

Administrator

Das Magazin für professionelle System- und Netzwerkadministration

NEU
am Kiosk

Hochverfügbarkeit

Im Test

**Marathon
everRun MX 6.0**

14

Im Test

**Double-Take
Availability 5.3**

33

Workshop

**Microsoft Hyper-V
Failovercluster einrichten**

38

Systeme

**Hochverfügbare
Xen-Umgebungen mit Remus**

42

Systeme

**Hochleistungscluster mit
Windows HPC Server 2008 R2**

59

STRATO PRO

Wähle Dein System!



Linux
Server



Windows
Server



Managed
Server



Dedicated Server Quad-Core

- AMD Opteron™ 1381 Prozessor
- 4 x 2,5 GHz CPU-Leistung
- 4 GB RAM
- 2 x 500 GB Festplatte (RAID 1)

3 Monate nur

29€
Mon.*

danach ab 59 €/Mon.

Dedicated Server Hexa-Core

- AMD Opteron™ 4180 Prozessor
- Bis zu 2 x 6 x 2,6 GHz CPU-Leistung
- 16 GB RAM
- 2 x 1.000 GB Festplatte (RAID 1)

3 Monate nur

99€
Mon.*

danach ab 129 €/Mon.

*** * * Keine Einrichtungsgebühr! * * * Aktion bis 31.07.2011 * * ***

Telefon: 0 18 05 - 007 677

(0,14 €/Min. aus dem dt. Festnetz, Mobilfunk max. 0,42 €/Min.)

strato-pro.de

* Mindestvertragslaufzeit 12 Monate (alternative Vertragslaufzeiten unter www.strato-pro.de). Preise inkl. MwSt.

 **STRATO** PRO

Was wirklich zählt

Liebe Leser,

nach dem wichtigsten Aspekt von Hochverfügbarkeit befragt, werden zehn Experten wohnmöglich zehn unterschiedliche Antworten geben: Der Geschäftsführer wird anmerken, dass eine Stunde Downtime der Warenwirtschaft eine ganze Stange Geld kostet, der Techniker verlangt nach einer fünften Netzwerkkarte für das Managementnetz und der Hersteller definiert Hochverfügbarkeit genau so, dass nur sein Produkt passt.



Die heute in vielen kleinen und mittleren Unternehmen mit virtualisierten Maschinen praktizierte Form der Hochverfügbarkeit, die beim Ausfall eines wichtigen Servers ein bis zwei Stunden zum Wiederanlauf benötigt, ist sicher ein gangbarer Weg. Einfach die zuletzt gesicherte virtuelle Festplatte als Ersatz für die ausgefallene Maschine einlesen und schon läuft der Laden wieder. Und auch wenn diese Art der Verfügbarkeit etwas hemdsärmelig daher kommt, handelt es sich dabei doch um einen geplanten Prozess und alle Beteiligten akzeptieren die mögliche Downtime. Für einen Experten oder Anbieter von Hochverfügbarkeit oder gar Fehlertoleranz mag dieses Vorgehen nicht sehr professionell wirken und einige würden zweifellos anmerken, dass das alles nichts mit Hochverfügbarkeit zu tun habe.

Und doch hat unser Beispielunternehmen in seiner Low-Budget-Verfügbarkeit den vielleicht wichtigsten Faktor berücksichtigt: Planung. Offensichtlich sind der IT-Verantwortliche und die Geschäftsführung zu der gemeinsamen Ansicht gelangt, dass bis zu zwei Stunden Ausfall auch für wichtige Server akzeptabel sind. Haben die Verantwortlichen bei der Erlangung dieser Erkenntnis alle Risiken und Konsequenzen korrekt einbezogen, dann passt die gewählte Methode zu den Anforderungen an die Verfügbarkeit. Naserümpfen hin oder her.

Auch wenn die Ihnen jetzt vorliegende Ausgabe des IT-Administrator mit dem Schwerpunkt Hochverfügbarkeit einmal mehr beweist, dass Hochverfügbarkeitsprodukte längst das Hochpreissegment verlassen haben – wie etwa unsere Tests von Marathon everRun MX ab Seite 14 oder avance von Stratus ab Seite 20 belegen –, bleibt eine sehr gute Planung doch unverzichtbar. Dies gilt bei der Auswahl und der Vorbereitung des Einsatzes solcher Produkte, aber natürlich auch für die restliche IT-Infrastruktur. So zeigen wir Ihnen ab Seite 38 den Aufbau eines Failover-Clusters für MS Hyper-V und ab Seite 56, wie die DHCP-Infrastruktur hochverfügbar gestaltet wird.

Viel Vergnügen beim Lesen, Ihr

John Pardey
Chefredakteur

Hochverfügbarkeit



Im Test: Acronis Disk Director 11 Advanced Server

Allen aktuellen Entwicklungen des Cloud Computings zum Trotz speichern Benutzer das Gros ihrer Daten immer noch auf Servern im lokalen Netzwerk. Administratoren sind dementsprechend häufig mit Themen wie dem Partitions-Layout oder dem Zusammenführen von Festplatten beschäftigt. Zwar wurden die Bordmittel von Microsoft Windows Server 2008 in Bezug auf die Datenträgerverwaltung deutlich aufgewertet, alle Anforderungen erfüllen sie jedoch immer noch nicht. Die entstehende Lücke zwischen den Wünschen des Administrators und den Fähigkeiten von Microsoft Windows will der Disk Director 11 Advanced Server von Acronis füllen.

Seite 28

Java Enterprise-Anwendungen mit JBoss bereitstellen



Das Entwickeln von Unternehmensanwendungen wird heutzutage immer umfangreicher und komplexer. Steht ein Entwickler vor der Aufgabe, eine Unternehmensanwendung zu entwickeln, so stehen ihm hierfür im Wesentlichen zwei Software-Architekturen zur Verfügung. Auf der einen Seite existiert die von Microsoft entwickelte .NET-Plattform, auf der anderen Seite die herstellerunabhängige Java Plattform, Enterprise Edition – aktuell auch als Java EE bekannt. Dieser Workshop gibt einen Einstieg in Java EE auf Basis des JBoss-Applikationsservers.

Seite 49

AKTUELL

06 News

10 ITANet aktuell: IT ADMIN Tech Talk 2011, 19. bis 22. September 2011, Frankfurt/Main

Der IT-ADMIN Tech Talk geht 2011 in seine zweite Auflage und bietet mit einem vielversprechenden Programm einen hervorragenden Anlass, um für zwei bis vier Tage nach Frankfurt zu reisen.

PRODUKTE

14 Im Test: Marathon everRun MX 6.0

Marathon everRun MX gehört in die Rubrik der fehlertoleranten Lösungen, um absolut unternehmenskritische Applikationen praktisch unterbrechungsfrei betreiben zu können.

20 Im Test: Stratus Avance R2.0.2

99,99 Prozent Verfügbarkeit, also einen Ausfall von weniger als einer Stunde pro Jahr, verspricht Stratus mit seiner Hochverfügbarkeitssoftware Avance.

28 Im Test: Acronis Disk Director 11 Advanced Server

Acronis Disk Director 11 Advanced Server (ADD) ist eine Software mit Funktionen für die Partitionierung und das Festplattenmanagement, um einen möglichst effizienten Betrieb der Server sicherzustellen.

33 Im Test: Double-Take Availability 5.3

Availability von Double-Take bietet eine Quasi-Hochverfügbarkeit mit Disaster Recovery in kurzer Zeit – wenn auch nicht ganz in Echtzeit.

PRAXIS

38 Workshop: Microsoft Hyper-V Failovercluster einrichten

Die neue Live Migration in Windows Server 2008 R2 erlaubt das Verschieben von virtuellen Maschinen ohne Ausfallzeit auf einen anderen Cluster-Knoten. Wie Sie ein solches Cluster einrichten, zeigt Ihnen dieser Workshop.

42 Systeme: Hochverfügbare Xen-Umgebungen mit Remus

Wir stellen die kostenlose HA-Erweiterung Remus für Xen vor und zeigen, welche Hochverfügbarkeitsfeatures das Werkzeug mit sich bringt und wie Sie Remus in Betrieb nehmen.

49 Workshop: Java-Anwendungen mit JBoss bereitstellen

Java EE stellt quasi einen De-facto-Standard bei der Entwicklung von Enterprise-Anwendungen dar. Dieser Workshop gibt einen Einstieg in Java EE auf Basis des JBoss Applikationsservers.

56 Workshop: Ausfallsicherheit der DHCP-Infrastruktur unter Windows Server 2008 R2

Dieser Workshop zeigt vier Maßnahmen zur Erhöhung der DHCP-Verfügbarkeit auf und wirft einen detaillierten Blick auf die Konfiguration von DHCP-Split-Scope unter Windows Server 2008 R2.

59 Systeme: Hochleistungscluster mit Windows HPC Server 2008 R2

HPC Server 2008 R2 ist der direkte Nachfolger von HPC Server 2008 mit erweiterten Funktionen. Welche Neuerungen das Release 2 mitbringt, erfahren Sie in diesem Beitrag.

62 Systeme: Zuverlässigkeit von Reputationsdiensten unter der Lupe

Dieser Artikel zeigt unterschiedliche Technologien von Reputationsdiensten auf. Gleichzeitig haben wir untersucht, wie zuverlässig schädliche URLs identifiziert werden, die der Angreifer verschleiert.

65 Workshop: Exchange Server 2010

Auch mit Exchange Server 2010 haben Sie die Möglichkeiten des Versands nur durch bestimmte Benutzer, allerdings ergänzt durch eine neue Möglichkeit der Moderation.

66 Tipps, Tricks & Tools

WISSEN

70 Reportage: Stratus Avance bei Röchling Automotive in Wolfsburg

Mit Stratus Avance hat Röchling Automotive eine hochverfügbare Virtualisierungslösung mit zwei synchronen Servern implementiert, die nur geringen Administrationsaufwand erfordert.

74 Know-how: Hochverfügbarkeit in komplexen Storage-Architekturen

Hochverfügbarkeit und die schnelle Wiederherstellung geschäftskritischer Daten nach einer Störung sind keine Option mehr, sondern eine Notwendigkeit – auch im Storage-Umfeld.

76 Know-how: Berechnung der Kosten von IT-Ausfällen

Für eine vernünftige Investitionsentscheidung gilt es, den richtigen Mittelweg zwischen Ausfallrisiko und Kosten der Backup-Infrastruktur zu finden. Wie Sie diesen berechnen können, lesen Sie in diesem Beitrag.

79 Buchbesprechung "Linux Hochverfügbarkeit" und "Microsoft SQL Server Integration Services"

80 Website & Fackartikel online

RUBRIKEN

03 Editorial

05 Inhalt

81 Das letzte Wort

82 Vorschau, Impressum, Inserentenverzeichnis



EXPERTeTeach

Ausfallsichere DHCP-Infrastruktur unter Windows Server 2008 R2



In den wenigsten Fällen machen sich Systemverantwortliche über eine ausreichende DHCP-Redundanz Gedanken. Dabei hat ein Ausfall eines DHCP-Servers für ein Unternehmen oft erhebliche Auswirkungen. Fällt der einzige DHCP-Server im Netzwerk aus und kommen

Leasetimes von mehr als fünf Tagen zum Einsatz, ist das Problem in den meisten Unternehmen zwar nicht allzu groß. Anders verhält es sich, wenn Technologien wie VPN, Provisioning und viele andere vom DHCP-Server abhängige Dienste genutzt werden. Dieser Workshop zeigt vier Maßnahmen zur Erhöhung der DHCP-Verfügbarkeit auf und wirft einen detaillierten Blick auf die Konfiguration von DHCP-Split-Scope unter Windows Server 2008 R2.

Seite 56



Hochverfügbarkeit in Wolfsburg

Gerade einmal 120 bis 210 Minuten hat Röchling Automotive als Automobilzulieferer in Wolfsburg Zeit, um einen kompletten Satz von Türverkleidungen für die

VW-Modelle Touran, Tiguan und Golf zu produzieren, vom Spritzen des Kunststoffrahmens über das Einbauen von Ausstattungsvarianten wie Fensterheber und Lautsprecher bis zur Abnahme. Diesem engen Zeitrahmen folgend, ist Röchling auf die Verfügbarkeit seiner IT-Infrastruktur und insbesondere der Server essentiell angewiesen. Mit Stratus Avance hat das Unternehmen nun eine hochverfügbare Virtualisierungslösung mit zwei synchronen Servern implementiert, die nur geringen Administrationsaufwand erfordert.

Seite 70

Themenübersicht



Server- und Systemmanagement



Netzwerkmanagement



Clientmanagement



Job/Weiterbildung



Storage



Virtualisierung



Sicherheit



Recht



Messaging

IT & TK Training



Unified Communications Training – Zertifizierung – Consulting



CCNA Voice – Kurse ICND1 + ICND2 + ICOMM

CCNP Voice – Kurse CVOICE + CIPT1 + CIPT2 + TVOICE + CAPPs

Microsoft
GOLD CERTIFIED

Partner

Microsoft Lync Server 2010

Design und Administration

Microsoft-Kenntnisse für Cisco UC

Active Directory, DNS, CA und Exchange

Microsoft Unified Communications Integration

Lync Server 2010, CUCM, CUP und CUCiLync

EXPERTeTeach
Networking

VoIP Fundamentals – SIP, H.323 & Co. im Einsatz

SIP – Das universelle Signalisierungsprotokoll

... und alles mit garantierten Kursterminen!



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

Batterieschonende USV

Eaton bringt eine neue **Line-interaktive USV** für Serverräume und Rechenzentren auf den Markt. Die **Eaton 5PX** integriert viele für IT-Manager praktische Funktionen: Sie misst den Stromverbrauch jedes angeschlossenen Verbrauchers. Zudem vereinfacht die große, intuitiv bedienbare

LCD-Anzeige die Wartung der USV und hebt die Anlage von Mitbewerbsprodukten ab. Die Messergebnisse können dabei direkt auf der drehbaren LCD-Anzeige der USV oder über das Netzwerk mit Eatons Power-Management-Software angezeigt werden. Der **Ausgangsleistungsfaktor von 0,9** soll zudem dafür sorgen, dass die Eaton

5PX mehr Endgeräte schützen kann als andere Anlagen mit dieser Topologie. Das Nachfolgemodell der Eaton Evolution S ist im Leistungsbereich von 1,5kVA bis 3kVA verfügbar. Bei der 5PX kommt die Eaton ABM (Advanced Battery Management)-Technologie zum Einsatz – eine Neuerung zum Vorgängerprodukt Evolution S –, was die Ausfallsicherheit erhöhen soll. Das ABM lädt die Batterien schonend über eine Dreistufen-Ladetechnik auf. Anstatt konstant Ladeerhaltungsspannung anzulegen, gibt es Pausen zwischen den einzelnen Ladezyklen. Dies verlängere die Lebensdauer der Batterie erheblich. Die Eaton 5PX soll zudem einen Wirkungsgrad von bis zu 99 Prozent erzielen. Alle Eaton 5PX-USVs kommen im RT-Format daher, so dass sie sowohl im Rack wie auch als Tower installiert werden können. Der Preis für die USV beträgt 850 Euro. (dr)

Die Eaton 5PX USV soll besonders batterieschonend arbeiten

Eaton: <http://powerquality.eaton.de/>



KVM-Schaltzentrale für Profis

ATEN erweitert seine Produktpalette um drei neue **Steuerungsgeräte für den professionellen Einsatz** in großen, wachsenden Rechenzentren: den **8-Port Dual Rail LCD KVMP-Switch CL5808**, die **16-Port-Variante CL5816** und die **Bedienkonsole CL5800**. Der **CL5808 beziehungsweise CL5816 Slideaway Dual Rail LCD KVMP** (P für Peripherie)-Switch ermöglicht Anwendern via zwei Konsolen (einem Bus) den parallelen Zugriff auf acht beziehungsweise 16 direkt angeschlossene Server. Dank seiner Skalierbarkeit können in einer Daisy Chain-Installation bis zu 31 weitere Geräte kaskadiert und somit bis zu **512 Server über eine Konsole** gesteuert werden. Darüber hinaus können per Broadcast Kommandos gleichzeitig an alle angeschlossenen Server gesendet werden. In einer Daisy Chain-Installation erkennt der Switch dabei automatisch seine eigene Position, an der Gerätefront zeigen LEDs die angeschlossenen Switches. Bei einer Sequenzänderung

der Station werden die Port-Namen im On Screen Display (OSD) automatisch neu konfiguriert. Das Umschalten zwischen den Computern erfolgt via Tasten an der Gerätefront, Hotkey-Kombinationen oder OSD-Menü. Dank **Hot Plug-Fähigkeit** des CL5808 / CL5816 ist es beim Hinzufügen oder Entfernen von Servern nicht erforderlich, den Switch auszuschalten. Bei der Installation des CL5808 / CL5816 ist keine zusätzliche Software nötig. In einer Daisy Chain-Installation können außerdem Firmware-Updates bei allen angeschlossenen KVM-Switches gleichzeitig durchgeführt werden. Der Preis liegt für den CL5808 bei 1.605 Euro, für den CL5816 bei

1.713 Euro und für die Bedienkonsole CL5800 bei 1.025 Euro. (dr)

ATEN: www.aten.com



Mit den ATEN KVMP-Switches lassen sich bis zu 512 Server verwalten

Mobile Kontrolle

Sophos stellt mit **Sophos Mobile Control** eine mobile Sicherheitsplattform zur Verfügung. Mit der Software sollen Unternehmen **Smartphones schützen** können, indem sie die Konfiguration mobiler Endgeräte verwalten und kontrollieren. Die Absicherung erstreckt sich auf **Apple iOS, Google Android** sowie **Windows Mobile**. Mobile Control bietet dabei einen Überblick über die auf dem Gerät installierten Apps und kann sie gegebenenfalls deinstallieren. Zukünftig will Sophos mit Unterstützung seines Analysezenentrums SophosLabs eine App Reputation-Funktion anbieten, die vor schädlichen oder vermutlich riskanten Apps warnt oder ihre Installation gar nicht erst zulässt. Mit einer webbasierten Konsole ermöglicht Mobile Control unter anderem, mobile Endgeräte mit zentralen Sicherheitseinstellungen zu sichern, um unerwünschte Features zu sperren und

Daten bei Verlust oder Diebstahl des Endgeräts zu löschen oder zu sperren. Zudem lassen sich einheitliche Sicherheitsrichtlinien durchsetzen, etwa eine starke Passwort-Policy, die Kontrolle und Installation von Applikationen sowie das Blockieren von Kameras, Browsern und des Aufrufs bestimmter Webseiten. Der Aufwand für die IT-Administration soll sich durch den Einsatz eines Self-Service-Portals reduzieren lassen, in dem Endanwender neue Mobilgeräte selbst registrieren oder verlorene Geräte sperren oder löschen können. Schließlich lässt sich der Zugang zu geschäftlichen E-Mails kontrollieren, indem nur diejenigen Endgeräte Nachrichten empfangen dürfen, die richtig gesichert und registriert sind. Der Preis für Sophos Mobile Control für 100 Geräte liegt bei 65 Euro je Gerät plus Wartung und Upgrade-Gebühr. (dr)

Sophos: www.sophos.de/products/

Flexibler Speicherplatz

Fujitsu führt mit der **ETERNUS DX S2** die nächste Generation seiner ETERNUS DX Disk-Storage-Systeme ein. Das flexible Daten-Management steht dabei im Fokus der neuen Generation. Die neue **ETERNUS SF-Software** bietet somit laut Hersteller ein besseres Monitoring über die gesamte ETERNUS DX Disk-Storage-Familie. Dadurch reduziere sie den Verwaltungsaufwand weiter und erhöhe die Effizienz. Einzelne Geräte könnten mit wenig Aufwand und Kosten durch Geräte aus derselben Produktfamilie ausgetauscht werden, da bei einem Update nur der Storage-Controller ausgetauscht werden müsse. Durch die hohe Konnektivität könnten die Speichersysteme zudem nahtlos in moderne Serverlandschaften eingebunden werden. Von iSCSI über Fibre Channel bis zu Fibre Channel over Ethernet (FCoE) lasse sich so beispielsweise die synchrone und asynchrone Datenreplikation zwischen allen Geräteklassen (von der ETERNUS DX80 bis zur ETERNUS DX 8000) durchführen. Für eine verbesserte Gerä-

teauslastung durch Thin Provisioning soll der Einsatz von Virtualisierungsstandards sorgen. Der Datendurchsatz ist laut Fujitsu im Vergleich zur Vorgängergeneration bis zu 140 Prozent schneller, die I/O-Leistung um 40 Prozent höher. Auf diese Weise gewährleisten die Systeme eine hohe Skalierbarkeit. Für die Sicherheit der Daten Sorge eine frühzeitige Hardware-Fehlererkennung und -Beseitigung. Um den unerlaubten Zugriff auf wichtige Daten zu verhindern, würden die Systeme bis zum Ende ihres Lebenszyklus zudem mit Verschlüsselungstechnologien geschützt. Mit 3,5-Zoll SAS 6 GBit/s-Festplattentechnologie und 2,9 TByte Speicherplatz kostet die ETERNUS DX80 S2 6.990 Euro inklusive zwei Jahre Vor-Ort-Service und Rack-mount Kit. (dr)

Fujitsu: <http://de.fujitsu.com/products/storage/eternus/dx/>



Die Fujitsu ETERNUS Storage-Systeme sollen 40 Prozent mehr I/O-Leistung bringen

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

M86 Security bringt den **M86 Security Reporter (SR) 3.1** auf den Markt. Dabei ist die Lösung nun auch als Virtual Appliance erhältlich. Die neue Version bietet zudem Produktivitäts-Reports und -Diagramme, die komplexe Daten in praxistaugliche Geschäftsinformationen aufbereiten sollen. Version SR 3.1 beinhaltet außerdem neue, individuell gestaltbare Berichte und Diagramme sowie verbesserte, zeitlich festgesetzte Auto-Deliverys und Trendanalysen. Diese sollen Administratoren dabei helfen, Daten gründlich zu analysieren, Ad-hoc-Reports zu erstellen und intelligente Sicherheitsempfehlungen zu geben. SR 3.1 ist ab sofort zu haben und kostet als Appliance für bis zu 750 Nutzer rund 9.600 Euro. (dr)

www.m86security.com

Red Hat hat **Red Hat Enterprise Linux 6.1** freigegeben. Die neue Version bietet laut Red Hat eine höhere Verfügbarkeit, Skalierbarkeit und Leistung, verbunden mit der Unterstützung neuer Hardware. Dazu kommen Patches und Sicherheits-Updates bei gleichzeitiger Kompatibilität mit verfügbaren Applikationen sowie der Zertifizierung durch Hardwarepartner und unabhängige Softwarehersteller (ISVs). Auch wurden die Optionen zur Nutzung moderner Speichertechnologien wie FCoE, Data Center Bridging und iSCSI Offload weiter ausgebaut. Für ein Zwei-Socket-System kostet die Standard-Subscription 799 US-Dollar. (dr)

www.redhat.de

Belkin stellt den nach eigenen Angaben kleinsten **N300 WLAN USB-Adapter** der Welt vor. Der Micro WLAN-USB-Adapter misst bei einem Gewicht von 10 Gramm nur 18 x 36 mm und lässt sich damit etwa als permanent angeschlossener WLAN-Booster für Notebooks und Netbooks verwenden. Die Übertragungsrate soll bis zu 300 MBit/s betragen. Für die schnelle und sichere Anbindung an WLAN-Netze soll WPS (WiFi Protected Setup) sorgen. WPA2 sichert zudem die Funkverbindung vor unbefugten Zugriffen ab. Für 21 Euro ist der Mini-USB-Adapter erhältlich. (dr)

www.belkin.de

Ipswitch stellt **Version 15** der **WhatsUp Gold IT Management-Lösung** vor. Damit verfügt das Tool über eine neue, verbesserte Benutzeroberfläche. Eine topologische Map bietet nun eine integrierte Ansicht von Netzwerk-Performance, Sicherheit und sämtlichen physischen und virtuellen IT-Ressourcen. Administratoren können zudem schnell Security-Übersichten, -Meldungen oder -Ereignisse visualisieren. Darüber hinaus ist das Ipswitch Event Log Management (ELM) jetzt in WhatsUp Gold integriert, so dass Anwender das Netzwerk von einer einzigen Oberfläche aus verwalten und absichern können. Ab 1.244 Euro ist die Lösung für 25 Devices erhältlich. (dr)

www.whatsupgold.com

Datenspeicher für KMUs

Die neuen **TeraStation Duo TS-WVH**, **4-Bay TS-QVH** und **Rack-mount TS-RVH** von **Buffalo Technology** sind ab sofort erhältlich. Die beiden **SoHo-** und **KMU-NAS** adressieren dank Intel Atom D510 Dual-Core-Prozessor und 64 Bit-Architektur sowie zwei GBit-Ethernet-Anschlüssen mit Port Trunking die gestiegenen Ansprüche an Speichersysteme in Unternehmen. Ergänzend sind die Netzwerkspeicher skalierbar und bieten RAID- sowie Backup-Funktionalitäten durch

die Software NovaBACKUP Professional. Daneben bieten die Geräte Datentransferraten von über 75 MByte/s und eine schnelle sowie einfache Integration in bestehende IT-Umgebungen. Für den Anschluss weiterer Massenspeicher oder einer unterbrechungsfreien Stromversorgung sind je zwei USB-2.0- und USB-3.0-Anschlüsse vorhanden. Damit der Zugriff auf die Private Cloud im Unternehmen auch von unterwegs gelingt, bieten beide NAS FTP-Server-Funktionalität und Web-Access. Eine App für Android

und iOS sorgt zudem für mobilen Zugang über Note- und Netbooks sowie Smartphones auf wichtige Daten und Dateien. Die TeraStation Duo TS-WVH ist bestückt mit zwei oder vier Terabyte ab 499 Euro erhältlich, der etwas größere Bruder TeraStation 4-Bay TS-QVH mit 4 oder 8 TByte als Desktop oder 1HE-Racksystem TS-RVH ab 899 Euro. (dr)

Buffalo Technology:
www.buffalotechnology.com



Die neuen TeraStation Duo-Modelle richten sich an den SoHo- und KMU-Bereich

Pilotenkanzel für den Druckeradmin

Netop hat die **Druckverwaltungssoftware Netop PrintLimit Pro** in der **Version 11.2** auf den Markt gebracht. Zu den wichtigsten neuen Funktionen von Netop PrintLimit Pro zählen die **Cockpit-Registerkarte**, mit der Administratoren den Status und die Aktivitäten des Systems in Echtzeit sehen können, sowie eine komplett überarbeitete grafische Benutzeroberfläche. Um Administratoren einen Echtzeitüberblick über Status und die Aktivitäten des Systems zu verschaffen, bietet die Lösung erstmals besagte Cockpit-Registerkarte. Das Cockpit stellt insgesamt sieben wichtige Druckverwaltungs-Indikatoren dar. Hierzu zählen unter anderem die Systemlaufzeit, heute gedruckte Seiten, Umwelteinfluss, Drucker mit aktuellen Fehlermeldungen und aktuelle Druckaufträge. Weitere neue Funktionen betreffen die Steuerung der Druckernut-

zung und die verursachungsgerechte Kostenzuweisung: So lassen sich über einen Filter nun einfach auf allen Druckern Benutzergruppen auswählen, denen zum Beispiel Farbdrucke erlaubt sind. Netop PrintLimit Pro richtet sich an Unternehmen, Behörden sowie Bildungseinrichtungen wie Schulen und Universitäten, die ihre Druckaktivitäten zentral steuern und überwachen wollen. Seit Version 10.5 war es – jedoch nur für Postscript-Drucker – möglich, dynamisch erstellten Text in Form einer Kennzeile (Watermark) zum Rand aller gedruckten Seiten hinzuzufügen. Ab sofort werden auch viele PCL6- und PCL5-Druckertreiber unterstützt. Der Preis für eine Lizenz inklusive kostenfreier Updates und Support für ein Jahr liegt beispielsweise für Unternehmen mit bis zu 1.000 Benutzern bei 1.848 Euro. (dr)

Netop: www.netop.com/de

Datenflusskontrolle

Citrix Systems hat gemeinsam mit Partnerunternehmen **AppFlow** vorgestellt. Dabei handelt es sich um ein Protokoll auf Basis des offenen **IETF-Standards IP Flow Information Export (IPFIX)**, das Informationen über den Datenverkehr im Netzwerk liefert. Damit sind genauere Erkenntnisse über den Zustand und die Auslastung geschäftskritischer Anwendungen möglich – sowohl in öffentlichen als auch in privaten Cloud-Umgebungen. AppFlow setzt hierfür auf vorhandene Netzwerkgeräte auf und soll eine Rundumsicht über den gesamten Datenverkehr und die Transaktionen von Anwendungen bieten. Daten, die bisher in Netzwerkgeräten wie etwa Service- und Application Delivery Controllern, WAN Optimization Controllern oder Firewalls verborgen blieben, würden damit zugänglich. Auch erübrigten sich damit typische Arbeitsschritte wie die Installation von Datenschnittstellen ins Netzwerk, von Software-Agenten auf jedem Server oder die Aufrüstung einzelner Anwendungen für ein spezielles Monitoring. Citrix NetScaler ist nach Herstellerangaben die erste Netzwerklösung für Service Delivery, die auf AppFlow aufsetzt. Dank der NetScaler Architektur laufe AppFlow mit Übertragungsgeschwindigkeiten von bis zu 50 GBit/s und mache damit auch komplexe Applikationsinfrastrukturen übersichtlich. Außerdem soll künftig auch Citrix Branch Repeater AppFlow unterstützen und damit Einblicke in alle Anwendungen und Services bieten, die über ein Wide Area Network (WAN) bereitgestellt werden. Dazu gehören unter anderem auch virtuelle Desktops und Anwendungen. Dadurch würden operative Abläufe transparenter und die Servicequalität besser kontrollierbar. AppFlow wird von der neuen AppFlow Community mit aktiver Beteiligung von Kunden, Anbietern und Branchenexperten unterstützt. (dr)

AppFlow: www.appflow.org

Virtuelle Identitäten

VMware stellt mit dem **Horizon App Manager** die erste Komponente des auf der VMworld 2010 angekündigten Project Horizon vor. Kernstück des Horizon App Manager bildet ein **Identity-as-a-Service Hub**, das die bestehende Identität eines Anwenders in Systemen wie Microsoft Active Directory oder anderen Directory Optionen in die Public Cloud-Applikationen Dritter überträgt. Damit soll das Management von unterschiedlichen Zugriffsinformationen erheblich einfacher werden – was in Anbetracht der wachsenden Anzahl von Cloud-Applikationen in Unternehmen durchaus sinnvoll scheint. Von dieser Vereinfachung profitieren laut VMware dann sowohl IT als auch Anwender, denn die Identitäts-Silos würden in eine einzige Unternehmens-Identität mit sicherem Zugriff auf

Private und Public Clouds zusammengeführt. Der App Manager bietet darüber hinaus eine offene, Anwender-zentrierte Plattform für den Zugang zu Cloud-Anwendungen über eine Vielzahl von Endgeräten in einem einzigen Applikations-Portal. Für 30 US-Dollar pro Anwender und Jahr ist der Horizon App Manager verfügbar. Künftige Versionen von VMware Horizon sollen den Zugriff der Anwender auf viele Applikationsarten, virtuelle Windows Desktops und Datenbestände vermitteln, zugleich aber die notwendige Sicherheit und Kontrolle garantieren. Als Resultat werden laut VMware Anwender über beliebige Geräte einfach und übergangslos auf Arbeitsressourcen in der Public oder Privat Cloud zugreifen können. (dr)

VMware: www.vmware.com/go/horizonappmanager

VPN-Anbindung über 3G

LANCOM Systems erweitert sein Portfolio um zwei neue **VPN-Router für den Außeneinsatz**: Der **LANCOM OAP-3G** ist ein Mobilfunkrouter mit integriertem Multimode HSPA+ Modem, der **LANCOM OAP-321-3G** bietet zusätzlich 802.11n WLAN. Die Geräte verfügen über ein wasserdichtes, sehr **robustes Metallgehäuse** (IP 66-Schutzklasse) und sind für den Einsatz bei -33 bis +70 °C ausgelegt. Mit den Routern können etwa Videokameras via Mobilfunk über das Internet vernetzt werden. Die WLAN-Variante eignet sich beispielsweise zum Aufbau nomadischer Hotspots auf Veranstaltungen. Im HSPA+ Betrieb erzielen die Geräte je nach Mobilfunkvertrag Spitzendatenraten von 21 MBit/s im Downlink und 5,76 MBit/s im Uplink. Für Flexibilität und Ausfallsicherheit ist das integrierte Funkmodem abwärtskompatibel zu UMTS, EDGE und GPRS. LAN-seitig verfügen sowohl der OAP-3G als auch der OAP-321-3G über eine GBit-Ethernet-Schnittstelle. Der OAP-321-3G bietet zusätzlich ein WLAN-Funkmodul gemäß IEEE 802.11n für den Aufbau eines lokalen drahtlosen Netzes im 2,4- oder 5-GHz-Band. Die Stromversorgung erfolgt über ein integriertes Weitbereichsnetzteil mit 10 bis 28 Volt Gleichspannung. Damit können die Geräte beispielsweise auch über Solarpaneele mit Strom versorgt werden. Vor Diebstahl soll eine integrierte GPS-Ortsbestimmung sorgen. IPsec VPN, Firewall und Virtualisierung inklusive bieten die Router serienmäßig fünf IPsec VPN-Kanäle und Hardwarebeschleunigung, die Anzahl der VPN-Kanäle kann auf 25 aufgerüstet werden. Außerdem bieten beide Geräte bis zu sechzehn virtuelle IP-Netze. Die integrierte Firewall bietet zudem Sicherheitsfunktionen wie Stateful Inspection, Intrusion Detection und DoS-Schutz. Beide Geräte sind ab sofort erhältlich. Der LANCOM OAP-3G wird zu einem Preis von 1.299 Euro angeboten, die Kosten für den LANCOM OAP-321-3G liegen bei 1.499 Euro. (dr)

LANCOM Systems:

www.lancom-systems.de/LANCOM-OAP-3G.2499.0.html

Firewall für dicken Durchsatz

SonicWALL bietet die **SonicWALL NSA E8510** an und erweitert damit das Produktportfolio an Next-Generation Firewalls. Die Appliance nutzt die Firmware **SonicWALL SonicOS 5.8**, die Intrusion Prevention und Schutz vor Malware bieten soll, ohne Latenzen zu verursachen. Die SonicWALL Network Security Appliance (NSA) E8510 für 10 GBit-Ethernet ist für Racks mit dem Formfaktor 1U ausgelegt. Die SonicOS-5.8-Funktionen für **Application Intelligence, Control & Visualization (AIC&V)** erlauben dabei laut Hersteller eine granulare Kontrolle über die genutzten Bandbreiten sowie den Datenverkehr der Anwendungen in Echtzeit. Auf Basis einer Datenbank, die aktuell mehr als 3.500 Anwendungssignaturen umfasst und kontinuierlich erweitert wird, können IT-Verantwortliche Richtlinien für die Nutzung von Anwendungen durchsetzen und Bandbreiten sehr einfach und übersichtlich verwalten. IT-Verantwortliche

haben so die Möglichkeit, die Nutzung bestimmter Anwendungen oder Anwendungskategorien wie Social Media Sites für einzelne Benutzer oder auch Benutzergruppen einzuschränken oder zu blockieren. Die Firewall nutzt Caviums OCTEON Multi-Core-Prozessoren und soll dank der 10 GBit Ethernet SFP+ Dual Ports sowie einer leistungsstarken DPI steigenden Anforderungen gerecht werden, ohne Latenzzeiten im Netzwerk zu verursachen. In Kombination mit SonicWALLs Application Intelligence Control & Visualization bietet die Next-Generation Firewall laut Hersteller die notwendige Leistung für Hochgeschwindigkeitsnetze und dank der integrierten Intrusion Prevention, Anti-Malware und der Absicherung des SSL-Verkehrs maximalen Schutz. Der empfohlene Verkaufspreis der Appliance liegt bei rund 45.000 US-Dollar. (dr)

SonicWALL: www.sonicwall.com/de/



Die Firewall NSA E8510 von SonicWALL soll 3.500 Applikationssignaturen beinhalten

IT ADMIN Tech Talk 2011, 19. bis 22. September 2011, Frankfurt/Main

Das volle Programm

von John Pardey

Der IT ADMIN Tech Talk geht 2011 in seine zweite Auflage und ist mit dem mittlerweile fertigen Programm ein hervorragender Anlass, um für zwei bis vier Tage nach Frankfurt zu reisen und sich in Sachen Netzwerk- und Systemverwaltung praxisgerecht fortzubilden. Dabei bietet die Veranstaltung durch die Kooperation mit dem IT-Administrator einerseits interessante Preisvorteile für Abonnenten, andererseits die seltene Gelegenheit, zahlreiche unserer Autoren live zu erleben. Dieser Beitrag führt Sie exklusiv vorab durch das Veranstaltungsprogramm.

