vorhandenen Monitore anschauen und prüfen, ob diese ausreichen. Für die Überwachung von Online-Systemen und Internet-Aktivitäten ist Monitis hingegen sehr gut gerüstet und liefert eine Vielzahl guter Überwachungsfunktionen. *(ln)* IT

Produkt
Webbasierte Plattform zur Serverüberwachung.

Hersteller
Monitis
www.monitis.com/de

Preis
Ab 30 US-Dollar pro Monat, abhängig von der Leistung und den zu überwachenden Servern.

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

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

Monitore	5
Benachrichtigungswege	6
Erreichbarkeit	6
Datenaufbereitung	6
Warnmeldungen	5

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

gut zur Überwachung von Online-Systemen unter Windows und Linux.

bedingt als Monitoring-System für Windows-Application-Server im LAN.

nicht zur Überwachung großer Serverfarmen auf Windows-Basis ohne Zugriff aus dem Internet.

Monitis


Quelle: Vitaly Titov – 123RF

Im Test: VMware vRealize Hyperic

Der Alles-Seher

von Thomas Bär

Umfassende Überwachung von Anwendungen, Middleware, Betriebssystem und Infrastruktur – so lautet das erklärte Ziel von VMware vRealize Hyperic. Es verspricht die sofortige, automatische Erkennung von über 120 gängigen Middleware-Lösungen und Anwendungen. Dabei soll eine vorkonfigurierte Best Practice-Sammlung für Key Performance Indicators für eine schnellere Einrichtung der Überwachung durch den Administrator sorgen. Solch vollmundige Versprechungen lassen das IT-Profi-Herz aufhorchen und stellen sich unserem Test.

Da ein Großteil aller Applikationsserver in den Rechenzentren und Serverräumen durch Administratoren virtualisiert betrieben wird, liegt es in der Natur der Sache, dass VMware auch eine eigene Überwachungslösung im Portfolio führt: VMware vRealize Hyperic, als Komponente von VMware vRealize Operations. Um dem Namensspiel noch das sprichwörtliche I-Tüpfelchen zu verpassen – das Programm hieß zuvor vCenter Hyperic. Wie alle Anbieter dieser Größenordnung beginnt auch das Produktmanagement bei VMware seine Kunden durch stetes Umbenennen der Lösungen zu quälen, dies aber nur am Rande bemerkt.

In einem Satz: Hyperic überwacht Betriebssysteme, Middleware und Applikationen, die in physischen, virtuellen oder Cloud-Umgebungen ausgeführt werden. Laut Produktbeschreibung erhält der Administrator so leicht den verständlichen Einblick in die Verfügbarkeit, Performance, Auslastung, Ereignisse, Protokolle und Änderungen auf jeder Ebene des Virtualisierungs-Stacks – vom vSphere Hypervisor bis hin zum eigentlichen Gastbetriebssystem. Die Integration in vRealize Operations Manager bietet dem Kunden die nötige Transparenz und ermöglicht ein einheitliches Management von Infrastruktur, Middleware und Anwendungen über eine einzige Oberfläche. Hyperic von VMware erfasst eine große Anzahl von Performance-Daten, laut Herstellerangaben rund 50.000 unterschiedliche Messwerte zu mehr als 70 Anwendungstechnologien. Eine Erweiterung, um beliebige Komponenten der eigenen Anwendungen oder im Middleware-Stack zu überwachen, ist laut VMware ebenfalls möglich.

Monitoring mit und ohne Plug-Ins

System- und Netzwerküberwachung von verschiedensten Komponenten, beispielsweise über Standards wie SNMP, gehört heute zum guten Ton. VMware findet für diese Aufgabe etwas beschwingtere Beschreibungen, beispielsweise "Komplette Runbook-Bereitstellungsautomatisierung mit wiederverwendbaren Überwachungskonfigurationen und Benachrichtigungsrichtlinien – Ressourcen können in weniger als einer Minute in die Managementabläufe einbezogen werden" oder "Umfassende Überwachung von Performance-, Konfigurations- und Sicherheitsänderungen, korreliert in einer einfach zu lesenden UI für eine schnelle Ursachenanalyse". Letztendlich geht es jedoch darum, die wichtigsten Eckdaten der eigenen Anlage im Blick zu behalten, um Service Level Agreements (SLAs) oder Operational Level Agreements (OLAs) und andere Verträge gegenüber dem Kunden oder dem IT-Management einzuhalten. Beispielsweise die Datenbank-Verfügbarkeit, Exchange-Datenaustausch, Plattenspeicher oder Netzwerkkomponenten-Erreichbarkeit.

Sollte es für die eigene Anwendung oder eine spezielle Serversoftware nicht das passende Plug-In für Hyperic geben, so erlaubt das so genannte "HQU-Plug-In-Framework von Hyperic" die Darstellung und Sammlung von Performance-Daten für eigene Applikationen. Das HQU-Framework erweitert das Hyperic-User-Interface und ermöglicht es, Routineaufgaben zu automatisieren und Hyperic in andere Managementsysteme zu integrieren. Die in Groovy, einer dynamischen Skriptsprache für die Java Virtual Machine, geschriebenen HQU-Plug-Ins können bei Bedarf gemeinsam genutzt und aktiven Umgebungen hinzugefügt werden, ohne dass der Administrator hierzu den Hyperic-Server stoppen und neu starten müsste.

Die Namensänderung zu vRealize Hyperic war natürlich nicht die einzige Veränderung, die mit der Produktversion 5.8.4. im Dezember 2014 Einzug hatte. Erstmalig unterstützt die Software nun andere Sprachvarianten von Microsoft Windows als nur Englisch. Java in der Runtime Edition 7u71 wird nun unterstützt, ebenso erhielten einige Plug-Ins

Systemvoraussetzungen

Sie benötigen eine aktuelle VMware vSphere-Umgebung. Je nach gewählter Variante ist die Installation auf aktuellem Microsoft Windows-Server oder aktuellem Red Hat Linux-Server möglich. Alternativ nutzen Sie die virtuelle Appliance von VMware.

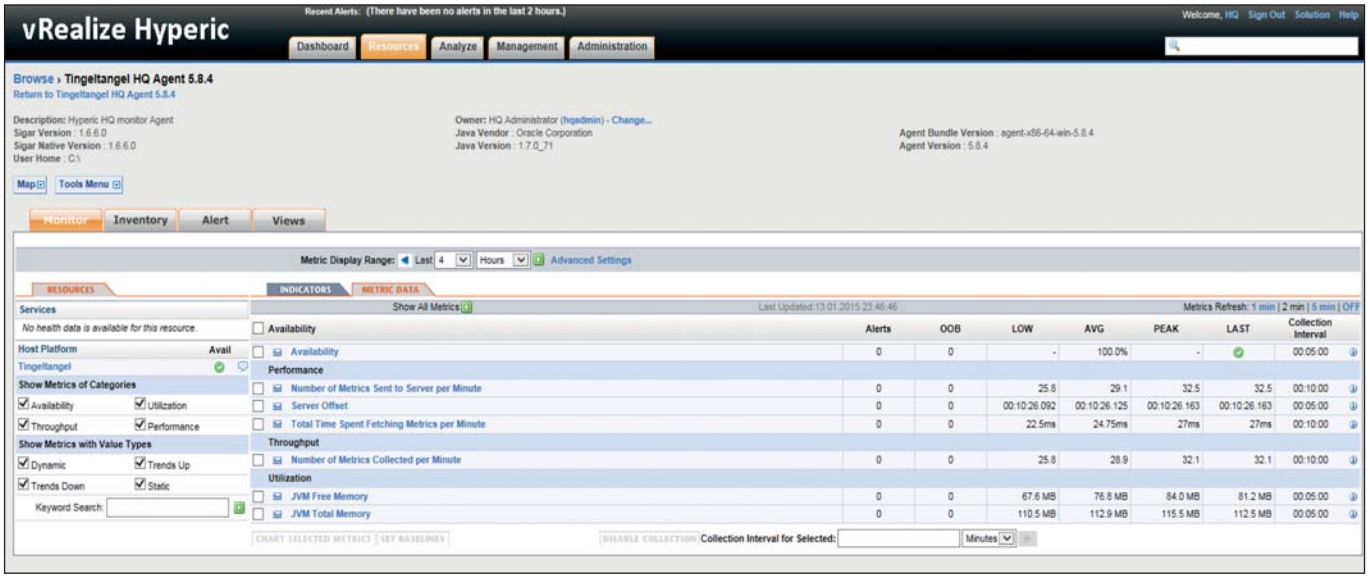


Bild 1: Hyperic ermittelt aus verschiedensten Plattformen und Applikationen Mess- und Kontrolldaten.

eine Verjüngung: PostgreSQL Plug-In Support für Windows 2012 R2 und SQL 9.2.x, bessere Erkennung von Speicherausnutzung und Swapping-Verhalten, Unterstützung von Hyper-V auf Windows Server 2012 R2, IBM DB2-Plug-In für Version 10 und das Oracle-DB-Plug-In arbeitet nun mit der Version 12 zusammen. Neue Plug-Ins haben die Entwickler für OpenStack, vCenter Orchestrator, vRealize Automation Appliance, vRealize Automation AppServices, vRealize Automation IaaS, vRealize Business Standard und vSphere SSO eingefügt.

Schnelle Installation als virtuelle Appliance

Erwartungsgemäß bietet VMware einen äußerst galanten Weg, um die Software im eigenen Rechenzentrum in Betrieb zu nehmen. Eine Testversion mit einer Laufzeit von 60 Tagen steht jedem Kunden zur Verfügung. Einzige Voraussetzung ist das Login mit einem VMware-Konto. Neben der vApp, die im OVF-Format mit 2,3 GByte Volumen heruntergeladen wird und über den vSphere-Client auf einen Hypervisor geladen wird, steht auch ein klassischer Installer für Microsoft Windows zur Verfügung. Die benötigte PostgreSQL-Datenbank richtet der Installer bei Bedarf mit ein. Eine Variante für RHEL 5 entdeckt der Linux-Administrator ebenfalls auf der Download-Webseite.

Wir nutzten in unserer Teststellung die vApp und spielten diese mit dem vSphere Windows-Client auf unserem ESXi 5.5-Testserver ein. Nach dem Dialogfenster "OVF bereitstellen…" erscheint direkt ein Software-Wizard, der die Passwörter für den Root-Zugang und für den Zugriff auf die Weboberfläche von Hyperic abfragt. Weitere Fragen an den Administrator beschränken sich auf das Zielsystem – auf welchem ESXi-Host die virtuelle Appliance zum Einsatz kommen soll und wie der Netzwerkzugriff zu erfolgen hat. Insgesamt dauerte der Vorgang der Grundeinrichtung nur ein paar Minuten und erforderte keinerlei Spezialkenntnisse.

Nach dem Upload der virtuellen Appliance entdeckt der Administrator in der Baumstruktur des vSphere-Clients zwei neue Server, die in einer vApp-Gruppe gemeinschaftlich ein- und ausgeschaltet werden können. Beim Einschalten startet der vFabric PostgreSQL-Datenbankserver innerhalb weniger Sekunden, es folgt der vCenter Hyperic Server. Sowohl die PostgreSQL-Datenbank als auch der Hyperic-Server zeigen den notwendigen Login-Link in der Konsole an. Es kommt das Passwort zum Einsatz, welches der Administrator im Zuge der Installation angelegt hat. Die wichtigsten Eigenschaften der vApp, wie IP-Bereiche, Port-Adressen oder Login-Namen, kann der IT-Profi im Eigenschaftendialog des vSphere-Clients anpassen. In der Standardkonfiguration ist der neue Hyperic-Server unter der Port-Adresse 7080 zu erreichen.

Ein erster Blick auf das Dashboard

Das erste Login auf der Port-Adresse 7080 öffnet das "vRealize Hyperic"-Dashboard für den Benutzer "HQ". Hier unterscheidet sich VMware kaum von anderen Anbietern von Überwachungsprogrammen und bietet eine hohe Anpassbarkeit durch den Benutzer. Jeder Anwender, ein Abgleich mit einem LDAP-Verzeichnis als Quelle ist möglich, kann sich seine Umgebung selbst anpassen, beispielsweise Messwerte oder Ereignisse.

Neben dem Dashboard gibt es Register für Ressourcen, Analyse, Management und die Administration der Software. Zu jeder Information auf dieser Intranet-Seite kann sich der IT-Profi über "New Feed" eine direkte Benachrichtigung zukommen lassen. Alle hinsichtlich der Plattform benötigten Einstellungen, beispielsweise unterschiedliche Benutzergruppen, definiert der Anwender über das Register "Administration". Dort legt der Administrator beispielsweise die Standard-Parameter für den Datenzugriff, SNMP-Anbindung oder die LDAP-Kommunikationsdaten fest. Wer schon einmal mit Monitoring-Lösungen gearbeitet hat, wird sich recht schnell zurechtfinden.

Agenten aufspielen und gruppieren

Dass noch keinerlei Messdaten von irgendwelchen Servern eingetroffen sind, zeigt ein Informationsbereich namens

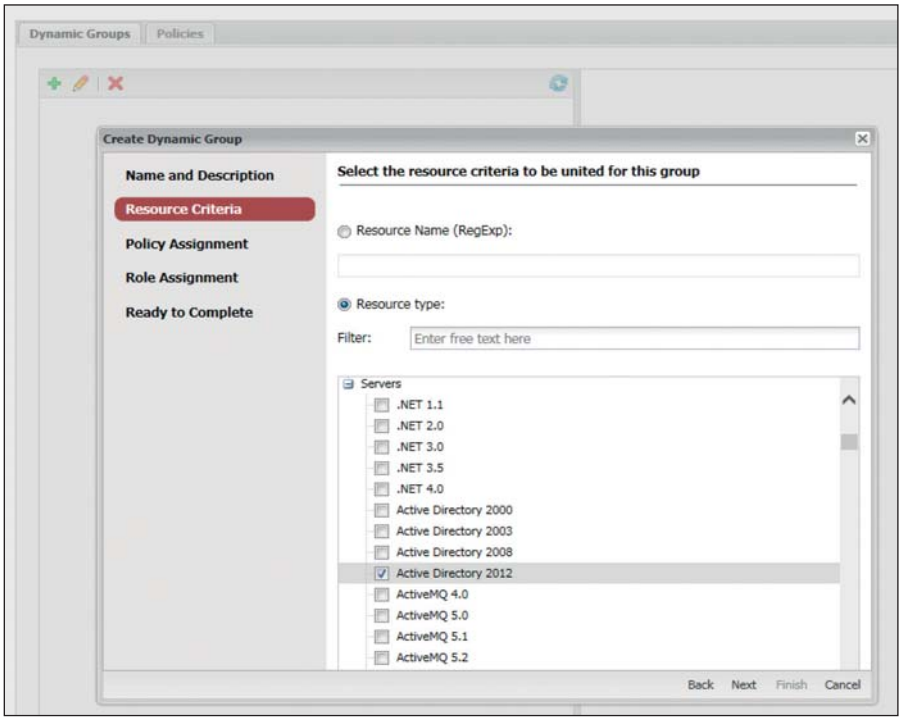


Bild 2: Dynamische Gruppen erlauben eine flexible Zuordnung. Kommt beispielsweise ein weiterer DC in die Überwachung, gelten automatisch die gewählten Richtlinien.

"Auto Discovery" an. Alle neuen Datenquellen, beispielsweise Server- oder Applikationsmessdaten, listet die Software zunächst hier auf und signalisiert so dem IT-Profi, dass diese Daten noch zugeordnet werden müssen. Einen Push-Befehl zum Ausbringen der Agent-Komponente sucht der Administrator jedoch vergeblich. Der Agent muss, je nach Plattform, auf dem Zielsystem unterschiedlich bereitgestellt werden. Hierfür gibt es viele verschiedene Varianten und Parameter, mit und ohne Java, als Kommando-Zeilen-Variante oder als klassischer Installer, beispielsweise für Microsoft Windows.

Die einfachste Installationsform besteht in der manuellen Installation des Agenten auf einem Server. Der Administrator muss nur wenige Fragen beantworten, beispielsweise nach der IP-Adresse des so genannten HQ-Servers, Login-Informationen und ob die Verbindung "unidirektional" und "verschlüsselt" eingerichtet werden soll. Die Installation nahmen wir im Test auf einem Microsoft Windows Server 2012 R2 mit aktiven Exchange- und Domänen-Diensten vor und auf einer einfachen Windows 7-Workstation. In der Grundeinstellung erkennt der Agent die wichtigsten messbaren Werte, beispielsweise CPU-, Festplatten- und Service-Daten, automatisch. Soll Hyperic weitere spezifische Anwendungsdaten abgreifen, so kann der IT-Profi durch einen Mausklick aus einer Liste von "Plug-Ins" auswählen und diese an den Agenten schicken. So gelang uns im Test die Ermittlung von Leistungs- und Messdaten von der Exchange-Installation. Wie bei vergleichbaren Lösungen, so ist auch bei Hyperic hier Detailwissen gefragt, da die Messdaten teilweise recht kryptische Namen besitzen.

Gruppieren nach Bedarf

Was uns indes recht gut gefiel, ist die Möglichkeit zur dynamischen Gruppenbildung. Die manuelle Zuordnung von Systemen oder Messdaten zu einer Übersicht, beispielsweise "Mailserver", ist in faktisch jeder Software – auch bei Hyperic – möglich. Die VMware-Lösung bietet jedoch die Definition von flexiblen Zuordnungen, beispielsweise "alle Anwendungen mit einer gewissen Eigenschaft" oder "alle Systeme, die weniger als n GByte freien Speicher besitzen". Solche dynamischen Gruppen erleichtern es den IT-Verantwortlichen, schnell den Blick auf kritische Systeme richten zu können. Die Anlage dieser Gruppen ist mit wenigen Mausklicks erledigt.

Administratoren definieren auf einzelnen Systemen, Applikationen oder auch Gruppen Überwachungseinstellungen – entsprechend einer klassischen Alarm-Definition. Das Dialogfenster hierzu ist glücklicherweise selbsterklärend und bietet zahlreiche Auswahlmöglichkeiten. Zunächst sorgten wir uns im Test dahingehend, ob eine Alarm-Regel "weniger als 1,5 GByte verfügbarer Speicher" wirklich funktioniert, da wir die Einheit "GByte" von Hand eingetippt hatten – aber die Entwickler haben mit einem derartigen Vorgehen wohl gerechnet.

Produkt

VMware vRealize Hyperic ist eine Komponente von VMware vRealize Operations. Sie überwacht Betriebssysteme, Middleware und Anwendungen, die in physischen, virtuellen und Cloud-Umgebungen ausgeführt werden.

Hersteller

VMware
www.vmware.com/de

Preis

VMware vRealize Hyperic ist ein Teil des vRealize Operations und wird für die Ausprägungen Advanced und Enterprise geliefert. Lizenzierung pro Prozessor oder pro virtueller/physischer Maschine in Paketgrößen je 25 Server. In der Advanced-Variante ist die Suite für 25 Server ab etwa 15.000 US-Dollar verfügbar.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

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

Installation und Bereitstellung	8
Leistungsumfang	7
Integration in eigene Umgebung	7
Integration in vSphere	9
Agenten-Verteilung	5

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Unternehmen, die bereits sehr stark auf den VMware-Hypervisor setzen.

bedingt für Firmen, die sich schon intensiv mit anderen Überwachungslösungen auseinandergesetzt haben.

nicht für sehr kleine Firmen ohne das Erfordernis zur Überwachung.

VMware vRealize Hyperic

VMware vRealize Hyperic ist für die Verwendung in großen Unternehmensumgebungen mit unterschiedlichen Benutzer-Rollen gut vorbereitet. So konfrontiert die Software nur die ausgewählten Benutzer und nicht gar alle Anwender der Software mit einem Problem. Eine Benachrichtigung per E-Mail an externe Dienstleister ist ebenfalls konfigurierbar. Wie es für große Monitoring-Systeme üblich ist, gibt es auch bei Hyperic ein Eskalationskettensystem zur Abarbeitung der Meldungen mit entsprechendem Reporting.

Automatisiert und rollenbasiert auf Alarme reagieren

Überwachung allein hilft dem Administrator zwar schon in vielen Fällen weiter, doch automatisierte Reaktionen sind häufiger besser, als erst nachträglich auf ein Fehlverhalten zu reagieren. Sinkt beispielsweise der freie verfügbare Arbeitsspeicher auf einem Server unter ein kritisches Niveau, wäre ein Neustart möglicherweise eine hilfreiche Reaktion. Droht eine Partition vollzulaufen, könnten temporäre Dateien gelöscht oder Protokolldateien durch einen Skript-Job wegkopiert werden. Derlei Reaktionen kann der Administrator als Reaktion auf einen "Alert" in Hyperic definieren. Aber auch traditionelle administrative Aufgaben wie tägliche, wöchentliche oder monatliche Ausführungen von Jobs mit geplanten "Down Times", in denen die Überwachungssoftware keine Warnmeldungen ausgeben und entsprechend auch nicht "Actions" triggern darf.

Mithilfe von erweiterten Benachrichtigungs- und Eskalations-Workflows können Administratoren doppelte oder irrelevante Warnmeldungen sowie Fehlalarme in Hyperic reduzieren, indem sie präzise Bedingungsdefinitionen für Warnmeldungen für eine Vielzahl von Performance-Werten festlegen. Die Warnmeldungen können entweder klassisch als E-Mail-Benachrichtigungen rausgehen oder der Administrator wählt Kontrollaktionen zur automatischen Behebung gängiger Probleme aus.

Dank der Rollenverwaltung erlaubt die Lösung auch die rollenbasierte Benachrichtigungsfunktion mit Zuweisung von Problemen an die entsprechenden Expertenteams, beispielsweise für Anwendungsserver, DBAs, Entwicklung oder Netzwerkadministratoren. Für eine Bearbeitung rund um die Uhr durch Mitarbeiter an unterschiedlichen geografischen Standorten sorgen in der Software entsprechende Warnmeldungskalender.

Fazit

VMware Hyperic ist eine ausgewachsene Monitoring-Lösung für Netzwerk- und Server-Umgebungen mit allen gängigen Variationen von Darstellungs- und Auswertungsformen. Dank der Plug-In-Technik bietet es die Möglichkeit, spezifische Anwendungsüberwachungen nachzurüsten, oder bei Bedarf gleich selbst zu entwickeln. Hyperic eignet sich für die Optimierung der täglichen Abläufe und die Verringerung von Risiken durch menschliche Fehleinschätzungen oder Versäumnisse. Ein Blick ist die Software in jedem Fall wert und weitaus bequemer in der Benutzung als beispielsweise Nagios. *(jp)*

Im Test: O&O Syspectr

Aus allen Wolken

von Sandro Lucifora

Mit Syspectr bietet das Berliner Unternehmen O&O Software seit gut einem Jahr einen Cloud-Dienst an, der Administratoren das Verwalten von Desktop-Systemen und Servern erleichtern soll. IT-Administrator hat sich den Dienst und dessen Möglichkeiten wie auch Schwächen näher angesehen.

Mit Syspectr folgt O&O Software dem Trend, Software in der Cloud anzubieten und lagert das IT-Management auf eine webbasierte Plattform aus. Dabei soll die Anwendung nicht nur einen umfassenden Überblick über die Windows-Infrastruktur geben, sondern auch Rechner überwachen und mögliche Probleme erkennen, bevor sie entstehen.

Für unseren Test richteten wir mehrere Windows-Rechner mit Windows 7 und Windows 8/8.1 sowie Windows Server 2008 R2 und 2012 R2 in Syspectr ein. Dazu erstellten wir uns auf der Internetseite einen Account und hinterlegten unsere Lizenz. Wer eine aktuelle Software-Lizenz eines O&O-Produktes im Einsatz hat, kann auch diese Lizenznummer eintragen, da diese bereits einige kostenlose Geräte-Lizenzen beinhaltet. Um einen Computer verwalten zu können, installierten wir anschließend auf dem lokalen Gerät einen Agenten. Dazu luden wir uns die Windows-Setup-Datei herunter, die Syspectr bereits mit unserem Konto verknüpfte.

Schweigsamer Client-Agent

Für das Ausrollen mit einer Softwareverteilung bietet O&O eine entsprechende MSI-Datei an. Diese haben wir über die Gruppenrichtlinien im Active Directory in unserer Testumgebung verteilt. Voraussetzung war ein bereits installiertes .NET Framework 4. Die manuelle Installation mittels Setup-Datei lädt bei Bedarf das benötigte Framework nach, um die Einrichtung erfolgreich abzuschließen.

Da sich die Setup-Datei wie auch das MSI-Paket direkt mit unserem Syspectr-Konto verknüpften, bedurfte es keiner weiteren Konfiguration. Überhaupt gibt es auf dem lokalen System weder eine Programmverknüpfung noch eine Programmoberfläche, um Aktionen auszuführen. Stattdessen läuft der Agent als Dienst und liefert dem Server alle notwendigen Informationen.

Bereits kurz nach der Installation erhielten wir eine E-Mail, die über die neu angemeldeten Computer informierte. Wir loggten uns bei Syspectr ein und das System forderte uns auf, einmalig eine vierstellige Syspectr-PIN festzulegen. Diese fragt das System bei sicherheitsrelevanten Funktionen ab. Danach zeigte uns das Dashboard die angemeldeten Computer und eine Liste der aktuellen Ereignisse. Der Ansicht der Computer-Symbole entnahmen wir neben dem Namen und dem Betriebssystem auch den Zusatz, ob es sich um einen physischen Rechner oder eine virtuelle Maschine handelt. Die Kopfleiste informierte uns über das Vorhandensein von Warnmeldungen und Hinweisen.

Nicht alle Fehler lassen sich beheben

Wir klickten auf einen Rechner, in unserem Fall ein Windows Server 2012, worauf sich eine detaillierte Übersicht zum System öffnete. Diese ist in die Kategorien "Hardware", "Software", "Windows Sicherheit", "Windows-Updates", "Festplatten", "O&O Defrag", "O&O DriveLED", "USB-Speicher" und "Prozesse überwachen" unterteilt. Gibt es in einem Bereich eine Warnmeldung oder einen Hinweis, ist dies durch ein rotes beziehungsweise gelbes Symbol direkt zu erkennen. Wir begannen, die Meldungen abzuarbeiten, indem wir auf die jeweils markierten Gruppen klickten.

Der Bereich "Windows Sicherheit" informierte uns zum Beispiel, dass die Firewall nicht aktiv sei. Klappten wir den Hinweis auf, konnten wir an dieser Stelle direkt die Firewall einschalten. Leider hatten wir keine Möglichkeit zu unterscheiden, auf welches Netzwerk – LAN und/oder WAN – diese

Systemvoraussetzungen

Der Client benötigt mindestens Windows XP, das .NET Framework 4.0 und eine Internet-Anbindung.

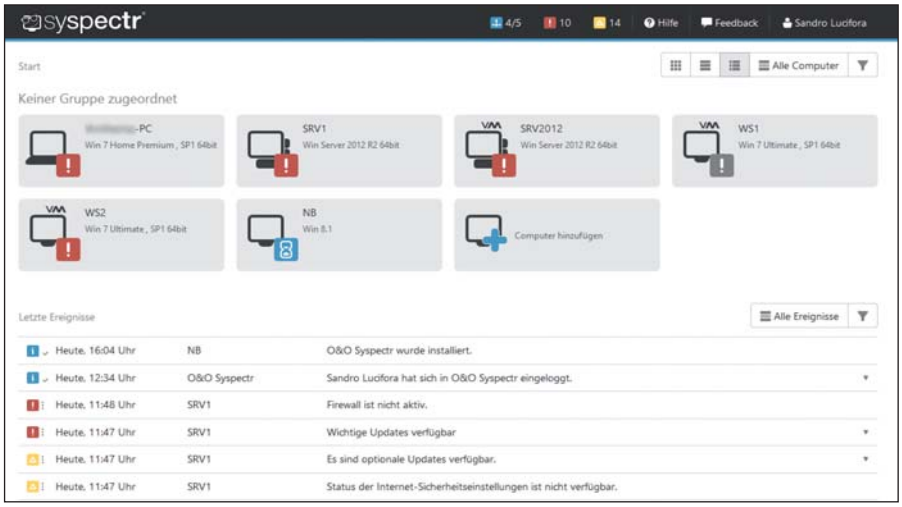


Bild 1: O&O Syspectr bietet ein übersichtliches und informatives Dashboard.

Einstellung greift. Syspectr schaltet lediglich die Firewall ein und übernimmt die in der Vergangenheit gesetzten Einstellungen. Auf einem anderen Rechner erhielten wir den richtigen Hinweis, dass das Windows-Gastkonto aktiviert und die Windows-Benutzerkontensteuerung (UAC) deaktiviert war. Korrigieren ließen sich beide Einstellungen jedoch nicht.

Im Bereich "Windows Updates" sahen wir, dass einige Aktualisierungen noch auf ihre Installation warteten. In der Übersicht der anstehenden Updates wählten wir die Einträge aus, die wir installieren wollten, und starteten diese durch einen Klick auf den Button "Installieren". Derzeit ist es nicht möglich, Drittanbieter-Software zu installieren oder vorhandene Software vom System zu entfernen. Auf Nachfrage erklärte der Hersteller, dass die Implementierung dieser Funktion in Arbeit sei und zeitnah zur Verfügung stehen soll. Über den Punkt "O&O Defrag" bot uns das System an, die gleichnamige Software remote auf dem PC zu installieren und darüber zukünftig die Defragmentierung zu steuern.

Defragmentieren von SSD-Festplatten möglich

Nach der Ferninstallation erhielten wir eine Übersicht der Partitionen und ließen den Zustand der Fragmentierung analysieren. Auch wenn es so aussieht, defragmentiert O&O Defrag logischerweise keine SSD-Platten. Statt den Inhalt zu sortieren, schickt Syspectr den üblichen Trim-Befehl. Bei herkömmlichen HDDs starteten wir die Defragmentierung, die im Hintergrund ablief. Die daraufhin zu 100 Prozent ausgelastete Festplatte dürfte den Arbeitsprozess der Benutzer allerdings mitunter stören. In den Einstellungen hatten wir noch die Auswahl, die "Automatische Defragmentierung im Hintergrund" zu aktivieren sowie "Optimieren, wenn Benutzer abwesend ist (wenn Bildschirmschoner aktiv)" einzuschalten. Gerade letztere Option ist sicher sinnvoll, um ein möglichst ungestörtes Arbeiten der User sicherzustellen. In den weiteren automatischen Optimierungen wählten wir "SSDs regelmäßig mit TRIM optimieren" sowie "Freien Speicherplatz auf Festplatten regelmäßig löschen".

Weiter zeigten uns die Punkte "Hardware" die verbundenen Komponenten und "Software" die installierten Programme an. Die Installation zusätzlicher oder die Deinstallation vorhandener Software war nicht möglich. Über "Festplatten" sahen wir eine Übersicht der Partitionen sowie eine grafisch aufbereitete Darstellung des verwendeten Speicherplatzes. Passend dazu zeigte uns das "O&O DriveLED" die Temperatur und Laufzeit der Festplatten an, wobei diese Angaben auf S.M.A.R.T.-Werten basieren. Weitere Details kamen nach dem Aufklappen des Eintrags zum Vorschein. Warnmeldungen versendet das Modul nach allgemeinen Grenzwerten, die sich nicht ändern lassen.

Zugriff auf USB-Speicher deaktivieren

Auf der Seite "USB-Speicher" listete Syspectr auf, ob und welche USB-Speicher angeschlossen waren. Über die Einstellungen konnten wir festlegen, ob Benutzer an dem Computer USB-Massenspeicher verwenden durften. Deaktivierten wir diesen Punkt, dauerte es wenige Sekunden, bis der Agent angeschlossene Geräte abmeldete und sich neue nicht mehr aktivieren ließen. Leider haben wir hier eine Differenzierung der USB-Speicher vermisst. So wäre es zum Beispiel wünschenswert, USB-Speicher nach Marke oder Modell zu erlauben, zu bestimmten Zeiten oder sofern ein festgelegter Benutzer angemeldet ist.

Prozesse werden bei der Eingabe nicht erkannt

In den Einstellungen unter "Prozesse überwachen" bot uns Syspectr zwei Eingabefelder an, in denen wir zum einen die Namen der Programme, Prozesse oder Dienste eintrugen, die auf dem Computer nicht laufen, und in der anderen Zeile diejenigen, die immer laufen sollten. Die Eingabe entpuppte sich jedoch als wenig komfortabel: Das System verlangte die Angabe des Dateinamens oder des Anzeigenamens der Prozesse. Während der Eingabe glich Syspectr diese Daten zwar mit dem Computer ab, doch egal welchen Eintrag wir vornahmen, Syspectr zeigte uns immer nur an, dass ein Prozess mit dem Namen nicht zu finden sei. Dennoch konnten wir den Eintrag zur Überwachung hinzufügen und das Tool erkannte trotzdem, ob der Prozess lief oder nicht. Denn ein nicht existierender Prozess oder das Beenden eines vorhandenen Prozesses erzeugte eine entsprechende Fehlermeldung. Besser wäre es an dieser Stelle, dass zumindest für die Angabe der Prozesse, die immer laufen sollten, eine entsprechende Liste die Auswahl erleichtert. Auch dies ist laut Hersteller in Arbeit und soll bald umgesetzt sein.

Fernbedienen von Konsole und Desktop

Zwei weitere Funktionen dienen mit "Remote Console" und "Remote Desktop" der Fernbedienung des Computers. Beide verlangten vor dem Start die Eingabe der zu Anfang festgelegten PIN. Die "Remote Console" startete eine webbasierte Eingabeaufforderung, über die wir genauso arbeiteten wie in der lokalen

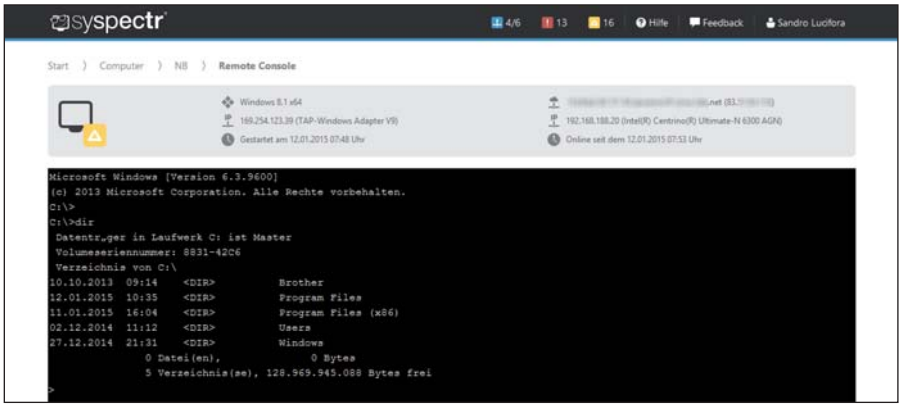


Bild 2: Die Remote-Konsole dient der Administration, ohne den Desktop des Anwenders zu blockieren.

Konsole. Die Verbindung baute das System über SSL auf, sodass die übertragenen Daten vor fremden Blicken geschützt sind.

Um über Syspectr einen webbasierten Remote Desktop aufzurufen, klickten wir auf den gleichnamigen Eintrag, woraufhin das System die Verbindung herstellte. Auf der Gegenseite fragte eine Dialogbox den Benutzer, ob er die Remote-Verbindung zulassen will. Als wir diese bestätigten, sahen wir kurze Zeit später den Desktop in unserem Browser, mit einer nur leichten Zeitverzögerung. Beim Zugriff auf einen gesperrten Rechner – in unserem Fall der Windows Server 2012 – baute sich die Verbindung ohne diese Benutzer-Interaktion auf und wir sahen den Anmeldebildschirm.

Für die bessere Bedienbarkeit erweiterten wir den Remote-Desktop auf Vollbildgröße. Grundsätzlich skalierte die Remote-Funktion die Anzeige. Wir schalteten die Skalierung aus, wodurch wir eine 1:1-Ansicht erhielten. Bei der Fernbedienung eines Computers mit mehreren Monitoren schalteten wir in der Ansicht zwischen den Monitoren um. Des Weiteren standen uns die üblichen Funktionen, wie das Senden von "Strg + Alt + Entf" oder die "Windows-Taste", zur Verfügung. Ebenso meldeten wir den Benutzer ab und sperrten den Computer aus der Ferne.

Beendeten wir die Sitzung, hatten wir die Möglichkeit, den Computer zu sperren und dem Anwender eine Nachricht zu hinterlassen. Meldete er sich lokal wieder an, zeigte ein Syspectr-Dialog Informationen zur Remote-Verbindung und gab die Nachricht aus.

Benachrichtigung per E-Mail

Damit sich der IT-Verantwortliche nicht immer wieder einloggen und den Zustand der Computer prüfen muss, hat O&O Software auch eine Benachrichtigungsfunktion implementiert. Über den gleichnamigen Menüpunkt stellten wir im Test ein, in welchen Fällen wir eine E-Mail erhalten wollten. Dabei unterscheidet der Dienst zwischen "Informationen", "Warnungen" und "Probleme" und listet die verschiedenen Bereiche auf. Wir wählten per Mausklick aus, zu welchen Ereignissen uns das System benachrichtigen sollte. Vermisst haben wir ergänzende Benachrichtigungswege wie Google Chat, SMS, WhatsApp oder eine iOS- und Android-App, um auch ohne ständigen E-Mail-Zugriff zumindest bei Problemen schnelle Nachricht zu erhalten.

Zusätzlich fiel uns auf, dass es Benachrichtigungen für ein Modul "Skripte" gab. Auf Rückfrage bestätigte der Hersteller, dass es sich hierbei um ein neues Modul handelt, das es ermöglicht, PowerShell-Skripte in Syspectr zu hinterlegen und auf dem PC auszuführen. Die Veröffentlichung dieser neuen Funktion ist für das erste Quartal dieses Jahres geplant.

Fazit

Die Inbetriebnahme von O&O Syspectr erfolgt schnell und die Installation beziehungsweise das Ausrollen der MSI-Pakete verläuft ohne Hürden. Die Weboberfläche ist modern gestaltet und zeigt keinerlei programmiertechnische Mängel oder Aussetzer. Die Funktionen selber sind solide umgesetzt und machen das, was sie sollen. An vielen Stellen macht sich jedoch die junge Geschichte des Tools bemerkbar, da uns Einstellungen und Funktionen fehlen. So wünschen wir uns sowohl detaillierte Optionen bei der USB-Überwachung als auch mehr Möglichkeiten, gerade Windows-Einstellungen vorzunehmen, zu denen Syspectr Warnungen ausgibt – wie UAC einzuschalten oder das Gastkonto zu deaktivieren. Die Installation von Windows-Updates gehört zur Basis-Funktion einer solchen Lösung, die derzeit fehlende Remote-Softwareinstallation hingegen wäre die Kür und ein besonderes Merkmal. Aber sie will der Hersteller noch implementieren. Gleiches gilt für das neue Modul zur Ausführung von PowerShell-Skripten. *(dr)*

Produkt
Cloud-basierter Dienst zur Verwaltung von Windows-Clients.

Hersteller
O&O Software GmbH
www.syspectr.com/de/

Preis
Bis zehn PCs kostenfrei. Danach 1 Euro pro PC sowie 5 Euro pro Server.

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

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

Fernadministration	5
Funktionsumfang	6
Remote-Bedienung (Konsole/Desktop)	8
Funktionsweise der Agenten	7
Systemüberwachung	5

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für die Fernverwaltung von Windows-PCs.

teilweise für die tiefergehende Fernadministration von Computern, da sich nur wenige Einstellungen remote vornehmen lassen.

nicht als Monitoring-Ersatz für Server, da sich die Überwachungsfunktionen auf den Status von Prozessen beschränken.

O&O Syspectr

IT-Administrator Sonderhefte

Je 180 Seiten geballtes Wissen!

Abonnenten erhalten Sonderhefte zum Vorzugspreis!

http://shop.heinemann-verlag.de/

Einkaufsführer: End-to-End-Monitoring

Durchgehende Einsichten

von Christian Hilbert

Quelle: Edhar Yuralaits – 123RF

Angesichts der kontinuierlich steigenden Anzahl geschäftskritischer Business-, Cloud- und Web-Anwendungen gewinnt das Monitoring der Anwendungs-Performance in Unternehmen jeder Größe an Bedeutung: Wer als IT-Administrator interne und externe Kunden optimal betreuen will, muss jederzeit wissen, wie es um die Service-Qualität seiner Anwendungen bestellt ist. Moderne Lösungen für das End-to-End-Anwendungs-Monitoring, die die Performance am Anwender-PC mithilfe von Mess-Robotern und Bilderkennungsverfahren analysieren, stehen bei den IT-Abteilungen daher hoch im Kurs. Unser Einkaufsführer untersucht, welche Fragen sich IT-Organisationen vor einer entsprechenden Investition stellen sollten.

Wer in seinem Unternehmen IT-Support leistet, weiß: Die überwiegende Mehrzahl der Beschwerden dreht sich um die Anwendungs-Performance. Dem einen Nutzer dauert es zu lange, bis eine Webseite aufgerufen wird, der andere beklagt die unzuverlässige SAP-Anbindung in der Remote-Niederlassung. Als interner Dienstleister muss die IT-Abteilung in der Lage sein, zu all diesen Fragen fundiert Stellung zu beziehen, berechtigten Einwänden nachzugehen und unberechtigte Kritik überzeugend zu entkräften.

Dafür reicht ein klassisches "Rot-Grün-Monitoring" der Netzwerkkomponenten, das nur den Ist-Zustand der einzelnen Systeme überwacht, heute jedoch nicht mehr aus. Der IT-Administrator ist vielmehr darauf angewiesen, proaktiv die End-to-End-(E2E-)Performance der Anwendungen im Blick zu behalten – und zwar nicht nur anhand statischer Kennzahlen, sondern aufgrund der echten, subjektiven User Experience am Anwender-PC.

Mess-Roboter simulieren Anwenderverhalten

Kein Wunder also, dass der Markt für End-to-End-Anwendungs-Monitoring boomt. Interessierte Unternehmen können heute zwischen einer Vielzahl softwarebasierter Lösungen großer und kleiner Hersteller wählen. In der Regel werden dabei zunächst die zu überwachenden Anwendungen auf einem dedizierten Client-System im Netzwerk implementiert. Anschließend simuliert ein auf dem Client laufender Mess-Roboter möglichst akkurat das Verhalten eines menschlichen Anwenders – etwa indem er Daten in Datenbanken eingibt, Webformulare ausfüllt oder E-Mails verschickt.

Die Abläufe auf dem Client-Bildschirm werden durchgehend mit einer leistungsfähigen Bilderkennungssoftware analysiert und ausgewertet, um objektive Daten zu Performance, Verfügbarkeit und Latenz an einem typischen Client-Arbeitsplatz zu erhalten. Die so gemessenen Daten werden auf einem zentralen Management-Server gesammelt, evaluiert und mit hinterlegten Grenzwerten abgeglichen, um proaktiv auf qualitative Einbrüche reagieren zu können und das IT-Service-Management nachhaltig zu optimieren.

Angesichts der breiten Palette verfügbarer Produkte tun sich allerdings viele Unternehmen schwer, eine Lösung zu finden, die optimal auf ihre Bedürfnisse abgestimmt ist und ihnen das volle Potenzial des Anwendungs-Monitorings bietet. Wir untersuchen im Folgenden wichtige Entscheidungskriterien für den Erwerb eines E2E-Werkzeugs.

Anforderungen an Flexibilität und Skalierbarkeit

Die meisten Unternehmen implementieren E2E-Monitoring zunächst für wenige ausgewählte Anwendungen, zum Beispiel den geschäftskritischen Webshop oder die ebenso wichtige ERP-Installation. Hat sich das System aber einmal bewährt und eingespielt, werden mit hoher Wahrscheinlichkeit sukzessive weitere Applikationen hinzukommen. Daher lohnt es sich, bei der Auswahl der Lösung darauf zu achten, dass diese flexibel skaliert und erweitert werden kann – beispielsweise für zusätzliche interne oder remote gehostete Linux-, Windows- und Mac-Anwendungen sowie für Cloud-, Terminalserver- und VMware-basierte Applikationen. Je offener die Plattform ist und je mehr Schnittstellen sie unterstützt, desto sicherer ist die Investition.

Eines der wichtigsten Einsatzfelder von E2E-Monitoring ist das Management der Service-Qualität von Web-Anwendungen. Webshops, Online-Portale sowie Social

Media- und Web 2.0-Anwendungen leben ausnahmslos davon, dass eine hohe User-Zahl in Echtzeit auf die gleichen Applikationen zugreift. Dafür ist es entscheidend, dass die Anwendungs-Performance durchgehend stabil bleibt und die User Experience selbst in Spitzenzeiten einwandfrei ist. E2E-Monitoring ist die geeignete Technologie, um Flaschenhälse und Qualitätseinbrüche frühzeitig zu erkennen und proaktiv zu beheben. Sollten die Wartezeiten zu lang sein oder gar Verbindungsabbrüche drohen, alarmiert die Lösung automatisch die zuständigen Administratoren und trägt so dazu bei, teure Umsatzeinbrüche zu vermeiden. Prüfen Sie daher bei der Auswahl einer E2E-Monitoring-Lösung unbedingt, ob diese auch für anspruchsvolle Webanwendungen und Multi-Link-Umgebungen geeignet ist – denn früher oder später wird dieser Einsatzbereich mit hoher Wahrscheinlichkeit in jedem Unternehmen auf der Agenda nach oben rücken.

E2E-Monitoring bietet über die reine Anwendungsüberwachung hinaus eine ganze Reihe weiterer spannender Einsatzfelder. Besonders interessant für Enterprise-Umgebungen ist das Qualitätsmanagement bei Updates und Migrationen tief integrierter Business-Anwendungen – etwa von ERP-, PPS- oder CRM-Lösungen. Wer sichergehen will, dass solche anspruchsvollen und hochgradig risikobehafteten Changes reibungslos vonstattengehen, kann ihren Ablauf mithilfe des E2E-Anwendungs-Monitorings vor dem echten Roll-out an einem einzelnen Standort testen, um sich gegen unliebsame Überraschungen zu wappnen.

Schnittstellen zum vorhandenen Netzwerk-Monitoring

E2E-Anwendungs- und Netzwerkmonitoring sind zwar grundverschieden, kommen in der Praxis aber häufig parallel zum Einsatz und ergänzen sich hervorragend, wenn es gilt, alle Warnmeldungen in einer einheitlichen Oberfläche zusammenzuführen. Daher sollte sich Ihre End-to-End-Monitoring-Lösung nahtlos in Ihre vorhandenen IT-Management-Systeme integrieren lassen.

Achten Sie vor allem auf die Unterstützung von Standard-Interfaces wie SNMP, SMTP und ODBC-Connect. Viele Unternehmen nutzen alternativ die Logfile-Analyse-Module ihrer Netzwerkmonitoring-Lösung, um die E2E-Monitoring-Daten einfach zu übernehmen. Ganz egal für welchen Weg Sie sich schlussendlich entscheiden: Berücksichtigen Sie bei der Produktauswahl auf jeden Fall die Schnittstellenproblematik.

Anbindung von Remote-Standorten

Aufgrund der rasant zunehmenden Zentralisierung von Anwendungen und Datenbeständen sind die Filialen, Niederlassungen und SoHos vieler Unternehmen darauf angewiesen, remote auf zentral vorgehaltene Applikationen und Informationen zuzugreifen. E2E-Monitoring ist eine probate Technologie, um in dezentralen Infrastrukturen gleichbleibend hohe Dienstgüte zu garantieren. Evaluieren Sie daher bereits bei der Produktauswahl, ob es möglich ist, die E2E-Monitoring-Clients auch in abgesetzten Standorten zu betreiben und über die vorhandenen WAN- beziehungsweise VPN-Links an den zentralen Monitoring-Server anzubinden.

Komplexität von Konfiguration und Management

Die Effizienz einer Monitoring-Lösung hängt maßgeblich davon ab, wie einfach und flexibel die Konfiguration ist. Achten Sie bei der Produktauswahl daher unbedingt darauf, dass sich die Monitoring-Clients mit minimalem Aufwand in Ihr Netzwerk integrieren und zentralisiert steuern lassen.

Eine intuitiv verständliche, grafische Benutzeroberfläche und durchdachte, übersichtliche Workflow-Editoren machen es Ihnen leicht, die an einzelnen Standorten oder Standortgruppen zu überwachenden Anwendungen zu definieren und das gesamte Monitoring gemäß Compliance-Richtlinien aufzusetzen. Auf diese Weise profitieren Sie vom ersten Tag an von der Lösung, ohne sich groß einarbeiten zu müssen, was im Endeffekt zu einer nachhaltigen Reduktion der Betriebskosten führt. Hinzu kommt, dass Sie durch die standardisierte Pflege der Client-Systeme viele Fehlerquellen vermeiden und so eine höhere Qualität der Monitoring-Ergebnisse gewährleisten.

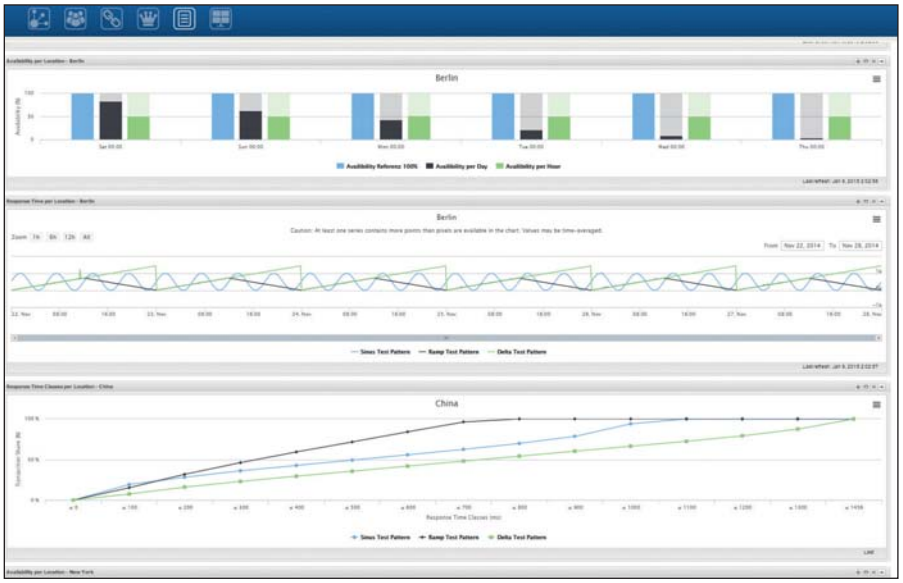
Verfahren der Datenerfassung am Client

Ein wichtiges Unterscheidungsmerkmal der verschiedenen E2E-Monitoring-Produkte ist die technische Umsetzung der Datenerfassung auf dem Monitoring-Client. Bei den meisten der heute verfügbaren Systeme basiert die Datenerfassung auf Bilderkennungsverfahren. Dies garantiert eine weitgehende Unabhängigkeit von der Applikationsplattform und deren Programmiersprache und ermöglicht so das Monitoring von Terminalservices, Webapplikationen, eigenentwickelten Applikationen und vielen weiteren Software-Lösungen am selben Client.

Allerdings ist die Qualität der Bilderkennungssysteme sehr unterschiedlich. Während manche Lösungen Grafiken wie ein menschlicher Anwender als Schemata erkennen und das Anwenderverhalten äußerst detailgetreu simulieren, lösen andere bereits bei minimalen Farbschwankungen in der Darstellung einen Fehlalarm aus. Daher sollte dieser Schlüsselfunktion im Rahmen der Evaluierung hohe Priorität zukommen. Überprüfen Sie bei einem sorgfältigen Proof-of-Concept, welche der Ihnen angebotenen Lösungen eine farbtiefen- und auflösungsunabhängige Identifizierung der Bildelemente auf einer Applikationsoberfläche ermöglicht und eine stabile Highspeed-Bilderkennung unter-

Betrieb als Managed Service

Die meisten zeitgemäßen E2E-Anwendungs-Monitoring-Lösungen sind relativ einfach zu implementieren. Erfahrungsgemäß dauern Implementierung und Inbetriebnahme im Schnitt zwischen drei und vier Manntagen. Auch das Management des laufenden Betriebs ist dank intuitiver Oberflächen und nahtloser Integration in das IT-Management vergleichsweise pflegeleicht. Gerade in kleinen und mittelständischen Unternehmen binden die Lösungen dennoch einen relevanten Teil der knappen IT-Ressourcen und erfordern zudem den Aufbau und das Vorhalten von umfangreichem Spezialwissen. Vor diesem Hintergrund ist die Implementierung von E2E-Monitoring als Managed Service häufig eine attraktive Alternative. Auf diese Weise profitiert Ihr Unternehmen von sämtlichen Vorteilen dieser State-of-the-Art-Technologie und kann budgetschonend mit den wichtigsten Applikationen starten. Prüfen Sie am besten frühzeitig, ob ein Outtasking für Sie attraktiv sein könnte und welche Produkte dafür in Frage kommen.



E2E-Monitoring-Werkzeuge wie etwa der hier gezeigte ServiceTracer-Client sind in der Lage, die subjektive Performance von Web-Applikationen zu messen.

stützt. Der Client sollte dabei in der Lage sein, die Maus auch dann noch korrekt zu positionieren und Tastatureingaben vorzunehmen, wenn beispielsweise die Position eines Bildes verändert wird.

Unterbrechungen dürfen nicht stören: Pop-ups und Security-Abfragen

Ein weiterer Bereich, in dem sich die Spreu der E2E-Monitoring-Systeme vom Weizen trennt, ist der Umgang mit Pop-ups und Security-Abfragen: Da die Monitoring-Clients typischerweise wie herkömmliche Desktop-Arbeitsplätze konfiguriert sind, werden sie wie diese zentral administriert und mit einer Reihe erforderlicher Security-Tools (AV-Scanner, Anti-Spam, Personal Firewall et cetera) abgesichert. Schließlich soll das Monitoring-System ja nicht zur Sicherheitslücke werden.

In der Praxis machen sich die Management- und Security-Suiten aber immer wieder durch Pop-up-Fenster, Eingabeaufforderungen sowie sonstige Rückfragen bemerkbar. Damit stellen sie für viele Monitoring-Lösungen ein erhebliches Problem dar – etwa wenn ein ungeplant aufgehendes Werbefenster im Best Case zur Fehlmessung und im Worst Case zum Absturz des Clients führt. Klären Sie daher rechtzeitig mit Ihrem Systemintegrator, wie die zur Disposition stehenden Lösungen mit plötzlich auftretenden Ausnahmesituationen umgehen.

Anwendungsfehlern begegnen

Ein spannendes Differenzierungsmerkmal zwischen den E2E-Monitoring-Lösungen ist ihr Umgang mit Ausfällen der zu überwachenden Anwendungen und Fehlern bei der Datenerfassung. So kommt es in der Praxis oft vor, dass die überwachte Applikation im Zuge geplanter Update-Prozesse heruntergefahren wird oder dass kritische Webanwendungen etwa nach einem Firefox-Update nicht mehr über den Browser verfügbar sind. Viele Produkte auf dem Markt brechen ihre Messung in solchen Fällen ohne verwertbares Feedback ab.

Testen Sie in der Evaluierungsphase, wie verschiedene Produkte mit solchen Szenarien umgehen. Sie werden überrascht sein, wie breit die Leistungskluft in diesem Bereich ist. Einige Lösungen sind von Haus aus so clever, dass sie bei Applikationsausnahmen Screenshots der jeweiligen Situation erstellen, eindeutige Logfiles anlegen und alle geöffneten Applikationen automatisch schließen – oder im Falle des Firefox-Updates einfach probehalber auf den Internet Explorer wechseln. Diese Evaluierung wird sich im laufenden Betrieb vielfach bezahlt machen.

Management und Compliance

Für die langfristige Usability der E2E-Monitoring-Lösung sollten Sie Ihr Augenmerk bei der Produktevaluierung nicht zuletzt auch auf die Management-Features der einzelnen Lösungen legen. Eine leistungsfähige, zentralisierte oder webbasierte Konsole wird es Ihnen leicht machen, sämtliche installierten Monitoring-Clients im Blick zu behalten, lokal auflaufende Auswertungsdaten in einer zentralen Datenbank zu bündeln und die Alarmierung und das Reporting effizient abzuwickeln. Hinzu kommt die erhebliche Zeitersparnis, wenn Sie in der Lage sind, Workflows für verteilte Clients einmalig in der Zentrale anzulegen und dann auf die Remote-Systeme zu pushen.

Unternehmen müssen heute einer steigenden Anzahl strenger interner und externer Richtlinien gerecht werden. Ein umfassendes E2E-Anwendungs-Monitoring kann viel dazu beitragen, die Einhaltung von Compliance-Vorgaben sicherzustellen und vor allem auch lückenlos zu dokumentieren. Ziehen Sie diese Funktion bereits bei der Produktevaluierung in Betracht und prüfen Sie, welche der Lösungen beispielsweise im Hinblick auf das Reporting, die Mandanten-Fähigkeit und die revisionssichere Dokumentation und Datenspeicherung Ihren konkreten Anforderungen am besten gerecht werden.