Mit zwei spannenden Keynotes eröffnet der IIR IT ADMIN Tech Talk 2011 das Geschehen am 20. September. Peer Heinlein, bekannt durch die gleichnamige Firma aus Berlin, die sich rund um die Administration von Mailservern einen Namen machte, konfrontiert im Eröffnungsvortrag die teilnehmenden IT-Verantwortlichen mit einer ganzen Reihe von Anstößen zum Nachdenken über den Status Quo des IT-Betriebs. Seiner Ansicht nach sind die Entwicklungen in den Serverräumen und Rechenzentren viel stärker von den Vertriebsmannschaften der IT-Hersteller getrieben als von dem, was für die Unternehmen sinnvoll und nützlich wäre. So legt er in seinem Vortrag "Umdenken! 11 Gebote zur IT-Administration" einen Fokus darauf, wie IT-Organisationen Projekte und Betrieb so umsetzen, dass Prioritäten (wieder) richtig gesetzt sind.

Die zweite Keynote widmet sich dann einem nicht minder brisanten Thema, indem Martin Dembrowski, entrada Kommunikations GmbH, – seines Zeichens auch Ethical Hacker – den "Wirtschaftszweig Cybercrime" beleuchtet. IT-Verantwortliche erfahren dabei, welche enormen wirtschaftlichen Interessen Personenkreise antreiben, die illegal Zugang zu Unternehmensdaten erlangen wollen. Gleichzeitig profitieren die Zuhörer, indem Dembrowski aktuelle Malware und Hacks demonstriert und so das Verständnis für sinnvolle Abwehrmaßnahmen erhöht. Anschließend

teilt sich der IT ADMIN Tech Talk in unterschiedliche Themen-Tracks, die wir Ihnen nunmehr vorstellen.

Virtualisierung und Cloud

Virtualisierung ist nach wie vor das zentrale Thema aktueller IT-Infrastrukturen und so dynamisch wie kaum ein zweites. War etwa Desktopvirtualisierung vor kurzem noch reine Zukunftsmusik, so können die Teilnehmer des IIR IT ADMIN Tech Talk von den Erfahrungen des Bankhauses B. Metzler Seel profitieren, das seine breite Einführung virtueller Desktops durch den Projektleiter Dr. Volker Kunert darstellt.

Und auch die Cloud-Dienste werden langsam, aber sicher erwachsen. Zwar sind diese vielfach noch belächelt und schlagen sich besonders in Deutschland mit allerlei Rechtsvorschriften herum, doch stehen mittlerweile auch Angebote bereit, die ein genaueres Hinsehen lohnen. So wendet sich einer der Vorträge "Windows Intune" zu. Dieser Web-basierte Dienst ermöglicht die Inventarisierung, Verwaltung und Sicherung von Arbeitsplatzrechnern. Die Präsentation gibt Aufschluss darüber, ob Intune gerade für kleine und mittlere Unternehmen eine echte Alternative zu einer ausgewachsenen Management-Suite ist.

Und Ulf B. Simon-Weidner, IT-Administrator-Lesern als ausgewiesener Experte für Windows Server und insbesondere das Active Directory bekannt,

macht sich Gedanken über die Frage "Wer bin ich in der Cloud?". Dabei stellt Simon-Weidner den Administrator in den Mittelpunkt seiner Überlegungen zum Cloud Computing und beleuchtet, welche Skills der Admin dabei benötigt, welche Bedeutung das Identity Management hat und auch, wie sich die Cloud im Fall der Fälle wieder verlassen lässt.

Aber auch die Server-Virtualisierung bleibt selbstverständlich nicht stehen und so ist die Vorstellung von VMware's anstehendem Major-Release vSphere 5 durch unseren Autoren Dennis Zimmer ein Highlight des zweiten Veranstaltungstages. Zimmer verbindet die Vorstellung der neuen Features mit Fragen der Lizenzierung und zeigt zudem Wege der Migration auf.

Und auch Microsofts Hyper-V in der Version 2 erfreut sich zunehmender Beliebtheit und macht VMware zunehmend Konkurrenz. So wird Nils Kaczenskis Vortrag zu Best Practices für Hyper-V

IT-Administrator lesen lohnt sich: Als Kooperationspartner des Tech Talk 2011 bietet IT-Administrator seinen Lesern besonders günstige Konditionen für die Teilnahme an der Veranstaltung an. Sichern Sie sich bei einer Anmeldung über unsere Website [1] bis zum 20. Juli neben dem **Leser-Rabatt von 100 Euro** auch noch die **Vergünstigung für Frühbucher!**

Preisvorteil für Abonnenten



sicher auf eine gespannte Zuhörerschaft treffen. Wie sicher auch Kaczyskis zweiter Vortrag, der Security-Fragen rund um die Virtualisierung zum Gegenstand hat.

Microsoft Sharepoint und Exchange

Hinsichtlich der Microsoft Serverprodukte bilden in diesem Jahr zweifellos Sharepoint und Exchange – beide aktuell in der Version 2010 – den thematischen Schwerpunkt. Da beide Microsoft-Produkte noch vergleichsweise neu sind, stehen sowohl für Sharepoint 2010 als auch für Exchange 2010 Migrations-Vorträge auf der Agenda. Aber auch hier wirft die Wolke ihren Schatten: Bei Migrationen stellt sich – und dies wird zukünftig sicher noch mehr in den Fokus der IT-Verantwortlichen rücken – die Frage, ob die Dienste im Haus oder eben in der Cloud betrieben werden sollen und wie eventuelle Mischformen zu gestalten sind. Besonders wichtig ist diese Frage bei Sharepoint, denn Microsoft stellt mit "Office 365" mittlerweile einen Cloud-Dienst bereit, der einen nahezu vollwertigen Ersatz für Sharepoint darstellen kann.

Und ein Evergreen der Mailserver-Administration darf natürlich auch nicht fehlen, besonders, wenn das Thema nach wie vor hochaktuell ist, indem es nach wie vor den wichtigsten Pfad von

Malware ins Unternehmen darstellt: E-Mail-Sicherheit. Hierzu zeigt Frank Carrius, seines Zeichens ausgewiesener Exchange-Fachmann und als Betreiber des MSXFAQ-Blogs sicher vielen Administratoren bekannt, Methoden auf, um die Kommunikation per Mail auf sicherere Füße zu stellen.

Dabei kommt aber auch der zugrundeliegende Windows-Server nicht zu kurz. So widmet sich Ulf B. Simon-Weidner in einem weiteren Vortragslot seinem Leib-und-Magen-Thema, dem Active Directory. Hier warten auf die Teilnehmer sicherlich ebenso interessante wie technisch tiefgehende Einsichten in den Verzeichnisdienst von Microsoft.

Security, Netze und Mobilität

Das komplette Programm der Veranstaltung vorzustellen, würde hier den Rahmen bei weitem sprengen, doch auch zu den Themen Security, Netzwerke und mobile Geräte hält der Tech Talk spannende und aktuelle Themen bereit. Gerade die Verwaltung von Apples iPhone und iPad stellt Administratoren in diesem und sicher auch in den kommenden Jahren vor einige Herausforderungen. Unser Autor Christian Knermann, stellvertretender Leiter IT-Management Fraunhofer-Institut UMSICHT, widmet sich dem Unternehmens Einsatz dieser Geräte und bietet Antworten auf Fragen nach Einrichtung, Rollout und zentraler Konfiguration.

Ungachtet der speziellen Probleme, die Apples mobile Begleiter dem Administrator bescheren, sind Tablets und

Smartphones sicher einer der großen IT-Trends, der auch mehr und mehr die Unternehmens-IT erfasst. Hier bietet IT ADMIN Tech Talk Vorträge zu Strategien rund um "Bring Your Own Device", die Sicherheit mobiler Endgeräte und auch die Virtualisierung mobiler Clients.

Ein 2011 besonders heißes Thema adressiert der Vortrag zur "Migration auf IPv6". Viele Admins haben in den vergangenen Jahren viel Zeit darin investiert, Know-how zu IPv6 aufzubauen – ohne dass sich in den Infrastrukturen etwas änderte. Doch 2011 ist der Startschuss für die Umsetzung der neuen IP-Welt gefallen. Die Präsentation stellt denn auch konkrete Migrationsszenarien, mögliche Stolperfallen und den Dualbetrieb mit IPv4 in den Mittelpunkt.

Neu: Intensiv-Workshops

Zusätzlich zu den zwei mit über 30 Vorträgen gefüllten Tagen des IT ADMIN Tech Talk am 20. und 21. September bietet der Veranstalter vor und nach der Konferenz (am 19. und 22. September) je einen ganztägigen Intensiv-Workshop an. Diese Workshoptage können die Teilnehmer optional buchen.

Dabei dreht sich der Workshop am 19. September um Microsoft Office 365 und dessen Einsatzmöglichkeiten sowie die konkrete Einführung im Unternehmen. Der Workshop am 22. September geht in Sachen IPv6 in die Tiefe. IT-Verantwortliche, die ihr Netzwerk auf IPv6 umstellen wollen und konkrete Antworten für die Umsetzung suchen, sollten diesen Workshop nicht verpassen.

[1] Programm und Anmeldung
IT ADMIN Tech Talk 2011
B7A21

Link-Codes



E-BOOK
SYSTEMS

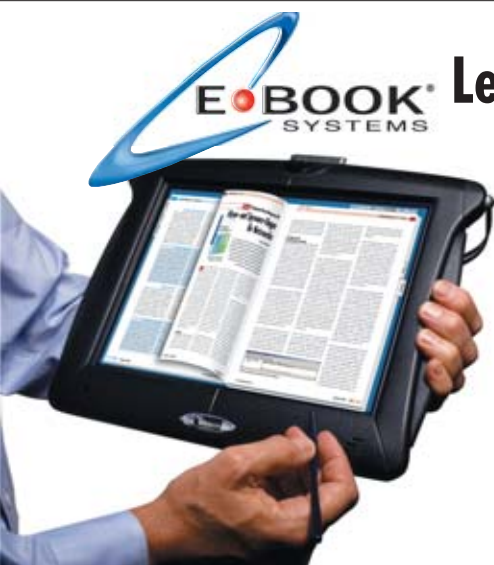
Lesen Sie den IT-Administrator als E-Paper

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

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

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

www.it-administrator.de/magazin/epaper 



1&1 DSL: DAS

Starten Sie jetzt mit 1&1 DSL in das beste WLAN aller Zeiten! Gemeinsam mit den Profis von AVM hat 1&1 den 1&1 HomeServer der nächsten Generation entwickelt. Er ist **DSL-Modem, Router und Telefonanlage in Einem**, als zentrale Schnittstelle für Ihre kabellose Kommunikation in allen Räumen. Und er bietet mehr Power, mehr Sicherheit und mehr Komfort als je zuvor!

HIGHSPEED-WLAN!

Mit bis zu 300 MBit/s und optimaler Frequenzwahl wird kabelloses Surfen zum echten Highspeed-Erlebnis!



BESTE REICHWEITE!

Dank MIMO Mehrantennentechnik findet der 1&1 HomeServer stets die beste Verbindung zu Ihren Geräten. Für optimale Reichweite und besten Datendurchsatz.

ECO-MODE!

Der 1&1 HomeServer funkt nur, wenn er aktiv ist und Daten überträgt. Das heißt für Sie: geringstmöglicher Stromverbrauch.



SICHERHEIT!

Die TÜV-geprüfte Firewall und die spezielle WPA2-Verschlüsselung des 1&1 HomeServers gewährleisten höchste Sicherheit.



WPS! (WI-FI PROTECTED SETUP)

Zur Einrichtung neuer WLAN-Geräte, die ebenfalls WPS unterstützen, drücken Sie einfach den WLAN-Knopf am 1&1 HomeServer – die Eingabe spezieller Zugangscodes ist nicht mehr notwendig!



GAST-ZUGANG!

Das gibt's nur bei 1&1: Bieten Sie Besuchern einen eigenen WLAN-Zugang (z. B. für Netbooks, Smartphones) – natürlich getrennt von Ihrem Heimnetzwerk zum Schutz Ihrer Daten.



100 GB SPEICHER!

Nutzen Sie 100 GB Online-Speicherplatz in einem der 1&1 Hochleistungs-Rechenzentren für Ihre Dateien, Bilder, Musik etc. Mit passwortgeschütztem Zugriff von zu Hause oder von unterwegs übers Internet.



GELD ZURÜCK!

Wir sind sicher, dass Sie von der Leistungsfähigkeit der 1&1 WLAN-Technik begeistert sein werden! Sollte das nicht der Fall sein, rufen Sie uns einfach an und schicken Sie uns den 1&1 HomeServer zurück. Ihr 1&1 DSL-Vertrag endet dann umgehend und wir zahlen Ihnen Ihr Geld zurück. Fairer geht's nicht!



BESTE WLAN!

INTERNET & TELEFON

19,99 €/Monat*

Für volle 24 Monate,
danach 24,99 €/Monat.

**Inklusive 1&1 HomeServer
der nächsten Generation!**

NEU!



Auszeichnungen der
1&1 HomeServer-Familie

1. connect
DSL-TK-Anlagen
des Jahres 2011

www.connect.de

Computer
Bild 03/2011
FRITZ!Box Fon WLAN 7390
„Der derzeit beste
WLAN-Router“

1&1

Jetzt informieren und bestellen: 0 26 02 / 96 90

www.1und1.de



Im Test: Marathon everRun MX 6.0

Den Ausfall überleben

von Jürgen Heyer

Bei den fehlertoleranten Lösungen von Marathon laufen die geschützten Applikationen auch bei einem schlagartigen Totalausfall eines ganzen Servers ohne Unterbrechung weiter. Mit der neuen Version Marathon everRun MX 6.0 soll dies sogar gelingen, wenn die Programme mehrere Prozessoren oder Cores für den Betrieb benötigen. IT-Administrator wollte wissen, wie gut es mit der Zuverlässigkeit und Stabilität tatsächlich bestellt ist. In unserem Test musste everRun MX 6.0 beweisen, wie gut das Produkt mit seinen drei Absicherungsstufen die Verfügbarkeit von Systemen und Applikationen gewährleistet.

Marathon everRun MX gehört in die Rubrik der fehlertoleranten Lösungen, um absolut unternehmenskritische Applikationen praktisch unterbrechungsfrei betreiben zu können. Dazu gehört auch, dass die Programme bei einem plötzlichen Ausfall eines ganzen Servers oder sogar einer ganzen Betriebsstätte weiterlaufen und weder Speicherinhalte noch Transaktionen verloren gehen. Bei der erreichbaren Verfügbarkeit werden gerne die fünf Neunen erwähnt, also eine Verfügbarkeit von 99,999 Prozent. Dies entspricht einer ungeplanten Downtime von etwa fünf Minuten pro Jahr.

Vom Prinzip her gelingt dies, indem zwei eigenständig installierte Server im sogenannten Lockstep-Verfahren absolut synchron arbeiten und die gleichen Operationen durchführen. Fällt eines der beiden Systeme aus, hat das andere immer noch sämtliche Speicherinhalte im RAM und alle Registerinformationen in der CPU, so dass es allein weiterarbeiten kann. Aus Sicht des Anwenders läuft die Applikation somit ohne Unterbrechung durch.

Besonders kompliziert wird die Sache, wenn nicht nur die Inhalte einer CPU oder eines Cores abzugleichen sind, sondern von mehreren, damit auch hohe Performanceanforderungen erfüllt werden können. everRun MX unterstützt nun genau diese Funktionalität mit SMP (Symmetric Multi-Processing).

Um die Serverhardware und die Applikationen, die fehlertolerant laufen sollen, zu trennen, setzt Marathon auf die Virtuali-

sierung mit XenServer. Schon seit einiger Zeit besteht hier eine Allianz mit Citrix und Produktteile wurden zusammen entwickelt. everRun MX nutzt zwei bis vier XenServer und lässt sich somit nach Bedarf skalieren. Pro fehlertoleranter Serverinstanz laufen immer zwei virtuelle Maschinen im oben beschriebenen Lockstep-Verfahren synchron auf zwei XenServern. Eine darunterliegende, ebenfalls synchrone Daten Spiegelung sorgt dafür, dass kein gemeinsamer Plattenspeicher (Shared Storage) benötigt wird, sondern jede VM eigene logische Laufwerke auf dem lokalen Plattensystem des jeweiligen XenServers nutzen kann. Für einen Disaster-resistenten Betrieb ist auch eine sogenannte SplitSite-Konfiguration möglich.

Eine Vorplanung ist unabdingbar

Nachdem everRun MX auf XenServer aufsetzt, muss sich ein Administrator bei der Hardwarebeschaffung an der XenServer Kompatibilitätsmatrix (HCL) [1] orientieren. Weiterhin ist zu beachten, dass pro Server mindestens vier Netzwerkanlüsse benötigt werden. Es lassen sich bis zu vier Server in einem Pool verschalten, zum Vermeiden von Problemen sollte die Hardware absolut identisch sein.

Dann muss sich der Administrator eingehend mit dem Konfigurationshandbuch beschäftigen, um zu entscheiden, welche der möglichen Konfigurationen er seinen Anforderungen entsprechend wählt, denn everRun MX kennt vier prinzipielle Hardwarekonfigurationen und drei Absicherungsstufen.

Die einfachste Konfiguration ist der Two-Host-Pool, bestehend aus zwei Servern. everRun MX nutzt grundsätzlich zwei private Netzwerkverbindungen, so genannte A-Links (Availability Links), für die Kommunikation der beiden Server untereinander. Hierzu werden in diesem Fall je zwei (Gbit)-Netzwerkkarten der Server mit Cross-Kabeln direkt miteinander verbunden. Die Direktverbindung reduziert die Wahrscheinlichkeit eines Ausfalls auf ein Minimum. 10 Gbit werden optional auch unterstützt. Weiterhin werden noch zwei Netze benötigt für das Management und die Verbindung in die Produktion, also zu den Anwendern. Bezüglich des Managementnetzes werden nach Möglichkeit zwei Netzwerkkarten pro Server empfohlen, die mit Bonding/Teaming arbeiten und über getrennte Switches geführt werden. Diese Konfiguration mit der Direktverbindung der A-Links ist die einzige, die SMP, also die Nutzung mehrerer CPUs in der virtuellen Maschine, unterstützt. Zu beachten ist, dass der Fokus auf der Prozessorskalierung liegen muss, die Applika-

Level-2-Absicherung: Jeder Intel VT-fähige Prozessor, bis 32 Cores pro Server

Level-3-Absicherung ohne SMP: Prozessor vom Typ Intel E54xx, L54xx, X54xx, E74xx, L74xx, X74xx, E52xx, L52xx, X52xx

Level-3-Absicherung mit SMP: Prozessor vom Typ E55xx ab 2,26 GHz, E56xx ab 2,4 GHz

Vier 1-Gbit-Netzwerkkarten

72 GByte Direct Attached Storage (DAS)

Systemvoraussetzungen



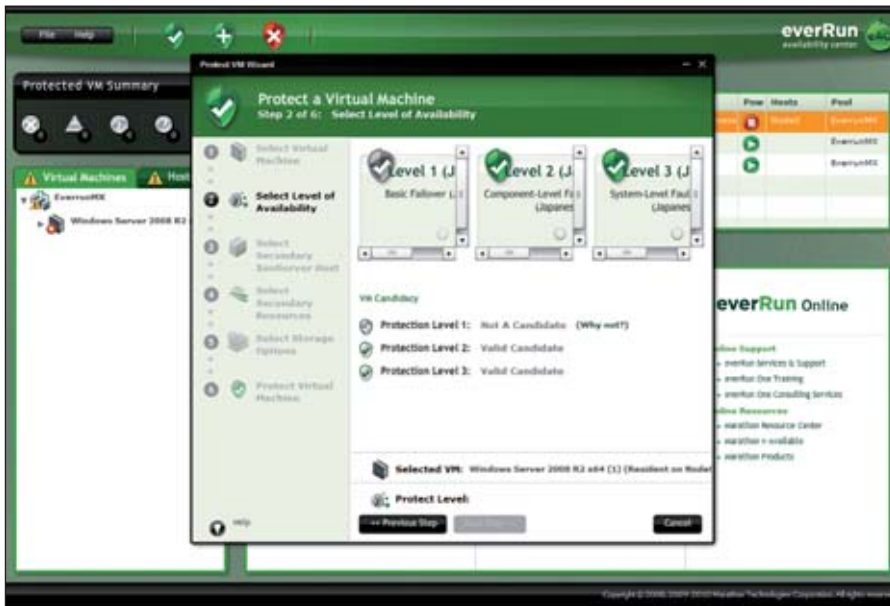


Bild 1: Der Absicherungs-Assistent bietet die drei Absicherungsstufen zur Auswahl an und zeigt auch an, welche Level aufgrund der Konfiguration möglich sind

tion aber keine absolut hohen Anforderungen hinsichtlich geringer Verzögerungen im Netzwerk haben darf.

Beim Multi-Host-Pool werden zwei bis vier Server zusammengeschaltet, wobei dann die A-Links über Switches verbunden sind. Da durch die zusätzlichen Switches und durch die eventuell höhere Anzahl der Server die Wahrscheinlichkeit steigt, dass der Pool bei einem Fehler womöglich auseinanderbricht und an zwei Stellen ohne Kommunikation untereinander läuft (Split Brain-Situation), ist hier zwingend ein Quorum Service einzurichten, ein Dienst auf einem weiteren unabhängigen System. Nur der Teil des Pools, der eine Verbindung zum Quorum besitzt, arbeitet dann weiter.

Die letzte Variante ist der Two-Host Split-Site Pool, also die Aufstellung von zwei Hosts über eine größere Entfernung hinweg. Hier ist darauf zu achten, dass die Verbindungen über redundante Core-Switches geführt werden, ansonsten findet aber das gleiche Konzept wie beim Multi-Host-Pool mit ein oder auch zwei Quorum-Diensten Verwendung. Welche Entfernungen sich überbrücken lassen, hängt von den zulässigen Latenzzeiten aus Sicht der Applikation ab.

Für den Test haben wir die zuerst beschriebene Variante Two-Host-Pool ge-

wählt, wobei uns für die Installation zwei Rackserver Dell Poweredge R610 zur Verfügung standen.

Installation in mehreren Schritten

Sowohl die genannten Konfigurationsmöglichkeiten als auch die eigentliche Installation sind sehr ausführlich beschrieben, so dass wir unsere Testumgebung nach der Verschaltung des Netzwerks zügig einrichten konnten. Alle benötigten Module hatten wir zuvor von der Marathon-Homepage heruntergeladen und auch entsprechende Lizenzen erhalten.

Auf den beiden zum Test zur Verfügung stehenden Servern richteten wir zuerst ein RAID-5-Array ein und installierten XenServer 5.5 Update 2. Im Management-LAN installierten wir auf einem Arbeitsplatz XenCenter und fassten beide Systeme in einem Ressource-Pool zusammen, so dass eines zum Pool Master und das andere zum Member Server bestimmt wurde. Über das XenCenter spielten wir noch das XenServer Update 3 ein. Anschließend legten wir, wie in der Anleitung empfohlen, auf dem Pool Master die erste VM an, einen Windows Server 2008 R2. Dann installierten wir everRun MX, wozu ebenfalls auf dem Pool Master zu beginnen ist. Dies hat auf der Konsole der XenServer zu erfolgen, was aber dank der guten Beschreibung reibungslos klappte.

Bei der anschließenden Installation von everRun MX auf dem Member Server war darauf zu achten, dass der Pool Master lief, damit die Software die übergreifende Verbindung einrichtete. Des Weiteren war noch auf beiden Seiten ein everRun-Hotfix zu installieren und erneut zu booten. Dies erforderte nochmals einige Eingaben auf den Konsolen, war aber ebenfalls gut beschrieben.

Die abschließende Konfiguration erfolgte über die Browser-basierte Konsole, genannt everRun Availability Center (eAC). Diese erreicht der Administrator über die URL des Master Servers und standardmäßig Port 8080. Im eAC sind die erhaltenen Lizenzen einzuspielen, eine IP-Adresse zur Pool-Isolierung anzugeben und die A-Link Netzwerke einzurichten, außerdem gegebenenfalls noch die Adressen für die Quorum-Dienste.

Neben der Konfiguration in der eAC sind auch in der XenCenter-Konsole einige Dinge zu kontrollieren. Wichtig ist hier die Vorgabe, dass nur den für die Verbindung zur Produktion gedachten Netzwerken neue VMs zugewiesen werden. Sonst sind innerhalb der VMs auch die A-Links und womöglich das Management-LAN zu sehen. Abgesehen davon erfolgt die Anlage von VMs im XenCenter unabhängig davon, ob später durch everRun MX eine Absicherung erfolgen soll. Wichtig ist nur, dass auf jeden Fall die paravirtualisierten Treiber (XenServer Tools) installiert werden, sonst ist eine weitere Absicherung durch everRun MX nicht möglich.

Drei Verfügbarkeitsstufen zur Auswahl

everRun MX unterstützt drei Stufen (Level) der Applikationsabsicherung. Die höchste Stufe 3 steht für die oben beschriebene Fehlertoleranz und Hochverfügbarkeit. Ideal ist dieser Modus für den Betrieb unternehmenskritischer Applikationen. Meist sind dies Dienste mit Außenwirkung auf externe Kunden oder Dienste, deren Ausfall auf einen Schlag Großteile der Produktion lahmlegt. Beispiele dafür sind der Betrieb von Anwendungen in Flughäfen oder transaktionskritische Dienste in Banken.

Die Stufe 2 eignet sich für viele geschäftskritische Applikationen wie das Mailsystem oder interne Datenbanken. Datenverluste und Ausfälle sind dort zwar sehr kostenintensiv, führen aber nicht zum massiven Zusammenbruch des Betriebs. Sie behandelt Komponentenausfälle (RAID-Verbunde, Speichereinheiten, Netzwerkverbindungen), die sich durch eine entsprechende Redundanz nicht auf die laufenden Applikationen auswirken. Beim Ausfall einer Platteneinheit wird weiterhin das Spiegelsystem genutzt, bei einer Unterbrechung der Netzwerkverbindung schaltet das System auf eine zweite auf dem anderen Server um. Benutzer und Clients merken letztendlich nichts von dem Ausfall. Auch die Wiederherstellung der Komponenten erfolgt ohne Auswirkungen auf die Produktion. everRun MX sorgt beispielsweise dafür, dass im Hintergrund eine ausgefallene Spiegelung wiederhergestellt wird oder die reparierte Netzwerkverbindung wieder genutzt wird. Erst wenn beispielsweise der hostende XenServer ausfällt oder doch mehrere Netzwerkverbindungen auf ein Mal, gibt es eine kurze Downtime, da die VM dann auf dem anderen Server neu gestartet werden muss.

Das niedrigste Level 1 ist letztendlich kein eigentlicher Bestandteil von everRun MX, kann aber auch über die eAC gesteuert werden. So bedeutet die Stufe 1 die Einbindung und Nutzung von XenServer High Availability (HA). Sofern die XenServer mit HA-Option lizenziert sind, kann sie für VMs verwendet werden, deren Betrieb nicht absolut kritisch ist und wo ein manueller Eingriff akzeptiert werden kann. Diese Stufe lässt sich durch die eAC einer VM zuweisen, es greift aber keinerlei Automatik.

Betreuung über zwei Konsolen

In der Praxis erfolgt die Betreuung einer everRun MX-Umgebung über zwei Konsolen, der eAC und dem XenCenter. In der eAC sind alle VMs zu sehen, die über das XenCenter angelegt wurden und es stehen die drei beschriebenen Absicherungsstufen zur Auswahl, Stufe 1 ist aber nur anwählbar, wenn XenServer HA aktiviert wurde. Hat der Administrator für eine VM eine zusätzliche Absicherung beauftragt, so erfolgt deren Umkonfiguration, indem unter anderem alle Netzwerkkarten durch einen Marathon Redirector ersetzt werden. In der XenCen-

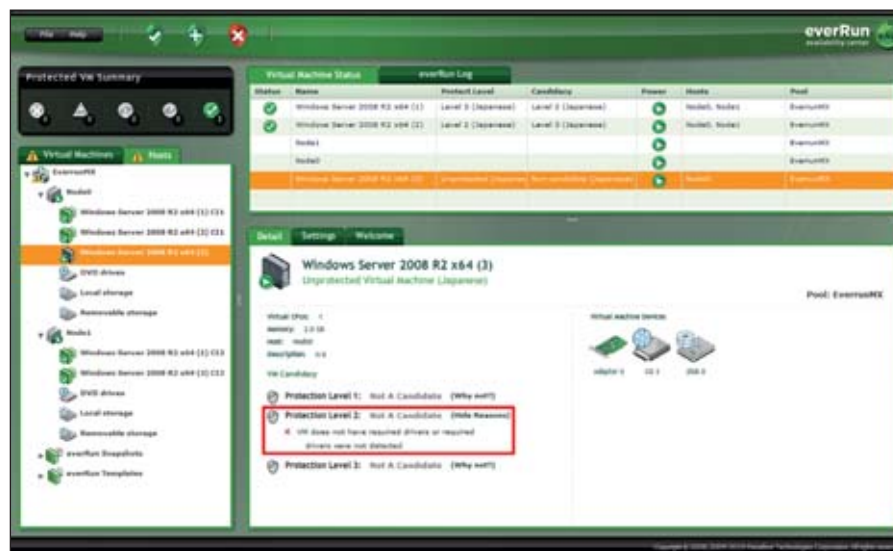


Bild 2: Sofern bei einer VM keine paravirtualisierten Treiber installiert sind, ist eine Absicherung mit everRun MX nicht möglich

ter-Ansicht haben diese VMs keine Netzwerkkarten. Erfahrung ist hier insofern erforderlich, damit ein Administrator nicht versucht, nachträglich wieder Netzwerkkarten zuzuweisen, was nicht verweigert wird. Weiterer Bestandteil der Umkonfiguration ist bei Stufe 2 und 3 die Einrichtung einer Datenspiegelung für die der VM zugewiesenen Volumes zwischen den lokalen Plattenpools der XenServer.

So abgesicherte VMs kann der Administrator via eAC im laufenden Betrieb migrieren und auch auf einzelnen Knoten deaktivieren. Ebenso lassen sich ganze Knoten beispielsweise für eine Wartung evakuieren. Dann werden VMs verschoben beziehungsweise bei einer Absicherung mit Stufe 3 die Instanzen auf dem entsprechenden Server beendet.

Zu beachten ist, dass über das XenCenter keine Aktionen an VMs durchgeführt werden dürfen, die mit einer Absicherung durch everRun MX arbeiten, diese haben ausschließlich über die eAC zu erfolgen. In der Beschreibung der VM ist auch ein entsprechender Hinweis zu finden, dass letztendlich nur der Konsolenzugriff genutzt werden darf. Eine Absicherung durch everRun MX ist daran zu erkennen, dass die VM-Bezeichnung durch ein Anhängsel wie CI1 oder CI2 ergänzt wurde, um die mehrfachen Compute Instanzen (CI) kenntlich zu machen und zu unterscheiden. Zu beachten ist auch, dass die Ansicht der Instanzen zwischen

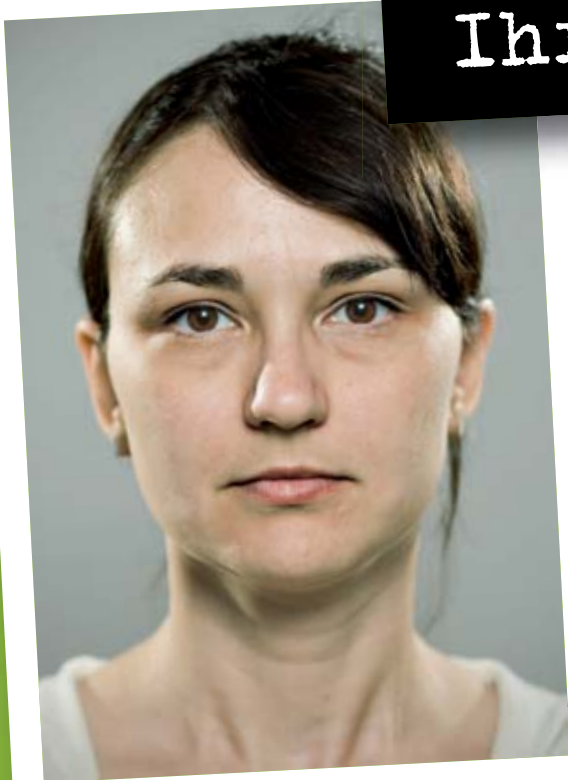
XenCenter und eAC abweichen kann. So sind im XenCenter bei mit Stufe 3 abgesicherten VMs alle Instanzen zu sehen, die synchron laufen, bei einer mit Stufe 2 abgesicherten VM ist aber nur die Instanz zu sehen, die tatsächlich aktiv ist. In der eAC dagegen sind auch die Standby-Instanzen aufgeführt.

Etwas verwundert waren wir, dass die eAC keine eigenen Mechanismen für eine Alarmierung des Administrators beispielsweise per SMTP enthält. Auch findet keine Überwachung der Hardware Sensoren statt, um beispielsweise per Stufe 2 gesicherte VMs bei einem Problem, welches nicht direkt die genutzten Ressourcen einschränkt (wie Ausfall eines redundanten Netzteils, Ausfall einer Platte im RAID-Verbund, drohende Überhitzung durch einen defekten Lüfter), präventiv auf einen "gesünderen" Server zu verschieben. everRun MX versucht nur, eine für den Betrieb relevante Komponente durch Nutzung der gleichen auf einem anderen Knoten zu ersetzen. Hier sehen wir noch eine Möglichkeit zur Optimierung.

Auf Nachfrage bei Marathon hinsichtlich der fehlenden Überwachung erfuhren wir, dass der Hersteller aktuell intensiv an der Unterstützung von XenServer 5.6 arbeitet, mit dem dann in Verbindung mit entsprechenden Agenten der renommierten Hardwarehersteller eine SNMP-Überwachung kommen soll. Möglich ist bereits eine Überwachung der VMs, hier stützt

Bekommt fürs Putzen
400,- Euro von Ihnen.

Plus 250,- von
Ihrer Konkurrenz.



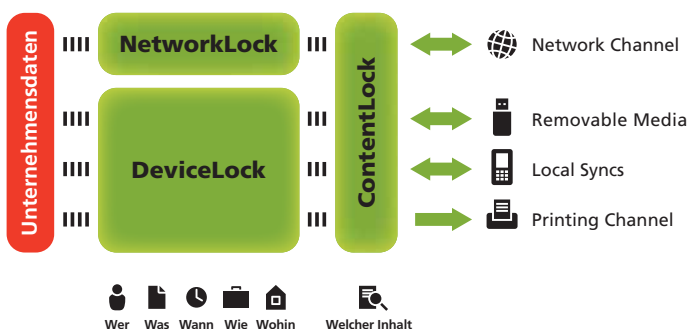
Mitarbeiter sind auch nur Menschen.

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

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

■ Neu! Jetzt mit vollständiger Content- und Kontext-Prüfung

Die Datenflusskontrolle der DeviceLock Endpoint DLP-Suite



Informieren Sie sich jetzt!

www.devicelock.de oder wählen Sie
die Nummer sicher: +49.2102.89211-0

[www.devicelock.de]

DeviceLock®
Proactive Endpoint Security

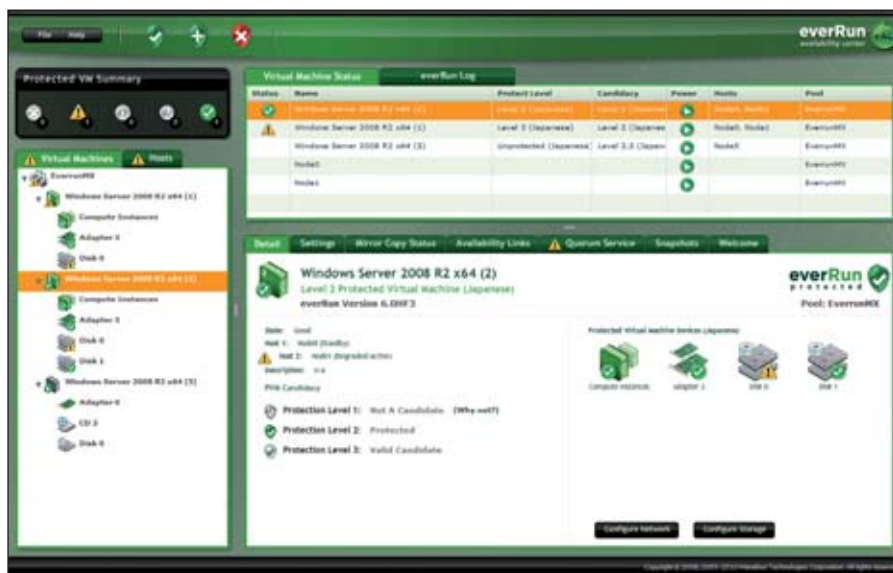


Bild 3: Manchmal dauert es einige Minuten, bis die Statusanzeige in der eAC den tatsächlichen Status anzeigt: Die fehlerhafte Plattenspiegelung wird hier nur bei einem Laufwerk angezeigt, der Gesamtstatus ist immer noch grün.

sich everRun MX auf SNMP. Auf jeder VM ist SNMP zu installieren, dabei wird auch ein SNMP-Agent für everRun MX eingerichtet. Dann lässt sich eine SNMP-basierte Überwachung mit einem geeigneten Monitoring-Tool realisieren.

Zu beachten ist, dass die Erstellung von Snapshots für abgesicherte VMs in die eAC verlagert ist. Beim Versuch, einen Snapshot über das XenCenter zu erstellen, reagiert die Konsole einfach nicht auf das Drücken der "Take Snapshot"-Schaltfläche. Es erscheint aber auch kein entsprechender Hinweis. everRun MX erstellt Snapshots wahlweise nur von einem Host oder von beiden. Vorhandene Snapshots werden in der eAC in einer Übersicht aufgelistet.

Im Zweifel die höchste Absicherung wählen

Um die Funktionsweise und Stabilität von everRun MX eingehender zu untersuchen, richteten wir drei VMs mit Windows Server 2008 R2 ein. Eine VM ließen wir ohne Absicherung, eine mit Stufe 2 und eine mit Stufe 3 laufen. Dann simulierten wir verschiedene Ausfälle, indem wir einzelne Netzwerkanschlüsse zogen oder auch an einem Server mehrere Festplatten aus dem genutzten RAID-5-Verbund, so dass kein Zugriff mehr möglich war. Während die VM ohne Absicherung von jedem Ausfall sofort betroffen war, liefen die beiden gesicherten VMs ohne Unterbrechung weiter. Die mit Stufe 3 gesicherte VM überlebte

auch einen abrupten Serverausfall durch Abschalten des Systems ohne Unterbrechung der Zugriffe. Die mit Stufe 2 gesicherte VM wurde auf dem verbleibenden Server automatisch neu gestartet. So weit arbeitete die Umgebung erwartungsgemäß.

Allerdings fielen uns einige Eigenheiten auf, die dem Administrator Erfahrung mit der Umgebung und überlegtes Handeln abverlangen. So muss er beachten, dass bei einem Ausfall des Pool Masters sowohl das XenCenter als auch die eAC mit der IP-Adresse des neuen Masters gestartet werden müssen. Die Umschaltung auf den neuen Master kann aber etwas dauern, so dass hier ruhiges Abwarten angesagt ist. Gut ließ sich beob-

achten, dass eine mit Stufe 2 abgesicherte VM in keinem Fall automatisch migriert wird, hier ist immer der manuelle Eingriff des Administrators erforderlich.

Allerdings konnten wir bei den Ausfalltests eine Situation erzeugen, in der das manuelle Migrieren nicht klappte: Als wir für ein Szenario die mit Stufe 2 gesicherte VM auf dem Master Server laufen ließen und dann sukzessive alle Festplatten zogen, ging der Zugriff auf die eAC verloren. Sie konnte über keine der beiden IP-Adressen mehr erreicht werden, die beiden abgesicherten VMs liefen aber noch. Aufgrund der fehlenden Administrierbarkeit war nun auch keine Migration mehr möglich. Schließlich mussten wir beide Server nacheinander booten, um die Umgebung wieder in einen Administrations-fähigen Zustand zu bringen. Während die mit Stufe 3 abgesicherte VM dabei in Betrieb gehalten werden konnte, indem sie immer den verbleibenden Knoten nutzte, mussten wir bei der mit Stufe 2 abgesicherten VM eine Downtime in Kauf nehmen. Zumindest konnten wir die VM per RDP kontrolliert herunterfahren und letztendlich auch den Zeitpunkt der Aktion selbst bestimmen.

Marathon konnte die Situation bei sich nachstellen und bezeichnete sie als sehr speziellen Doppelfehler. Der fehlende Plattenzugriff betraf die VM direkt und wirkte sich auch auf die Funktionsweise von Xen aus, dem in unserer Konfiguration die Betriebssystempartition fehlte.

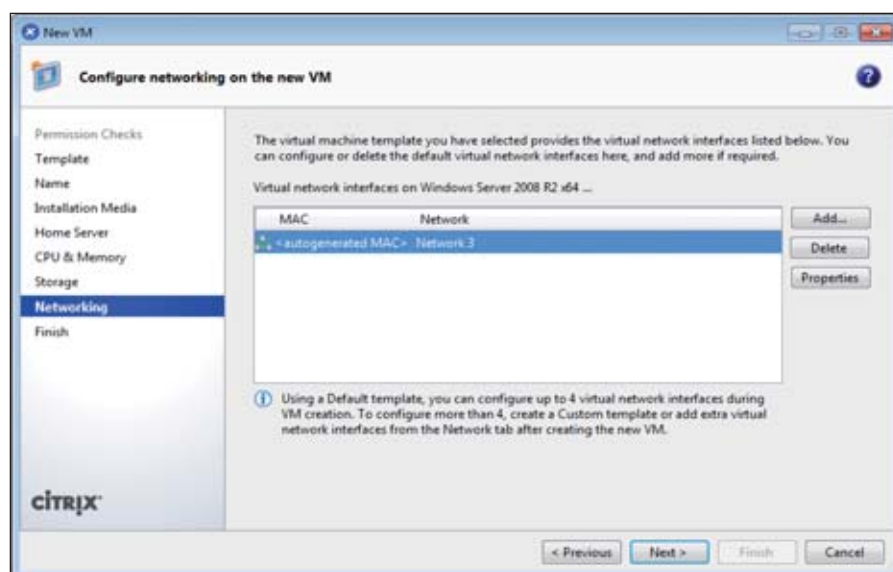


Bild 4: Aufgrund der vielen benötigten Netzwerkkarten ist es notwendig, innerhalb von XenCenter die automatische Zuweisung bei der VM-Erstellung anzupassen



So konnte Xen selbst nicht mehr problemlos arbeiten, was sich dann auf die Funktion der eAC auswirkte. Letztendlich empfahl der Spezialist bei Marathon, VMs, bei denen auch eine kurze Downtime nicht akzeptabel ist, auf jeden Fall mit Stufe 3 abzusichern.

Produkt

Hochverfügbarkeitssoftware für zertifizierte Standardhardware zum Aufbau einer fehlertoleranten Serverumgebung mit 99,999 Prozent Verfügbarkeit.

Hersteller

Marathon
www.marathontechnologies.com

Preis

everRun MX gibt es als Standard- und Enterprise-Version. Diese sind technisch identisch, entscheidend ist, welche Applikationen abzusichern sind. everRun MX Standard für Microsoft-Applikationen für zwei Server kostet 9.090 Euro, die Enterprise-Version ist bei der Absicherung von Dritthersteller-Applikationen notwendig und kostet 13.600 Euro.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Einrichtung der VMs	8
Verfügbarkeit	9
Failoververhalten	7
Wiederherstellung eines Basiservers	5
Hardwareunterstützung	8

Dieses Produkt eignet sich

optimal für mittlere und größere Umgebungen, wo überaus unternehmenskritische Applikationen unter fachkundiger Administration absolut fehlertolerant betrieben werden müssen.

bedingt für den Einsatz in kleineren Umgebungen oder Außenstellen, wo eine fachkundige Administration vor Ort nicht gegeben ist. Die Betreuung von everRun MX erfordert einige Erfahrung.

nicht in Situationen, wo eine CPU-lastige Applikation mit SMP fehlertolerant betrieben werden soll, aber gleichzeitig eine SplitSite-Konfiguration erforderlich ist. Beide Anforderungen sind nicht gleichzeitig zu erfüllen.

Marathon everRun MX 6.0

In der Tat haben wir die Erfahrung gemacht, dass die mit Stufe 3 abgesicherte VM bei keinem unserer Tests durch einen Ausfall betroffen war oder wir diese für eine Reparaturaktion herunterfahren mussten. Marathon plant Verbesserungen, damit das System in solch speziellen Situationen kontrollierter reagiert. Abgesehen davon ist zu berücksichtigen, dass für den von uns simulierten Verlust eines RAID-5-Plattenarrays erst einmal mindestens zwei Festplatten ausfallen müssen, ohne dass ein Administrator bereits im Vorfeld reagiert.

Bezüglich der Performance stellten wir positiv fest, dass sich die Absicherung der Stufe 3 trotz des genutzten Lockstep-Verfahrens nicht merklich negativ auf die Rechenleistung auswirkte. Wir konnten keine nennenswerten Unterschiede feststellen. Anders sah es mit der Plattenperformance aufgrund der aktiven Spiegelung aus. Schreib- und Leseoperationen dauerten rund viermal solange, die gemessenen Zugriffszeiten verdoppelten sich. Sollten also Applikationen mit vielen Plattenzugriffen genutzt werden, so ist vorher eingehend zu prüfen, ob die Leistung ausreicht.

Hinsichtlich eines kompletten Ausfalls eines XenServers inklusive seiner Daten ist in everRun MX nichts implementiert, was eine Wiederherstellung beschleunigt. Vielmehr ist dann eine komplette Installation des Servers identisch zur oben beschriebenen Neueinrichtung erforderlich. Die notwendigen Datenträger samt Anleitung sollten also jederzeit griffbereit sein, um die Redundanz möglichst schnell wiederherstellen zu können.

Fazit

Der klare Fokus von Marathon everRun MX ist der fehlertolerante Betrieb von Applikationen, indem in der höchsten Absicherungsstufe zwei virtuelle Maschinen die gleichen Operationen im Lockstep-Verfahren synchron berechnen. Auch bei einem schlagartigen Ausfall eines kompletten physikalischen Servers läuft die Applikation unbeeinträchtigt weiter. Neu ist die SMP-Unterstützung, so dass auch sehr CPU-lastige Applikationen betrieben werden können. everRun MX setzt auf XenServer als Virtualisierungsplattform auf und es können bis zu vier Server zu

einem Pool zusammengefasst werden. Neu ist die Kombinationsmöglichkeit verschiedener Absicherungsstufen in einem Pool, so dass sich die verwendete Hardware optimal nutzen lässt und jeder VM genau die passende Absicherung zuordnen lässt.

Bei den Ausfalltests haben sich fehlertolerant laufende VMs (Stufe 3) als sehr stabil erwiesen. Die von uns simulierten Ausfälle und die eventuell erforderlichen Reparaturmaßnahmen haben deren Verfügbarkeit in keinem Fall beeinträchtigt. In diesem Modus ist eindeutig die Stärke von everRun MX zu sehen.

Bei der mittleren Absicherungsstufe 2, die nur Ausfälle einzelner Komponenten überbrücken soll, sehen wir dagegen einen Ansatz zur Optimierung. Statt bei einem Ausfall einer Komponente nur genau die fehlende Funktion durch eine Ressource eines anderen Servers im Pool zu ersetzen, wäre es unserer Meinung nach besser, die betroffenen virtuellen Maschinen gleich auf den anderen Server zu migrieren. So konnten wir im Test gezielt Situationen forcieren, wo die abgesicherten VMs zwar noch liefen, eine manuelle Migration aber nicht mehr möglich war. Hier hätte eine präventive, automatische Migration die eine oder andere Downtime eventuell vermeiden können.

Nicht ganz trivial ist das Management, da ein Administrator zwei Konsolen (everRun Availability Center/eAC und XenCenter) bedienen muss, um alle administrativen Aufgaben zu erledigen. Dabei muss er genau wissen, welche Tätigkeiten wo zu erledigen sind. Interessierten Administratoren empfehlen wir die Nutzung der 30-tägigen Trialversion für eigene Tests, um den erzielbaren Mehrwert abzuschätzen. Zu empfehlen sind in diesem Zusammenhang auch Performance-Tests. Bei der CPU-Leistung konnten wir keine merkliche Reduzierung feststellen, jedoch bei den Plattenzugriffen aufgrund der integrierten Datenspiegelung. (jp)

IT

[1] Citrix XenServer Kompatibilitätsmatrix
B7T11

Link-Codes





Im Test: *Stratus Avance R2.0.2*

Doppelpack mit vier Neunen

von Jürgen Heyer

99,99 Prozent Verfügbarkeit, also einen Ausfall von weniger als einer Stunde pro Jahr, verspricht Stratus mit seiner Hochverfügbarkeitssoftware Avance. Weiterhin wirbt der Hersteller mit einfachster Bedienbarkeit, geringem Administrationsaufwand und attraktiven Preisen, was die Lösung gerade für kleinere Unternehmen interessant machen soll. IT-Administrator wollte genauer wissen, wie Stratus alle diese attraktiven Eigenschaften in ein Produkt gepackt hat.

Stratus ist seit 30 Jahren im Sektor hochverfügbarer Serversysteme tätig und verfügt daher über umfassende Erfahrungen auf diesem Gebiet. Am meisten bekannt dürften die fehlertoleranten Stratus ftServer mit einer Verfügbarkeit von über 99,999 Prozent sein, bei denen die Applikationen auch bei Ausfall eines kompletten Servers unterbrechungsfrei weiterlaufen. Dies wird erreicht, indem ein virtueller Server im Lockstep-Verfahren gleichzeitig auf zwei identischen physikalischen Servern läuft und alle Operationen parallel berechnet werden. Der Einsatz dieser Technik rechtfertigt sich angesichts der hohen Investition allerdings erst, wenn es sich um den Betrieb absolut unternehmensbeziehungsweise betriebskritischer Applikationen handelt.

In den meisten Fällen ist diese extrem hohe Verfügbarkeit und der damit verbundene Aufwand nicht erforderlich, der Betrieb nur auf einem herkömmlichen Server wäre aber auch zu riskant, da ein Hardwaredefekt womöglich einen mehrstündigen Ausfall nach sich ziehen könnte. Die Verfügbarkeit eines einzelnen Standardservers liegt üblicherweise bei etwa 99 Prozent. Gefragt ist letztendlich oft ein preislich attraktiver Kompromiss, bei dem ein Defekt keine oder zumindest nur eine kurze Downtime der Applikationen nach

sich zieht. Genau diese Anforderung will Stratus mit Avance abdecken.

Stratus Avance ist als kostengünstige Software-Lösung konzipiert, die eine hohe Verfügbarkeit in kleineren Unternehmen, Abteilungen und Niederlassungen sicherstellen soll. Dazu macht die Software aus zwei identischen Standard-x86-Servern ein hochverfügbares System, wobei die Virtualisierungssoftware Xen als technische Basis dient. Avance übernimmt die permanente Überwachung der Rechner sowie die Synchronisation der Daten (Spiegelung) zwischen den beiden Servern, so dass kein teurer Shared Storage benötigt wird. Zu jedem Zeitpunkt ist einer der beiden Server das Primärsystem, wobei die Rolle im laufenden Betrieb verschoben werden kann.

Die produktiv genutzten Applikationen laufen auf einem oder mehreren virtuellen Servern, die wiederum das Primärsystem als physikalische Basis nutzen. Durch eine integrierte Prognose lassen sich auftretende Hardware- und Softwareprobleme frühzeitig erkennen und die Avance-Software sorgt vorausschauend dafür, dass im Zweifelsfall stets das "gesündere" System als primäres agiert. Sie verschiebt dazu bei Bedarf automatisch die Primärrolle und somit die virtuellen Maschinen im laufenden Betrieb ohne Unterbrechung.

Dadurch gewinnt ein Administrator Zeit für eine eventuell notwendige Reparatur der "kranken" Hälfte, während die Applikationen auf der "gesunden" Hälfte weiterlaufen. Eine Überwachung aus der Ferne ist zudem einfach realisierbar, so dass Fachpersonal nicht ständig vor Ort sein muss.

Installation nur auf zertifizierter Hardware

Entscheidend für einen stabilen Betrieb von Avance ist der Einsatz zertifizierter Hardware, es reichen aber letztendlich aktuelle Standardserver der renommierten Hersteller Dell, HP, Intel, Seneca, Tarox oder Wortmann, was sowohl die Anschaffung als auch die Wartung vergleichsweise preiswert macht. Stratus pflegt zu diesem Zweck eine Kompatibilitätsübersicht [1], in der die zertifizierten Komponenten genau aufgeführt sind. Prinzipiell setzt die aktuelle Avance-Version 2.0.2 eine Nehalem-Architektur voraus. Getestet haben wir auf zwei Rackservern Dell Poweredge R610, die uns von Stratus zur Verfügung gestellt wurden.

In der Regel werden die Server von den Distributoren vorinstalliert ausgeliefert oder einer der über 180 Systempartner übernimmt diese Tätigkeit. Nichtsdestotrotz gibt es bei Stratus sehr detaillierte Installationsanweisungen für die verschiedenen Servertypen. Dabei erweist sich die Installation von der CD als überaus einfach und es werden nur die IP-Parameter abgefragt, unter denen später die WebGUI erreichbar ist. Umfangreicher und absolut genau zu befolgen sind die Vorgaben, bis

Zwei identische, zertifizierte Server von Dell, HP, Intel, Seneca, Tarox oder Wortmann (das Angebot an zertifizierten Systemen soll noch erweitert werden); für das Management Microsoft Internet Explorer ab Version 8, Mozilla Firefox 3.6 oder höher.

Unterstützte Gastbetriebssysteme: Windows 2000 Server SP4, XP SP3, Windows Server 2003 (R2), 32/64 Bit, Windows Server 2008 (R2), 32/64 Bit, RHEL 4.6, 4.7, 5.1 bis 5.5 WS, AS, ES, CentOS Linux 4.6, 4.7, 5.1 bis 5.5.

Systemvoraussetzungen



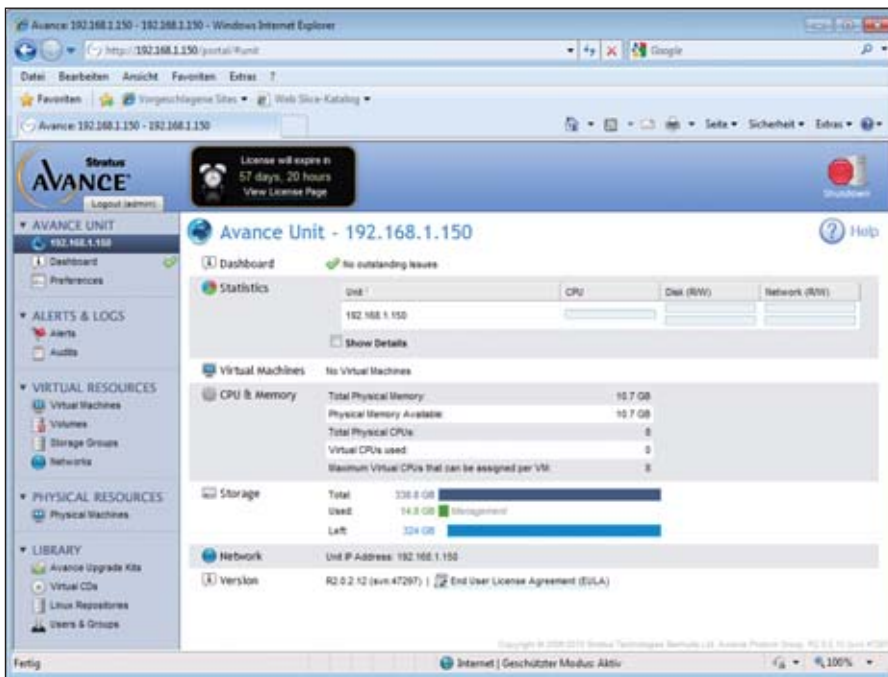


Bild 1: Die Hauptansicht liefert Informationen zum Status und zur Auslastung des Systems auf einen Blick

die Installation überhaupt starten kann. Dies betrifft die Raid-Konfiguration der Platten, die Bios-Einstellungen, die Netzwerkverschaltung und die genaue Bootreihenfolge. So müssen die Server zuerst per PXE von der ersten Netzwerkkarte booten und anschließend von der ersten logischen Platte. Bei den Netzwerkkarten dient die erste als privater Link zwischen den beiden Servern, die zweite zur Verbindung in das Firmennetzwerk. Werden gegebenenfalls weitere Netzwerkkarten benötigt, sind diese erst im Anschluss an die Installation zu ergänzen. Die Verschaltung der Netzwerkkarten in Verbindung mit der Bootreihenfolge ermöglicht es, dass bei einem Ausfall eines Servers und dessen Reparatur oder auch Tausch sich dieser die Konfiguration vom noch laufenden per PXE-Boot holen kann. Sofern ein Administrator die Installation selbst übernimmt, muss er nur ein System einrichten, das zweite installiert sich dann mittels PXE-Boot und Imaging vom ersten Server komplett eigenständig. Auch die Datenspiegelung zwischen den Systemen wird vollautomatisch eingerichtet.

Als Resultat der Installation läuft auf beiden Systemen, die standardmäßig mit Node0 und Node1 benannt sind, Xen als Virtualisierungsplattform. Die weitere Bedienung erfolgt über eine Weboberfläche und es ist nicht notwendig, sich später

nochmals an den Konsolen der beiden Server anzumelden. Auch die Xen-eigene Konsole XenCenter wird für den Betrieb nicht benötigt.

Ein sogenanntes SplitSite Deployment für eine Disaster-resistente Anordnung, also eine Aufteilung der beiden Systeme auf zwei weiter voneinander entfernten Standorten ist durchaus möglich. Zu beachten ist nur, dass die Latenzzeit auf der privaten Netzwerkverbindung zwischen den beiden Systemen zehn Millisekunden nicht überschreiten darf.

Eine Konsole für zwei Systeme

Aus Sicht der Konsole präsentieren sich beide Server als ein System mit nur einer IP-Adresse. Nur in der Rubrik "Physikalische Ressourcen" lassen sich beide Systeme getrennt auswählen, um Hardware-details auszulesen oder die ermittelten Sensordaten einzusehen. Ansonsten wird das Serverpaar aus dem Blickwinkel des Administrators wie eine Maschine betrachtet. Die Konsole beinhaltet die komplette Bedienung inklusive der Installation der virtuellen Maschinen. Sie hat sich im Test als übersichtlich und sehr intuitiv bedienbar erwiesen.

Die Funktionen der Konsole gliedern sich in die fünf Rubriken "Avance Unit", "Alarmer" und "Logs", "Virtuelle Ressourcen", "Physikalische Ressourcen" sowie "Bibliothek". Sie sind über ein Menü am linken Konsolenrand auswählbar. Innerhalb der Rubrik Avance Unit ist die Dashboard-Seite sicher die wichtigste Ansicht, da sie einen schnellen Blick auf den Gesundheitszustand des Gesamtsystems ermöglicht. Ein Symbol wie ein grüner Haken oder ein rotes Kreuz zeigt bereits im Menü an, ob ein Problem vorliegt oder nicht. Als Blockgrafik sind die beiden Knoten mit den Netzwerkverbindungen, die Avance-Einheit und die aufgesetzten VMs dargestellt. Etwaige Fehler werden innerhalb dieser Grafik symbolisch dargestellt, außerdem sind darunter die relevanten Meldungen aufge-



Bild 2: Das Dashboard der Avance-Konsole zeigt in einer Blockgrafik, wo sich eine ausgefallene Komponente befindet und listet Warnungen und Alarmer ihrer Schwere nach auf

listet. Rechts neben der Grafik befindet sich weiterhin ein Fenster mit entsprechenden Hilfehinweisen.

Einen umfassenden Blick auf den aktuellen Ressourcenverbrauch wie CPU-, Arbeitsspeicher- und Plattenspeichernutzung sowie eine Liste der laufenden VMs liefert eine weitere Seite in dieser Rubrik. Hier lassen sich auch CPU-Last, Platten- sowie die Netzwerkauslastung als Verlaufsgrafik aufblättern. Verfügbar sind die Daten hier bis zu einem Jahr. Ansichten lassen sich allerdings nur vom aktuellen Zeitpunkt zurück in die Vergangenheit auswählen (letzte Stunde, letzte vier oder 24 Stunden, letzte Woche, Monat oder Jahr), der Administrator kann aber nicht einen bestimmten Zeitraum in der Vergangenheit herausgreifen.

Der dritte Punkt der Rubrik Avance Unit ermöglicht diverse Einstellungen wie die Vorgabe eines Zeitervers, die Einbindung einer USV, die Einrichtung von Benachrichtigungen per SMTP und SNMP sowie die Aktivierung eines Remote Supports durch Stratus beziehungsweise einen Partner. So kann Avance auf Wunsch selbst einen Hilferuf absetzen (Call Home) und es besteht die Möglichkeit zur Aktivierung einer Einwahl (Dial-In). Die Nutzung von Proxies ist dabei berücksichtigt und lässt sich konfigurieren. Die Nutzung der Call Home- und Dial-In-Funktion ist optional. Je nach Vereinbarung werden die Aktionen durch Stratus selbst oder einen der zertifizierten Systempartner durchgeführt. In der Rubrik Alarme und Logs findet der Administrator eine Liste mit allen Alarmmeldungen sowie eine Auflistung aller Konsolenzugriffe mit Angabe des verwendeten Benutzers sowie der genutzten IP-Adresse.

Unter der Rubrik Virtuelle Ressourcen kann der Administrator die eingerichteten virtuellen Maschinen und deren Status, die verwalteten Volumes, Storage-Gruppen sowie die Netzwerke einsehen.

In der Rubrik Physikalische Ressourcen sind umfassende Hardware-Informationen über die beiden eingesetzten Server zu finden. Beeindruckend ist die Anzahl von rund 150 überwachten Sensoren (unter



Bild 3: Bei einem Fehler kann der sekundäre Server problemlos in Wartung genommen und repariert werden, während die VMs auf dem primären weiterlaufen

anderem Temperaturen, Lüfterdrehzahlen, Spannungen der Netzteile, ECC-Status des Arbeitsspeichers, Raid-Batterie-Status, Link-Status der Netzwerkkarten), die allesamt ausgewertet werden, um den Betriebszustand zu ermitteln. Im Fehlerfall ist vor den einzelnen Komponenten ein entsprechendes gelbes oder rotes Warnsymbol zu finden.

Die Rubrik Bibliothek beinhaltet Objekte wie Upgrade Kits, Virtuelle CDs, Linux Repositories sowie eine Benutzer- und Gruppenverwaltung, um die Administratoren des Avance-Systems festzulegen. Wahlweise kann hier mit lokalen Benutzern und Gruppen oder mit entsprechenden aus dem Active Directory gearbeitet werden.

Um VMs zu installieren, ist es zuerst notwendig, die benötigten ISO-Dateien zu importieren. Dies kann auf zwei Arten erfolgen. Entweder legt der Administrator die Installations-CD/DVD am primären Node ein, damit sie eingelesen und als ISO-Datei gespeichert wird. Alternativ können fertige ISO-Dateien per http heruntergeladen werden, sie müssen also auf einem Webserver zum Download bereitgestellt werden. Einen anderen Import-Weg gibt es nicht, was die Bereitstellung von Installationsquellen unserer Meinung nach etwas umständlich gestaltet. Allerdings muss man berücksichtigen, dass sich die Anzahl der benötigten ISO-Dateien in Grenzen halten dürfte, da diese nur zur Installation erforderlich sind. Für die Installation von Linux-VMs lassen sich zudem Repositories für RPM-Pakete sowie Kickstart-Dateien einrichten beziehungsweise registrieren.

Unter Upgrade Kit können Avance Upgrades, eine neue Firmware, bei HP-Servern die HP Tools sowie neue paravirtualisierte Windows-Treiber und Linux-Kernel-Patches eingespielt werden. Das integrierte Hilfesystem der Konsole ist erfreulicherweise in mehreren Sprachen verfügbar, auf Wunsch kann es auf Deutsch umgestellt werden. Dann werden auch sämtliche Fehlermeldungen in Deutsch ausgegeben, während die GUI an sich weiterhin in Englisch ist.

Der Installationsprozess einer VM unter Avance unterscheidet sich nicht von der üblichen Vorgehensweise in einer virtuellen Infrastruktur. Der Administrator muss nichts Avance-spezifisches berücksichtigen, was den Ablauf sehr vereinfacht. Ein Assistent fragt die Eckdaten der VM ab, um diese als Objekt anzulegen, damit der Administrator dann darin die Gastinstallation durchführen kann. Es ist nicht möglich, optional nur einige VMs hochverfügbar zu betreiben und andere nicht, die dann auf beide Knoten verteilt würden. Vielmehr laufen grundsätzlich immer alle VMs hochverfügbar auf dem primären Knoten, die Ressourcen des sekundären Knoten dienen nur dem Failover für alle VMs.

Intelligentes Failover

Bei einer reinen Virtualisierungslösung werden die virtuellen Maschinen in der Regel nicht präventiv zwischen den physikalischen Servern verschoben, außer aus Lastgründen. Erst wenn ein Server tatsächlich ausfällt, werden die VMs in einer Farm auf einem anderen System neu gestartet. Außerdem setzen derartige virtuelle Infrastrukturen Plattenspeicher

1&1 DUAL HOSTING

DER NEUE STANDARD IM HOSTING

Kein anderer Webhoster
überzeugt durch so viel
Kompetenz, Know-how
und Qualität wie 1&1.