Fazit

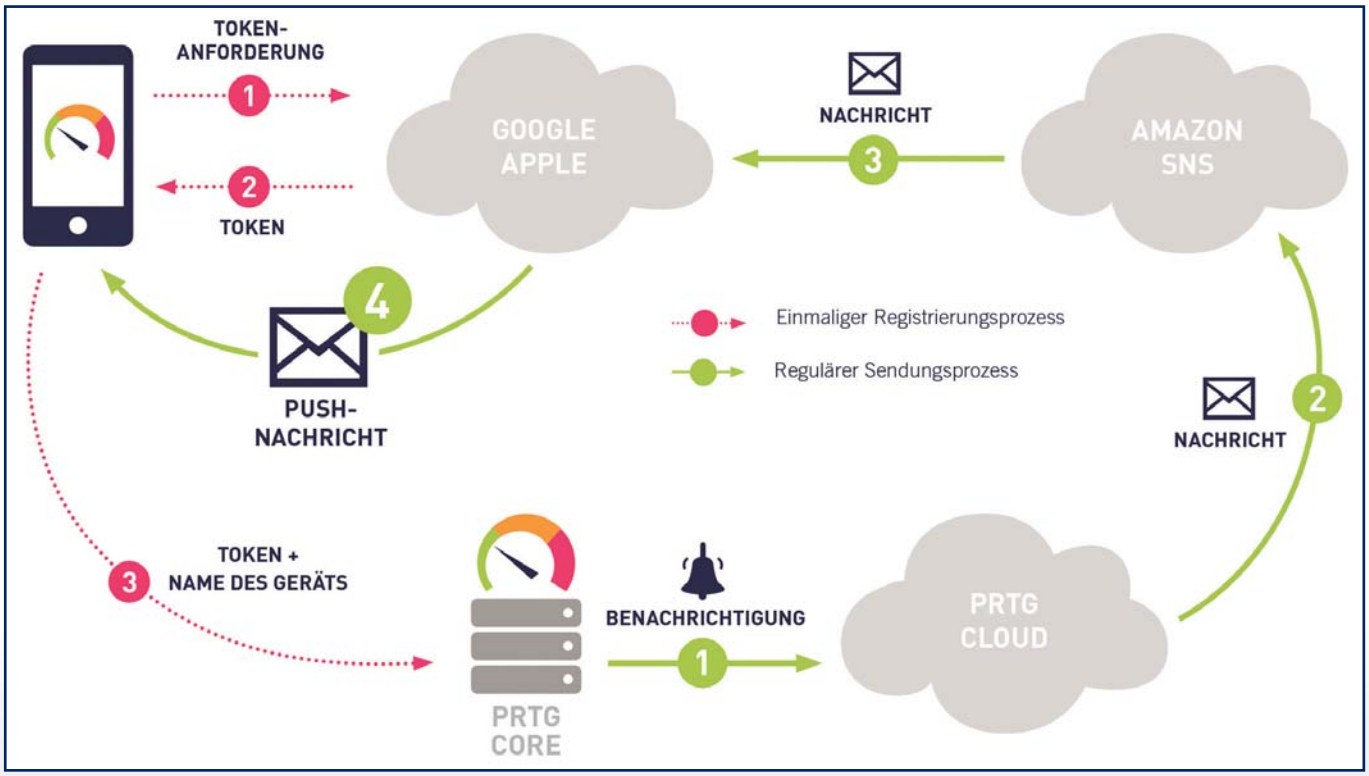
Mit einem zeitgemäßen End-to-End-Anwendungs-Monitoring erhalten Unternehmen jeder Größe ein leistungsstarkes IT-Management-Werkzeug an die Hand, um die Kunden- und Mitarbeiterzufriedenheit nachhaltig zu steigern und die lückenlose Einhaltung von Service-Level- und Compliance-Vorgaben sicherzustellen. Der IT-Abteilung bleibt damit mehr Zeit, das Business des Unternehmens konstruktiv weiterzuentwickeln. Zudem können IT-Teams in ihrer Rolle als Dienstleister durch verbesserte Service-Qualität überzeugen und sich von externen Wettbewerbern positiv abheben. Angesichts der Komplexität des Themas sind die Unternehmen aber gut beraten, bereits bei der Produktauswahl einen erfahrenen Systemintegrator hinzuzuziehen, um sicherzustellen, dass die Lösung optimal auf ihre Bedürfnisse zugeschnitten ist. *(jp)*

Christian Hilbert ist IT-Management-Consultant bei der Controlware GmbH in Dietzenbach.

Mobile Apps informieren ortsunabhängig über den Netzwerkstatus

Vorsprung durch Push-Benachrichtigungen

„Hätte ich das doch nur früher gewusst!“ – Weil die Störung zu spät erkannt wurde, ist plötzlich der Server down. Während sich die Mitarbeiter der anderen Abteilungen fragen, was passiert ist, kämpft der Administrator gegen die Uhr… Dieser Zeitdruck muss nicht sein. Eine Netzwerk-Monitoring-Lösung hätte Schlimmeres verhindern können, da sie präventiv alarmiert. Modernes Monitoring geht sogar noch einen Schritt weiter: Damit der Administrator nicht nur von seinem Schreibtisch aus, sondern auch unterwegs alles im Blick hat, bietet PRTG Network Monitor kostenlose Apps für mobile Endgeräte. Den entscheidenden Informationsvorsprung sichern die neuen Push-Nachrichten, die direkt auf dem Display den aktuellen Netzwerkstatus anzeigen.



Schematischer Ablauf der Push-Benachrichtigungen in PRTG

Die kostenfreien Push-Mitteilungen ergänzen SMS und E-Mail-Benachrichtigungen um eine noch schnellere Option. Sie werden über eine eigene Cloud-Infrastruktur übermittelt und informieren direkt über eventuelle Vor- bzw. Ausfälle im Netzwerk. Ein weiteres Plus: Push belastet den Akku des Endgeräts weniger als die bisherige „Pull“-Methode. Mit einem Fingertipp auf die Push-Info kann der Admin die PRTG-App anzeigen lassen und Details zu den Warnungen oder Ausfällen einsehen: Wann wurde der Alarm abgesetzt, wie sieht der Graph dazu aus, welche weiteren Geräte sind betroffen?

Speziell für iOS und Android

Die Push-Nachrichten sind speziell auf die iOS- und Android-Apps von PRTG Network Monitor angepasst. Die PRTG for iOS App gibt Apple-Usern Zugriff auf Übersichten und zeigt Details. Darüber hinaus können Nutzer Alarme bestätigen, das Monitoring pausieren lassen, Graphen und Übersichtskarten (sogenannte Maps) sowie die PRTG-Logs abrufen. Der Admin bleibt über mehrere PRTG-Installationen auf dem Laufenden.

Verantwortliche mit Endgeräten auf Basis des Google-Betriebssystems können auf die PRTG for Android App zurückgreifen. Eine spezielle „Dashboard“-Ansicht macht den globalen Sensorstatus zudem auf Tablets und Android TVs sichtbar. Dadurch kann der Zustand der ganzen IT-Infrastruktur beispielsweise auf einem Monitor in der Technikabteilung angezeigt werden. Die Registrierung innerhalb der App erfolgt über einen QR-Code-Scan – ohne aufwändige Eingabe von IP-Adressen, Passwörtern oder Nutzernamen.

Option für Windows Phones und Blackberry

Für Nutzer anderer Betriebssysteme hat Paessler außerdem die App PRTG for Windows Phone mit Anlehnung an die Kachel-Optik sowie eine PRTG Blackberry-Anwendung entwickelt, die einen ähnlichen Funktionsumfang bieten.

Die Apps stehen unter folgenden Links kostenfrei in den jeweiligen App Stores zum Download bereit:

www.paessler.com/apps

PAESSLER
the network monitoring company
Paessler AG
Bucher Str. 79a
D-90419 Nürnberg
Tel.: +49 (911) 9 37 75 - 0
Fax: +49 (911) 9 37 75 - 409

E-Mail: info@paessler.com
URL: www.de.paessler.com
Ansprechpartner:
Fabian Konitzko

Workshop: SSD-RAIDs mit optimaler Performance betreiben

Flash-Stapel mit Turbo

von Werner Fischer und Georg Schönberger

Quelle: iStockphoto – 12381

Bis vor wenigen Jahren kamen in einem RAID-Verbund ausschließlich Festplatten zum Einsatz. Dementsprechend waren bis dahin Hardware-RAID-Controller ausschließlich auf die I/O-Charakteristiken von Festplatten optimiert. Die unterschiedlichen I/O-Eigenschaften von SSDs erfordern jedoch entsprechend optimierte RAID-Controller und RAID-Einstellungen. Wie Sie Ihr SSD-RAID zu optimaler Performance bringen, zeigen wir Ihnen in diesem Workshop.

Konventionelle Festplatten speichern ihre Daten auf einer oder mehreren Magnetscheiben, die über einen Schreib-/Lesekopf beschrieben und ausgelesen werden. SSDs kommen im Gegensatz dazu ohne mechanische Bauteile aus. Die Daten werden hier in Flash-Speicherzellen abgelegt. Chips mit SLC (Single Level Cell) speichern 1 Bit pro Speicherzelle, jene mit MLC (Multi Level Cell) 2 Bits, TLC (Triple Level Cell) speichert 3 Bits. Mehrere Speicherzellen sind in einem Flash-Chip zu einer Page (zum Beispiel 8 KiB) organisiert. Mehrere Pages bilden dann einen Block (etwa 2 MiB).

Auf dieser Ebene kommt auch schon die erste Eigenheit von Flash-Speichern ans Tageslicht: Neue Daten können zwar in ungenutzte Pages geschrieben werden – ein nachträgliches Ändern ist jedoch nicht möglich. Das funktioniert erst dann wieder, wenn der SSD-Controller zuvor den gesamten zugehörigen Block löscht. Damit immer ausreichend ungenutzte Pages bereitstehen, verfügen SSDs über zusätzliche Speicherzellen (Spare Area). Je nach SSD ist die Größe der Spare Area zwischen 7 und 78 Prozent der Nennkapazität.

Eine Möglichkeit, der SSD mitzuteilen, welche Datenbereiche nicht mehr verwendet und somit gelöscht werden können, ist TRIM. Hier teilt das Betriebssystem dem SSD-Controller mit, welche Datenbereiche gelöscht werden können. TRIM lässt sich für eine einzelne SSD einfach implementieren, für Paritäts-RAIDs wäre die Umsetzung aber durchaus aufwändig. Daher unterstützt bislang auch kein Hardware RAID-Controller die TRIM-Funktionalität. Dieses Manko lässt sich aber recht leicht umschiffen: Die meisten Enterprise-SSDs kommen von Haus aus mit einer vergleichsweise großen Spare-Area, weshalb die TRIM-Unterstützung kaum eine Rolle spielt. Und wem die Performance noch nicht reicht, der kann zusätzlich noch mit Over-Provisioning arbeiten – dazu später mehr.

Performance: IOPS, Latenz und Durchsatz

Bei der Messung der SSD-Performance sind vor allem drei Messgrößen entscheidend: IOPS, Latenz und Durchsatz. Der Begriff IOPS (Input/Output Operations Per Second) beschreibt die Anzahl an Ein/Ausgabe-Operationen pro Sekunde. Read IOPS beziehen sich konkret auf Ausgaben pro Sekunde, Write IOPS auf Eingaben. Die Größe einer solchen I/O-Operation beträgt 4 KiB (sofern nicht anders angeführt). IOPS werden meistens "random", also mit zufällig verteilten Zugriffen gemessen, um tatsächlich Worst-Case-Werte zu erfassen. Während Festplatten nur rund 100-300 IOPS schaffen, bieten aktuelle Enterprise-SSDs bis zu 36.000 Write und 75.000 Read IOPS (beispielsweise das 800 GByte-Modell Intel DC S3700 SSD).

Latenz beschreibt die Wartezeit in ms, bis eine einzelne I/O-Operation durchgeführt wurde. Die typische durchschnittliche Latenz beträgt bei SSDs zwischen 0,1 und 0,3 ms, bei Festplatten zwischen 5 und 10ms. Hierbei ist zu beachten, dass die Festplatten-Hersteller mit der Latenz nur die Zeit einer halben Umdrehung der Scheibe beschreiben. Zur echten Latenz, also der mittleren Zugriffszeit, ist hier noch die Spurwechselzeit (Seek Time) zu addieren.

Der Durchsatz schließlich bezeichnet die Datentransferrate in MByte pro Sekunde (MB/s). Er wird typischerweise mit größeren und sequenziellen I/O-Operationen gemessen. SSDs schaffen etwa den doppelten bis dreifachen Durchsatz von Festplatten. Bei SSDs mit wenigen Flash-Chips (SSDs mit geringerer Kapazität) ist die Schreibperformance etwas eingeschränkt und liegt etwa auf Festplatten-Niveau.

Folgende Faktoren beeinflussen die Performance einer SSD:

- Read/Write Mix: Bei SSDs unterscheiden sich Lese- und Schreiboperationen auf Hardware-Ebene deutlich. Aufgrund des höheren Controller-Overheads von

Schreiboperationen erzielen SSDs typischerweise mehr Lese-IOPS als Schreib-IOPS. Besonders hoch ist dieser Unterschied bei Consumer-SSDs. Bei Enterprise-SSDs verbessern die Hersteller die Schreibperformance durch eine größere Spare-Area und optimierte Controller-Firmware.

- Random/Sequential Mix: Die Anzahl an möglichen IOPS hängt außerdem davon ab, ob die Zugriffe zufällig über den gesamten Datenbereich (LBA-Bereich) verteilt sind oder sequenziell durchgeführt werden. Bei zufälligen Zugriffen steigt der Managementaufwand des SSD-Controllers und die Anzahl an möglichen IOPS nimmt damit ab.
- Queue Depth: Die Queue Depth bezeichnet die Länge der Warteschlange im I/O-Pfad zur SSD. Bei einer größeren Warteschlange (zum Beispiel 8, 16 oder 32) fasst das Betriebssystem die konfigurierte Anzahl an I/O-Operationen zusammen, bevor es diese an den SSD-Controller sendet. Eine größere Queue Depth erhöht die Anzahl der möglichen IOPS, da die SSD die Anfragen parallel an die Flash-Chips senden kann. Sie erhöht aber auch die durchschnittliche Latenz, und damit die Wartezeit auf eine einzelne I/O-Operation – weil eben nicht jede Operation einzeln sofort an die SSD geleitet wird, sondern erst, wenn die Warteschlange voll ist.
- Spare Area: Die Größe der Spare Area hat einen direkten Einfluss auf die Random Write-Performance der SSD (und damit auch auf die Kombination aus Lese- und Schreib-Performance). Je größer die Spare Area, desto seltener muss der SSD-Controller intern Daten umstrukturieren. Der SSD-Controller hat damit mehr Zeit für Host-Anfragen – die Random Write-Performance steigt.

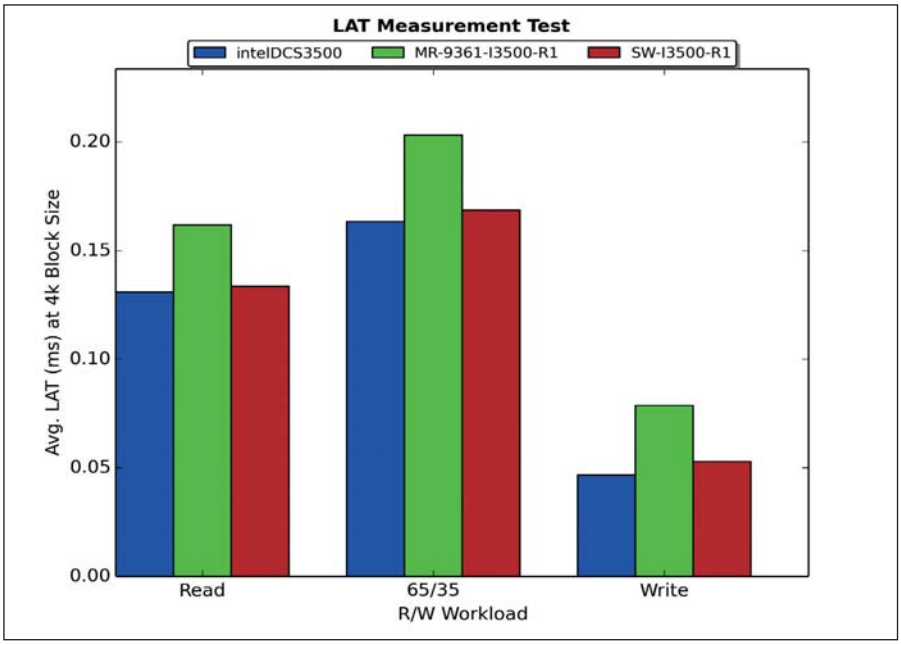


Bild 1: Der Overhead für Latenzen im HWR beträgt etwa 0,04 ms. RAID 1 als SWR erhöht die Latenzen gegenüber einer einzelnen SSD minimal.

Bestimmen der Baseline Performance

Die zuvor genannten Eigenschaften von SSDs erfordern speziell abgestimmte Performance-Tests. Konkret erschweren der FOB-Zustand (Fresh out of the Box) und die Übergangsphasen zwischen Workloads eine Bestimmung von stabilen Performance-Werten. Die resultierenden Werte sind daher von folgenden Faktoren abhängig:

- Schreibende Zugriffe sowie Prekonditionierung – der Zustand der SSD vor dem Test.
- Workload Pattern – I/O Pattern (Read/Write Mix, Blockgrößen) während des Tests.
- Data Pattern – die geschriebenen Daten.

Die Anforderungen an aussagekräftige SSD-Tests hat die Organisation SNIA sogar dazu veranlasst, eine eigene "Enterprise Performance Test Specification" (PTS) zu veröffentlichen.

In den meisten Fällen besteht jedoch nicht die Möglichkeit, in diesem Umfang Tests durchzuführen. Oftmals reicht es im ersten Schritt aus, mit einfachen Mitteln eine "Baseline Performance" der SSD zu bestimmen. Dadurch erhalten Sie in Form von MB/s und IOPS auf Ihr System zugeschnittene Kenngrößen.

Die Tabelle "Performance-Messung mit FIO" geht näher auf das Performance-Werkzeug "Flexible IO Tester" (FIO) ein. FIO ist vor allem unter Linux verbreitet, aber auch für Windows und VMware ESXi verfügbar. Entwickelt vom Maintainer des Linux Block Layers, Jens Axboe, steckt einiges an Wissen und Funktionalität darin. Nutzen Sie die Tabelle für einen einfachen Performance-Test Ihrer SSD unter Linux. Windows-Nutzer müssen die Parameter "libaio" und "iodepth" entfernen.

Performance-Messung mit FIO

Durchsatz Lesen	fio --name=readTP --rw=read --size=5G --bs=1024k --direct=1 --refill_buffers --ioengine=libaio --iodepth=16
Durchsatz Schreiben	fio --name=writeTP --rw=write --size=5G --bs=1024k --direct=1 --refill_buffers --ioengine=libaio --iodepth=16
IOPS Lesen	fio --name=readIOPS --rw=randread --size=1G --bs=4k --direct=1 --refill_buffers --ioengine=libaio --iodepth=16
IOPS Schreiben	fio --name=writeIOPS --rw=randwrite --size=1G --bs=4k --direct=1 --refill_buffers --ioengine=libaio --iodepth=16
IOPS Mixed Workload, 50 Prozent Lesen und 50 Prozent Schreiben	fio --name=mixedIOPS --rw=randrw --size=1G --bs=4k --direct=1 --refill_buffers --ioengine=libaio --iodepth=16

RAID 1, RAID 5 und RAID 10 mit SSDs

Unsere Analyse von SSDs im RAID-Verbund zeigt, wie sich die Performance-Werte beim Erhöhen der Anzahl an SSDs entwickeln. Außerdem gehen die Tests auf

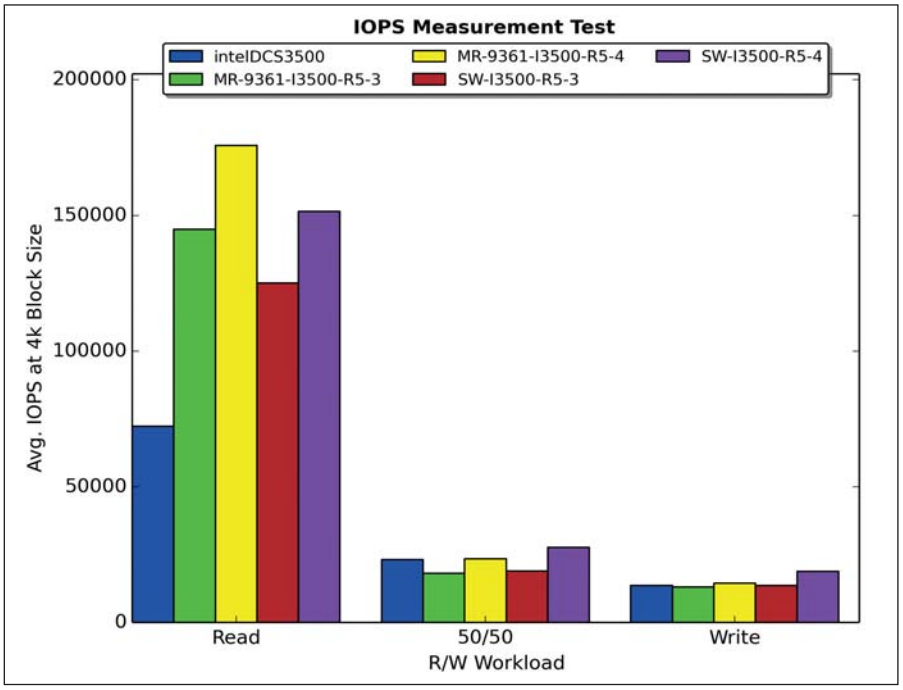


Bild 2: Auffällig sind die geringen IOPS-Zahlen bei zufälligem Schreiben im RAID 5. Beim Vergleich von HWR mit SWR spielt der Workload eine Rolle.

die unterschiedlichen Charakteristika der RAID-Level ein.

Das Hardware-Setup für die RAID-Tests besteht aus Intel SSDs der DC S3500er Serie, einem Avago (vormals LSI) MegaRAID 9365 RAID-Controller und einem Supermicro X9SCM-F Mainboard. Die Größe der SSD beläuft sich auf 80 GByte. Beachten Sie, dass die Performance einer SSD innerhalb einer Serie auch von ihrer Kapazität abhängt. Ein 240 GByte-Modell etwa hat gegenüber einem 80 GByte-Modell Performance-Vorteile.

Als Performance-Software setzen wir TKperf unter Ubuntu 14.04 ein. TKperf setzt die PTS der SNIA unter Verwendung von FIO um. Seit Version 2.0 erstellt es Linux Software-RAIDs (SWR) automatisch mit mdadm, Hardware-RAIDs (HWR) für Avago MegaRAID Controller mit storcli. Eine Unterstützung für Adaptec RAID-Controller ist geplant.

RAID 1

RAID 1 ist aufgrund gegebener Ausfallsicherheit sehr verbreitet. Bei Lesezugriffen profitieren Sie zusätzlich davon, dass auf beide SSDs gleichzeitig zugegriffen wird. Sowohl SWR als auch HWR bestätigen diese Annahme und liefern bei zufälligem Lesen mit 4K-Blockgröße etwa 107.000 und 120.000 IOPS – immerhin mehr als das 1,4-fache einer einzelnen SSD. Zufällige Schreibzugriffe sollte der RAID-Verbund eigentlich so schnell wie eine SSD abarbeiten. Die Tests offenbaren jedoch für SWR und HWR Performance-Einbußen von zirka 30 Prozent bei zufälligem Schreiben und 50/50 Mixed Workloads.

Erfreuliche Ergebnisse liefert der Latenz-Test für SWR. Die Latenzen liegen bei allen drei Workloads nur minimal über jener einer einzelnen SSD. In Bezug auf HWR fügt der RAID-Controller Latenzzeit hinzu. Ein konstanter Overhead von ca. 0,04 ms zeigt sich bei allen Workloads (Bild 1).

RAID 5

Kennzeichen von RAID-Level 5 sind Paritätsdaten, die beim Schreiben von Daten zusätzlichen Aufwand verursachen. Der Mehraufwand spiegelt sich deutlich in den Ergebnissen des IOPS-Tests wider. Ein RAID 5 mit drei SSDs erreicht bei zufälligem Schreiben mit 4K genauso viele IOPS wie eine einzelne SSD. Wer glaubt, das Hinzufügen einer weiteren SSD zum RAID 5 steigert die Schreibperformance erheblich, liegt falsch. Intel analysiert diesen Umstand umfassend im Whitepaper "Intel SSD DC S3500 Series Workload Characterization in RAID Configurations" [1]. Erst bei acht SSDs im RAID 5 werden beim Schreiben die doppelten IOPS gegenüber drei SSDs erreicht. Beim Vergleich von HWR mit SWR liegen bei drei SSDs beide gleichauf. Das Setup mit vier SSDs im RAID 5 fällt für SWR günstiger aus. Mixed Workloads und reines Schreiben bei 4K befinden sich zirka 4.000 IOPS über HWR. Bild 2 fasst die Ergebnisse einer einzelnen SSD, von HWR und SWR mit drei und vier SSDs im RAID 5 zusammen.

Je leselastiger der Workload wird, umso weniger machen sich die Paritätsberechnungen bemerkbar. HWR liefert mit vier SSDs im RAID 5 fast 180.000 IOPS – das ist mehr als das Doppelte einer einzelnen SSD. SWR liegt nicht ganz auf diesem Niveau und überschreitet knapp die 150.000 IOPS-Marke. Der Latenz-Test verdeutlicht den Unterschied bei Lese- und Schreib-Zugriffen auf ein Weiteres. Von Lesen über 65/35 mixed zu Schreiben addieren sich bei HW 0,12 ms hinzu. SWR verzeichnet pro Workload einen Anstieg von etwa 0,10 ms.

Keine Blöße gibt sich RAID 5 beim Lese-Durchsatz mit 1.024K-Blöcken. HWR verarbeitet bei vier SSDs im RAID 5 über 1,2 GBit/s, SWR pendelt sich etwas dahinter bei 1,1 GBit/s ein. Der Schreibdurchsatz wird durch das 80 GByte-Modell begrenzt, der laut Spezifikation beim Schreiben bei 100 MBit/s endet. Die vier SSDs im RAID liefern bei den Tests von HWR rund 260 MBit/s, SWR schafft 225 MBit/s.

RAID 10

Wie der Name bereits vermuten lässt, ist RAID 10 eine Kombination aus RAID 1 und RAID 0. Im Einsatz mit vier SSDs bietet sich ein direkter Performance-Vergleich mit RAID 5 an. In puncto Kapazität stehen bei RAID 10 zwar nur 50 Prozent der Netto-Kapazität zur Verfügung, wer viel zufällig schreibt, wird gegenüber RAID 5 aber große Vorteile haben. Bild 3 zeigt deutlich die Schreib-Schwäche von RAID 5 hinsichtlich IOPS. Ebenso machen sich die erhöhten Latenzen bei RAID 5 aufgrund der erforderlichen Paritätsberechnungen bemerkbar. RAID 10 liefert dagegen Latenzen, die sich an den Zeiten einer einzelnen SSD orientieren. Wem Schreib-Perfor-

mance und Latenzen egal sind, kann dennoch beruhigt auf RAID 5 setzen.

Wirksame Tuningmaßnahmen

Beim Einsatz von Hardware-RAID-Controllern für SSD-RAIDs gilt folgende Empfehlung: möglichst aktuelle RAID-Controller verwenden! Die Firmware von neueren RAID-Controllern ist deutlich besser auf SSDs optimiert als ältere Modelle. Bei den Avago MegaRAID Controllern haben beispielsweise die neuen 12 GBit-SAS-Controller das Feature zur Optimierung von SSD-RAID-Performance (FastPath) nun standardmäßig integriert.

Zur Performance-Steigerung von HDD-RAIDs wurden Hardware-RAID-Controller schon bald mit einem Cache ausgestattet. Aktuelle Controller verfügen über 512 MByte bis 1 GByte Cache. Dieser kann sowohl für Schreib- (Write Cache) als auch Lesezugriffe (Read Ahead) genutzt werden. Bei SSD-RAIDs sollten Sie auf den Einsatz dieser Caches jedoch aus den gleich näher beleuchteten Hintergründen verzichten.

Write Cache deaktivieren

Bei HDD-RAIDs bringt der Schreibcache (Write Back Policy) einen spürbaren Performance-Schub. Vor allem kleine und zufällige Schreibzugriffe kann der RAID-Controller optimal im Cache zwischenspeichern, bevor er sie auf vergleichsweise träge Festplatten schreibt. Die Anzahl an möglichen Write IOPS steigt entsprechend von wenigen hundert auf mehrere tausend IOPS. Zusätzlich sinkt die Latenz spürbar – von 5 bis 10 ms auf unter 1 ms. Bei RAID 5 und 6 mit HDDs bringt der Schreibcache einen weiteren Vorteil: Ohne Cache würde die erforderliche Leseoperation für die Paritätsberechnung (Stichwort Read-Modify-Write) nämlich zusätzlich bremsen. Dank Cache kann dies zeitversetzt passieren. Damit bei einem Stromausfall keine Daten verloren gehen, muss ein verwendeter Schreibcache mit BBU- oder Flash-Schutz-Modul (LSI CacheVault oder Adaptec ZMCP) geschützt werden.

Bei SSDs ist alles anders: Ihre Performance ist bereits so hoch, dass ein Schreibcache durch den damit verbundenen Overhead nur bremst. Das bestätigen auch unsere Messergebnisse in Bild 4: Bei einem RAID 5 mit vier SSDs sinken die Write IOPS bei aktiviertem Write Back von 14.400 auf 3.000 – das sind fast 80 Prozent weniger IOPS. Der einzige Vorteil des Schreibcaches sind geringe Schreiblatenzen bei RAID 5 RAID-Sets. Da diese aber bei RAID 1 (ohne Paritätsberechnungen und ohne Schreibcache) noch niedriger sind, fällt auch dieser Vorteil schnell weg. Daher lautet die Empfehlung: SSD-RAIDs ohne Schreibcache betreiben (also "Write-Through" statt "Write-Back"). Damit können Sie sich die zirka 150 bis 200 Euro für das BBU- oder Flash-Schutz-Modul sparen.

Read Ahead abschalten

Read Ahead – das Lesen von Datenblöcken, die hinter den aktuell abgefragten Daten liegen – ist ebenfalls eine Performance-Optimierung, die nur mit Festplatten wirkliche Vorteile bringt. Beim RAID 5 mit vier SSDs bremst aktiviertes Read Ahead die Lese-IOPS in unseren Tests um 20 Prozent (von zuvor 175.000 auf 140.000 Read IOPS). Beim Durchsatz gibt es beim Lesen mit 64 K- oder 1.024 K-Blöcken keine Performance-Unterschiede. Einzig beim Durchsatz mit 8 K-Blöcken zeigt Read Ahead in unseren Tests Vorteile. Daneben kann Read Ahead nur bei single-threaded Lesetests (zum Beispiel mit dd unter Linux) Vorteile bringen. Beide Zugriffsmuster sind im Serverbetrieb aber untypisch. Unsere Empfehlung lautet daher: SSD-RAIDs ohne Read Ahead betreiben.

Over-Provisioning

Wie bereits erwähnt, hat die Größe der Spare Area einen direkten Einfluss auf die Random Write-Performance einer SSD. Bereits eine kleine Erhöhung der Spare Area kann die Random Write-Performance und die Haltbarkeit (Endurance) einer SSD signifikant erhöhen. Diese Empfehlung aus den Anfangstagen der SSD-Ära hat auch heute noch ihre Gültigkeit. Bei aktuellen SSDs ist die Haltbarkeit allerdings schon so ausreichend, dass eine Vergrößerung der Spare Area in erster Linie aus Performance-Gründen sinnvoll ist.

Die Größe der Spare Area können Sie durch manuelles Over-Provisioning sehr einfach erhöhen, indem Sie nur einen Teil der Kapazität der SSD für das RAID-Set

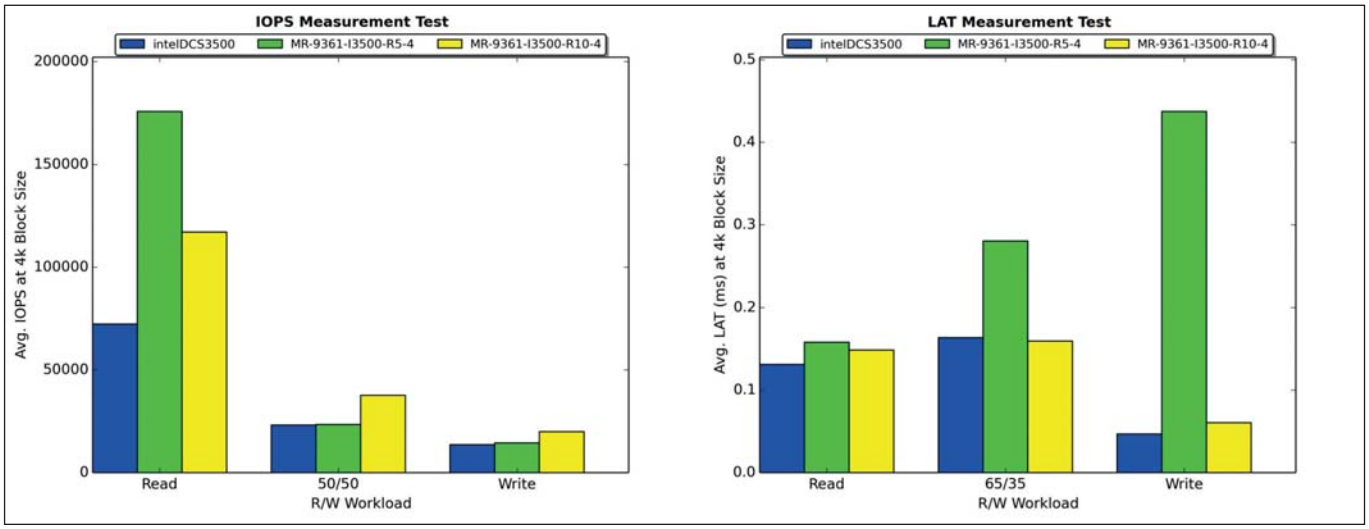


Bild 3: Die Performance von RAID 5 und RAID 10 hängt stark vom Einsatzzweck ab. Die IOPS bei zufälligem Lesen sind bei RAID 5 deutlich höher. Je mehr zufällig geschrieben wird, umso besser kommt RAID 10 in Fahrt. Latenzen auf SSD-Niveau erhalten Sie nur mit RAID 10.

konfigurieren (etwa 80 Prozent) und den Rest einfach frei lassen. Falls Sie die SSD zuvor verwendet haben, führen Sie noch ein Secure Erase durch – damit löschen Sie sämtliche Flash-Zellen. Nur dann kann der SSD-Controller diese freien Bereiche auch als Spare Area verwenden. Wie Bild 5 zeigt, verdreifachen sich beinahe die Write IOPS bei 20 Prozent Over-Provisioning (am Beispiel der Intel DC S3500 800 GByte-SSD).

Eine Anmerkung am Rande: Over-Provisioning hat keinen Einfluss auf die reine Lese- oder sequenzielle Schreib-Performance – bringt also Performance-Vorteile nur bei zufälligen mixed read/write- oder reinen write-Workloads.

Unter Linux verwenden: Deadline I/O Scheduler

Für SSDs und SSD-RAIDs bringt der Deadline I/O Scheduler erfahrungsgemäß die höchste Performance. Ubuntu verwendet seit Ubuntu 12.10 standardmäßig den Deadline Scheduler, andere Distributionen setzen teilweise noch auf den CFQ Scheduler, der vor allem auf Festplatten hin optimiert ist. Mit einem einfachen *cat /sys/block/sda/queue/scheduler* überprüfen Sie, welcher Scheduler (in diesem Falle für das Device sda) zum Einsatz kommt.

Bis zum nächsten Reboot können Sie als root den Scheduler per *echo deadline > /sys/block/sda/queue/scheduler* auf Deadline setzen. Informationen zum permanenten Ändern des Schedulers entnehmen Sie der Dokumentation der verwendeten Linux Distribution. Mittelfristig wird der Linux Multi-Queue Block IO Queueing Mechanism (blk-mq) die traditionellen I/O Scheduler für SSDs ablösen. Bis blk-mq aber auch bei den Long-Term-Support Enterprise Distributionen zum Einsatz kommt, wird es noch etwas dauern.

Gesundheitszustand von SSD und RAID überwachen

Flash-Zellen einer SSD verkraften nur eine begrenzte Anzahl an Schreibzyklen. Die endliche Lebensdauer ist auf den internen Aufbau der Speicherzellen zurückzuführen, die bei Schreibzugriffen sogenannten Program/Erase-Zyklen (P/E) unterliegen. Das Floating Gate der Zellen, das zum Beschreiben der Zelle verwendet wird, nutzt sich mit jedem Zyklus ab. Überschreitet die Abnutzung einer Zelle einen gewissen Schwellenwert, markiert der Controller der SSD diese als Bad Block und ersetzt ihn durch einen aus der Spare Area. Zumindest zwei Indikatoren leiten sich aus dieser Funktionsweise direkt ab:

1. Die Abnutzung der Flash-Zellen, der Media Wearout Indicator.
2. Die Anzahl an übrigen Spare Blocks, auch Available Reserved Space genannt.

Im optimalen Fall gibt der Hersteller diese beiden Werte über SMART-Attribute an den Nutzer weiter. Zur einwandfreien Überwachung der Attribute ist eine detaillierte SMART-Spezifikation der SSD unerlässlich. Denn die Interpretation der Werte ist nicht standardisiert und von Hersteller zu Hersteller unterschiedlich. Als Beispiel dienen hier Intel und Samsung. Deren Attribute unterscheiden sich zwar in ID und Namen, der verwendete Wert ist aber zumindest gleich. Mit dem Kommandozeilen-Werkzeug smartctl rufen Sie für eine SSD SMART-Attribute ab, mit megaraid- und sg-Devices auch hinter Avago MegaRAID und Adaptec Controllern:

```
smartctl -a /dev/sda
smartctl -a -d megaraid,6 /dev/sda
smartctl -a -d sat /dev/sg1
```

Dies verdeutlicht, wie wichtig eine offengelegte Spezifikation der Hersteller für eine zuverlässige Überwachung ist. Intel ist übrigens bei seinen Data-Center-SSDs vorbildlich und stellt eine detaillierte Spezifikation inklusive SMART-Attributen bereit.

Die Integration der SMART-Überwachung in ein Monitoring Framework wie Icinga ist der nächste Schritt. Ein Plug-In muss dazu auf die Spezifikation der Hersteller eingehen und die Werte der Attribute richtig deuten. Das Thomas-Krenn-Team entwickelte dazu mit check_smart_attributes [2] ein Plug-In, das in einer JSON-Datenbank die Spezifikation der Attribute abbildet. Seit Version 1.1 überwacht das Plug-In auch SSDs hinter RAID-Controllern.

Die SMART-Attribute bestimmen eindeutig die Abnutzung der Flash-Zellen, die Haltbarkeit einer SSD leitet sich daraus ab. Weitere Attribute komplettieren den Gesundheits-Check für SSDs im Unternehmenseinsatz. Bei Intel ist ein solches Beispiel das Attribut Power_Loss_Cap_Test für die Funktionstüchtigkeit des integrierten Cache-Schutzes der SSD. Der Cache-Schutz stellt sicher, dass beim Verlust der Stromversorgung keine Daten verloren gehen. Dieses Attribut verdeutlicht, wie wichtig die regelmäßige Prüfung der SMART-Attribute von SSDs ist. Stellen Sie daher

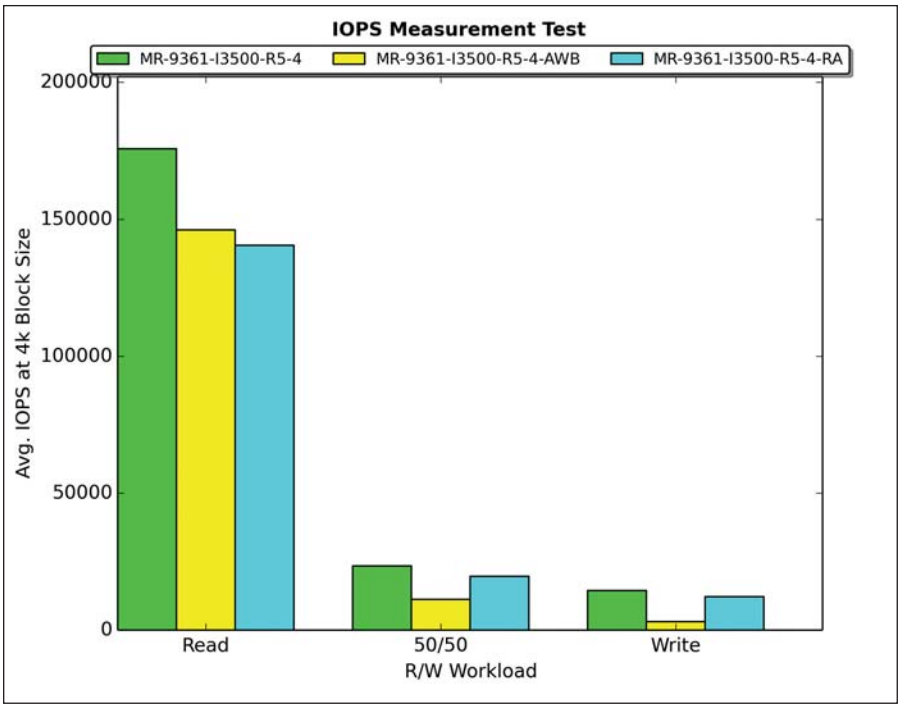


Bild 4: Der Avago MegaRAID 9361 liefert ohne Write Cache und ohne Read Ahead die beste IOPS Performance für SSD RAIDs.

auf jeden Fall sicher, dass detaillierte Informationen zu den SMART-Attributen vorliegen, bevor Sie SSDs in größerem Umfang einsetzten. Der Prüfung des Gesundheitszustands Ihrer SSDs steht dann nichts mehr im Weg.

RAID-Konsistenz prüfen

Neben der Prüfung von SMART-Attributen sind Consistency Checks weiterer Bestandteil eines optimalen RAID-Betriebs. Hardware-RAID-Hersteller verwenden für die Konsistenz-Prüfung auch den Begriff "Verify". Linux Software-RAID setzt die Funktionalität über ein eigenes Skript namens checkarray um. Egal welche Technologie Sie einsetzen, regelmäßige Consistency Checks decken Inkonsistenzen in Daten oder Prüfsummen auf. Stellen Sie daher sicher, dass auf Ihren Systemen regelmäßig Consistency Checks laufen:

1. Mdadm richtet in den meisten Fällen einen Cronjob in */etc/cron.d/mdadm* ein. Der Job startet jeden ersten Sonntag eines Monats einen Consistency Check für alle eingerichteten Software-RAIDs. Aber Achtung – prüfen Sie nach dem Check unbedingt, ob der zugehörige Counter im sysfs gleich 0 ist:

```
$ cat sys/block/md0/md/
mismatch_cnt
0
```

   Das Skript *checkarray* prüft zwar das RAID auf Konsistenz, führt aber von selbst keine Korrekturen durch. Für die RAID-Level 4, 5 und 6 sind Mismatches ein Anzeichen auf Hardware-Probleme. RAID 1 und 10 produzieren unter Umständen auch Mismatches, ohne dass ein Fehler vorliegt, vor allem wenn sich SWAP-Devices darauf befinden. Im Fehlerfall verschickt mdadm E-Mails übrigens nur dann, wenn Sie in der Datei *mdadm.conf* unter "MAILADDR" die richtige Adresse eintragen.
2. Der Megaraid Storage Manager (MSM) ist bei LSI erste Anlaufstelle für regelmäßige Consistency Checks. Klarer Vorteil ist, dass der MSM unter Windows, Linux und VMware ESXi läuft. Die Sektion "Controller" führt zum Reiter "Schedule Consistency Check". Dort definieren Sie, wann und wie oft ein Check laufen soll.
3. Das Adaptec Kommandozeilen-Werkzeug ermöglicht Consistency Checks per datascrub-Kommando. Data Scrubbing wird oft im Zusammenhang mit Consistency Checks verwendet, da es den Vorgang der Fehlerkorrektur bezeichnet. Das folgende Beispiel richtet einen regelmäßigen Check im Abstand von 30 Tagen ein:

```
$ arcconf datascrub 1 period 30
```

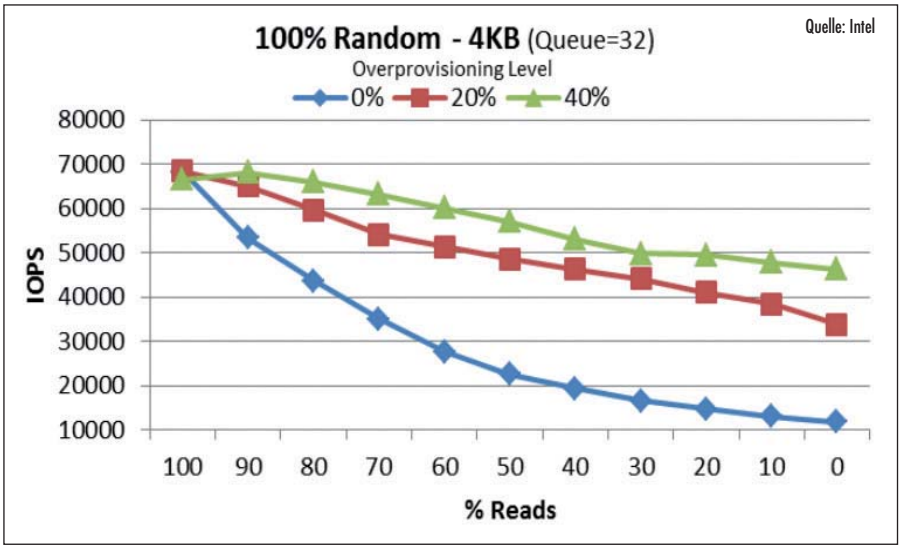


Bild 5: Bei einer Intel DC S3500 800 GByte-SSD steigen mit 20 Prozent Over-Provisioning die möglichen Write IOPS von rund 12.000 IOPS auf etwa 33.000 IOPS, bei 40 Prozent sogar auf zirka 47.000 IOPS. Bei reinen Lesezugriffen bleibt die Performance unverändert.

Fazit

Aktuelle RAID-Controller haben keine Probleme mit SSDs. Sie brauchen außerdem den Performance-Vergleich mit Linux Software-RAID nicht zu fürchten. Die Wahl der RAID-Technologie wird daher vor allem eine Frage des eingesetzten Betriebssystems und persönlicher Vorlieben sein. Linux hat mit aktuellen Kerneln und mdadm jedenfalls alle Werkzeuge für SSD-RAIDs an Board. Freunde von RAID-Controllern brauchen sich über das Betriebssystem keine Gedanken machen. Eines ist aber klar: Controller-Cache und Read-Ahead haben bei SSD-RAIDs nichts verloren. Die BBU oder Flash-basierte Cache-Schutzlösungen sparen Sie dann gleich mit ein.

Die Entscheidung für das richtige RAID-Level kann Ihnen niemand abnehmen. Hier müssen Sie selbst Hand anlegen und Ihre Applikationen beziehungsweise Ihre Systeme analysieren. Schreiben oder lesen Sie vorwiegend von Ihrem I/O-System? Steht zufälliges Lesen im Vordergrund ist RAID 5 eine gute Wahl, bei dem noch dazu die Kapazitätseinbußen gering sind. Der Klassiker RAID 1 kommt auch mit SSDs nicht außer Mode. Solide Latenzen und 40 Prozent mehr Lese-IOPS als mit einer SSD sprechen für sich. Verluste bei den Schreib-IOPS werden Sie bei RAID 5 und bei RAID 1 vorfinden. Schaffen Sie sich SSDs im großen Stil an und möchten ausgewogene Performance erreichen, führt kein Weg um RAID 10 herum. Schreib-Performance, Latenzen und Lese-IOPS lassen bei RAID 10 die Herzen höher schlagen. *(ln)*

1. Bei HWR aktuellen RAID Controller einsetzen.
2. Unter Linux bei HWR und SWR Deadline I/O Scheduler verwenden.
3. HWR Cache-Einstellungen: Write-Through, Kein Read Ahead.
4. Over-Provisioning bei höheren Random Write-Anforderungen.
5. SSDs verwenden, für die SMART-Attribute öffentlich dokumentiert sind.
6. Die Write Endurance bestimmt die Haltbarkeit der SSD, SMART-Attribute zeigen den aktuellen Status.

Checkbox für SSD-RAIDs

[1] Whitepaper zur Perfmance-Messung bei SSDs F3P41

[2] Plug-In "SMART Attributes Monitoring" F3P42

Link-Codes

Workshop: Hochverfügbarkeit mit der Oracle Standard-Edition

Einfach dauerhafter Betrieb

Quelle: Nemanja Trifunovic – 123RF

von Sebastian Winkler

Ausfallsicherheit ist für eine produktive Datenbank nahezu unverzichtbar. Strebt der IT-Verantwortliche dieses Ziel mit seiner Oracle-Datenbank an, scheint die Standard-Edition dafür ungeeignet und nur der tiefe Griff ins Portemonnaie zum Erwerb der passenden Lizenz hilft weiter. Doch so kommt er nicht nur in den Genuss einer hochverfügbaren Datenbank, sondern kauft auch zahlreiche Features, die er nicht benötigt. Unser Workshop berichtet von Projekterfahrungen bei der Nutzung der Standard-Edition für HA-Aufgaben und gibt Hinweise zur eigenen Umsetzung.

Geht es im Oracle-Umfeld um den Aufbau einer Hochverfügbarkeitsumgebung, wird Ihnen Oracle seine "Maximum Availability Architecture", bestehend aus RAC (Real Application Cluster), Data Guard und GoldenGate, liefern. Doch dieses Paket aus unterschiedlichen Lösungen für unterschiedliche Probleme führt zu Fragen hinsichtlich der Notwendigkeit und der Eignung der verschiedenen Produkte für das eigene Unternehmen. Halten wir uns die Definition von Hochverfügbarkeit vor Augen, müssen wir uns für unsere Datenbankumgebung fragen: Was soll überhaupt abgesichert werden?

So splittet sich die Hochverfügbarkeit in mehrere Teile: Soll primär der Ausfall einer Anwendung abgesichert werden oder – in vielen Fällen wahrscheinlicher – soll eine Absicherung gegen einen möglichen Datenverlust erfolgen? So kommen wir dann auch zu den technischen Unterschieden zwischen RAC und Data Guard. Denn allein mit dem Aufbau eines RACs haben Sie keinerlei Absicherung gegen einen Ausfall des Rechenzentrums, beispielsweise durch einen Brand. Dazu bedarf es einer Standby-Lösung, für die Sie eine Data Guard-Konfiguration aufbauen. Leider lässt sich aber gerade Data Guard ausschließlich in der Enterprise-Edition nutzen. In der Data Guard-Dokumentation findet sich neben dem Hinweis darauf auch eine nette Anmerkung: So ist es zwar möglich mit der Standard Edition selbst eine Standby-Datenbank-Umgebung manuell aufzusetzen, indem archivierte Redolog-Files per OS-Befehl auf die Standby-Seite verschoben und anschließend per Skript eingespielt werden, aber natürlich nicht mit den Überwachungs- und Verwaltungsfunktionen, die Data Guard bietet.

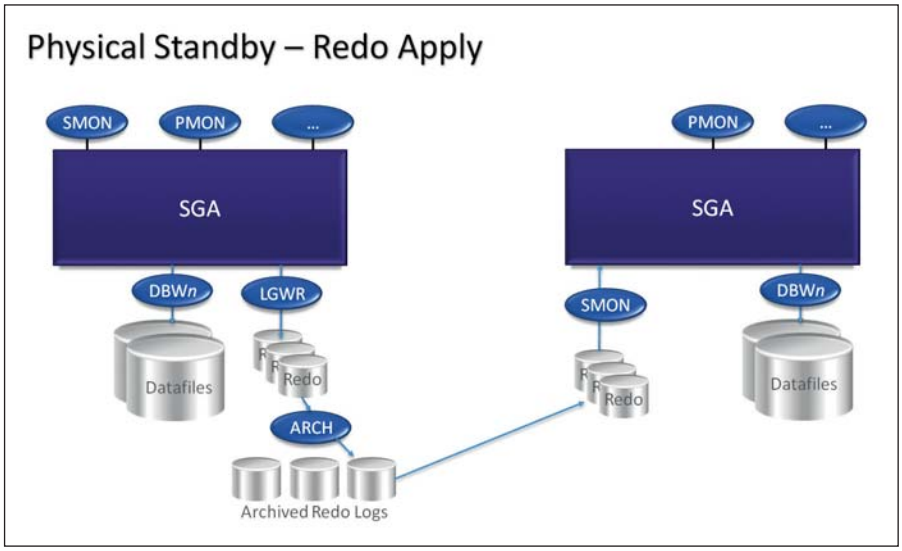
Standard-Edition und Hochverfügbarkeit

Ist Hochverfügbarkeit also nur mit der Enterprise-Edition realisierbar? Schauen wir uns Oracle GoldenGate an, das auch mit der Standard-Edition nutzbar ist, stellen wir fest, dass es im Vergleich mit Data Guard eine Reihe zusätzlicher Features bietet. Dazu zählen etwa plattformübergreifende und versionsübergreifende Nutzung oder auch eine bidirektionale Replikation. Dies sind jedoch Features, die wir für unsere Zwecke – eine HA-Umgebung mit der Standard-Edition – gar nicht benötigen.

Jetzt ist es also an der Zeit, über den Tellerrand zu schauen und uns mit verschiedenen Drittanbieter-Lösungen zu beschäftigen, die hier Abhilfe schaffen. Denn wenn die Standard-Edition für Ihre Zwecke ausreicht, Sie aber trotzdem auf einen bezahlbaren Schutz vor Ausfällen und Datenverlust nicht verzichten wollen, finden Sie hier Ihre Lösung. Neben dem bekannten "SharePlex" von Quest respektive Dell hat vor allem Dbvisit mit seinem Standby-Produkt zuletzt von sich reden gemacht. Daneben hat Dbvisit mit "Replicate" auch eine eigene Replikationslösung entwickelt. Dies stellt eine Alternative zu Oracle Streams dar, die Sie sich vor allem ansehen sollten, weil die Streams mit Datenbank-Release 12c R1, neben Advanced Replication, den Status "deprecated" erhielten. Was bedeutet, dass das Feature in 12c noch enthalten ist, Oracle aber die Entwicklung eingestellt hat. Somit ist es nur eine Stufe vor "desupported" und letztlich neben der eingeschränkten Nutzbarkeit in der Standard-Edition auch ein Grund, warum es aus unserer Betrachtung herausfallen muss.

Tolerierbaren Datenverlust definieren

Mit Replikation und Standby haben wir verschiedene Lösungen, denn abseits von gespiegelten Platten ist eine redundante Datenhaltung über eine Replikation – logisch oder physisch – als Standby möglich.



Funktionsweise einer manuellen Standby-Konfiguration und Dbvisit Standby (Physical Standby / Redo Apply): Die Standby-Datenbank befindet sich im Recovery-Modus, archivierte Redo-Logs werden auf die Zielseite verschoben und auf dem Standby-Server wiederhergestellt.

Leider stiften die Begrifflichkeiten und deren Nutzung auch und gerade mit Data Guard gerne Verwirrung. Die Unterschiede liegen in der Nutzbarkeit des Replikats. Während ein "Physical Standby" ausschließlich für den Fehlerfall aufgebaut wird, lässt sich bei einer logischen Replikation die Zieldatenbank voll nutzen, zum Beispiel als Reporting-Datenbank.

Beim Einsatz der Enterprise-Edition mit "Active Data Guard" und "Logical Standby" stehen gleich mehrere Lösungen für eine verlustfreie Replikation bei gleichzeitiger Nutzung des Replikats zur Verfügung. Die Herausforderung bei der Standard-Edition ist jedoch ungleich höher. Lösungen wie Dbvisit Standby, die auf einem Redolog-Shipping basieren, erlauben zwar eine elegante und schnell zu realisierende Hochverfügbarkeit, allerdings mit dem Nachteil, dass bei einem Fehler ein Datenverlust von mehreren Minuten (in der Praxis etwa 15 Minuten) in Kauf genommen werden muss und sich das Replikat während des normalen Betriebs nicht nutzen lässt.

Daher lautet die wohl wichtigste Frage bei der Analyse einer Hochverfügbarkeitsumgebung mit der Standard-Edition: Wie viel Datenverlust ist tolerierbar? Ist die Anzahl der Transaktionen eher gering, kommt eventuell eine Standby-Lösung in Frage, bei der die Redolog-Dateien alle fünf Minuten übertragen werden. Aber Vorsicht: Bei Batchläufen oder anderen größeren Aktionen kann dies schnell zu einem Engpass werden. Das bedeutet, wenn der maximale Datenverlust unterhalb von 15 Minuten liegen muss, sollten Sie von einer physischen Replikation absehen. Hier spielt die logische Replikation ihre Stärken aus, denn sie kann den Datenverlust bei einem Failover auf ein Minimum reduzieren.

Bei der logischen Replikation erfolgt im Gegensatz zum "Physical Standby" kein Recovery der archivierten Redolog-Dateien, sondern die DML- und DDL-Befehle werden direkt aus den Redolog-Dateien wiederhergestellt und auf dem Standby-Server ausgeführt. Data Guard geht hier inzwischen noch andere Wege und schreibt direkt per Logwriter von der primären Datenbank parallel in eigene Standby Redo-Logs auf der Zielseite. In der Physical Standby-Variante wird dann hieraus ganz normal recovert und beim Logical Standby eben per SQL Apply bei geöffneter Datenbank. Der minimale Datenverlust bei einer logischen Replikation beschränkt sich auf Transaktionsdaten, die bis zum Failover noch nicht von der Primärseite zur Replikationsseite verschickt wurden. Das heißt, alles, was in den Redolog-Files gelandet ist und appliziert wurde, befindet sich auch in der replizierten Datenbank. Bei der Übertragung der Daten gibt es zwei konzeptionelle Unterschiede: SharePlex und Dbvisit Replicate übertragen die Daten, bevor das Commit erfolgt, während GoldenGate die Daten gemeinsam mit dem Commit überträgt. Im Fehlerfall könnte also ein einzelnes "Commit" noch durchgeführt worden sein, während größere Transaktionen, die als Gesamtheit übertragen wurden, wahrscheinlich nicht erfolgreich sind.

Herausforderungen der HA-Umgebung

Während ein Physical Standby schnell aufgebaut ist und generell neben einem Monitoring kein weiterer Aufwand nötig ist, handelt es sich bei einer logischen Replikation um eine eigenständige Datenbank, die Sie separat verwalten und bei produktiver Nutzung auch sichern müssen. Letzteres sollte kein unlösbares Problem sein. Mehr Schwierigkeiten bereitet die Tatsache, dass Änderungen in den SYS- und SYSTEM-Schemas bei der logischen Replikation nicht erfasst werden. Gleiches gilt für ROWIDs.

Weitere Probleme können sich aus speziellen Datentypen ergeben, die von einer Replikationslösung nicht unterstützt werden, wie beispielsweise XMLTYPE. Eine weitere Aufgabe stellen Trigger dar, die jetzt vielleicht zweimal feuern. Und das Problem bei den Sequences, die von einigen Anwendungen gerne als eindeutige IDs verwendet werden, ist, dass – mit und ohne Replikation – eine ununterbrochene Zahlenfolge mit Sequences nicht garantiert werden kann. Ein einfacher Rollback einer Transaktion erzeugt bereits eine Lücke. Trotz dieses Umstands verlassen sich viele Anwendungen für die Nummerierung von Rechnungen auf Sequences beziehungsweise den Primary-Key, der zwar garantiert eindeutig ist, aber nicht garantiert fortlaufend. Bei einem Failover kann es hier zu Diskrepanzen kommen.

Ein weiteres unbedingt zu vermeidendes Problem betrifft Konflikte, die entstehen können, wenn Constraints auf der Replikationsseite verhindern, dass Daten von der Primärseite eingefügt werden können. Dieses Problem kann aber nur auftreten, wenn Änderungen von Dritten in der Replikationsdatenbank vorgenommen wurden. Hierfür müssen Sie einen entsprechenden Zugriffsschutz gewährleisten. Die letzte große Herausforderung liegt darin, die Komplexität so niedrig wie möglich zu halten und ein praktikables

System zu entwickeln, das nicht nur die Anforderungen erfüllt, sondern auch beherrschbar bleibt. Und bei allen Überlegungen rund um eine Hochverfügbarkeit dürfen Sie natürlich menschliches Versagen nicht außer Acht lassen und müssen für diesen Fall auch hier eine belastbare Backup-Strategie umsetzen.

Replikation ist ein Projekt

Schnell eine funktionierende Replikation einzurichten, wird funktionieren – in der Regel allerdings nicht sehr lange. Als Zeitraum für ein solches Projekt sollten Sie inklusive Evaluation und Testen mindestens sechs Monate bis Inbetriebnahme einplanen. Nachfolgend beschreiben wir ein Projekt, in dem – zusammen mit einer Hardwaremigration – von einer ehemals Oracle Enterprise-Edition 11g mit Data Guard-Umgebung auf eine Oracle Standard-Edition One 11g mit Dbvisit Replicate migriert wurde.

Somit waren für die verantwortlichen Datenbankadministratoren und Entwickler gleich mehrere Probleme zu bewältigen. Dieser Umbau erfolgte, um aus veralteter Hardware mit auslaufendem Support, wenig Leistung und hohen Lizenzkosten eine neue Umgebung mit leistungsfähiger Hardware, erheblich geringeren Lizenzkosten und verbessertem Backup-Konzept zu machen. Wir beschränken uns im Folgenden auf Einrichtung, Probleme und Lösungen im Zusammenhang mit der Hochverfügbarkeitsumgebung. Auf Seiten der Datenbank umfasst die Datenmenge mehrere 100 GByte, mit Zugriffen von internen und externen Mitarbeitern aus verteilten Standorten neben Deutschland aus Süd-, West- und Osteuropa.

Realisiert wurde die Lösung mit einem Windows Server 2008 R2, der über 64 GByte RAM mit zwei Octa-Core-Prozessoren und SAS-Festplatten mit 6 GBit/s Übertragungsrate verfügt. Für die Hochverfügbarkeitsumgebung wurde der Server entsprechend ein zweites Mal in einem weiteren Rechenzentrum aufgebaut. Ziel war es, mit diesen Voraussetzungen eine HA-Umgebung zu schaffen, die den geringsten Datenverlust gewährleistet. Wie bereits beschrieben, sind die Möglichkeiten mit einer Physical Standby-Datenbank dabei auf einen gewissen Zeitfaktor beschränkt. Daher kam eine logische Replikation zum Einsatz und wir wählten dafür Dbvisit Replicate als Drittanbieter-Produkt aus.

Replikation konfigurieren

Bevor die Replikation beginnen kann, muss sichergestellt sein, dass auf beiden Seiten die gleiche Datenbank-Struktur und -Inhalte bereitstehen. Da wir mit einer bereits gewachsenen Datenbank arbeiten, setzen wir dies am besten mit einem RMAN Duplicate um. Nach der Software-Installation auf der Standby-Seite klonen wir die Datenbank einfach 1-zu-1 mit Hilfe von Bordmitteln. Damit haben wir Konflikte, die beispielsweise durch ein manuelles Aufsetzen der Datenbank und deren Strukturen sowie ein manuelles Laden der Daten entstehen können, vermieden. RMAN macht es uns an dieser Stelle recht einfach: Nach dem Erstellen und Mounten einer Instanz auf der Standby-Seite müssen wir lediglich ein DUPLICATE absetzen:

```
RMAN> DUPLICATE TARGET DATABASE TO
  'prod' FROM ACTIVE DATABASE NO-
  FILENAMECHECK;
```

Nach dem vollständigen Klonen der Datenbank beginnen wir mit der Installation und Einrichtung von Dbvisit Replicate, indem wir es auf beide Seiten aufspielen. Danach verläuft die Konfiguration der Replikation in vier Schritten. Dabei erfolgt die Verwaltung und das Logging der Replikation über ein Schema, das jeweils auf beiden Seiten für Dbvisit angelegt wird. Die Replikation selbst kann sowohl in eine Richtung als auch bidirektional erfolgen. Wobei für uns, zur absoluten Konfliktvermeidung, nur die Replikation von Primary in Richtung Standby in Frage kommt. Wir können genau festgelegen, welche Tabellen und/oder Schemas wir replizieren. Schließlich konfigurieren wir einen "MINE Process" auf der Primary- und ein "APPLY Process" auf der Standby-Seite. Nach dem Start der vorkonfigurierten Services läuft die Replikation bereits. Dazu generiert Dbvisit aus den Redo-Logs der Datenbank sogenannte PLOGs auf der Primary-Seite, schiebt diese über das Netzwerk auf die Standby-Seite und appliziert diese auf die Standby-Datenbank.

Anpassungen erforderlich

Wie bereits beschrieben, müssen wir zu typischen Problemen einer Replikationslösung auch für diese Umgebung individuelle Lösungen finden. Alle nachfolgenden Aussagen beziehen sich ausschließlich auf eine Replikation mit Dbvisit Replicate und können sich von anderen Werkzeugen unterscheiden. Dabei müssen wir beachten, dass es sich bei der replizierten Datenbank um eine eigenständige Datenbank handelt. Eigenständig heißt zunächst, dass SYS- und SYSTEM-Objekte nicht repliziert werden. Dies bedeutet weiter, dass hier ein entsprechendes Monitoring stattfinden muss. Noch entscheidender ist, dass dadurch nicht jedes DDL unterstützt wird und somit beispielsweise das Anlegen eines neuen Tablespaces nicht auf beiden Seiten automatisch erfolgt.

In unserem aktuellen Setup repliziert Dbvisit grundsätzlich keine Trigger, Constraints, Sequences, ALTER DATABASE- und ALTER SYSTEM-Kommandos oder Datenbankstrukturen. Hierfür schaffen wir einen entsprechenden Ablauf im Betrieb, der dafür sorgt, dass derartige Änderungen auf beiden Seiten angewendet und auf Konformität hin überprüft werden. Ein weiteres Problem stellen spezielle Datentypen dar, die Dbvisit Replicate nicht unterstützt und daher – sofern genutzt – anderweitig auf die replizierte Datenbank gebracht werden müssen. In diesem Projekt betraf das den XMLTYPE. Mit Hilfe von TOAD und einem DB Compare ließen sich Unterschiede an dieser Stelle am schnellsten aufdecken und je nach Bedarf auf die andere Seite anwenden.

Da unsere Entwickler häufig Trigger nutzen, trat bereits bei den ersten Tests das Problem auf, dass diese nun auf beiden Seiten feuerten. Zu diesem Zeitpunkt des Replikations-Setups wurden Trigger-Kommandos noch repliziert. Das bedeutet, dass ein durch einen Trigger ausgelöstes DML-Kommando auf der Primärseite einmal durch die Replikation eingetragen wird und der Trigger selbst durch die Replikation ein zweites Mal auf der Standby-Seite ausgeführt wird. Durch den doppelten Eintrag beziehungsweise den Versuch, diesen durchzuführen, entsteht sofort ein Konflikt und die Replikation steht still, weil sie so-

lange einen "retry" durchführt, bis der Konflikt aufgelöst ist. Dbvisit bietet dazu einen "Conflict Handler", der uns generell zwei Möglichkeiten gibt: den Konflikt ignorieren und das Statement zurückrollen oder einen Overwrite und die Zieldaten unter Missachtung der WHERE-Klausel einfach überschreiben. Keine der Methoden verschafft die Gewissheit, dass wir am Ende eine Datenkonsistenz erreichen und sicher sein können, dass auf beiden Seiten der gleiche Inhalt geschrieben wurde. Was für eine Test-Umgebung vielleicht tolerabel ist, muss für die Sicherung einer Produktionsdatenbank ausgeschlossen werden. An dieser Stelle wird also nochmal deutlich, warum wir keinerlei Konflikte tolerieren können. Die Lösung für das Trigger-Problem ist dann auch denkbar einfach. Da wir vollständigen Zugriff auf das Replikat haben, müssen wir vor Beginn der Replikation alle Trigger ausschalten.

```
SQL> ALTER TABLE table_name DISABLE
  ALL TRIGGERS;
```

Die letzte Herausforderung, der wir uns stellen müssen, ist das Umschalten bei einem Ausfall. Den Hauptzweck unserer Hochverfügbarkeitsumgebung – den geringstmöglichen Datenverlust – haben wir durch die Replikation realisiert. Das genügt aber nicht, denn das Replikat sollte im Zweifel als Produktiv-Umgebung nutzbar sein. Die Hürde, die genommen werden muss, heißt also Switchover und Failover. Als erste Maßnahme, um die Replikation vor ungewollten Zugriffen zu schützen, legen wir auf beiden Seiten einen gleichnamigen dynamischen Datenbank-Service an, den wir über das "DBMS_SERVICES Package" steuern. Damit wird der Zugriff der Anwender-PCs ausschließlich über diesen Service realisiert, den wir jederzeit starten und stoppen können.

Auf Seiten der Clients sind beide Server eingetragen und eine Anmeldung kann nur auf der Produktionsseite erfolgen, auf der der Service gestartet wird. Im Falle eines Ausfalls der Produktion geben wir dann den Service auf der Replikationsseite frei, wenn wir sichergestellt haben, dass hier alle produktionsrelevanten Daten bereitstehen:

```
SQL> EXEC DBMS_SERVICE.START_SER-
  VICE('PRODUSER');
```

Es gibt noch ein weiteres Problem, das die Replikation verursacht: Da Sequences nicht repliziert werden, müssen wir diese vor dem Freischalten für die Produktion an den aktuell höchsten Wert anpassen. Zur Sicherheit empfiehlt es sich, den höchsten Wert zu ermitteln und noch beispielsweise 100 zu addieren, um ganz sicherzugehen, dass keine Konflikte entstehen. Dieser Umstand lässt oft Diskussionen aufkommen, die in Richtung Buchhaltung und Finanzamt führen, die für Rechnungen unbedingt eine fortlaufende Nummer einfordern.

Die Ursache für das Problem sind Sequences, die nicht unter allen Umständen eine fortlaufende Nummerierung garantieren. Ein einfacher Test mit einem Rollback zeigt, dass eine einmal verwendete Sequence weg ist und sofort eine Lücke verursacht. Die Aufgabe für die Entwickler ist an dieser Stelle also, einen anderen Weg zu finden, denn eine Sequence ist nicht das geeignete Mittel, eine fortlaufende Nummerierung zu garantieren. Im Internet finden sich hierzu – abhängig vom erzeugten Overhead – gute und weniger gute Alternativen.

Live-Schaltung

Es folgte die Live-Schaltung der Replikation. Diese lief am Anfang sauber durch, doch leider stellten wir fest, dass erst mit laufender Produktion und über eine längere Zeitspanne nach und nach weitere Probleme auftraten. Das betrifft kleinere Bugs unter Windows und ein größeres Problem im Zusammenhang mit CLOBs, die nicht sauer repliziert wurden. Zusammen mit dem Support mussten wir diese Schritt für Schritt abarbeiten. Da in dieser Zeit natürlich die Bereitstellung der Hochverfügbarkeitsumgebung nicht gewährleistet war, entschlossen wir uns parallel eine Standby-Datenbank mit Dbvisit Standby aufzubauen. Sowohl aus Performancegesichtspunkten als auch lizenztechnisch war dies kein Problem. Dbvisit stellte uns die Standby-Lizenz kostenfrei zur Verfügung, solange die Probleme der Replikation nicht gelöst waren.

Alles in allem müssen für den regelmäßigen Betrieb, einen möglichen Switchover und auch für den Failover eine Reihe von Checks und Abläufe geschaffen werden, um eine reibungslose Replikation und eine sichere Hochverfügbarkeitsumgebung zu gewährleisten. Schwierigkeiten, Komplexität und Einschränkungen führten in diesem Projekt am Ende zu einer unerwarteten Lösung. Zusammen mit Dbvisit Standby fuhren wir am Ende sozusagen eine Doppelstrategie und machten uns die Vorteile beider Lösungen zunutze. Mit Dbvisit Standby umgingen wir alle Einschränkungen bezüglich nicht replizierter DDLs, SYS- und SYSTEM-Schemas sowie Datentypen. Mit der Replikation konnten wir Verluste der eigentlichen Produktionsdaten so gering wie möglich halten.

Ein weiterer Vorteil ergibt sich aus der einfacheren Handhabung von Dbvisit Standby im Falle eines Switchovers. Die Replikation wird solange einfach ausgesetzt. Bei einem Failover, also einem Totalausfall des Primary-Servers, lässt sich nun die Standby-Datenbank aktivieren und im Zweifel lassen sich mit einem DB Compare verloren gegangene Daten, die per Replikation noch die andere Seite erreicht haben, einspielen.

Fazit

Eignet sich also eine logische Replikation dazu, eine Hochverfügbarkeitsumgebung zu realisieren? Leider lautet die unbefriedigende Antwort: Es kommt darauf an. Eine Standby-Datenbank bietet den Vorteil der engen Integration in die Datenbankarchitektur, ist dagegen statisch, aber sehr robust, wenn sie richtig aufgesetzt wird. Im vorliegenden Fall sehen wir, dass eine Reihe von Problemen und eine in all ihren Möglichkeiten genutzte Oracle-Datenbank in der Standard-Edition die logische Replikation an ihre Grenzen bringt. Je komplexer die genutzte Datenbankstruktur, desto weniger empfiehlt es sich, allein auf die logische Replikation zu setzen. Kommen noch Wünsche wie ein bedienungsfreundlicher Switchover hinzu, muss sich der IT-Verantwortliche zwangsläufig für die einfachere Standby-Lösung mit Zeitversatz entscheiden oder Mehrkosten in Richtung Enterprise-Edition und Data Guard (oder anderen Produkten) in Kauf nehmen. *(jp)*

Workshopserie: Azure Active Directory einrichten und nutzen (2)

Gewusst wer

von Florian Frommherz

Mit dem Azure Active Directory bietet Microsoft seinen Verzeichnisdienst auch in der Cloud an. Im ersten Teil unserer Workshopserie haben wir die Grundlagenarbeit geleistet und die Verzeichnis-Infrastruktur mit Azure Active Directory Sync und ADFS aufgesetzt. Im zweiten Teil der Artikelreihe konfigurieren wir das Azure AD und nutzen es, um Single Sign-On über Microsofts Dienste hinaus zu Dropbox und Twitter zu ermöglichen.

Quelle: photomak – 123RF

Eine Anmeldung an den Active Directory Federation Services (ADFS) und damit an Azure AD soll in unserem Workshop für den Nutzer genügen, um alle Online-Dienste erreichen zu können. Dabei steht natürlich die Steuerung des Zugriffs auf die Cloud-Dienste über Gruppen im Mittelpunkt. Gelingt der Zugriff auf externe Online-Dienste, schauen wir uns die Sicherheitsberichte in Azure genauer an und wollen mehr über mögliche Gefahren wissen – eine Funktion, die Azure AD in der Premium-Variante anbietet. Für administrative Benutzer richten wir im Anschluss dann eine weitere Authentifizierung ein und nutzen dazu die Azure Multifaktor-Authentifizierung.

Gruppen in Azure AD bilden

Für das Erteilen von Zugriffsrechten und die Steuerung der Berechtigungen auf Anwendungen bedient sich Azure AD eines bekannten und erprobten Mittels: Gruppen. Während das Windows Active Directory generell zwischen Sicherheits- und Distributionsgruppen unterscheidet und diese weiter in verschiedene Gültigkeitsbereiche für lokale, globale und domänenlokale Zwecke unterteilt, existieren in Azure AD einfach nur Gruppen. Liegen die Sicherheitsgruppen im Bereich der Azure AD-Synchronisierung, werden diese inklusive der Gruppenmitgliedschaft nach Azure AD synchronisiert. Die Gruppenmitgliedschaft umfasst dabei alle Windows AD-Benutzeraccounts und weiter verschachtelte Gruppen – sofern die Mitglieder ebenfalls im Scope der Synchronisation liegen.

Wie auch bei Benutzerkonten unterscheidet Azure AD zwischen Gruppen, die im lokalen AD erstellt wurden, und Cloud-basierten Gruppen. Es gelten sogar dieselben Regeln: Gruppen aus dem lokalen Windows AD können nur durch die Synchronisation aus dem Windows AD heraus geändert werden. Cloud-basierte Gruppen hingegen lassen sich durch das Azure Management-Portal und das Office 365-Portal verwalten. Im Office-Portal gibt es vom Dashboard aus im linken Menü die Option "Groups", die zur Übersicht der bekannten Gruppen führt. Im Azure-Portal navigieren Sie zuerst zu "Active Directory" im linken Menü, wählen das richtige Verzeichnis aus und nutzen im oberen Menü "Groups". Das Azure Management-Portal ist für Modifikationen von Gruppen derzeit die geeignetere Variante: Die Benutzeroberfläche zeigt deutlicher, welche Gruppen geändert werden können und woher sie stammen.

Die Gruppen werden später für den Zugriff auf freigegebene und föderierte Anwendungen im Azure AD genutzt. Wir wollen typischerweise Anwendungen nicht für einzelne Benutzer freigeben, sondern für Gruppen, und steuern so über die Mitgliedschaften den eigentlichen Zugriff. Abhängig von der Unternehmensstrategie und der Existenz eines Identity Management-Systems sollten Sie sich überlegen, ob Sie die Verwaltung des App-Zugriffs in Azure AD-Gruppen oder Windows AD-Gruppen abbilden. Im Verlauf des Workshops nutzen wir eigens erstellte Cloud-Gruppen. Die Szenarien lassen sich gleichermaßen mit Gruppen aus dem lokalen Windows AD realisieren – der Unterschied liegt in der Synchronisation: Die Änderungen müssen dann im Windows AD stattfinden und durch AADSync in die Cloud getragen werden, was einige Zeit dauern kann.

SaaS-Angebote einrichten

Microsoft versucht, das Einrichten der Föderierung mit Cloud-Software aus dem Azure AD heraus so einfach wie möglich zu gestalten. Bislang mussten Angebote wie etwa Salesforce.com mit der lokalen ADFS-Infrastruktur föderiert werden, um ein Single Sign-On (SSO) für Benutzer zu ermöglichen. Die lokale Föderierung verlangte, dass eine manuelle Synchronisation von Benutzer-Accountdaten zu Salesforce.com erstellt wurde und die Zertifikate und SSO-Einstellungen manuell getätigt wurden. Salesforce wurde dabei als Relying Party in ADFS eingerichtet,

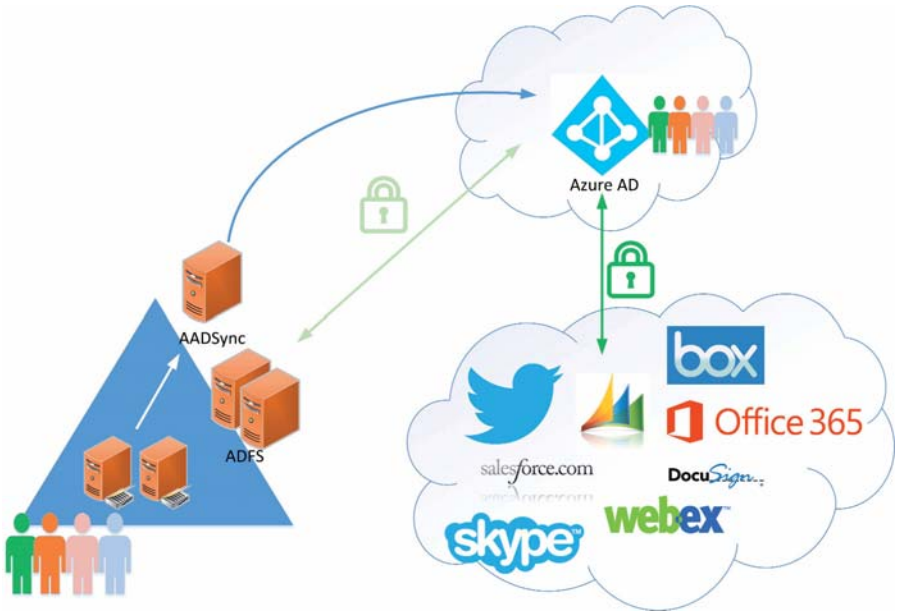


Bild 1: Azure Active Directory dient als SSO-Plattform für weitere Dienste aus der Cloud, von unterschiedlichen Herstellern.

die Konfiguration wird vom ADFS-Team überwacht und gepflegt. Diesen Teil übernimmt nun das Azure AD als Dienst. Die Föderierung wird zwischen dem Azure AD und den Online-Angeboten erstellt – die einzige Relying Party, die Sie dann noch pflegen müssen, ist die zwischen ADFS und Azure AD (in Bild 1 als hellgrüne Verbindung dargestellt).

Wir wollen für unser Beispiel den Dienst Dropbox for Business einrichten. Hierfür benötigen wir ein Dropbox for Business-Konto. Eine Probeversion für 14 Tage ist ausreichend, solange die "for Business"-Variante zum Einsatz kommt. Dropbox verlangt zwischenzeitlich die Angabe einer Kreditkarte, um die Probeversion nach Ablauf der 14 Tage zu verlängern – Sie sollten also daran denken, das Konto rechtzeitig zu löschen, sofern Sie nicht weiter mit dem Dienst arbeiten und nur testen möchten. In Dropbox for Business angekommen, vollziehen Sie im Admin-Portal die ersten Einstellungen. Unter "Authentication" schalten Sie "Enable Single Sign-On" per Klick auf die Checkbox ein. Das erlaubt Ihnen, weitere Optionen für Feineinstellungen zu wählen. Unter der Checkbox klicken Sie zunächst auf "More", um weitere Details zu Ihrem Dropbox-Abonnement zu erhalten.

Interessant ist dabei die von Dropbox zugewiesene, eindeutige Sign-On-URL für Ihr Abonnement, in unserem Beispiel *https://www.dropbox.com/sso/12018794*. Speichern Sie die URL in die Zwischenablage, bevor Sie in den weiteren Einstellungen die Option "Required" für die SSO-Einstellung für Dropbox wählen. Diese zwingt die Benutzer dazu, ein SSO durch das Azure AD zu vollziehen – es gibt keine Passwörter, die Dropbox für Ihre Benutzer speichern soll. Keine Sorge, administrative Benutzer können sich weiterhin bei Dropbox anmelden, falls das Azure AD oder ihr lokaler ADFS einmal nicht verfügbar sind.

Online-Dienst hinzufügen

Machen wir uns nun an das Erstellen des Dropbox-SSO über das Azure AD-Portal. Hierzu melden Sie sich als Global Administrator am Azure Management-Portal an. Unter "Active Directory" sehen Sie alle registrierten Verzeichnisse. Wählen Sie Ihr Verzeichnis aus und suchen Sie im oberen Menü anschließend die Option "Applications". Dort finden Sie alle registrierten Anwendungen aufgelistet. Sollten Sie das Directory für Office 365 nutzen, erscheinen dort Exchange Online und SharePoint Online als die ersten beiden Anwendungen. Per Klick auf "Add" im unteren Menü starten Sie den Assistenten für neue Anwendungen. Bestätigen Sie nun Azure AD, dass Sie fortfahren möchten mit "Add an application from the gallery".

Die Galerie kennt mehr als 2.400 Anwendungen, die in verschiedenen Kategorien zusammengefasst sind. Im rechten oberen Suchfeld tippen Sie "Dropbox" als Suchbegriff ein, wonach Sie "Dropbox for Business" vorgeschlagen bekommen. Ein Klick auf den Bestätigungsbutton erstellt das Grundgerüst für die Föderierung in Ihrem Azure AD. Das Azure-Portal springt zur Übersichtsseite der Anwendung. Sie gelangen immer wieder zu dieser Übersicht zurück, wenn Sie im Azure Portal über "Active Directory" das richtige Verzeichnis und dann "Applications" auswählen und die gewünschte Anwendung anklicken. Die Übersicht zeigt drei Schritte, die zur Single Sign-On-Beziehung notwendig sind:

1. SSO erlauben.
2. Benutzerprovisionierung für Dropbox aktivieren.
3. Die Erlaubnis für einzelne Benutzer erteilen, Dropbox zu nutzen.

Wir klicken auf Schritt 1 (Configure single sign-on), um den Assistenten zu öffnen. Die Verbindung zwischen Dropbox und dem Azure AD kann auf drei Arten geschehen – alle als "SSO" benannt. Wählen Sie für diesen Workshop "Windows Azure AD Single Sign-On" und schreiten Sie zum nächsten Punkt des Assistenten fort. Die beiden anderen Optionen bedienen weitere Szenarien: Die zweite Option "Password Single Sign-On" erlaubt Azure AD die Speicherung von Anmeldedaten, die beim Logon eines Benutzers transparent an die Zielapplikation geschickt werden. Wir werden diese Option später mit Twitter einsetzen. Die letzte Option "Existing Single Sign-On" führt durch ein Setup für die Föderierung mit der lokalen ADFS-Farm. Während auch diese Option zu einer SSO-Beziehung zu Dropbox führt, würden wir einige Vorteile von Azure AD verlieren: die automatische User-Provisionierung in die Cloud-Anwendung, das Monitoring der Föderierungsbeziehung und Azure AD als zentrale SSO-Schnittstelle.

Die zweite Seite des Assistenten verlangt nun die Sign-On-URL von Dropbox. Hier fügen Sie die URL ein, die Sie von der Dropbox-Administrationsseite kopiert haben – Azure AD möchte die komplette URL *https://www.dropbox.com/sso/12018794*. Auf Seite 3 erhalten Sie zwei letzte, wichtige Informationen: die eigent-

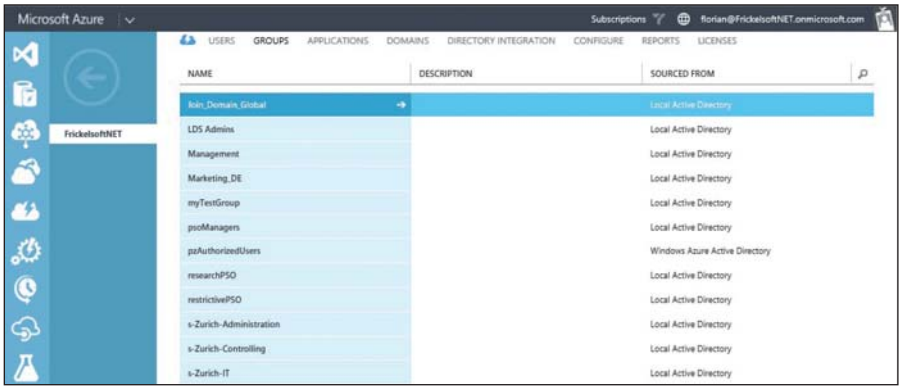


Bild 2: Gruppen in Azure AD werden manuell am besten im Azure Management Portal verwaltet.

liche Sign-In-URL für Azure AD und ein Zertifikat, mit dem die Föderierungsbeziehung erstellt wird.

Kopieren Sie nun die Sign-In-URL für Azure AD, die typischerweise mit *https://login.windows.net* beginnt, in die Zwischenablage. Anschließend laden Sie das angebotene Zertifikat herunter. Sowohl die URL als auch das Zertifikat verwenden Sie nun für die Einrichtung von Dropbox: Zurück im Dropbox-Adminportal fügen Sie die Sign-In-URL für Azure AD ein. Das Zertifikat laden Sie ebenfalls im gleichen Schritt als CER-Datei in Dropbox hoch. Damit wäre Dropbox fertig konfiguriert. Was fehlt, ist der Abschluss des Assistenten in Azure AD. Bestätigen Sie die Checkbox im dritten Schritt und beenden Sie den Assistenten. Die Checkbox weist Azure AD an, das heruntergeladene Zertifikat für Dropbox freizugeben. Sonst bliebe das Zertifikat "pending" und wird nicht freigeschaltet.

Der zweite Schritt findet unter dem Punkt "Configure user provisioning" statt. Der Assistent ermöglicht das Provisionieren von Benutzern über einen einzelnen Schritt. Die nötige Erlaubnis, Benutzer erstellen, modifizieren und löschen zu dürfen, erteilen Sie Azure AD dabei in Dropbox. Mit einem Klick auf "Enable user provisioning" öffnet sich ein neues Dropbox-Fenster, das um die Autorisierung von Azure AD bittet. Sind Sie mittlerweile nicht mehr bei Dropbox eingeloggt, werden Sie erneut aufgefordert, sich anzumelden.

Der dritte Schritt heißt "Assign users": Der Button wechselt auf die "Users and Groups"-Übersicht für die Anwendung. Von hier aus werden die Benutzer und gegebenenfalls Gruppen für die Anwendung aktiviert. Abgesehen von einzelnen Testbenutzern sollten Sie hier im Zuge der Übersicht nur Gruppen gestatten, die Anwendung zu benutzen.

Hier unterscheidet sich die Ansicht in Azure Active Directory Premium von der normalen Ansicht: Haben Sie Azure AD Premium lizenziert (selbst als Trial), zeigt die Übersicht eine Filtermöglichkeit für Benutzer und Gruppen an. Sie können Benutzer und Gruppen auswählen und sie der Anwendung zuweisen. Ohne Azure AD Premium sind es nur Benutzer. Sehen Sie trotz Azure AD Premium nur Benutzer in der Übersicht, müssen Sie Ihrem Administrator eine Premium-Lizenz zuweisen: Im "Active Directory"-Teil des Azure-Portals wählen Sie Ihr Verzeichnis aus und wechseln zu "Licenses" im oberen Menü. In der Lizenzübersicht können Sie per "Assign" eine neue Lizenz zuweisen. Haben Sie besonders viele Benutzer im Verzeichnis, wählen Sie den Suchfilter an der rechten, oberen Ecke der Tabelle an, indem Sie auf das Lupensymbol klicken.

SSO testen

Azure AD provisioniert in zyklischen Abständen neue Benutzer in föderierte Anwendungen. Nach maximal 15 Minuten sollten die neu zugewiesenen Benutzer in Dropbox for Business erscheinen. Die Provisionierung erfolgt dabei von Azure AD aus und ist mit dem Erstellen beziehungsweise dem Löschen eines Benutzeraccounts in der jeweiligen Anwendung beendet. Sind weitere Schritte für das Erstellen der SSO-Eigenschaft erforderlich, werden diese von der SaaS-Anwendung aus gesteuert.

Provisionierte Benutzer in Dropbox for Business erhalten eine Willkommens-E-Mail, in der sie ihren Dropbox-Account aktivieren müssen, bevor SSO funktioniert. Die E-Mail beinhaltet den Namen des Unternehmens, das Dropbox-Projekt, in das der Benutzer eingeladen wird, und einen Link für die Aktivierung. Nach der Aktivierung ist Single Sign-On für die

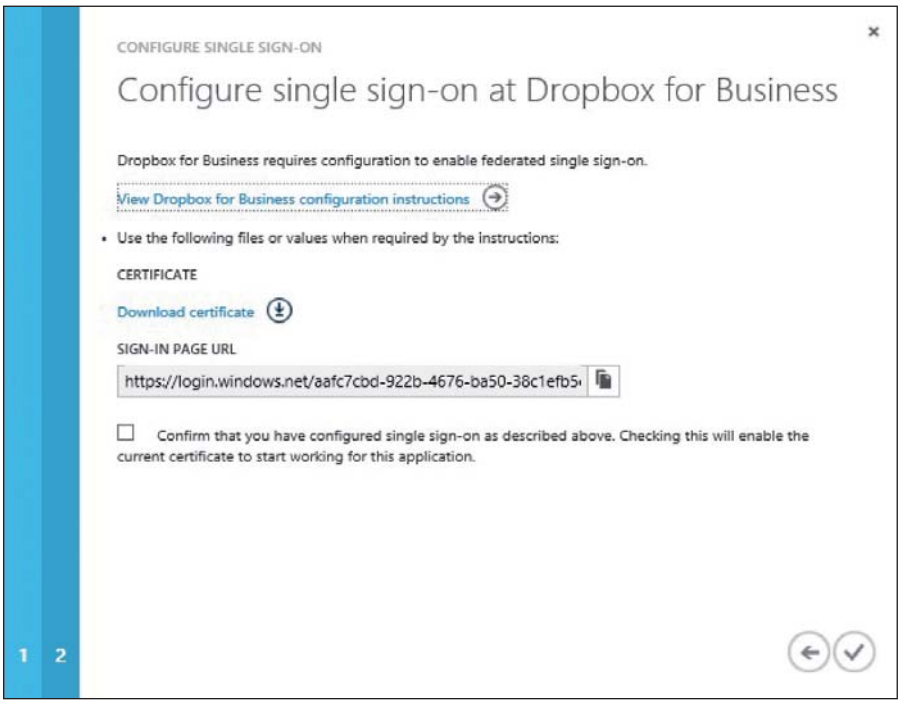


Bild 3: Für die Föderierung von Anwendungen mit Azure AD müssen die Anmelde-URLs und ein Zertifikat ausgetauscht werden.

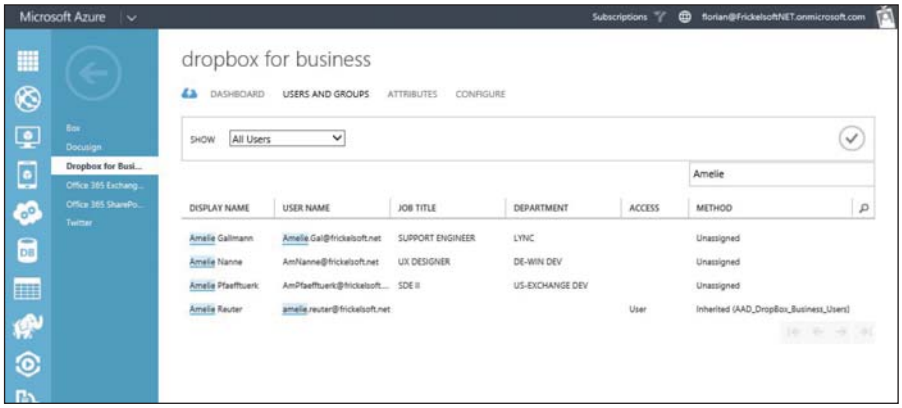


Bild 4: Zugriffe auf SaaS-Angebote werden zentral gesteuert und entweder direkt an Benutzer zugewiesen oder über die Mitgliedschaft in Zugriffsgruppen.

Benutzer möglich. Am Anmeldefenster geben sie ihren Benutzernamen ein und werden dann von ADFS authentifiziert. SSO gelingt also, ohne dass der Benutzer erneut das Passwort eingibt.

Twitter für das Unternehmen einrichten

Wir wollen mit Twitter eine weitere Webanwendung per SSO anbinden. Anders als bei Dropbox wird nicht für alle zugriffsberechtigten Mitarbeiter ein eigenes Konto erstellt; stattdessen müssen Sie mehreren Mitarbeitern Zugriff auf ein gemeinsames Twitter-Konto geben. Unser Corporate Communications-Team beispielsweise soll Zugriff auf den Twitter-Account erhalten, um Tweets für die Leser absetzen zu können. Twitter kennt allerdings kein Mehrbenutzersystem, sodass mehrere User mit unterschiedlichen Konten auf denselben Twitter-Kanal zugreifen können. Deshalb nutzen wir eine der bereits zuvor beschriebenen SSO-Varianten namens "Password Single Sign-On".

Die ersten Schritte für das Erstellen der Anwendung in Azure AD sind mit unserem Dropbox-Beispiel identisch: Anstelle von Dropbox erstellen Sie im Azure Management Portal "Twitter" als neue Anwendung für das Verzeichnis. In der Übersichtsseite wählen Sie für "Configure single sign-on" die Option "Password Single Sign-On". Damit fragt Azure AD bei der Zuweisung von Benutzern für Twitter nach, welche Anmeldedaten es nutzen soll. Die Anmeldedaten lagern gesichert in Azure AD und sind für Außenstehende nicht einsehbar – auch nicht für die Mitarbeiter. Unter "Assign users" filtern Sie nun nach der neu erstellten Gruppe "AAD_Twitter_Access". Wählen Sie die Gruppe aus und klicken Sie auf "Assign" im unteren Menü. Azure AD öffnet daraufhin einen Webdialog, in dem Sie auf "I want to enter Twitter credentials to be shared among all group members" klicken. Dann fügen Sie Benutzernamen und Passwort des Twitter-Accounts ein.

Diese Konfiguration bietet einige Vorteile: Sie können Zugriff auf den Twitter-Kanal über die Mitgliedschaft einer Sicherheitsgruppe steuern. Außerdem haben Sie das Twitter-Konto so gesichert, dass keinem Ihrer Mitarbeiter das Passwort bekannt ist. Diese loggen sich jeweils nur mit ihrem Benutzerkonto aus dem Active Directory ein. Scheidet einer der Mitarbeiter aus dem Unternehmen aus, aktualisieren Sie die Gruppenmitgliedschaft in "AAD_Twitter_Access", was den Zugriff auf das Konto ändert – ohne, dass Sie das Twitter-Konto oder das Passwort dazu ändern müssen.

Zugang über MyApps-Portal

Möchten Mitarbeiter nun auf den Twitter-Kanal zugreifen, können Sie sich nicht bei Twitter anmelden – sie kennen das Passwort für den Kanal schließlich nicht. Azure AD muss ihnen daher eine Möglichkeit bieten, den Logon transparent durchzuführen. Teil des Azure-Angebots ist das "MyApps"-Portal [1], über das Mitarbeiter die ihnen zugänglichen Anwendungen aufrufen können. Alle Anwendungen sind mit einer Grafik hinterlegt, die dann per Klick eine Weiterleitung auf die entsprechende Applikation auslöst.

Die Transparenz des Logons ermöglicht ein Plug-In für den Browser, das beim Zugriff auf die Anwendung die Logon-Daten einspeist. Für den Internet Explorer bittet Microsoft beim ersten Klick auf die Anwendung im MyApps-Portal um die Installation eines MSI-Paketes. Für Firefox reicht die Installation des Plug-Ins. Einmal aktiviert, funktioniert der Single Sign-On für alle Anwendungen mit hinterlegten, geschützten Passwörtern immer wieder.

Unter dem Tab "Profile" finden Benutzer Informationen über ihren Benutzeraccount in Azure AD. Außerdem stehen dort weitere Funktionen wie AD-Passwortänderung zur Verfügung, falls der Azure AD-Admin diese aktiviert hat.

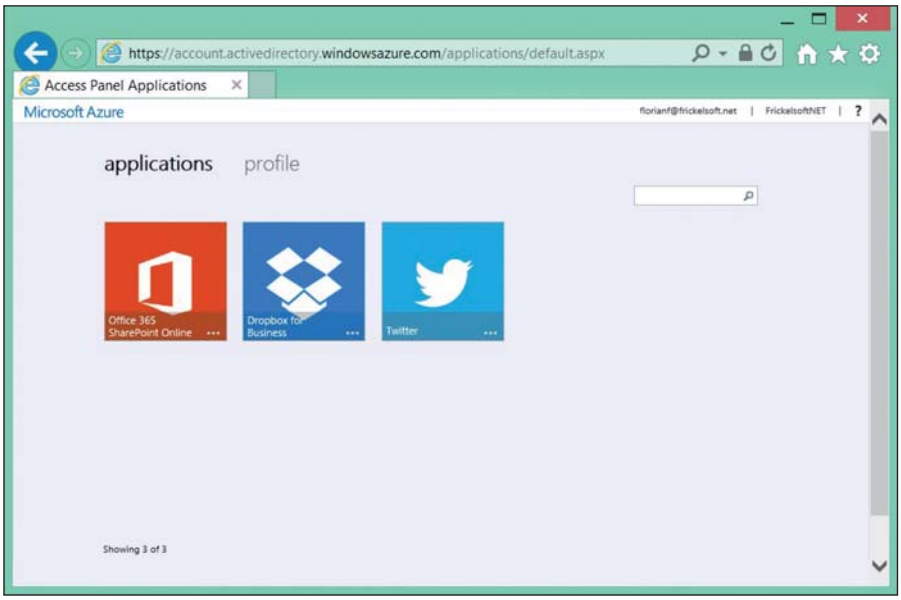


Bild 5: Das MyApps-Portal zeigt die Übersicht über die dem Benutzer freigegebenen Anwendungen – und vollzieht auf Knopfdruck den Logon transparent.

Multifaktor-Authentifizierung

Microsoft erweitert derzeit seine Online-Dienste um Multifaktor-Authentifzierung (MFA). Das erschwert nicht nur den Accountdiebstahl beim Zugriff auf Online-Ressourcen, sondern sichert auf Wunsch auch den Zugriff auf lokale Anwendungen oder auf das Firmen-VPN ab. Zwei neue Angebote sind gerade für Online-Abonennten interessant: Kunden von Office 365 können MFA für alle Benutzer aktivieren, Azure- und Azure-AD-Kunden für ihre administrativen Konten – und das gratis. Selbst wenn also die Azure AD-Premium Lizenzen knapp sind oder nur ein Office 365-Abo zur Verfügung steht, können Administrator-Accounts geschützt werden.

Das Aktivieren für Administratoren erfolgt dabei in drei Schritten: Zunächst erzwingen Sie MFA für ein administratives Konto. Sie müssen dann bei der nächsten Anmeldung Ihre Präferenzen bezüglich des zusätzlichen Faktors angeben: Telefonat, SMS oder Einmalcode durch eine App sowie eine Mobilfunknummer, unter der Azure MFA die Kontaktaufnahme versuchen soll. Anschließend ist MFA für Sie als Administrator eingeschaltet.

Die Aktivierung von MFA stellen Sie in der Benutzerübersicht des Verzeichnisses ein. Wenn Sie einen beliebigen Benutzer des Verzeichnisses auswählen, können Sie die Option "Manage Multi-Factor Auth" mit dem Vorhängeschloss-Symbol auswählen. Das Portal wechselt dann zur Konfigurationsseite für MFA. Mit Auswahl des gewünschten Benutzers erscheint die Option "Enable" unter "Quick Steps". Dort wird MFA für den Benutzer freigeschaltet. Soll MFA erzwungen werden, ist ein weiterer Klick auf "Enforce" fällig.

Erst dann wird der Benutzer bei der nächsten Anmeldung durch den Assistenten geführt. Im "Enforced"-Modus müssen Administratoren das Setup einmalig durchlaufen, bevor sie wieder auf den Dienst zurückgreifen können. Der zweite Faktor wird immer dann aufgerufen, wenn die erste Passwortabfrage und Authentifizierung durch ADFS erfolgreich war.

Das Bestätigen des zweiten Faktors geht via Telefonfunktionen wie Anruf oder SMS oder über die "Multi-Factor Auth"-App für Windows Phone, iOS und Android. Der Benutzer wählt seine favorisierte Methode aus und konfiguriert sie. Bei der Telefonvariante steht ein Anruf und SMS zur Auswahl – außerdem wird eine Mobilnummer hinterlegt. Die kostenlose App kann für ein One-Time-Password konfiguriert werden oder als Push-Nachricht, die akzeptiert werden muss. Der Unterschied: Im OTP-Fall ist nicht zwingend Empfang auf dem Mobiltelefon erforderlich, für die Push-nachricht schon.

Verdächtige Aktivitäten überprüfen

Ist der Azure AD-Administrator mit einer Premium-Lizenz ausgestattet, existiert eine Reihe von Reporting-Möglichkeiten, um auffällige oder nicht gewünschte Nutzungsverhalten des Dienstes zu berichten. Die Berichte werden in drei Kategorien veröffentlicht und sind unter "Reports" verfügbar. Besonders interessant sind die Berichte für atypische Anmeldungen am Verzeichnis. Wenn Benutzer Anmeldungen an unbekannten Geräten oder über nicht zurückverfolgbare Verbindungen vornehmen, generiert Azure AD dazu ein Audit-Ereignis.

Alle Alarmglocken sollten bei gleichzeitigen Anmeldungen aus verschiedenen Regionen schrillen: Entdeckt Azure AD, dass sich ein Benutzer aus mehreren Regionen anmeldet, obwohl die Zeit zwischen den Anmeldungen nicht ausreicht, um von der einen Region zur anderen zu reisen, wird eine Warnung generiert. Ein Benutzer kann sich nämlich nicht in München und drei Stunden später in New York anmelden. Die Reisezeit ist deutlich höher als die Zeit zwischen den Anmeldungen und würde in diesem Fall einen kompromittierten Account oder eine Mehrfachnutzung eines Benutzerkontos bedeuten.

Der Bericht "Sign Ins from possible infected devices" gleicht die IP-Adressen von Nutzergeräten mit auffälligen IP-Adressen aus dem Internet ab. Sollten sich Benutzer von Rechnern aus anmelden, die das Microsoft Security Research Center durch Beobachtungen des Internets als infiziert erkannt hat, wird dies in dem Report aufgelistet. Azure AD bezieht also Information aus unterschiedlichen Quellen mit in die Erstellung dieser Berichte ein. Natürlich können hinter diesen erkannten Anomalien auch tatsächliche, gewünschte Logons stecken, die fälschlich als verdächtig markiert wurden.

Sie können Berichte auf verschiedene Zeitbereiche fokussieren und so je nach Bericht die letzten 30 Tage genauer betrachten oder einen Zeitraum zwischen zwei Daten fixieren – um etwa zwei Monate, Juli und Dezember, miteinander vergleichen zu können. Alle Berichte besitzen im unteren Menü einen "Download"-Knopf, mit dem Sie die aufgezeichneten Aktivitäten als CSV-Datei herunterladen können. Microsoft verspricht, hier künftig noch weitere Berichte bereitzustellen.

Fazit

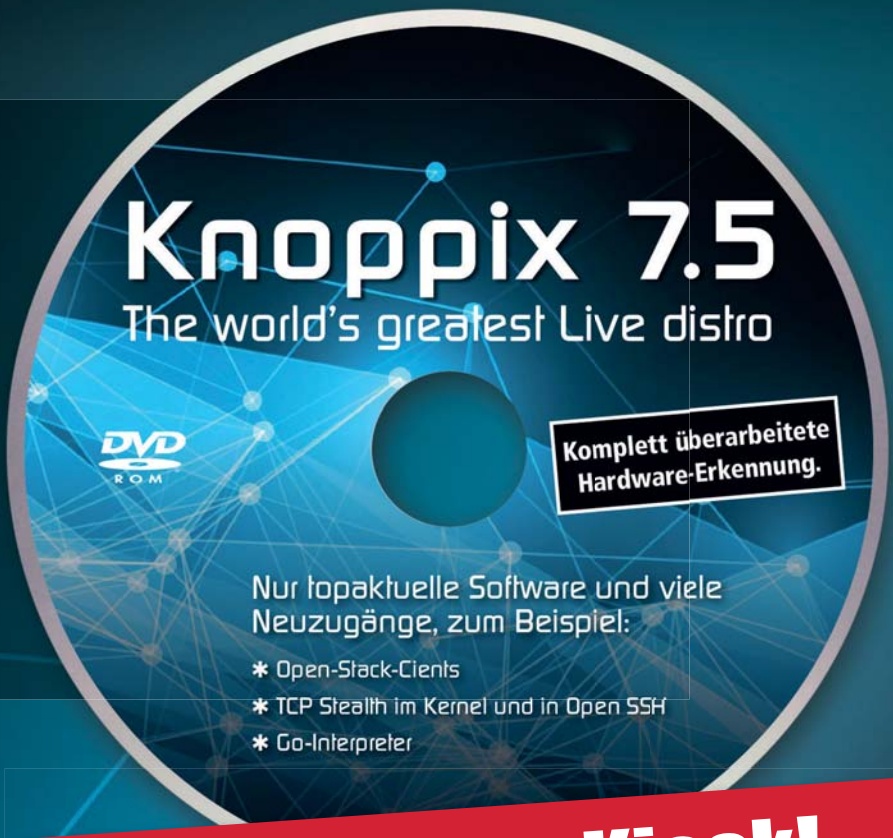
Das Azure Active Directory ist mehr als das Active Directory in der Cloud. Es wächst allmählich zum zentralen Verzeichnis für Authentifizierung mit vielen weiteren Software-as-a-Service-Angeboten heran, weit über die Microsoft-Grenzen heraus. Office 365 ist lange nicht das Ende der Fahnenstange – die Software-Galerie zeigt das sehr deutlich. Wenn Sie bei der Konfiguration der genannten Beispiele achtsam waren, haben Sie die Option für die Einbindung von selbsterstellten Anwendungen gesehen. Dort sieht Microsoft die nächste große Investition: Neu entwickelte Anwendungen werden auf Dauer nicht auf gewöhnlicher Infrastruktur laufen, sondern zunehmend für und in die Cloud hinein entwickelt. Auch dafür stehen Schnittstellen und Möglichkeiten zur Integration mit Azure AD bereit. Denn ein Vorteil bietet Azure AD gegenüber dem lokalen AD: Es skaliert deutlich besser und ist von überall erreichbar. Die Grundsteine für weitere Funktionen und einen flexiblen Umgang mit potenziell weiteren Szenarien haben wir in diesen beiden Workshopteilen gesetzt. *(dr)* IT

[1] MyApps-Portal
F3P11

Link-Codes

START IN DEN LINUX-FRÜHLING:
KNOPPIX 7.5

Prof. Klaus Knopper hat exklusiv fürs Linux-Magazin 04/2015 seine Cebit-Frühjahrs-Version zusammengestellt. Im Heft beschreibt er in einem Artikel Neuigkeiten, coole Knoppix-Tricks und die Installation auf USB-Stick oder Festplatte.



Ab 5. März am Kiosk!
Oder bequem online bestellen

Bequem online bestellen: shop.linux-magazin.de

Workshopserie: Toolbox für Admins (2)

Auch eine schwere Tür braucht nur einen kleinen Schlüssel

von Thomas Joos

Quelle: Corina Rosu – 123RF

Exchange-Server halten für Administratoren täglich zahlreiche Aufgaben bereit. Dazu zählen unter anderem das Monitoring der Exchange-Organisation, die Spambekämpfung, die Verwaltung mobiler Devices und auch die Rechteverwaltung. Dabei stellt Exchange für einige dieser Tätigkeiten nur unzureichende oder unkomfortable Bordmittel bereit, die die Administration wie eine schwere Tür unnötig blockieren. Gut, wenn der Admin einen Bund passender Schlüssel in Form von kostenlosen Drittanbietertools bereithält. Der zweite Teil unserer Workshopserie aus dem kommenden IT-Administrator Sonderheft "Die große Admin-Toolbox" stellt nützliche Exchange-Helfer vor.

Den Auftakt bei den wertvollen Helfern für Exchange bilden nicht klassische Tools, sondern drei kostenlose PowerShell-Skripte. Diese mächtigen Werkzeuge zeigen dergestalt auch die zunehmende Bedeutung der Microsoft-eigenen Skriptumgebung für die Verwaltung der Kommunikationsinfrastruktur.

Monitoring mit PowerShell-Skripten

Der Vorteil der Skripte ist die schnelle, installationsfreie Integration: Sie passen lediglich die Skripte an Ihr Netzwerk an, erstellen eine geplante Aufgabe und lassen die Skripte arbeiten. Alle drei Skripte erstellen grafische Berichte und informieren Sie über Probleme.

Die beiden bekannteren Skripte sind "Exchange Reporter" [1] und "Exchange Monitor" [2]. Beide Tools sind vom gleichen Entwickler und stehen kostenlos zur Verfügung. Es gibt Versionen für Exchange Server 2010 und für Exchange Server 2013 SP1.

Exchange Reporter verschickt Status-E-Mails über den Zustand Ihrer Exchange-Server, Datenbanken und anderer Objekte in der Exchange-Organisation. Nachdem Sie sich die passende Version für Ihren Exchange-Server (2010 oder 2013) heruntergeladen haben, müssen Sie das Skript zunächst an Ihre Umgebung anpassen. Danach erstellen Sie eine Windows-Aufgabe, die den Bericht startet.

Exchange Monitor ist das zweite Skript des Entwicklers. Dieses sendet Test-E-Mails zu einem externen Server, wartet auf die automatische Antwort und stellt damit sicher, dass der E-Mail-Fluss der Exchange-Organisation in das Internet funktioniert. Sie können auch hier das Skript anpassen und wie beim Exchange-Reporter gibt es auch für dieses Tool eine umfangreiche Hilfedatei. Klappt der E-Mail-Fluss nicht, kann das Tool Administratoren benachrichtigen, zum Beispiel über eine SMS.

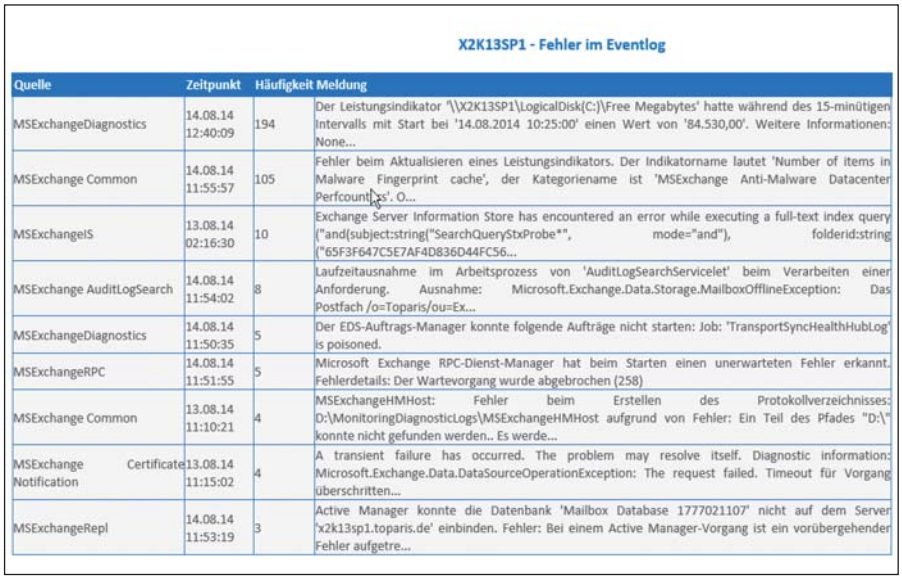
Sie können den gleichen Test auch in der Exchange-Verwaltungsshell vornehmen. Dazu verwenden Sie das Cmdlet

```
test-mailflow -SourceMailboxServer
  Postfach-Server
```

Sie erhalten auch hier das passende Ergebnis und können feststellen, ob der E-Mail-Fluss auf dem entsprechenden Postfach-Server funktioniert. In diesem Zusammenhang sollten Sie auch die Abarbeitung der Warteschlangen auf den Transportservern überprüfen. Dies erledigen Sie in der Exchange-Verwaltungsshell über

```
Get-TransportServer | Get-Queue
```

Die einzelnen Ports auf den Servern sollten Sie auch testen. Dazu verwenden Sie das Cmdlet *test-port* und den entsprechenden Port. Vor allem die Ports 25 (Transport-Server), 135 (Clientzugriff-Server und Postfach-Server), 443 (Clientzugriff-Server), 587 (Transport-Server) müssen offen sein und kommunizieren können.