- ✓ **Maximal sicher:**
Paralleles Hosting Ihrer
Website in zwei Hightech-
Rechenzentren an ver-
schiedenen Orten!
- ✓ **Superschnell:**
210 GBit/s Anbindung!
- ✓ **Umweltschonend:**
Grüner Strom!
- ✓ **Zukunftssicher:**
1.000 eigene Entwickler!

1. connect
Webhosting-Anbieter
des Jahres 2011

Ausgabe 08/11

SOMMER-SPECIAL: 1&1 DUAL PERFECT 1 JAHR 0,- €!*

- 6 Domains inklusive
- 5 GB Webspace
- UNLIMITED Traffic
- 20 FTP-Accounts
- 1&1 Webanalytics

- 10 MySQL Datenbanken (je 1 GB)
- UNLIMITED Click & Build Apps
(Auswahl aus 65 Applikationen, z. B.
Joomla!, WordPress, eCommerce, CMS)
- PHP5, PHP Dev, Zend Framework,
Ruby, SSI, git Versionsmanagement

- **NEU: Geo-Redundanz!** Maximale
Verfügbarkeit durch paralleles
Hosting in zwei Hightech-
Rechenzentren
- u. v. m.

Weitere reduzierte 1&1 Dual Hosting-Pakete und weitere Sparangebote unter www.1und1.info



0 26 02 / 96 91



0800 / 100 668



www.1und1.info

* 1&1 Dual Perfect 1 Jahr für 0,- €/Monat, danach 9,99 €/Monat. Einmalige Einrichtungsg Gebühr 9,60 €. 24 Monate Mindestvertragslaufzeit. Preise inkl. MwSt.



Der Test zweier ähnlicher Produkte zum Betrieb hochverfügbarer Applikationen hat gezeigt, dass es durchaus funktionale und konzeptionelle Unterschiede gibt, die letztendlich entscheiden, welche Lösung in welcher Situation besser geeignet ist. Nachfolgend stellen wir die beiden Produkte hinsichtlich wichtiger Aspekte gegenüber.

Hardwareauswahl

In beiden Fällen ist eine zertifizierte Hardware Voraussetzung für den produktiven Betrieb. Dabei decken sich die Hardwareanforderungen weitgehend, so dass im Prinzip für beide Produkte die gleiche Hardware benötigt wird. Hinsichtlich der Bedarfsorientierung erscheint uns everRun MX etwas flexibler, da hier virtuelle Maschinen unterschiedlicher Absicherungslevel parallel betrieben werden können. Durch eine Reduzierung der Absicherung können mehr VMs parallel betrieben werden. Außerdem lassen sich zwei bis vier Server zu einem Pool verschalten, was die Flexibilität nochmals steigert. Bei Avance sind grundsätzlich Serverpaare zu bilden, ein Server ist primär, auf ihm laufen alle VMs, der andere dient als Backup. Alle VMs arbeiten mit der gleichen Absicherung. Deutlich höher sind allerdings bei everRun MX die Anforderungen an das Netzwerk, denn in jedem Server werden mindestens vier Netzwerkkarten benötigt, empfohlen werden sogar fünf, bei Avance reichen zwei. Entsprechend höher ist auch der Verschaltungsaufwand. Bei everRun MX wird bei bestimmten Konstellationen noch ein zusätzlicher Quorum-Dienst benötigt, der im Netzwerk auf einem unabhängigen System einzurichten ist. Eine SplitSite-Konfiguration zur Verteilung der Server über größere Entfernungen ist in beiden Fällen möglich.

Installation und Betrieb

Stratus liefert eine DVD mit allen Inhalten. Dadurch gibt es nur einen Installationsvorgang, bei dem alles eingerichtet wird. Die Installation muss auch nur auf einem Server erfolgen, der zweite installiert sich selbst vom ersten per PXE-Boot, Imaging und Spiegelung. Muss einmal ein Server neu eingerichtet werden, wegen Defekt oder Tausch, geschieht dies ebenso fast ohne Benutzer-eingaben. Die Möglichkeit zur schnellen Wiederherstellung ist fester Bestandteil des Betriebskonzepts. Bezüglich der Updates liefert Stratus komplette Pakete für den Server. Bei everRun MX erfolgt die Installation in zwei Schritten. Zuerst ist auf jedem Server Xen einzurichten und ein Pool zu bilden, anschließend ist everRun MX zu ergänzen. Alle Installationsschritte sind auf beiden Servern erforderlich. Dies bedeutet einigen manuellen Aufwand. Muss hier ein System neu eingerichtet werden, ist für dieses wieder eine komplette Installation erforderlich. Das ist deutlich zeitaufwändiger als bei Stratus. Hinsichtlich Updates gibt Marathon Patches und Hotfixes für Xen explizit frei, für Aktualisierungen von EverRun MX liefert der Hersteller eigene Pakete.

Management

Bei Avance erfolgt das gesamte Management über nur eine Konsole. Das Serverpaar ist immer über dieselbe IP-Adresse erreichbar, egal welcher Knoten der primäre ist. Damit bricht die Konsolenverbindung bei Ausfall eines Systems in keinem Fall ab. Aus Sicht des Administrators stellt sich das Paar wie ein Server dar. Dieses Verhalten ist ideal, um eine derartige Lösung mit wenig Administrationsaufwand und eventuell nur aus der Ferne erreichbar zu betreiben. Bei everRun MX verteilt sich die Administration auf zwei Konsolen, das XenCenter und das everRun Availability Center, wobei die Aufgaben verteilt sind. Jeder Server im Pool hat seine eigene IP-Adresse für das Management, der Zugriff hat immer über den Pool Master zu erfolgen. Fällt der Pool Master aus, reißen die Konsolenverbindungen ab. Dann muss ein anderer Server im Pool diese Rolle übernehmen, wobei die Konsolen mit dessen IP-Adresse neu aufzurufen sind.

Hardwareüberwachung

Bei Avance ist die Überwachung aller Sensoren fester Bestandteil des Produkts und des Konzepts, um sofort auf jegliche funktionalen Probleme reagieren zu können, damit jederzeit der stabilere Server der primäre ist. Der Administrator muss sich daher um die Implementierung nicht extra kümmern. Bei everRun MX hat die Überwachung der Hardware unabhängig auf Xen-Basis zu erfolgen. Die Software reagiert nicht auf Detailprobleme der Basisserver, sondern wird erst aktiv, wenn wichtige Komponenten den Betrieb einer abgesicherten VM tatsächlich beeinträchtigen. Für einen produktiven Betrieb sind daher noch zusätzliche Vorkehrungen notwendig.

Arbeitsweisen und Verfügbarkeit

Avance ist konzipiert für eine Verfügbarkeit von 99,99 Prozent, die betriebenen VMs laufen immer nur auf einem Basisserver und werden bereits bei geringsten Fehlersymptomen auf das zweite System verschoben, um so Auswirkungen präventiv zu vermeiden. Ein plötzlicher Totalausfall des primären Servers hat auf jeden Fall einen Neustart der VMs zur Folge. everRun MX selbst unterstützt zwei Absicherungsstufen bis hin zu 99,999 Prozent Verfügbarkeit. Bei der höchsten Absicherung läuft eine VM gleichzeitig auf zwei Basisservern im Lockstep-Verfahren. Bei einem schlagartigen Ausfall eines Servers läuft eine so gesicherte VM ohne Unterbrechung weiter. Die Absicherung gemäß Level 2 schützt vor einem Komponentenausfall, verschiebt die VMs aber nicht präventiv. Ein kompletter Serverausfall zieht wie bei Avance einen Reboot der darauf laufenden VMs nach sich.

Fazit

Liegt bei einer vorgegebenen Aufgabe der Fokus des Einsatzes auf bestmöglicher Fehlertoleranz, kommt die Stärke von Marathon everRun MX am besten zur Geltung. Im Test haben sich fehlertolerant abgesicherte VMs bei allen Ausfalltests als sehr stabil erwiesen, wobei auch SMP unterstützt wird. Der Administrationsaufwand ist auf jeden Fall höher als bei Avance, da zwei Konsolen zu bedienen sind und die ganze Umgebung insgesamt komplexer gestaltet ist. Nicht so überzeugt haben uns das Verhalten und die Arbeitsweise bei der reinen Komponentenabsicherung (Level 2). Steht nicht die Fehlertoleranz, sondern eine insgesamt sehr hohe Verfügbarkeit im Fokus, konnte sich Stratus Avance im Test besser behaupten. Das Produkt überzeugt durch ein in sich geschlossenes Konzept, welches alle Betriebsaspekte berücksichtigt. Der Zugriff über nur eine IP-Adresse, das komplette Management über eine Konsole und die integrierte Hardwareüberwachung machen das Produkt überaus einfach bedienbar und erfordern nur wenig Administrationsaufwand.

Marathon everRun MX vs. Stratus Avance



im SAN, via iSCSI oder als NFS-Share voraus, auf den mehrere Server zugreifen können. Eine Datenspiegelung ist zudem aus Sicht der Virtualisierungssoftware meist nicht vorgesehen. Beispielsweise unterstützt auch der Marktführer VMware keine Host-basierte Spiegelung. Diese muss letztendlich mit anderen Mitteln quasi im Hintergrund zusätzlich realisiert werden. Eine aus mehreren Servern bestehende virtuelle Infrastruktur steigert zwar unbestritten die Verfügbarkeit gegenüber einem einzelnen Server, es ist aber gar nicht so einfach und meist auch recht kosten-aufwändig, einen Single Point of Failure (SPoF) zu vermeiden.

Stratus Avance dagegen berücksichtigt genau diese Aspekte in seinem Konzept und weist keinen SPoF auf. Realisiert wird dies durch eine integrierte Spiegelung der Volumes, die die virtuellen Maschinen nutzen, und durch eine gegenseitige Überwachung der beiden physikalischen Server. Weiterhin überwacht Avance alle Komponenten des Servers sowie die schon erwähnten Sensoren der Hardware. Aufgrund aller dieser Faktoren entscheidet Avance, welcher der beiden Server der "gesündere" ist und lässt die VMs dort laufen beziehungsweise verschiebt die VMs skriptgesteuert im laufenden Betrieb dorthin, ohne dass es aus Applikationssicht zu einer Unterbrechung kommt. Führt nun ein sich langsam abzeichnendes Problem zu einem Ausfall eines der beiden Server, so hat Avance die VMs mit großer Wahrscheinlichkeit schon vorher auf den anderen verschoben, so dass deren Verfügbarkeit somit gar nicht beeinträchtigt wird. Nur ein plötzlicher Totalausfall des primären Knotens zieht auch die VMs in Mitleidenschaft. Diese werden dann innerhalb weniger Sekunden auf dem verbleibenden Knoten neu gestartet.

Im Labor haben wir das Verhalten intensiv getestet, indem wir durch Ziehen von Festplatten, Unterbrechung der Netzwerkverbindung und eines Stromkabels an einem der beiden redundanten Servernetzwerke verschiedene Defekte simuliert haben. Neben dem Testen mit solchen praxisnahen Fehlern konnten wir auch

über ein kleines Portal Fehler einspielen. Das über einen undokumentierten Link erreichbare Portal hat Stratus für Demonstrationzwecke eingebaut.

Alle Fehlersituationen haben wir stets am primären Knoten initiiert, um zu sehen, ob die VMs verschoben werden und die Alarmierung beziehungsweise Benachrichtigung klappt. Dabei hat uns die zuverlässige Arbeitsweise sehr beeindruckt. So führt beispielsweise eine Unterbrechung der Netzwerkverbindung des primären Servers in das Anwendernetz nur zu einem Aussetzer beim mitlaufenden Ping-Test, während bestehende Netzwerkverbindungen nicht unterbrochen werden. Die Kommunikation schaltet sofort auf die verbleibende Verbindung um, während Avance im Hintergrund den anderen Knoten zum primären macht und die VMs verschiebt.

Nur massive Fehler wie das gleichzeitige Ziehen aller Netzwerkverbindungen oder das plötzliche Abschalten des primären Servers führten dazu, dass ein Verschieben nicht mehr möglich war und die VMs auf dem anderen Server neu gestartet werden mussten. Die prognostizierten 99,99 Prozent Verfügbarkeit dürfte Stratus Avance im produktiven Betrieb tatsächlich erfüllen oder gar übertreffen können.

Als sehr angenehm erwies sich die Tatsache, dass das Serverpaar nach außen nur über eine IP-Adresse sichtbar ist und auch nicht zwischen Management- und Benutzerzugriff unterschieden wird. Dadurch riss nie die Verbindung zur Konsole ab und wir konnten immer die glei-

che Adresse zur Anmeldung nutzen, egal, welcher Server gerade aktiv war.

Schnelle Wiederherstellung

Neben der intelligenten Failover-Technik ist es für eine dauerhafte hohe Verfügbarkeit unbedingt erforderlich, dass ein aufgetretener Defekt möglichst schnell wieder behoben wird. Ist ein Knoten ausgefallen, laufen die VMs zwar erst einmal weiter, ein weiteres Problem am verbliebenen Knoten könnte dann aber einen längeren Ausfall nach sich ziehen. Je nach Supportvertrag sollten also das verpflichtete Systemhaus oder der Administrator selbst zügig aktiv werden, um wieder völlige Redundanz herzustellen. Die beiden Optionen Call Home und Dial-In stellen auf Wunsch eine schnelle Benachrichtigung und Reaktion sicher.

Was die Fehlerbehebung an sich anbetrifft, gibt es hierfür ein umfassendes Handbuch, in dem die möglichen Vorgehensweisen detailliert beschrieben sind. Sobald es sich hierbei nicht um eine reine Hardware-Reparatur handelt, sondern auch die Daten auf einem Server in Mitleidenschaft gezogen wurden, sind in Avance entsprechende Mechanismen implementiert, die eine schnelle Wiederherstellung ermöglichen. Letztendlich läuft dies ähnlich ab wie die Einrichtung der zweiten Maschine bei der Installation. Dazu wählt der Administrator in der Konsole die gewünschte Wiederherstellung aus. Beispielsweise kann ein Recovery mit oder ohne Plattenformatierung erfolgen. Dann startet er den ausgefallenen Knoten, der nun mittels PXE über den privaten Link bootet und sich auf diesem Wege die eigene Konfiguration holt,



Bild 4: Ein Highlight von Avance ist die überaus einfache Wiederherstellung einer ausgefallenen Site oder Node per PXE-Boot und Imaging

Citrix XenApp 6 und XenDesktop 5



- Planung, Installation, Konfiguration und Verwaltung
- Alle Editionen von XenApp 6 und XenDesktop 5
- Inkl. Best Practices und Troubleshooting

608 S., 4. Auflage 2011, 59,90 €
» www.galileocomputing.de/2465



VMware vSphere 4



- Installation, Konfiguration, Administration
- Sicherheit, Migration, Backup, Lizenzierung
- Storage Design, Storage Konfiguration u. v. m.

1.052 S., 2010, 89,90 €
» www.galileocomputing.de/2179



Linux Hochverfügbarkeit



- Lokale HA: RAID, LVM, NIC-Bonding und SMART
- Linux HA-Cluster: Corosync/OpenAIS, Pacemaker, DRBD und CLVM
- Xen/KVM-VMs im Cluster, Backup und Disaster Recovery

454 S., 2011, 49,90 €
» www.galileocomputing.de/1999



Linux-Server

Das Administrationshandbuch



- Linux-Server distributions-unabhängig einrichten und administrieren
- Backup, Sicherheit, Samba, LDAP, Webserver, Mailserver, Datenbanken
- Inkl. Best Practices und Praxislösungen

815 S., 2011, 49,90 €
» www.galileocomputing.de/2205



www.GalileoComputing.de

booksonline



» www.facebook.com/GalileoPressVerlag



» www.twitter.com/Galileo_Press



indem er die primäre Maschine quasi klonet. Anschließend wird die Spiegelung der Nutzdaten wieder eingerichtet. Sehr gut gefallen hat uns hier, dass die komplette Wiederherstellung keine Benutzereingaben erfordert und somit den Stressfaktor beim Administrator nicht unnötig erhöht. Auch das Handbuch mit den genauen Anweisungen hilft dabei, etwaige Unsicherheiten abzubauen. Nichtsdestotrotz sollte ein Administrator, der möglicherweise einmal eine Wiederherstellung durchführen muss, dies vorher getestet haben.

Neben dem Recovery beschreibt Stratus übrigens auch die genaue Vorgehensweise bei Aufrüstungen. Durch eine wechselweise Erweiterung oder gar einen Hardwaretausch mit jeweiligem Verschieben des primären Knotens lassen sich sogar diese Arbeiten durchführen, ohne dass die auf der Umgebung laufenden VMs heruntergefahren werden müssen. Nur falls bei einem Hardwaretausch auf inkompatible Komponenten gewechselt werden soll (beispielsweise Upgrade auf eine inkompatible Prozessorgeneration), ist eine kurze Downtime erforderlich.

Insgesamt haben uns sowohl die Einfachheit in der Handhabung als auch die sehr genaue Beschreibung der notwendigen Schritte bei einer Wiederherstellung oder auch einer Hardwareaufrüstung recht gut gefallen.

Zum Abschluss des Tests konnten wir noch einen kurzen Blick auf die Version 2.1 und deren Neuerungen werfen. So ist es damit möglich, für die Synchronisation der Laufwerke einen eigenen 10 GBit-Link einzurichten, was die Plattenperformance um bis zu 40 Prozent verbessern soll. Auch kann Avance nun mit vertauschten Netzwerkanschlüssen umgehen, falls hier bei einem Systemwechsel ein Fehler unterlaufen ist. Weiterhin können jetzt in einem Server Netzwerkkarten unterschiedlichen Typs verwendet werden. Hinzu gekommen sind auch weitere Gastbetriebssysteme, die wir in der Übersicht bereits berücksichtigt haben.

Fazit

Normalerweise ist es ein Administrator gewohnt, dass ein hochverfügbares System auch eine größere Komplexität in

der gesamten Bedienung mit sich bringt. Stratus Avance hat uns hier eines Besseren belehrt und geradezu begeistert. Die aus wenigen Schritten bestehende Installation ist erfreulich einfach, wobei sie oft auch durch einen Stratus-Systempartner erfolgt. Im Vorfeld ist nur zu beachten, dass es sich um zertifizierte Hardware einiger bekannter Serverhersteller handeln muss und die beiden Server idealerweise identisch aufgebaut sein sollten. Die integrierte Spiegelung der Daten zwischen den beiden Systemen macht die Lösung sehr kompakt und zugleich preiswert. Eine getrennte Aufstellung an zwei entfernten Standorten ist möglich, es sind nur die Latenzzeiten im Netzwerk zu beachten.

Die Betreuung eines laufenden Systems hat sich im Test als sehr einfach erwiesen, da der Administrator letztendlich zwei Server nutzt, diese aber wie einen über eine zentrale Konsole bedient. Die Lösung ist durchaus geeignet in Situationen, wo eine hohe Verfügbarkeit bei geringem Administrationsaufwand gefordert ist. Durch spezielle Features wie Call Home und Dial-In kann sich das System bei Problemen zuverlässig selbst bemerkbar machen und ermöglicht zudem eine einfache Betreuung aus der Ferne. Für gut gelungen halten wir auch die vorgesehenen Wiederherstellungsmechanismen, bei denen eine ausgefallene Seite durch PXE-Boot und Imaging mit anschließender Datenspiegelung fast ohne Benutzereingaben in kurzer Zeit wieder in Betrieb genommen werden kann.

Der Test verschiedener Ausfallszenarien hat gezeigt, dass die interne Überwachung gut funktioniert und die laufenden virtuellen Maschinen zuverlässig auf den gesünderen Knoten verschiebt. Nur ganz schwere Hardwaredefekte oder ein Totalausfall einer Seite können dazu führen, dass die hochverfügbaren VMs booten müssen. Durch den komplett redundanten Aufbau ist aber ein weiterer Betrieb sichergestellt und es bleibt ausreichend Zeit für eine Reparatur beziehungsweise völlige Wiederherstellung. Die avisierte Verfügbarkeit von 99,99 Prozent und besser halten wir daher für sehr realistisch. Insgesamt überzeugt Stra-

tus Avance durch ein attraktives Preis-/Leistungsverhältnis, eine für die meisten Anforderungen völlig ausreichende Verfügbarkeit und eine überaus einfache Bedienung. (jp)



Produkt

Hochverfügbarkeitssoftware für zertifizierte Standardhardware zum Aufbau einer HA-Lösung mit über 99,99 Prozent Verfügbarkeit.

Hersteller

Stratus
www.de.stratus.com

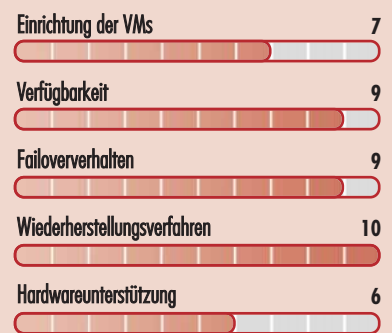
Preis

Avance kostet 4.000 Euro pro Serverpaar, unabhängig von der Anzahl der CPUs und VMs. Wartung und Updates kosten 960 Euro jährlich.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für kleinere Unternehmen und Außenstellen, die auf eine preiswerte und zugleich sehr hohe Applikationsverfügbarkeit angewiesen sind.

bedingt in Umgebungen, die bereits auf eine andere Virtualisierung als Xen setzen, da eine Integration der verschiedenen Virtualisierungsplattformen nicht möglich ist.

nicht für absolut unternehmenskritische Anwendungen. Hier sind für eine noch höhere Verfügbarkeit ausfalltolerante Lösungen sinnvoll.

Stratus Avance R2.0.2

[1] Kompatibilitätsmatrix
B7T21

Link-Codes



Ausfallsichere IT-Überwachung mittels Clustering

Netzwerk-Monitoring hochverfügbar und wachsam

Das allgemeine Wachstum im IT-Markt und die zunehmende Abhängigkeit von IT-Systemen macht es für Administratoren immer wichtiger, den Überblick über ihr komplexes Netzwerk zu behalten und rechtzeitig auf Störungen zu reagieren. Um diesen Anforderungen gerecht zu werden, ist es notwendig, das Firmennetzwerk permanent und unterbrechungsfrei zu überwachen. Dazu sollte eine hochverfügbare Monitoring-Software eingesetzt werden, die durch eine Failover-Cluster-Lösung selbst unterbrechungsfrei zur Verfügung steht.

Vermehrt rüsten Unternehmen ihre interne IT-Infrastruktur aus Effizienzgründen auf hochverfügbare virtualisierte Systeme um. Denn durch die Konsolidierung möglichst vieler Anwendungen auf einer zentralen Hardware können Ressourcen eingespart werden. Allerdings ergibt sich daraus gleichzeitig ein erhöhtes Bedürfnis nach Ausfallsicherheit.

Welche Strategie ein Unternehmen auch ergreift, um hochverfügbare, ausfallsichere Systeme aufzubauen: Die Anforderungen an heutige IT-Systeme und deren Administratoren steigen – und damit auch die Gefahr von Netzwerküberlastungen und -ausfällen. Um die ständige Verfügbarkeit der IT-Infrastruktur zu gewährleisten, ist es ratsam, die Planung und Erfolgskontrolle mit einer hochverfügbaren Monitoring-Lösung zu begleiten. Eine geeignete Monitoring-Lösung leistet wertvolle Dienste, um die Infrastruktur kosteneffizient in die nächste Stufe der Hochverfügbarkeit zu überführen. Beispielsweise sammelt ein fortlaufendes Monitoring detailliert und verständlich aufbereitete Netzwerkdaten, Trendanalysen sowie „harte Fakten“ zu Ausfällen und Auslastung aller überwachten Komponenten der IT-Umgebung als Basis für fundiert geplante Anschaffungen.

Redundante Netzwerküberwachung

Im Punkt Ausfallsicherheit setzt der Netzwerküberwachungsspezialist Paessler auf einen Failover-Cluster, der in die Software PRTG Network Monitor integriert ist. Damit wird ein ausfallsicheres Monitoring ermöglicht, in dem ein „Master“ und bis zu vier „Failover“-Knoten parallel die IT-Umgebung im Blick behalten. An jedem Knotenpunkt führt jeweils eine vollständige Installation des PRTG Network Monitor selbstständig

die komplette Überwachung des Netzwerks durch. Mit Hilfe dieser Cluster-Installation wird die Betriebszeit nicht mehr durch Verbindungsstörungen, einen Ausfall der Internetanbindung am PRTG Server, fehlerhafte Hardware oder Software-Upgrades beeinträchtigt. Selbst bei einem Crash des Hauptservers („Master“) läuft das Monitoring ganz normal weiter.

Die Monitoring-Konfiguration sowie Software-Updates



Bereits eine „Single Failover“-Installation ermöglicht ausfallsicheres Monitoring und die Abfrage von Überwachungsdaten aus unterschiedlichen Perspektiven.

werden automatisch im Cluster verteilt, was die Handhabung sehr einfach macht. Auf Basis dieser Konfiguration überwachen die einzelnen Installationen parallel das gesamte Netzwerk – optional aus verschiedenen Perspektiven und, falls erforderlich, auch in verteilten Netzwerken. Anschließend speichern sie die Resultate in ihrer eigenen Datenbank ab, wodurch selbst bei einem kompletten Datenverlust auf einem Knoten immer noch die Monitoring-Ergebnisse auf den anderen Nodes bereitstehen. Für den Fall, dass ein oder mehrere Knoten Ausfälle oder Schwellenwertüberschreitungen erkennen, erhält der Administrator per E-Mail, SMS etc. eine zentrale Benachrichtigung durch den „Master Node“. Im Falle eines Systemausfalls wird die „Master“-Rolle von einem „Failover“-Knoten übernommen, sodass Benachrichtigungen und Berichte unterbrechungsfrei zur Verfügung stehen.

Weitere Informationen finden Sie unter <http://www.de.paessler.com/prtg/features>.



Paessler AG

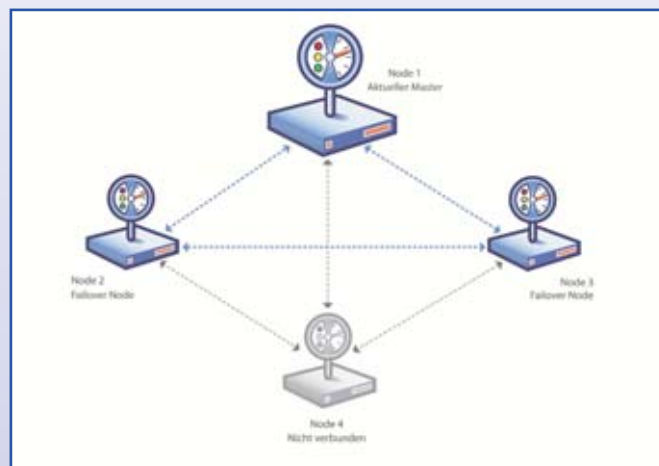
Burgschmietstraße 10
D-90419 Nürnberg
Tel.: +49 (911) 9 37 75 - 0
Fax: +49 (911) 9 37 75 - 409

E-Mail: info@paessler.com

URL: www.de.paessler.com

Ansprechpartner:

Dorte Winkler



In einem PRTG-Cluster führen alle „Knotenpunkte“ ein selbstständiges Monitoring durch. Dies ermöglicht eine lückenlose Datenaufzeichnung, selbst wenn ein Node ausfällt

Im Test: Acronis Disk Director 11 Advanced Server

Zentrales Festplattenmanagement

von Thomas Bär

Allen aktuellen Entwicklungen des Cloud Computings zum Trotz speichern Benutzer das Gros ihrer Daten immer noch auf Servern im lokalen Netzwerk. Administratoren sind dementsprechend häufig mit Themen wie dem Partitions-Layout oder dem Zusammenführen von Festplatten beschäftigt. Zwar wurden die Bordmittel von Microsoft Windows Server 2008 in Bezug auf die Datenträgerverwaltung deutlich aufgewertet, alle Anforderungen erfüllen sie jedoch immer noch nicht. Die entstehende Lücke zwischen den Wünschen des Administrators und den tatsächlichen Fähigkeiten des Windows Servers will der Disk Director 11 Advanced Server von Acronis füllen.

Acronis Disk Director 11 Advanced Server (ADD) ist eine Software mit Funktionen für die Partitionierung und das Festplattenmanagement, um einen möglichst effizienten Betrieb der Server sicherzustellen. Der Hersteller Acronis bietet bereits seit vielen Jahren Produkte für Microsoft Windows an und ist in erster Linie durch die Produktlinie "True Image" am Markt bekannt geworden.

Die aktuelle Version des Disk Director vom Herbst 2010 fasst wichtige Funktionalitäten zusammen und bietet dem Administrator so die Möglichkeit, die Festplattenverwaltung zentral durchzuführen, fortgeschrittene Disk Layout-Operationen anzuwenden, Partitionen wiederherzustellen oder mit dem Disk Editor direkt auf die Rohdaten zugreifen zu können. Selbst die Extraktion von Informationen von Datenträgern, die aufgrund eines Software- oder Hardware-Fehlers oder eines Virenangriffs verschwunden sind, so der Hersteller, ist mit der Software möglich. Das aktuelle Windows Server 2008 R2-System, einschließlich Microsoft Small Business Server, wird ebenso unterstützt wie dynamische Festplatten oder GPT-Festplatten (siehe Kasten "GPT-Festplatten").

Installation ohne Schwierigkeiten

Die Installation der Software ist insgesamt sehr einfach und in wenigen Minuten er-

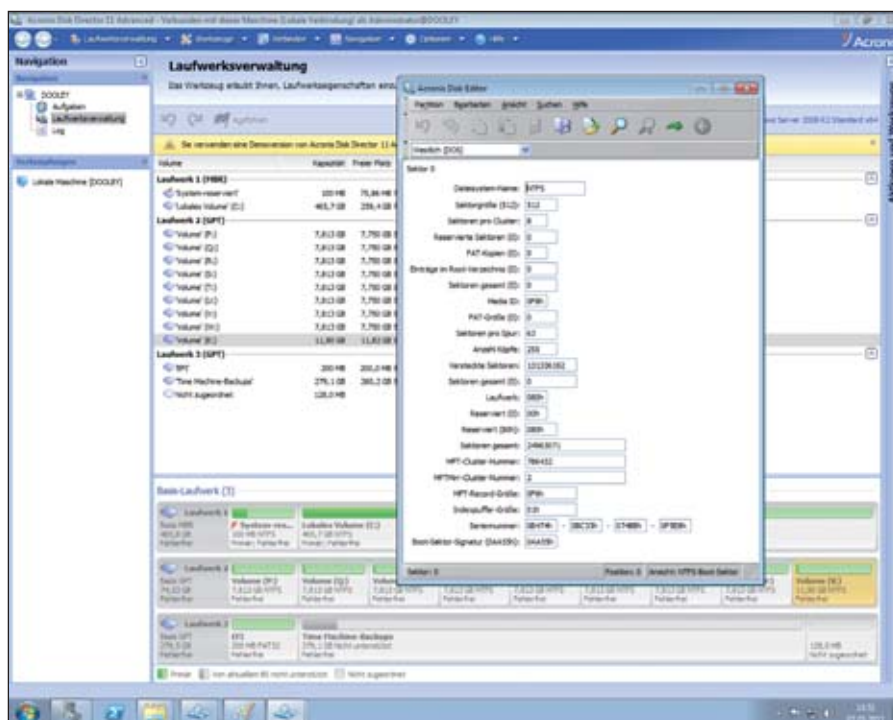


Bild 1: Alle Festplatten-Details listet der Disk Director auf – hier Informationen zum NTFS-Bootblock

ledigt. Ein Neustart ist nicht erforderlich. Die im Internet angebotene Trial-Version für einen 15-tägigen Test ist gelinde gesagt überflüssig, da faktisch keine Funktion tatsächlich einsetzbar ist. Das Einzige, das der Anwender sieht, ist die Oberfläche, die Auflistung der Laufwerke und dass ein Zugriff auf entfernte Rechner, auf denen ebenfalls ADD eingerichtet ist, möglich wäre. Nicht einmal das Umbenennen eines Volumes am lokalen Rechner ist aus

der Demo-Software heraus möglich. Andere Hersteller bieten zumindest die volle Funktionalität auf kleineren Volumes an. Welchen Sinn in diesem Fall eine Demoversion haben soll, das sei dahingestellt.

Erwartungsgemäß betreibt Acronis die Agent-Komponenten als Windows-Dienst. Der Administrator kann während der Installation diesem Dienst ein zuvor angelegtes, spezielles Konto zuweisen oder



verwendet den vom Installer automatisch eingerichteten User. Der Fernzugriff auf Acronis-Installationen über Domänen-grenzen hinweg aus der Management-Konsole ist losgelöst von diesem Account möglich, da im Zweifelsfall ein Anmelde-dialog eingeblendet wird. Glücklicherweise ist es möglich, die Zugriffsinformationen abzuspeichern.

In der Summe richtete der Installations-Assistent bei der Vollinstallation drei Komponenten der Software ein: den Agent für Windows, den "Bootable Media Builder" und die "Management Console". Die Kommunikation zwischen den entfernten Agents und der Konsole findet über den TCP-Port 9876 statt. Ein Blick in die "Well known Port"-Liste der IANA offenbart, dass dieser Port nicht von Acronis reserviert ist. Eine entsprechende Anpassung der Windows-Firewall-Richtlinien muss der Administrator selbst vornehmen. Ist im Unternehmen eine Anpassung des Ports notwendig, so kann der Administrator dies über eine Gruppenrichtlinie recht elegant durchführen. Wer in seiner Umgebung viele Rechner außerhalb einer Domänenstruktur betreut,

Die Konsole lässt sich auf allen Windows-PCs mit Windows XP SP2 oder höher installieren (auch auf den Home-Editionen). Die Serverkomponenten erfordern Windows XP Professional SP2 oder höher und unterstützen sowohl die x86- als auch x64-Ausprägung. Home- oder Starter-Editionen sind hier ebenso ausgeschlossen wie der Einsatz unter IA64-Windows. Als Dateisysteme unterstützt die Software FAT16, FAT32, NTFS, Ext2, Ext3, Reiser und Linux Swap. Die Erstellung, Größenänderung, Kopie, Verschiebung, Aufteilung und Zusammenführung von Volumes ist jedoch unter Reiser4 nicht anwendbar.