X2K13SP1 - Fehler im Eventlog

Quelle	Zeitpunkt	Häufigkeit	Meldung
MSExchangeDiagnostics	14.08.14 12:40:09	194	Der Leistungsindikator '\\X2K13SP1\LogicalDisk(C:)\Free Megabytes' hatte während des 15-minütigen Intervalls mit Start bei '14.08.2014 10:25:00' einen Wert von '84.530,00'. Weitere Informationen: None...
MSExchange Common	14.08.14 11:55:57	105	Fehler beim Aktualisieren eines Leistungsindikators. Der Indikatorname lautet 'Number of items in Malware Fingerprint cache', der Kategoriename ist 'MSExchange Anti-Malware Datacenter Perfcounters'. O...
MSExchangeIS	13.08.14 02:16:30	10	Exchange Server Information Store has encountered an error while executing a full-text index query ("and(subject:string("SearchQueryStxProbe*", mode="and"), folderid:string ("65F3F647C5E7AF4D836D44FC56...
MSExchange AuditLogSearch	14.08.14 11:54:02	8	Laufzeitausnahme im Arbeitsprozess von 'AuditLogSearchServicelet' beim Verarbeiten einer Anforderung. Ausnahme: Microsoft.Exchange.Data.Storage.MailboxOfflineException: Das Postfach /o=Toparis/ou=Ex...
MSExchangeDiagnostics	14.08.14 11:50:35	5	Der EDS-Auftrags-Manager konnte folgende Aufträge nicht starten: Job: 'TransportSyncHealthHubLog' is poisoned.
MSExchangeRPC	14.08.14 11:51:55	5	Microsoft Exchange RPC-Dienst-Manager hat beim Starten einen unerwarteten Fehler erkannt. Fehlerdetails: Der Wartevorgang wurde abgebrochen (258)
MSExchange Common	13.08.14 11:10:21	4	MSExchangeHMHost: Fehler beim Erstellen des Protokollverzeichnisses: D:\MonitoringDiagnosticLogs\MSExchangeHMHost aufgrund von Fehler: Ein Teil des Pfades "D:\" konnte nicht gefunden werden.. Es werde...
MSExchange Certificate Notification	13.08.14 11:15:02	4	A transient failure has occurred. The problem may resolve itself. Diagnostic information: Microsoft.Exchange.Data.DataSourceOperationException: The request failed. Timeout für Vorgang überschritten...
MSExchangeRepl	14.08.14 11:53:19	3	Active Manager konnte die Datenbank 'Mailbox Database 1777021107' nicht auf dem Server 'x2k13sp1.toparis.de' einbinden. Fehler: Bei einem Active Manager-Vorgang ist ein vorübergehender Fehler aufgetre...

Bild 1: Das PowerShell-Skript "Exchange Reporter" liest Informationen zur Exchange-Umgebung aus – auch Einträge der Ereignisanzeigen.

Microsoft bietet in der TechNet-Gallery ebenfalls ein kostenloses Exchange-Skript mit der Bezeichnung "Generate Exchange Environment Reports using Powershell" [3]. Dieses erstellt Informationen zu Exchange-Umgebungen und kann diese ebenfalls per E-Mail zustellen. Auch hier erhalten Sie eine grafische Auswertung.

Spam effizient blockieren

SPAMfighter [4] bietet kleinen und mittelständischen Unternehmen kostengünstigen Schutz vor unerwünschten E-Mails. Das Produkt ist schnell installiert und einfach zu verwalten. Der Hersteller bietet eine 30-Tage-Test-Version an, die Sie nach dem Testzeitraum freischalten können, ohne die Einstellungen erneut vornehmen zu müssen.

SPAMfighter unterstützt alle aktuell verfügbaren Exchange-Versionen – auch Exchange Server 2013. Nach der Installation verwalten Sie die Lösung über eine Weboberfläche, auf Wunsch auch über das Netzwerk. Sobald das Tool auf einem Server installiert ist, wird dieser automatisch vor Spam geschützt. Nach der Installation öffnet sich die Weboberfläche des Tools. Hierüber verwalten Sie den Spamschutz. Um die Funktionalität zu testen, können Sie über "Hilfe / Diagnostik" Spam-Mails versenden und Daten zur Exchange-Organisation abrufen. Im Rahmen der Installation wird auch der Dienst mit dazugehörigem Benutzernamen angelegt, dessen Anmeldedaten Sie eingeben müssen. Der Benutzer wird Mitglied der lokalen Administratorgruppe auf dem Exchange-Server.

Es ist keine großartige Einarbeitung notwendig, um mit dem Produkt zu arbeiten. Daher eignet sich SPAMfighter auch für kleine Unternehmen, die auf SBS 2011 oder älter setzen.

Active Sync-Troubleshooting

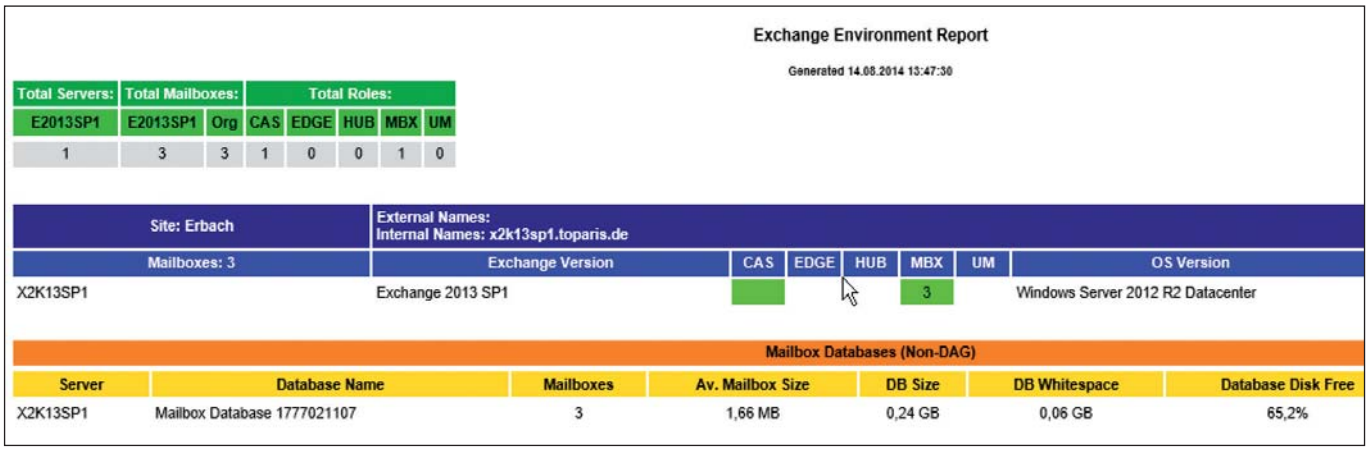
Immer, wenn neue Updates für Smartphones veröffentlicht werden, zum Beispiel neue iOS-Versionen für iPhones und iPads, kann es passieren, dass sich die Geräte nicht mehr ordnungsgemäß mit dem Exchange-Server verbinden. Mit dem kostenlosen Tool "Log Parser" lassen sich Verbindungsprobleme finden und beheben. Um Verbindungsprobleme mit ActiveSync zu lösen, helfen die beiden kostenlosen Analysetools Log Parser 2.2 [5] und Log Parser Studio [6]. Die beiden Tools lesen die Protokolldateien des Webservers (IIS) auf dem Exchange-Server aus. Vor allem iPhones haben bei neuen Versionen von iOS Probleme bei der Anbindung an Exchange.

In der Exchange-Verwaltungsshell zeigen Sie zum Beispiel mit

```
Get-ActiveSyncDevice | where
  {$_.DeviceOs -match "iOS 8.1.1 }
```

iOS-Geräte mit der Version 8.1.1 an. Treten Probleme auf Smartphones auf, nachdem Anwender diese auf eine neue Version aktualisiert haben, hilft es oft, die Synchronisierung mit Exchange neu einzurichten. Um Exchange ActiveSync zu analysieren, installieren Sie Log Parser und entpacken das Zip-Archiv von Log Parser Studio. Starten Sie Log Parser Studio und lassen die Protokolldateien auslesen.

Um ActiveSync-Probleme zu lösen, müssen beide Tools auf dem entsprechenden Server



Exchange Environment Report

Generated 14.08.2014 13:47:30

Total Servers:	Total Mailboxes:	Total Roles:					
E2013SP1	E2013SP1	Org	CAS	EDGE	HUB	MBX	UM
1	3	3	1	0	0	1	0

Site: Erbach	External Names: Internal Names: x2k13sp1.toparis.de						
Mailboxes: 3	Exchange Version	CAS	EDGE	HUB	MBX	UM	OS Version
X2K13SP1	Exchange 2013 SP1				3		Windows Server 2012 R2 Datacenter

Mailbox Databases (Non-DAG)

Server	Database Name	Mailboxes	Av. Mailbox Size	DB Size	DB Whitespace	Database Disk Free
X2K13SP1	Mailbox Database 1777021107	3	1,66 MB	0,24 GB	0,06 GB	65,2%

Bild 2: Microsoft stellt ebenfalls ein Skript bereit, das Berichte zur Exchange-Organisation in der PowerShell ausliest und als E-Mail versendet.

verfügbar sein. Anschließend erstellen Sie über "File / New / Query" im Log Parser Studio eine neue Abfrage in den IIS-Protokolldateien, die hilft, ActiveSync-Probleme zu finden. Die folgende Abfrage ist zum Beispiel geeignet, um Fehler zu finden. Der Text muss in das untere Feld der Log Parser Studio-Gui eingetragen und bereits vorhandener Text gelöscht werden:

```
SELECT
   Cs-username AS User,
   MyDeviceId AS DeviceId,
   COUNT(*) AS Hits
USING
   EXTRACT_VALUE(cs-uri-query,
   'DeviceId') AS MyDeviceId
FROM '[LOGFILEPATH]'
WHERE  cs-uri-query LIKE
  '%Error:WrongObjectTypeException%'
GROUP BY DeviceId,User
ORDER BY Hits DESC
```

Bild 3: SPAMfighter ist eine kostengünstige Lösung für den Spamschutz in kleinen Unternehmen.

Um eine Abfrage häufiger zu verwenden, können Sie diese in Log Parser Studio speichern und jederzeit abrufen. Beim Start wählen Sie die Protokolldateien des IIS aus. Die Protokolldateien können in einem beliebigen Verzeichnis abgelegt werden und befinden sich standardmäßig im Verzeichnis *\inetpub\logs\LogFiles*.

Microsoft Office 365 Best Practices Analyzer

Microsoft bietet mit "Microsoft Office 365 Best Practices Analyzer for Exchange Server 2013" [7] ein Tool an, das den aktuellen Zustand der lokalen Exchange-Organisation misst. Auch wenn der Name anderes vermuten lässt, hat das Tool im Grunde genommen überhaupt nichts mit Office 365 zu tun, es ist nur mit Exchange Server 2013 kompatibel. Die Hauptaufgabe des Werkzeugs ist es sicherzustellen, dass die lokale Exchange-Organisation mit Exchange 2013 optimal funktioniert. Unter Exchange Server 2010 verwenden Sie einfach den BPA im Bereich "Tools" der Exchange-Verwaltungskonsole. Hier benötigen Sie kein zusätzliches Tool.

Sie benötigen für den Download des Tools eine Office 365- oder Windows Azure-Anmeldung. Danach läuft das Tool auch vollständig ohne Anbindung an Office 365 oder Windows Azure. Für den Download können Sie aber auch eine Testlizenz mit Office 365 nutzen. Um den BPA für Exchange Server 2013 herunterzuladen, rufen Sie die Tools-Seite im Office 365-Portal auf und klicken auf "Ihren lokalen Exchange Server mit Office 365 Best Practices Analyzer testen".

Nach dem Download installieren Sie das Tool auf Ihrem Exchange-Server. Im ersten Schritt müssen Sie für einige Voraussetzungen des BPA die Lizenzbedingungen bestätigen. Office 365 Best Practices Analyzer for Exchange Server 2013 lädt die notwendigen Erweiterungen danach automatisch aus dem Internet und installiert sie auf dem Server:

- Microsoft Online Services Sign-in Assistant
- .NET Framework 3.5 SP1
- Windows Azure Active Directory Module for Windows PowerShell

Sind die Voraussetzungen installiert und auch der BPA auf dem Server integriert, starten Sie ihn über die Startseite in Server 2012/2012 R2. Beim ersten Start bestätigen Sie die Lizenzbedingungen.

Lassen Sie Ihre Exchange-Organisation scannen, erhalten Sie nach kurzer Zeit ein Ergebnis. Hier sehen Sie die durchgeführten Tests sowie Informationen, Warnungen und schwerwiegende Fehler in der Exchange-Organisation. Markieren Sie einen Bereich und klicken auf "View Details", zeigt der BPA das Ergebnis ausführlich an. Klicken Sie auf einen Fehler, erhalten Sie durch Auswahl von "Learn

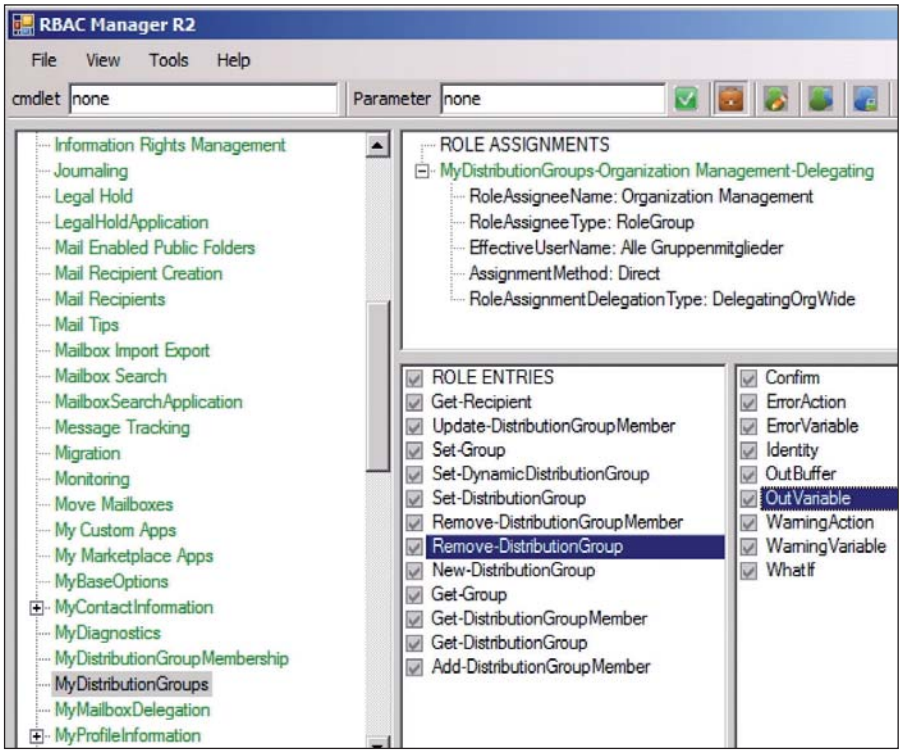


Bild 4: Die Verwaltung der Exchange-Berechtigungen mit dem RBAC-Manager macht es Administratoren einfacher, den Überblick in der Organisation zu behalten.

more" mehr Informationen. Hier öffnet sich automatisch die TechNet-Seite mit Hinweisen, wie Sie das gefundene Problem lösen können.

Klicken Sie auf "Save Scan Results", speichern Sie den Bericht als HTML-Datei ab. Starten Sie Microsoft Office 365 Best Practices Analyzer for Exchange Server 2013 nach der Installation und einem ersten Test neu, müssen Sie sich nicht erneut an Office 365 anmelden, sondern können die Organisation und die installierten Exchange-Server auch ohne die Verbindung zu Office 365 scannen lassen. Sie können bei jedem Scanvorgang selbst entscheiden, ob Sie sich an Office 365 anmelden wollen oder nicht.

Wenn Sie sich trotzdem an Office 365 im entsprechenden Fenster anmelden, dann scannt der BPA nicht nur die lokale Konfiguration Ihrer Exchange-Server, sondern auch die Office 365-Einstellungen. Brechen Sie in diesem Fall einfach die Anmeldung an Office 365 ab, um nur die lokale Exchange-Organisation zu testen. Das Tool scannt allerdings keine Einstellungen und Daten in Office 365, sondern nur die Verbindung des lokalen Exchange-Servers zu Office 365.

Rechte in Exchange einfacher verwalten

Sie verwenden normalerweise den Internet Explorer und die Adresse *https://Servername/ecp*, um auf die Exchange-Verwaltungskonsole zuzugreifen. Komfortabler wird dies mit dem RBAC-Manager [8], der die Bedienung in Windows, ohne auf einen Browser zurückgreifen zu müssen, erlaubt. Das Tool ermöglicht die Steuerung der Verwaltungsrollen, der Zuweisungsrichtlinien und der Verwaltungsrollengruppen.

Das Tool benötigt keine Installation, sondern besteht aus einer EXE-Datei und einer XML-Steuerungsdatei. Starten Sie es, läuft es im Kontext des aktuell angemeldeten Benutzers. Sind die Exchange-Verwaltungstools auf einer Arbeitsstation installiert, können Sie RBAC-Manager auch von dieser Arbeitsstation aus nutzen.

Im RBAC-Manager lassen sich Rollen anzeigen und die Rechte delegieren. Sobald das Programm gestartet ist, geben Sie den Namen des Servers ein, mit dem Sie sich verbinden wollen, sowie die Anmeldeinformationen. Anschließend verbindet sich der RBAC-Manager mit der Exchange-Organisation und verwendet die Rechte des angemeldeten Benutzers. Sie müssen dazu auf dem Server .NET Framework 3.5 installieren.

Über die Symbolleiste schalten Sie zwischen der Verwaltung von Verwaltungsrollen ("Management Roles"), Zuweisungsrichtlinien ("Assignment Policies"), Verwaltungsrollengruppen ("Role Groups") und Verwaltungsbereichen ("Management Scopes") um. Schalten Sie die Ansicht auf "Management Roles" um, lassen sich Verwaltungsrollen konfigurieren und erstellen sowie die Cmdlets festlegen, die in der Verwaltungsrolle integriert sind. Verwaltungsrollen stellen die Rechte dar, die Administratoren haben. Sie können die Einstellungen dann vollständig im RBAC-Manager durchführen und müssen nicht die webbasierte Exchange-Verwaltungskonsole verwenden.

Über "Assignment Policies" legen Sie fest, welche Verwaltungsrollen in den verschiedenen Verwaltungsrollenzuweisungen integriert sind, also welche Rechte die Benutzer haben sollen. Und mit "Role Groups" steuern Sie die Mitglieder und die Verwaltungsrollen sowie die Rollenzuweisungen. Hier lassen sich eigene Rollengruppen erstellen oder vorhandene anpassen. Über das Kontextmenü lassen sich einfach neue Mitglieder hinzufügen. Bei der Erstellung einer neuen Verwaltungsrollengruppe legen Sie im Bereich "Select Management Roles" die Verwaltungsrollen, also Rechte, fest, die Mitglieder der Verwaltungsrollengruppe erhalten sollen.

Sind in der Organisation auch Verwaltungsbereiche festgelegt, zum Beispiel für einzelne Benutzerdatenbanken, Exchange-Server oder Domänen, lassen sich die Rechte auf diese einschränken. Diese "Management Scopes" lassen sich auch im RBAC-Manager steuern. Haben Sie eine neue Rollengruppe erstellt, teilen Sie dieser über das Kontextmenü Mitglieder zu. Dazu kann RBAC-Manager natürlich auch das Active Directory durchsuchen.

Nach dem Erstellen einer Verwaltungsrollengruppe sind anschließend rechts in der Mitte im Fenster die ausgewählten Verwaltungsrollen zu sehen, oben die da-

zugehörigen Verwaltungsrollenzuweisungen und ganz rechts die Mitglieder. Erteilte Rechte lassen sich auf einzelne Bereiche einschränken. Das können zum Beispiel Domänen, Datenbanken oder einzelne Exchange-Server sein. Auch hierzu gibt es im RBAC-Manager einen eigenen Bereich.

Durchgeführte Änderungen speichert RBAC-Manager in einer Protokolldatei. Diese lässt sich über den Bereich "Tools" öffnen. In der Protokolldatei ist das PowerShell-Cmdlet zu sehen, mit dem RBAC-Manager die entsprechende Konfigurationsaufgabe durchgeführt hat. Über den Menübereich "Tools / Options" stellen Sie den standardmäßigen Exchange-Server ein, mit dem sich das Tool verbindet, den Domänencontroller und den Pfad der Protokolldatei. Normalerweise sind hier keine Änderungen notwendig, sondern nur, wenn es zu Verbindungsproblemen kommt.

Ein Beispiel: Die Verwaltungsrollengruppe "MyDistributionGroup" darf in Exchange Server 2013 nicht nur Mitglieder bestimmter Verteilergruppen hinzufügen oder entfernen, sondern auch Verteilergruppen selbst entfernen und erstellen. Solche Vorgänge wollen Administratoren aber möglichst verhindern. Es reicht oft aus, wenn bestimmte Anwender die Mitgliedschaften steuern dürfen. Welche Rechte die Benutzerrollengruppe "MyDistributionGroups" hat, sehen Sie auch in der Exchange-Verwaltungsshell, wenn Sie diesen Befehl eingeben:

```
Get-ManagementRoleEntry -Identity
  MyDistributionGroups\*
```

Die Einstellungen vorhandener Verwaltungsrollengruppen sollten Sie nicht anpassen. Besser ist es, wenn Sie eine neue Verwaltungsrollengruppe erstellen und dieser die entsprechenden Mitglieder und Rechte zuweisen. In der Exchange-Verwaltungsshell verwenden Sie für die Verwaltung von Verteilergruppen zum Beispiel den Befehl:

```
New-ManagementRole -Parent
  "MyDistributionGroups"
  -Name Contoso-MyDistributionGroups
```

Sie erstellen mit dem Befehl eine neue Gruppe und weisen dieser die Rechte der übergeordneten Gruppe hinzu.

Im RBAC-Manager klicken Sie die entsprechende Gruppe mit der rechten Maustaste an und wählen "New Role from Here". Anschließend geben Sie einen Namen ein. Sie können für die neue Gruppe Rechte anpassen, indem Sie die Haken bei den Rechten der übergeordneten Rollengruppe aus der untergeordneten Gruppe entfernen.

Sie können die Rechte dafür auch in der Exchange-Verwaltungsshell steuern. Wollen Sie zum Beispiel verhindern, dass die Anwender zukünftig Verteilergruppen anlegen und löschen dürfen, verwenden Sie die beiden Befehle:

```
Get-ManagementRoleEntry -Identity
  "Contoso-MyDistributionGroups\
  New-DistributionGroup" |
  Remove-ManagementRoleEntry
```

und

```
Get-ManagementRoleEntry -Identity
  "Contoso-MyDistributionGroups\
  Remove-DistributionGroup" |
  Remove-ManagementRoleEntry
```

Auf diesem Weg entfernen Sie auch von anderen Verwaltungsrollengruppen alle Art gewünschter Rechte.

Haben Sie die Rechte konfiguriert, können Sie in der Exchange-Systemsteuerung über die Zuweisungsrollenrichtlinie diese den Anwendern zuweisen. In Exchange Server 2013 verwenden Sie dazu die Exchange-Verwaltungskonsole und den Bereich "Berechtigungen / Benutzerrollen".

In den Eigenschaften der "Default Role Assignment Policy" weisen Sie die neu erstellte Verwaltungsrollengruppe hinzu und bestätigen die Änderung. Haben Sie eine zugewiesene Rollengruppe kopiert, entfernen Sie den Haken für die bereits zugewiesene und setzen den Haken bei der von Ihnen erstellten Richtlinie, sodass die Anwender nur die neuen Rechte erhalten.

Anschließend wird über die Richtlinie allen Anwendern, für die diese Richtlinie gilt, die Verwaltungsrollengruppe zugewiesen. Sie können für den Vorgang aber auch den RBAC-Manager verwenden. Dazu klicken Sie auf die Schaltfläche "Show Assignment Policies", wählen die "Default Role Assignment Policy" aus und weisen die von Ihnen erstellte Verwaltungsrollengruppe zu. Durch die Zuweisung an die Richtlinie werden allen Benutzern, denen diese Richtlinie zugewiesen ist, die Rechte erteilt, die Sie der Verwaltungsrollengruppe zugewiesen haben.

Welche Richtlinie einem Benutzer zugewiesen ist, sehen Sie in den Einstellungen des Postfachs. In Exchange Server 2013 finden Sie die Einstellung über "Empfänger" und dann über das Menü "Postfachfunktionen".

Fazit

Schwere Türen in Exchange lassen sich erfreulicherweise in vielen Fällen mit kleinen Schlüsseln – kostenlosen Tools – öffnen. Die vorgestellten Werkzeuge erleichtern in vielen Fällen die Administration und sparen so wertvolle Zeit. Die komplette Sammlung an Türöffnern für Exchange, Windows-Server und -Client sowie VMware und mehr finden Sie im kommenden IT-Administrator Sonderheft "Die große Admin-Toolbox". *(jp)*

Link-Codes

[1] Exchange Reporter
Für Exchange Server 2013: F3P21
Für Exchange 2010: F3P22

[2] Exchange Monitor
F3P23

[3] Generate Exchange Environment Reports using Powershell
F3P24

[4] SPAMfighter
F3P25

[5] Log Parser 2.2
F3P26

[6] Log Parser Studio
D8PE3

[7] Microsoft Office 365 Best Practices Analyzer for Exchange Server 2013
F3P27

[8] RBAC-Manager
F3P28

DevOpsCon

NICHT VERPASSEN!
EARLY-BIRD-PREISE BIS 29. APRIL SICHERN!

1. – 3. JUNI 2015
nhow Berlin

RETHINK IT

Die Konferenz für Docker, Infrastruktur as Code, Continuous Delivery, Cloud und Lean Business

Das Thema DevOps verändert unsere IT-Welt. Kürzere Lieferzyklen, schnellere Wechsel der Funktionalität und mehr Qualität in den Auslieferungen erfordern ein Umdenken. Der Einsatz neuer Prozesse und der Containertechnologie, Linux-Kernel-Virtualisierung, Netzwerke, Microservices und Clouds sind eine große Herausforderung. Wir wollen mit der DevOpsCon einen Platz für aktiven Erfahrungs- und Wissensaustausch bieten. Wir sind der Überzeugung, dass jetzt der Moment gekommen ist, sich zu informieren, um die Weichen der IT in Unternehmen neu zu justieren. Erleben Sie die bekanntesten Köpfe der DevOps-Welt in einer neuen und einzigartigen Konferenz, und erhalten Sie geballtes Wissen für Ihren entscheidenden Wettbewerbsvorsprung!

www.devops-conference.de

Präsentiert von: entwickler magazin

Powered by: Business Technology, eclipse MAGAZIN, Javamagazin, PHPmagazin, windows .developer

Veranstalter: S&S Media Group

Systeme: Neuerungen in Android 5

Dauerlutscher

von Thomas Joos

Mit Android 5 "Lollipop" hat Google sein Betriebssystem für Mobilgeräte zahlreichen Änderungen unterworfen, die auch für Unternehmenskunden von Bedeutung sind. In diesem Beitrag stellen wir die Aktualisierungen vor und zeigen, wie Unternehmen von der neuen Version profitieren können.

Quelle: Maksim Shebeko – 123RF

Am auffallendsten an Android 5 ist das neue Design. Dieses setzt weniger auf dreidimensionale Effekte, ist flacher und insgesamt stärker an Google-Webdienste angeglichen. Bezüglich der Leistung ist erfreulich, dass Android 5 64 Bit-Prozessoren unterstützt. Ebenso will Google generell die Hardware-Basis erweitert sowie die Zusammenarbeit mit anderen Geräten verbessert haben.

Längere Akku-Laufzeit

Eine der wesentlichen Neuerungen ist die weitaus bessere Akku-Laufzeit von Android 5. Das Betriebssystem arbeitet mit der neuen Android RunTime (ART), die besser mit den Java-basierten Android-Apps umgehen kann als der Vorgänger Dalvik. Nach ersten Messungen lässt sich die Laufzeit um bis zu 40 Prozent erhöhen. In diesem Zusammenhang ist auch der neue Energiesparmodus interessant. Dieser lässt sich automatisiert oder manuell aktivieren, um die Laufzeit noch weiter zu erhöhen. Die Schwellenwerte können Anwender in den Einstellungen selbst festlegen.

Außerdem kann Android 5 mehr Statistiken und Informationen zum Akku-Verbrauch anzeigen. Das ist vor allem für Entwickler interessant und für Administratoren, die einen Überblick darüber erhalten wollen, welche Apps den Akku von Geräten am meisten belasten. Außerdem informiert das Betriebssystem darüber, wie lange der Akku unter den aktuellen Bedingungen voraussichtlich noch läuft. Beim Aufladen wird auf dem Lock-Screen zudem angezeigt, wie lange es noch dauern wird, bis der Akku voll aufgeladen ist.

Sicher wie Fort KNOX

Android 5 hat Funktionen von Samsung KNOX im Betriebssystem fest integriert. Über diesen Weg lassen sich private und Unternehmensdaten besser voneinander trennen – für Unternehmen mit BYOD-Ansatz eine wertvolle Neuerung. Es gibt zum Beispiel die Möglichkeit, Container zu erstellen, auf die nur der lokale Anwender Zugriff hat. Zentraler Bestandteil von KNOX in Android 5 sind außerdem MDM APIs, das KNOX-Standard-SDK, früher bekannt unter dem Namen SAFE, sowie einige Bereiche von SE for Android.

Viele KNOX-Funktionen lassen sich jedoch nicht ohne KNOX-Infrastruktur in Android 5 verwenden. Dazu gehören Hardware-abhängige Sicherheitselemente wie ARM TrustZone-basierte Integrity Management Architecture (TIMA), Trusted Boot, Client Certificate Management (CCM), TrustZone-based KeyStore, Remote Attestation, Biometric Authentication und Common Access Card Authentication. Auch Single Sign-On (SSO) und VPN Frameworks. Cloud-Dienste wie KNOX Enterprise Mobility Management und KNOX Marketplace sind nicht vollständig integriert. Zusätzliche App-Stores wie Galaxy Apps, KNOX Apps, Device Theft Recovery und KNOX Customization sind nicht direkt in Android 5.0 integriert, sondern müssen ebenso nachträglich über KNOX Enterprise eingebunden werden.

Neue Benutzerverwaltung

Schon bei Smartphones und Tablets ab Android-Version 4.2.2 gab es eine Benutzerverwaltung. Release 5.0 hat diese weiter verbessert und enger in das System integriert. Mehrere Personen können mit demselben Gerät arbeiten, wobei jeder seine eigene Umgebung erhält und sich über den Sperrbildschirm anmelden kann. Dies funktioniert jetzt ab Werk auch mit Smartphones und nicht nur mit Tablets.

Mit Android 5 will Google auch die Funktionen des Geräte-Managers im Web anpassen. Dieser soll zukünftig mehr

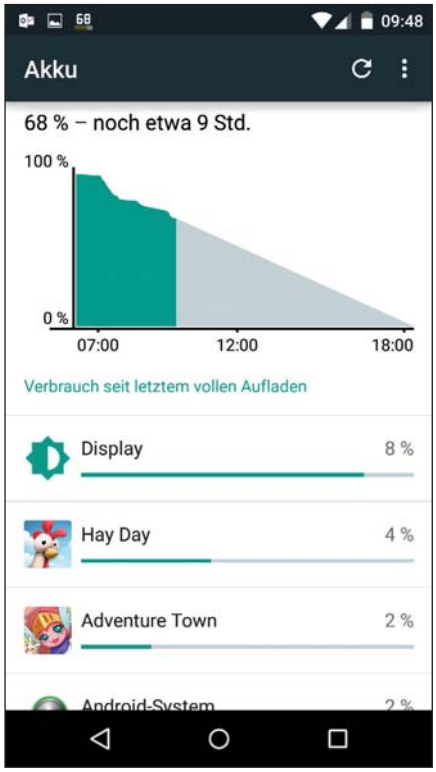


Bild 1: Über die Schnelleinstellungen finden Sie Stromfresser und die restliche Akku-Laufzeit am schnellsten.

Funktionen bieten, zum Beispiel verlorene Geräte auf den Werkszustand zurücksetzen. Das so gelöschte Gerät lässt sich erst dann wieder verwenden, wenn sich der ursprüngliche Anwender mit seinem Google-Konto anmeldet.

Sperrbildschirm mit mehr Benachrichtigungen

Benachrichtigungen von verschiedenen Apps sind in Android 5 direkt auf dem Sperrbildschirm zu sehen. Diese Liste kann das Betriebssystem nach Prioritäten sortieren. Insgesamt lassen sich die Benachrichtigungen besser anpassen und zeigen mehr Informationen. Durch das doppelte Antippen einer Benachrichtigung öffnet sich die dazugehörige App automatisch. Auf diesem Weg lassen sich zum Beispiel E-Mails oder der Kalender schnell öffnen. Sollen bestimmte Nachrichten-Arten, zum Beispiel Firmen-E-Mails, nicht auf dem Sperrbildschirm, also für alle lesbar, angezeigt werden, kann der Nutzer dies in den Settings so festlegen.

Das Konzept, Benachrichtigungen auf dem Sperrbildschirm anzuzeigen, hat aber auch Nachteile. Der Sperrbildschirm ist fest für Benachrichtigungen reserviert. Es ist also kein Platz mehr vorhanden für das Entsperr-Feld, mit dem sich das Smartphone durch eine bestimmte Geste entsperren lässt. Selbst wenn keine Benachrichtigungen vorhanden sind, sind drei Schritte nötig, um zum Home-Screen zu gelangen: An-Schalter drücken, den Lock-Bildschirm nach oben wegwischen, Wisch-Geste zum Entsperren eingeben. Umgehen lässt sich dies nur durch automatisches Entsperren, etwa in der Nähe eines anderen Geräts, eines NFC-Chips oder, nun auch ab Werk integriert, wenn sich das Telefon an bestimmten Koordinaten befindet.

Usability mit Licht und Schatten

Außerdem hat Google die Tastatur überarbeitet, die von vielen Anwendern nun allerdings als recht klein empfunden wird. Neue Wortvorschläge sollen das Schreiben von Nachrichten beschleunigen. Auch die in der Oberfläche integrierte Suchfunktion wurde aktualisiert und liefert schnellere und übersichtlichere Ergebnisse. Benötigt ein Suchergebnis eine bestimmte App, wird diese automatisch geöffnet, wenn ein Anwender das Suchergebnis antippt.

Wer den mobilen Datenverkehr einschränken will, kann Android 5 so konfigurieren, dass Apps ihre Daten nur noch über WLAN synchronisieren. Auch eine Nicht-Stören-Funktion, in Android 5 "Unterbrechungen" genannt, hat Google eingeführt. So können Anwender steuern, wann Sie keine Benachrichtigungen bei neuen Nachrichten oder Anrufen erhalten sollen. Der Modus lässt sich manuell aktivieren oder nach einem Zeitplan.

Beim Drücken des Lautstärke-Reglers lassen sich die Unterbrechungen manuell über einen Schieberegler steuern. Wer nur für im Adressbuch als wichtig markierte Kontakte erreichbar sein will, kann dies ebenfalls hier einstellen. Im gleichen Atemzug hat Google dem Nutzer allerdings die Option genommen, das Telefon rein durch das Betätigen des Lautstärke-Reglers lautlos zu schalten. Vibration ist nun die kleinste Stufe. Wer ein wirklich lautloses Handy haben möchte, muss nun zwangsläufig mit den Unterbrechungs-Einstellungen arbeiten.

Den Kalender hat Google ebenfalls überarbeitet und optisch aufgefrischt. Noch immer fehlt für die Aufgabenverwaltung eine interne App. Hier müssen Anwender weiter auf Dritt-Anbieter ausweichen, was ein echtes Manko im Vergleich zu Windows Phone 8.1 oder iOS ist.

Allerdings lässt sich Android 5 weiterhin problemlos an Exchange/Office 365 anbinden. Leider funktioniert auch in der neuesten Android-Version das AutoDiscovery noch nicht optimal. Wird der Posteingangsserver von Office 365 nicht gefunden, lässt sich das Problem allerdings lösen, wenn *outlook.office365.com* als E-Mail-Server angegeben wird. Die App zur Multi-Faktor-Authentifizierung für Office 365 unterstützt auch Android 5. Hier sollten Administratoren aber auf regelmäßige Updates prüfen.

Das Wischen von oben nach unten blendet auf dem Home-Screen die aktuellen Benachrichtigungen ein, ein nochmaliges Wischen führt zu den Schnelleinstellungen. Hier sehen Sie auch die WLAN-Verbindung und mit welchem WLAN das Gerät aktuell verbunden ist. Tippen Sie auf den Namen des WLANs, springt Android direkt in die WLAN-Konfiguration in den Einstellungen. Den Task-Manager hat Google ebenfalls überarbeitet. Er kann im neuen Karteikarten-Look nicht nur zwischen einzelnen Apps wechseln, sondern teilweise auch deren Funktionen ansteuern. Die APIs dazu hat Google zur Verfügung gestellt.

Fazit

Android 5 bringt Verbesserungen im Betrieb, bei der Sicherheit und bei der Akkulaufzeit. Selbst wenn es bei einigen Geräten in der Startphase zu Problemen kam und Google schnell auf 5.0.1 gesprungen ist, sollte es sich mittlerweile lohnen, Geräte auf die neue Version zu aktualisieren. Übrigens ist es sauberer und effizienter, Android 5 komplett neu zu installieren und nicht nur die alte Version zu aktualisieren. Zuletzt bleibt ein altbekanntes Android-Problem: Nur wenige auf dem Markt befindlichen Geräte lassen sich auf die jüngste Android-Version hochstufen – jeder Hersteller hat seinen eigenen Fahrplan. *(ln)*

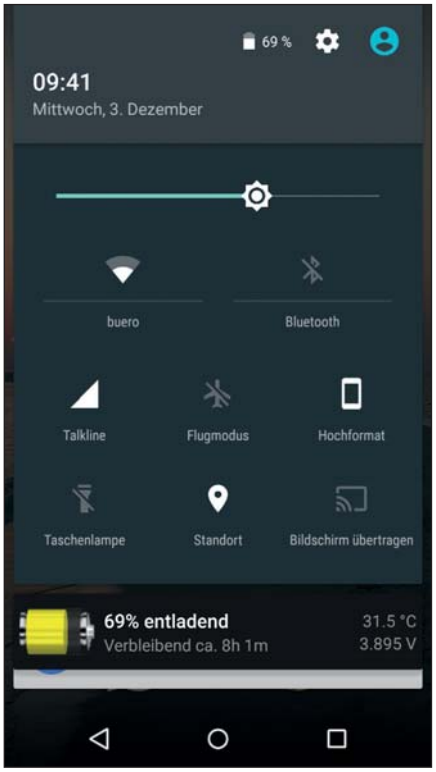


Bild 2: In den Schnelleinstellungen sind die WLAN-Verbindung ersichtlich.

Workshop: Docker-Container mit Kubernetes managen

Container-Management


Quelle: samarttiw – 123RF

von Thorsten Scherf

Wer im Virtualisierungsmarkt auf das Container-Schiff aufgesprungen ist, hat bald Bedarf nach performanten Lösungen zum Management seiner Docker-Landschaft. Diverse Hersteller bieten hierfür spezielle Betriebssystem-Images mit entsprechenden Management-Tools an. Red Hat setzt in seinem neuen Container-Betriebssystem Atomic auf Kubernetes vom Branchenriesen Google.

Die eigenen Applikationen in Containern zu betreiben, wird immer populärer und bietet im Vergleich zum Betrieb auf herkömmlichen virtuellen Maschinen zahlreiche Vorteile. Die Container basieren dabei zumeist auf der Docker-Engine, die nur einen sehr minimalistischen Unterbau zum Betrieb der Container voraussetzt. Daher stellt der Einsatz herkömmlicher Betriebssysteme zumeist einen zu großen Overhead dar, wenn bereits im Vorfeld klar ist, dass auf den betroffenen Systemen ausschließlich Container zum Einsatz kommen sollen. Zwar lassen sich diese ohne weiteres mit dem Docker-eigenen Management-Tool erzeugen, starten und stoppen, jedoch skaliert dieser Ansatz nicht sehr gut.

Gerade in großen Enterprise-Umgebungen möchte sich der IT-Verantwortliche keine Gedanken mehr darüber machen, auf welchem System ein Container läuft und welche Hardware hierfür zum Einsatz kommt. Stattdessen geht es nur noch darum, eine Applikation mit den benötigten Anforderungen zu definieren und diese dann auf den vorhandenen Ressourcen bereitzustellen. Ob die Applikation dann in einem Container auf Hardware A im Rechenzentrum X oder aber auf Hardware B im Rechenzentrum Y abläuft, spielt keine Rolle mehr. Ausnahmen bestehen natürlich, beispielsweise wenn einzelne Anwendungen in einer bestimmten geografischen Lokation bereitgestellt werden müssen. Aber eine solche Information lässt sich natürlich in den Anforderungen hinterlegen und beim Deployment entsprechend berücksichtigen.

Atomare Host-Images

Einige Linux-Distributionen bieten aus diesem Grund spezielle Betriebssystem-Images an, die auf speziell diesen Einsatzzweck zugeschnitten sind. Neben dem heute aktuellen Init-System systemd und einigen grundlegenden Kernel-Komponenten, wie beispielsweise SELinux und CGroups, enthalten diese nur einen sehr kleinen Software-Stack. Dazu gehört natürlich Docker als Container-Engine sowie oftmals Kubernetes [1] von Google als Management- und Orchestrierungs-Tool für die Container.

Ein solches Betriebssystem-Image lässt sich zumeist in unterschiedlichen Umgebungen einsetzen. So existieren Images für den Einsatz auf klassischen Bare-Metal Systemen, aber natürlich auch für den Betrieb in öffentlichen und privaten Cloud-Umgebungen. Dazu zählen beispielsweise Google Cloud Engine (GCE), Red Hat OpenShift, OpenStack, Amazon Web Services oder andere Virtualisierungsumgebungen. Wir verwenden in diesem Artikel beispielsweise eine einfache KVM-Installation.

In dieser Umgebung kommt ein Image aus dem Project Atomic [2] zum Einsatz. Dieses ist speziell für den Einsatz von Containern auf Basis von Docker und Kubernetes ausgelegt. Project Atomic stellt dabei das Upstream-Projekt für diverse andere Images dieser Art dar. So greifen beispielsweise Red Hat [3], Fedora [4] und auch CentOS [5] auf das Project Atomic zurück, um ihre jeweils eigenen Cloud-Images für den Einsatz von Docker Containern zu erzeugen.

Es ist wichtig zu verstehen, dass diese Atomic-Images einen anderen Aufbau besitzen, als man es von solchen RPM-basierten Distributionen gewohnt ist. So kommt beispielsweise kein Paket-Manager zum Verwalten der Software zum Einsatz. Stattdessen greift das Project Atomic hier auf das Tool rpm-ostree zurück. Hiermit lassen sich atomare Updates des Atomic-Hosts durchführen. Das ist deshalb möglich, da sich die komplette Betriebssystem-Instanz in einem einzelnen Dateisystem-Pfad unterhalb des Ordners */ostree/deploy* befindet.

Beim Systemstart wird die aktuelle Version des Betriebssystems dann unterhalb der Dateisystemwurzel eingehängt, wobei lediglich die Ornder */etc* und */var* beschreibbar sind. Alle anderen Ordner unterhalb von */ostree* sind lediglich lesbar.

Bei einem Update wird nun einfach eine komplett neue Betriebssystem-Instanz von dem Update-Server nach */ostree/deploy* kopiert und die Änderungen an den Konfigurationsdateien unterhalb von */etc* auf die neue Betriebssystem-Instanz angewendet. Das Verzeichnis */var* wird zwischen allen Instanzen geteilt, da sich hier beispielsweise auch das Home-Verzeichnis der Benutzer befindet. Der Ordner */home* ist lediglich ein symbolischer Link auf */var/home*. Um die neue Instanz des Betriebssystems zu starten, ist somit ein Neustart des Host-Systems notwendig. Der ganze Vorgang erinnert ein wenig an das Versionskontroll-System Git und in der Tat basiert ostree (die Basis von rpm-ostree) auf diesem Tool.

Wollen Sie zusätzliche Software auf einem Atomic-Host installieren, klappt das nicht auf die gewohnte Weise mit rpm oder yum. Stattdessen wird empfohlen, die Software entweder in einem eigenen Container auf dem Atomic-Host zu betreiben oder aber sie in einen Ordner unterhalb von */var* zu kopieren. In diesem Fall sollte es sich um statisch übersetzte Programme handeln. Sämtliche Änderungen an den einzelnen Betriebssystem-Instanzen in diesem Ordner nehmen Sie über das Tool rpm-ostree vor und nicht etwa manuell. Mittels *rpm-ostree update* führen Sie ein Update des Systems durch. Hat dieser nicht so funktioniert, wie Sie es sich vorstellen, versetzen Sie das System mittels *rpm-ostree rollback* wieder in den ursprünglichen Zustand. Anstelle von rpm-ostree können Sie auch einfach das Tool atomic aufrufen. Es verweist über einen Softlink ebenfalls auf rpm-ostree.

```
# mkdir /tmp/atomic/
# cd /tmp/atomic/

# cat > meta-data <_eof
instance-id: Atomic0
local-hostname: atomic-00
_eof

# cat > user-data <_eof
#cloud-config
password: atomic
chpasswd: {expire: False}
ssh_pwauth: True
ssh_authorized_keys:
  - ssh-rsa AAA...SDvz centos@atomic.example.com
_eof

# genisoimage  -output cloud-init-config.iso
   -volid cidata -joliet -rock user-data meta-data
```

Listing 1: Meta-Dateien zur Konfiguration

Arbeiten mit Docker-Containern

Wenn Sie mit Docker-Containern vertraut sind, wissen Sie, dass sie ebenfalls auf Images basieren. Diese beziehen Sie entweder von einem zentralen oder lokalen Docker-Registry-Server oder erzeugen Sie mit Hilfe eines Dockerfile selber. Über den Aufruf von *docker run* starten Sie dann die gewünschte Applikation innerhalb eines Containers. Das folgende Beispiel zeigt das bekannte "Hello World" innerhalb eines Fedora-Containers:

```
docker run fedora /bin/echo
  "hello world"
```

Ist das Image mit dem Namen "fedora" zu diesem Zeitpunkt noch nicht lokal vorhanden, lädt docker es selbstständig vom voreingestellten Registry-Server herunter und führt dann das Kommando */bin/echo "hello world"* innerhalb der Fedora-Instanz aus. Im Anschluss wird der Container beendet. Der Aufruf *docker ps -a* zeigt alle gestarteten Container auf dem Host an.

Anstelle des echo-Befehls könnten Sie an dieser Stelle natürlich auch ein Skript aufrufen, das einen vorkonfigurierten Webserver startet. Nutzt dieser eine Datenbank als Backend, erzeugen Sie einen zusätzlichen Container mit eben dieser Datenbank und verlinken die beiden. In kleinen Umgebungen ist dieser Ansatz sicherlich ausreichend, ab einer gewissen Größe sollte die Lösung aber besser skalieren. Beispielsweise sollte es möglich sein, einen Container oder aber auch ein Set von Containern auf entfernten Hosts zu starten. Auch ist es wünschenswert, einen Status für die Applikationen zu definieren. Starten Sie mittels docker einen Container auf einem Host, so ist nicht sichergestellt, dass im Fehlerfall des Hosts der Container auf einem anderen System wieder neu startet.

Container-Orchestrierung mit Kubernetes

Ein Management- und Orchestrierungs-Tool wie Kubernetes bietet genau solche Möglichkeiten. Das Tool besteht aus einer ganzen Reihe von Services, von denen einige auf einem Steuerungssystem, dem Master-Host, andere auf den einzelnen Docker-Hosts, den sogenannten Minions, laufen. Der app-service auf dem Master stellt eine REST-API zur Kommunikation zur Verfügung, über die der Service Anweisungen von Clients erhält. Eine Anweisung könnte beispielsweise sein, einen bestimmten Container auf einem beliebigen Minion-Host zu erzeugen, in der Kubernetes-Welt Pod genannt. Dieser kann lediglich einen einzelnen oder auch mehrere Container enthalten.

Üblicherweise enthält ein Pod Container für Dienste, die man auf herkömmlichen Systemen gerne zusammen installieren würde. Eine Datei im JSON-Format enthält alle hierfür notwendigen Informationen. Beispielsweise, welches Image für die Container des Pods zum Einsatz kommen soll und auf welchem Port die Dienste innerhalb der Container lauschen sollen. Auf den Minion-Hosts läuft ein Agent-Service mit dem Namen "kubelet" und empfängt Anweisungen des Masters.

Als Kommunikationsbus kommt der etcd-Service zum Einsatz. Hierbei handelt es sich um eine verteilte Key/Value-Datenbank [6], die mittels einfacher HTTP-GET- und PUT-Anweisungen bedient wird. Diese hält Konfigurations- und Sta-

```
kubectl get pods
NAME          IMAGE(S)        HOST                LABELS                  STATUS
apache-dev    fedora/apache   atomic-host-001/    name=apache,stage=dev   Running
```

Listing 2: Kubectl zeigt aktiven Pod

tus-Informationen des Kubernetes-Clusters vor und liefert diese bei Bedarf im JSON-Format zurück. Der kubelet-Service auf einem Minion-Host fragt diese Datenbank ständig nach Änderungen ab und führt sie gegebenenfalls aus. Beispielsweise kann die Datenbank eine Liste sämtlicher Minion-Hosts des Clusters enthalten. Diese Information wird dann vom app-service dazu verwendet, um zu entscheiden, auf welchen Hosts ein neuer Container erzeugt werden kann.

Installation des Atomic-Hosts

Um in die Welt von Kubernetes einzutauchen, laden Sie sich eines der unter [3,4,5] bereitgestellten Images herunter und installieren es in Ihrer Virtualisierungsumgebung. Wir verwenden für diesen Artikel eine lokale KVM-basierte Installation auf Fedora 21 mit einem CentOS 7 Docker-Image von [5]. Das Image lässt sich hier einfach mittels des Tools virt-manager oder virt-install installieren. Unter [7] finden Sie Setup-Anweisungen für verschiedene Virtualisierungsumgebungen.

Für den ersten Start sollten Sie der so erzeugten virtuellen Maschine eine CD-ROM in Form einer ISO-Datei zur Verfügung stellen. Diese enthält grundlegende Informationen über das virtuelle Atomic-System, beispielsweise den Maschinennamen und das Passwort für den Default-Benutzer. Auch einen SSH-Schlüssel zum Login auf das System oder die gewünschte Netzwerkkonfiguration können Sie an dieser Stelle übergeben. Legen Sie hierfür die beiden Dateien *meta-data* und *user-data* an und erzeugen Sie hieraus im Anschluss die ISO-Datei (Listing 1). Diese stellen Sie dem Atomic-Host dann als virtuelles CD-ROM-Laufwerk zur Verfügung. Beim ersten Start des Systems startet der Dienst cloud-init, liest die so zur Verfügung gestellten Informationen ein und konfiguriert anhand dieser das System. Unter [8] finden Sie weitere Informationen zum Thema cloud-init.

```
{
    "apiVersion": "v1beta1",
    "kind": "Pod",
    "id": "apache-dev",
    "namespace": "default",
    "labels": {
        "name": "apache",
        "stage": "dev"
    },
    "desiredState": {
        "manifest": {
            "version": "v1beta1",
            "id": "apache-dev",
            "volumes": null,
            "containers": [
                {
                    "name": "master",
                    "image": "fedora/apache",
                    "ports": [
                        {
                            "containerPort": 80,
                            "hostPort": 80,
                            "protocol": "TCP"
                        }
                    ],
                }
            ],
            "restartPolicy": {
                "always": {}
            }
        },
    },
}
```

Listing 3: Definition eines Pods

Haben Installation und Konfiguration soweit funktioniert, können Sie sich im Anschluss daran an dem virtuellen System anmelden, um ein Update durchzuführen. Wie zuvor beschrieben, wird in diesem Falle eine neue Instanz des Systems heruntergeladen und beim nächsten Systemstart aktiviert:

```
ssh centos@atomic.example.com
rpm-ostree upgrade
systemctl reboot
```

Da es sich bei diesem System um den Master-Host handelt, können Sie direkt im Anschluss an dessen Konfiguration einen zweiten Host mit dem gleichen Image installieren. Dieser wird im Folgenden als Minion-Host dienen, auf denen die Container Pods laufen. Natürlich steht es Ihnen an dieser Stelle frei, beliebig viele Minions zu installieren. Um die grundlegende Funktion von Kubernetes zu verstehen, reicht allerdings ein einzelner Minion-Host aus. Erzeugen Sie hierfür eine zweite virtuelle Maschine und, wie in Listing 1 beschrieben, eine zusätzliche ISO-Datei, die Sie dem Minion-Host bei der Installation zur Verfügung stellen. Im Anschluss an die Installation sollten Sie auch dieses System aktualisieren und neu starten.

Sind Master und Minion auf dem aktuellen Stand, sind die beiden Rechner in der Datei */etc/hosts* einzutragen und die Kubernetes-Konfigurationsdatei */etc/kubernetes/config* anzupassen. Dort tragen Sie auf beiden Systemen über die Variable "KUBE_ETCD_SERVER" den Master-Server ein. In der aktuellen Version von Kubernetes wird lediglich ein einzelner Master unterstützt, was sich aber in zukünftigen Releases ändern soll. Auf dem Master sind dann zusätzlich die beiden Dateien */etc/kubernetes/apiserver* und */etc/kubernetes/controller-manager* anzupassen. Hier definieren Sie den Hostnamen und den Port des API-Services sowie den Hostnamen des Minion-Servers. Im Anschluss starten Sie auf dem Master alle notwendigen Dienste und überzeugen sich anschließend davon, dass alles fehlerfrei geklappt hat:

```
systemctl start etcd kube-apiserver
  kube-controller-manager kube-sche-
  duler
systemctl enable etcd kube-apiserver
  kube-controller-manager kube-sche-
  duler
systemctl status etcd kube-apiserver
  kube-controller-manager kube-sche-
  duler
```

Auf dem Minion-Host ist neben der Datei */etc/kubernetes/config* auch noch die Konfigurationsdatei des Minion-Agents anzupassen. Tragen Sie hierfür in der Datei */etc/kubernetes/kubelet* den Hostnamen, den Port und die IP-Adresse, auf der der Service lauschen soll, ein. Anschließend starten Sie auch hier die notwendigen Dienste:

```
# docker ps
CONTAINER ID  IMAGE                 COMMAND           CREATED         STATUS          PORTS       NAMES
a9548bd9ecb1  fedora/apache:latest  "/run-apache.sh"  9 minutes ago   Up 9 minutes ago  k8s_master.39902450_apache.default.etcd_37e66e65-8454-11e4-b2be-5254008d3d8e_e8c7bae6
```

Listing 4: Docker zeigt aktive Container

```
systemctl start kube-proxy kubelet
  docker
systemctl enable kube-proxy kubelet
  docker
systemctl status kube-proxy kubelet
  docker
```

Zu diesem Zeitpunkt sollten Sie den Minion-Host auf dem Master sehen. Zur Kommunikation mit dem API-Server kommt das Tool kubectl zum Einsatz:

```
kubectl get minion
NAME
atomic-host-001
```

Im nächsten Schritt können Sie Ihren ersten Pod erzeugen. Zur Erinnerung, hierbei handelt es sich um einen oder mehrere Container, die auf einem der zur Verfügung stehenden Minion-Hosts bereitgestellt werden. Die Definition des Pods erfolgt über eine Datei im JSON-Format, in der Sie sämtliche Informationen zu dem Pod festlegen. Dazu gehören beispielsweise das zu verwendende Docker-Image, der Port der Services und ein optionales Port-Mapping zwischen Container und Host. Sie können hier auch Dateisysteme des Hosts bestimmen, die Sie an den Container binden möchten. Dies ist besonders wichtig, da sämtliche Daten, die Sie innerhalb des Containers ändern, nach dem Beenden des Containers verloren sind.

Jeder Pod lässt sich mit einem oder mehreren Labels versehen. Beispielsweise könnten Sie für alle Apache-Server in Produktion die Label "name=apache" und "stage=prod" in die JSON-Datei aufnehmen. Über eine entsprechende Abfrage mittels kubectl können Sie dann später sehr leicht Ihre produktiven Apache-Server identifizieren und feststellen, auf welchem Minion diese eigentlich gerade laufen. Doch zuerst erzeugen Sie Ihren ersten Pod mit der Datei aus Listing 3. Rufen Sie hierfür das Tool kubectl wie folgt auf:

```
kubectl create -f /tmp/apache-
  pod.json
```

Im Hintergrund wird nun auf dem Minion der Docker Prozess aktiv und fängt an, das "fedora/apache"-Image herunterzuladen, wenn es noch nicht vorhanden ist. Das kann durchaus eine gewisse Zeit in Anspruch nehmen. Rufen Sie danach erneut kubectl auf, so sollten Sie sehen, dass der Container nun aktiv ist (Listing 2).

Dass der Apache-Service innerhalb des Containers wie gewohnt funktioniert, überprüfen Sie mit einem einfachen Aufruf von curl:

```
curl http://atomic-host-001
Apache
```

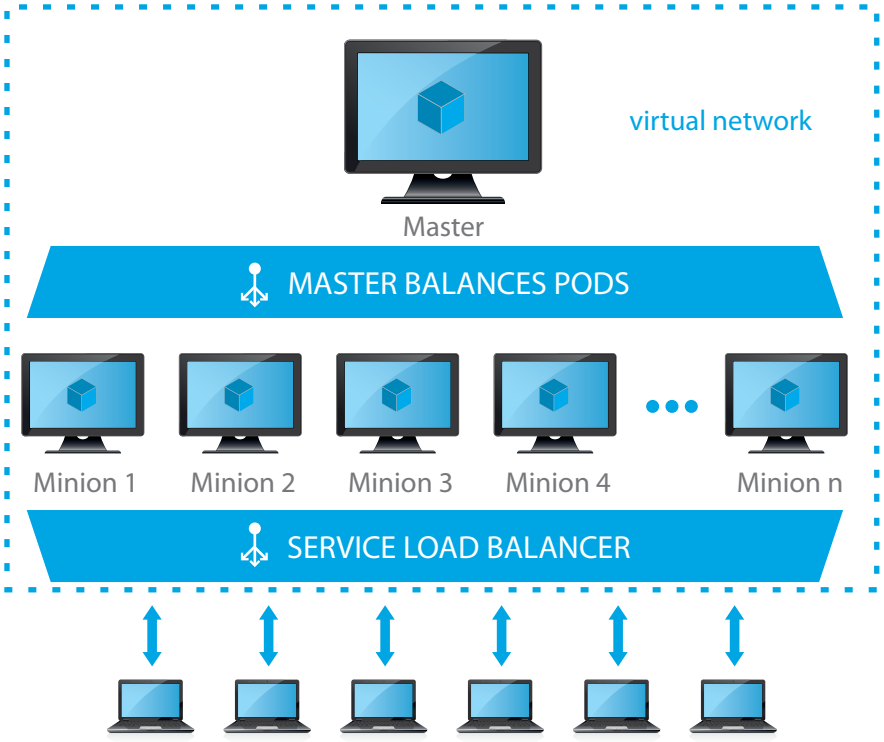
Wenn mehrere Apache-Container in Ihrer Umgebung laufen, können Sie die Ausgabe von "kubectl get pod" anhand der zuvor definierten Labels einschränken. Mittels "kubectl get pods -l name=apache -l stage=prod" würde Kubernetes lediglich die Container anzeigen, die über die beiden Labels name=apache und stage=prod verfügen.