Für eine vollständige Installation der Software wird kurzfristig bis zu 2 GByte freier Speicherplatz auf dem Server verlangt. Für den Regelbetrieb ist rund 1 GByte Speicherplatz auf dem Server erforderlich. Die Agent-Komponenten benötigen 500 MByte Platz zur Installation und 260 MByte im normalen Betrieb. Da eine der wichtigsten Aufgaben der Software eine Zusammenführung oder Vergrößerung von Volumes ist, kann das halbe Gigabyte bei der Installation schon zu einem Hemmnis werden. Für diese Fälle bietet Acronis die Möglichkeit, aus der Software eine Boot-CD zu erstellen und über das so gestartete, externe Betriebssystem Anpassungen an der Volume-Zusammenstellung vorzunehmen.

Systemvoraussetzungen

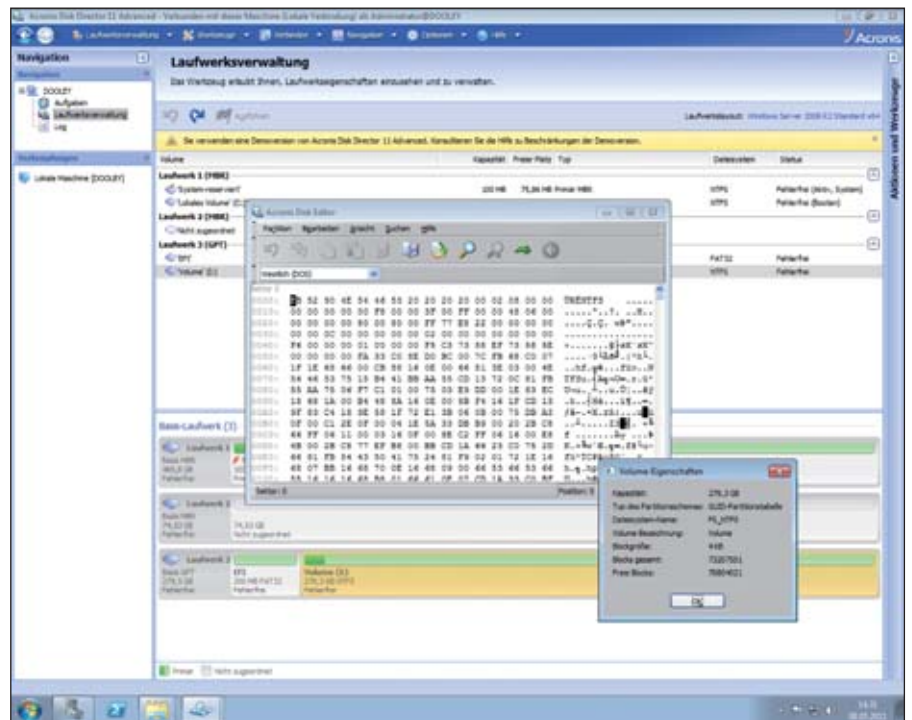


Bild 2: Der Disk Editor ermöglicht die direkte Bearbeitung von Daten auf dem Laufwerk. Die gezielte Manipulation von einzelnen Dateien ist jedoch mit dem Tool eher schwierig.

wird wohl oder übel die Anpassung in der Registry der Zielrechner manuell durchführen müssen.

Moderne Konsole sorgt für strukturiertes Arbeiten

Die Laufwerksverwaltung mit ADD verdient in der Kategorie "Design" ohne jede Frage einen der obersten Ränge. Die Oberfläche ist modern, sehr gut strukturiert und weitgehend angenehm in der Bedienung. Die angezeigten Informationen sind stets aktuell und die Software aktualisiert die Darstellung in Echtzeit. Selbst wenn über die Standard-Bordmittel von Windows eine Umkonfiguration vorgenommen wird, so ist dies in der Acronis-Konsole sofort zu sehen. Jedoch geschah es mehrmals im Test, dass bei massiven Anpassungen in der Datenträgerverwaltung von Windows die Acronis-Konsole mit einem spontanen Absturz reagierte.

Die kontextsensitive Hilfefunktion in einer CHM-Datei ist komplett in deutscher Sprache gehalten und erklärt alle Sachverhalte der Software kurz und prägnant. Auf der linken Fensterseite ist ein Navigationselement angebracht, in dem auch die Verknüpfungen zu anderen Computern und Servern aufgerufen werden. Alle

Befehle der Software sind sowohl über das Kontextmenü als auch über die Menüleiste erreichbar. Zusätzlich kann sich der Administrator auf der rechten Fensterseite die "Aktionen und Werkzeuge" noch einmal einblenden lassen.

Dass ein Befehl nicht entdeckt werden kann, sollte bei so vielen Wegen kaum zu erwarten sein. Und doch ist es den Entwicklern bei Acronis gelungen, für Verwirrung zu sorgen. Befehle, die sich im Zusammenhang mit dem aktuell gewählten Element nicht ausführen lassen, werden überhaupt nicht angezeigt. Anders als es beispielsweise bei Microsoft-Produkten üblich ist, bei denen der Befehl grau dargestellt wird. So fehlt der Befehl "Verstecken" unter GPT-Laufwerken, während er bei MBR-Laufwerken erscheint. Da die Gesamtanzahl der Befehle die Darstellung in der Konsole noch nicht überschreitet, wäre es wünschenswert, dass Acronis diese "harsche" Form der Kontextdarstellung unterlässt.

Unter "Aktionen" fasst ADD Befehle zusammen, die sich im Zusammenhang mit dem Laufwerk oder Volume ausführen lassen. Jede Aktion öffnet ein eigenes Aktionsfenster mit grafischer Darstellung der Auswirkung des Befehls und sehr gut er-



klären Optionen. Wird beispielsweise der Dialog “Größe von Volume ändern” geöffnet, so sieht der Administrator ein kompaktes Fenster mit der Möglichkeit, über einen “Schieber” die Größe zu verändern. Thematisch passende Optionen, wie beispielsweise das Volume zu “Einfach/Übergreifend” zu konvertieren, sind in diesem Fenster für den Administrator sofort im Zugriff. Kommandos werden in ADD nicht unmittelbar ausgeführt, sondern zunächst in einer Liste gesammelt. Wie sich die Befehle auf das Layout der Laufwerke auswirken werden, zeigt die Darstellung jedoch sofort an. Vor- und Zurück-Schaltflächen ermöglichen dem Administrator die Anpassungen noch einmal Revue passieren zu lassen. Möchte der Administrator die gesammelten Kommandos tatsächlich durchführen, so klickt er auf die Schaltfläche “Ausführen”. Ähnlich verhält sich die Software bei den anderen Funktionen, zumindest wenn sie von Acronis selbst geliefert werden. Die Kommandos “Prüfen” und “Defragmentieren” verweisen schlicht auf die Windows-Basisfunktionen.

Partitionen durch Klonen zusammenführen

Die Besonderheiten des ADD liegen in der Fähigkeit, Partitionen wiederherzustellen und Volumes ohne Datenverlust zusammenzuführen. Beim einfachen Kopieren von Partitionen bestand immer die Problematik, dass ein System-Volume

GPT steht für “GUID Partition Table” und ist ein Nachfolger für die bisher gebräuchliche Festplatten-Organisation mit MBR (Master Boot Record). GPT ist somit ein Standard für das Format von Partitionstabellen auf Festplatten oder auch anderen Datenträgern. Die GPT-Spezifikation ist ein Teil des EFI-Standards, der langfristig das traditionelle BIOS bei Computern ersetzen soll. Das aktuell verbreitete Datenträger-Partitionsformat MBR unterstützt Volumes mit einer Größe von bis zu 2 TByte und bis zu vier Primärpartitionen pro Datenträger beziehungsweise drei Primärpartitionen, eine erweiterte Partition und eine unbegrenzte Anzahl logischer Laufwerke. Im Vergleich dazu unterstützt das Partitionsformat GPT Volumes mit einer Gesamtgröße von bis zu 18 Exabyte bei bis zu 128 Partitionen pro Datenträger. Die Integrität der Partitionsdatenstruktur ist bei GPT durch redundante Primär- und Sicherungspartitionstabellen verbessert worden.

GPT-Festplatten

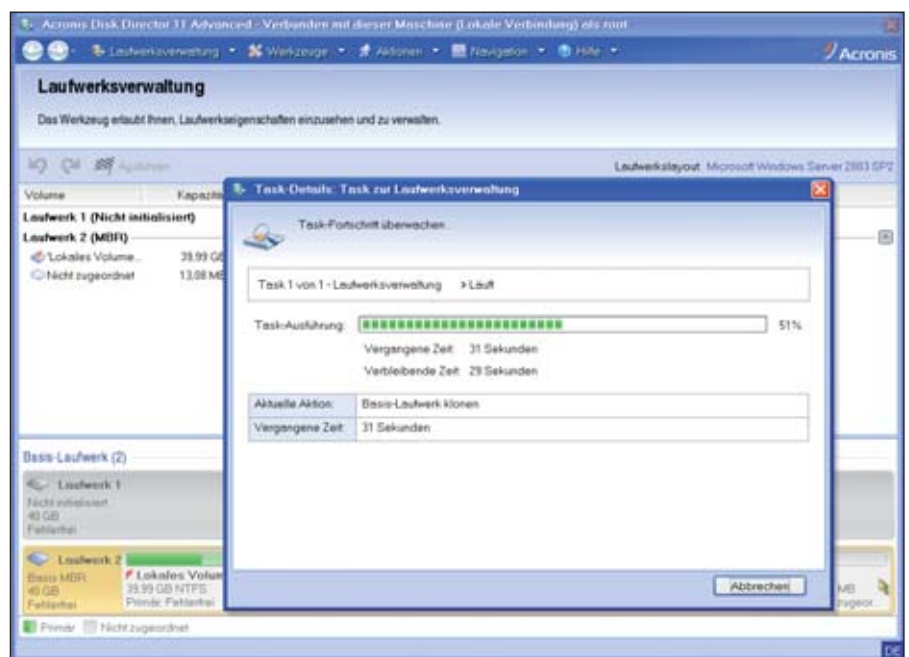


Bild 3: Acronis Disk Director bietet spezielle Boot-Medien unter WinPE und Linux an. Alle Funktionen, auch das Klonen ganzer Festplatten, stehen zur Auswahl.

mit Betriebssystem möglicherweise nicht mehr startete. In der jüngsten Version des Disk Directors wird dieses Problem durch ein neues Feature gelöst: Klonen. Mit einem Assistenten zum Klonen von Laufwerken können Anwender ein Basis-Laufwerk vom MBR-Typ durch ein neues ersetzen, ohne das Betriebssystem oder Anwendungen neu installieren zu müssen. Alle Daten des Quelllaufwerks werden direkt auf das Ziellaufwerk übertragen. Die Volumes des Quelllaufwerks werden dabei entweder 1-zu-1 übernommen oder automatisch an die üblicherweise größere Kapazität des Ziellaufwerks angepasst.

Im Test funktionierte das Klonen ohne jegliche Schwierig- oder Auffälligkeit, selbst beim Wechsel von SCSI nach IDE. Die Zusammenführung zweier Volumes funktionierte im Test ebenso einfach. Wir hängten ein FAT32-Volume an ein Volume mit NTFS-Filesystem und nach wenigen Minuten war das vereinte Laufwerk nutzbar. Der Anwender findet in diesem Fall alle Dateien aus dem untergeordneten Laufwerk in einem Ordner namens “Merged Files”.

Leistungsfähiges Recovery für Partitionen

Die Wiederherstellung verschwundener oder versehentlich gelöschter Partitionen

dürfte jedem Administrator schon einmal als Aufgabe zuteilgeworden sein. Gründe für den Verlust von Partitionen gibt es genug: menschliches Versagen bei Verwendung der Datenträgerverwaltung, Stromausfälle, maligne Software oder sonstige Hard- und Softwarefehler. Hierfür integriert Acronis den “Recovery Expert” in ADD. Es handelt sich dabei um ein insgesamt einfach zu bedienendes Tool zur Rekonstruktion von Volumes. Damit der korrigierende Eingriff funktioniert, gibt es zwei Bedingungen: Es muss sich um ein Basislaufwerk handeln und es muss im MBR-Typ vorliegen. Verwendet der Administrator die Funktion auf einem GPT-Laufwerk, so erscheint jedoch kein Warnhinweis – das Fenster des Recovery Experts schließt sich einfach nur still von selbst.

Der Recovery Expert arbeitet im automatischen Modus faktisch von allein und versucht die ursprüngliche Struktur auf einem Laufwerk komplett wiederherzustellen. Die Software analysiert dazu auf jedem Laufwerk zunächst nur die ersten Einträge der Zylinder und des Boot-Sektors. Wird bei diesem Vorgang kein reaktivierbares Layout gefunden, steht dem Administrator noch die “vollständige Methode” zur Verfügung. Da hierbei das komplette Laufwerk Sektor für Sektor abgearbeitet wird, dauert dieser

2. unabhängiges
IT TECH FORUM für System- und
Netzwerk-Administratoren

IT Admin



20.–21. September 2011,
Holiday Inn Frankfurt City-South, Conference Centre

Tech Talk 2011

Workshop A: Microsoft Office 365 (19. September 2011, separat buchbar)

Workshop B: IPv6 – Technologie und Migration (22. September 2011, separat buchbar)

Top IT-Tech-Experten



Nico Lüdemann,
acocon GmbH



Ulf B. Simon-Weidner,
Computacenter AG & Co. oHG



Dennis Zimmer,
icomsoft ag



Nils Kaczinski,
WITstor GmbH

30 Sessions bieten Ihnen erprobtes Praxis-Know-how aus den Bereichen:

- Server-/Desktop-/Applikationsvirtualisierung
- Microsoft Sharepoint 2010/Office 365/
Exchange/Windows Intune
- Mobile Devices/Bring your own Device (ByoD)
- Mobile und IT Security
- Active Directory
- IPv6 Migration
- Cloud Computing
- Enterprise Monitoring mit Open Source
- Storage/Deduplizierung

+++ 895,- Euro für Frühbucher +++ Weitere Preisvorteile für Abonnenten des IT-Administrator +++

in Kooperation mit der Fachzeitschrift:



Info-Telefon: 02 11/96 86-34 48 (Tatiana Sacchi)

www.iir.de/administrator

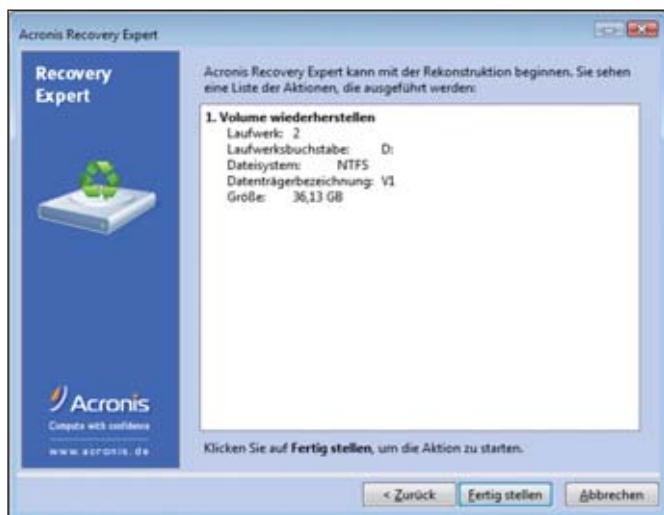


Bild 4: Das Wiederherstellen versehentlich gelöschter oder defekter Partitionen geschieht im Idealfall vollautomatisch innerhalb weniger Minuten

Vorgang entsprechend lange. Im Test konnten im Vorfeld bewusst gelöschte Laufwerke komplett wiederhergestellt werden. Mitunter entdeckt der Recovery Expert viele Partitionen auf einer Festplatte, je nachdem wie "bewegt" die Vergangenheit des Laufwerks ist.

Disk-Editor für Experten

Der in ADD enthaltene Acronis Disk Editor erlaubt das Sichern, Wiederherstellen und Editieren von Festplattenbereichen, indem er die Festplatteninhalte direkt auf der Hexadezimal-Ebene darstellt. Der Editor verfügt über einfache Navigations- und Suchfunktionen und ist in der Lage, Sektoren in Dateien zu speichern und wieder auszulesen. Wie die anderen Programme in ADD führt der Editor auch erst dann die Änderungen tatsächlich durch, sofern der Administrator die Speicherung im Sektor bestätigt. Leider ist dem Anwender nicht möglich den aktuellen Sektor in der An-

sische Möglichkeit, Informationen aus Datenbereichen von Festplatten extrahieren und bearbeiten zu können, darf nicht darüber hinwegtäuschen, dass für eine solche Bearbeitung ein fundiertes Detailwissen erforderlich ist. Leider fehlt dem Programm die Möglichkeit, über eine Explorer-Funktion direkt nach Dateien zu suchen. Die in der Webseite vollmundig als Schlüsselfunktion benannte "Multi-Window"-Fähigkeit ist leider nicht nutzbar, da nur ein Editor-Fenster geöffnet werden kann, welches stets den Fokus behält, bis es geschlossen wird.

Besonders praktisch für Administratoren, die eine exakte Protokollierung ihrer Aktionen benötigen, ist die "Log"-Funktion von Acronis. Das Log speichert den Verlauf der Aktionen, die auf der Maschine durchgeführt wurden. Bei dem Log handelt es sich um eine XML-Datei, die in der Oberfläche von Acronis als Tabelle dargestellt wird. Durch Filter-Funktionen ist es dem Anwender sehr leicht möglich, die Darstellung auf die tatsächlich gewünschten Informationen zu begrenzen.

Fazit

Acronis Disk Director 11 Advanced Server ist eine äußerst kompakte und funktionelle Software für die Bearbeitung von Festplatten und deren Layouts. Besonders im Zusammenspiel mit dem Windows Server 2003 ist der Administrator durch die Software in der Lage, alle Datenträger-Aktionen durchzuführen, die sonst nur der Windows Server

sicht zu verlassen, sofern eine Änderung nicht gespeichert oder verworfen wird.

Der Acronis Disk Editor lässt sich direkt über die Konsole starten oder über das Acronis Boot-Medium. Die Unterstützung für IDE-, SCSI-, USB- oder IEEE 1394-Festplatten ist auch über das Boot-Medium gewährleistet. Die tech-

2008 bietet. Aber auch für Windows Server 2008 bietet die Software einige Mehrwerte, wie das Klonen von Laufwerken oder die Wiederherstellung gelöschter Partitionen.

Es gibt zwar einige Open Source-Produkte am Markt, die annähernd ähnliche Funktionen bieten, jedoch nicht in dieser kompakten Form. Üblicherweise fehlen diesen zumeist als Freeware angebotenen Programmen zudem die Möglichkeit, die Aktionen über das Netzwerk auf entfernten Servern durchzuführen. Der mit über 500 Euro doch recht hohe Lizenz-Listpreis lohnt sich jedoch nur dann, wenn regelmäßige Änderungen an Volumes durchgeführt werden sollen. (jp) **IT**

Produkt

Software zur Verwaltung und Wiederherstellung von Festplatten.

Hersteller

Acronis Germany GmbH
www.acronis.de/enterprise/products/diskdirector-server/

Preis

551 Euro

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Laufwerksverwaltung	7
Laufwerke klonen	9
Wiederherstellung	8
Boot-Medium	9
Disk-Editor	5

Dieses Produkt eignet sich

optimal für Unternehmen, die regelmäßig Verwaltungsaufgaben von Laufwerken und Volumes im Netzwerk durchführen.

bedingt für Unternehmen, die nur sehr selten Datenträgerverwaltungsaufgaben erledigen.

nicht für Unternehmen, in denen keine Windows-Server betrieben werden.

**Acronis Disk Director 11
Advanced Server**

Mit dem Acronis Bootable Media Builder ist die Software in der Lage, die Funktionen losgelöst von einem lokalen Betriebssystem durchzuführen. Als Basis verwendet Acronis, je nach Auswahl des Administrators, WinPE oder Linux. Der Vorteil der WinPE-Variante liegt darin, dass sich Treiber für SCSI-, RAID- oder SATA-Controller explizit einbinden lassen. Das Boot-Medium muss nicht notwendigerweise auf eine CD/DVD oder einen USB-Stick installiert werden. Auch eine Einbindung in eine PreBoot-PXE-RIS Umgebung ist denkbar.

Unabhängig vom Betriebssystem





Im Test: Double-Take Availability 5.3

Ausfallsicherheit mit Hyper-V

von Thomas Bär

“Nichts kann einem den Tag so verderben wie ein Server-Ausfall” – mit dieser Überschrift leitet der Hersteller Vision Solutions, einst Sunbelt, das Thema “Double-Take Availability für Windows” auf seiner Homepage ein. Jeder Administrator, der schon einmal einen Komplettausfall eines wichtigen Servers im Betrieb miterlebt hat, weiß, wie viel Wahrheit in diesen Worten steckt. Dass sich nicht jede Serverinstallation mit einer kostenintensiven Cluster-Sicherung vor Ausfällen schützen lässt, das ist ebenfalls eine anerkannte und verbreitete Weisheit. Clustering ist nicht nur teuer, die Technologie erfordert auch ein deutlich größeres Know-how der Administratoren. Auf der Suche nach einem Mehr an Sicherheit, ohne große IT-Infrastruktur-Kosten und hohe Anforderungen an das Wissen, schweben Administratoren Backup-Lösungen vor, die bei einem Server-Ausfall innerhalb kürzerer Zeit einen Weiterbetrieb der IT-Services erlauben. In diese Richtung geht Double-Take Availability, das wir im folgenden Test auf Herz und Nieren geprüft haben.

Availability von Double-Take (ADT) bietet eine quasi Hochverfügbarkeit mit Disaster Recovery in kurzer Zeit – nicht ganz in Echtzeit. Anstelle jedoch Stunden für die Wiederherstellung eines Backups auf einem Ersatzsystem einplanen zu müssen, erlaubt Double Take den Weiterbetrieb in wenigen Minuten. Die Lösung für Windows bietet einen weitreichenden Schutz für Applikationen, Daten und ganze Serverinstallationen.

Ob es sich bei den Quellsystemen um traditionelle, physische Server unter Windows oder um virtuelle Windows-Maschinen handelt, ist beim Einsatz von ADT unerheblich. Die vorhandene Hardware-, Software- und Netzwerk-Infrastruktur kann durch den Administrator für das Sicherungskonzept genutzt werden und ganze Server bei Bedarf aus Stand-By-VMs unter VMware ESX oder Microsoft Hyper-V aktiviert werden.

ADT unterstützt insbesondere Microsoft Exchange, Microsoft SQL Server, Oracle, Microsoft SharePoint und andere Applikationen. Die Integration von Microsoft Volume Shadow Copy Service (VSS) erlaubt die Erstellung und das Recovery von Kopien von bis zu 64 verschiedenen Zeitpunkten auf ein physisches oder virtuelles Ziel-System.

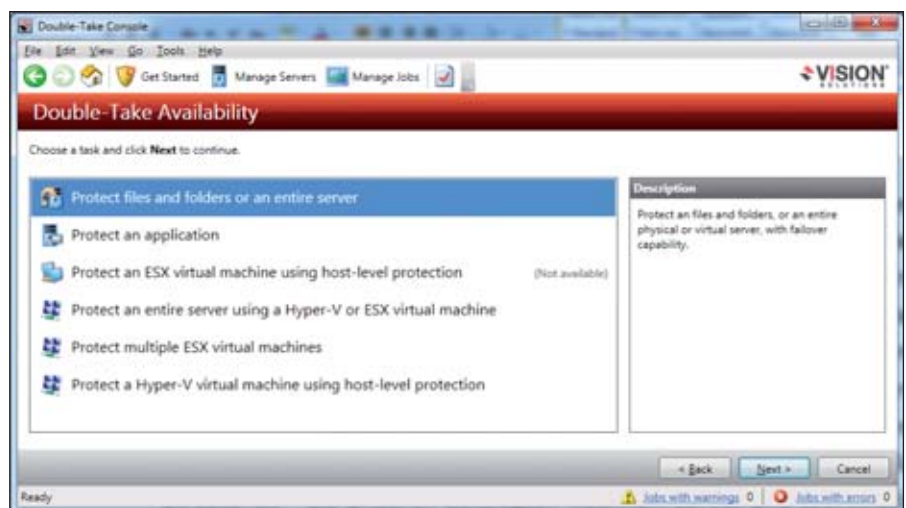


Bild 1: Double-Take Availability ermöglicht die automatische Sicherung ganzer Server oder einzelner Dateien in beliebigen Konstellationen

Anforderungen an die Umgebung

Auf jedem System, ob es sich nun um ein Quell- oder Zielsystem handelt, muss die Double-Take-Software installiert werden. Ohne diese Software können die Funktionen von Double-Take nicht genutzt werden. Die Mindestanforderung an die Betriebssystemumgebung hängt ganz von den genutzten Funktionen ab. Auf den Serversystemen muss ein Windows Server 2003 oder höher in der Standard-, Enterprise oder Datacenter-Edition installiert sein. Double-Take unterstützt sowohl die 32-Bit als auch die 64-Bit Edition von Windows. Die Client-Komponente –

hierbei handelt es sich nicht um den Agent für den Server, sondern um die Management-Oberflächen für Double-Take – kann der Administrator auf Windows XP oder höher installieren.

Soll die Funktionalität der kontinuierlichen Sicherung von Servern in eine Microsoft Hyper-V-Umgebung eingesetzt werden, so ist auf dem Server mindestens das .NET Framework 3.5 mit Service Pack 1 und Windows Server 2008 Standard, Enterprise oder Datacenter in der 64 Bit-Ausprägung erforderlich. Für die zu sichernden Maschinen gilt ebenfalls die Anforderung des .NET 3.5 mit Ser-

vice Pack 1, jedoch kann es sich dabei auch um Windows Server 2003 in der x86-Variante handeln. Die virtuellen Maschinen müssen auf einem Laufwerk mit Standard-NTFS-Dateisystem gespeichert werden. Die TCP/IP-Adressen der gesicherten Server müssen entweder statisch vergeben werden oder durch einen reservierten DHCP-Bereich zugewiesen werden. Welche Ports Double-Take für die Interaktion der Server- und Client-Software verwendet, kann der Administrator bei Bedarf den eigenen Vorstellungen nach anpassen. Die Standard-Ports schaltet der Installer auf Wunsch des Benutzers automatisch auf der Windows-Firewall frei. Kommen andere Firewall-Lösungen zum Einsatz, so müssen die Änderungen manuell vorgenommen werden.

Neben Hyper-V unterstützt ADT auch die laufende Sicherung in eine VMware-Hypervisor-Landschaft mit ESX. Die Systemanforderungen belaufen sich bei VMware auf ein Virtual Center in der Version 2 und höher, VMware ESX-Server 3.x oder höher und mindestens 130 MByte freien Festplattenspeicher für die Programme selbst. VMware ESXi wird derzeit noch nicht unterstützt.

Funktionsweise im Detail

ADT kombiniert eine kontinuierliche Replikation mit der Fähigkeit zum automatischen Failover für Disaster Recovery, Hochverfügbarkeit und zentrales Backup auf physischen und virtuellen Windows-Servern. Double-Take Availability setzt dabei auf ein durch ein Patent geschütztes Replikations- und Failover-Verfahren. Änderungen am Datenbestand registriert die Software auf Byte-Ebene und übermittelt nur diese Änderung unmittelbar an den Backup-Server. Der Hersteller hebt besonders hervor, dass sich diese Technik auch über schmalbandige WAN-Verbindungen problemlos einsetzen lässt.

Die Software fängt durch systemnahe Treiber Schreibzugriffe auf der Dateisystem-Ebene des Hosts ab. Alle Programme, auch virtuelle Maschinen, die auf virtuelle Disks schreiben, arbeiten oberhalb dieser Ebene. Somit kann die Software alle Änderungen mit dem Byte-Level-Mechanismus auf einen Ziel-Server replizieren, auf dem eine

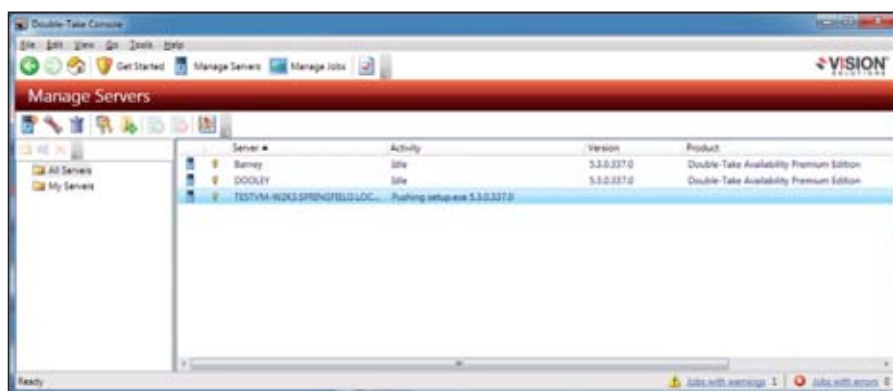


Bild 2: Dank der Push-Funktionalität ist die Ferninstallation von Double-Take Availability sehr einfach

andere Installation von ADT läuft. Diese wendet dann auf dem Ziel-Server dieselben Schreiboperationen an, die zuvor auf dem Quell-System registriert wurden. Es werden nur die tatsächlich geänderten Bytes übertragen. Wie viele Bytes dies sind, hängt von der Art der Serversoftware ab.

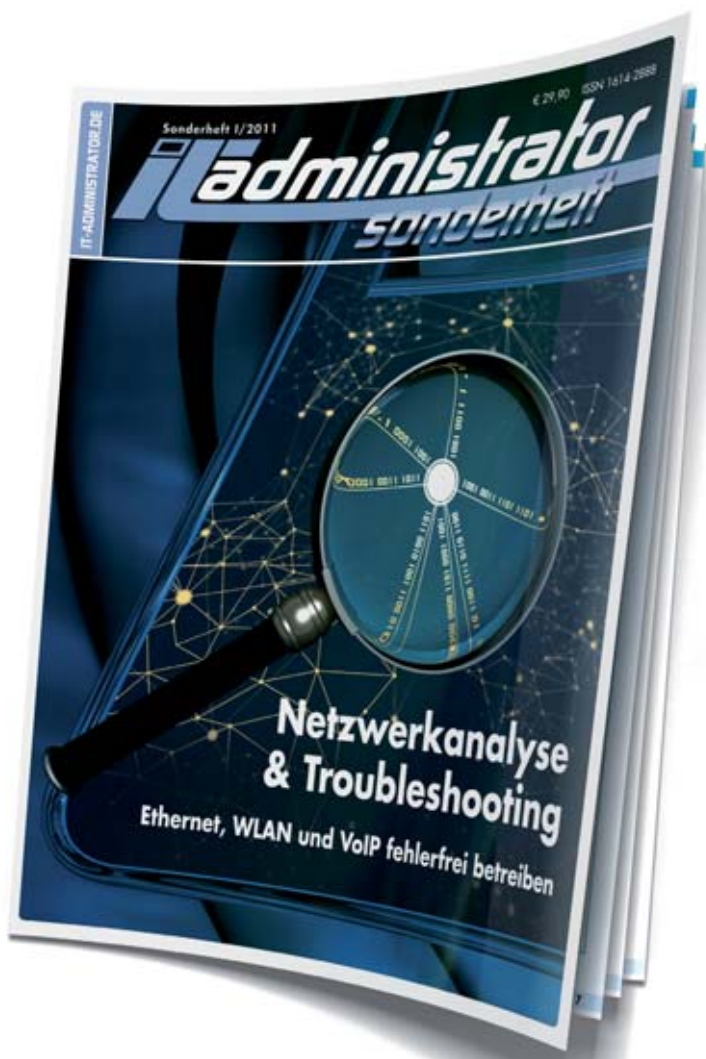
Double-Take bietet durch diese Architektur den Aufbau von komplexen Szenarien. Eine Replikation muss sich nicht immer auf eine 1-zu-1-Abbildung zwischen Quell- und Ziel-Server beschränken. Der Administrator ist mit der Software in der Lage, beliebige Konstellationen mit mehreren Quell- und Zielsystemen zu bilden. Beispielsweise können mehrere physikalische Server in virtuelle Maschinen gesichert oder ganze Hyper-V-Installationen mit aktiven virtuellen Maschinen auf andere physikalische Maschinen übertragen werden.

Einfache Installation und nicht ganz intuitive Nutzung

Die Installation von ADT ist einfach. Der Hersteller stellte uns eine Testvariante der Version 5.3 per Download zur Verfügung. Das Installationspaket mit dem "x64" im Dateinamen eignet sich auch für die x86-Umgebung. Die Installation beginnt auf einer Windows 7 x64-Workstation, von der die Server aus verwaltet werden sollen. Von der Workstation aus wird die Software auf drei Server im Push-Verfahren verteilt: einem physikalischen Windows Server 2003, einer virtuellen Windows Server 2003-Installation unter VMware Workstation und der physikalischen Windows Server 2008 R2 x64-Maschine, die über den Hyper-V-Service verfügt und als Notfallziel verwendet wird.

Die beiden Windows Server 2003-Installationen sind Teil eines Active Directory – die anderen beteiligten Rechner, Server und Workstation sind außerhalb der Domäne. Probleme im Zusammenhang mit dem Domänenzugriff stellten wir dabei nicht fest. Lediglich die Eingabe der Zugriffsinformationen ist bei Double-Take seltsam – das Feld "Domain" verbirgt sich unter "More Options". So wie sich die Eingabemaske präsentiert, geht der Benutzer davon aus, dass die Eingabe des Benutzernamens im Format "Domäne\Benutzername" durchzuführen ist – falsch gedacht. Insgesamt richtet der Installer sechs unterschiedliche Konsolen im Start-Menü von Windows ein – es dauerte einige Zeit, bis wir feststellten, dass die "Double-Take Console" den gezielten Zugriff auf alle "Unterkonsolen" erlaubt. Zwar ist die Konsole modern und an sich aufgeräumt – doch bis zur intuitiven Nutzung vergeht einige Zeit.

Das Menü "Availability" der Double-Take Console besteht in der Summe aus sechs Menüpunkten. Neben dem Schutz ganzer Server durch Verwendung der Stand-By-VMs unter Hyper-V und ESX findet der Administrator hier die Assistenten für die Einrichtung von "Protect files and folders or an entire server", "Protect an application", "Protect an ESX virtual machine using host-level protect", "Protect multiple ESX virtual machines" und "Protect a Hyper-V virtual machine using host-level protection". Kurzum: In jede erdenkliche Richtung bietet die Software eine Lösung. Im Test beschränkten wir uns in erster Linie auf die Funktion der Sicherung von Servern mit Failover in eine Microsoft Hyper-V-VM.