Wie Sie in Listing 3 sehen, enthält die Definition des Pods auch den Hinweis, dass im Fehlerfall ein Container sofort wieder neu zu starten ist (restartPolicy: always). Ob das funktioniert, lässt sich sehr leicht überprüfen. Melden Sie sich hierfür mittels SSH auf dem Minion-Host an und weisen Sie docker an, die gerade aktiven Container anzuzeigen (Listing 4).

Beenden Sie den Container manuell, indem Sie ihn mittels *docker stop a9548 bd9ecb1* anhalten, werden Sie nach kurzer Zeit feststellen, dass Docker ihn automatisch wieder neu startet. Achten Sie hier auf den Wert in der Spalte "CREATED" in der Ausgabe von "docker ps", bevor und nachdem Sie den Container manuell gestoppt haben.

Services und Replication

Kubernetes kennt zwei weitere sehr interessante Features, die bisher noch nicht erwähnt wurden. Mittels eines sogenannten Replication-Controllers können Sie Pods in der Breite skalieren. Anhand eines Pod-Labels können Sie Kubernetes anweisen, diesen Pod x-fach zur Verfügung zu stellen. Kubernetes erzeugt dabei die gewünschte Anzahl von Instanzen der Container und stellt sie auf den vorhan-



Kubernetes bietet einen Service-Loadbalancer an, mit dem der Zugriff auf mehrere Pods über eine einzelne IP-Adresse funktioniert.

denen Minions zur Verfügung. Kubernetes kümmert sich auch darum, die Anzahl der Instanzen aktuell zu halten. Haben Sie also beispielsweise definiert, dass Sie gerne vier Instanzen Ihres Apache-Pods haben wollen, würde Kubernetes automatisch Apache-Docker-Instanzen starten oder beenden, bis die Anzahl der Instanzen der Definition entspricht.

Auch wenn die einzelnen Container IP-Adressen aus einem zuvor in Docker definierten Netzwerkbereich bekommen, erfolgt der Zugriff auf die einzelnen Instanzen eines Pods eher über sogenannte Services. Kubernetes legt hierfür eine Art Abstraktionslayer über bestimmte Pods vom gleichen Typ und weist diesem Service eine IP-Adresse zu. Der Zugriff auf die einzelnen Instanzen eines Pods erfolgt dann über diese Service-IP. Dafür wird die Anfrage an die Service-IP an die einzelnen Minions weitergeleitet und der Dienst kubelet-proxy auf den Minions ist dafür zuständig, die Anfrage an die richtigen Container weiterzuleiten.

Man kann sich einen solchen Service als eine Art Load-Balancer für ein bestimmtes Set an Pods vorstellen (siehe Bild). Damit das funktioniert, muss jeder Minion-Host über ein zusätzliches Netzwerk-Segment verfügen, aus dem der Pod dann eine IP-Adresse zugewiesen bekommt. Die kubelet-proxy-Dienste leiten die Anfrage dann genau an diese IP-Adresse weiter. Der einzige Cloud-Anbieter, der eine solche Netzwerkkonfiguration von Haus aus anbietet, ist jedoch die Google Cloud Platform. Bei allen anderen Anbietern, auch beim Einsatz des hier verwendeten Atomic-Images in einer lokalen Virtualisierungsumgebung, ist eine manuelle Konfiguration des Docker-Dienstes erforderlich. Diese hier zu beschreiben würde jedoch den Umfang des Artikels sprengen, weshalb der Autor an dieser Stelle auf die entsprechende Dokumentation [9] zu dem Thema verweist.

In den neuesten Releases des Atomic-Images wurde das Tool flannel [10] mit in das Image aufgenommen. Hiermit lassen sich sehr leicht sogenannte Overlay-Netzwerke einrichten, auf die Docker dann zurückgreifen kann. Dies erspart eine recht umfangreiche manuelle Konfiguration.

Fazit

Auch wenn Kubernetes aktuell noch tief in der Beta-Phase steckt und die Ausrichtung des Tools auf die Google Cloud Engine sichtbar ist, so ist der Zugewinn an Flexibilität im Vergleich zu nackten Docker-Installationen bereits jetzt schon enorm. Kubernetes legt über die vorhandenen Hardware-Ressourcen einen zusätzlichen Abstraktionslayer und stellt sie als großen Hardware-Pool zur Verfügung.

Auf welchem System ein Container letztlich läuft, spielt keine Rolle mehr. Kubernetes sucht sich die hierfür notwendigen Ressourcen selbstständig zusammen und startet den Container dort, wo die Ressourcen vorhanden sind. Durch den Einsatz von Replication-Controllern hilft das Framework dabei, die vorhandenen Container in der Breite zu skalieren. Dies gelingt innerhalb kürzester Zeit.

Kubernetes-Services helfen dabei, den Zugang zu einem Dienst über eine einheitliche IP-Adresse zur Verfügung zu stellen. Somit entfällt das umständliche Heraussuchen von Container-IPs. Dies ist gerade auch dann besonders wertvoll, wenn man daran denkt, dass Container sehr kurzlebig sein können, um kurze Zeit später auf einem anderen Host wieder neu gestartet zu werden, wodurch sich die IP-Adresse ändert. Services abstrahieren diese Änderungen und erfordern keine Neukonfiguration, beispielsweise von vorgeschalteten Loadbalancern. *(of)*

[1] Google Kubernetes
F3P61

[2] Project Atomic
F3P62

[3] Red Hat Enterprise Linux 7 Atomic Host
F3P63

[4] Fedora Atomic Host
F3P64

[5] CentOS 7 Atomic Host
F3P65

[6] Etcd API-Dokumentation
F3P66

[7] Setup-Anweisungen für eine Atomic-VM
F3P67

[8] cloud-init-Dokumentation
F3P68

[9] Docker-Netzwerk-Dokumentation
EBP13

[10] flannel Overlay-Netzwerk
F3P60

Link-Codes

12 Monatsausgaben im Print- & E-Paper-Format

+ 2 Sonderhefte pro Jahr

+ Jahres Archiv-CD
mit allen Monatsausgaben im PDF-Format

Das Abo All-Inclusive

http://shop.heinemann-verlag.de/

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

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Workshop: Open Source-Tipp

Schlüsselübergabe

von Thorsten Scherf

In den meisten Unternehmen kommt zur Verwaltung der Benutzer ein Directory-Server zum Einsatz. Der 389DS aus dem Fedora-Projekt ist ein weniger bekannter Vertreter aus der Open Source-Welt. Die letzten Releases haben einige wesentliche Vereinfachungen für das Management der Benutzer-Passwörter mitgebracht.

Der 389DS verwendet als globalen Service-Administrator den Account "cn=Directory-Manager". Er bekommt beim Setup ein Passwort zugewiesen, danach gelten für diesen Account keinerlei Einschränkungen mehr. Meldet man sich mit diesem Konto am Directory-Server an, lassen sich ohne weiteres die Passwörter anderer Benutzer zurücksetzen, neu definieren oder der eingesetzte Verschlüsselungsalgorithmus und andere Eigenschaften eines Passworts ändern. Dummerweise war es lange Zeit so, dass kein anderer Benutzer die soeben aufgeführten Änderungen an Benutzer-Passwörtern durchführen konnte. Dies hatte oftmals zur Folge, dass das Passwort für den Directory-Manager allen Passwort-Administratoren bekannt war und sie somit komplette Kontrolle über den Server hatten.

Mittlerweile bietet der Server eine neue Funktion an, mit der sich eine Gruppe von Passwort-Administratoren definieren lässt, die Änderungen an Benutzer-Passwörtern durchführen dürfen, ohne hierfür die komplette Kontrolle über das gesamte System zu erhalten. Auch das Setzen bereits verschlüsselter Passwörter funktioniert ohne Probleme.

Die Gruppe der Passwort-Administratoren können Sie global für alle Konten des Directory-Servers definieren oder aber nur für einen bestimmten Teilbaum des Servers. Das ist sehr hilfreich, wenn Sie Benutzer beispielsweise in verschiedenen Containern verwalten, die einzelne Abteilungen oder Standorte widerspiegeln. Somit können Sie dann für jeden Container eine eigene Gruppe von Passwort-Administratoren definieren, die nur Zugriff auf Konten des jeweiligen Containers haben. Damit der Zugriff funktioniert, muss die Gruppe natürlich auch über die entsprechenden Rechte für den Container verfügen, in dem sich die Benutzer-Objekte befinden. Der 389DS regelt diesen Zugriff über sogenannte Access Control Instructions (ACIs).

Passwort-Policy

Üblicherweise besitzt jeder Container eine bestimmte Passwort-Policy, die die Eigenschaften der Benutzer-Passwörter definiert. Das Tool ns-newpwpolicy.pl aus dem Software Repository des 389DS können Sie dazu verwenden, um die benötigten Attribute und Objekte für eine solche lokale Passwort-Policy zu erzeugen. Listing 1 zeigt einen beispielhaften Aufruf für den Benutzer-Container "ou=people, dc=example,dc=com".

```
# /usr/lib64/dirsrv/slapd-ldap/ns-newpwpolicy.pl
   -D "cn=Directory Manager" -w password -S
   ou=people,dc=example,dc=com
adding new entry
   "cn=nsPwPolicyContainer,ou=people,dc=example,
   dc=com"

adding new entry
   "cn=cn\=nsPwPolicyEntry\,ou\=people\,dc\=exam-
   ple\,dc\=com,cn=nsPwPolicyContainer,ou=people,
   dc=example,dc=com"

adding new entry
   "cn=cn\=nsPwTemplateEntry\,ou\=people\,dc\=exam
   ple\,dc\=com,cn=nsPwPolicyContainer,ou=people,
   dc=example,dc=com"

adding new entry
   "cn=nsPwPolicy_cos,ou=people,dc=example,dc=com"

modifying entry "cn=config"
```

Listing 1: Attribute und Objekte für eine lokale Passwort-Policy

Im Container "cn=nsPwPolicyContainer" können Sie dann dem Eintrag "cn=ns PwPolicyEntry" die gewünschten Policy-Informationen hinzufügen. Dies geschieht am einfachsten über eine LDIF-Datei, die Sie mit ldapmodify in den Directory-Server laden. Listing 2 zeigt ein einfaches Beispiel für eine solche LDIF-Datei.

```
dn:
   cn="cn=nsPwPolicyEntry,ou=People,dc=example,dc=
   com",cn=nsPwPolicyContainer,ou=People,dc=exam-
   ple,dc=com
changetype: modify
add: passwordMustChange
passwordMustChange: on
-
add: passwordMinAlphas
passwordMinAlphas: 1
-
add: passwordHistory
passwordHistory: on
-
add: passwordMinDigits
passwordMinDigits: 1
-
add: passwordMinAge
passwordMinAge: 0
-
add: passwordMinLowers
passwordMinLowers: 1
-
add: passwordChange
passwordChange: on
-
add: passwordMinUppers
passwordMinUppers: 1
-
add: passwordCheckSyntax
passwordCheckSyntax: on
-
add: passwordStorageScheme
passwordStorageScheme: ssha256
-
add: passwordAdminDN
passwordAdminDN:
   cn=password_admins,ou=Groups,dc=example,dc=com
```

Listing 2: LDIF-Datei mit Policy-Informationen

Alle Listings zum Download unter www.it-administrator.de

Die LDIF-Datei laden Sie wie folgt in den Directory-Server:

```
ldapmodify -v -x -a -h localhost -p
  389 -D "cn=Directory Manager" -w
  password -f /tmp/pw-policy-
  local.ldif
```

Der letzte Eintrag in der Datei bestimmt die Gruppe der Passwort-Administratoren für den Container "ou=People,dc=example,dc=com". Dieser Gruppe müssen Sie noch Zugriff auf den Container einräumen. In diesem Beispiel bekommen die Mitglieder der Gruppe lediglich das Recht zugewiesen, die Passwörter der Benutzer neu definieren zu dürfen – natürlich können Sie an dieser Stelle auch weitere Rechte zugestehen. Hierfür kommt erneut eine LDIF-Datei (Listing 3) zum Einsatz, die Sie wieder mit ldapmodify in den Server laden:

```
ldapmodify -v -x -a -h localhost -p
  389 -D "cn=Directory Manager" -w
  password -f /tmp/pw-policy-admin-
  aci.ldif
```

Eine genaue Übersicht sämtlicher Policy-Einstellungen und weitere Informationen zu den Access Control Instructions (ACI) finden Sie in der Dokumentation des 389DS [1].

Passwort-Administratoren

Um einzelne Konten in die Gruppe der Passwort-Administratoren aufzunehmen, greifen Sie entweder auf das grafische Administrationstool "389-console" zurück oder legen die Benutzer über eine LDIF-Datei an. Listing 4 zeigt ein Beispiel. Die Datei laden Sie wie gehabt mit ldapmodify in den Directory-Server.

Sämtliche Mitglieder der Gruppe "cn=password_admins" sind nun berechtigt, die Passwörter von Benutzern aus dem Container "ou=People,dc=example,dc=com" neu zu setzen. Dafür können sie sich mit ihrem eigenen Konto am Directory-Server anmelden und müssen nicht mehr auf das bisher verwendete Konto des Directory-Managers zurückgreifen. Listing 5 zeigt ein Beispiel für die Änderung eines Benutzers-Passworts mittels einer LDIF-Datei. Mittels ldapmodify meldet sich diesmal der Passwort-Administrator mit seinem eigenen Konto am

```
dn: ou=People,dc=example,dc=com
changetype: modify
add: aci
aci: (targetattr ="userpassword")(version 3.0;acl
   "Allow password admins to write user pass-
   words";allow (write)(groupdn =
   "ldap:///cn=password_admins,ou=Groups,dc=exam-
   ple,dc=com");)
```

Listing 3: Vergabe von Benutzerrechten

```
dn: cn=password_admins,ou=Groups,dc=example,dc=com
changetype: add
objectClass: top
objectClass: groupOfUniqueNames
cn: password admins
ou: groups
uniqueMember:
   cn=admin1,ou=People,dc=example,dc=com

dn: cn=admin1,ou=People,dc=example,dc=com
changetype: add
objectClass: top
objectClass: person
cn: admin1
sn: admin1
userPassword: password
```

Listing 4: Benutzer in die Admin-Gruppe aufnehmen

```
dn: cn=user1,ou=People,dc=example,dc=com
changetype: modify
replace: userPassword
userPassword: {SSHA}aMzZ1DZsBXz\FZAL5rT4xQiPhmuke-
   D
```

Listing 5: Änderung eines Benutzerpassworts

Directory-Server an, um die Datei in den Server zu laden:

```
ldapmodify -v -x -a -h localhost -p
  389 -D
  "cn=admin1,ou=People,dc=example,
  dc=com" -w password -f /tmp/user-
  password-change.ldif
```

Fazit

Die hier dargestellte Methode stellt eine Möglichkeit dar, um beispielsweise Helpdesk-Mitarbeitern den Zugriff auf Benutzer-Passwörter zu gestatten, ohne ihnen die Kontrolle über den kompletten Server einzuräumen. Wie das Beispiel zeigt, funktioniert dies auch in Kombination mit zuvor eingerichteten Passwort-Regeln. *(of)*

[1] 389-Dokumentation
F3P01

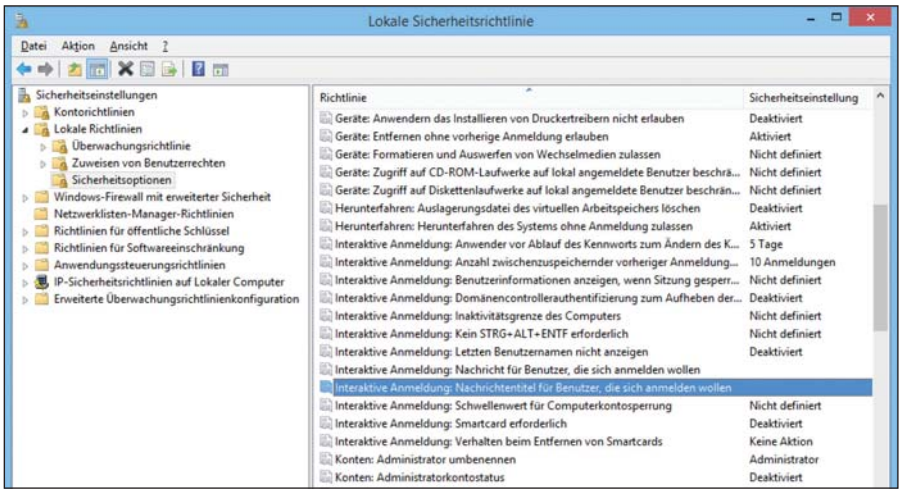
Link-Codes

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

Microsoft Windows

Manchmal fände ich es äußerst praktisch, den Nutzer eines bestimmten Rechners schon beim **Anmelden an Windows 8** mit einer kurzen Nachricht auf etwas aufmerksam zu machen, etwa ein bevorstehendes Wartungsfenster. Gibt es irgendeine Möglichkeit, vor dem Logon-Screen **eine Mitteilung einzublenden**, deren Inhalt ich frei bestimmen kann?

Wenn Sie lokalen Zugriff auf den entsprechenden Rechner haben oder eine Remote-Verbindung starten können, führt Sie der Weg über die Sicherheitsrichtlinien. Geben Sie nach dem Drücken von [WIN+R] *secpol.msc* ein. Nach wenigen Sekunden öffnet sich das "Lokale Sicherheitsrichtlinie" getaufte Fenster, wo Sie sich in den Bereich "Lokale Richtlinien / Sicherheitsoptionen" durchklicken. Im rechten Teil des Fensters finden Sie nun die beiden selbsterklärenden Einträge "Interaktive Anmeldungen: Nachrichtentitel für Benutzer, die sich anmelden wollen" sowie "Interaktive Anmeldungen: Nachrichten für Benutzer, die sich anmelden wollen". Mit einem Rechtsklick auf den jeweiligen Eintrag und der Option "Eigenschaften" können Sie den Titel und den Inhalt der Nachricht nach Ihren Wünschen festlegen. Beim nächsten Login sollte die Mitteilung auf dem Bildschirm erscheinen. Das Ganze klappte übrigens schon bei Windows 7-Rechnern, von den Home-Editionen einmal abgesehen. Wenn Sie mit einer oder mehreren Domänen arbeiten, können Sie für diese Einstellungen natürlich auch die Group Policy Management Console (*gpmc.msc*) verwenden. *(ln)*



Wer nicht über Gruppenrichtlinien gehen will oder kann, der konfiguriert eine beim Login erscheinende Nachricht einfach über die lokalen Sicherheitsrichtlinien.

CITRIX

Bei uns kommt noch **XenApp 5.0 für Windows Server 2008** zum Einsatz, da wir noch **Programme mit 16 Bit-Anteil** verwenden müssen. Hier haben wir leider mit einer schlechten Bildwiederholungsfrequenz und einer daraus resultierenden **fehlerhaften Bilddarstellung** zu kämpfen. Manche Teile der Anwendung erscheinen grau oder verfälscht. Die Probleme treten immer dann auf, wenn wir per Passthrough Client auf dem Server auf eine veröffentlichte **Anwendung im Seamless-Modus** zugreifen. Mit einer festgelegten Fenstergröße hingegen funktioniert es. Ein manueller Refresh der Anwendung hilft leider auch nicht. Haben Sie noch einen Tipp?

Dieses Problem kann neben XenApp 5.0 für Windows Server 2008 auch die Versionen 6.0 und 6.5 für Windows Server 2008 R2 betreffen. Folgende Schritte helfen, das Problem zu lösen. Geben Sie zunächst im Abschnitt [wfclient] der Datei *Appsrv.ini* – Sie finden diese im Verzeichnis *%SystemRoot%\system32\ICAPassthroughDirectory* – folgende zwei Werte ein:

```
ForceLVBMode=1
DeferredUpdateMode=True
```

Fügen Sie dann für den Client 10.x unter "HKEY_LOCAL_MACHINE \ SOFTWARE \ Citrix \ ICA ClientEngine \ Configuration \ Advanced \ Modules \ WFClient" folgende zwei Keys hinzu:

```
ForceLVBMode=1
DeferredUpdateMode=True
```

Alternativ lässt sich das Problem wie folgt lösen: Nutzen Sie ICA-Dateien für den

Zugriff auf eine Anwendung, müssen die gleichen Werte, die Sie der Datei *Appsrv.ini* hinzugefügt haben, auch in den ICA-Dateien enthalten sein. Deaktivieren Sie dazu "Client Info Sync", zu finden unter "CTX101644 - Seamless Configuration Settings". *(Citrix/ln)*

Wir nutzen bei uns **Amazon EC2** und würden hier nun gerne eine **virtuelle Maschine importieren**. Können Sie in Grundzügen schildern, was wir hierbei beachten sollten?

Die Funktion "VM Import/Export" bietet zwei Methoden zum Importieren Ihrer virtuellen Maschine in Amazon EC2. Bei der ersten importieren Sie VM-Images mit den Amazon EC2 API-Tools. Importieren Sie dafür die VMDK-, VHD- oder RAW-Datei über die ec2-import-instance-API. Bei der Instance-Importaufgabe werden die Parameter erfasst, die erforderlich sind, um die Amazon EC2-Instance-Eigenschaften ordnungsgemäß zu konfigurieren (Instance-Größe, Availability Zone und Sicherheitsgruppen), und das Image wird in Amazon S3 hochgeladen. Wenn *ec2-import-instance* unterbrochen oder ohne abgeschlossenen Upload beendet wird, verwenden Sie *ec2-resume-import*, um den Upload-Vorgang fortzusetzen. Der Importvorgang findet an der Stelle, an der er unterbrochen wurde, seine Fortsetzung. Nutzen Sie zur Überwachung des Fortschritts des Importvorgangs den Befehl *ec2-describe-conversion-tasks*. Dadurch erhalten Sie die Amazon EC2 Instance-ID. Sobald der Importvorgang abgeschlossen ist, können Sie die Amazon EC2-Instance neu starten, indem Sie für die ec2-run-instances-API die Instance-ID angeben. Löschen Sie abschließend mit dem Befehlszeilenprogramm *ec2-delete-disk-image* Ihr Datenträger-Image aus Amazon S3, da es nicht mehr benötigt wird. Bei der zweiten Methode können Sie Ihre virtuelle Maschine mittels einer grafischen Benutzeroberfläche des Amazon EC2 VM Import Connector in Amazon EC2 importieren, sofern Sie die VMware vSphere-Virtualisierungsplattform verwenden. Zum Start mit dem Connector laden Sie die Amazon EC2 VM Import Connector vApp für VMware vCenter herunter und installieren die Connector vApp auf dem vCenter Server. Wählen Sie mithilfe des VMware vSphere-Clients das VM-Image, das zu Amazon EC2 importiert werden soll. Auf der Registerkarte "Import to EC2" (Zu EC2 importieren) wählen Sie die Region, die Verfügbarkeitszone, das Betriebssystem, die Instance-Größe sowie (bei Bedarf) VPC-Details für den Import des Images aus und beginnen Sie den Importprozess. Starten Sie die Amazon EC2-Instance, nachdem der Importprozess abgeschlossen ist.

(AWS/ln)

Android

Da die integrierte E-Mail-App ja selbst unter **Android 5** doch sehr rudimentär ist, nutze ich schon lange die App **K-9 Mail**, die in meinen Augen so gut wie keine Wünsche offenlässt – vielleicht einmal abgesehen von einem schönen Widget für die Startseite, aber hier kann man sich ja durch Drittanbieter behelfen. Mein großes Problem ist nun jedoch, dass K-9 seit dem Update auf Android 5 **ständig Zertifikatsprobleme** meldet. Laut Hersteller lässt sich dies durch ein Update beheben, doch das **Update bricht immer mit der Fehlermeldung 505 ab**. Als ich nun versucht habe, K-9 zu deinstallieren und neu aufzuspielen, funktioniert auch das nicht mehr und die App findet gar nicht mehr den Weg auf mein Smartphone. Was kann ich hier tun?

Auch wenn es für die beschriebene Fehlermeldung viele Gründe geben kann, tippen wir stark auf einen Konflikt mit einer anderen installierten App. Da Sie es schon indirekt erwähnt haben, vermuten wir, dass Sie ein Mail-Widget für den Homescreen benutzen, etwa das beliebte "MailListWidget for K9". Mit Android 5 kann es hier aufgrund einer geänderten Berechtigungspolitik zu Problemen kommen. Unter Lollipop ist es nicht mehr möglich, dass zwei Programme auf den exakt gleichen Berechtigungs-String eines Programms zugreifen – etwa die Funktion, E-Mails zu löschen, was bisher sowohl aus K-9 als auch aus dem Widget möglich war. Wenn Sie nun unter Lollipop K-9 aktualisieren oder neu installieren wollen, meldet das Betriebssystem, dass ein anderes Programm den exakt gleichen Berechtigungs-String anspricht und verweigert die Installation. Im Moment gibt es dafür keine Lösung, solange der Anbieter des Widgets seinen Code nicht anpasst. Um K-9 weiterhin nutzen zu können, müssen Sie bis auf weiteres also leider das Widget vom Smartphone werfen. Das gleiche Problem ist übrigens von Kalender-Widgets bekannt, die auf die integrierte Kalender-App zugreifen. Für K-9 Mail gibt es unter [Link-Code F3PE4] übrigens ein recht annehmbares Hilfe-Forum bei Google Groups. *(ln)*

Linux

Wir nutzen das **Intelligent Platform Management Interface (IPMI)**, um einen Linux-Server zu warten und automatische Berichte über auftretende Fehler zu erzeugen. Beim **Abfragen der IPMI-Sensoren** über das Netzwerk mit Hilfe des IPMI-Sensors "FreeIPMI" kommt es manchmal zur **Fehlermeldung "Internal IPMI Error"**. Haben Sie eine Idee, was die Ursache hierfür sein könnte und wie wir das Problem beheben können?

Über die standardisierten IPMI-Schnittstellen zu gehen, ist an sich eine sehr gute Möglichkeit, Hardware im Auge zu behalten. Es kann aber auch zu Problemen kommen, wenn solche Abfragen beispielsweise vom IPMI Sensor Monitoring Plug-In (check_ipmi_sensors) ausgeführt werden. Eine mögliche Ursache sind gleichzeitige IPMI-Zugriffe, die direkt lokal am Server zur Ausführung kommen, zum Beispiel, wenn Linux am betroffenen Server läuft und der Kernel IPMI-Treiber geladen ist. Wenn es sich wie in Ihrem Fall um ein Linux-System handelt, führen Sie folgende Schritte zur Fehlerbehebung durch: Überprüfen Sie

mit folgendem Kommando, ob IPMI-Module des Kernels geladen sind:

```
lsmod | grep -i ipmi
```

Falls hier Module geladen sind und Sie diese nicht benötigen, entfernen Sie diese. Führen Sie dann noch einen Neustart Ihres IPMI-Microcontrollers durch. Nun sollte die Fehlermeldung nicht mehr auftauchen. *(ln)*

THOMAS KRENN *Viele weitere Tipps und Tricks zum Server-Management, Virtualisierung und Linux finden Sie im Thomas-Krenn-Wiki unter www.thomas-krenn.com/de/wiki/Hauptseite*

Hardware

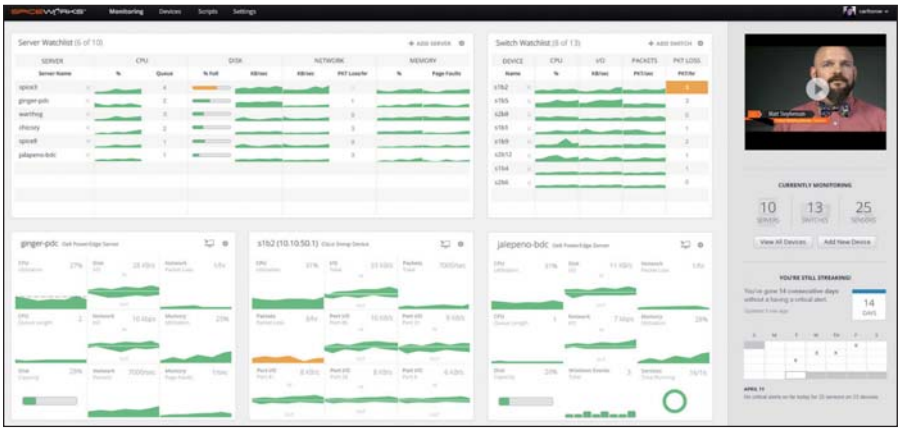
Wir sind eine private **Multimedia-Hochschule mit sechs Standorten** in Deutschland und auf Grafik-, Web- und Kommunikationsdesign sowie Marketing und Kommunikation im Allgemeinen spezialisiert. Da unsere Studenten das Studium finanziell unterstützen müssen, erwarten sie den **höchsten technischen Standard**, den eine Universität bieten kann, und es ist unser Anspruch, diese hohen technischen Standards zu erfüllen. Unsere IT-Infrastruktur ist mittlerweile etwas veraltet und wir wollen an unseren Standorten eine neue IT-Infrastruktur implementieren, die die Bereiche **Datenspeicher, schnelle Netzwerk-Vernetzung sowie performante WLAN-Anbindung** bietet. Was raten Sie uns?

Als moderne und hochgradig technische Bildungsstätte sollten Sie auf die neueste Technik und auf eine Kombination von 10-GBit-Ethernet-Storage (10GbE), 10-GbE-PoE-Switches zusammen mit kleineren Gigabit-Switches und moderne, PoE-fähige Wireless-Controller und Wireless-Access-Points setzen. Folgender Aufbau wäre naheliegend: An ihre virtualisierten Server-Strukturen an den Standorten binden Sie zum Beispiel performante 10-GbE-NAS-Systeme als Datenspeicher sowohl für die tägliche Datenbearbeitung als auch für die Datensicherung und Datenverteilung über idealerweise eine Private-Cloud-Lösung auf dem NAS an. Diese erwerben Sie je nach Gegebenheit im Rackmount-Format für Ihren Serverschrank oder auch im Desktop-Format. Sie können sich hier entscheiden, am Hauptstandort einen etwas größeren Datenspeicher anzubinden, auf den die NAS-Systeme an den anderen Standorten ihre Daten replizieren, das heißt, jedes NAS-System an einer Zweigstelle sichert zum Beispiel nachts die täglich bearbeiteten oder erstellten Daten in der Hauptzentrale. Die Server und NAS-Systeme werden dann über 10-GbE-Switches an das restliche kabelgebundene Hochschulnetz und an die Wireless-Controller angeschlossen, worüber der Datenaustausch mit den kabelgebundenen und den kabellosen Client-Geräten mit Geschwindigkeiten bis zu 10 GBit/s erfolgen kann. An die Wireless-Controller binden Sie per Netzwerkkabel die Wireless Access Points an, die möglichst flächendeckend in der gesamten Bildungsstätte angebracht werden. Die Stromversorgung der Access Points können Sie mit Power-over-Ethernet (PoE) realisieren– die Energieversorgung erfolgt über das Netzwerkkabel. Zu guter Letzt können Sie noch die einzelnen Seminarräume mit GBit-Switches an die Infrastruktur anbinden, damit dortige Client-PCs und Übungsrechner für die Studenten einfach und schnell auf Daten zugreifen können. Das ganze System lässt auch den Sicherheitsaspekt nicht außer Acht. Unterschiedliche Datenbereiche für Professoren und Studenten werden über die mit Smart Switchen mögliche VLAN-Segmentierung voneinander abgetrennt. So hat jeder nur Zugriff auf Daten, für die er berechtigt ist. Für das WLAN-Netz können Sie eine einfache Login-Funktionalität einrichten. Dabei müssen Studenten ihre Geräte erst über die Mac-Adresse im Hochschulnetz registrieren und freigeschaltet werden. Somit ist sichergestellt, dass erstens kein Eindringen von außen in das Hochschulnetz möglich ist und sich zweitens illegale Aktivitäten durch die Studenten im Internet schnell entdecken und unterbinden lassen. *(Netgear/ln)*

Tools

In unserer Schwerpunktausgabe zum **Monitoring** darf natürlich ein freies Werkzeug zur Überwachung der IT nicht fehlen. Abgeleitet vom altbekannten Leitspruch "Was sich nicht messen lässt, lässt sich nicht managen" bietet das Tool unserer Wahl Monitoring **in Echtzeit** und somit auch ein IT-Management in Echtzeit.

Die Rede ist hier vom **"Spiceworks Network Monitor"**. Mit der neuen, kostenlosen Anwendung behalten IT-Profis ihre Server und Netzwerkgeräte in Echtzeit im Blick. Die IT-Abteilung erkennt anhand des Tools auf einen Blick, wie es um den Zustand und die Verfügbarkeit der Geräte bestellt ist. Der Spiceworks Network Monitor lässt sich auf einem Windows-Server in zehn Minuten installieren und liefert Angaben zur IT-Umgebung – etwa zur **Netzwerkauslastung und Serveraktivität** – übersichtlich auf einem Dashboard. Auch Daten zu Festplatten- und CPU-Auslastung, Systemspeicher sowie aktiven Services und Prozessen lassen sich abrufen. **Echtzeit-Alerts** und Konfigurationsoptionen für verschiedene Netzwerkkonditionen sind ebenfalls eingebaut. Je nach Schweregrad des Problems und eigenen Präferenzen können Administratoren einstellen, ob sie über das Dashboard oder per E-Mail über Vorfälle benachrichtigt werden wollen. Zudem informiert die Software darüber, ob ein Nutzer unerlaubterweise eine Software installiert oder sich die Farbpatronen der Netzwerkdru-



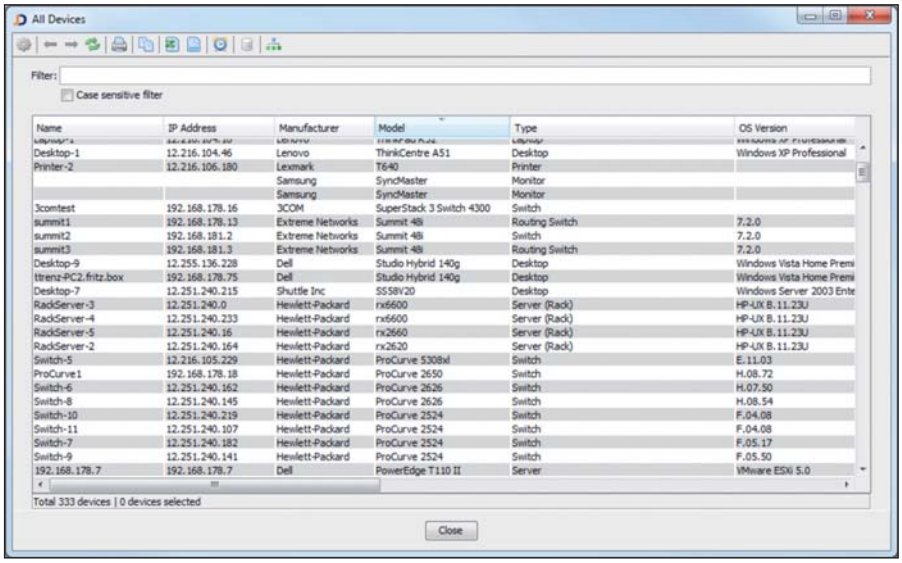
Für ein kostenloses Tool bietet der Spiceworks Network Monitor eine beeindruckende Vielfalt an Monitoring-Funktionen.

cker zum Ende neigen. Managen lassen sich solche Ereignisse über **selbsterstellte Kontroll-Profile**, in denen der Administrator Schwellenwerte und Zustände individuell definiert und bei Abweichungen entsprechende Hinweise erhält. Dies gilt im Übrigen auch für Netzwerk-Schnittstellen, über die sich beispielsweise ermitteln lässt, wie viel Bandbreite ein Endgerät oder ein Router benötigt. Darüber hinaus lassen sich ermittelte Werte im Berichtswesen des Tools grafisch aufbereiten. Abschließend sicher noch erwähnenswert: Der Spiceworks Network Monitor ist in der Lage, Exchange-Server detailliert zu überwachen. Der Download ist nach einer kurzen Registrierung auf der Herstellerseite möglich. *(jp)*
Link-Code: F3PE1

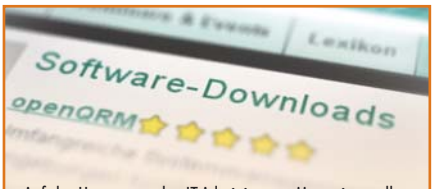
Viel zu oft finden sich zu den in kleinen und mittelständischen Firmen vorhandenen Computern nur veraltete und manuell erstellte **Inventar-Listen**. Die Folge: Niemand weiß wirklich so ganz genau, **welche Komponenten in den einzelnen Rechnern verbaut sind** oder wie aktuell die eingesetzte Software ist. Doch vergleichbar mit den Daten, mit denen ein professionelles Monitoring über die Aktivitäten in der IT-Infrastruktur informiert und somit sinnvolle Maßnahmen ermöglicht, muss für die Wartung und den Betrieb der Hardware der aktuelle Ist-Zustand bekannt sein. Nur so ist es beispielsweise möglich, die richtige Anzahl der benötigten Lizenzen einer Software zu ermitteln oder zu budgetieren, wie viel im kommenden Jahr in die Client-PCs gesteckt werden muss.

Doch sollte ein solches Tool gerade für kleine Unternehmen am besten kostenlos sein, denn ansonsten lohnt es sich unter Umständen, im Zweifelsfall lieber eine Lizenz einer Office-Anwendung zu viel zu erwerben, als einen substantiellen Betrag in eine Software zur Inventarisierung zu stecken. Passend zu diesem Paradigma ist das kostenlose **"JDisc Discovery Starter Edition"**. Das erlaubt Firmen, ihr **Netzwerk zu dokumentieren,** und ermittelt dabei die elementaren Attribute der Geräte, darunter etwa IP- und MAC-Adressen, Typ, Model und Seriennummer. Das zeitlich unbeschränkt nutzbare Werkzeug erfasst zudem die **Informationen zu allen im Netzwerk vorhandenen SNMP-basierten Geräten**. Dazu zählen etwa Router, Switches, Drucker und natürlich auch die Betriebssysteme wie etwa Windows, Linux, VMware ESX(i), Mac OS X, HP-UX, AIX und Solaris. Darüber hinaus erkennt das Tool **IPv4- und IPv6-Netzwerke** sowie **Windows-Domänen und Active Directory-Installationen** und ordnet sie den einzelnen Geräten zu. So lassen sich Zusammenhänge über die Grenzen der einzelnen Geräte hinaus erkennen. *(jp)*
Link-Code: F3PE2

Fast jedem Admin sind die Kommandozeilenwerkzeuge "tracert" und "pathping" im Umfeld des **Netzwerk-Troubleshootings** ein Begriff. Mit diesen bewährten Mitteln lassen sich einfache Verbindungsprobleme im LAN schnell ausfindig machen. Der Einsatzbereich ist jedoch begrenzt auf einfaches Routing. Sollen **umfangreichere Traces professionell analysiert** werden, ist eine Visualisierung mit einer GUI unumgänglich.
Diese liefert das freie **"WhatsUp Visual Traceroute"**. Doch neben der **Netzvisualisierung per GUI** kommt dieser praktische Helfer mit einem weiteren großen Vorteil gegenüber der Kommandozeile daher: **Unterstützung von ICMP**. Denn oft blocken Firewalls ICMP-Pakete, was die Analyse mit den in der Einleitung erwähnten Werkzeugen erschwert bis unmöglich macht. Gerade in Internetapplikationen können TCP- und UDP-Pakete nämlich eine andere Route nutzen als ICMP, was wertvolle Informationen über das aktuelle Netzwerkproblem unzugänglich macht. Auch erlaubt WhatsUp Visual Traceroute, zahlreiche Parameter bei der Verbindungsanalyse zu setzen, um so das Problem gezielt einzugrenzen. Dazu zählen die Definition der Quell- und Zielports, das Setzen der SYN- oder FIN-Flags in TCP-Paketen und vieles mehr. Zusätzlich bereitet die Software **Netzwerklatenzen** grafisch auf und zeigt die Qualität der jeweiligen Verbindungen in einem Ampel-System an. Eine weitere Visualisierung der Latenz als unterschiedlich große Kreise rund um ein Netzwerkelement klärt den IT-Verantwortlichen über die Veränderung der Performance im Zeitablauf auf. Ein großer Kreis legt somit einen hohen **Jitter-Wert zwischen der Quelle und dem Ziel** nahe. Eine solche Information wird auf der Kommandozeile nur zu leicht übersehen. Der Download des Tools erfordert eine Registrierung auf der Webseite des Herstellers. *(jp)*
Link-Code: F3PE3



Die JDisc Discovery Starter Edition ermittelt zahlreiche Inventardaten zu allen im Netz vorhandenen Geräten.



Auf der Homepage des IT-Administrator-Magazins stellen wir jede Woche für Sie ein praktisches Tool zum Download bereit. Neben einer Kurzbeschreibung finden Sie Systemvoraussetzungen und alle weiteren wichtigen Informationen auf einen Blick. Und können so gezielt Werkzeuge für Ihren täglichen Administrationsbedarf herunterladen.

www.it-administrator.de/downloads/software/

Download der Woche

Vertrauen ist besser mit Kontrolle

von Klaus Bierschenk

Die Active Directory-Verbunddienste spielen in Unternehmen eine immer wichtigere Rolle, insbesondere für darauf basierende Vertrauensstellungen zu Office 365 oder zu Partnerunternehmen. Daher sollte der IT-Verantwortliche die Farm stets im Auge behalten, denn Störungen im Betrieb werden dem Anwender mitleidlos quittiert und der Zugriff auf die gewünschte Webseite verweigert. Unser Workshop zeigt Wege, diesen Dienst zu überwachen – sei es nun mit der großen Lösung System Center oder kostenlosen Skripten und Bordmitteln.

Die Implementierung der Active Directory-Verbunddienste (AD Federation Services, ADFS) unterliegt zahlreichen Abhängigkeiten, die den Betrieb in unterschiedliche Weise stören können. Da ist zum einen das Active Directory, in dem sich das Dienstkonto, unter dessen Kontext der jeweilige ADFS Service läuft, befindet. Das Konto hat zwar keine speziellen Berechtigungen, die es zu überwachen gilt, aber ein gesperrtes Konto kann dennoch für Unmut sorgen. Gleiches gilt für die im AD verwalteten Service Principal Names (SPN). Läuft hier etwas schief, weil etwa ein SPN doppelt registriert wurde, dann ist die Fehlersuche meist schwierig. Eine bis dato intakte ADFS-Farm sorgt dann aus heiterem Himmel und scheinbar ohne Anlass für teilweise massive Probleme.

Darüber hinaus sind Zertifikate eine der häufigsten Fehlerquellen im Federation-Server-Umfeld. Zertifikate sind nicht ewig gültig und ein Dienst oder eine Vertrauensstellung, die auf einem Zertifikat basiert, ist eben nur solange intakt, wie das Zertifikat vorzeigbar ist. Die Liste der Abhängigkeiten ist aber noch länger: Egal, ob die Verbunddienste in einer Farm laufen – also die Konfiguration auf einem SQL-Server liegt – oder ob eine WID (Windows Internal Database, ehemals SQL Express) zum Einsatz kommt, die SQL-Datenbank ist in jedem Fall wichtig. Zwar speichert ADFS keine Anwenderdaten, sondern nur Konfigurationsdaten und wenn der SQL-Server Probleme hat, werden trotzdem noch SAML-Token ausgestellt. Haben Sie sich beispielsweise in der Farm für den Einsatz einer WID ent-

schieden und der primäre ADFS-Server fällt mit einem Defekt aus, sind Änderungen an der Konfiguration der Farm nicht mehr möglich, ADFS wird aber weiter authentifizieren. Das Problem taucht ohne Monitoring somit erst später auf.

Monitoring mit SCOM

Haben Sie in Ihrem Netzwerk mehrere Dienste von Microsoft, kann es der System Center Operations Manager (SCOM) sein, dem Sie die Überwachung der Federation Services anvertrauen. Frei definierbare Ansichten liefern einen schnellen Überblick und dabei greift SCOM nicht nur stupide die Events der Server ab, sondern schaut auch, ob alle Komponenten richtig "ticken" – beispielsweise, ob Endpunkte erreichbar sind oder ob eines der Zertifikate Probleme bereitet. Sind Schwellenwerte überschritten, erhält der diensthabende Administrator über frei definierbare Kanäle rund um die Uhr Nachrichten und kann sofort reagieren.

Die Inbetriebnahme des "SCOM Monitoring for Federation Server" ist denkbar einfach, funktioniert sie doch wie in SCOM üblich über produktspezifische Management Packs. Jenes mit der Bezeichnung "Active Directory Federation Services 2012 R2" [1] lässt sich problemlos integrieren und die Ermittlung der ADFS 3.0-Server verläuft ohne spezielles Zutun. Wichtig zu wissen ist an dieser Stelle noch, dass das Management Pack versiegelt ist und keine Änderungen direkt darin erfolgen können. Ist dies gewünscht, müssen Sie es duplizieren, um zum Beispiel spezielle Regeln oder Monitore an Ihre Anforderungen anzupassen. Das ist übrigens empfohlenes Best Practice von Microsoft und bietet den Vorteil, dass Änderungen immer separat von weiteren Management Packs und deren Abhängigkeiten sind. Kopieren, Sichern und Transfers aus Testumgebungen erleichtern sich dadurch.

Übrigens ergibt es Sinn, das Management Pack über die Downloadseite herunterzuladen und dann in SCOM zu importieren und es nicht direkt innerhalb der SCOM-Konsole zu beziehen. Dadurch besteht die Möglichkeit, die Dokumentation gleich mit herunterzuladen. Diese ist zuletzt im April 2014 angepasst worden und beinhaltet alle aktuellen Informationen zu ADFS 3.0, wie beispielsweise Hinweise zur Installation oder auch welche Quellen überwacht werden. Da das Management Pack nicht abwärtskompatibel zu älteren ADFS-Versionen ist, müssen Sie in diesem Fall die jeweils passenden Management Packs hinzufügen.

Kostenlose Hilfe

Die Liste kommerzieller Monitoring-Software ist lang. Setzen Sie bereits ein Produkt zur Überwachung ein, ist es meist ein Leichtes, die Server für ADFS im Sinne einer einheitlichen Überwachung gleichfalls zu integrieren. Doch welche Möglichkeiten bestehen, wenn bislang keine Überwachungssoftware zum Einsatz kommt? Oder in netzwerktechnisch abgeschotteten Implementierungen, wie zum Beispiel in Testumgebungen? Auch diese können produktiven Charakter haben, etwa aus Sicht der Entwickler, was aber die Lizenzkosten für die Monitoring-Suite nicht unbedingt rechtfertigt.

In diesem Fall müssen Sie schauen, was die Bordmittel hergeben. Bevor wir uns diesen Möglichkeiten widmen, noch ein wichtiger Aspekt vorweg: Eine ADFS-Farm hat selten den Umfang wie ihn Administratoren von einer typischen Webserverfarm mit zwanzig oder noch mehr Servern kennen. Bei ADFS sind die Kapazitäten architekturbedingt kleiner. Als Richtwert empfiehlt Microsoft [2] beispielsweise für 15.000 zu authentifizierende Benutzer lediglich zwei ADFS-Server. Etwas anders sieht es zwar aus, wenn Office 365 ins Spiel kommt, trotzdem wird die Infrastruktur überschaubar bleiben und da bieten sich die Windows Server 2012-Bordmittel an.

Server-Manager als Schaltzentrale

Ein ADFS-Server protokolliert alle relevanten Ereignisse im "AD FS"-Protokoll in den Anwendungs- und Dienstprotokollen der Ereignisanzeige. Um nicht auf allen Servern in der Farm die Protokolle hinsichtlich möglicher Probleme anschauen zu müssen, kann es sinnvoll sein, sämtliche Server der Farm von einem zentralen Ort aus zu verwalten. Der Server-Manager bietet hier viel mehr als nur das simple Installieren von Serverrollen und Funktionen. Wurden alle Server im Server-Manager hinzugefügt, gibt das Dashboard gesammelte Statusinformationen wieder.

Ein praktisches Beispiel könnte so aussehen: Über das Kontextmenü lassen sich gezielt Server von der Ferne aus administrieren und nach Wartungsarbeiten zum

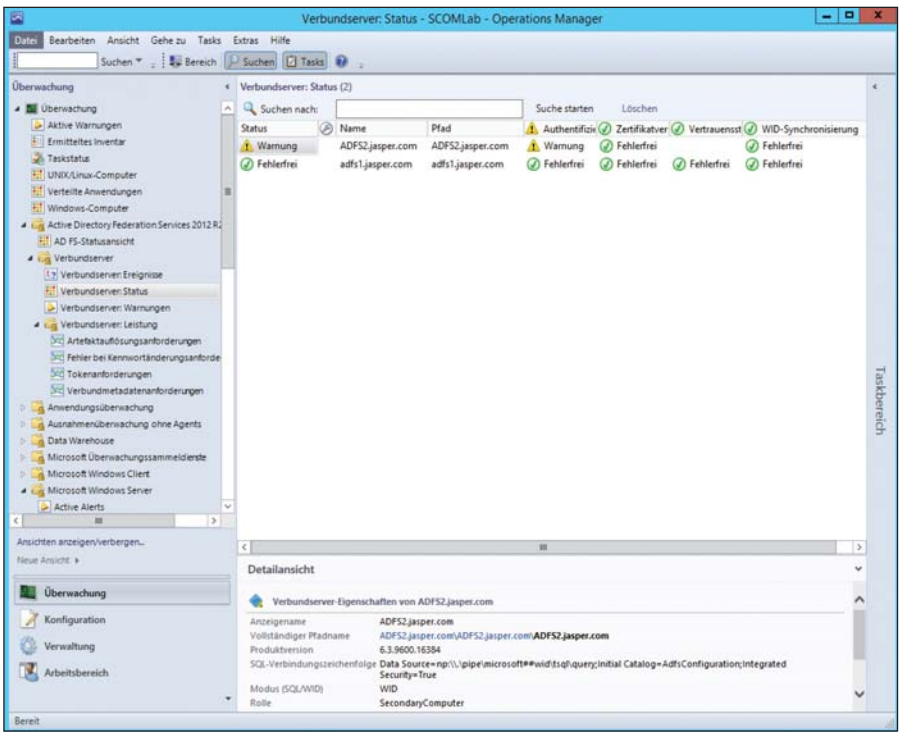


Bild 1: Die zentrale Statusansicht im SCOM fasst alle wichtigen ADFS-Informationen zusammen.

Beispiel neu starten. Ist der Server wieder online, wird innerhalb des Dashboards dann ersichtlich, dass der Remote Server zwar gestartet worden ist, der ADFS Service aber hängt. Wiederum über das Kontextmenü lässt sich nun der Dienst von hier aus direkt neu starten und die rot markierten Warnhinweise aus dem Server-Manager verschwinden.

Das Dashboard bietet auch die Möglichkeit, auf die erwähnten ADFS-Ereignisprotokolle der Server zuzugreifen. So werden zentral alle Einträge der Farm angezeigt und geben Aufschluss über den Zustand der Umgebung. Über Filter lässt sich die Ansicht einschränken, um beispielsweise nur Ereignisse mit dem Schweregrad "Kritisch" aus einem bestimmten Zeitraum zu suchen. Im unteren Bereich der Anzeige findet sich noch der "Best Practices Analyser", der für das Monitoring weitere wichtige Informationen liefert.

Der Server-Manager ersetzt kein reinrassiges Monitoring-System, ist aber insbesondere bei einer geringen Anzahl von Verbundservern durchaus eine Alternative, um nach dem Rechten zu schauen. Die Möglichkeiten des Server-Managers bieten selbst erfahrenen Administratoren Erkenntnisse, die sich im Alltag durchaus als nützlich erweisen.

Eventlog als Datenbasis

Ein Verbundserver ist von Haus aus recht geschwätzig, er schreibt zahlreiche Informationen in das Eventlog und bietet somit eine gute Basis für das Monitoring. Zwar ist es schwierig, bei der Fülle an Informationen die Spreu vom Weizen zu trennen, doch mit etwas Übung und Erfahrung bekommen Sie aber ein Gefühl für die wichtigen Informationen.

Grundlegend lässt sich in den Eigenschaften des ADFS-Servers einstellen, welche Art von Events protokolliert werden sollen. Navigieren Sie hierfür in der ADFS-Verwaltungskonsole mit der rechten Maustaste auf das Element "AD FS" und wählen Sie die Eigenschaften des Verbundservers aus. In den Verbunddiensteigenschaften enthält die rechte Registerkarte mit dem Namen "Ereignisse" die gewünschten Einstellungen.

Es hat sich im Übrigen gezeigt, dass Änderungen an diesen Einstellungen immer nur auf dem primären ADFS-Server gespeichert werden und nicht für die Farm gelten. Wechseln Sie häufiger den primären Server, beispielsweise zu Wartungszwecken, sollten Sie bedenken, dass dann die Einstellungen des neuen Servers gelten und Sie eventuell hier nachjustieren müssen, damit das "Logging" wieder passt. Administratoren, die lieber in der PowerShell agieren, können das Kommando

```
Get-AdfsProperties | select loglevel
```

nutzen, um zu sehen, welche Art von Informationen aktuell protokolliert werden. Das Get-AdfsProperties-Cmdlet sollten Sie auch einmal ohne Parameter ausprobieren, um sich einen Überblick über die Konfiguration des Verbundservers zu schaffen. Sie werden zahlreiche interessante Optionen finden. Das Gegenstück, um den Loglevel zu setzen, lautet übrigens *Set-ADFSProperties* und lässt sich auch automatisiert in einem Skript verwenden. Wenn Sie häufiger die Rolle des primären Servers in einer Farm per Powershell wechseln und auch den Loglevel dabei an aktuelle Bedürfnisse anpassen, ist so ein einheitlicher Stand garantiert.

Protokolle automatisiert auslesen

Suchen Sie konkret nach einer Information oder Ursache eines Problems, ist es sinnvoll, das Ereignisprotokoll von Hand zu durchstöbern. In der täglichen Praxis und in Bezug auf das Monitoring ist dies aber wenig tauglich. Welcher Admin macht schon morgens gerne als Erstes das Eventlog auf, um zu prüfen, ob alles in Ordnung ist? Im administrativen Alltag funktioniert es eigentlich nur automatisiert und zum Glück gibt es die PowerShell.

Ein Cmdlet, um auf das Ereignisprotokoll zuzugreifen, lautet "Get-WinEvent". Mit den entsprechenden Parametern versehen lässt es sich an beliebige Bedürfnisse anpassen. Folgender Befehl beispielsweise listet alle Fehler der vergangenen zwei Tage aus dem ADFS-Log eines Federation-Servers:

```
Get-WinEvent -FilterHashTable
  @{LogName='AD FS/Admin'; Level=2;
  StartTime=(Get-Date).AddDays(-2)}
  -ComputerName adfs2
```

Der Parameter "Level=2" veranlasst das Kommando, nur Einträge mit Fehlern auszugeben. "Level=2,3" listet zusätzlich noch alle Warnungen für den Zeitraum.

Mehr Details zu dem Cmdlet finden Sie im TechNet [3]. Etwa, wie mehrere Computer abgearbeitet werden, um die Logs aller ADFS-Server in der Farm einzusammeln oder auch wie sich Ereignisse zählen lassen, um zu ermitteln, ob überhaupt Einträge vorhanden sind. Das lässt sich beliebig ausbauen. Lassen Sie das Skript in Intervallen durch den Zeitplaner ausführen. Sind Events vorhanden, kann die Reaktion vielfältig sein: Das Erzeugen einer Datei mit den Events beispielsweise, die der Administrator dann auf seinem Desktop findet.

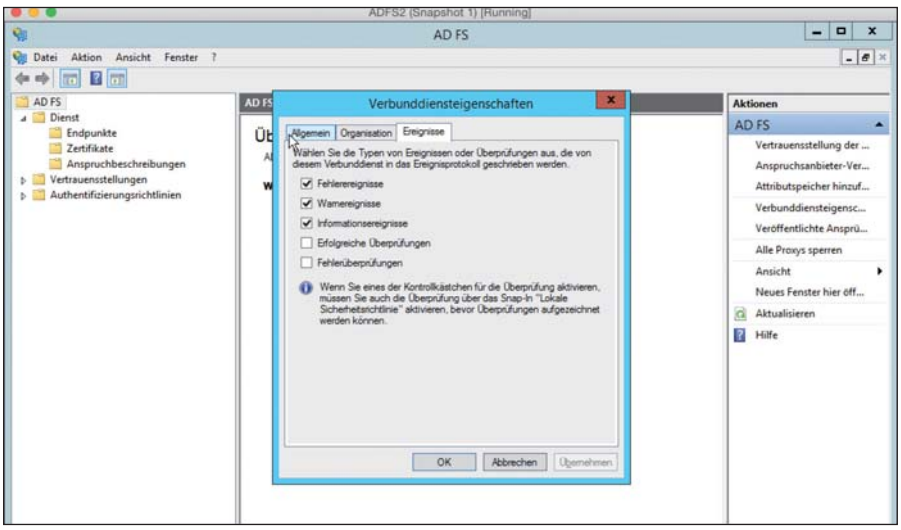


Bild 2: In den Eigenschaften des Federation-Servers lässt sich festlegen, was protokolliert werden soll.