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

180 Seiten Praxis-Know-how rund um das Thema

Netzwerkanalyse & Troubleshooting

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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



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

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

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

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

Ich zahle ☐ per Bankeinzug

Firma: _____

Geldinstitut: _____

Name, Vorname: _____

Kto.: _____

BLZ: _____

Straße: _____

oder ☐ per Rechnung

Land, PLZ, Ort: _____

Datum: _____

Tel: _____

Unterschrift: _____

E-Mail: _____

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

leserservice@it-administrator.de

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



Heinemann Verlag

Leopoldstraße 85

D-80802 München

Tel: 089-4445408-0

Fax: 089-4445408-99

Geschäftsführung:

Anne Kathrin Heinemann

Matthias Heinemann

Arbeitsgericht München HRB 151585

ITA 07/11

Anstoßen der ersten Replikation

Die Installation und die Einrichtung der Jobs zur Sicherung auf dem Hyper-V-Server dauerte lediglich einige Minuten. Zunächst stolperten wir im Test darüber, dass sich der Hyper-V-Server mit Namen "Dooley" nicht auswählen ließ, obwohl die Double-Take-Software installiert war. In dem Auswahlfenster für "Target" muss der Name des Servers schlicht eingegeben werden. Warum ausgerechnet die Hyper-V-Maschine in der Auflistung fehlte, konnten wir nicht feststellen. Bei der Einrichtung eines zweiten Jobs war der Eintrag jedenfalls vorhanden.

Welche Laufwerke gesichert werden sollen, welche Netzwerkkarte auf dem Hyper-V-Server im Fehlerfall für die Anbindung der VM ins Netzwerk genutzt werden soll und welche Parameter für die Netzwerkumgebung zum Einsatz kommen – Gateway, DNS oder IP-Adressen –, richtet der Administrator mit wenigen Mausklicks ein. Außerdem lässt sich in diesem Dialog die Bandbreite für die Replikation festlegen. Dadurch wird verhindert, dass während der Dauer der Replikation andere Systeme zu wenig Bandbreite erhalten und damit ausgebremst werden. Ebenfalls Einstellungssache des Administrators: Soll der Failover automatisch durchgeführt werden, sobald die Quell-Maschine über das Netzwerk nicht erreichbar ist, oder möchte der IT-Profi in diesem Fall von Hand umstellen – was einen Mausklick auf "Failover" im Kontextmenü der Software bedeutet?

Die erste Replikation des Datenstands dauerte einige Minuten bis Stunden – je nachdem, wie groß das Datenvolumen ist, wie die Netzwerkbandbreite eingestellt ist und mit welcher Netzwerkanbindung gearbeitet wird. In der Testumgebung verwendeten wir unterschiedliche Netzwerkgeschwindigkeiten von 10 MBit Half-Duplex bis 1 GBit Full-Duplex. Zwar änderte sich das Tempo, aber die Software arbeitete stets ohne erkennbare Probleme weiter. Nach der Einrichtung des Jobs bleibt dem Administrator zunächst nichts anderes übrig als warten. Ein Blick in den Hyper-V-Manager zeigte, dass Double-Take die virtuellen Maschinen gemäß den Wünschen des Administrators angelegt hat. Typischerweise

werden diese im Jargon des Herstellers als "Replica" bezeichnet – eine insgesamt sinnvolle Bezeichnung. Da sich die VMs auch von Hand starten lassen würden, ist der Hinweis "Replica" für Mit-Administratoren als Warnung zu verstehen, dass diese Maschinen unter keinen Umständen im Regelbetrieb aktiviert werden dürfen.

Der Status der aktuellen Verbindung ist jederzeit unter "Manage Jobs" zu sehen. Bis die erste Synchronisierung abgeschlossen ist, wird der Status durch ein gelbes Ausrufezeichen mit "Warning" markiert. Die Übermittlung der Dateien geht mit einer deutlichen Systemlast auf den Quellservern einher – eine maximale Auslastung von bis zu 100 Prozent im Task-Manager wurde in der Teststellung beobachtet. Nach Abschluss der Erstübertragung sinkt die Auslastung auf die für den Server üblichen Werte.

Nach dem Anlegen des "Spiegels" auf eine zweite Rechnerkopie werden alle Änderungen auf Bytelevel-Ebene repliziert. Gleichzeitig ist ein Überwachungsmodus aktiviert. Zur Replikation klinkt sich das Werkzeug in die IO-Prozesse des Betriebssystems ein. Aufgrund dieser Unabhängigkeit

von Applikationen können somit jegliche Inhalte in der virtuellen Maschine repliziert werden. Gleichzeitig ist dies aber auch die logische Einschränkung des Verfahrens: Daten, die sich noch nicht in einer Datei befinden, also im Arbeitsspeicher der Maschine gehalten werden, sind solange nicht Teil der Replikation, bis sie gespeichert wurden. Für die gängigen Microsoft-Produkte – Microsoft SQL-Server und Microsoft Exchange – bietet Double-Take aus diesem Grunde eine spezielle Variante der Software, die sich direkt in die Applikation einklinkt.

Problemloses Failover, Failback mit Handarbeit

Es kam der spannende Moment im Test: wir deaktivierten die virtuelle Maschine unter VMware. Rund zehn Sekunden später stellte Double-Take den Missstand in der Console fest und startete automatisch die "Replica" unter Hyper-V. In der Summe drei Minuten später war das Ersatzsystem online. Bis zum Abschluss der für Hyper-V spezifischen Treiberinstallation verlangte die Hyper-V-Ersatzmaschine einen Neustart. Der auf dem Testserver installierte Microsoft SQL-Server 2005 war jedoch bereits wieder über ODBC von außen erreichbar.

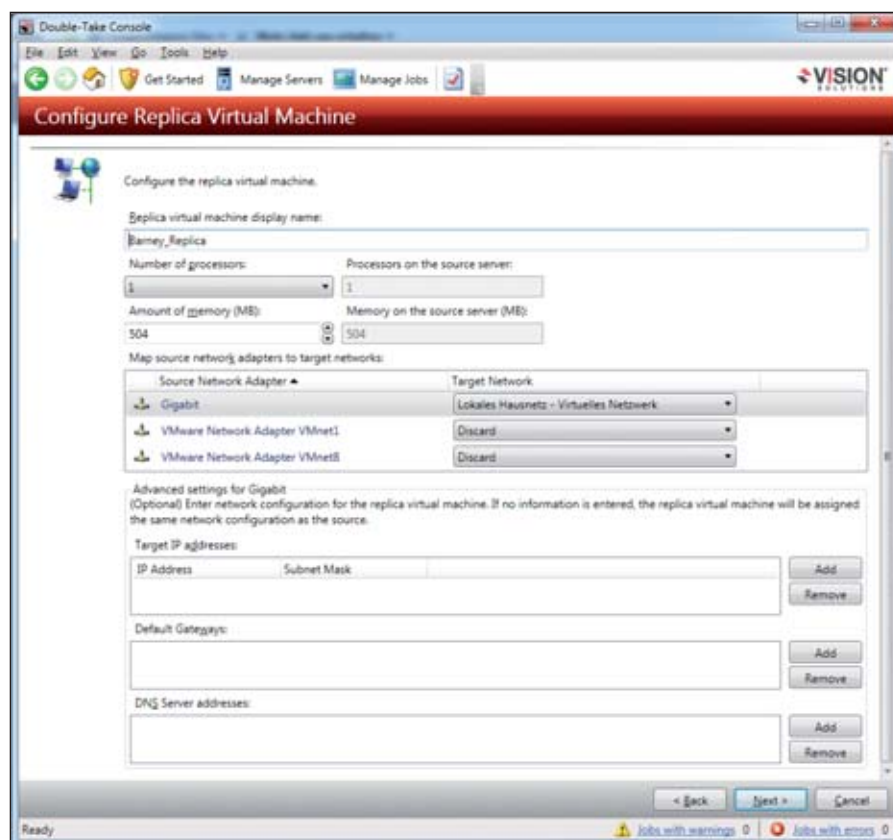


Bild 3: Double-Take Availability nennt die Stand-By-Sicherung auf ESX/Hyper-V "Replica" – welche virtuellen Hardware-Eigenschaften die Systeme haben sollen, stellt der Administrator über die grafische Oberfläche ein

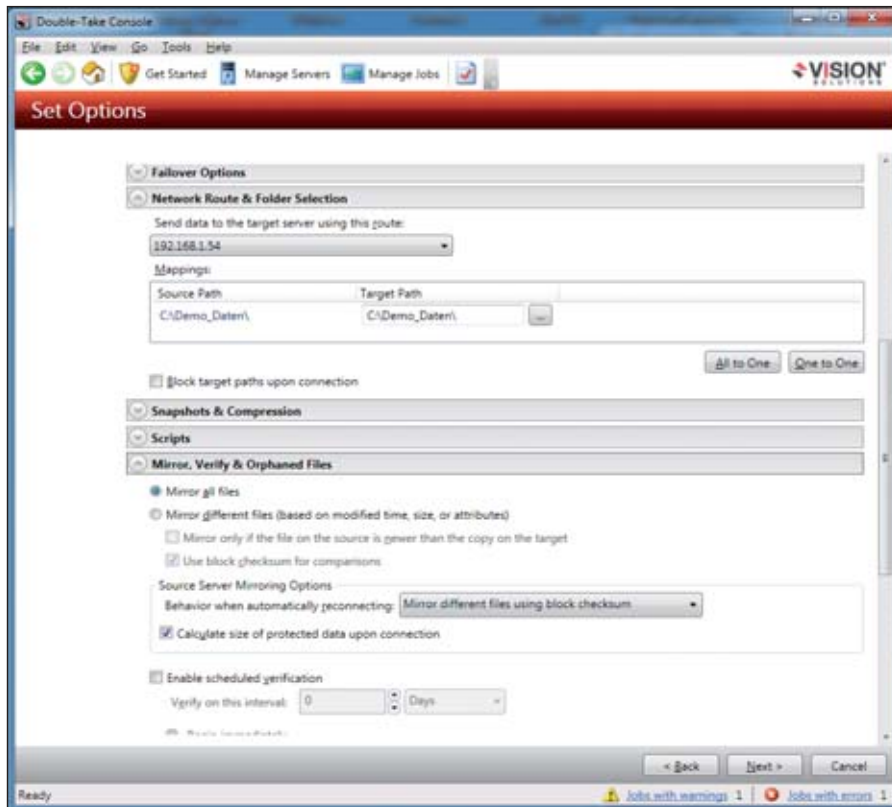


Bild 4: Neben der Sicherung in virtuelle Maschinen kann Double-Take Availability beliebige Daten über Byte-Level-Replikation spiegeln

und einen Datenverlust konnten wir im Test nicht feststellen. Somit war der wichtigste Teil der Prüfung erfolgreich abgeschlossen: Auch ohne ein Clusterbetriebssystem vorzuhalten, ist eine zügige Ausfallsicherheit mit Hyper-V möglich.

Während der Weg hin zu einem virtuellen Ausfallsystem recht einfach zu erreichen ist, stellt die Wiederherstellung in der ursprünglichen Form eine etwas größere Herausforderung dar. Während der Vorbereitung zur Wiederherstellung arbeiten alle Benutzer weiter auf der Hyper-V-VM, somit hat der Administrator ausreichend Zeit und somit die nötige Ruhe, die erforderlichen Schritte vorzubereiten. Der Failover findet gewöhnlich in einem Notfall statt – die ursprüngliche Maschine lässt sich entweder wieder einsatzbereit machen oder sie ist defekt. Unabhängig davon, ob es sich um denselben Ursprungsserver handelt oder um ein komplett neues Austauschgerät, der Weg zurück geht über Double-Take Availability "Protect an entire server".

Handelt es sich um das Ursprungssystem, so ist eine Rückübertragung unter Verwendung der Option "Checksum mode" mög-

lich. Hierbei werden nur die tatsächlich veränderten Daten übermittelt, was die Übertragungsdauer stark verkürzt. Ist es ein anderes System, so müssen alle Informationen der virtuellen Festplatte auf das neue Zielsystem übermittelt werden und dauert entsprechend länger. Das neue Zielsystem muss sich außerhalb einer Domäne befinden und möglicherweise muss eine kleine Datei im Verzeichnis von "Double Take" manuell gelöscht werden. Da die IP-Adresse bei dem Wechsel nicht übernommen wird, muss für den abschließenden "Full-Server Failover" im DNS möglicherweise ebenfalls eine manuelle Anpassung vorgenommen werden.

Fazit

Double-Take Availability ist eine spannende Software mit vielen Einsatzmöglichkeiten. Besonders Unternehmen, die die Kosten einer Cluster-Lösung scheuen, aber gleichzeitig das lange Wiederherstellungsfenster aus dem Backup umgehen wollen, haben mit dieser Software eine Alternative. Die Integration von Hyper-V als Ziel für die Sicherung ist angesichts der Lizenzpreispolitik von Microsoft nur verständlich. Im Regelfall dürfte der Ad-

ministrator einen leistungsfähigen Windows Server 2008 aufbauen und die für das Unternehmen benötigten Server auf diesem virtualisiert betreiben. Was liegt also näher, als die anderen, physikalischen Windows-Server am Standort in Form von virtuellen Maschinen auf diesen Server mit zu sichern. Kommt es zu einem Ausfall des eigentlichen Servers, so springt die virtuelle Maschine ein. Dass in dieser Zeit die gesamte Einrichtung etwas langsamer als gewohnt läuft und das Umspringen auf das Ersatzsystem einige Minuten dauert, ist in vielen Fällen besser, als mit dem manuellen Aufbau von Ersatzmaschinen zu beginnen. (jp)



Produkt

Software für Hochverfügbarkeit und Disaster Recovery unter Windows-Systemen.

Hersteller

Double-Take / Vision Solutions
www.double-take.com

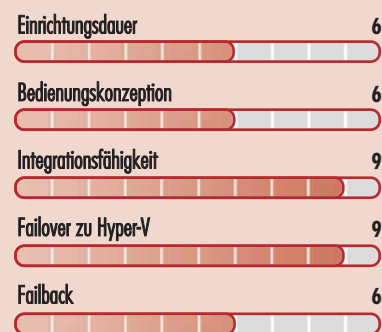
Preis

Die Lizenzierung erfolgt abhängig vom Hyper-V-Host: Für die Standard-Version kostet Double-Take Availability 1.795 Euro, für die Enterprise-Version 2.495 Euro inklusive einem Jahr Support.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)



Dieses Produkt eignet sich

optimal für Unternehmen, die eine Failover-Fähigkeit im Windows-Umfeld benötigen und über Hyper-V/ESX-Hypervisoren verfügen.

bedingt für Unternehmen, die über wenig Know-how im Bereich Windows verfügen.

nicht für Unternehmen, in denen eine reine Clusterfähigkeit ohne Zeitausfall benötigt wird.

Double-Take Availability 5.3



Microsoft Hyper-V Failovercluster einrichten

Virtueller Zwilling

von Marc Grote

Nachdem sich immer mehr Firmen mit dem professionellen Einsatz von Hyper-V beschäftigt haben, stieg auch der Bedarf nach Hochverfügbarkeit der Hyper-V-Rolle und den darin betriebenen virtuellen Gastsystemen. Die neue Live Migration in Windows Server 2008 R2 erlaubt hierfür das manuelle oder automatische Verschieben von virtuellen Maschinen ohne Ausfallzeit auf einen anderen Cluster-Knoten.

Sie verwendet hierfür eine neue Failovercluster-Funktion, das "Cluster Shared Volume" (CSV).

Wie Sie ein solches Cluster einrichten, zeigt Ihnen dieser Workshop.

Dem steigenden Bedarf an Hochverfügbarkeit hat Microsoft zunächst mit einer Funktion namens Quick-Migration Rechnung getragen. In Verbindung mit den Failovercluster, Funktionalitäten von Windows Server 2008 Enterprise und Datacenter, wird der Betrieb der Hyper-V Rolle in einem Cluster unterstützt und mit Hilfe der Quick-Migration für Hochverfügbarkeit gesorgt. Dank dieser Quick-Migration-Funktion lässt sich auch Hyper-V hochverfügbar betreiben. Sollte einer der Cluster-Knoten ausfallen, werden die virtuellen Maschinen, die im SAN (Storage Area Network) gespeichert sind, auf einen anderen verbliebenen Cluster-Knoten verschoben.

Doch bei der Quick-Migration kam es aufgrund der Architektur der Funktion immer zu kurzen Ausfallzeiten, bis die virtuelle Maschine auf dem anderen Cluster-Knoten vollständig bereitgestellt war. Denn durch die Natur eines Failoverclusters sorgt diese Funktion nur für eine automatische Bereitstellung der virtuellen Maschinen auf einem anderen Cluster-Knoten bei einem Ausfall. Eine intelligente Funktion zur Platzierung von virtuellen Maschinen auf unterschiedlichen Cluster-Knoten basierend auf Parametern wie CPU-Last, Speicherauslastung und weiteren Parametern war nicht möglich.

Um diesen und weiteren Anforderungen Rechnung zu tragen, stellt Microsoft ein Produkt mit dem Namen SCVMM

(System Center Virtual Machine Manager) [3] zur Verfügung, das eine zentrale Verwaltungskonsole für alle Hyper-V-Server und viele weitere Funktionen beinhaltet. Eine der Funktionen von SCVMM ist das "PRO Feature" [4]. Es ermöglicht in Verbindung mit dem System Center Operations Manager 2007, virtuelle Maschinen, die durch Hyper-V bereitgestellt werden, intelligent auf andere Hyper-V Cluster-Knoten anhand von vielen Kriterien wie Auslastung der Server oder verfügbarer Arbeitsspeicher zu verschieben.

SCVMM und Quick Migration decken damit zwar die Bedürfnisse vieler Administratoren ab, doch Microsoft kam im Bereich der Hochverfügbarkeit noch immer nicht an die Qualität von VMware ESX Server heran. Aus diesem Grund wurde mit Windows Server 2008 R2 eine neue Hochverfügbarkeitsoption für die Cluster-Funktionalität – speziell für die Hyper-V-Rolle – namens "Hyper-V Live Migration" [5] eingeführt.

Die Live Migration erlaubt das manuelle oder automatische Verschieben von virtuellen Maschinen ohne Ausfallzeit auf einen anderen Cluster-Knoten. Sie verwendet hierfür eine neue Failovercluster-Funktion, das "Cluster Shared Volume" (CSV). Dabei handelt es sich um eine Speichertechnik, bei der Cluster-Knoten gleichzeitig auf Shared Storage, in dem die virtuellen Maschinen gespeichert sind, über iSCSI oder Fibre Channel zugreifen.

Failovercluster einrichten

Der erste Schritt zur Einrichtung der Live Migration Funktion für Hyper-V ist die Installation der Hyper-V-Rolle von Windows Server 2008 R2 mit Hilfe des Servermanagers, dem Tool "Server-ManagerCMD" beziehungsweise der Windows PowerShell auf jedem Clusterknoten. Danach können Sie die Installation mit der Einrichtung der Windows-Funktion "Failoverclustering" fortsetzen. Die komplette Einrichtung eines Failoverclusters würde den Rahmen dieses Artikels überschreiten, da viele Bedingungen erfüllt sein müssen, damit eine erfolgreiche Inbetriebnahme des Cluster

Microsoft begann mit Windows Server 2008 und Hyper-V in den Markt der Enterprise-Virtualisierungslösungen einzusteigen und hat sich vom bisherigen Virtualisierungsprodukt Microsoft Virtual Server 2005 verabschiedet. Die als Version 1.0 bekannte Virtualisierungssoftware stand als Serverrolle in Windows Server 2008 zur Verfügung. Windows Server 2008 R2 nutzt dagegen Hyper-V in der Version 2.0, das auch als eigenständiges, kostenloses Produkt verfügbar ist [1].

Hyper-V ist in allen Windows Server 2008 R2-Versionen verfügbar [2] – ausgenommen Itanium, Web und Foundation Edition. Je nach Geschmacksrichtung können Administratoren Hyper-V in der GUI (Graphical User Interface) Version von Windows Server 2008 R2 oder in der Server Core-Version, einer optimierten Version von Windows Server 2008 R2 ohne grafische Benutzeroberfläche, betreiben. Microsoft empfiehlt die Installation eines Hyper-V-Servers auf einem Windows Server 2008 R2 Core, weil diese Version unter anderem auf Performance und Sicherheit optimiert wurde und somit einem Baremetal Hypervisor recht nah kommt.

Die Entwicklung von Hyper-V



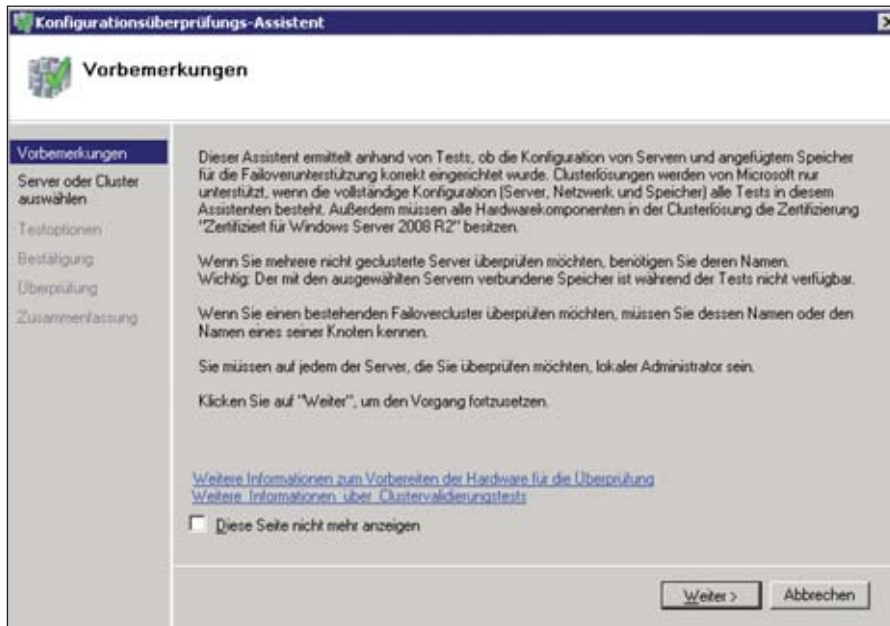


Bild 1: Microsoft unterstützt nur Cluster-Lösungen, die den Konfigurations-Test erfolgreich bestanden haben

sichergestellt ist, weshalb wir nur auf die wichtigsten Schritte eingehen können.

Der erste Schritt ist immer der Planungsprozess der entsprechenden Hardware, Netzwerkkomponenten und des Storage für den Failovercluster. Als Minimalanforderung für einen Failovercluster mit Hyper-V sind zwei für das Clustering geeignete physikalische Server erforderlich, die jeweils mindestens drei Netzwerkkarten besitzen. Eine Netzwerkkarte wird für die LAN-Kommunikation, eine Netzwerkkarte für das Cluster-Heartbeat und eine Netzwerkkarte für die Live-Migration verwendet. Verwenden Sie für den Zugriff auf das SAN iSCSI anstatt Fibre Channel (FC), sollten Sie auch eine dedizierte Netzwerkkarte für den iSCSI-Zugriff nutzen. Eine dedizierte Netzwerkkarte für das Hyper-V-Management ist optional, jedoch empfehlenswert.

Als SAN-Lösung stehen eine Reihe von iSCSI und Fibre Channel basierten Produkten von diversen Speicheranbietern zur Verfügung. Hierbei sollte man auf die entsprechenden zertifizierten Produkte des Windows-Hardware-Katalogs und die allgemeinen Hyper-V-Installationsanforderungen [6] achten. Nachdem die Hardware nach den allgemeinen Anforderungen eingerichtet worden ist, kann zunächst Windows Server 2008 R2 Enterprise oder Datacenter und daraufhin die Hyper-V-

Rolle auf jedem Cluster Knoten sowie abschließend die Windows Server 2008 R2 Funktion des Failoverclustering installiert werden. Nach Installation und Konfiguration der Hyper-V Rolle, zu der auf alle Fälle die korrekte Konfiguration der virtuellen Hyper-V Netzwerke gehört, empfiehlt sich die Ausführung des Hyper-V Best Practice Analyzer (BPA), welcher die installierte Hyper-V Rolle gegen Best Practices von Microsoft prüft. Die Installation eines Failovercluster wird durch Starten des Failovercluster Konfigurationsüberprüfungsassistenten gestartet, welcher die Hardware, die Software und den Speicher (SAN) auf Cluster-Tauglichkeit überprüft.

Nur wenn das Ergebnis des Konfigurationsüberprüfungsassistenten einwandfrei ist, sollten Sie mit der Erstellung des Failovercluster fortfahren. Microsoft gibt nämlich nur Support für Cluster, die den Test erfolgreich bestanden haben. Doch auch

wenn nicht alle Tests erfolgreich waren, bedeutet das nicht, dass eine Failovercluster-Installation unmöglich ist. In Testszenarien können Sie einen Cluster sicherlich auch ohne Bestehen aller Tests betreiben. In einer Produktivumgebung hingegen beginnen Sie am besten erst mit der Installation nach erfolgreichem Abschluss aller Tests.

Nach dem Durchlauf der Validierungstests können Sie mit der Erstellung des Failovercluster beginnen. Sie haben dabei die Wahl, im Cluster-Assistenten alle Clusterknoten auf einmal auszuwählen oder nur mit einem Clusterknoten zu beginnen. Erfahrungsgemäß sollten Sie mit der Erstellung von nur einem Cluster-Knoten anfangen und erst, wenn dieser erfolgreich installiert wurde, weitere Knoten hinzufügen.

Nach dem Erstellen des Clusters sind noch ein paar weitere Schritte erforderlich, bevor Sie mit der eigentlichen Cluster-Einrichtung für das Cluster Shared Volume (CSV) und die Hyper-V-Funktion beginnen. Zu den essenziellen Aufgaben gehört dabei die korrekte Einrichtung der Cluster-Netzwerke, die Benennung der Cluster-Festplatten, die Festlegung eines zentralen Ablageorts für ISO-Dateien für virtuelle Maschinen und weitere Schritte. Für eine komplette Übersicht der weiteren Schritte, der Ein-

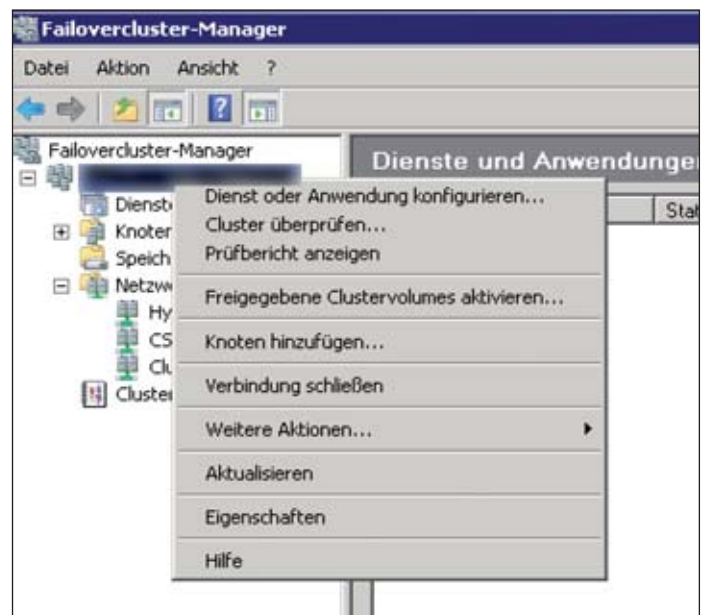


Bild 2: Mit einem Rechtsklick im Failovercluster-Manager gelangen Sie in das Kontextmenü zum Installieren des CSV

richtung der Hyper-V Rolle sowie der Live Migration verweisen wir auf den Artikel unter [7].

Nachdem nun die Failovercluster-Funktion korrekt installiert wurde, die entsprechenden Cluster-Knoten im Cluster integriert sind und erste simulierte Failovertests erfolgreich waren, kann mit der Installation des CSV begonnen werden. Die Installation des CSV ist unspektakulär und wird im Failovercluster-Manager durch einen Rechtsklick auf den erstellten Failovercluster gestartet.

Besonderer Aufmerksamkeit ist dann der folgenden Meldung zu widmen, die ausdrücklich darauf hinweist, dass es nicht erlaubt ist, das CSV wie ein normales Datenträgervolume zu nutzen. Ein Zugriff auf das CSV darf immer nur über die Hyper-V-Rollenverwaltung erfolgen. Nachdem Sie das Cluster Shared Volume erstellt haben, taucht in der Failovercluster-Verwaltung ein neuer Eintrag mit dem Namen "Freigegebene Clustervolumen" auf. Jetzt lässt sich die entsprechende LUN (Logical Unit) aus dem SAN hinzufügen. Manche Administratoren mag es verwirren, dass die CSV-LUN nicht als zusätzlicher Laufwerksbuchstabe im Windows Explorer auftaucht. Das CSV ist als zusätzliches Verzeichnis im System Volume (Laufwerk C:) zu finden.

Virtuelle Maschinen im Failovercluster installieren

Nachdem alle Voraussetzungen für einen funktionsfähigen Hyper-V Failovercluster geschaffen worden sind, kann mit der Erstellung einer virtuellen Maschine im Cluster begonnen werden. Das Importieren von vorhandenen virtuellen Maschinen in den Hyper-V Failovercluster ist ebenfalls möglich. Das Erstellen einer neuen virtuellen Maschine starten Sie im Failovercluster-Manager durch einen Rechtsklick auf "Dienste und Anwendungen / Virtueller Computer / Neuer virtueller Computer". Das Anlegen einer virtuellen Maschine im Cluster unterscheidet sich dabei nicht vom Erstellungsprozess ohne Failovercluster. Sie müssen lediglich darauf achten, dass der Speicherort für den virtuellen Computer das CSV ist, damit die virtuelle Maschine hochverfügbar gemacht werden kann. Nach erfolgreicher Erstellung der virtuellen Maschine erscheint diese in der Failovercluster-Verwaltung unterhalb von Dienste und Anwendungen und Sie können jetzt mit der weiteren Anpassung der VM beginnen.

Nach der Konfiguration der neuen virtuellen Maschine können Sie die Funktion der Live Migration testen. Um eine Live Migration einer virtuellen Maschine zu starten, klicken Sie in der Fail-

overcluster-Verwaltung mit der rechten Maustaste auf die virtuelle Maschine, die verschoben werden soll. Im Kontextmenü können Sie dann die Live Migration auf einen anderen Hyper-V Clusterknoten initiieren.

Die Live Migration der virtuellen Maschine erfolgt ohne Unterbrechung der Netzwerkkonnektivität. Setzen Sie während des Vorgangs der Live Migration ein Ping auf die virtuelle Maschine ab, so werden Sie feststellen, dass es keine Verbindungsprobleme in Form von Ping-Fehlern gibt. Wie das technisch realisiert wird, ist einer näheren Betrachtung wert. Der Ablauf einer Live Migration setzt sich aus folgenden Schritten zusammen:

1. Alle Memory Pages der virtuellen Maschine werden von einem Hyper-V-Host auf den anderen übertragen.
2. Änderungen in den Memory Pages in der virtuellen Maschine werden ebenfalls aufgezeichnet.
3. Veränderte Memory Pages in der virtuellen Maschine werden anschließend auf den Ziel Hyper-V-Host übertragen.
4. Hyper-V verschiebt die Storage Zuweisung der VHD-Dateien auf den Ziel Hyper-V-Host.
5. Die verschobene virtuelle Maschine wird auf dem Ziel Hyper-V-Host gestartet.

Integration in Microsoft SCVMM

Mit Hilfe der Hyper-V-Verwaltungskonsolle und dem Failovercluster Manager lassen sich die meisten Aufgaben der Cluster- und Hyper-V-Verwaltung durchführen. Für kleinere Umgebungen sind diese Verwaltungstools auch ausreichend, doch in größeren Virtualisierungsumgebungen kommen Administratoren schnell an die Grenze der Möglichkeiten. Aus diesem Grund stellt Microsoft seit Jahren ein Produkt zur Verwaltung von Hyper-V-Umgebungen mit dem Namen "Microsoft System Center Virtual Machine Manager" zur Verfügung, das zurzeit in der aktuellen Version SCVMM 2008 R2 vorliegt. Die Version 2012 des SCVMM ist noch für das erste Halbjahr 2011 zu erwarten und zu Redaktionsschluss dieser Ausgabe als Betaversion verfügbar. Mit Hilfe des SCVMM steht eine zentrale Verwaltungskonsolle für alle Hyper-V Hostsysteme und deren virtuellen Maschinen (VM) zur

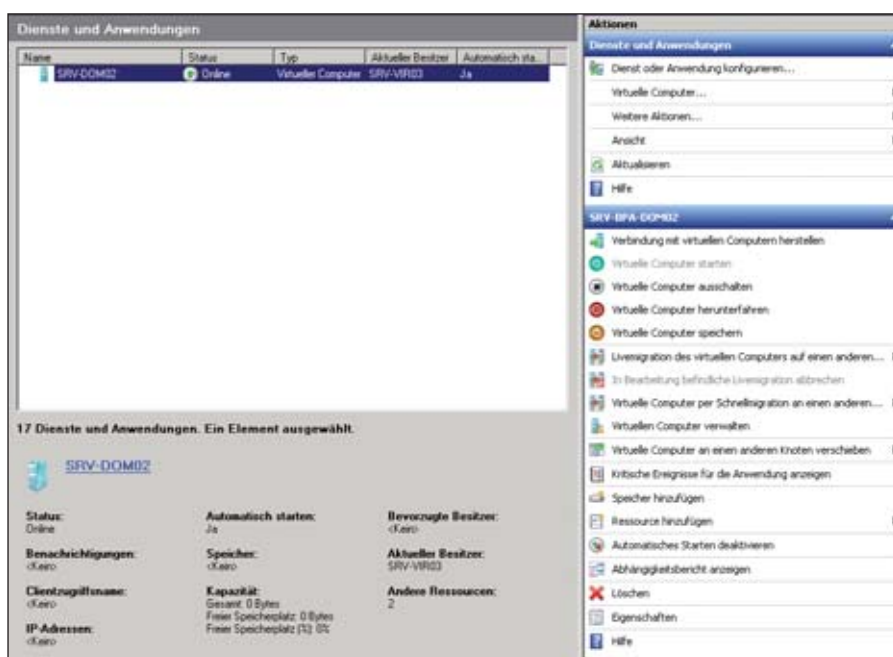


Bild 3: Taucht die virtuelle Maschine in der Failovercluster-Verwaltung auf, wurde sie erfolgreich angelegt

Automatisierte SAP-Systemkopien auf Knopfdruck

SAP® Certified
Integration with SAP NetWeaver®

Libelle SystemCopy

PRE COPY

- ✓ Ohne in Ihre SAP-Umgebung einzugreifen bzw. diese zu verändern
- ✓ Ohne aufwändige Vorplanung
- ✓ Mit minimaler Durchlaufzeit
- ✓ Bei gleichbleibender Qualität der Kopie

... mit deutlich reduzierten Prozesskosten

Hans-Joachim Krüger
Chief Technology Officer
Libelle AG

Erfahren Sie mehr:
www.libelle.com/systemcopy



Libelle

Libelle AG
Gewerbestr. 42 • 70565 Stuttgart, Germany
T +49 711 / 78335-0 • F +49 711 / 78335-149
www.libelle.com • sales@libelle.com

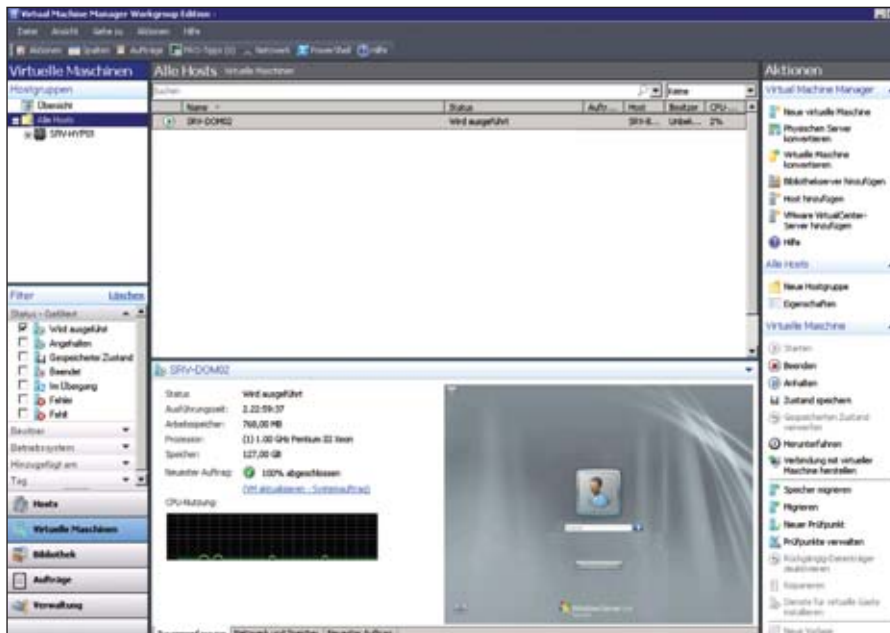


Bild 4: Dank der PRO-Funktion lassen sich VMs anhand von Kriterien wie etwa der RAM-Auslastung verschieben

Verfügung. SCVMM ist sogar in der Lage, Microsoft Virtual Server 2005 Hosts sowie VMware VMCenter Maschinen zentral zu verwalten.

Zahlreiche Funktionen wie Assistenten zur Migration physikalischer Maschinen zu virtuellen Maschinen, P2V genannt, ein Self Service Portal für Benutzer zur eigenen Verwaltung und Erstellung virtueller Maschinen und eine zentrale Library für ISO-Dateien sowie Vorlagen für virtuelle Maschinen runden das SCVMM-Portfolio ab, sind aber nur einige Funktionen des System Center Virtual Machine Manager. Mit der anfangs im Artikel erwähnten PRO-Funktion in Ver-

bindung mit System Center Operations Manager stellt SCVMM auch intelligente Optionen zur manuellen oder automatischen Verschiebung von virtuellen Maschinen zwischen Hyper-V-Hosts anhand der RAM-Auslastung und weiteren Parametern zur Verfügung.

Fazit

Mit Hilfe von Hyper-V 2.0, der Fail-overcluster-Funktionalitäten von Windows Server 2008 R2 und des Cluster Shared Volume stellt Microsoft eine robuste Virtualisierung für Unternehmen zur Verfügung, die durch den System Center Virtual Machine Manager 2008 R2 optimal ergänzt und erweitert wird.

Das auf der TechEd 2010 in Berlin gezeigte Nachfolgeprodukt SCVMM 2012 lässt übrigens klar erkennen, welches Potenzial in der derzeit zur Verfügung stehenden Virtualisierungslösung steckt: Die Zeichen zeigen klar in Richtung Private Cloud, die sich mit Hyper-V und SCVMM 2012 optimal realisieren lassen dürfte. Die bereits zum Zeitpunkt der Erstellung dieses Artikels zur Verfügung stehenden Ressourcen mit dem Namen Hyper-V Cloud Fast Track stellen Unternehmen jetzt schon die Möglichkeit zur Verfügung, sich mit privatem Cloud Computing zu beschäftigen. (dr) 

Marc Grote ist MVP für Forefront.

- [1] Microsoft-Seite zu Hyper-V Server 2008 R2 B7P21
- [2] Windows Server 2008 R2-Versionen B7P22
- [3] Microsoft-Seite zu SCVMM B7P23
- [4] PRO-Feature von SCVMM B7P24
- [5] Die Hyper-V Live Migration B7P25
- [6] Hyper-V Installationsanforderungen B7P26
- [7] Hyper-V Live Migration Step-by-Step Einrichtung B7P27 und B7P28

Link-Codes



Link-Codes eingeben auf www.it-administrator.de

Hochverfügbare Xen-Umgebungen mit Remus

Nahtloser Übergang

von Thomas Drilling

Hochverfügbarkeits-Infrastrukturen funktionieren auch mit virtuellen Maschinen – doch nicht nur das: Vielmehr bietet Virtualisierung als Technologie an sich die Chance, Hochverfügbarkeitssysteme ohne spezielle Hardware oder angepasste Betriebssysteme beziehungsweise Anwendungslogik zu realisieren. Basierend auf einer freien Virtualisierungslösung wie Xen sind leistungsfähige Hochverfügbarkeitscluster mit freier Software möglich, die klassischen Open Source-Lösungen wie dem Linux-HA-Projekt sogar überlegen sind. Wir stellen die kostenlose HA-Erweiterung Remus für Xen vor und zeigen in diesem Beitrag auf, welche Hochverfügbarkeitsfeatures das Werkzeug mit sich bringt und wie Sie Remus in Betrieb nehmen.

Was Hochverfügbarkeits-Lösungen mit freier Software angeht, orientieren sich die meisten Setups am Linux HA-Projekt [1], das als Cluster Resource Manager auf Heartbeat setzt. Heute kommt für das Verwalten von Ressourcen in mit Linux betriebenen Hochverfügbarkeits-Clustern allerdings oft der Heartbeat Fork “Pacemaker” [2] zum Einsatz. Pacemaker unterstützt unter anderem auch mehr als zwei Nodes pro Cluster und als Cluster-Stack (Kommunikation der Knoten untereinander) kommt bei Pacemaker wahlweise Heartbeat oder OpenAIS – eine freie Implementierung des AIS-Protokolls – zum Einsatz. Pacemaker verwaltet darüber hinaus den Betrieb von Server-Diensten auf einem Rechnercluster und überwacht Server und Dienstprogramme. Pacemaker war früher ebenfalls Teil des Linux-HA-Projektes und ist im Prinzip ein im Jahr 2008 neugeschriebener Nachfolger von Heartbeat.

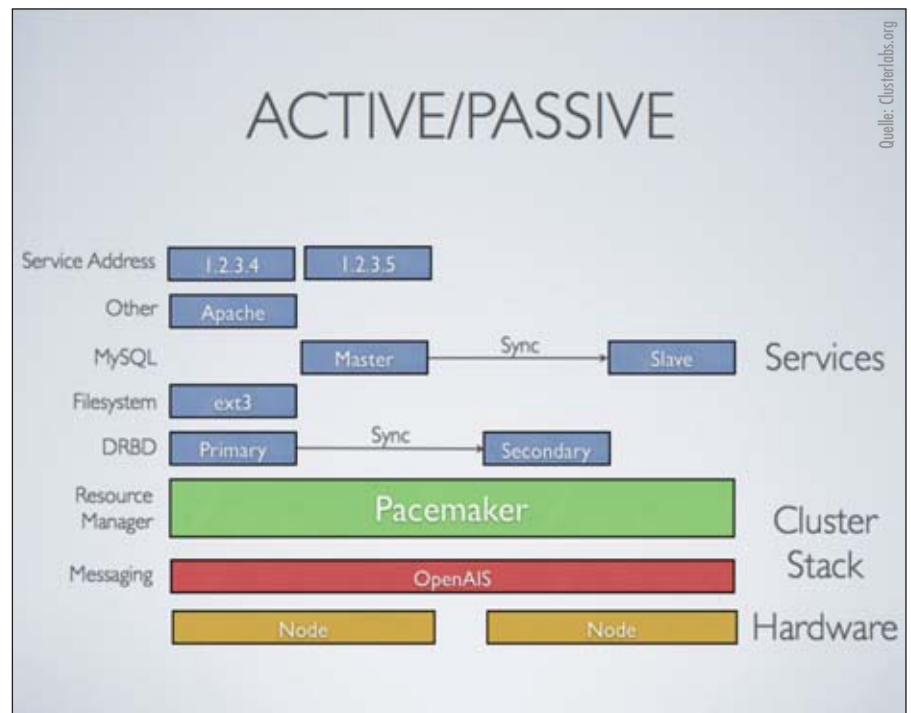


Bild 1: Ein typisches HA-Setup mit freier Software orientiert sich in der Regel am Linux-HA-Projekt, wobei Pacemaker als Cluster-Ressource Manager zum Einsatz kommt

Bild 1 zeigt den Aufbau eines typischen Cluster-Stacks mit Pacemaker, wobei als Netzwerkspeicher-Software zur Replikation meist DRBD (Distributed Replicated Block Device) zum Einsatz kommt. DRBD arbeitet innerhalb des Linux-Kernels auf Blockebene und ist daher für darauf aufsetzende Schichten transparent. Die Clustersoftware muss zu jeder Zeit sicherstellen, dass sich das aktive System und sein Schattensystem stets in einem identischen Zustand befinden. Ein gängiges Verfahren dazu ist etwa CPU-Lockstepping, eine Techno-

logie, die im Prinzip sicherstellt, dass beide Prozessoren stets exakt die gleichen Befehle ausführen. Arbeiten zudem beide CPUs in einer identischen Umgebung mit gleichen Daten und gleichen Codebestandteilen, sollte jede Instanz problemlos die andere ersetzen können. Beim Cluster-Aufbau mit Xen und Remus entfällt der Einsatz von DRBD oder ähnlichen Lösungen dagegen, weil das Prinzip von Remus ohnehin auf dem Replizieren der (virtuellen) Festplatten basiert, um die sich Remus also selbst kümmert.

Hochverfügbarkeitssysteme für Virtualisierung

Virtualisierung bietet die Chance, Hochverfügbarkeit technologisch einfacher und prinzipiell kostengünstiger zu realisieren, denn virtuelle Systeme lassen sich schnell sichern beziehungsweise in einen definierten Ausgangszustand versetzen. Die Hersteller von Enterprise-Virtualisierungslösungen reagieren auf diesen Trend mit speziellen Produkten und Erweiterungen, die im Einzelfall ordentlich ins Geld gehen. Bei VMware heißt die Hochverfügbarkeits-Lösung für vCenter VMware



vCenter Server Heartbeat [3]; bei vSphere muss es mindestens die Advanced Edition [4] sein, die allerdings mit etwa 2.000 Euro pro Prozessor zu Buche schlägt. Wie HA unter VMware funktioniert, lässt sich unter [5] nachlesen. Beim Citrix Xen Server ist Hochverfügbarkeit ebenfalls ab der Advanced Edition zu haben. Für Xen gibt es seit geraumer Zeit externe Lösungen für Hochverfügbarkeit, wie SecondSite [6], Kemari [7] oder Remus [8], von denen Letzteres in einer funktionalen Weiterentwicklung inzwischen offiziell in Xen 4.0 und 4.1 enthalten ist.

Typische HA-Lösungen in Virtualisierungs-Szenarien bestehen in der Regel aus einem Hypervisor, einem SAN als Speicherbackend (Fibre Channel oder iSCSI) nebst DRBD als Netzwerkspeicher-Software zur Replikation und Heartbeat oder Pacemaker als Cluster Resource Manager. Zum Aufsetzen eines solchen Szenarios installiert der Admin die gewünschten Netzwerkdienste in einer virtuellen Maschine, welche auf einem Hypervisor läuft. Ein zweiter Host greift über das Storage-Backend auf die Festplatte zu, während Heartbeat fortlaufend die Verfügbarkeit prüft. Fällt der aktive Host aus, kann die Clustersoftware die virtuelle Maschine auf dem zweiten Virtualisierungs-Host starten. Im Gegensatz zum aufwändigen Lockstepping machen sich Hochverfügbarkeits-Lösungen für virtuelle Infrastrukturen den Umstand zunutze, dass sich in Sekundenschnelle eine Kopie jeder laufenden virtuellen Maschine erstellen lässt. Daraus resultiert insbesondere bei der HA-Implementation Remus ein gänzlich anderer Ansatz als in herkömmlichen HA-Szenarien.

Xen als Virtualisierungs-Host

Wirklich fit für den praktischen Einsatz ist Xen eigentlich erst seit der Bereitstellung von Funktionen wie PCI-Pass-through oder einer dynamischen Speichervergrößerungen, welche mit Xen-Version 3.4 upwards implementiert sind. Der Linux-Kernel besitzt nämlich seit der Version 2.6.23 die theoretische Fähigkeit für den Betrieb unterhalb eines beliebigen Hypervisors. Mit "paravirt-ops" (pv_ops) ermöglicht der Linux-Kernel so eine transparente Paravirtualisierung, welche den Betrieb des glei-

chen Kernels sowohl im paravirtualisierten Modus auf einem Hypervisor als auch auf der ursprünglichen Hardware erlaubt, sodass insgesamt weniger Linux-Kernel unterstützt und betrieben werden müssen.

Paravirt-ops war erstmals im Linux-Kernel Version 2.6.20 enthalten, steht allerdings bisher nur für DomU-Kernel zur Verfügung. Übrigens unterstützt schon Xen 3.4 das Durchreichen von PCI-Geräten auch in virtuelle Maschinen, die ein unverändertes Betriebssystem ausführen. Dies war vorher nur für virtuelle Maschinen möglich, die ein modifiziertes (paravirtualisiertes) System ausführen, eine Funktion, die wie bei KVM den Einsatz eines Prozessors mit VT-Erweiterung am Hostsystem voraussetzt. Aus dieser Sicht ist Xen also schon seit der Version 3.4 gegenüber KVM nicht mehr im Hintertreffen, von der Patchproblematik der Kernel abgesehen.

Maßgeblichen Anteil am bisher kaum erloschenen Interesse an Xen haben auch Drittanbieter-Produkte, wie Kemari [9] und Remus, mit deren Hilfe sich virtuelle Maschinen detailliert überwachen lassen, um beim Ausfall einer Maschine unmittelbar eine Kopie auf einem Backup-System aktivieren zu können. Trotz alledem prophezeiten viele Fachleute angesichts des Erfolgs von KVM das baldige Ende für Xen, doch mit Xen 4.0 muss das Rennen um die Nutzergunst insbesondere im Bezug auf KVM neu bewertet werden, weil die XenSource-Entwickler ein beachtliches Bündel an Neuerungen geschnürt haben, das in seiner Gesamtheit einem Paukenschlag gleichkommt. Allem voran relativiert Xen 4.0 den meist angeführten Kritikpunkt eines veralteten Referenz-Kernels.

Xen 4.0 nutzt erstmals einen Dom0-Kernel auf Basis von 2.6.31, was zuvor nicht möglich war, weil die Xen-Entwickler die vom Xen Dom0-Kernel benötigten Funktionen in neueren Kernels durch die pv_ops-Schnittstelle – eine Technik, die es dem Kernel zu erkennen ermöglicht, ob er auf "nacktem Metall" (bare metal), also physikalischer Hardware, oder auf dem Xen-Hypervisor läuft – veränderten hatten. Für unprivilegierte Domains

(DomU) ist dieses Feature bereits seit geraumer Zeit wie oben beschrieben im Linux-Kernel verfügbar, für Dom0 ist es neu und muss über den neuen Kernel des Xen-Projektes zur Verfügung gestellt werden. Dabei soll aber nicht verschwiegen werden, dass 2.6.18 immer noch der offizielle Referenz-Kernel für Dom0 bleibt und dass die Hochverfügbarkeits-Erweiterung Remus nicht mit pv_ops-Kerneln funktioniert, also den Referenzkernel 2.6.18 voraussetzt.

Funktionsweise von Remus

Die Zielsetzung bei der Entwicklung von Remus orientiert sich an drei zentralen Punkten: Allgemeingültigkeit, Transparenz und der Fähigkeit zur nahtlosen Wiederherstellung im Fehlerfall. Mit allgemeingültig beschreiben die Entwickler die Tatsache, dass Remus als Low-Level-Service realisiert ist, ausschließlich mit allgemein zugänglichen Technologien, die unabhängig von der jeweiligen Anwendung funktionieren oder von der Hardware, auf der sie laufen. Mit Transparenz wird Remus dem Umstand gerecht, dass es normalerweise nicht möglich ist, Anpassungen am Code von Betriebssystemen oder Anwendungen hinsichtlich der Zusammenarbeit in einem Hochverfügbarkeits-Setup vorzunehmen, um Funktionen wie Fehlererkennung oder Statuswiederherstellung

Der dienstälteste freie Virtualisierer Xen wird seit einigen Jahren insbesondere im Lichte des aufstrebenden Newcomers KVM, dessen Quellen im Gegensatz zu denen des Konkurrenten in relativ kurzer Zeit den Sprung in den offiziellen Linux-Kernel schafften, in schöner Regelmäßigkeit für tot erklärt. Das liegt vorrangig daran, dass Xen sehr zum Verdross der Xen-Entwickler bis heute nicht in den Mainstream-Kernel integriert wurde, vorrangig ein Politikum, denn technisch hat der Virtualisierungs-Veteran eine Menge zu bieten, neben einer regen Entwicklergemeinde vor allem eine Reihe interessanter Third-Party-Erweiterungen, wie etwa die Hochverfügbarkeits-Lösung Remus. Insbesondere die Version 4.0 vom April 2010 macht das Rennen um die Nutzergunst mit der offiziellen Integration von Remus wieder spannend. Zudem hat die Remus-Erweiterung für fehlertolerante Gastsysteme mit der neuesten Version 4.1 vom März dieses Jahres weitere Fixes erfahren, sodass dem Aufbau von Enterprise-Hochverfügbarkeits-Systemen auch in virtuellen Umgebungen nichts im Wege stehen sollte.

Xen als HA-Plattform



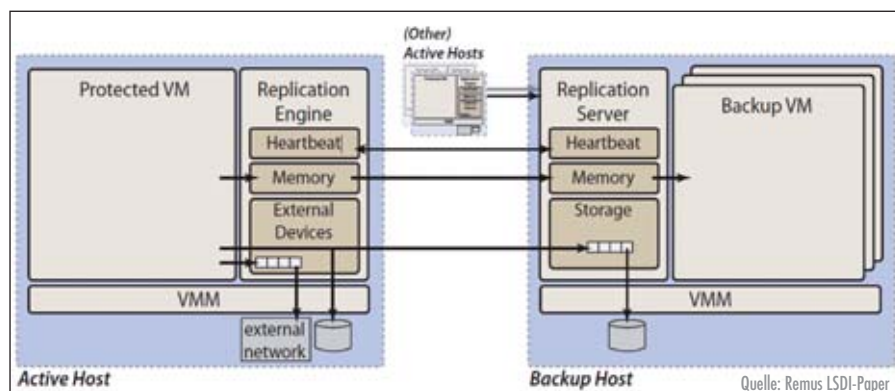


Bild 2: Die Architektur von Remus aus High-Level Sicht

zu realisieren. Die nahtlose Wiederherstellung nach einem Fehler garantiert, dass eine solche so schnell erfolgt, dass sie aus Sicht eines (Netzwerk-) Clients beziehungsweise externen Benutzers nicht zu bemerken ist, bis auf den Verlust etwaiger temporärer IP-Pakete. Dazu dürfen einmal initiierte TCP-Verbindungen nicht verloren gehen oder zurückgesetzt werden.

Clustersoftware, die Fehlertoleranz etwa mit CPU Lockstepping realisiert, erfordert einen extrem hohen Aufwand. Remus beschreitet einen gänzlich anderen Weg und stützt sich dabei maßgeblich auf das Live-Migration-Feature von Xen, gepaart mit einer intelligenten Buffer-Technologie für Netzwerkverbindungen zwischen Client und Cluster beziehungsweise einem intelligenten Schreibpuffer für das Backup-System. Architektonisch basiert Remus auf einem gewöhnlichen asymmetrischen Cluster mit nur einem aktiven Knoten und einer Schattenkopie. Zwar stellt das von Remus implementierte Verfahren im Hinblick auf 100-prozentige Hochverfügbarkeit nur eine Näherung dar, funktioniert dafür aber völlig transparent ohne spezielle Hardware und mit unveränderter Software.

TCP-Pufferung

Remus setzt also gar nicht erst voraus, dass sich das aktive System und das Backup-System stets im exakt gleichen Zustand befinden, sondern sorgt lediglich dafür, dass beide Systeme nach außen hin für einen Netzwerk-Client identisch aussehen. Der Client bemerkt also keinen Unterschied, ob er mit dem aktiven System oder bei dessen Ausfall mit dem Schattensystem verbunden ist. Die per Default alle 25 ms erzeugte Kopie bleibt auf dem

Schattensystem resident im Hauptspeicher und steht als Schattenkopie jederzeit zur Verfügung, während das aktive System weiterläuft. Die Schatteninstanz kann so sofort aktiv werden, wenn die Clustersoftware (Heartbeat) einen Fehler auf dem aktiven System feststellt.

Da aber das aktive System nach Anlegen eines solchen "Checkpoints" weiterläuft, ist die Schattenkopie prinzipiell nur alle 25 ms mit dem aktiven System identisch. Remus löst dieses Problem mit einer intelligenten Netzwerk-Puffer-Strategie zwischen dem Cluster und den verbundenen Clients. Remus puffert dazu sämtliche Netzwerkverbindungen und hält während der Zeit der Replikation sämtliche IP-Pakete zurück, sodass die jeweilige Antwort aus Sicht des anfragenden Clients immer noch aussteht. Fällt dann das aktive System aus, kann die Schattenkopie die Funktion exakt an dieser Stelle übernehmen. Denn alle Pakete bestehender TCP-Verbindungen, welche der Client während dieser Zeit an das vormalig noch aktive System verschickt hat, werden vom TCP-Protokoll erneut angefordert und landen dann automatisch bei der Schatteninstanz. Läuft das aktive System dagegen anstandslos weiter, synchronisiert Xen/Remus nach Ablauf von 25 ms die Schattenkopie wieder mit dem aktiven System. Erst nach Abschluss der Replikation erhalten alle wartenden Clients die zurückgehaltenen Pakete.

Komponenten der Remus-HA

Das HA-Design von Remus basiert auf drei wesentlichen Mechanismen und Technologien: Kern des Systems ist ein hochfrequent durchgeführtes Checkpoint-Verfahren, welches auf der Live-Migration

von Xen basiert. Zu den weiteren Eckpfeilern der Remus-Hochverfügbarkeit zählt ein intelligenter Netzwerkpuffer, der den Cluster gegenüber anfragenden Netzwerk-Clients stets als integeres, homogenes System erscheinen lässt, auch wenn einer der Knoten ausfällt. Schließlich haben die Entwickler einen intelligenten Schreibpuffer für die Festplatte des Backup-Systems implementiert. Bild 2 illustriert den prinzipiellen Aufbau und zeigt die wichtigen Kommunikationspfade.

Neben Heartbeat kommunizieren außerdem die VMs untereinander sowie das Speichernetzwerk. Das Setup geht dabei davon aus, dass beide Cluster-Knoten Xen-VMs sind, die ihrerseits auf dedizierten Xen-Hosts (Dom0) laufen. Außerdem müssen auf beiden Maschinen alle benötigten Ressourcen (Speicher) vorhanden sein und beide Xen-Hosts müssen Zugriff auf das gleiche Dateisystem beziehungsweise Speichernetzwerk haben.

Xen Live-Migration

Da die Xen Live-Migration ein wesentliches Architekturmerkmal des Remus-Designs darstellt, ist es ratsam sich zu verinnerlichen, was bei der Live-Migration mit Xen normalerweise passiert. Diese lässt sich in der Regel in fünf Phasen gliedern:

- Stage 0 – Pre-Migration: Ausgangspunkt ist eine aktive virtuelle Maschine auf Host 1. Im ersten Schritt ist ein Ziel-Host 2 auszuwählen, auf dem die notwendigen Ressourcen vorhanden sind.
- Stage 1 – Reservation: Dazu sendet Host 1 einen Request an Host 2, der die vorhandenen und notwendigen Ressourcen überprüft und anschließend einen Container reserviert, der dem Container der virtuellen Maschine auf Host 1 entspricht.
- Stage 2 – Iterative Pre-Copy: Phase 2 der Live-Migration ist ein iteratives Verfahren. In der ersten Iteration transferiert Xen sämtliche Speicherseiten (Pages) der virtuellen Maschine, anschließend nur noch solche, die seit der letzten Iteration verändert wurden, so genannte "Dirty Pages", wozu sämtliche Schreibzugriffe während der Migration abgefangen und gepuffert werden. Erst nach einer bestimmten Anzahl von Iteratio-

Kompetentes Schnupperabo sucht neugierige Administratoren

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

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

Damit Sie sich Zeit,
Nerven und Kosten sparen.

**Teamwork in Bestform.
Überzeugen Sie sich selbst!**



6

**Monate
lesen**

3

**Monate
bezahlen**

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 85
D-80802 München

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

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

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

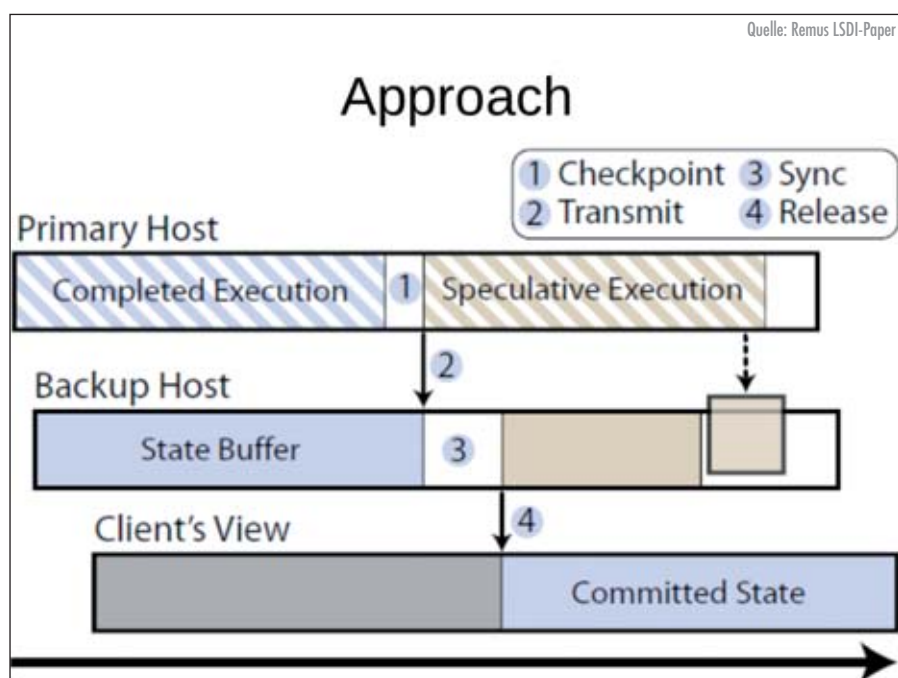


Bild 3: Die Remus Pipelining-Strategie wandelt das Einmal-Verfahren der Xen Live-Migration in ein hochfrequentes Checkpointing um, das den Inhalt der kompletten VM bis zu 40 Mal in der Sekunde repliziert

nen oder wenn es beim Übertragen der Dirty-Pages keine Veränderungen mehr gibt, kann der Zyklus beendet werden.

- Stage 3 – Stop-and-Copy: Jetzt stoppt Xen die virtuelle Maschine auf Host 1 und lenkt jeglichen Netzwerkverkehr auf Host 2 um. Danach transferiert Xen den CPU-Zustand sowie sämtliche übrig gebliebenen Speicherseiten, also solche, die relativ oft verändert wurden. Im Anschluss existieren auf Host 1 und auf Host 2 zwei identische virtuelle Maschinen, Host 1 ist aber immer noch primärer Host.
- Stage 4 – Commitment: Host 2 bestätigt, dass er eine mit Host 1 identische virtuelle Maschine hat. Host 1 kann also demnach seine virtuelle Maschine beenden und Host 2 wird primärer Host.
- Stage 5 – Activation: Die virtuelle Maschine auf Host B ist jetzt aktiv.

Das HA-Design von Remus basiert auf der Idee, mit einer extrem hochfrequenten Live-Migration (Checkpointing) fortlaufend einen näherungsweise identischen Zustand zwischen zwei virtuellen Maschinen herzustellen. Allerdings gibt es bei der Live-Migration mit Xen das Problem, dass diese einerseits nur exakt einmal funktioniert, weil Xen die ursprüngliche VM nach erfolgreicher Migration zerstört und andererseits, dass die im Xen-

Code implementierten Methoden für eine Hochfrequenz-Migration viel zu viele Ressourcen verschlingen. Normalerweise dauert eine einzige Live-Migration mehrere Minuten. Soll aber der Systemzustand bis zu 40 Mal pro Sekunde migriert werden, stellt dies enorme Anforderungen an das Host-System. Die Remus Entwickler haben daher den originalen Live-Migration-Code von Xen analysiert und an zahlreichen Stellen für Ihren Einsatzzweck optimiert.

Remus begegnet diesen Anforderungen mit einer sehr aggressiven Pipelining-Strategie beim Anlegen der Checkpoints. Dabei sorgt Remus dafür, dass die VM in jeder Iteration jeweils für kurze Zeit pausiert. Im Prinzip entspricht diese Strategie dem oben erläuterten – jedoch optimierten – “Stage 3”. Remus unterteilt diesen Prozess dazu in vier Phasen, während der Remus die VM in jedem Zyklus für eine kurze Zeitspanne anhält, um sämtliche veränderten Zustände in einen Puffer zu kopieren. Anschließend aktiviert Remus die VM mit den gepufferten Zustandsänderungen erneut und setzt sie mittels “spekulative Ausführung” fort. Dann überträgt Remus die gepufferten Zustandsänderungen auf den Backup-Host. Erst wenn alle Zustandsänderungen vollständig übertragen sind, wird der

Checkpoint als primäres System anerkannt und der bis dato zurückgehaltene und gepufferte Netzwerkverkehr freigegeben.

Pufferung der Netzwerkverbindungen

Ein weiterer wesentlicher Bestandteil von Remus besteht im Zurückhalten der Netzwerkverbindungen zwischen Cluster und Client. Dieser Trick macht sich den Umstand zunutze, dass niedere Netzwerk-Protokolle in der Regel sowieso keine 100 Prozent zuverlässige und fehlerfreie Datenübermittlung garantieren; daher müssen vernetzte Anwendungen entweder mit Verlust, Vervielfältigung oder dem Neuanfordern von (IP-) Datenpaketen umgehen können oder ein High-Level-Protokoll wie TCP benutzen, bei dem entsprechende Garantien Teil der Protokoll-Spezifikationen sind.

Dieser Umstand vereinfacht die für Remus erforderliche Pufferung des Netzwerkverkehrs, denn einmal gesendete Pakete erfordern keine Replikation, weil ihr Verlust aus Sicht des Clients beziehungsweise des Protokolls schlicht und einfach wie ein vorübergehender Netzausfall aussieht, die jeweilige Bestätigung aus Sicht des Clients also einfach noch aussteht. Dabei ist es allerdings entscheidend, dass Daten-Pakete so lange in der Warteschlange verbleiben, bis der Checkpoint-Status des Zyklus, in dem sie erzeugt wurden, vollständig auf die Backup-Domain übertragen ist.

Fällt der primäre Host aus, spiegeln die generierten IP-Pakete in der Warteschlange den spekulativen Zustand der verloren gegangenen Pakete wider (siehe Bild 4). Eingehender Traffic wird unmittelbar zur aktiven VM durchgestellt, ausgehende Pakete allerdings, die seit dem letzten Checkpoint erzeugt wurden, werden gepuffert, bis alle Statusänderungen gesichert sind und der Backup-Host den Checkpoint übernommen hat. Der Puffer ist als Linux-Warteschlange realisiert und reagiert auf dem Gast-Netzwerk-Device in Dom0 mit zwei “RT NETLINK”-Meldungen.