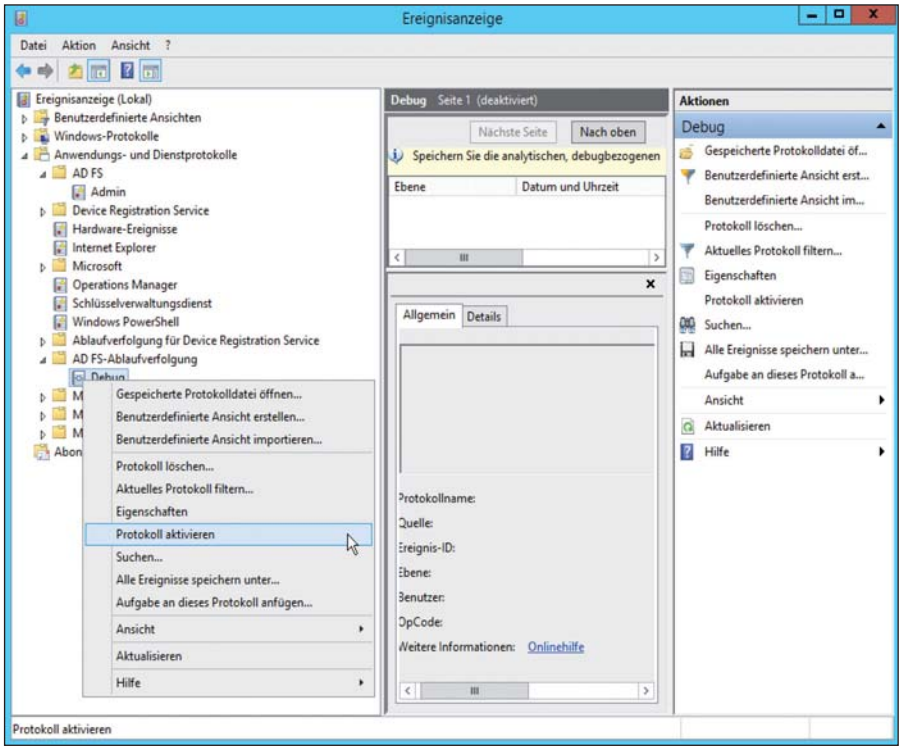


Bild 3: Der letzte Schritt der Konfiguration der Ablaufverfolgung ist die Aktivierung des Protokolls.

Detaillierte Ereignisprotokollierung

Suchen Sie die Ursache für ein Problem und werden in der Ereignisanzeige nicht fündig, kann eine Option sein, das Monitoring aufzumotzen und dem ADFS-Server noch mehr Informationen zu entlocken. Eine Möglichkeit besteht darin, die Ablaufverfolgung einzuschalten. Dazu öffnen Sie auf dem Verbunddienstserver die Datei *Microsoft.IdentityServer.Servicehost.exe.config* im Verzeichnis *C:\Windows\ADFS* und passen Sie den "switchValue" wie in der Datei beschrieben an. Anschließend müssen Sie noch in der Ereignisanzeige im Ansicht-Menü die analytischen Debug-Protokolle einblenden und diese über das Kontextmenü aktivieren.

Das Logging ist auch für den Microsoft-Support hilfreich, um bei der Problemanalyse fündig zu werden. Im Regelbetrieb ist es deaktiviert, da es Ressourcen des Servers verbraucht. Vergessen Sie daher nicht, alle Schritte später wieder rückgängig zu machen, um es zu deaktivieren.

In Umgebungen mit höheren Anforderungen für eine Überwachung der Sicherheit sollten Sie das Protokoll für die Sicherheitseinstellungen einschalten. Auch das finden Sie in der ADFS-Verwaltungskonsole unter "Eigenschaften" im Dialog zu den Eigenschaften des Servers. Ein paar weitere Handgriffe sind noch vonnöten, was genau beschreibt Microsoft in der Technet [4]. Nach erfolgreicher Konfiguration landen alle Einträge im Sicherheitsprotokoll. Gepaart mit dem oben beschriebenen Get-WinEvent-Cmdlet zum Auslesen von Ereignisprotokollen lässt sich eine Liste mit Benutzern, die durch den ADFS-Server authentifiziert worden sind, oder eine Übersicht derer, bei denen es fehlgeschlagen ist, erstellen.

Hilfsmittel zur Diagnose

Microsoft hat eine kleine Bibliothek veröffentlicht, die eine sinnvolle Ergänzung zu den vorhandenen Cmdlets in Windows Server 2012 R2 darstellt. Beim "AD FS Diagnostics Module" [5] stand wohl der Eigennutz für das MS-Supportteam im Vordergrund, um wiederkehrende Analyseaufgaben in ADFS durchzuführen. Dem Administrator soll es recht sein, erhält er doch kostenlos einige gute Werkzeuge an die Hand, auch wenn es keinen offiziellen Support für diese Cmdlets gibt. Die Befehle zeigen sich stabil (auch unter ADFS 3.0) – egal, ob auf einem deutschen oder auf einem englischen Federation-Server.

Die Kommandos sind darauf ausgelegt, einerseits Informationen über die Umgebung einzusammeln und auch um "Health Checks" der wichtigsten Komponenten in ADFS durchzuführen. Beispielsweise ersparen Hinweise zu Zertifikaten, die in naher Zukunft ablaufen, dem Administrator einiges an Ärger. Eines der nützlichsten Cmdlets ist "Test-AdfsServerHealth". Haben Sie einen Trust zu Office 365, wird die Verbindung dorthin auch gleich mit getestet. Es lohnt sich, ein wenig mit den Cmdlets zu spielen, sie bieten gutes Anschauungsmaterial für eigene ADFS-Powershell-Projekte.

Fazit

Verantwortliche für unternehmenskritische ADFS Implementierungen, beispielsweise weil die E-Mails der Anwender in Office 365 liegen und der Zugriff dorthin über einen Federation Trust mit Identitäten aus dem eigenen Active Directory erfolgt, sollten sich solide Gedanken über das Monitoring machen. Treten Probleme in der Federation Server-Farm auf und die Benutzer können nicht authentifiziert werden, ist kein Zugriff auf Office 365 mehr möglich. Gleiches gilt natürlich auch für eine Federation mit einem Partnerunternehmen. Wie kritisch ADFS für Ihr Unternehmen ist und auch wie redundant die Farm ausgelegt ist, ist wichtig, um zu entscheiden, mit welchen Mitteln das Monitoring erfolgt. Dass es nicht immer eine teure Monitoring Suite sein muss, haben wir in diesem Beitrag gezeigt. Und mit etwas programmiertechnischem Eifer und Kenntnissen in PowerShell lassen sich die gezeigten Möglichkeiten noch deutlich erweitern. *(jp)*

[1] System Center Management Pack for Active Directory Federation Services 2012 R2
F3Z21

[2] Plan your AD FS deployment
F3Z22

[3] TechNet zu Get-WinEvent-Cmdlet
F3Z23

[4] Enabling auditing for AD FS
F3Z24

[5] AD FS Diagnostics Module
F3Z25

Link-Codes

Workshop: Open Source-Tools zum Log-Management unter Linux

Ausgesiebt

von Tim Schürmann

Schon in kleinen Netzen spucken die laufenden Dienste zahlreiche Log-Daten aus. Administratoren laufen dann nicht nur Gefahr, eine Fehlermeldung zu übersehen: Einem Problem auf die Spur zu kommen, ähnelt dann auch der Suche nach einer Nadel im Heuhaufen. Die Informationsflut bändigen wollen Fluentd, Graylog2, Logstash und Octopussy.

Werkzeuge zum Log-Management sammeln Log-Daten aus zahlreichen Quellen ein, werfen nicht benötigte Informationen über Bord und bereiten den Rest zur Weiterverarbeitung auf. So lassen sich etwa gezielt die Fehlermeldungen aller im Netz laufenden Apache-Webserver herausfischen. Die dabei zugrunde liegenden Filter-Kriterien gibt der Administrator vor. Je nach Werkzeug klickt er entweder passende Regeln in einer Benutzeroberfläche zusammen oder notiert einen regulären Ausdruck. Die gefilterten und aufbereiteten Daten wandern zur Archivierung in eine Datenbank oder aber weiter in andere Anwendungen. Die komplette Vorgehensweise veranschaulicht Bild 1. Nach diesem Prinzip arbeiten Fluentd, Graylog2, Logstash und Octopussy. Alle vier Werkzeuge werden aktiv weiterentwickelt, stehen unter einer Open Source-Lizenz, können Daten aus mehreren Quellen gleichzeitig anzapfen und lassen sich über Plug-Ins in ihrem Funktionsumfang erweitern. Graylog2, Logstash und Octopussy können zudem die Log-Daten durchsuchen, analysieren und Statistiken erzeugen.

Fluentd

Der "Open Source Data Collector" Fluentd sammelt lediglich die Log-Daten von verschiedenen Quellen ein, filtert die Informationen und leitet den bereinigten Datenbestand weiter [1]. Administratoren dürfen die Ereignisse weder statistisch auswerten noch gezielt durchsuchen. Intern wandelt Fluentd die eingehenden Daten wann immer möglich in das JSON-Format um [2]. Auf diese Weise will das Werkzeug die Weiterverarbeitung vereinheitlichen. Die Entwickler bezeichnen Fluentd daher auch als "Unified Logging Layer".

Die einströmenden Daten kann Fluentd sowohl im Hauptspeicher als auch in Dateien puffern, sodass im Fall der Fälle keine wichtigen Informationen verloren gehen. Darüber hinaus lassen sich mehrere Fluentd-Instanzen starten und sowohl parallel betreiben als auch hintereinanderschalten. Dies erhöht die Ausfallsicherheit und verteilt Lasten. Laut Entwicklerangaben belegt das Werkzeug lediglich 30 bis 40 MByte Hauptspeicher und kann dabei 13.000 Ereignisse in einer Sekunde verarbeiten.

Jedes eingehende Ereignis erhält automatisch ein frei wählbares Tag. Administratoren können über Regeln festlegen, welche Daten mit welchen Tags Fluentd wohin weiterleiten soll. Alternativ lassen sich Ereignisse mit einem neuen Tag versehen und wieder in Fluentd einspeisen. Die Auswahl der Tags geschieht über die Angabe eines Musters. So steht etwa "apache.*" für alle Tags, deren erster Bestandteil der Begriff "apache" ist. Alle Einstellungen nehmen Administratoren in Konfigurationsdateien vor, die denen von Apache ähneln. Mit folgendem Eintrag würde Fluentd beispielsweise all jene Ereignisse in die Log-Datei */var/log/fluent/apache.log* schreiben, deren Tags mit dem Begriff "apache" beginnen:

```
<match apache.*>
  type file
  path /var/log/fluent/apache
</match>
```

Die Syntax der Muster ist allerdings recht limitiert. Wollen Administratoren die Ereignisse mit regulären Ausdrücken aus-

Bild 1: Die Werkzeuge zum Log-Management sind modular aufgebaut und verarbeiten die eingehenden Daten in mehreren Stufen beziehungsweise Schritten.

wählen, müssen sie auf ein entsprechendes Filter-Plug-In zurückgreifen. Weitere bereitstehende Plug-Ins heften unter anderem auch Geo-Informationen an oder anonymisieren die Daten. Plug-Ins können aber nicht nur Daten verändern, sondern auch Datenquellen und Anwendungen anbinden. Auf diese Weise integrieren Administratoren unter anderem die Amazon Web Services, CouchDB, MongoDB, MySQL, Elasticsearch, Statsd oder Graphite. Es gibt sogar ein Plug-In, das die von Fluentd aufbereiteten Informationen via IRC verbreitet. Bislang hat die Community bereits über 300 Plug-Ins entwickelt, die auf [3] zu finden sind.

Wer Fluentd nicht über Konfigurationsdateien einrichten möchte, kann auf die eigens für diese Zwecke entwickelte Weboberfläche Fluentd-UI zurückgreifen [4]. Mit ihr dürfen Administratoren über ihren Browser bequem die Fluentd-Plug-Ins verwalten, den Fluentd-Prozess starten und stoppen, an der Konfiguration schrauben und das Fluentd-Log einsehen (siehe Bild 2). Zugriff auf die Benutzeroberfläche erhält jeder, der den Benutzernamen und das Passwort kennt.

Fluentd ist in der Skriptsprache Ruby geschrieben, zeitkritische Teile sind hingegen in C implementiert. Die Installation erfolgt über den Ruby-eigenen Paketmanager Gem. Fluentd steht unter der Apache-2.0-Lizenz, der Quellcode liegt auf GitHub [5]. Kommerziellen Support für Fluentd bietet die Firma Treasure Data, die derzeit auch maßgeblich die Weiterentwicklung finanziert [6]. Treasure Data stellt zudem unter dem Namen td-agent eine stabile Distribution von Fluentd bereit. td-agent erhält weniger häufig Updates, lässt sich aber in Form eines Deb- oder RPM-Pakets installieren und enthält von Haus aus Startskripte sowie Rezepte für die Konfigurationsmanagement-Software Chef.

Graylog2

Das Werkzeug Graylog2 [7] entstand 2010 als privates Projekt zweier Xing-Mitarbeiter. Mittlerweile entwickelt es die TORCH GmbH aus Hamburg weiter. Die Entwickler versprechen, dass die Verarbeitung der Log-Daten in Echtzeit geschieht, die Suche soll binnen Sekunden die gewünschten Ergebnisse liefern. Graylog2 kann zudem mehrere TByte Daten verarbeiten. Administratoren bedienen Graylog2 wahlweise über die komfortable Weboberfläche aus Bild 3 oder aber über die ebenfalls angebotene REST-Schnittstelle. Letztgenannte erlaubt die einfache Einbindung in Skripte, selbst geschriebene Anwendungen oder Monitoring-Tools.

Graylog2 verdaut von Haus aus Log-Daten im Syslog-Format (gemäß den Standards RFC 5424 und RFC 3164) sowie dem eigenen Graylog Extended Log Format (GELF). Wer ein anderes Format einlesen möchte, muss dessen Aufbau erst definieren. Die Log-Daten möchte Graylog2 per TCP oder UDP angeliefert bekommen, Dateien kann das Werkzeug nicht einlesen. Wer Letzteres benötigt, soll laut Graylog2-Homepage einen Konkurrenten wie Logstash einspannen und dann dessen Ausgaben an Graylog2 übergeben.

Die eintrudelnden Meldungen leitet Graylog2 in sogenannte Streams um. Administratoren dürfen nicht nur beliebig viele dieser Streams erstellen, sondern auch über Regeln festlegen, welche Meldungen in welchen Streams landen sollen. So ließe sich etwa ein Stream erstellen, in den sämtliche Fehler der Datenbank-Server wandern. Eine Nachricht landet dabei in allen Streams, zu deren Regeln sie passt. Die Regeln kann der Administrator recht komfortabel im Webinterface zusammenklicken. Die in die Streams geleiteten Nachrichten lassen sich durchsuchen und können zudem einen Alarm (Alert) auslösen.

Die eingegangenen Daten durchsucht der Administrator mithilfe der Search Query Language, die sich an die Syntax der Suchmaschine Lucene [8] anlehnt. Die Suchanfrage "ssh AND source:example.org" würde beispielsweise alle Meldungen liefern, in denen der Begriff "ssh" auftaucht und die von "example.org" stammen. Solche Suchanfragen müssen Administratoren auch in der Weboberfläche eintippen, zusammenklicken lassen sie sich nicht. Um eine möglichst hohe Antwortgeschwindigkeit zu erzielen, nutzt Graylog2 im Hintergrund Elasticsearch [9].

Für die gefundenen Meldungen generiert Graylog2 auf Wunsch Statistiken und Diagramme (Bild 4) oder exportiert sie als CSV-Tabelle. Die Statistiken können zudem sogenannte Widgets anzeigen, die sich wiederum auf Übersichtsseiten, den sogenannten Dashboards, gruppieren lassen. Auf diese Weise haben Administratoren die wichtigsten Informationen direkt nach dem Login im Blick.

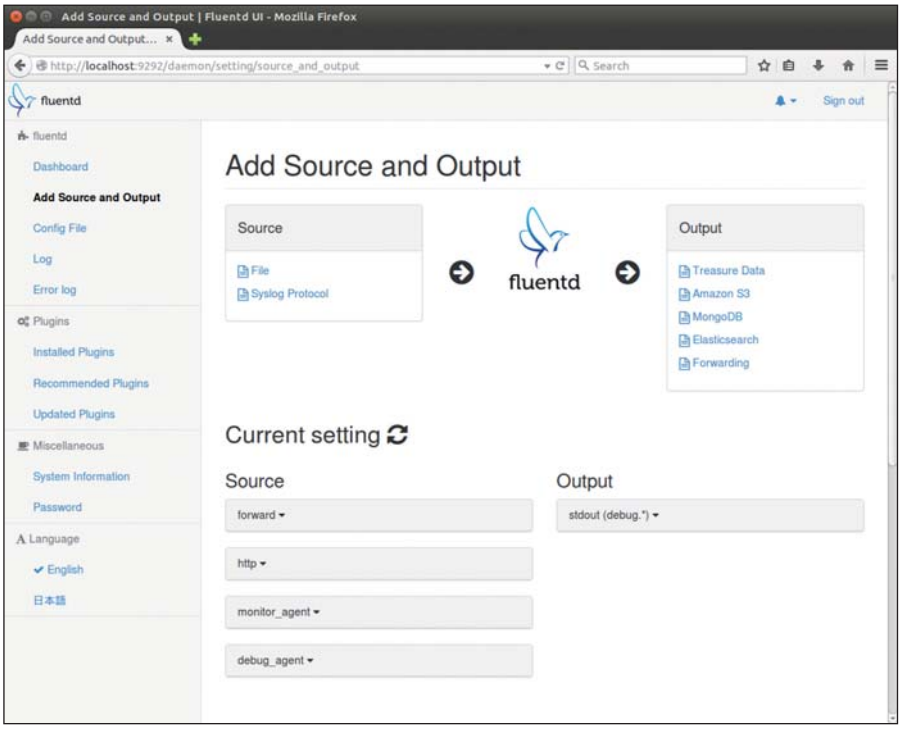


Bild 2: Mit der Fluentd-UI lassen sich schnell neue Quellen und Outputs einrichten.

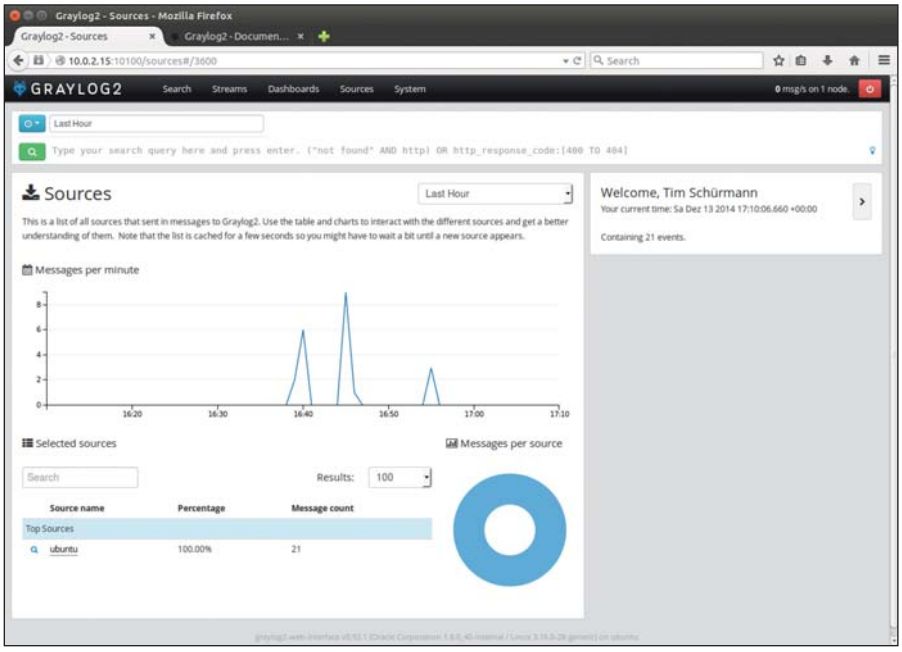


Bild 3: Die Weboberfläche von Graylog2 liefert auch statistische Daten, wie hier die Anzahl der von einer Quelle angelieferten Meldungen.

Graylog2 besitzt eine einfache Benutzerverwaltung, über die der Administrator weiteren Personen eingeschränkten Zugriff auf die Log-Daten und Statistiken gewähren kann. Die Authentifizierung geschieht dabei entweder über einen Benutzernamen und Passwort oder via LDAP. Graylog2 unterscheidet dabei nur zwischen Mitlesern und Admins. Während erstgenannte Gruppe lediglich ausgewählte Informationen und Statistiken zu Gesicht bekommt, dürfen Admins auf sämtliche Funktionen zugreifen.

Die TORCH GmbH [10] stellt fertige Pakete für Ubuntu, Debian und CentOS bereit. Zusätzlich gibt es fertige Appliances für Amazon Web Services und Vagrant sowie Docker-Images. Darüber hinaus bieten die Entwickler Anleitungen für eine Installation via Puppet und Chef an. Für Einsteiger existiert ein Quick Setup Tool, mit dem sich Graylog2 samt aller Abhängigkeiten schnell einrichten und ausprobieren lässt.

Graylog2 steht unter der GPLv3-Lizenz, den Quellcode des Werkzeugs und der Weboberfläche stellen die Entwickler jeweils als Archiv zur Verfügung. Zusätzlich gibt es noch graylog2-radio, das vor Graylog2 geschaltet die eingehenden Log-Daten in einer Queue sammelt. Graylog2 ist in Java geschrieben und benötigt neben dem erwähnten Elasticsearch zwingend die Datenbank MongoDB. Ohne Installation ausprobieren lässt sich Graylog2 mit einer Online-Demo, die jedoch eine Registrierung voraussetzt.

Logstash

Logstash ist Teil des Elasticsearch-Projektes und steht unter der Apache 2.0-Lizenz [11]. Das Werkzeug ist in JRuby geschrieben und benötigt daher eine möglichst aktuelle Java-Laufzeitumgebung. Intern delegiert Logstash jede einzelne Aufgabe an ein entsprechendes Plug-In. So liest etwa ein Plug-In die Log-Daten aus einer Sqlite-Datenbank, während ein weiteres anhand der IP-Adressen noch Geo-Informationen hinzufügt, bevor ein drittes die so aufbereiteten Daten in eine CSV-Datei schreibt. Die Plug-Ins teilen sich abhängig von ihrer Aufgabe in vier Gruppen ein: Input-Plug-Ins lesen Daten ein, Codec-Plug-Ins wandeln Daten in andere Formate um, Filter ändern oder reduzieren die Informationen, während Output-Plug-Ins die Log-Daten speichern oder an andere Stellen weiterleiten.

Wann welche Plug-Ins zum Einsatz kommen, bestimmt der Administrator über eine Konfigurationsdatei. Ein einfaches Exemplar zeigt Listing 1: Mit ihr nimmt zunächst das Input-Plug-In "stdin" Daten von der Standardeingabe entgegen. Dann wandelt ein weiteres Plug-In jede Zeile in das JSON-Format um ("codec => json"). Schließlich schreibt das Output-Plug-In "stdout" diese Daten wieder auf die Standardausgabe.

Logstash erlaubt dabei auch Bedingungen. So lässt sich etwa per "if [path] =~ "error"" prüfen, ob der Dateiname eines Logs die Zeichenkette "error" enthält. Besonders nützlich ist auch der mitgelieferte Grok-Filter, der unter anderem die angelieferten Daten in ein einheitliches Format presst und überflüssige Informationen wegschneidet. Der Multiline-Filter wiederum kann mehrere Zeilen aus einem Log zu einem

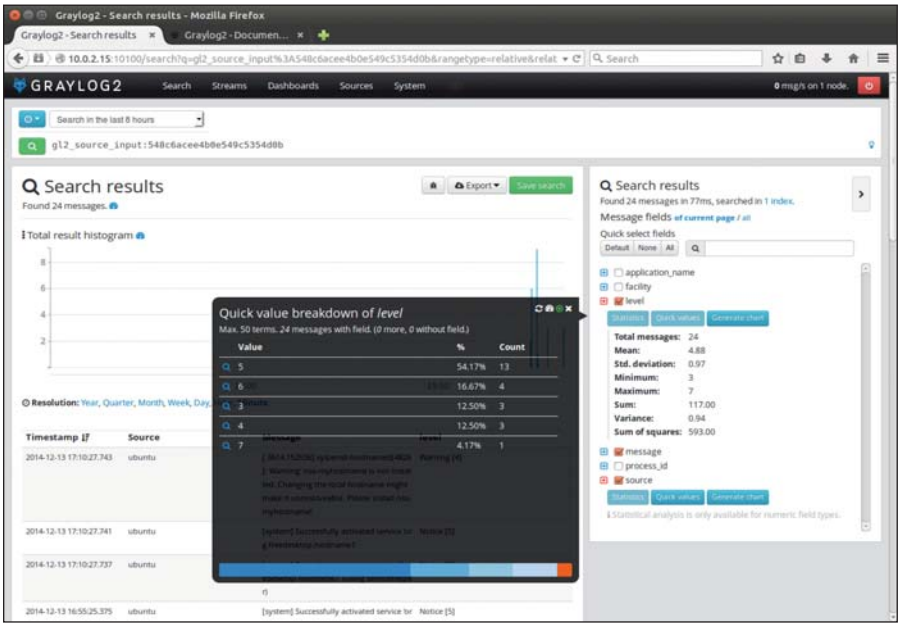


Bild 4: Die hier von Graylog2 gefundenen Ereignisse waren überwiegend als Level 5 klassifiziert.

Ereignis zusammenfassen. Zum Lieferumfang von Logstash gehören unter anderem auch Input-Plug-Ins, die Ereignisse von RabbitMQ oder Redis entgegennehmen. Als Datenspeicher kommt bevorzugt Elasticsearch zum Einsatz, wobei sich Logstash automatisch um dessen Einrichtung kümmert. Mitgelieferte Output-Plug-Ins binden aber unter anderem auch Nagios, Graphite oder Statsd ein.

Logstash selbst bringt keine Weboberfläche mit, Administratoren können jedoch Kibana aus dem Elasticsearch-Projekt verwenden [12]. Dieses Frontend für Elasticsearch setzt jedoch voraus, dass Logstash dort die aufbereiteten Daten ablegt. Neben einer Suchfunktion stellt Kibana ein Dashboard bereit, das direkt wichtige Statistiken liefert und sich vom Administrator an die eigenen Bedürfnisse anpassen lässt. Ein eigenes Repository führt die Plug-Ins von Drittentwicklern [13].

Octopussy

Octopussy [14] steht unter der GNU GPLv3, der Quellcode liegt auf Github [15]. Octopussy erkennt von Haus aus zahlreiche verschiedene Log-Formate, darunter das des BIND-Nameservers, des Linux-Kernels, des Squid-Proxys, von PostgreSQL oder Cisco-Geräten. Weitere Formate lassen sich Octopussy nachträglich beibringen. Intern verarbeitet das Werkzeug allerdings nur Syslog-Meldungen.

Die Bedienung von Octopussy erfolgt über eine Weboberfläche, die sich über Themes optisch anpassen lässt. Eine Anmeldung erfolgt wahlweise mit Benutzername und Passwort oder aber über einen LDAP-Server. Auf Wunsch spricht die Benutzeroberfläche Deutsch. Im Test führte ein Umschalten der Sprache jedoch zu fehlerhaften Übersetzungen.

```
input {
   stdin { }
}

output {
   stdout {
            codec => json
   }
}
```

Listing 1: Beispiel für eine einfache Logstash-Konfiguration

In der Weboberfläche legt der Administrator zunächst sogenannte Geräte an, von denen Octopussy die Logs einsammeln soll. Mehrere Geräte lassen sich dabei in einer Gruppe zusammenfassen. Erst in einem zweiten Schritt bestimmt der Administrator, welche Log-Daten Octopussy von einem Gerät abholen und verarbeiten soll. Mit einem Mausklick lässt sich das Einsammeln der Informationen anhalten und fortsetzen. Auf Basis der vom Administrator eingerichteten Geräte kann Octopussy eine Karte der Server-Architektur erstellen. Die von den Geräten abgeholten Log-Daten lassen sich filtern und in Reports zusammenfassen. Auch hier klickt der Administrator jeweils die entsprechenden Kriterien in der Weboberfläche zusammen. Reports lassen sich zeitgesteuert auf Basis von Vorlagen (Themes) erstellen und dann als E-Mail verschicken oder aber via FTP und SCP auf einen Server schieben. Treten wichtige Ereignisse ein, alarmiert Octopussy auf Wunsch seinen Administrator per E-Mail, Jabber, Nagios oder Zabbix_sender.

Octopussy ist in Perl geschrieben, benötigt neben der Skriptsprache aber noch viele weitere Softwarepakete. Dazu zählen unter anderem Apache, MySQL, das RRDTool, Rsyslog und htmldoc. Über die Installationsanleitung hinausgehende Informationen liefert die Dokumentation nicht, die Bedienung müssen sich Administratoren mit der kargen Online-Hilfe selbst beibringen. Als Stolperstein erweisen sich Sicherheitsframeworks wie SELinux oder AppArmor, die den Betrieb von Octopussy behindern können.

Fazit

Alle vier Log-Management-Tools lösen ihr Versprechen ein: Sie sammeln aus unterschiedlichen Quellen brav Log-Daten, filtern diese und reichen sie weiter. Die Unterschiede liegen wie so oft im Detail.

Fluentd ist äußerst leichtgewichtig und auf Hochverfügbarkeit ausgelegt. Im Gegenzug bietet es keinerlei Analyse-Tools. Es eignet sich daher als flinker Datensammler in größeren Netzen, der die gefilterten Informationen einem weiteren Tool zukommen lässt. Die Weboberfläche dient im Wesentlichen nur als hübscher Editor für die Konfigurationsdatei.

Graylog2 lockt mit einer schnellen Installation und einer schicken Weboberfläche, nimmt die Log-Daten standardmäßig aber nur via TCP oder UDP entgegen. Die Datenabfrage erfolgt zudem mit einer eigenen Sprache. Im Gegenzug ist eine recht flexible Auswertung und Suche möglich.

Logstash glänzt dank des erhältlichen Buchs mit umfangreicher Dokumentation. Komplexere Konfigurationsdateien wirken jedoch etwas unübersichtlich. Als Teil des Elasticsearch-Projekts arbeitet es besonders gut mit den anderen dort entwickelten Komponenten zusammen.

Nutzer von Octopussy benötigen mangels Dokumentation Experimentierfreude. Die Weboberfläche wirkt veraltet und ist umständlich in der Bedienung. Immerhin kann Octopussy zeitgesteuert Reports erstellen. *(of)*

Link-Codes

[1] Fluentd
F3Z51

[2] Wikipedia-Eintrag zu JSON
F3Z52

[3] Fluentd-Plug-Ins
F3Z53

[4] Fluentd-UI
F3Z54

[5] Quellcode von Fluentd
F3Z55

[6] Treasure Data, Inc.
F3Z56

[7] Graylog2
F3Z57

[8] Apache Lucene
F3Z58

[9] Elasticsearch
F3Z59

[10] Support für Graylog2
F3Z50

[11] Logstash
F3Z5A

[12] Kibana
F3Z5B

[13] Plug-Ins für Logstash
F3Z5C

[14] Octopussy
F3Z5D

[15] Quellcode von Octopussy
F3Z5E

Workshop: Eclipse SCADA

Industrielle Datenverarbeitung

von Dr. Holger Reibold

In produzierenden Unternehmen kommen die unterschiedlichsten Geräte, Computersysteme, Hard- und Software sowie Sensoren zum Einsatz. Dabei geht es primär um die Überwachung industrieller und technischer Prozesse. Mit Eclipse SCADA schickt sich eine freie Lösung an, den Markt der Software-Produkte für das Überwachen und Steuern dieser Prozesse aufzumischen.

Quelle: onizu3d – 123RF

Das Akronym SCADA steht für "Supervisory Control and Data Acquisition" und markiert in vielen Unternehmen die Trendwende hin zu einer einheitlichen Umgebung für das Monitoring und die Steuerung von Industrieprozessen. SCADA-Systeme gehören zur Kategorie der Industrial Control Systems, kurz ICS, die der Überwachung und Kontrolle von Industrieprozessen dienen. Nun zeigt sich in der Praxis allerdings, dass die klassischen ICS-Systeme meist nur für sehr spezifische Aufgaben konzipiert sind und schon am Monitoring anderer Unternehmensvorgänge scheitern – von fehlenden Remote Control-Möglichkeiten einmal ganz zu schweigen.

An diesem Punkt setzt Eclipse SCADA an. Vereinfacht ausgedrückt besteht das primäre Ziel der freien Umgebung in der Verbindung unterschiedlicher industrieller Geräte über ein einheitliches Kommunikationssystem, um die darauf ausgeführten Prozesse zu steuern und die Daten zu visualisieren. Konzeptionell ist Eclipse SCADA sehr flexibel ausgelegt. Für die Umgebung macht es prinzipiell keinen Unterschied, ob die Daten von einem einfachen Sensor oder einer komplexen Produktionsanlage stammen. Zum Einsatz kommen überwiegend skalare Werte anstelle komplexer Datenstrukturen. Überall dort, wo es notwendig ist, werden Datenstrukturen in mehrere skalare Werte gesplittet. Dadurch beschleunigt sich die Datenverarbeitung und allgemeine Verarbeitungsmechanismen können eingesetzt werden.

Stammen die Daten beispielsweise von einer Wetterstation, könnte diese als Rohdaten die Temperatur und die Sonnenscheindauer liefern. Dabei handelt es sich um zwei Fließkommawerte, die unabhängig voneinander verarbeitet werden. Dennoch lässt sich auf beide das gleiche Alarmschema anwenden. Den Werten kann dann beispielsweise eine Qualitätsinformation und/oder ein Hinweis zugewiesen werden, die bei Erreichen bestimmter Grenzwerte an den Benutzer über eine Schnittstelle ausgegeben wird. Dabei lässt sich das identische Visualisierungsschema nutzen. Nach diesem Prinzip verarbeitet Eclipse SCADA die verschiedensten Quelldaten.

Zwei Ebenen einer SCADA-Umgebung

In der Industrie sind SCADA-Systeme längst Realität. Als Netzleitsysteme dienen Sie vorwiegend der Überwachung, aber auch Steuerung und Optimierung von Industrieanlagen. Sie kommen bei Windkraftwerken, energieerzeugenden und verteilenden Anlagen, in der Wasseraufbereitung oder in den Smart Grids zum Einsatz. Auch werden sie in Telekommunikationseinrichtungen, Chemieanlagen, Anlagen für die Stahlerzeugung oder in der PKW-Produktion verwendet. Die Steuerung und Regelung vieler Systeme wie beispielsweise einer Windenergiean-

lage funktioniert automatisiert und ein Eingreifen der Betreiber oder Hersteller ist nur selten notwendig, weshalb der SCADA-Fokus auf der Überwachung liegt.

Mit Hilfe von SCADA-Systemen können Sie also aus den Quellsystemen relevante Daten in eine Art Überwachungszentrale übertragen. SCADA-Systeme sind in der Lage, die gesammelten Informationen nach definierbaren Kriterien zu bewerten und in Falle von Fehlersituationen diese in einem logischen Kontext darzustellen. Prinzipiell können SCADA-Systeme eine recht einfache Architektur besitzen, wenn sie beispielsweise "nur" die Umgebungsbedingungen eines vernetzten Einfamilienhauses überwachen, aber es sind natürlich auch höchst komplexe Architekturen denkbar, mit denen sie beispielsweise ein Heizkraftwerk überwachen. Theoretisch kann ein solches Überwachungssystem mehrere Hundert bis mehrere Hunderttausend I/O-Kanäle verwenden.

Eine SCADA-Umgebung kennt zwei Ebenen: Auf der Client-Ebene findet die Mensch-Maschinen-Interaktion und auf der Daten-Server-Ebene das eigentliche Monitoring statt. Die Kommunikation innerhalb von SCADA-Systemen erfolgt auf TCP/IP-Basis. Doch das genügt natürlich nicht, um mit den verschiedensten Quellen kommunizieren zu können. Welche Protokolle beispielsweise für den Datenaustausch mit Feldbussystemen zum Einsatz kommen, ist von Umgebung zu Umgebung unterschiedlich.

Zwar gibt es Bestrebungen, die Kommunikation insbesondere in der Automatisierungstechnik zu standardisieren – Stichwort OPC (OLE for Process Control) –, doch ist die Praxis noch weit davon entfernt und gekennzeichnet von proprietären Protokollen. Immerhin: Offene Protokolle wie Modbus erfreuen sich großer Beliebtheit. Über spezielle Gateways lässt sich zudem die Kommunikation vereinfachen. Damit Eclipse SCADA überhaupt mit den unterschiedlichen Systemen kommunizieren und deren Daten einsammeln kann, benötigt es Kommunikationsschnittstellen. Die werden durch spezielle Treiber realisiert – ähnlich den Software-Treibern auf PCs. Bislang gibt es folgende Treiber:

- Exec
- JDBC
- Modbus
- SNMP
- OPC
- Proxy

Eclipse SCADA mit drei Kernfunktionen

Das Grundprinzip von Eclipse SCADA ist kein neues – im Gegenteil –, denn Sie begegnen ihm in jeder Netzwerkmonitoring-Umgebung: das Aggregieren und Konsolidieren von Daten, damit diese dem Administrator oder Benutzern in einer verständlichen Form präsentiert werden. Eclipse SCADA muss natürlich flexibel ausgelegt sein, um mit den unterschiedlichen Quellen kommunizieren zu können. Das System stellt Ihnen drei Kernfunktionen bereit:

- DA (Data Access): Das Sammeln von Prozessdaten, möglichst in Echtzeit.
- AE (Alarms &Events): Die Überwachung der DA-Informationen, deren Auswertung und gegebenenfalls Ausgabe von Warnungen.
- HD (Historical Data): Das Speichern der gesammelten Daten über einen längeren Zeitraum hinweg.

Die wichtigste Aufgabe des DA-Moduls ist das Einlesen von Daten aus unterschiedlichsten Datenquellen, die dann der Auswertung und Visualisierung zugeführt werden können. Angenommen, die Quelldaten stammen von einer Wetterstation und beinhalten Werte über die Windrichtung und -geschwindigkeit und verschiedene weitere mögliche Parameter wie Temperatur oder Luftfeuchtigkeit, generiert das System daraus analoge Werte. Die Struktur ergibt sich dabei durch einen Namespace anstelle einer Datenstruktur. Das sorgt für eine deutlich einfachere Verarbeitung, da Sie alle Werte gleichberechtigt behandeln können. Ein weiterer Vorteil: Benötigen Sie für eine Anwendung lediglich einen spezifischen Wert, können Sie nur diesen herauspicken.

Durch die umfangreichen sowie flexiblen Datenzugriffs- und Einlesemöglichkeiten ist es also recht einfach, ein System zu implementieren, das beim Erreichen bestimmter Schwellenwerte Alarm schlägt. Das Eclipse SCADA-System besitzt eine weitere wichtige Komponente: das VI (Visual Interface), das auf Draw2D basiert und die GUI-Komponenten für die Visualisierung zur Verfügung stellt. Ursprünglich wurde dieses System als OpenSCADA entwickelt, wird aber seit geraumer Zeit unter dem Dach der Eclipse Foundation weiterentwickelt.

Erste Gehversuche

Damit Sie das Eclipse SCADA-System bequem kennenlernen können, hat das Entwicklerteam ein Demosystem realisiert, auf das Sie mit einem lokalen Admin-Client zugreifen können. Dazu laden Sie sich zunächst den Eclipse SCADA Admin Client [1] für das jeweilige Betriebs-

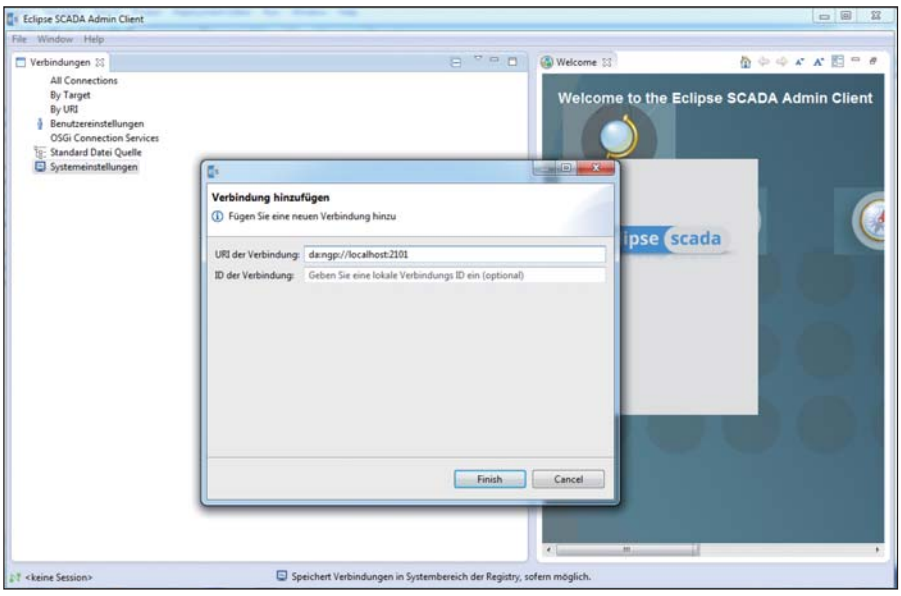


Bild 1: Mit dem Eclipse SCADA Admin Client können Sie auf das Demo-System zugreifen und so erste Schritte unternehmen.

system herunter. Im Download-Bereich finden Sie den Client für Linux, Mac OS X und Windows. Starten Sie als Nächstes den Client und erzeugen Sie eine neue Verbindung. Dazu klicken Sie mit der rechten Maustaste auf "Systemeinstellungen" und wählen "Neue Verbindung …". Als URL verwenden Sie *da:ngp://scada.eclipse.org:2101*. Weisen Sie der Verbindung außerdem eine ID zu und speichern Sie diese mit einem Klick auf "Finish".

Nun können Sie mit einem Doppelklick auf den Verbindungseintrag eine Verbindung zu dem SCADA-Server herstellen. Als Benutzernamen verwenden Sie "guest", als Passwort "guest12". Dann navigieren Sie im Verzeichnisbaum zum Eintrag "LUX.V". Wie Sie der Eclipse-basierten Umgebung entnehmen können, umfasst das Beispiel-Setup vier Knoten:

- scada.eclipse.org: Hierbei handelt es sich um den Hauptserver, der die Middleware und das Wertearchiv hostet.
- demo.openscada.org: Der zweite Server hostet ebenfalls die Middleware und das Archiv. Es handelt sich um einen Klon von "scada.eclipse.org".
- ostest1.muc.ibhmgt.de: Dieser Server hostet den Arduino-Treiber.
- arduino: Hierbei handelt es sich um das Arduino-Board.

Die Verbindung von "scada.eclipse.org" und seinem Klon zum Server "ostest1" findet über das DA/NGP-Protokoll und TCP/IP statt. Die Aufgabe des Arduino-Treibers ist es, über die Ethernet-Schnittstelle die Daten von dem Board zu lesen. Ein Treiber besteht üblicherweise aus zwei Teilen: Dem "Auffangkorb" der Daten und dem Protokoll-Exportmechanismus. Da in der Industrie Modbus ein weit verbreitetes BUS-System ist, stellt die Demoversion ein entsprechendes Modul zur Verfügung, wobei "scada.eclipse.org" als Modbus-TCP-Slave agiert. Über einen speziellen Demo-Client können Sie die verschiedenen Werte und die Auswertung des Beispiel-Arduino-Systems in Echtzeit verfolgen.

SCADA-Projekte selbst entwickeln

Das Demo-System bietet Ihnen bereits einen unkomplizierten Einstieg in die Welt von Eclipse SCADA. Mit überschaubarem Aufwand können Sie bei Bedarf aber auch eine lokale Entwicklungsumgebung aufsetzen. Dabei müssen Sie zunächst dafür sorgen, dass Ihr Rechner über eine aktuelle Java-Installation verfügt. Als Nächstes laden Sie sich die Eclipse-Entwicklungsumgebung herunter. Dazu laden Sie sich aus dem Download-Bereich der Eclipse-Projektseite [1] die aktuellste Programmversion herunter und installieren diese. Wenn Sie unter Windows entwickeln möchten, ist außerdem die Installation des WIX-Toolsets [2] erforderlich. Nach dem Download starten Sie die zugehörige EXE-Datei und führen über den WIX-Toolset-Dialog mit einem Klick auf "Install" die Installation durch.

Der nächste Schritt dient der Installation des SCADA-Plug-Ins in der Eclipse-Umgebung. Nach dem Download entpacken Sie das Archiv und starten Eclipse. Über den Menübefehl "Help / Install New Software" installieren Sie das SCADA-Plug-In. Dazu geben Sie im Eingabefeld "Work with" die URL zum Eclipse SCADA-Repository an. Nach einer kurzen Suche werden gefundene Einträge in dem Listenfeld ausgegeben. Aktivieren Sie zumindest den Eintrag "Eclipse SCADA IDE" und klicken Sie auf "Next". Sie müssen der Auswahl ein weiteres Mal zustimmen und können anschließend die SCADA-IDE als Eclipse-Modul installieren. Möchten Sie mit einem lokalen Server spielen, sollten Sie außerdem die Installation der Server-Komponente aktivieren. Nach einem Neustart von Eclipse steht Ihnen die Entwicklungsumgebung samt SCADA-Plug-In zur Verfügung.

Damit sind die Vorbereitungen für das Erstellen eines eigenen SCADA-Projektes geschafft. Um nun ein Projekt anzulegen, führen Sie in Eclipse den Befehl "New / Other / Eclipse SCADA Configuration / Configuration Project" aus. Weisen Sie dem ersten Testprojekt eine Bezeichnung zu. Um das Erstellen des Grundgerüstes Ihres ersten SCADA-Projekts kümmert sich Eclipse. In diesem Beispielsprojekt sind bereits einige grundlegenden Funktionalitäten implementiert.

Die Datei *nodeMapping.esdi* kann beispielsweise die IP-Adresse von Knoten durch eine andere ersetzen. Das ist beispielsweise praktisch, um bestimmte Konfigurationen zu testen. Die Deployment-Artifakte erzeugen Sie, in dem Sie eine Recipe-Datei *productive.recipe* mit der rechten Maustaste markieren und dann aus dem Untermenü "Eclipse SCADA Configuration" den Befehl "Recipe" ausführen.

Verbindung zu Modbus-Devices

Modbus ist in der Industrie ein weitverbreitetes Bus-System. Mit der zuvor angelegten Entwicklungsumgebung können Sie die Integration eines solchen Systems simulieren. Die praktische Vorgehensweise unterscheidet sich bei realen Modbus-Systemen dabei nicht, aber für ein erstes Kennenlernen ist das auf jeden Fall ausreichend.

Eine SCADA-Konfiguration besteht im Wesentlichen aus zwei Dateien: dem In-

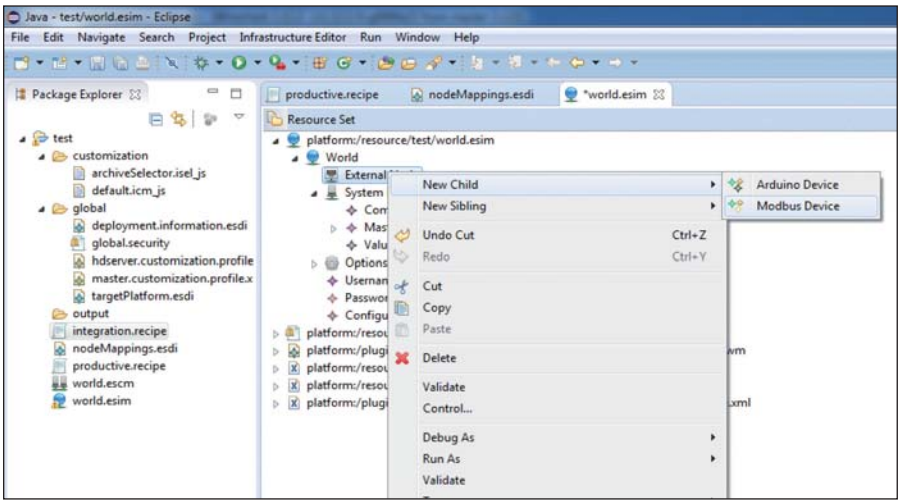


Bild 2: Mit Hilfe von Eclipse SCADA ist es für routinierte Anwender einfach, Systeme in die Überwachung zu integrieren.

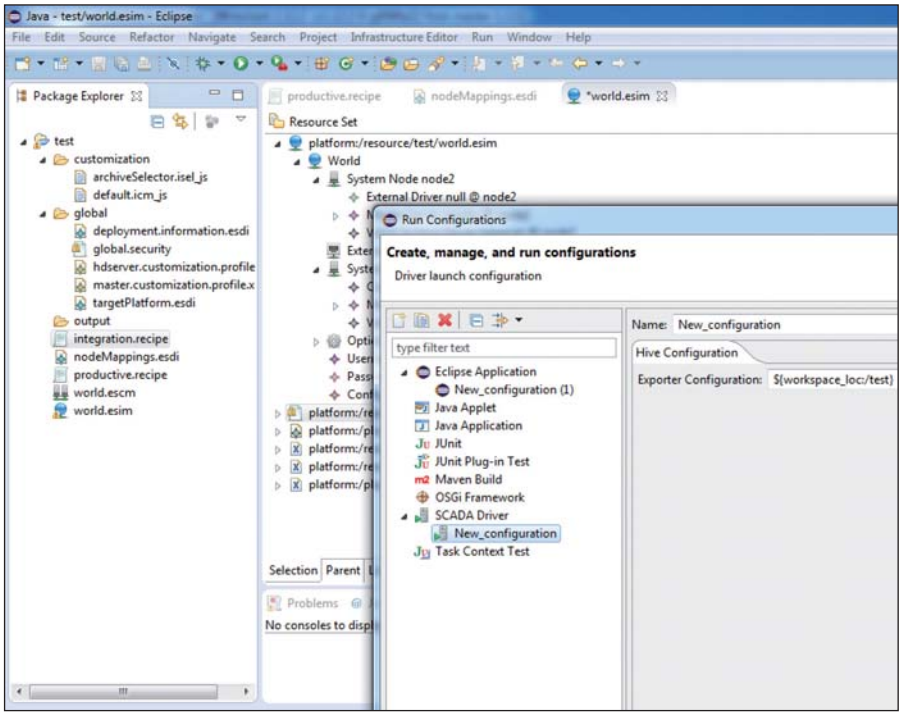


Bild 3: Das SCADA-Plug-In erlaubt die lokale Simulation von Konfigurationen, die beispielsweise Daten über Modbus beziehen.

frastruktur- und dem Komponentenmodell. Das Infrastrukturmodell ist in Form der Datei *world.esim* implementiert. Diese öffnen Sie in Eclipse. Innerhalb der Struktur erzeugen Sie mit Hilfe der rechten Maustaste einen neuen Knoten ("New Child / Externe Node"). Weisen Sie diesem neuen Knoten wieder mit einem Rechtsklick ein Modbus-Device zu. Als Nächstes bearbeiten Sie dessen Einstellungen und weisen diesem eine Bezeichnung zu. Sie sollten außerdem einen 16 Bit-Integerwert und eine Variable angeben.

Der nachfolgende Schritt dient dem Anlegen eines Slave-Knotens. Modbus verwenden wir in diesem Beispiel dazu, um von diesem Knoten Daten abzurufen. Es gibt ein Startregister und Sie können festlegen, wie viele weitere Register abgerufen werden sollen. In der Eclipse SCADA-Terminologie sind dies die sogenannten "Blocks". Sie können für jeden dieser Blöcke festlegen, wie häufig sie abgerufen werden. Typische Werte sind 250 und 10.000 Millisekunden für den Timeout-Wert.

Das SCADA-Plug-In stellt Ihnen außerdem über das Kontextmenü der rechten Maustaste verschiedene Standardtreiber zur Verfügung. Der muss noch dem zu überwachenden Knoten zugewiesen werden. Um die angelegte SCADA-Konfiguration auszuführen, markieren Sie die Datei *productive.receipe* und führen den Befehl "Run As / Run Configurations" aus. Im gleichnamigen Dialog finden Sie die zuvor angelegte Konfiguration. Markieren Sie diese und starten Sie die Ausführung mit einem Klick auf "Run". Die Ausgabe der Modbus-Simulation finden Sie anschließend im "Output"-Verzeichnis.

Fazit

Mit Eclipse SCADA steht Unternehmen eine interessante und vielversprechende Entwicklungsumgebung für das Erstellen von typischen SCADA-Applikationen zur Verfügung. Bislang befindet sich das Tool noch in einer sehr frühen Entwicklungsphase, doch unter dem Dach der Eclipse Foundation stehen die Zeichen gut, dass die Weiterentwicklung in großen Schritten erfolgen wird. *(dr)*

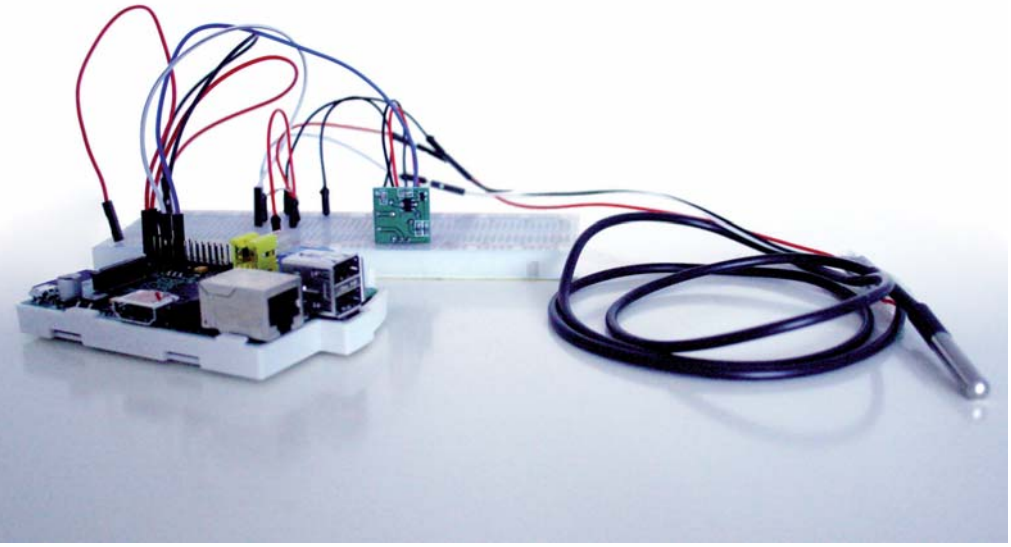
[1] Eclipse SCADA Admin Client
F3Z11

[2] WIX-Toolset
F3Z12

Link-Codes

Workshop: Serverraumüberwachung mit dem Raspberry Pi

Marke Eigenbau



von Thomas Rose

Die kleinen und günstigen Raspberry Pis bestechen durch ihre Flexibilität. Mit einigen grundlegenden Programmierkenntnissen lassen sich die Mini-Rechner auch im Unternehmen sinnvoll einsetzen. In diesem Workshop zeigen wir Ihnen, wie Sie einen Raspi für die Temperaturüberwachung im Serverraum nutzen. Wird es zu heiß, startet das System einen Ventilator und schlägt per E-Mail Alarm.

Zunächst benötigen wir für unser Überwachungssystem einen Raspberry Pi. Diesen gibt es in den Varianten A, B, B+ und 2. In diesem Workshop verwenden wir das Modell B. Sie können die Anleitung aber problemlos auch für die Modelle B+ und 2 verwenden, da alle verwendeten GPIO-Anschlüsse bei diesen Modellen identisch sind. Zudem benötigen Sie eine SD-Karte mit mindestens 4 GByte Speicher für das Betriebssystem, eine Stromversorgung via Mini-USB sowie ein Ethernet-Kabel. Bei einschlägigen Händlern gibt es Raspberry Starter Kits für um die 80 Euro, die auch eine Steckplatine und Drahtbrücken beinhalten, die wir später noch brauchen werden.

Installation des Betriebssystems

Als Betriebssystem für den Raspberry verwenden wir das auf Debian basierende Raspbian. Laden Sie sich ein Raspbian-Image unter [1] herunter und klonen Sie es mit Hilfe der Software Win32Disk-Imager auf eine SD-Karte. Sobald sich das Betriebssystem auf der Karte befindet, fügen Sie alle Komponenten zusammen: die SD-Karte kommt in den Slot und ein Ethernetkabel in die entsprechende Buchse. Weil der Raspi über keinen Ein- und Ausschalter verfügt, bootet er automatisch, sobald Sie ihn über die Mini-USB-Buchse mit Strom versorgen. 50 Sekunden später ist das System hochgefahren.

Über die Routersoftware in Ihrem Netzwerk finden Sie die IP-Adresse des Raspi heraus und verbinden sich erstmalig über Putty oder ssh mit ihm. Als Benutzername ist "pi" voreingestellt, das Passwort lautet "raspberry". Dieses Standardpasswort sollten Sie natürlich umgehend ändern. Dazu benötigen Sie den Befehl *passwd*. Noch sicherer wird der Remote-Zugang zum Raspberry übrigens mit einem SSH-Key, den Sie in wenigen Minuten selbst erstellen können. Unter [2] finden Sie im Netz die entsprechende Anleitung.

Temperatursensor anschließen

Als Temperatursensor dient ein DS18B20 (siehe Bild 1), den Sie für wenige Euro bestellen können. Den Sensor gibt es in verschiedenen Bauformen – die Ausführung mit Kabel ist besonders praktisch, wenn Sie den Sensor an unterschiedlichen Stellen platzieren möchten. Der Aufbau der Schaltung ist denkbar einfach: Sie benötigen dazu eine Steckplatine, ein paar Steckbrücken männlich/männlich und männlich/weiblich sowie einen Widerstand von 680 Ohm. Stecken Sie die Schaltung dann so wie in Bild 2 dargestellt. Das von uns verwendete Raspbian hat alle nötigen Treiber bereits an Bord, diese sind aber noch nicht geladen. Das holen Sie mit den Befehlen

```
sudo modprobe w1_gpio
sudo modprobe w1_therm
```

nach. Mit *sudo* geben Sie sich als Superuser (Admin) zu erkennen, der Befehl *modprobe* lädt die gewünschten Kernelmodule nach. Damit diese Module bei einem Neustart automatisch geladen werden, hängen Sie sie an die Datei */etc/modules* an. Mit

```
sudo nano /etc/modules
```

öffnen Sie die Datei im Editor nano. Anschließend fügen Sie am Ende die Zeilen

```
w1-gpio
w1-therm
```

an, speichern mit der Tastenkombination "Strg + O" die Datei und mit "Strg + X" verlassen Sie den Editor wieder.

Schauen wir uns nun an, welche Daten der Sensor liefert. Nach der Unix-Philosophie "Alles ist eine Datei" speichert er seine Daten in einer Datei ab. Die finden Sie im Verzeichnis */sys/bus/w1/devices*, wohin Sie mit

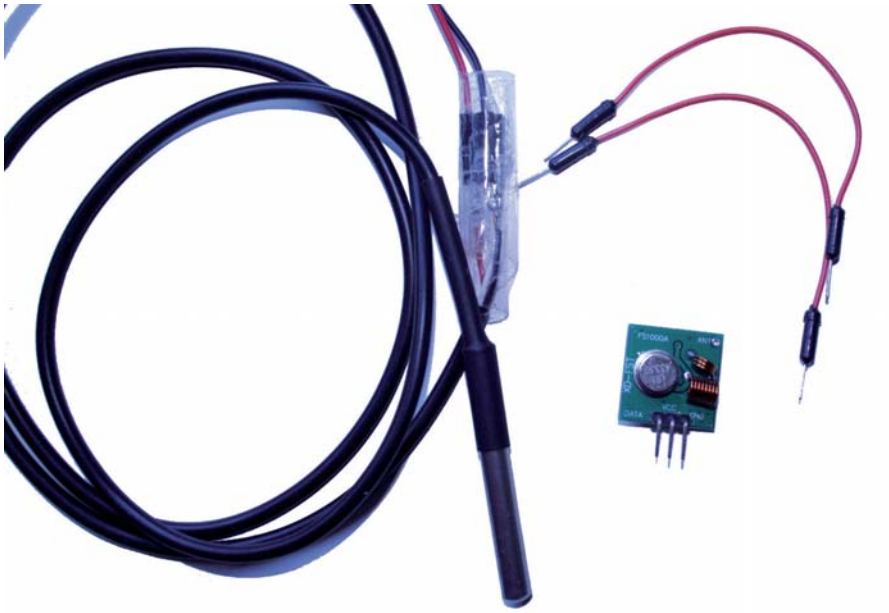


Bild 1: Temperatursensor mit Kabel, ein Funkchip zum Steuern von Funksteckdosen und zwei Kabelbrücken: Bauteile für unter zehn Euro machen den Raspberry zu einem System zur Temperaturüberwachung.

```
cd /sys/bus/w1/devices/
ls -l
```

wechseln können. Der Befehl *ls -l* listet alle Dateien im aktuellen Verzeichnis auf. Darin befindet sich ein Unterordner mit einem etwas kryptischen Namen, beispielsweise *28-0014106c92ff*. Das ist die digitale Kennung des verwendeten Sensors, die bei Ihnen natürlich abweichen kann. Wechseln Sie in dieses Verzeichnis und sehen Sie sich die darin enthaltene Datei *w1_slave* an:

```
cd 28-0014106c92ff
cat w1_slave
```

Der Inhalt der Datei sieht in etwa so aus:

```
26 01 55 00 7f ff 0c 10 f3 : crc=f3
  YES
26 01 55 00 7f ff 0c 10 f3 t=18375
```

Uns interessiert die letzte Zahl in der zweiten Zeile, im Beispiel ist das t=18375. Der Sensor misst eine Temperatur von 18,3 Grad Celsius. Für einen Serverraum gar nicht mal so schlecht. Jetzt brauchen Sie nur noch ein Bashscript, das im Minutentakt die Temperatur mitloggt und Alarm schlagen kann (siehe auch Listing 1).

Mit *cd ~* wechseln Sie ins Homeverzeichnis, mit *nano temperatur.sh* legen Sie eine neue Datei an und fügen den Code aus Listing 1 ein. Mit "Strg + O", Return und "Strg + X" speichern Sie die Datei unter dem gewünschten Namen ab und verlassen den Editor.

In den ersten beiden Zeilen definieren Sie den oberen und unteren Grenzwert, der einen Alarm auslöst. In Zeile 4 und 5 lesen Sie den Temperaturwert aus. Gegebenenfalls müssen Sie den Pfad in Zeile 3 ("28-0014106c92ff") anpassen. Da die Shell nur Ganzzahlen unterstützt, rechnen Sie den gemessenen Wert mit *printf "%.1d", t/1000* in einen ganzzahligen Wert um, der die Temperatur in Grad Celsius angibt. Anschließend wird der Wert in ein Logfile geschrieben und bei Bedarf ein Alarm ausgelöst.

Die zugehörige E-Mail verschicken Sie mit einem Python-Skript. Damit Sie nicht jede Minute eine E-Mail bekommen, sondern beispielsweise nur alle fünf Minuten, prüfen Sie mit dem Befehl *date -r /home/pi/mailsent.log +%s*, wann die letzte Alarm-E-Mail verschickt wurde. Nur wenn das lange genug her ist, schicken Sie eine erneute E-Mail. Um diesen Mechanismus erstmalig nutzen zu können, müssen Sie mit

```
touch /home/pi/mailsent.log
```

eine Datei anlegen. Anhand des Zeitstempels, wann diese Datei zuletzt angefasst ("touch") wurde, legen Sie fest, ob das System eine erneute E-Mail verschicken soll oder nicht. Abschließend müssen Sie natürlich mit dem Befehl *chmod 755 temperatur.sh* das Skript noch ausführbar machen.

Alarm-E-Mail mit Python verschicken

Jetzt kennt der Raspberry zwar die Temperatur im Serverraum, aber Sie als Administrator wissen davon noch nichts. Mithilfe der Programmiersprache Python verschicken Sie nun die bereits erwähnte Alarm-E-Mail. Python ist auf Raspbian vorinstalliert und kann sofort genutzt werden. Legen Sie mit *nano mail.py* eine Datei an und kopieren Sie das Listing 2 hinein. Fügen Sie anschießend Ihre eigenen SMTP-Zugangsdaten in die Zeilen 11 bis 14 ein und bestimmen Sie in Zeile 43, wer die Alarm-E-Mail bekommen soll.

Jetzt müssen Sie nur noch mit einem Cronjob das Bashscript regelmäßig starten. Tippen Sie dazu *crontab -e* und fügen Sie am Ende die Zeile

```
* * * * * /home/pi/temperatur.sh
```

ein. Mit "Strg + O", Return und "Strg + X" verlassen Sie den Editor und installieren die Crontab neu. Die ersten fünf Sternchen bedeuten, dass der Cronjob zu jeder Minute, in jeder Stunde, an jedem Tag des Monats, in jedem Monat und an jedem Wochentag das Skript *temperatur.sh* ausführen soll. Der Raspberry

```
#!/bin/bash
min=15
max=16
lastmail=300
temp=$(cat /sys/bus/w1/devices/28-0014106c92ff/w1_slave  |
   grep t= | awk -F '=' '{print $2}')
temp=$(awk -v t="$temp" 'BEGIN{printf "%.1d", t / 1000}')

echo $(date) $temp > temperatur.log

if [ "$temp" -gt "$max" ]
   then
      lastmail=$(($(date +%s) - $(date -r /home/pi/mail
         sent.log +%s)))
      if [ "$lastmail" -gt "$neuemail" ]
         then
            python mail.py $temp
            touch /home/pi/mailsent.log
      fi
fi

if [ "$temp" -lt "$min" ]
   then
         echo "Minimaltemperatur unterschritten"
fi
```

Listing 1: Temperatur-Bashscript

überprüft nun also jede Minute die Temperatur im Serverraum und sendet in den von Ihnen definierten Fällen eine Alarm-E-Mail an Sie.

Als nächsten Schritt möchten wir im Alarmfall nicht nur eine E-Mail verschicken, sondern auch einen Ventilator einschalten, der für frischen Wind sorgt. Dazu nutzen wir eine Funksteckdose, die wir mit dem Raspberry ansteuern.

Funksteckdose für den Raspberry vorbereiten

Um mit dem Raspberry Funksteckdosen schalten zu können, benötigen Sie Geräte, die auf 433 MHz empfangen können. Suchen Sie dazu im Web einfach nach "Funksteckdose 433". Wir verwenden für unseren Workshop die günstigsten von "mumbi" für knappe zehn Euro und haben damit gute Erfahrungen gemacht. Den Funkchip gibt es schon für deutlich unter fünf Euro, suchen Sie dazu nach "433MHZ Wireless Transmitter" oder nach "MX-FS-03V". Möchten Sie später auch Funksignale mit dem Raspberry empfangen, kaufen Sie sich gleich ein Set aus Sender und Empfänger. Für diesen Workshop genügt aber der Sender.

Funksteckdosen und ihre Fernbedienungen sind mit Jumpern ausgestattet, mit deren Hilfe verhindert wird, dass Sie Ihrem Nachbarn versehentlich die Wohnzimmerlampe ausschalten. Öffnen Sie die Steckdose und die Fernbedienung und setzen Sie die Jumper in beiden Geräten gemäß der mitgelieferten Bedienungsanleitung. Sie können die Jumper zwar in eine beliebige Position bringen, diese muss aber in Sender und Empfänger identisch sein. Merken Sie sich die Position der einzelnen Jumper, denn Sie benötigen sie später für die Programmierung des Raspberry.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from email.mime.text import MIMEText
import smtplib
import sys

####################################
# declaration of default mail settings #
####################################
sender = '<NAME><EMAILADRESSE>'
smtpserver = '<SMTP-SERVER>'
smtpusername = '<SMTP-USER>'
smtppassword = '<SMTP-PASS>'
usetls = True

####################################
# function to send a mail          #
####################################
def sendmail(recipient,subject,content):
  # generate a RFC 2822 message
  msg = MIMEText(content)
  msg['From'] = sender
  msg['To'] = recipient
  msg['Subject'] = subject

  server = smtplib.SMTP(smtpserver)

  if usetls:
    server.starttls()

  if smtpusername and smtppassword:
    server.login(smtpusername,smtppassword)

  server.sendmail(sender,recipient,msg.as_string())

  server.quit()

####################################
# main function                    #
####################################
def main():
  sendmail('<EMAILADRESSE>','Warnung: ' + sys.argv[1],'Die
   Temepratur wurde überschritten. Im Serverraum hat es '
   + sys.argv[1] + ' Grad.')

  sys.exit(0)

if __name__ == '__main__':
  main()
```

Listing 2: Alarm-Mails mit Python

```
if [ "$temp" -gt "$max" ]
   then
      lastmail=$(($(date +%s) - $(date -r /home/pi/mail
         sent.log +%s)))
      if [ "$lastmail" -gt "$neuemail" ]
         then
            python mail.py $temp
            touch /home/pi/mailsent.log
      fi
      sudo /home/pi/rcswitch-pi/send 10101 3 1
   else
      sudo /home/pi/rcswitch-pi/send 10101 3 0
fi
```

Listing 3: if-Zweig in temperatur.sh

Der Funkchip wird anders als der Temperatursensor nicht mit 3,3 Volt, sondern mit 5 Volt betrieben. Deswegen bekommt dieser den Strom aus einem anderen GPIO-Stift. Den Datenstift schließen Sie an GPIO 17 an, das ist der sechste Stift von links in der unteren Reihe. Den genauen Aufbauplan sehen Sie in Bild 2.

Nun haben Sie alles vorbereitet und können sich an die Tastatur setzen und sich über putty mit dem Raspberry verbinden. Zum Schalten der Funksteckdose benö-

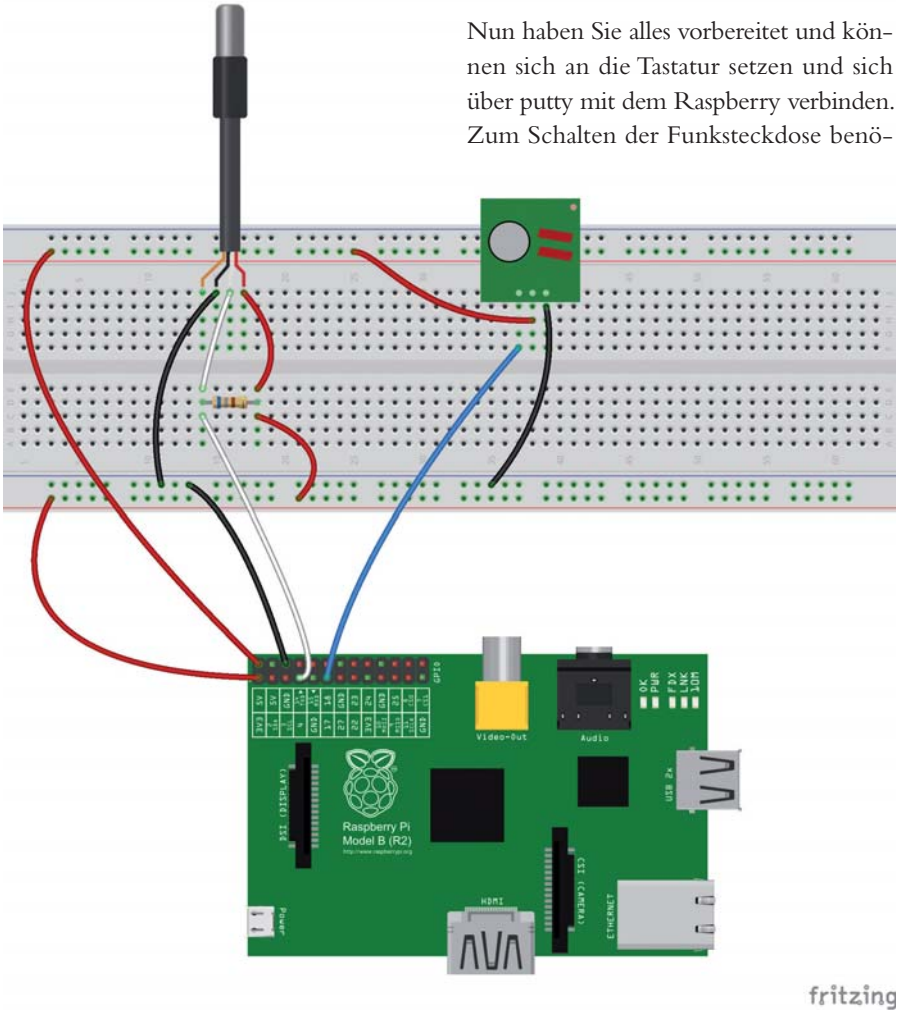


Bild 2: Mit nur wenigen Handgriffen schließen Sie einen digitalen Temperatursensor und ein Modul zum Schalten von Funksteckdosen an den Raspberry an.

tigen Sie die Software rcswitch-pi, die auf WiringPi aufbaut. Beides klonen Sie sich zunächst von github und installieren es im Anschluss:

```
cd ~
git clone git://git.drogon.net/
  wiringPi
cd wiringPI
./build
cd ~
git clone https://github.com/r10r/
  rcswitch-pi.git
cd rcswitch-pi
make
```

Mit *cd ~* wechseln Sie ins Homeverzeichnis des aktuellen Users und mit *git clone* laden Sie die gewünschte Software herunter. Weil beide Programme in unterschiedlichen Sprachen (C und C++) geschrieben sind, benötigen Sie die Befehle *build* und *make* zum Kompilieren des Codes. Nachdem die benötigte Software nun installiert ist, können Sie den ersten Test wagen. Tippen Sie

```
sudo ./send 10101 3 1
```

ein, wobei die ersten fünf Ziffern Ihre individuelle Jumper-Stellung definieren, gefolgt von einem Leerzeichen und der Nummer der anzusprechenden Funksteckdose. Es kann sein, dass diese Nummer auf Ihrer Fernbedienung als Buchstabe gekennzeichnet ist. Erst die letzte Ziffer gibt an, ob die Steckdose ein- oder ausgeschaltet werden soll.

Nun fügen Sie die entsprechenden Befehle zum Ein- und Ausschalten der Funksteckdose nur noch in das Skript *temperatur.sh* ein. Ergänzen Sie dazu in der Datei *temperatur.sh* den if-Zweig, der das Überschreiten der Maximaltemperatur regelt, um die Zeile

```
sudo /home/pi/rcswitch-pi/send 10101
  3 1
```

Achten Sie darauf, Ihre individuelle Jumper-Einstellung zu verwenden. Beachten Sie auch die absolute Pfadangabe, die mit */home/pi* beginnt. Ohne absoluten Pfad kann das Skript, das als Cronjob ausgeführt wird, den Befehl *send* nicht finden. Abschließend sollten Sie die Funksteckdose wieder ausschalten, sobald die Maximaltemperatur wieder unterschritten wird. Dazu fügen Sie einen else-Zweig ein; die gesamte if-Anweisung sehen Sie in Listing 3.

Fazit

Mit nur wenigen Bauteilen im Wert von unter 100 Euro können Sie die Temperatur im Serverraum überwachen und automatisch Gegenmaßnahmen ergreifen, und das ohne Lötkolben oder Schraubenzieher. Dabei können Sie an den Raspberry auch noch weitere kostengünstige Sensoren anschließen – zum Beispiel einen Entfernungsmesser, der feststellt, ob die Tür zum Serverraum oder eines Serverracks geöffnet wurde. Oder Sie werten die Temperaturlogfiles grafisch aus. Ihrer Kreativität sind dabei kaum Grenzen gesetzt. *(dr)*

Link-Codes

[1] Raspbian-Image herunterladen
F3Z41

[2] SSH-Key selbst erstellen
F3Z42

Workshop: Netflow-Reporting mit Google Analytics

Verkehrsanalyse

von Markus Stubbig

Viele Webmaster setzen zur Nutzungsanalyse ihrer Webseiten das kostenlose Google Analytics ein. Mit geringen Modifikationen kann der Dienst auch für einfache Auswertungen von beliebigen Verkehrsdaten im Unternehmensnetz verwendet werden. Unser Workshop zeigt, wie sich Google Analytics zum Speichern und Auswerten von NetFlow-Daten einsetzen lässt.

Eine wertvolle Informationsquelle für Systemadministratoren zur tiefen Einsicht in Netzwerkaktivitäten ist NetFlow [1]. Bei NetFlow sammeln Router und Layer 3-Switche die Verbindungsinformationen der Clients und senden diese in unregelmäßigen Abständen an einen zentralen Server. Seit der Einführung von NetFlow durch Cisco haben die anderen großen Hersteller von Netzwerkhardware nachgezogen und ihre eigene oder die RFC-basierte Version implementiert. Das Grundprinzip ist weitgehend dasselbe.

Beim professionellen Einsatz vom NetFlow steht der Administrator vor der Wahl zwischen einem kommerziellen NetFlow-Analyser mit vielen Features oder einer Open Source-Implementierung zum Nullkostenpreis. Dieser Artikel beschreibt eine neue, dritte Variante: Die Analyse von Verkehrsdaten "aus der Cloud". Dabei sammelt ein firmenlokaler NetFlow-Collector alle Informationen und sendet sie (oder nur einzelne Stichproben) an Google Analytics (GA) zur weiteren Speicherung und Auswertung.

Google Analytics bietet mit Dashboards und "Benutzerdefinierten Berichten" viele Möglichkeiten, die Informationsflut übersichtlich anzuzeigen. Neben den üblichen Hitlisten der meistfrequentierten Server lassen sich unerwünschte Protokolle (etwa SIP, OpenVPN oder POP3) aufzeigen oder ermitteln, welcher Client die meisten Internetzugriffe erzeugt. Auch Fragen wie "Welche Windows-Fileserver werden verwendet und welche Maschinen stellen unerwartet Freigaben bereit?" oder "Welcher Client greift auf die Managementoberfläche der Firewall zu?" lassen sich mit den verfügbaren Reports beantworten.

Informationen bereitstellen

Die Informationen über IP-Verbindungen erhalten Sie von Routern, Multi-Layer-Switchen, Firewalls oder virtuellen Umgebungen (Hypervisor, vSwitch). Alle namhaften Hersteller bieten eine Möglichkeit an, diese Informationen zu exportieren. Dazu stehen Protokolle wie NetFlow (Cisco), JFlow (Juniper) oder die standardisierten Varianten sFlow und IPFIX zur Verfügung. Aufgrund seiner Popularität ist dieser Workshop auf NetFlow ausgerichtet.

Die vorhandenen Router stellen die NetFlow-Funktionalität meist ohne Mehrkosten bereit und die Konfiguration ist denkbar einfach. Bevorzugt werden Router mit NetFlow beglückt, die nahe beim Collector wohnen und noch ausreichend Kapazitäten haben. Bei der Auswahl der Interfaces muss sichergestellt werden, dass Netzwerkverkehr nicht doppelt gezählt wird (eingehend bei Router A und ausgehend bei Router B). Die Konfiguration der Geräte lässt meistens schon einen ersten Filter zu, sodass uninteressante oder sicherheitskritische Verkehrsdaten nicht berücksichtigt werden.

Im SOHO-Bereich ist das NetFlow-Angebot dünn gesät, aber mit etwas Glück besitzen Sie einen Router mit DD-WRT oder pfSense. Leider bieten die verbreiteten DSL-Router von AVM keine Unterstützung für NetFlow.

Aber was passiert, wenn die eigenen Router keinen Flow-Export anbieten?

Google Analytics

Google Analytics ist ein Webanalyseprogramm, das mit NetFlow nur wenig gemeinsam hat. Es werden Informationen über das Verhalten von Besuchern auf Webseiten gesammelt und ausgewertet. Der Fokus von Google Analytics liegt auf Effektivitätsmessung, Verkaufszahlen, Webseitenoptimierung und Erfolgskontrolle von Marketingaktionen. Schätzungsweise 50 bis 60 Prozent aller Webseiten verwenden Google Analytics.

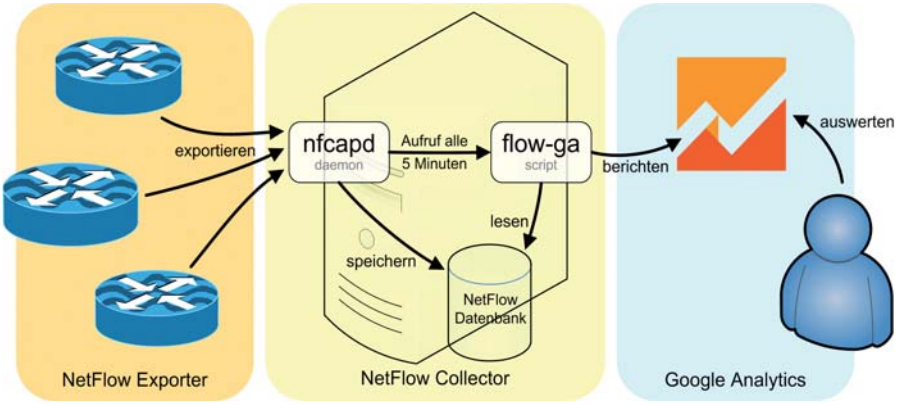


Bild 1: Schematischer Überblick der NetFlow-Datenanalyse mit Google Analytics.

Hier können Sie mit einem Workaround arbeiten, bei dem ein Linux-Rechner über einen Mirror-Port eine Kopie aller Netzwerkpakete erhält und daraus einen NetFlow-Export erstellt. Passende Open Source-Software dafür sind beispielsweise das iptables-Modul "ipt_netflow" oder die Programme "pmacct" und "softflowd".

Verkehrsdaten sammeln

Sobald der erste Router als NetFlow-Exporter konfiguriert ist, sendet dieser in unregelmäßigen Abständen Informationen über beendete (oder ausgetimte) Verbindungen an die angegebene IP-Adresse, hinter der sich unser NetFlow-Collector befindet. Dieser Collector ist ein Linux-Dienst und lauscht auf UDP-Port 2055. Aus den empfangenen NetFlow-Samples werden die Verbindungsinformationen (siehe Kasten "NetFlow") herausgelöst und auf der lokalen Festplatte kurz zwischengespeichert.

Die Open Source-Software "nfdump" [2] erledigt diesen Job auf einem bestehenden Linux-Server oder einer schlanken virtuellen Maschine. Für die VM sind ein CPU-Kern, 256 MByte RAM und eine 2 GByte-Festplatte ausreichend. Die Installation erfolgt auf CentOS-, Fedora- oder Red Hat-Systemen über den Paketmanager yum. Das Paket "nfdump" ist im EPEL-Repository verfügbar:

```
$ yum install nfdump
```

Vor dem Start erweitern Sie die lokale Firewall noch um eine Regel für eingehende Pakete auf Port 2055 (SELinux benötigt keine Anpassung):

```
$ iptables -I INPUT -p udp -m state
  --state NEW -m udp --dport 2055 -j
  ACCEPT
$ ipt6ables -I INPUT -p udp -m state
  --state NEW -m udp --dport 2055 -j
  ACCEPT
```

Zum Testen der Installation wird der Collector mit

```
$ nfcapd -E -T all -p 2055 -l /tmp
  -I any
```

gestartet. Nach kurzer Zeit sollten die ersten NetFlow-Daten in der Linux-Konsole sichtbar sein.

Google Analytics vorbereiten

Zur Nutzung von Google Analytics [4] muss ein Google-Konto vorhanden sein, das Sie um den Analytics-Dienst erweitern. Der vorsichtige Admin vergleicht vorher noch die Bedingungen von GA mit der eigenen Unternehmenspolicy. Anschließend erstellen Sie innerhalb von GA ein Konto und eine Property. Danach gibt Google die Tracking-ID – beispielsweise UA-12345678-1 – bekannt. Diese wird im Skript *flow-ga.pl* (siehe nächster Abschnitt) eingetragen und verbindet die berichteten NetFlow-Daten mit dem Google-Account.

Die Property benötigt noch "Benutzerdefinierte Definitionen", die die Feldnamen von NetFlow darstellen und händisch angelegt werden. Hierbei ist die Reihenfolge und Schreibweise wichtig. Dazu zählen zunächst die "Benutzerdefinierten Dimensionen" (alle vom Umfang "Hit"):

1. srcaddr
2. dstaddr
3. srcport
4. dstport
5. protocol
6. exporter_id
7. input_if
8. output_if
9. tos

Darüber hinaus gibt es die "Benutzerdefinierten Messwerte" (Umfang "Hit"):

1. bytes (Ganzzahl)
2. packets (Ganzzahl)
3. duration_sec (Zeit)
4. duration_msec (Ganzzahl)

NetFlow-Einträge berichten

Dummerweise kennt Google Analytics weder NetFlow noch die meisten NetFlow-Variablen wie Portnummer oder IP-Protokoll. Gleichzeitig sind Kategorien wie "Seitenaufrufe", "Ereignisse", "E-Commerce" oder "Timing" vorhanden. Die Kunst liegt also in der richtigen Zu-

Beispielkonfiguration eines Cisco Router 1921 mit IOS 15.2:

```
interface GigabitEthernet0/1
ip flow ingress
ip flow-export version 5
ip flow-export destination 10.10.1.1 2055
```

Beispielkonfiguration HP 9300 Serie:

```
interface ethernet 1/1
ip route-cache flow
ip flow-export enable
ip flow-export version 5
ip flow-export destination 10.10.1.1 2055 1
```

NetFlow-Konfiguration

Ein NetFlow-Paket [3] beinhaltet bis zu 30 unidirektionale Verbindungseinträge (je nach Version und Paketgröße). Zum Beispiel beinhaltet jeder Eintrag von Version 5:

- Quell- und Ziel-IPv4-Adresse
- Quell/Ziel-Portnummer
- IP-Protokoll (zum Beispiel TCP, UDP oder ICMP)
- Eingehendes und ausgehendes Routerinterface
- Anzahl der transportierten Bytes und Pakete
- Beginn und Ende der Verbindung
- Type of Service (Prioritätsbits)

Neuere Implementierungen mit NetFlow Version 9 bieten zusätzliche Infos über Multicast, IPv6, BGP und MPLS. Die Informationsfülle des Pakets kann beliebig gewählt werden, so dass keine leeren Felder und uninteressanten Einträge versendet werden.

NetFlow

ordnung. Als sehr vorteilhaft und flexibel hat sich der Bereich "Ereignisse" im Zusammenhang mit "Benutzerdefinierte Dimensionen/Messwerte" erwiesen. Diese Bereiche bieten genug Spielraum, um alle NetFlow-Informationen aufzunehmen.

Die Umwandlung vom NetFlow-Format in das "Google Analytics Measurement Protocol" [5] und das anschließende Berichten erfolgt über das selbstentwickelte Tool "flow-ga" [6]. Dieses wird vom NetFlow-Collector "nfcapd" nach jedem Fünf-Minuten-Intervall aufgerufen. Nach dem Download platzieren Sie die Dateien unter */usr/bin/*. Eventuell sind weitere Perl-Module nötig, die Sie über den Paketmanager nachladen:

```
$ yum install  perl-Time-HiRes
  perl-Digest-HMAC perl-DateTime
  perl-libwww-perl
```

Das Logging erfolgt wie unter Linux üblich über Syslog:

```
$ echo "local5.*  /var/log/flow-
  ga.log" > /etc/rsyslog.conf
$ service rsyslog restart
```

Vor dem Start ist ein Blick in die Funktionen "_anonymizeIp()" und "get_hostname()" von *flow-ga.pl* sinnvoll. Dort sollten Sie eine Form der Anonymisierung aktivieren, um nicht zu viele Informationen über das eigene Netzwerk auszuplaudern. Voreingestellt ist eine einfache Anonymisierung, die das zweite Oktett der IP-Adresse invertiert und den Rechnernamen unkenntlich macht. Zuletzt starten Sie den NetFlow-Collector als Daemon:

```
$ nfcapd -D -w 5 -T all -p 2055 -l
  /tmp -I any -P /var/run/nfcapd.pid
  -x "/usr/bin/flow-ga.sh %d/%f"
```

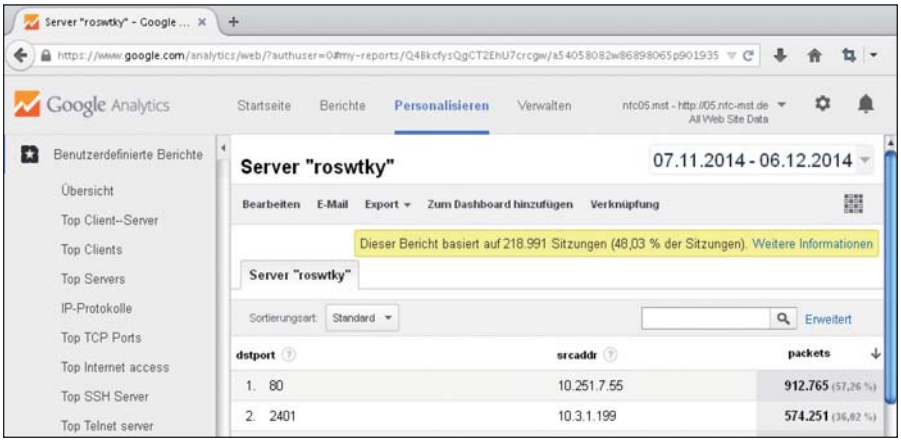


Bild 2: Über die Personalisierung in GA lassen sich tiefe Einblicke in die NetFlow-Daten – hier am Beispiel der überwachten Server – erstellen.

Gesammelte Daten auswerten

Sobald die ersten Einträge bei GA eintreffen, wird die Webseite im Bereich "Echtzeit" farbenfroher und interessanter. Die Auflistung der IP-Adressen ist hilfreich für eine schnelle Top 10-Übersicht. Die Daten für professionelle Berichte, die dem Administrator zusätzliche Einsicht in sein Netzwerk bieten, stellt Google erst nach 24 Stunden bereit.

Nach einigen Tagen sind auch Werte in den Bereichen "Verhalten / Ergebnisse" vorhanden. Hier lässt sich nach IP-Adressen, Traffic oder Zugriffen innerhalb von beliebigen Zeitintervallen (zum Beispiel letzter Monat) sortieren. Dabei entspricht die Ereigniskategorie der Ziel-IP-Adresse und das Ereignislabel ist die Quelladresse. Der Hostname wird als Ereignisaktion geführt. Der Bereich "Personalisieren" bietet mit benutzerdefinierten Berichten den tiefsten Einblick in die NetFlow-Daten. Neben den üblichen "Top Talkers" ermitteln Sie hier unerwünschte Protokolle (beispielsweise Telnet, WINS) oder Server.

Begrenzte Möglichkeiten

Leider ist nicht alles Gold, was glänzt, denn Google setzt dem Nutzer klare Grenzen. Google Analytics limitiert die Anzahl der Samples auf 200.000 Hits pro User und Tag. Das sind circa 700 Samples pro Fünf-Minuten-Interval. Wenn tatsächlich mehr NetFlow-Samples anfallen, gibt es verschiedene Lösungsmöglichkeiten. Neben der Anschaffung eines eigenen NetFlow-Servers liessen sich anhand von Stichproben weniger Samples versenden. Wenn der Routerhersteller keine Funktion zum Reduzieren der Datenmenge anbietet, hilft unser Tool *flow-ga.pl*. Über die Variable "$sampling_rate_N" versendet das Skript nur noch jeden N-ten NetFlow-Eintrag. Alternativ sendet jeder Router über einen separaten NetFlow-Collector-Daemon an unterschiedliche GA-Properties. Google empfiehlt in dieser Situation natürlich das Upgrade auf den kostenpflichtigen Dienst "Google Analytics Premium", der auch ohne Sampling arbeiten kann (wenn gewünscht).

Beim Einsatz der Sampling-Rate sind die GA-Daten nicht mehr 100 Prozent exakt, aber die allgemeine (Trend-)Analyse oder Reporte zum Aufdecken von unbekannten

Google Analytics beschränkt die Nutzung seines Dienstes keinesfalls auf Webseiten oder Webdienste. In der offiziellen Dokumentation sind Anwendungsbeispiele angegeben, die Installationen einer iPhone/Android-App zählen, In-App-Käufe ermitteln oder Zeitmessungen protokollieren. Die Schulungsmaterialien bezeichnen diese web-freien Anwendungen als "digital environment" oder "offline business data". Ein Zitat aus der "Analytics Academy", Lektion 1.2: "Sie können Google Analytics auf richtig kreative Weise nutzen, um Unternehmensdaten offline zu sammeln, wie beispielsweise Finanzumsätze in Ladengeschäften, solange Sie eine Möglichkeit finden die Daten zu sammeln und an Ihren Analytics Account zu senden."

Duldung durch Google

[1] Cisco IOS NetFlow
F3Z71

[2] NFDUMP
F3Z72

[3] NetFlow Export Datagram Formats
F3Z73

[4] Google Analytics
F3Z74

[5] Google Analytics Measurement Protocol
F3Z75

[6] Download Skripte
F3Z76

Link-Codes

Protokollen, Diensten oder Servern sind auch dann noch möglich. Lediglich unternehmenskritische Anwendungen, wie zum Beispiel Abrechungssysteme, sollten diesen Daten fernbleiben.

Weiterhin sind viele vorgefertigte GA-Bereiche auf die Webseitenoptimierung ausgelegt und daher im NetFlow-Umfeld nutzlos: Interessen, Technologie, Mobil, Demografische Merkmale, Conversions, AdWords und Kampagnen.

Alle Informationen, die an GA gesendet werden, sind erst nach ungefähr 24 Stunden für die Auswertung bereit. Eine Echtzeitüberwachung ist nur eingeschränkt unter "Echtzeit" verfügbar und sicherheitskritisches Monitoring (etwa DoS-Erkennung) entfällt.

Eigener NetFlow-Analyser als Alternative

Professionelle Netflow-Analyser bestechen durch ausgefeilte Reporte, Unterstützung bei der Kapazitätsplanung und jede Menge Statistiken mit bunten Diagrammen. Allerdings erwarten die Hersteller einen Platz im ohnehin schon zu schlanken IT-Budget. Beim gelegentlichen Blick in die gesammelten Netflow-Daten genügt meistens auch eine gute Open Source-Software. Die Installation, Konfiguration und der Pflegeaufwand sind jedoch genauso aufwändig wie bei der vollwertigen Nutzung.

Es gibt mehrere ausgezeichnete Open Source-Produkte für NetFlow-Auswertungen: NTop, EHNT oder FlowViewer. Für den Einsatz dieser Tools wird ein Server mit ausreichend Speicherplatz und Disk-I/O benötigt. Die Installation erfordert Linuxkenntnisse und passt möglicherweise nicht in eine homogene Windowsumgebung.

Das Problem der lokalen Speicherung von NetFlow-Informationen ist die große Datenmenge. Diese Herausforderung übergeben wir an Google Analytics; leider auf Kosten der zeitnahen Bereitstellung.

Ein Hinweis zum Datenschutz

Bei den Worten "Google Analytics" klingeln bei vielen kritischen Admins die Alarmglocken. Wie bei allen externen Diensten muss vor der Nutzung stets geprüft werden, ob die Datenübertragung mit der firmeninternen Richtlinie und dem Datenschutz harmoniert. GA bietet Anonymisierungsroutinen für IP-Adressen an, die zusätzlich im flow-ga.pl-Skript enthalten sind. Es verlassen folglich nur die Informationen das Unternehmen, die gewünscht und anonymisiert sind.

Fazit

Die Verwendung von Google Analytics als NetFlow-Analyzer ermöglicht die Auswertung und Überwachung des eigenen Netzwerks ohne die Bereitstellung eines ausgewachsenen Servers. Nach mehreren Tagen stehen genug Informationen bereit, um sinnvolle Berichte über Nutzung und Missbrauch der IT-Infrastruktur zu erkennen. Auch wenn keine 100-prozentig exakten Werte zu verwendeter Bandbreite oder Paketen möglich sind, überwiegen dennoch die Vorteile und der Reiz eines NetFlow-Analysers aus der Cloud. *(jp)*

Workshop: Monitoring von Exchange 2013 mit Bordmitteln

Hintergrundbewegung

von Christian Schulenburg

In vorangegangenen Exchange-Versionen war der Exchange Best Practice Analyser stets eine wichtige Anlaufstelle, um den Gesundheitsstatus des Servers zu überprüfen. Mit Exchange 2013 gibt es ExBPA nicht mehr. Microsoft hat dafür jedoch eine direkte Echtzeitüberwachung mit dem Namen Managed Availability in Exchange 2013 eingebaut. Dieser Workshop bringt Ihnen die wichtigsten Aspekte dieser neuen Funktion näher und beschreibt wichtige Befehle.

Managed Availability (MA) ist eine neue Funktion, die im Hintergrund den Status von Exchange und seinen Komponenten permanent prüft und sich bei Problemen nicht nur meldet, sondern gleich eine Fehlerbehebung einleitet. Dieses neue Werkzeug ist vor allem Office 365 und der Vielzahl an Servern geschuldet, die Microsoft selbst im Blick behalten muss. Eine automatische Fehlerbehebung auch auf lokalen Exchange-Systemen ist ein wichtiger Schritt, um administrative Aufwände in den Griff zu bekommen und größere Umgebungen effizient zu betreuen.

Der Administrator bekommt von der Funktion nur am Rande etwas mit, trotzdem sollte ein grundsätzliches Verständnis vorhanden sein, damit Sie zum Beispiel bei Updates richtig mit MA umgehen oder Dienste nach einem geplanten Deaktivieren nicht einfach wieder starten. Auch für Nutzer des Microsoft System Center Operation Managers (SCOM) hat diese Funktion Konsequenzen, denn das Management Pack für Exchange 2013 wurde stark abgespeckt und SCOM dient primär als Dashboard zum Anzeigen von Statusinformationen. Das Management Pack greift nur noch die Eskalationsmeldungen ab – Anpassungen müssen Sie direkt am Exchange-Server setzen.

Implementierung durch neuen Exchange Dienst

MA wird über den Microsoft Exchange-Integritätsdienst (*MSExchangeHMHost.exe*) und den Exchange-Integritäts-Manager-Arbeitsprozess (*MSExchangeHMWorker.exe*) implementiert. Der Integritätsdienst ist ein Controller-Prozess und ist für die Verwaltung von Arbeitsprozessen zuständig. Hierüber wird der Arbeitsprozess nach Bedarf gesteuert und gegebenenfalls wiederhergestellt, sodass dieser nicht selbst zur Fehlerquelle wird. Der Arbeitsprozess als zweiter Prozess ist für die Ausführung der Laufzeitaufgaben in der verwalteten Verfügbarkeit zuständig.

Wichtig ist es, vor allem den Exchange-Integritätsdienst im Blick zu behalten, denn sofern dieser nicht gestartet ist, ist die Überwachung des Servers nicht aktiv. Sofern Sie mehrere Exchange-Server einsetzen, wird der Dienst automatisch zur Sicherheit von einem entfernten Exchange-Server überwacht, die Exchange 2013-Server behalten sich also gegenseitig im Auge. Welche Server dies sind, bringen Sie mit folgendem Befehl auf den Bildschirm:

```
Get-ServerHealth -Server LABO1EX01
  -HealthSet RemoteMonitoring |
  Where Name -eq "HealthManager-
  ObserverMonitor" |
  ft Name,TargetResource
```

Microsofts Process Explorer offenbart zudem die Abhängigkeit zwischen dem Microsoft Exchange-Integritätsdienst und dem Exchange-Integritäts-Manager-Arbeitsprozess etwas genauer.

Die Konfiguration von MA wird an verschiedenen Stellen gespeichert. Die lokalen Einstellungen, wie lokale (serverspezifische) Außerkraftsetzungen, finden sich in der Registry unter "HKLM \ SOFTWARE \ Microsoft \ ExchangeServer \ v15 \ ActiveMonitoring \ Overrides", während globale Einstellungen in "Active Directory Container Monitoring Settings" gespeichert werden. Zudem werden in XML-Dateien im Exchange-Installationsverzeichnis im Ordner *\bin\Monitoring\config* Config-Einstellungen für einige der Test- und Überwachungsarbeitsaufgaben abgelegt.

Weiterhin gibt es noch die Integritätspostfächer, die für Prüfaktivitäten zur Anwendung kommen. Dabei werden in jeder Postfachdatenbank mehrere Integritätspostfächer vorgehalten. Anzeigen lassen können Sie sich die Postfächer über

```
Get-mailbox -monitoring | ft
  Name,Database
```

Am wichtigsten ist aber das Ereignisprotokoll, da hier sämtliche Tests und Ergebnisse zu finden sind. Da es einige hundert

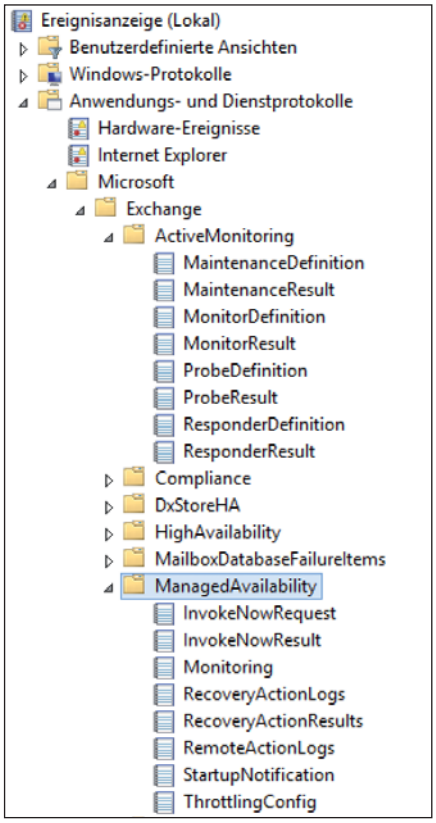


Bild 1: Das Event Log ist bei MA eine sehr auskunftsfreudige Anlaufstelle, die sich am besten über die PowerShell abfragen lässt.

Tests gibt, fallen die Einträge sehr umfangreich aus. Schauen Sie hierzu in die Punkte "Microsoft / Exchange / ActiveMonitoring" und "Microsoft / Exchange / ManagedAvailability" des Event Logs.

Aufbau Managed Availability

MA besteht aus den drei Komponenten Testmodul, Monitor und Antwortdienst, die folgende Aufgaben haben:

- Testmodul (Probe): Das Testmodul ist für die Durchführung von Messungen und das Sammeln von Daten verantwortlich. Die Konfiguration ist im Event Log unter dem Punkt "Microsoft / Exchange / Active Monitoring / ProbeDefinition" einzusehen.
- Monitor: Die gesammelten Daten fließen in den Monitor, der die Logik zur Definition des fehlerfreien Zustandes enthält. Anhand verschiedener Muster entscheidet die Komponente, ob eine Serverkomponente fehlerfrei oder fehlerhaft ist.
- Antwortdienst (Responder): Der Dienst ist für die Wiederherstellungs- und Weiterleitungsaktionen verantwortlich. Dabei wird auch versucht, fehlerhafte Komponenten wiederherzustellen, was den Neustart von Diensten oder des Servers bedeuten kann. Erst wenn die Wiederherstellungsaktionen keinen Erfolg verzeichnen, erfolgt eine Ereignisprotokollbenachrichtigung. Damit Wiederherstellungsversuche nicht immer wieder angestoßen werden, beschreiben Throttling-Einträge in der ResponderDefinition, wie häufig eine Aktion ausgeführt werden darf. Informationen zu aktuellen Vorgängen finden Sie ebenfalls im Event Log unter "Microsoft \ Exchange \ ActiveMonitoring \ ResponderResult".

Die verschiedenen Komponenten werden in einer Integritätssammlung (Health Set) logisch zusammengefasst, die den Zustand des Server wiederspiegelt. Mit *Get-ServerHealth* können Sie sich den Status der einzelnen Health Sets anzeigen. Mit dem Befehl *Get-HealthReport* gruppieren Sie die einzelnen Health Sets auch gleich und Sie erhalten einen besseren Überblick.

Die einzelnen Komponenten eines Health Sets listen Sie mit dem Befehl *Get-MonitoringItemIdentity* auf. Das folgende Beispiel betrachtet die Einträge zum Outlook-Protokoll näher:

```
Get-MonitoringItemIdentity -Identity
  Outlook.Protocol -Server LAB01EX01
  | ft Name,ItemType,Targetresource
  -AutoSize
```

Als Zustand zeigt ein Health Set das Ergebnis der enthaltenen Monitore an. Die Monitore befinden sich grundsätzlich im Status Healthy (fehlerfrei) oder Unhealthy (fehlerhaft). Darüber hinaus können auch weitere Zustände auftauchen:

- Beeinträchtigt (Degraded): Befindet sich ein Monitor im Fehlerzustand, wird er in den ersten 60 Sekunden als "Beeinträchtigt" betrachtet, bevor dieser in den Zustand "Fehlerhaft" wechselt.
- Deaktiviert (Disabled): Bei diesem Zustand wurde der Monitor vom Administrator deaktiviert.
- Nicht verfügbar (Unavailable): Sofern der Microsoft Exchange-Integritätsdienst bei der Abfrage des Monitor-Zustands keine Antwort erhält, ändert sich der Zustand des Monitors in "Nicht verfügbar".
- Reparatur (Repairing): Dieser Status wird vom Administrator definiert, um dem System anzuzeigen, dass Reparaturmaßnahmen ausgeführt werden. Den Status eines Monitors können Sie mit dem Befehl *Set-ServerMonitor* und dem Parameter "Repairing" auf Reparatur setzen:

```
Set-ServerMonitor -Server LabO1Ex01
  -Name DatabaseSizeEscalationPro-
  cessingMonitor -TargetResource
  DB04 -Repairing $true
```

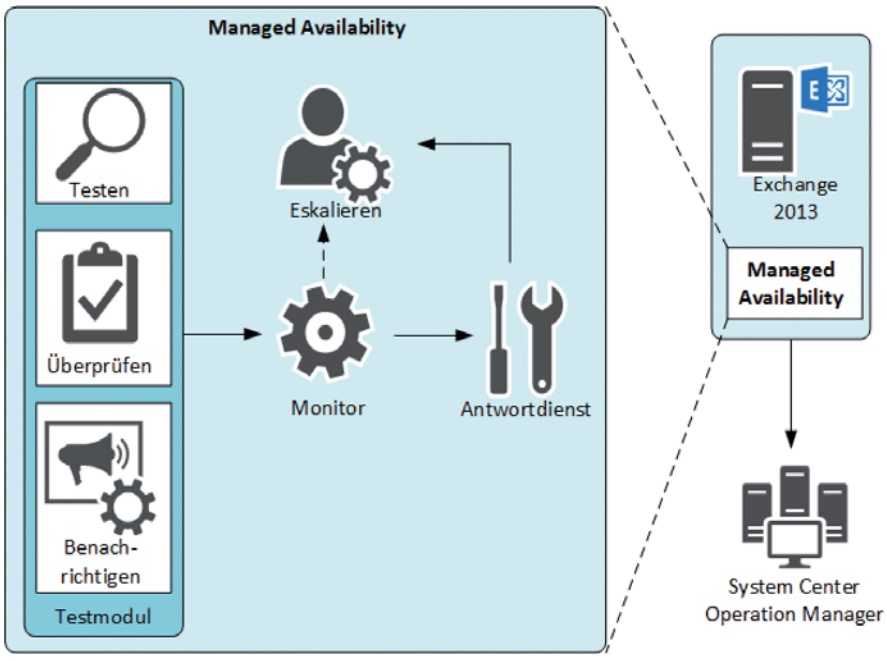


Bild 2: Diese Übersicht zeigt die verschiedenen Komponenten der Managed Availability in Exchange 2013.

Sofern MA eine Komponente als ungesund einstuft, markiert er diese Komponente als "Offline" oder "Inactive". Dadurch wird keine Tätigkeit in dem Bereich ausgeführt. Andere Server sehen den Status einzelner Komponenten und ignorieren diese im Fehlerfall. Den Status der einzelnen Komponenten eines Servers zeigen Sie sich mit folgendem Befehl an:

```
Get-ServerComponentState -Identity
  LAB01EX01
```

Monitoring der MA-Aktivitäten

Prüfen Sie zunächst mit *Get-HealthReport* regelmäßig die Integrität des Servers. Da nur fehlerhafte Zustände interessieren, können Sie diese auch direkt abfragen:

```
Get-HealthReport -Server LAB01EX01 |
  Where AlertValue -ne "Healthy"
```

Mit *Get-ServerHealth* prüfen Sie als Nächstes, welcher Monitor des Health Sets fehlerhaft ist:

```
Get-ServerHealth -Server LAB01EX01
  -HealthSet Outlook
```

Die Details zum fehlerhaften Monitor finden Sie im "Event Log" – die Abfrage über die PowerShell ist der schnellere Weg:

```
(Get-WinEvent -ComputerName
  LAB01EX01 -LogName Microsoft-Ex-
  change-ActiveMonitoring/Monitorde-
  finition | %
  {[XML]$_.toXml()}).event.userDa-
  ta.eventXml | Where Name -like
  "OutlookRpcCtpMonitor"
```

Hier sehen Sie nun eine genauere Beschreibung unter dem Punkt "ScenarioDescription". In den Eigenschaften finden Sie auch das Testmodul, das zur Anwendung kommt und das über *Invoke-MonitoringProbe* erneut gestartet wird. In der Rückmeldung erkennen Sie auch mögliche Fehler:

```
Invoke-MonitoringProbe -Server
  LAB01EX01 OutlookMapiHttp\Out-
  lookRpcCtpProbe|fl
```

Die genaue Beschreibung des Testmoduls fragen Sie ebenfalls über das Event Log ab:

```
(Get-WinEvent -ComputerName
  LAB01EX01 -LogName Microsoft-Ex-
  change-ActiveMonitoring/Probedefi-
  nition | %
  {[XML]$_.toXml()}).event.userDa-
  ta.eventXml | Where Name -like
  "OutlookRpcCtpProbe"
```

Sollten Sie während dieser Schritte unerwarteter Weise einen Blue Screen beziehungsweise einen ungeplanten Neustart feststellen, prüfen Sie die Initialisierung eines durch Exchange ausgelösten Reboots mit folgendem Befehl:

```
(Get-WinEvent -LogName Microsoft-Ex-
  change-ManagedAvailability/* | %
  {[XML]$_.toXml()}).event.userDa-
  ta.eventXml | Where ActionID -like
  "*ForceReboot*" | ft RequesterName
```

Im CU2 von Exchange 2013 führte zum Beispiel eine falsche Active Directory-Abfrage in einer Multi Domain-Umgebung zu einem Serverneustart, der durch eine Ausnahme umgangen und erst mit dem CU3 behoben wurde [1]. Auch eine falsche DNS-Konfiguration kann einem schnell zum Verhängnis werden und zu einem Serverneustart führen [2].

Ausnahmen schaffen

Es gibt immer Szenarien, in denen in die Überwachung eingegriffen werden muss und in denen Einstellungen gezielt anzupassen sind. Hierfür gibt es globale und lokale Overrides. Lokale Overrides wirken dabei nur auf einen Server, während globale mehrere Server betreffen.

Eine Einstellung wirkt dabei nicht sofort, da der Microsoft Exchange Health Management-Dienst nur alle zehn Minuten Konfigurationsänderungen prüft und übernimmt. Durch einen Dienste-Neustart wird die Anpassung sofort aktiv. Overrides sind nur für einen bestimmten Zeitraum vorgesehen, weshalb eine Laufzeit beziehungsweise eine Serverversion angegeben werden muss.

Einen globalen Override legen Sie mit dem Befehl *Add-GlobalMonitoringOverride* an, während Sie eine lokale Außerkraftsetzungsregel mit dem Befehl *Add-ServerMonitoringOverride* erstellen. Um zum Beispiel die Fernüberwachung eines Exchange Servers temporär zu deaktivieren, ist es möglich bei dem zu überwachenden Server eine Ausnahme zu schaffen. Welche Server eine Überwachung übernehmen, wurde bereits am Anfang des Artikels mit dem Befehl *Get-ServerHealth* beschrieben. Die Ausnahme erstellen Sie mit folgendem Befehl:

```
Add-ServerMonitoringOverride -Server
  LAB01EX01 -Identity 'RemoteMonito-
  ring\HealthManagerObserverProbe\
  Persephone.schulenburg.lab' -Item-
  Type Probe -PropertyName Enabled
```

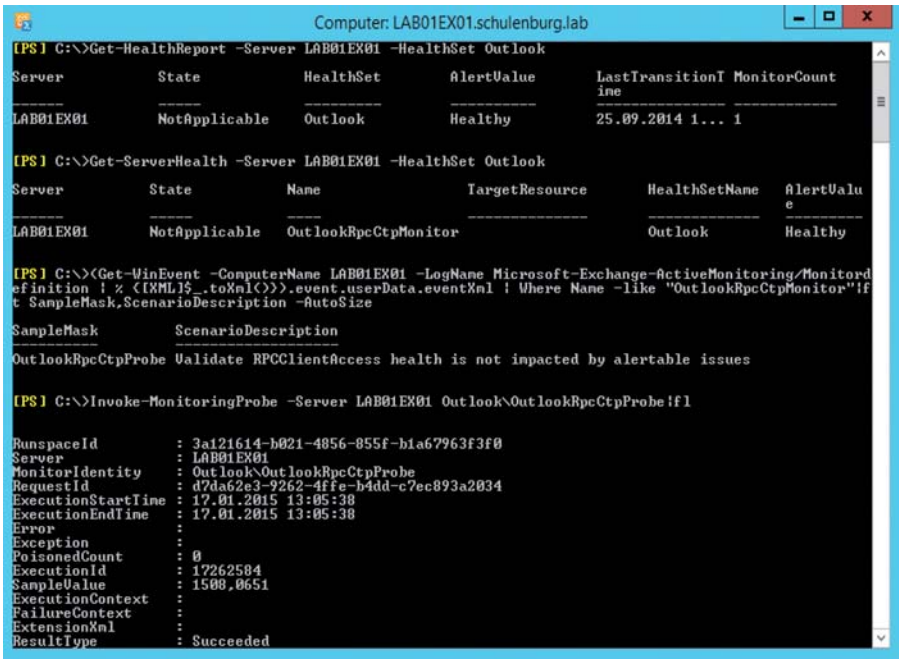


Bild 3: Die aufgeführten Befehle unterstützen Sie im Fehlerfall bei der Lokalisierung eines Problems.

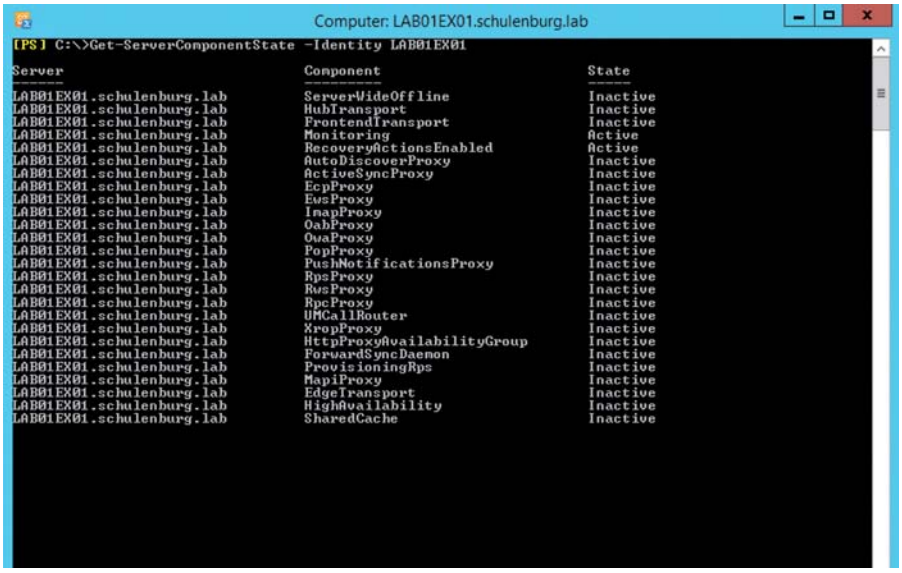


Bild 4: Der Komponentenstatus eines Exchange-Servers, der in Wartung versetzt wurde.

```
-PropertyValue 0 -Duration
60.00:00:00 -Confirm:$FALSE
```

Prüfen können Sie die Umsetzung mit *Get-ServerMonitoringOverride*. Das oben angesprochene Problem bei der Active Directory-Abfrage deaktivieren Sie für alle Server global mit folgendem Befehl:

```
Add-GlobalMonitoringOverride -Iden-
tity Exchange\ActiveDirectoryCon-
nectivityConfigDCServerReboot
-ItemType Responder -PropertyName
Enabled -PropertyValue 0 -Duration
60:00:00:00
```

Die Konfigurationsänderung prüfen Sie wieder im Event Log oder mit dem folgenden PowerShell-Befehl:

```
(Get-WinEvent -LogName Microsoft-Ex-
change-ActiveMonitoring/responder-
definition | %
{[XML]$_.toXml()}).event.userData.
eventXml | Where Name -like "Acti-
veDirectoryConnectivityConfigDCSer-
verReboot" | ft Name,Enabled
```

Lokale Ausnahmen löschen Sie mit *Remove-ServerMonitoringOverride* und globale Einstellungen entfernen Sie mit *Remove-ServerMonitoringOverride*.

Wartung durchführen

Durch die eingebaute Überwachung sollten Sie MA über Wartungsarbeiten informieren, damit MA und die Wartungsarbeiten nicht gegenläufige Aktionen durchführen und am Ende der Server durch einen Blue Screen neu gestartet wird. So werden zum Beispiel beim Einspielen eines Cumulative Updates Dienste angehalten oder deaktiviert und MA sollte in diesen Fällen nicht eingreifen. Aus diesem Grund zeigen wir im Folgenden die Schritte, wie eine Wartung korrekt angezeigt wird. Das Vorgehen unterscheidet sich dabei zwischen Standalone-Servern und DAG-Mitgliedern. Aufgrund der hohen Verbreitung gehen wir von einem DAG-Mitglied aus.

Einen einfachen Wartungsmodus gibt es bei Exchange nicht. Sie müssen verschiedene PowerShell-Befehle ausführen, um alle Komponenten geordnet in die Wartung zu überführen und wieder zurückzuholen.

Damit keine Nachrichten während des Vorganges hängen bleiben, leeren Sie zunächst die Warteschlangen, bevor der Transport deaktiviert wird. Diese Aktion ist nur auf Servern mit der Mailboxrolle nötig, da ein Client Access Server (CAS) keine Warteschlangen hat, sondern nur als Proxy fungiert. Stoppen Sie die Mailzustellung und sorgen Sie für die Abarbeitung der Warteschlange. Dies erreichen Sie durch den Status "Draining":

```
Set-ServerComponentState LAB01EX01
-Component HubTransport -State
Draining -Requester Maintenance
```

Da es durch erneute Zustellversuche länger dauern kann, bis eine Nachricht aus der Warteschlange abgearbeitet ist, können Sie die Nachricht aus der Warteschlange auf einen anderen Server verlagern, damit dieser die Aufgabe übernimmt:

```
Redirect-Message -Server LAB01EX01
  -Target LAB01EX02.schulenburg.lab
```

Um zu prüfen, ob die Warteschlangen leer sind, nutzen Sie den folgenden Befehl:

```
Get-Queue -Server LAB01EX01 | Select
  Identity,MessageCount
```

Bei DAG-Mitgliedern pausieren Sie den Clusterknoten und verschieben die Datenbanken. Darüber hinaus blockieren Sie die Aktivierung einer DAG-Kopie:

```
Suspend-ClusterNode LAB01EX01
Set-MailboxServer LAB01EX01 -Data-
  baseCopyActivationDisabledAndMoveNow
  $true
Set-MailboxServer LAB01EX01 -Data-
  baseCopyAutoActivationPolicy Blocked
```

Damit zum Abschluss nicht alle Komponenten einzeln inaktiv gesetzt werden, gibt es die Erweiterung "ServerWideOffline":

```
Set-ServerComponentState LAB01EX01
  -Component ServerWideOffline
  -State Inactive -Requester
  Maintenance
```

Mit *Get-ServerComponentState* prüfen Sie wiederum, ob alle Komponenten auf "Inaktiv" stehen. Das Ergebnis mit einem in den Wartungsmodus versetzten Server sehen Sie in Bild 4. Einen reinen CAS-Server setzen Sie mit dem letzten Befehl in den Wartungsmodus. Die anderen Schritte entfallen, da der Server weder Warteschlangen noch Datenbank hält.

Wartungsmodus beenden

Um die Wartung zu beenden, aktivieren Sie zunächst alle Komponenten und setzen die DAG-Mitgliedschaft wieder fort, damit sich Datenbanken wieder in Betrieb nehmen lassen:

```
Set-ServerComponentState LAB01EX01
  -Component ServerWideOffline -State
  Active -Requester Maintenance
Resume-ClusterNode LAB01EX01
Set-MailboxServer LAB01EX01 -Data-
  baseCopyActivationDisabledAndMove-
  Now $false
Set-MailboxServer LAB01EX01 -Data-
  baseCopyAutoActivationPolicy Un-
  restricted
```

Zum Abschluss aktivieren Sie wieder den Transportdienst, damit E-Mails wieder übermittelt werden:

```
Set-ServerComponentState LAB01EX01
  -Component HubTransport -State
  Active -Requester Maintenance
```

Nun starten Sie den Transportdienst neu:

```
Restart-Service MSExchangeTransport
Restart-Service MSExchangeFrontEnd-
  Transport
```

Bei einem reinen CAS ist der erste Befehl zum Beenden des Wartungsmodus ausreichend. Auch hier muss der Transportdienst (MSExchangeFrontEndTransport) neu gestartet werden, damit Anpassungen umgehend umgesetzt werden.

Wichtige Managed Availability-Befehle

Befehl	Beschreibung
Get-ServerHealth	Abruf einzelner Integritätsinformationen und deren aktuelle Zustände (fehlerfrei oder fehlerhaft).
Get-HealthReport	Abruf einer zusammenfassenden Statusinformation einzelner Health Sets mit deren aktuellen Stati.
Get-MonitoringItemIdentity	Anzeige der Tests, Monitore und Responder für einen bestimmten Health Set.
Get-MonitoringItemHelp	Anzeige von Beschreibungen einiger Eigenschaften von Tests, Monitoren und Respondern.
Add-ServerMonitoringOverride	Erstellen einer lokalen, serverspezifischen Außerkraftsetzung eines Tests, Monitors oder Responders.
Get-ServerMonitoringOverride	Anzeige einer Liste lokaler Außerkraftsetzungen auf dem angegebenen Server.
Remove-ServerMonitoringOverride	Entfernen einer lokalen Außerkraftsetzung von einem bestimmten Server.
Add-GlobalMonitoringOverride	Erstellen einer globalen Außerkraftsetzung für eine Gruppe von Servern.
Get-GlobalMonitoringOverride	Anzeige einer Liste globaler Außerkraftsetzungen in der Organisation.
Remove-GlobalMonitoringOverride	Entfernen einer globalen Außerkraftsetzung.
Set-ServerComponentState	Konfiguration des Status einer oder mehrerer Komponenten.
Get-ServerComponentState	Anzeige des Status einer oder mehrerer Komponenten.

Der Exchange-Server ist im Anschluss wieder vollständig einsatzbereit. Prüfen Sie das Ergebnis mit *Get-HealthReport*. Beachten Sie, dass die Datenbank zwischen den DAG-Mitgliedern nicht automatisch zurückgeschoben wird und Sie dies manuell durchführen müssen.

Fazit

In Exchange 2013 hat sich bei der Serverüberwachung durch die neue Funktion Managed Availability viel geändert. Der Workshop sollte Ihnen viele nützliche Informationen geliefert haben, um den Umgang mit der neuen Selbstüberwachung von Exchange leichter zu machen. Die wichtigsten MA-Kommandos sind noch einmal in der Tabelle "Wichtige Managed Availability-Befehle" zusammengefasst. *(ln)*

[1] Exchange 2013 restarts frequently after CU2 is installed
F3Z61

[1] Exchange Server 2013 restarts with Stop Error
F3Z62

Link-Codes

Know-how: *Aufbau und Betrieb von organisationsweitem Security-Monitoring*

Wichtiges sehen, Gefährliches bekämpfen

von Felix von Eye, Wolfgang Hommel und Stefan Metzger

Täglich entstehen im IT-Betrieb unzählige Daten, in denen sich sicherheitsrelevante Informationen verbergen. Doch händisch ist diesem Datenmeer keine sinnvolle Information abzuringen. Security Information & Event Management-Systeme sollen helfen, die organisationsweite Sicherheitslage der IT abzubilden. Dies kann jedoch nur funktionieren, wenn IT-Verantwortliche beim Design der SIEM- und Sensorarchitektur einige wichtige Grundregeln beachten. Im Folgenden stellen wir die wichtigsten Eckpunkte vor, die bei der Auswahl eines SIEM-Systems und beim Design des Zusammenspiels mit Datenquellen und nachgeordneten Systemen zu berücksichtigen sind.

Ein gut organisiertes Monitoring umfasst nicht nur klassische Kennzahlen wie etwa zur Verfügbarkeit, Auslastung und Antwortzeit von Diensten und Systemen, sondern gibt auch Auskunft über die aktuelle Lage aus Perspektive der IT-Sicherheit. Eine wichtige Voraussetzung dafür ist, dass sicherheitsrelevante Logfile-Einträge von Applikationen und dedizierten Sicherheitskomponenten wie Intrusion Detection-Systemen zentral zusammengeführt, korreliert und als Ganzes ausgewertet werden. Auf diese Aufgabe haben sich Security Information & Event Management (SIEM)-Systeme spezialisiert, von denen sich inzwischen einige Open Source- und zahlreiche kommerzielle Vertreter etabliert haben.

Wichtige Auswahlkriterien

Wie bei anderen Monitoring-Tools sind Funktionalität, Skalierbarkeit und Kosten drei offensichtliche Kriterien für die Auswahl eines SIEM-Produkts. Funktional liegen viele Produkte nahezu gleichauf und unterscheiden sich überwiegend durch Features, deren Sinn und Notwendigkeit im jeweiligen Einsatzszenario zu prüfen ist. Dies trifft leider auch auf fehlende Funktionalität zu: Beispielsweise ist eine durchgängige Unterstützung von IPv6 auch Anfang 2015 immer noch rar.

Die Skalierbarkeit wird üblicherweise in der Anzahl von Sicherheitsmeldungen pro Sekunde, die vom SIEM-System entgegengenommen und verarbeitet werden, gemessen. Einige Open Source- und Community-Edition-Varianten sind diesbezüglich zum Teil künstlich auf eine zweistellige Anzahl von Events pro Sekunde (EPS) beschränkt und eignen sich deshalb nur für kleinere Umgebungen oder einen sehr selektiven Einsatz. Bei kommerziellen Produkten, an die beispielsweise auch NetFlows von Routern als Datenquelle angebunden werden, sind sechsstellige EPS-Zahlen keine Seltenheit, aber häufig auch Bemessungsgrundlage für die Lizenzkosten.

SIEM-Architektur

Bild 1 zeigt die typische Architektur eines SIEM-Systems: Es bindet über SIEM-Kollektoren verschiedenste Datenquellen wie Server, Netzkomponenten, Managementsysteme, Firewalls und Intrusion Detection-Systeme an und konvertiert deren Sicherheitsmeldungen in ein einheitliches, SIEM-internes Format. SIEM-Prozessoren korrelieren diese Meldungen systemübergreifend und werten sie regelbasiert aus.

Das SIEM-Frontend ist bei den meisten aktuellen Produkten webbasiert und dient den Administratoren zur interaktiven Konfiguration des Systems und der Auswertung erkannter Sicherheitsprobleme. Diese verwalten die meisten SIEM-Systeme in einer Art integriertem Ticketsystem und ermöglichen so Drill-Down-Ansichten auf die auslösenden Meldungen der Datenquellen. Für Alarmierungen und automatisierte Reaktionen lassen sich nachgeordnete Systeme anstoßen. Eine je nach Produkt mehr oder weniger umfangreiche Scripting-Schnittstelle oder API ermöglicht das Manage-

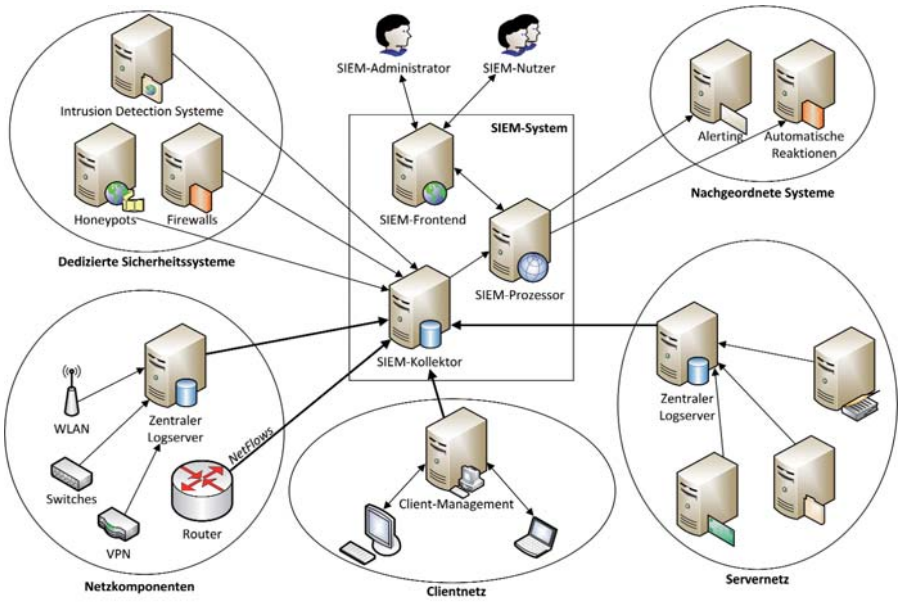


Bild 1: Architektur eines SIEM-Systems mit Datenquellen und nachgeordneten Systemen.

ment des SIEM-Datenbestands durch eigenen Code und ergänzt so die interaktive Arbeit mit dem SIEM-System.

Aufgaben der SIEM-Grundkonfiguration

Die Voraussetzung dafür ist beispielsweise das Befüllen des SIEM-internen Asset Managements, idealerweise durch Anbindung an eine vorhandene DCIM-Lösung oder ein Configuration Management-System. Daraus erschließen sich beispielsweise die Kritikalität einzelner Systeme und grundlegende Eigenschaften wie das eingesetzte Betriebssystem und die Position im überwachten Netz: Falls später zum Beispiel ein Intrusion Detection-System einen Angriff zur Ausnutzung einer aktuellen Windows-Sicherheitslücke meldet, kann das SIEM-System anders reagieren, wenn das Ziel ein kritischer Windows-Server im Produktionsnetz ist als wenn es um einen Linux-Server im Testlabor geht. Der Aufwand für das Einbringen solcher Basisinformationen ist hoch, insbesondere wenn die Daten nicht einfach aus bereits vorhandenen Systemen importiert werden können. Viele Produkte enthalten als Alternative eine Auto Discovery-Funktion, die Sie jedoch nur nutzen sollten, wenn Sie sicherstellen können, dass sich dadurch keine Inkonsistenzen mit anderen Datenbeständen ergeben. Letztere können im laufenden Betrieb mehr Aufwand verursachen, als Sie sich durch anderweitigen Import oder manuelles Eintragen ersparen.

Ebenso sollten Sie vorab festlegen, welche Benutzer mit welchen Berechtigungen mit dem SIEM-System arbeiten werden. Anbindungen an zentrale Authentifizierungsinstanzen wie LDAP-Server oder Active Directory gehören zum Standardumfang. Da über Drill-Down-Möglichkeiten zum Teil auf sensible Details aus Logfiles und IP-Paketen zugegriffen werden kann, entscheidet das Need-to-Know-Prinzip über individuelle Berechtigungen. Viele SIEM-Frontends stellen hübsch anzuschauende Dashboards mit Übersichten und Statistiken bereit, für die sich auch Vorgesetzte und Entscheider interessieren; diese Nutzergruppe muss aber nicht zwingend mit weiterführenden technischen Details und Bearbeitungsmöglichkeiten irritiert werden. Da nachträgliche größere Änderungen an Rollen und Berechtigungen möglicherweise unbeabsichtigte Seiteneffekte haben, empfiehlt es sich, mit den entsprechenden Einstellungen vorab in einer Testinstallation zu experimentieren.

Die richtigen Datenquellen nutzen

Die Anbindung der eigentlichen SIEM-Datenquellen verfolgt zwei ähnliche, aufeinander aufbauende Ziele. Zum einen sollen die Sicherheitsmeldungen möglichst aller relevanten Systeme an zentraler Stelle zusammengeführt werden. Dies reduziert den Aufwand auf jedem einzelnen System, etwa in den Logfiles nach sicherheitsrelevanten Einträgen suchen zu müssen. Zum anderen soll systemübergreifend korreliert werden, um komplexere Angriffsmuster erkennen und nachvollziehen zu können, deren einzelne Teile auf den einzelnen Systemen ansonsten vielleicht im Grundrauschen untergehen würden. Zur Übermittlung der Daten aus der jeweiligen Quelle an das SIEM-System stehen in der Regel verschiedene Optionen zur Verfügung, von der Konfiguration des SIEM-Systems als zentraler Logserver über die Installation von SIEM-Agent-Software auf dem Quellsystem bis zum regelmäßigen Abruf ganzer Logfiles über Secure-Copy oder SFTP. Jedes SIEM-System bringt Unterstützung für einige weit verbreitete Logfile-Formate out-of-the-box mit. Anders formatierte Logfile-Einträge erfordern eine zusätzliche Parser-Konfiguration, die je nach Hersteller über eine einfache Regelsprache oder reguläre Ausdrücke erstellt werden kann. Üblicherweise erfolgt die Anbindung von Datenquellen ans SIEM-System hierarchisch kaskadiert: Wenn beispielsweise bereits ein zentraler Logserver von diversen Servern und Diensten genutzt wird, wird nur dieser ans SIEM-System angeschlossen und nicht jeder einzelne Server. Auch wenn beispielsweise auf Arbeitsplatz-PCs und anderen Clients gefundene Malware ausgewertet werden soll, bietet es sich an, den zentralen Antivirus-Management-Server ans SIEM-System anzubinden und nicht jeden einzelnen Client direkt.

Unabhängig von den Grenzen, die dem auswertbaren Datenvolumen durch Hardware und SIEM-Lizenzierung gesetzt werden, müssen Sie bei der Einführung einer SIEM-Lösung überlegen, welche Datenquellen überhaupt sinnvoll sind. Faustregel ist, dass Sie nur solche Quellen anbinden sollten, deren Meldungen durch Analyse- und Korrelationsregeln automatisch ausgewertet werden oder die regelmäßig bei der manuellen Prüfung und Bearbeitung von Sicherheitsvorfällen relevant sind. Insbesondere bei SIEM-Produkten von Herstellern aus dem Netzbereich gehört es zum guten Ton, neben verschiedensten Logfiles von Servern und Netz- sowie Sicherheitskomponenten auch NetFlow-Informationen von IP-Routern einzuspeisen. Mehrere Hersteller kombinieren ihr SIEM-System mit Deep-Packet-Inspection-fähigen Intrusion Detection-Systemen und können somit auch Layer 7-Auswertungen vorneh-

Bild 2: Typische SIEM-Dashboardansicht mit Fokus auf beobachtete Signaturen.

men. Als Vorteil erweist sich dabei die Integration verschiedener Security-Funktionen unter einer gemeinsamen Benutzeroberfläche: Stellt sich beispielsweise auf Basis der Kommunikation mit einem bekannten Command-and-Control-Server im Internet heraus, dass ein System kompromittiert und mit Malware infiziert wurde, lässt sich schnell zusammenstellen, welche weiteren ungewöhnlichen Kommunikationsziele der Maschine es gegeben hat, die auf einen Missbrauch zum Sprung ins eigene interne Netz oder beispielsweise eine Beteiligung an DDoS-Angriffen auf Dritte im Internet hindeuten.

Neben dem eher passiven Empfangen oder Abrufen von Sicherheitsmeldungen von den Datenquellen sind in viele SIEM-Systeme auch aktive Mechanismen zur Informationsakquise integriert oder können modular nachgerüstet werden. Das Spektrum erstreckt sich von relativ einfachen Portscannern wie nmap bis zu kompletten Vulnerability-Management-Lösungen, bei denen die überwachten Systeme regelmäßig oder auf Knopfdruck Scans mit Tools wie OpenVAS unterzogen werden können. Die dabei gewonnenen Ergebnisse können nicht nur bei der Aufklärung gemeldeter Sicherheitsvorfälle helfen, sondern werden in der SIEM-internen Asset-Datenbank gespeichert und können bei nachfolgenden Analysen und Korrelationen und insbesondere bei zur Priorisierung vorgenommenen Bewertung von Alarmmeldungen herangezogen werden.

Eine hübsche Oberfläche ist nicht alles

Einsatzschwerpunkt aktueller SIEM-Produkte ist die interaktive Auswertung der erkannten Sicherheitsprobleme. Die SIEM-Produkte unterscheiden sich zum Teil stark in ihrer Bedienphilosophie und in der zur Gestaltung der Bedienoberfläche eingesetzten Technologie. Der möglichst intuitive und effiziente Umgang mit dem SIEM-GUI ist deshalb aus Administratorsicht meist das wichtigste Akzeptanzkriterium für ein SIEM-Produkt – träge Weboberflächen oder die fehlende Unterstützung für Kontextmenüs über die rechte Maustaste bei Flash-basierten GUIs können dabei schnell zum Produktivitätskiller werden.

Neben der Bearbeitung von Sicherheitsvorfällen ist ein Hauptaspekt bei der täglichen Arbeit mit dem SIEM-System die kontinuierliche Optimierung der Regelsätze auch unter der Zielsetzung, unnötige Meldungen und Fehlalarme (False Positives) zu minimieren, damit sich das Security-Team auf die wirklich wichtigen Fälle konzentrieren kann. Über die Ansicht einer Sicherheitsmeldung im SIEM-GUI sollten deshalb nicht nur vertiefende Informationen im Sinne eines Drill-Downs einfach abrufbar sein, sondern sich auch ähnliche Fälle einfach finden und das Zustandekommen der Meldung durch die Analyse- und Korrelationsregeln genau nachverfolgen lassen. Bei akuten Fällen, in denen noch laufende Angriffe beobachtet werden können, ist zudem die Latenz entscheidend, mit der neue Meldungen über das SIEM-GUI eingesehen werden können. Nahezu Echtzeit-fähige SIEM-Systeme spielen hier ihre Vorteile gegenüber Produkten aus, die neu eingehende Daten lediglich intervallgesteuert im Blockbetrieb abarbeiten.

Automatisierung vereinfacht das Tagesgeschäft

Oft fehlt Administratoren im Tagesgeschäft die Zeit, regelmäßig proaktiv im SIEM-GUI nachzusehen, ob neue wichtige Meldungen vorliegen. SIEM-Systeme bieten deshalb in der Regel ein konfigurierbares Eskalationssystem an, das zum Beispiel mit regelmäßigen Erinnerungs-E-Mails verhindern soll, dass wichtige Meldungen unbearbeitet liegen bleiben. Wichtig ist auch hierbei, dass etwa über Ausnahmeregelungen festgelegt werden kann, über welche Vorfallstypen oder betroffenen Systeme keine Alarme generiert werden sollen, um E-Mail-Fluten zu vermeiden.

Da auf viele Arten von Sicherheitsvorfällen sehr ähnlich reagiert werden muss, bietet es sich an, zumindest unkritische Teile davon ebenfalls zu automatisieren. Während einige SIEM-Produkte analog zu diversen Monitoring-Systemen primär als reine Datensenken fungieren, bieten andere die Möglichkeit, im Kontext des Anlegens einer neuen internen Meldung oder beim Eintritt von Eskalationskriterien beliebige Skripte oder Programme anzustoßen, denen die individuellen Parameter des Vorfalls als Parameter übergeben oder über eine Programmierschnittstelle zugänglich gemacht werden. Fällt also beispielsweise ein Mitarbeiter-PC im Client-Netz durch ein charakteristisches Malware-Kommunikationsverhalten auf, könnte er beispiels-

Bild 3: Ansicht eines SIEM-Dashboards mit Quelle und Ziel von Sicherheitsvorfällen.

weise parallel zur Alarmierung des zuständigen Administrators per Skript an der Firewall des Internet-Uplinks oder direkt am Switch-Port des entsprechenden Büros gesperrt werden, um größeren Schaden zu verhindern. Wie bei allen automatisierten Reaktionen muss jedoch darauf geachtet werden, dass ein Angreifer sie nicht gezielt ausnutzen kann, um noch mehr Schaden etwa durch Denial-of-Service zu verursachen, als eigentlich verhindert werden soll.

Sinnvolle Regelsätze erstellen

Neben einer möglichst genauen Beschreibung der eigenen Infrastruktur, dem Asset-Management oder -Modeling müssen Sie entweder die meist zahlreichen, bereits vom Hersteller einer SIEM-Lösung zur Verfügung gestellten Korrelationsregeln auf die eigene Umgebung und ihre Besonderheiten hin anpassen oder unternehmensspezifische Regelsätze erstellen. Korrelationsregeln beschreiben, vereinfacht ausgedrückt, Bedingungen, die ein von einem Security-Monitoring-Sensor gemeldetes Ereignis erfüllen muss und die, sollten alle Bedinungen einer Regel erfüllt sein, anschließend automatisch ausgelöste Reaktion der SIEM-Lösung.

Als sehr einfache Bedingung kann etwa das Zählen eines bestimmten Ereignistyps, zum Beispiel eine von einem IDS erkannte und an das SIEM weitergeleitete Kommunikation mit einem Command-and-Control-Server eines bekannten Botnetzes, von derselben Quell-IP-Adresse innerhalb eines bestimmten Zeitraumes betrachtet werden. Übersteigt die gezählte Ereignisanzahl einen ebenfalls in der Korrelationsregel definierten Schwellenwert, erfolgt die in der Regel beschriebene Reaktion, die etwa in einer E-Mail-Benachrichtigung des zuständigen Administrators, dem Aufruf eines Skripts, dem automatisiert als Parameter die Quell- und Ziel-IP-Adressen, der Zeitpunkt des Auftretens oder der ermittelte Event-Counter übergeben werden, oder dem Erzeugen eines neuen Ereignisses, das wiederum in die SIEM-Lösung für weitere Korrelationsschritte eingespeist wird, bestehen kann. Über das einfache Zählen hinaus lassen sich auch komplexe und verschachtelte Bedingungen zu einer Regel zusammenfassen.

Dabei lässt sich – um einer E-Mail-Flut zu begegnen – über einen Limitierungsparameter die Anzahl der verschickten Benachrichtigungs-E-Mails auf beispielsweise eine pro Minute, basierend auf der Ziel-IP-Adresse, begrenzen. In der Praxis weisen jedoch derart auf Signaturen basierende Erkennungsmethoden, die den während der Kommunikation zwischen zwei IT-Systemen übertragenen Inhalt auswerten, eine Reihe von Schwächen auf. Typischerweise findet die Kommunikation zwischen einem mit einer Malware infizierten IT-System und den CC-Servern verschlüsselt statt. Die hierbei übertragene Payload ist also im Klartext nicht sichtbar und das sicherheitsrelevante Ereignis lässt sich nicht einfach erkennen. Als Lösung bietet die NetFlow-basierte Korrelation einer SIEM-Lösung eine Erkennungsmöglichkeit, bei der entweder die Überschreitung eines vom SIEM-Administrator definierten Schwellenwertes oder die Abweichung von einem durch die SIEM-Lösung selbst erlernten typischen Kommunikationsverhalten zu einer Alarmierung des Systembetreibers führt.

Auch die Alarmierung kann dabei in mehreren Stufen erfolgen. So erzeugt das erste Auftreten einer bestimmten Auffälligkeit nur ein weiteres, wenn auch bereits korreliertes Ereignis. Tritt dieselbe Auffälligkeit innerhalb eines bestimmten Zeitintervalls mehrfach oder in Kombination mit anderen, ebenfalls korrelierten Ereignissen auf, so ist dies nun der Auslöser für eine E-Mail- oder SMS-Benachrichtigung des Systemverantwortlichen. Über das Einbeziehen des Zeitpunktes, zu dem die Auffälligkeit erkannt wurde, lassen sich von der Tageszeit abhängige Reaktionen definieren. Beispielsweise erfolgt während der üblichen Bürozeiten eine E-Mail-Benachrichtigung des Systemadministrators, während die Kommunikation nachts automatisch durch eine Skript-gesteuerte Umkonfiguration des Switchports oder Erstellung spezifischer Firewallregeln gestoppt wird.

Updates genau planen

Neben den angebundenen Datenquellen gilt es, die SIEM-Lösung regelmäßig, insbesondere dann, wenn Security-Updates oder eine neue Software-Version, die für ein Unternehmen interessante Funktionen bietet, anstehen, zu aktualisieren. Neben Fehlerbehebung, Schließen vorhandener Sicherheitslücken zielt dies auch auf Änderungen bei der Verarbeitung neuer oder geänderter Logformate oder die Unterstützung einer effizienteren Möglichkeit der Anbindung einer Datenquelle. Für das Upgrade der SIEM-Lösung sollten Sie sich jedoch die Vorgehensweise genau überlegen. Ein vor dem Update durchgeführtes Backup sämtlicher Ereignisse und der aktuellen SIEM-Konfiguration sollte gängige Praxis sein. Da das Upgrade eine Zeit dauern kann, sollten Sie zuvor sichergestellt haben, dass die Datenquellen Ereignisse, die während der temporären Nichterreichbarkeit der SIEM-Lösung erkannt werden, für einen kurzen Zeitraum zwischenpuffern.

Aber nicht nur auf eine durch ein Update hervorgerufene Unterbrechung sollte zuverlässig reagiert werden, sondern auch, wenn etwa in der Software vorhandene Speicherlecks oder ein durch einen Programmierfehler verursachter Pufferüberlauf auftreten. Insofern sollten Sie auch integrierte Systemmonitoring-Mechanismen, aber vor allem auch ein entferntes System-Monitoring etablieren, um zeitnah über den aktuellen Systemzustand informiert zu sein und entsprechende Maßnahmen einleiten zu können.

Fazit

Die Bedeutung von SIEM-Systemen für den sicheren Betrieb großer, heterogener und verteilt administrierter Infrastrukturen steigt. Mit Möglichkeiten zur Korrelation, Aufbereitung und automatisierten Verarbeitung von Sicherheitsmeldungen verschiedener Dienste, Systeme und Komponenten sind sie ein fähiges Werkzeug. Die Einführung und der Betrieb gelingen aufgrund der Komplexität von SIEM-Systemen aber nicht einfach nebenher. Vielmehr müssen Sie einiges an Zeit und Sorgfalt in die Produktauswahl, Planung, Basiskonfiguration, Anbindung von Datenquellen und Konfiguration von Analyseregeln und Automatismen investieren, um das Potenzial auszuschöpfen. Trotz sich abzeichnender Produktreife bleibt als Wermutstropfen, dass die Ansteuerung nachgeordneter Systeme noch weitgehend mit eigenen Skripten implementiert werden muss. Es bleibt zu hoffen, dass sich die Produkte auch in diesem Bereich noch weiterentwickeln. *(jp)* IT

PowerShell 4.0 für die Windows-Administration

Das vorliegende Buch ist bestrebt, alle nötigen theoretischen Aspekte für den Einsatz der PowerShell zu liefern, den administrativen Alltag zu automatisieren und vereinfachen sowie einen Ausblick auf Desired State Configuration (DSC) – dem von Microsoft in der Zukunft geplanten Standard in Sachen Server-Konfiguration – zu liefern.

Die historische Entwicklung und die ersten Schritte mit der PowerShell nehmen knapp zehn Prozent des Buchumfangs ein und genügen bereits, um den elementaren Einsatz der PowerShell zu bewältigen. Nach einem kurzen Abriss über die PowerShell-Cmdlets analysiert Autor Peter Monadjemi das zentrale Element – die Objektpipeline – ausführlich. Das Verständnis dieses Abschnitts ist insbesondere für Admins aus dem Linux-Umfeld oder jene, die in erster Linie mit der Windows-Befehlszeile arbeiten, grundlegend. Neben der Bedeutung des Objekts im Allgemeinen stellt Monadjemi auch die Cmdlets vor, die speziell für die Abarbeitung des Pipeline-Inhalts zur Verfügung stehen.

Mit viel theoretischem Background, wenn auch fachgerecht aufbereitet, arbeitet sich der Leser beim Durcharbeiten der Folgekapitel weiter, indem er das Provider-Konzept, PowerShell ISE – Testen mit Hilfe des integrierten Debuggers beim Ausführen von Skripten –, die Fehlerbehandlung und Module sowie Snap-ins kennenlernt. Dazwischen zeigen praktische Beispiele, wie Ad-hoc-Administration, der Zugriff auf das Active Directory oder die Verarbeitung von Texteingaben erfolgen. Seit Windows Server 2012 R2 gibt es mit DSC zudem einen Ausblick auf die Serverkonfiguration der Zukunft. Mit insgesamt fünf Seiten wird das Thema aber nur grob gestreift. Der Aufbau von Remote Sessions mit Azure kommt ebenfalls eher kurz – der umfangreiche Satz an Cmdlets zur Konfiguration von Azure-Umgebungen ist nicht Bestandteil des Buches.

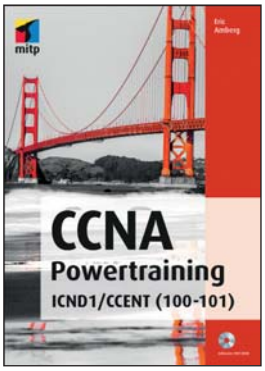
Fazit

Der grundlegende Tenor des Buches ist akademischer Natur, weswegen sich die Lesbarkeit etwas zähflüssig gestaltet. Dennoch sind die Ausarbeitungen gründlich und insbesondere die primär theoretischen Abschnitte zur Objektpipeline, dem Provider-Konzept oder der PowerShell ISE lassen kaum Fragen offen. Die knapp über 500 Seiten umfassende Dokumentation weiß ihre Stärken in der Kompaktheit und Vermittlung der PowerShell-Philosophie.

Frank Große

Autor	Peter Monadjemi
Verlag	Springer Verlag
Preis	29,99 Euro
ISBN	978-3658029630
Bewertung *(max. 10 Punkte)*	**7**

CCNA Powertraining



Die Zertifizierungen von Cisco gelten nach wie vor als die anspruchsvollsten. Aus diesem Grund möchte das vorliegende Buch die nötige Hilfestellung geben und sowohl auf die Anforderungen an die Zertifizierungen als auch auf die Prüfungen optimal vorbereiten.

Die ICND1-Prüfung ist zu großen Teilen auf die Praxis ausgerichtet, was die Vorbereitung erschwert. Autor Eric Amberg hat sich deshalb darauf konzentriert, die Theorie anschaulich zu vermitteln und praktische Szenarien der täglichen Arbeitsumgebung im Cisco-Umfeld nachzustellen. Das ist ihm mittels Workshops samt Schritt-für-Schritt-Anleitungen ausgesprochen gut gelungen. Detaillierte Erklärungen inklusive Hinweise auf entsprechend eingesetzte Software lassen kaum Fragen offen und erlauben dem Leser, das Netzwerk quasi zu erleben. Auch wenn sich die fünf Abschnitte des Buches an den Inhalten der CCENT-Prüfung orientieren, gehen die Inhalte praktischerweise zum besseren Verständnis über das geforderte Prüfungswissen hinaus. Das schließt insbesondere in den theoretischen Abschnitten potentielle Wissenslücken, was dem Leser erlaubt, die Thematik Netzwerk wirklich zu verstehen.

Neben den theoretischen Aspekten zu Netzwerk-Grundlagen findet sich Wissenswertes zu Ethernet und Switching-Technologien, VLANs sowie VLAN-Trunking und die Absicherung eines Switches. Die Planung von IPv4-Netzwerken inklusive Subnetting und VLSM fehlt ebenso wenig wie WAN-Technologien, ACL und NAT. Das finale Kapitel konzentriert sich ausschließlich auf IPv6 und dessen Konfiguration unter Windows, Linux und Cisco bis hin zu OSPF und Neighbor Discovery. Dass die Inhalte dabei nicht ausschließlich auf die knapp 1.000 Seiten beschränkt sind, kommt der Publikation nur zugute. Fünf Stunden Videotraining, zahlreiche prüfungsvorbereitende Fragen und über 100 Flashcards zum Vertiefen der theoretischen Aspekte sollten nicht nur mögliche Prüfungsangst verbannen.

Fazit

Das CCNA Powertraining ist keineswegs nur ein Buch zur Prüfungsvorbereitung, sondern möchte zwei Aspekte abdecken: Zum einen soll das Verständnis für die Funktionsweise der jeweiligen Technologie geweckt werden, zum anderen bieten praxiserprobte Szenarien (und deren Lösung) das Rüstzeug für den täglichen Umgang mit Cisco-Geräten – was ganz nebenbei eine gelungene Vorbereitung auf die Prüfung darstellt. *Frank Große*

Autor	Eric Amberg
Verlag	mitp Verlag
Preis	49,99 Euro
ISBN	978-3826616945
Bewertung *(max. 10 Punkte)*	**10**

Besser informiert: Mehr Fachartikel auf www.it-administrator.de

Unser Internetauftritt versorgt Sie jede Woche mit neuen interessanten Fachartikeln. Als Heftleser können Sie über die Eingabe des Link-Codes schon jetzt exklusiv auf alle Online-Beiträge zugreifen.

End2End-Monitoring mit dem Open Source-Tool Sakuli

Das Monitoring kritischer Applikationen setzt auf eine Vielzahl von Checks. Aus deren Summe lässt sich jedoch kein qualifizierter Gesamtstatus ableiten. Hier ist End2End-Monitoring gefragt, etwa mit dem Open Source-Tool Sakuli. Es simuliert Maus- und Tastatureingaben des Anwenders in der Applikation, wertet Inhalte aus, misst Laufzeiten und integriert die Ergebnisse in Nagios. Dabei vereint es die Stärken der Test-Werkzeuge Sahi und Sikuli. Wir beschreiben im Online-Artikel, wie Sie mit Sakuli funktionelle und inhaltliche Störungen frühzeitig erkennen.

Link-Code: F3W51

Möglichkeiten der Standortvernetzung – Von Ethernet bis MPLS

Die Wahl einer Standortvernetzung zur Anbindung von Unternehmensniederlassungen ans Firmennetz, oder auch mobiler Mitarbeiter im Home Office, stellt jeden Netzwerkadministrator vor eine Herausforderung. Die Entscheidung zwischen Internet-VPN, Ethernet-Netzwerk oder MPLS-VPN ist nicht leicht. Der Beitrag auf unserer Homepage zeigt, welche Faktoren bei der Wahl der Netztechnologie Sie berücksichtigen sollten, um ein optimales Ergebnis für das eigene Unternehmen sicherzustellen.

Link-Code: F3W52

Neun Punkte für ein modernes IP-Adressmanagement

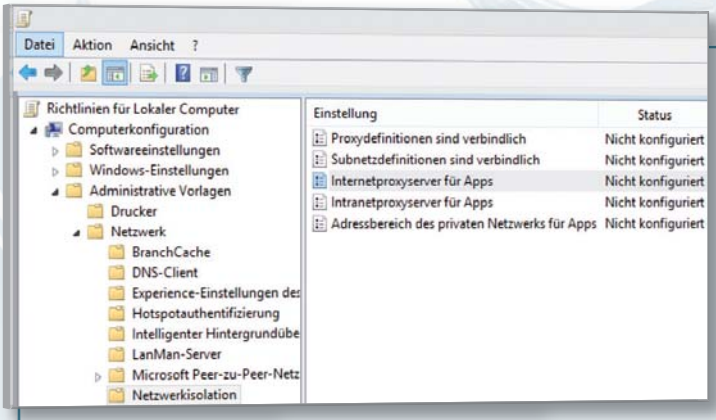
IP-Adressmanagement (IPAM) kann heutzutage in Unternehmen nicht mehr stiefmütterlich behandelt werden. Die Netzwerke werden immer größer, komplexer und dynamischer. Gerade die fortschreitende Virtualisierung mit zahlreichen virtuellen Maschinen sorgt hier schnell für unübersichtliche Verhältnisse. Umso wichtiger sind moderne IPAM-Lösungen, die Kosten reduzieren, Fehler beseitigen und Prozesse beschleunigen. In unserem Online-Fachartikel gehen wir auf neun wichtige Punkte ein, die Sie für ein erfolgreiches IP-Adressmanagement unbedingt berücksichtigen sollten.

Link-Code: F3W53

Office- und Produktions-LAN sicher verbinden

Die unterschiedlichen Anforderungen an das Büro- oder Verwaltungsnetzwerk auf der einen Seite und an das Fertigungs- oder Produktionsnetzwerk auf der anderen Seite bereiten vielen IT-Verantwortlichen Kopfzerbrechen. Was für das eine gut ist, muss für das andere längst keinen Nutzen bringen. Dem Verwaltungsnetzwerk dienliche Maßnahmen wie Anti-Viren-Tools oder Netzwerk-Tests können im Produktionsnetzwerk massiven Schaden anrichten. Der Beitrag im Web stellt die Frage, inwieweit sich beide Welten sicher miteinander verbinden lassen.

Link-Code: F3W54



Windows 8.1 mit Gruppenrichtlinien verwalten

Viele Einstellungen in Windows 8.1 lassen sich mit Gruppenrichtlinien anpassen. Das gilt auch für die Steuerung der Windows-Apps. Die neuen Funktionen in Windows 8.1 stehen allerdings nur zur Verfügung, wenn Sie die Richtlinien lokal einsetzen oder mindestens einen Domänencontroller auf Windows Server 2012 R2 umstellen. Die Anpassungen lassen sich als Gruppenrichtlinien an mehrere Rechner verteilen oder auf Basis einzelner Settings in der lokalen Richtlinienverwaltung von Windows 8.1 in den Editionen Pro und Enterprise. Wir zeigen Ihnen in unserem exklusiven Online-Workshop wichtige Einstellungen und Möglichkeiten, die Server 2012 R2 zusammen mit Windows 8.1 bietet. Dabei gehen wir beispielsweise auf den Offline-Domänenbeitritt sowie die Festplattenverschlüsselung mit BitLocker ein.

Link-Code: F3W55

»Echtzeitanalysen sind für das Monitoring eine Herausforderung«

Innerhalb von 75 Jahren hat sich die Nietiedt-Gruppe vom traditionellen Malerbetrieb zu einem mittelständischen Unternehmen der Bau- und Oberflächentechnik entwickelt. Das Unternehmen beschäftigt in neun Niederlassungen mehr als 450 Mitarbeiter. Für das breite Dienstleistungsspektrum spielt eine funktionierende IT eine maßgebliche Rolle. Timo Hermes (44) ist als Administrator für die Infrastruktur des Unternehmens verantwortlich.

Warum sind Sie IT-Administrator geworden?

Weil mich die IT einfach begeistert hat und sich für mich rechtzeitig verschiedene Türen in diesem Bereich öffneten.

Und warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Der Beruf bedient verschiedene Felder und ist dadurch sehr abwechslungsreich. Zusätzlich trägt man eine große Verantwortung für die IT-Infrastruktur des Unternehmens und hat gleichzeitig engen Kontakt zu vielen interessanten Menschen. Dadurch wird der Arbeitsalltag nie langweilig. Außerdem ist es meiner Einschätzung nach ein Beruf mit Zukunft.

Welche Aspekte Ihres Berufs machen Ihnen am meisten Spaß?

Die Arbeit ist sehr vielseitig und abwechslungsreich. Mir gefällt der Kontakt zu den vielen unterschiedlichen Menschen, mit denen ich zu tun habe. Die meisten meiner Aufgaben sind anspruchsvoll und verlangen eine verantwortungsvolle Handhabung. Das gefällt mir sehr gut.

An welchem Projekt werden Sie in nächster Zeit arbeiten?

Wir arbeiten am Aufbau und der Integration einer kompletten Test-Domäne in eine andere virtuelle Umgebung auf Hyper-V-Basis. Ein weiteres Projekt ist das Netzwerk-Performance-Tuning.

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

Ein richtig lästiges Problem war die Anbindung von externen (USB) ISDN-Controllern zur Übertragung der Faxe an Tobit-David. Die Faxtechnologie ist inzwischen einfach veraltet und anfällig. Die Treiberprogrammierung war und ist schwierig, gerade im Zusammenspiel mit Windows-Systemen.

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

Es würde mir sämtliche Informationen eines Systems frei zusammenstellbar zur Verfügung stellen. Dabei machte es keinen Unterschied zwischen Linux, Mac OS, Windows oder Solaris. Mein Wunschtool könnte über frei anwählbare Funktionen selbstständig Programme schreiben und wäre natürlich Open Source.

Und wie überwachen Sie Ihre IT-Umgebung in der Realität?

Wir nutzen die Lösung PRTG-Netmon von Paessler. Unsere Logdaten werten wir dabei möglichst grafisch aus. In erster Linie, weil die erfassten Daten sich so schneller und übersichtlicher darstellen lassen. Es gibt aber auch Auswertungen, für die das nicht notwendig ist.

Welche Applikation verursacht die größten Kopfschmerzen?

Ein Office-Plug-In für unser Dokumenten-Management-System macht immer wieder Schwierigkeiten. Da die Software zur Zeit noch nicht für Office 2013 freigegeben ist, die Standard PCs aber alle mit einer Office 2013 Version ausgeliefert werden, müssen wir die Systeme mit Office 2010 ausstatten. Und Office ist ja nun einmal bekannt dafür, bei Deinstallation viele Datenreste auf dem Rechner zu lassen. Nur mit speziellen Microsoft-Säuberungspaketen bekommen wir das System dazu, die beschriebenen Plug-Ins ins neu installierte Office 2010 zu integrieren.

Und was ist die größte Herausforderung beim Monitoring?

Eine Herausforderung, wenn auch keine richtig große, sind Echtzeitanalysen. Wollten wir beispielsweise die aktuelle Bandbreitennutzung von 40 Rechnern abgreifen, dann müsste ich das Monitoring auf den LAN-Karten der Rechner in einem Intervall von 1 bis 2 Sekunden abfragen. Unser Standard liegt aktuell bei 60 Sekunden. Was sich noch etwas schwieriger gestaltet, ist das Monitoring von Rechnern, die nicht an eine Domäne angebunden sind.

Gibt es dadurch Bereiche, die sich Ihrem Monitoring gänzlich entziehen?

Mir fallen keine ein. Soweit ich das abschätzen kann, haben wir dank unseres Monitorings alles im Griff.

Wie denken Sie, arbeitet ein Administrator in 10 Jahren?

Ich gehe davon aus, dass wir Administratoren von den unterschiedlichen Orten aus weitestgehend remote arbeiten werden. IT

Das Interview führte Petra Adamik.

Geburtstag: 15. .März 1971
Admin seit: 10 Jahren
Hobbys: Kiten, Inliner, Surfen, Natur, IT, Poker, Psychologie und Philosophie

Timo Hermes, IT-Administrator

Ausbildung und Tätigkeit

- Ausbildung im Bereich System-, Netzwerk- und Datenbankadministration.
- davor Personalbearbeitung bei der Bundeswehr.
- Heute System-, Netzwerk- und Datenbankadministrator.

Betreute Umgebung

- In den neun Niederlassungen sind fünf verschiedene Domänen.
- Mehr als 30 Server und 200 Clients.
- Hauptsystem ist eine gespiegelte Datacore VMware Umgebung mit LWL-Verbindung auf 2 x 10 TByte SAS.

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 04/15 erscheint am 1. April 2015

Schwerpunktthema
Netzwerksicherheit

Das lesen Sie in den nächsten Ausgaben des IT Administrator

In der **Mai-Ausgabe** des IT-Administrator dreht sich alles rund um den Schwerpunkt **Servervirtualisierung & Cloud**. Im Praxisteil werfen wir einen Blick auf die zahlreichen Neuerungen in vSphere 6 und gehen darauf ein, wie Sie 64 Bit-Server mit VirtualBox virtualisieren. Außerdem lesen Sie, was Sie beim Praxiseinsatz von OpenStack beachten sollten. Im **Juni** beschäftigt sich IT-Administrator dann mit dem Thema **Backup & Recovery**.

Im Test: macmon Network Access Control

Workshop: OpenVPN einrichten

Workshop: So sorgen Sie für Layer 2 Security

Workshop: Automatisierung mit Ansible

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

IMPRESSUM

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

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

Oliver Frommel (of), *Leitender Redakteur*
oliver.frommel@it-administrator.de

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

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

Autoren dieser Ausgabe
Petra Adamik, Thomas Bär, Klaus Bierschenk, Werner Fischer, Florian Frommherz, Frank Große, Jürgen Heyer, Christian Hilbert, Wolfgang Hommel, Thomas Joos, Sandro Lucifora, Stefan Metzger, Dr. Holger Reibold, Thomas Rose, Thorsten Scherf, Georg Schönberger, Tim Schürmann, Christian Schulenburg, Markus Stubbig, Felix von Eye, Sebastian Winkler

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

Es gilt die Anzeigenpreisliste Nr. 12 vom 01.11.2014

LAC/2011

Produktion / Anzeigendisposition
Lightrays: Andreas Skrzypnik, Gero Wortmann
dispo@it-administrator.de
Tel.: 089/4445408-88
Fax: 089/4445408-99
Titelbild: Tomasz Wyszolmirski – 123RF

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

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

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

Vertriebsbetreuung
DPV GmbH
www.dpv.de
lange.guido@dpv.de

Erscheinungsweise
monatlich

Bezugspreise
Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-
Jahresabonnement Inland mit Jahres-CD: € 144,84
Studentenabonnement Inland mit Jahres-CD: € 77,34
Jahresabonnement Ausland mit Jahres-CD: € 159,84
Studentenabonnement Ausland mit Jahres-CD: € 84,84
All-Inclusive Jahresabo (incl. E-Paper Monatsausgaben, 2 Sonderheften und Jahres-CD) Inland: € 184,64
All-Inclusive Studentenabo Inland: € 117,14
All-Inclusive Jahresabo Ausland: € 199,64
All-Inclusive Studentenabo Ausland: € 124,64
E-Paper-Einzelheftpreis: € 8,99
E-Paper-Jahresabonnement: € 99,-
E-Paper-Studentenabonnement: € 49,50
Jahresabonnement-Kombi mit E-Paper: € 168,-

(Studentenabonnements nur gegen Vorlage einer gültigen Immatrikulationsbescheinigung)

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

Verlag / Herausgeber
Heinemann Verlag GmbH
Leopoldstraße 87
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des Amtsgerichts München unter HRB 151585.

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

ISSN
1614-2888

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

Bankverbindung für Abonnenten
Kontoinhaber: Vertriebsunion Meynen
Postbank Dortmund
IBAN: DE96440100460174966462
BIC: PBNKDEFFXXX

So erreichen Sie die Redaktion
Redaktion IT-Administrator
Heinemann Verlag GmbH
Leopoldstr. 87
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. 87
80802 München
Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

INSERENTENVERZEICHNIS

Die Ausgabe enthält eine Teilbeilage der Firma Hackattack und eine Gesamtbeilage der Firma Minerva.

Bestellen Sie jetzt das IT-Administrator Sonderheft 1/2015

NEU ab 31.3.

- 180 Seiten Praxis-Know-how zu nützlichen Software-Helfern.
- Zahllose freie Tools aus der Community, von namhaften Herstellern und Open Source-Projekten.
- Zur Optimierung der Systemsicherheit, dem reibungslosen Systemmanagement, der Virtualisierung und vielem mehr.

zum Abonnenten-Vorzugspreis von*

nur € 24,90!

** IT-Administrator Abonnenten erhalten das Sonderheft I/2015 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.*

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

Mehr Infos und Bestellung unter http://shop.heinemann-verlag.de/

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

CeBIT

Besuchen Sie uns in Halle 6
im *Open Source Park*
16.-20. März '15
Hannover

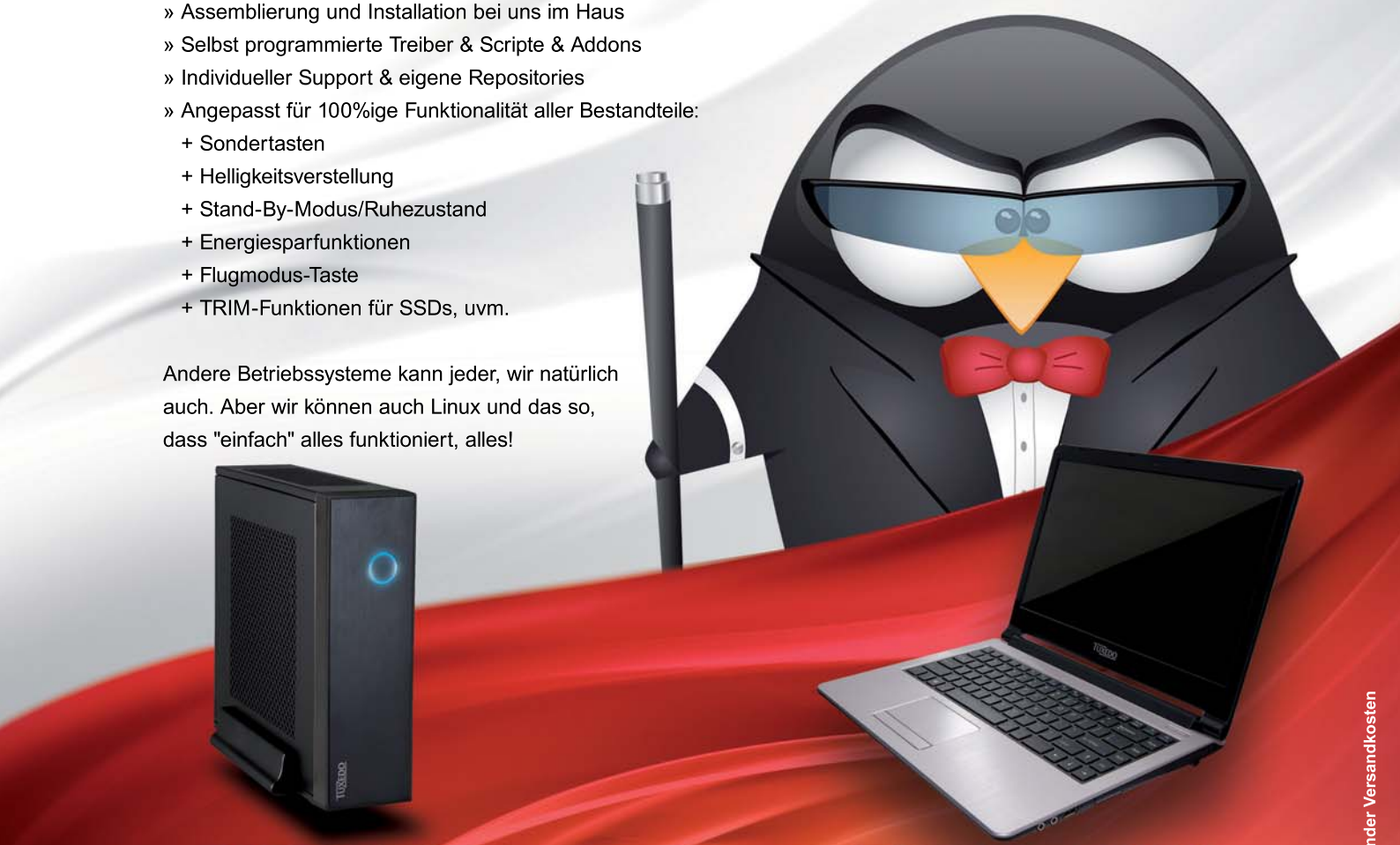
TUXEDO COMPUTERS

Hardware im Maßanzug

TUXEDO Computers sind individuell gebaute Computer und Notebooks die vollständig Linux tauglich sind, Windows natürlich auch, eben Hardware im Maßanzug :)

» Assemblierung und Installation bei uns im Haus
» Selbst programmierte Treiber & Scripte & Addons
» Individueller Support & eigene Repositories
» Angepasst für 100%ige Funktionalität aller Bestandteile:
+ Sondertasten
+ Helligkeitsverstellung
+ Stand-By-Modus/Ruhezustand
+ Energiesparfunktionen
+ Flugmodus-Taste
+ TRIM-Funktionen für SSDs, uvm.

Andere Betriebssysteme kann jeder, wir natürlich auch. Aber wir können auch Linux und das so, dass "einfach" alles funktioniert, alles!



TUXEDO Micro

+ klein*modular*effizient
+ Energiespar-CPUs
+ bis Intel Core i7
+ VESA-Halterung
+ bis zu 3 HDD oder SSD
+ DVD oder Blu-Ray Brenner

ab 349 €*

TUXEDO Book UX1403

+ Slim-Book, **14"** matt HD+
+ bis 14 Std. Akkulaufzeit
+ Intel Core i5 Energiespar-CPU
+ bis zu 3 HDD oder SSD
+ bis zu 16 GB RAM
+ DVD oder Blu-Ray Brenner

ab 699 €*

* Alle Preise inkl. MwSt. zzgl. evtl. anfalender Versandkosten

Mehr Infos unter **www.Linux-Onlineshop.de** und **www.TUXEDOComputers.com**