Disk Buffering

Eine Pufferstrategie für Festplatten stellt eine gänzlich andere Herausforderung als das Puffern von Netzwerk-Schnittstellen,

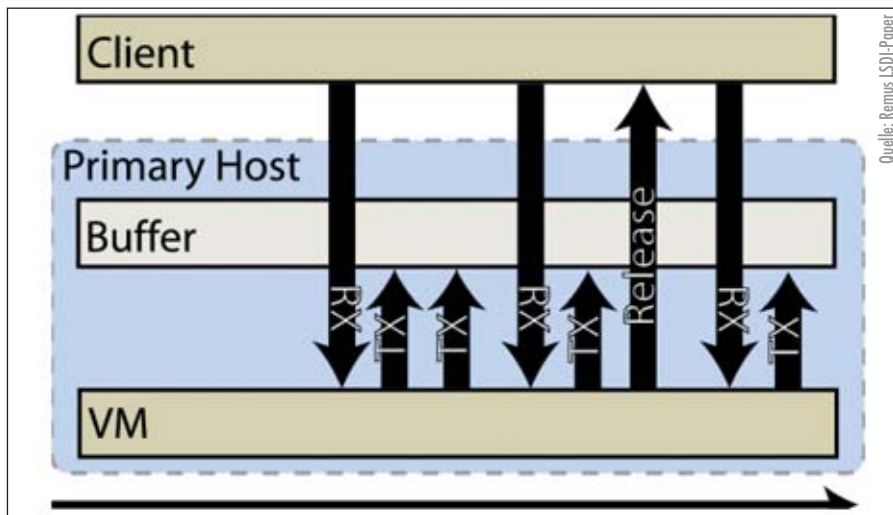


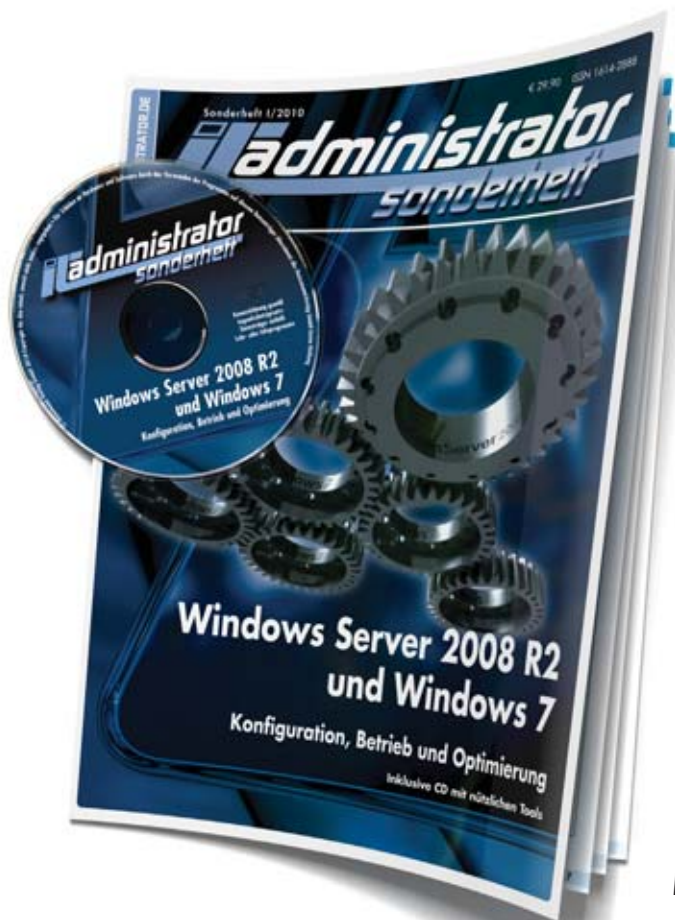
Bild 4: Der von Remus implementierte Netzwerk-Puffer sorgt dafür, dass der Cluster aus Sicht des Clients stets als homogenes System erscheint. Der Client merkt daher nicht, ob er mit dem aktiven oder (im Fehlerfall) dem Schattensystem verbunden ist, auch wenn die CPU-Zustände (intern) nur alle 25 ms identisch sind.

weil hierbei eine viel höhere Zuverlässigkeit erforderlich ist. Sobald etwa eine Schreiboperation vom Datenträger bestätigt wurde, erwartet eine Anwendung oder das Dateisystem zu Recht, die Daten rekonstruieren zu können. Während Remus vorrangig das Ziel verfolgt, den Ausfall eines einzelnen Hostsystems zu kompensieren, muss eine

Festplatte konsistente Daten garantieren, auch wenn beide Hosts ausfallen.

Allerdings verbietet diese Zielsetzung einer allgemeintauglichen Lösung spezielle Storage-Hardware. Remus hält deshalb einen kompletten Spiegel der Disks des primären Systems auf dem Backup-Host vor.

Mit dem Einschalten des Clusters verfolgt der Schreibpuffer persistente Schreibzugriffe der primären VM. Da Schreibzugriffe der VM des aktiven Systems als write-through-Zugriffe behandelt werden, landen diese unmittelbar im Disk-Image der primären VM. Zusätzlich sorgt Remus dafür, die Daten asynchron zum Disk-Puffer des Backup-Systems zu übertragen. Dieser Ansatz bietet zwei Vorteile: Erstens ist sichergestellt, dass die Disk der aktiven VM jederzeit konsistent ist. Fallen beide Hosts aus, spiegelt die Festplatte des aktiven Systems damit stets den Stand der äußerlich sichtbaren VM zum Zeitpunkt der Störung wider. Das äußerlich (aus Sicht des Clients) sichtbare System (VM) befindet sich solange auf dem primären Host, wie dieser nicht von der Störung betroffen ist, und außerdem dann, wenn das Backup-System ebenfalls in Mitleidenschaft gezogen wurde, bevor es aktiviert werden konnte. Zweitens spiegelt das direkte Schreiben (write through) ins Disk-Image des primären Systems die Latenz- und Durchsatz-Charakteristik der physischen Festplatte wider.



Bestellen Sie jetzt das IT-Administrator Sonderheft I/2010!

180 Seiten Praxis-Know-how rund um das Thema

Windows Server 2008 R2 und Windows 7 + Tools-CD

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

* IT-Administrator Abonnenten erhalten das Sonderheft I/2010 für € 24,90. Nichtabonnenten zahlen € 29,90.
Alle Preise verstehen sich inklusive Versandkosten und Mehrwertsteuer.

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier
www.it-administrator.de/kiosk/sonderhefte/



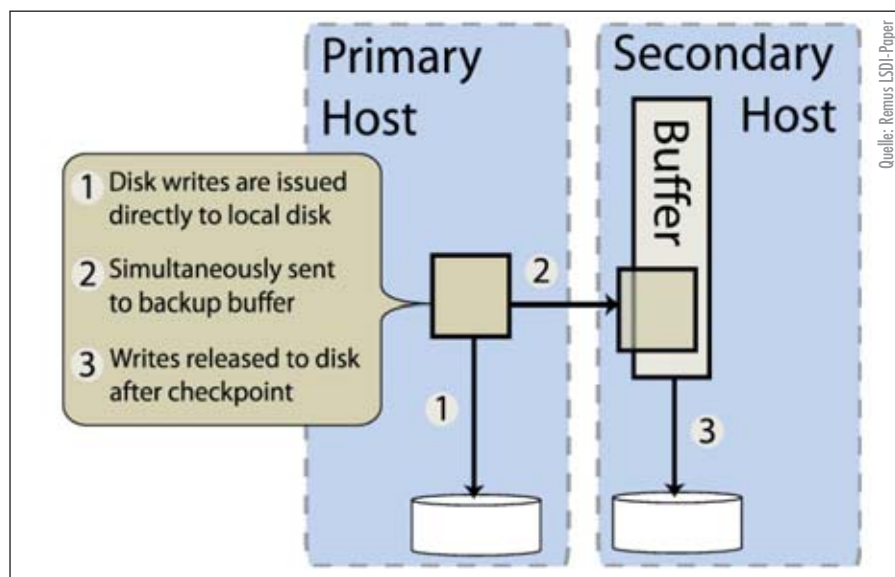


Bild 5: Remus trackt permanent sämtliche Schreibzugriffe des primären Systems. Schreibzugriffe der primären VM werden als Write-Through-Zugriffe behandelt und direkt ins Disk-Image der primären Festplatte geschrieben. Gleichzeitig überträgt Remus sämtliche Schreibzugriffe asynchron zum Disk-Puffer des Backup-Systems, wo sie so lange zurückgehalten werden, bis der Checkpoint komplett übertragen ist.

Bis das Backup-System den Checkpoint komplett empfangen und quittiert hat, verbleiben sämtliche Festplatten-Änderungen vollständig im Disk-Puffer des Backup-Systems (Bild 5). Erst wenn der Checkpoint komplett empfangen wurde, schreibt Remus den Inhalt des Diskpuffers auf die Festplatte des Backup-Systems. Im Fehlerfall wartet Remus, bis sämtliche gepufferten Schreibzugriffe empfangen wurden, obwohl das Backup-System im Prinzip auch früher mit der Ausführung fortfahren könnte, indem es den empfangenen Disk-Puffer als Overlay benutzt. Allerdings würde dieses Vorgehen im Zweifel die Disk-Semantik aus Sicht der geschützten VM verletzen, denn falls dann das Backup-System nach seiner Aktivierung ebenfalls ausfällt, noch bevor sämtliche Statusänderungen komplett auf die Backup-Disk geschrieben wurden, wäre der Disk-Status inkonsistent.

Erste Schritte mit Remus

Remus ist seit November 2009 offizieller Bestandteil von Xen. Haben Sie also Xen installiert, finden Sie automatisch sämtliche Remus-Tools im bin-Verzeichnis. Zu beachten ist allerdings, dass Remus nicht mit paravirtops-Kerneln funktioniert, weshalb der Xen-Default-Kernel 2.6.18-8 erste Wahl für Experimente mit Remus ist.

Wenn Sie Remus im jetzigen Entwicklungsstadium ausprobieren möchten, soll-

ten Sie sich die Empfehlungen der Entwickler [10] genau ansehen, worin diese darauf hinweisen, zunächst die korrekte Funktionsweise des Virtualisierungs-Systems sowie der Live-Migration zu testen. Hierzu benötigen Sie zunächst nur zwei Xen Dom0-Hosts mit VMs sowie ein funktionierendes Speicher-Backend, auf das beide Xen-Hosts zugreifen können – im einfachsten Fall eine NFS-Freigabe auf einem dritten (externen) System, das Sie dann lediglich auf beiden Xen-Hosts am gleichen Mountpoint einbinden. Jetzt müssen Sie lediglich noch dafür sorgen, dass die virtuellen Disk-Images beider virtueller Maschinen auf diesem NFS-Share liegen. Danach steht einem Test der Live-Migration nichts mehr im Wege, welche unbedingte Voraussetzung für das Funktionieren von Remus ist. Dazu genügt der Befehl:

```
xm migrate -live {vmname} {IP-Dom0-Zielsystem}
```

Sofern die Live-Migration einwandfrei funktioniert, empfehlen die Remus-Entwickler im nächsten Schritt zunächst die Replikation ohne Pufferung des Netzwerkverkehrs durchzuführen, wozu der Parameter “-no-net” dient. Allerdings weisen die Entwickler für diesen Schritt des Test-Szenarios darauf hin, dass die virtuelle Festplatte des primären Systems

hierbei beschädigt wird, weshalb Sie etwaige Versuche am besten mit einer Kopie durchführen. Der Start von Remus erfolgt dann mit

```
remus -no-net {vmname} {IP-Dom0-Zielsystem}
```

Hat auch dies fehlerfrei funktioniert, kann auch das Replizieren der Festplatte scharf geschaltet werden.

Fazit

Der dienstälteste freie Virtualisierer Xen bietet mit der seit 2009 integrierten Remus-Erweiterung eine leistungsfähige und kostengünstige Hochverfügbarkeitslösung, in welche die Entwickler eine Menge Gehirnschmalz investiert haben. Deren Verfügbarkeit ist nicht nur als weiteres Pro-Argument für die Auswahl des geeigneten Hypervisors zu werten, sondern vor allem eine technologisch interessantere und gleichzeitig übersichtliche freie HA-Lösung gegenüber klassischen Open Source-HA-Stacks auf Basis von Heartbeat, OpenAIS und DRBD. Die Remus-Lösung macht nämlich unter anderem insbesondere das Storage-Management mittels DRBD überflüssig und erreicht (zumindest der Papierform nach) extrem hohe Verfügbarkeit. (jp)

- [1] Linux-HA-Projekt
B7P31
- [2] Clustermanager Pacemaker
B7P32
- [3] VMware vCenter Server Heartbeat
B7P34
- [4] VMware vSphere Advanced Edition
B7P35
- [5] Funktionsweise HA mit VMware
B7P36
- [6] SecondSite
B7P37
- [7] Kemari
B7P38
- [8] Remus
B7P39
- [9] NSDI-Paper Remus
B7P30
- [10] Kemari und Xen
B7P3A

Link-Codes



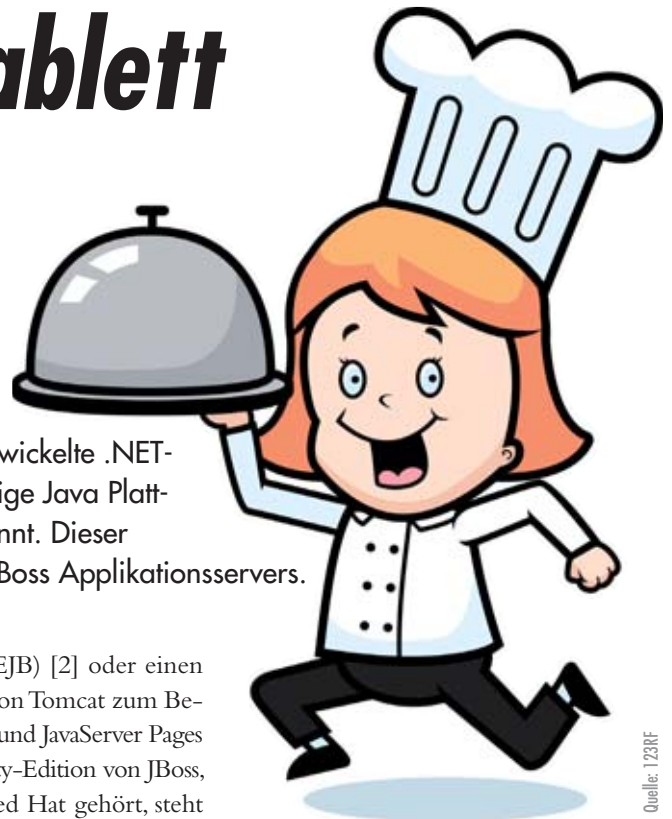


Java Enterprise-Anwendungen mit JBoss bereitstellen

Webanwendungen auf dem Silbertablett

von Thorsten Scherf

Das Entwickeln von Unternehmensanwendungen wird heutzutage immer umfangreicher und komplexer. Steht ein Entwickler vor der Aufgabe, eine Unternehmensanwendung zu programmieren, so stehen ihm hierfür im Wesentlichen zwei Software-Architekturen zur Verfügung. Auf der einen Seite existiert die von Microsoft entwickelte .NET-Plattform, auf der anderen Seite die herstellerunabhängige Java Plattform, Enterprise Edition – aktuell auch als Java EE bekannt. Dieser Workshop gibt einen Einstieg in Java EE auf Basis des JBoss Applikationsservers.



Quelle: 123RF

Java EE ist eine Ansammlung diverser Softwarekomponenten und Dienste, die quasi einen De-facto-Standard bei der Entwicklung von Enterprise-Anwendungen darstellen. Durch klar definierte APIs können dabei Komponenten unterschiedlichster Hersteller problemlos miteinander agieren. Jede Java EE basierte Anwendung benötigt natürlich eine entsprechende Umgebung, in der diese ablaufen kann und die die notwendigen Komponenten und Services zur Verfügung stellt, beispielsweise Transaktionsmanagement, Namens- und Verzeichnisdienste, Persistenz- und Deployment-Dienste sowie ein Sicherheits-Framework (siehe Bild 1). Eine vollständige Liste findet sich in der Java EE-Spezifikation [1].

enterprise Java Beans (EJB) [2] oder einen Webserver auf Basis von Tomcat zum Bereitstellen von Servlets und JavaServer Pages (JSP). Eine Community-Edition von JBoss, das inzwischen zu Red Hat gehört, steht unter [3] zum Download zur Verfügung.

JBoss installieren

Der JBoss Applikationsserver (AS) steht ebenfalls unter [3] als ZIP-Datei zum Download bereit. Bevor es jedoch an dessen Installation geht, müssen Sie sicherstellen, dass das System entweder über ein aktuelles Java Development Kit (JDK) oder ein Java Runtime Environment (JRE) verfügt. Frühere Versionen von JBoss AS benötigten zwingend ein JDK,

da dieses über einen entsprechenden Compiler für Java-Code verfügt. Dieser ist zum Übersetzen von JSP-Dateien notwendig. Aktuelle Versionen, also AS5 oder AS6, genügt jedoch auch ein JRE, da JBoss eine Eclipse-JDT Bibliothek mit ausliefert, die ebenfalls Java-Code übersetzen kann. Handelt es sich bei dem System, auf dem Sie JBoss installieren wollen, jedoch um einen Entwicklungsrechner, so bevorzugen Sie wahrscheinlich den-

Im kommerziellen Umfeld existieren mit IBM Websphere und BEA WebLogic zwei weitverbreitete Schwergewichte entsprechender Server-Implementierung. Mit JBoss steht solch ein Server als Open Source-Produkt unter der GNU Lesser General Public License (LGPL) zur Verfügung. Dieser stellt alle notwendigen Softwarekomponenten, Dienste und Container der Spezifikation zur Verfügung und erweitert diese um eigene, Server-spezifische Konfigurationsmöglichkeiten. Beispielsweise enthält JBoss einen EJB-Container für En-

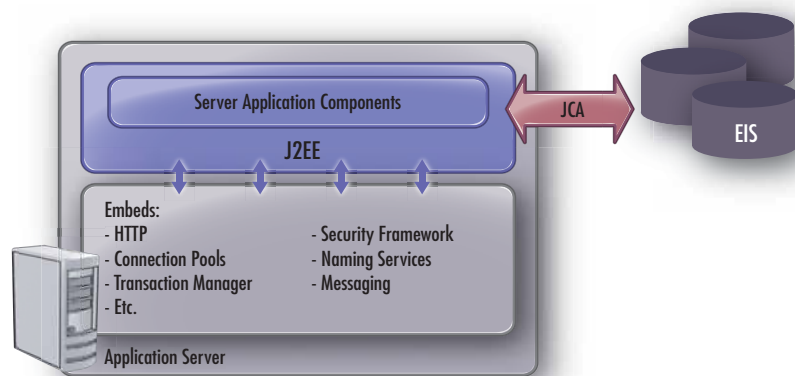


Bild 1: Ein Applikationsserver besteht aus verschiedenen Komponenten, die auf ein Enterprise-Information-System (EIS) zurückgreifen können



Die ersten Versionen von JBoss basierten auf einem sogenannten Java-Management-Extension Kernel (JMX). Sämtliche Services des Anwendungsservers wurden hier als Managed Beans (MBeans) in den JMX-Kernel geladen, um ihre Funktionen zur Verfügung zu stellen. Mit der Version AS4 begann dann die Migration auf eine Microcontainer-Architektur, in der nun leichtgewichtige Plain Old Java Objects (POJOs) statt MBeans zum Einsatz kommen. MBeans unterstützt JBoss allerdings immer noch, da der JMX-Kernel nun selbst als POJO auf dem Microcontainer aufsetzt. Für die Zukunft ist geplant, sämtliche MBeans als reine POJOs zu implementieren, so dass der Einsatz des JMX-Kernels nicht mehr notwendig ist.

Architektur



noch das JDK. Nach der Installation der Java-Umgebung ist darauf zu achten, dass die JAVA_HOME-Variable auf das Java Root-Verzeichnis zeigt:

```
# export JAVA_HOME=/usr/lib/jvm/
jre-1.6.0-openjdk
# echo $JAVA_HOME
/usr/lib/jvm/jre-1.6.0-openjdk
# java -version
java version "1.6.0_18"
OpenJDK Runtime Environment
(IcedTea6 1.8.3)
(fedora-46.1.8.3.fc13-i386)
OpenJDK Server VM
(build 14.0-b16, mixed mode)
```

Nach diesen Vorarbeiten entpacken Sie das ZIP-Archiv des JBoss AS in ein beliebiges Verzeichnis, beispielsweise nach /opt, und passen die JBOSS_HOME-Variable entsprechend an, so dass diese auf das Installationsverzeichnis zeigt. Zur Administration ist ein grundlegendes Verständnis der Verzeichnisstruktur des Servers wichtig. Nach dem Auspacken des Archivs befinden sich im Root-Verzeichnis diverse Ordner:

- **bin-Verzeichnis:** Enthält alle Skripte, die zum Starten und Stoppen des Servers notwendig sind. Außerdem ist hier auch das JMX-Kommandozeilentool twiddle abgelegt, mit dem Sie den Server administrieren können.
- **client-Verzeichnis:** Enthält Bibliotheken, die eventuell beim Zugriff von Standalone-Clients benötigt werden. Bei Standalone-Clients handelt es sich beispielsweise um GUI-Clients auf Basis

von Swing oder AWT, Webservice-Clients oder JMS-Clients.

- **doc-Verzeichnis:** Enthält hauptsächlich DTD-Dateien und XML-Schemadateien für die JBoss Konfigurationsdateien, da diese auf XML basieren. Konfigurationsbeispiele finden sich unterhalb von docs/examples/.
- **lib-Verzeichnis:** Enthält Bibliotheken, die zum Starten des JBoss AS notwendig sind.
- **server-Verzeichnis:** JBoss kommt von Haus aus mit verschiedenen Konfigurationen daher. Dieses Verzeichnis enthält diverse Unterverzeichnisse, die jeweils einer bestimmten Konfiguration entsprechen. Beim Starten des Servers können Sie dann bestimmen, welche Konfiguration zum Einsatz kommen soll. Natürlich lassen sich die einzelnen Konfigurationen ändern oder neue hinzufügen. Bild 2 zeigt das Konfigurationsverzeichnis "all". Im Vergleich zur Default-Konfiguration sind hier beispielsweise auch die JBoss-Clusterservices aktiviert.

Durch das Auswählen einer bestimmten Server-Konfiguration können Sie nun also bestimmen, welche JEE-Services und Komponenten der JBoss AS starten soll. Passt keine der vorhandenen Konfigurationen, kopieren Sie einfach einen vorhandenen Ordner, benennen diesen um und passen die Kopie entsprechend an.

Wie das genau geht, erfahren Sie später in diesem Workshop. Möchten Sie den JBoss-Server mit sämtlichen Services starten, so ist hierfür der folgende Aufruf notwendig:

```
# /opt/jboss-5.1.0.GA/bin/run.sh -c
all
```

Auf der Konsole sind nun die Startmeldungen der einzelnen Services zu sehen und am Ende sollte schließlich eine Statuszeile Auskunft darüber erteilen, wie lange die Startup-Prozedur dauerte:

```
19:58:19,965 INFO [ServerImpl]
JBoss (Microcontainer) [5.1.0.GA
(build:SVNTag=JBoss_5_1_0_GA
date=200905221634)] started in
54s:991ms
```

Alternativ ist es auch möglich, den Server im Hintergrund zu starten und die Status-Meldungen der einzelnen Services in eine Log-Datei zu schreiben. Das hat unter anderem den Vorteil, dass die Konsole nicht durch den Server belegt ist:

```
/opt/jboss-5.1.0.GA/bin/run.sh -c
all > console.log &
```

Ein Zugriff auf den Web-Container des Servers sollte zu diesem Zeitpunkt bereits funktionieren (siehe Bild 3). Die Startseite bietet Zugriff auf diverse Online-Res-

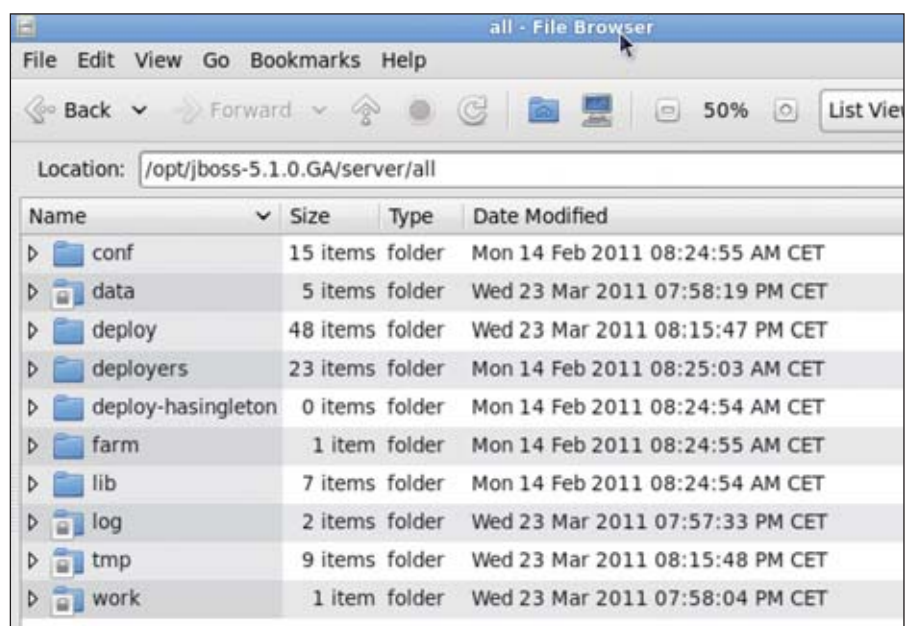


Bild 2: Jedes JBoss-Konfigurationsverzeichnis enthält eine Vielzahl von Unterverzeichnissen, mit denen Sie das Verhalten des Servers anpassen können

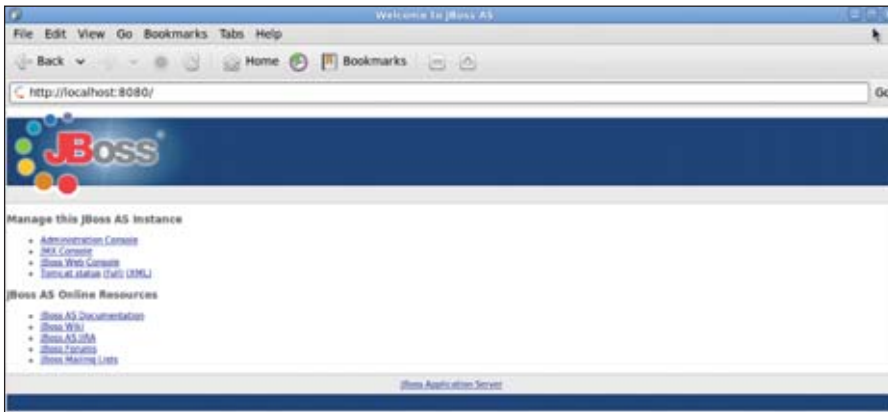


Bild 3: Nach dem Hochfahren des Servers erhalten Sie über die Startseite des Web-Containers Zugriff auf diverse Anwendungen und Online-Ressourcen

sourcen und JBoss interne Applikationen, die sich zur Administration des Servers verwenden lassen.

Erste Java-Webanwendung bereitstellen

Um nun die erste Schritte auf dem neuen Server aufzuzeigen, beginnen wir an dieser Stelle mit dem Bereitstellen einer Java-basierten Webanwendung mit Hilfe des JBoss Web-Services. Dieser basiert auf dem bekannten Tomcat für dynamische Inhalte, kann aber ebenfalls auf die Apache Portable Runtime (APR) zurückgreifen, wenn es darum geht, statische Inhalte schnell auszuliefern. JBoss unterstützt mit dem integrierten Web-Server von Haus aus das sogenannte Hot-Deployment. Hierzu kopieren Sie beispielsweise die gewünschte Webanwendung in ein bestimmtes Verzeichnis der aktiven Server-Konfiguration und JBoss stellt diese Anwendung unmittelbar bereit.

```
<html><head><title>JSP Test</title>
<%!
String message = "Hello, World.";
%>
</head>
<body bgcolor="white">
<h2><%= message%></h2>
<%= new java.util.Date() %>
</body></html>
```

Listing: JSP-Datei

```
<web-app>
<display-name>Hello world</display-name>
</web-app>
```

Listing: Deployment-Deskriptor

Zuerst ist jedoch die entsprechende Anwendung zu erzeugen und vorzubereiten. Da die Entwicklung von komplexen Anwendungen den Rahmen dieses Artikels sprengen würde, greifen wir hier auf die bekannte "Hello World"-Anwendung zurück. Diese liegt hier als JavaServerPage vor. JBoss übersetzt diese dynamisch, erzeugt ein Servlet und stellt dieses einem Client über eine Webschnittstelle zur Verfügung. Es existieren mehrere Methoden, diese Anwendung nun bereitzustellen, beispielsweise in Form eines Webarchives (WAR-Archiv). Für dieses Archiv müssen Sie zuerst eine entsprechende Verzeichnis-Struktur erzeugen, wobei die JSP-Datei im Root-Verzeichnis liegt. Hierhin gehört ebenfalls ein Unterverzeichnis WEB-INF mit einem Deployment-Deskriptor namens *web.xml*. Dieser Deployment-Deskriptor ist Teil der JEE-Spezifikation, sodass auch Servlets von anderen Servern unter JBoss lauffähig sind. Server-spezifische Konfigurationsanweisungen liest JBoss aus der Datei *WEB-INF/jboss-web.xml* ein. Dazu zählt beispielsweise die Konfiguration einer Security-Domäne für Ihre Anwendung. Hiermit können dann unter anderem Benutzer authentifiziert und autorisiert werden, bevor diese Zugriff auf die Anwendung oder Teile davon erhalten. Die JSP-Datei sowie der Deployment-Deskriptor sind in den beiden Listingkästen dargestellt.

Mit Hilfe des Tools "jar" lässt sich aus diesen Dateien nun ein WAR-Archiv erzeugen (siehe Listing "WAR-Archiv mit jar erzeugen"). Das so erzeugte Archiv kopieren Sie dann in das Host-Deployment-Verzeichnis des aktiven JBoss-Konfigura-

tionsverzeichnisses. JBoss nimmt in diesem Falle sofort Notiz von der neuen Web-Anwendung und stellt diese unmittelbar zur Verfügung. Der Aufruf von *http://localhost:8080/helloworld/hello.jsp* im Webbrowser bestätigt dies (siehe Bild 4).

```
# jar -cvf helloworld.war *.jsp
WEB-INF/
added manifest
adding: hello.jsp(in = 159)
(out= 131)(deflated 17%)
adding: WEB-INF/(in = 0)
(out= 0)(stored 0%)
adding: WEB-INF/web.xml(in = 63)
(out= 48)(deflated 23%)
```

```
# cp helloworld.war ../../jboss-
5.1.0.GA/server/all/deploy/
20:15:48,905 INFO [TomcatDeploy-
ment] deploy, ctxPath=/helloworld
```

Statt das WAR-Archiv in das Deployment-Verzeichnis zu kopieren, lässt sich auch das bereits erwähnte Admin-Tool twiddle verwenden. Mit Hilfe der Operation *deploy* der JBoss MBean "jboss.system:service=MainDeployer" stellen Sie die Webanwendung auch dann bereit, wenn Sie beispielsweise gar kein Schreibrecht auf das Deployment-Verzeichnis besitzen. Ein Nachteil dieser Methode besteht jedoch darin, dass die Anwendung nach einem Neustart des Servers nicht wieder automatisch gestartet wird.

```
# ./twiddle.sh invoke "jboss.sys-
tem:service=MainDeployer" deploy
/opt/examples/Helloworld/hello-
world.war
```

Anstatt mit komprimierten Archiv-Dateien kann JBoss auch mit kompletten Verzeichnis-Strukturen umgehen. Dies ist manchmal einfacher, als Archive bereitzustellen, da sich in Verzeichnissen einzelne Dateien leichter verändern oder hinzufügen lassen, ohne dass bei jeder Änderung ein neues Archiv zu erzeugen ist. Ein Neustart des Servers ist nach einer Änderung an einer Anwendung nicht notwendig, JBoss erkennt diese automatisch anhand aktualisierter Zeitstempel an den Dateien. Wichtig vor dem Bereitstellen ganzer Verzeichnisse ist jedoch, dass diese den passenden Suffix besitzen, ansonsten

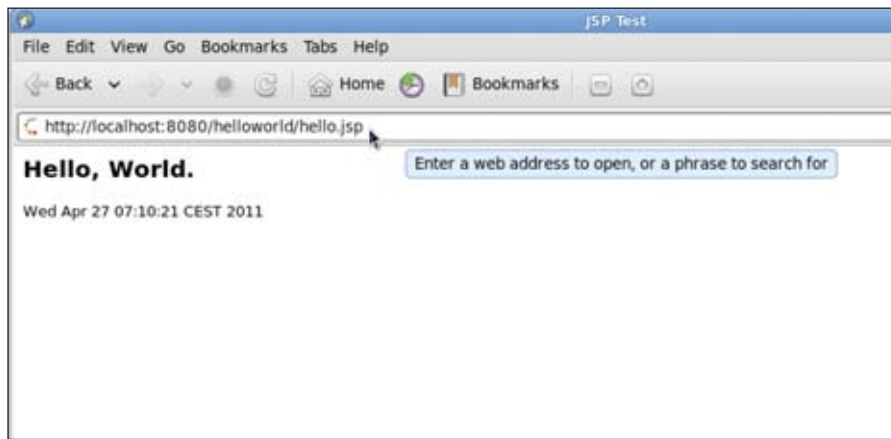


Bild 4: Im Webbrowser lässt sich schließlich die Ausgabe der Webanwendung bewundern

weiß der Server nicht, welcher Deployer zum Bereitstellen zu verwenden ist:

```
# mv /opt/examples/helloworld/
/opt/examples/helloworld.war/
# rm -f /opt/jboss-
5.1.0.GA/server/all/deploy/
helloworld.war
10:25:22,371 INFO [TomcatDeploy-
ment] undeploy, ctxPath=/
helloworld
# cp -r
/opt/examples/helloworld.war/
/opt/jboss-5.1.0.GA/server/all/
deploy/
10:25:22,412 INFO [TomcatDeploy-
ment] deploy, ctxPath=/helloworld
```

Passende Server-Konfiguration

Nachdem Sie nun wissen, wie Sie eine einfache Webanwendung auf dem JBoss AS bereitstellen können, lohnt es sich, einen genaueren Blick in die Konfiguration des Servers zu werfen. Wie bereits weiter oben erwähnt, enthält JBoss AS mehrere Konfigurations-Verzeichnisse. Beim Starten des Servers wurde in unserem Beispiel die all-Konfiguration ausgewählt. Der entsprechende Konfigurationsordner `/opt/jboss-5.1.0.GA/server/all` enthält diverse Unterverzeichnisse (siehe Bild 2).

Auch hier ist ein grundlegendes Verständnis der einzelnen Verzeichnisse wichtig:

- **conf-Verzeichnis:** Enthält sämtliche Konfigurationsdateien für den JBoss-Kernservice, die einzelnen Services sowie für das Logging-Subsystem log4j [4].
- **deploy-Verzeichnis:** Dieser Ordner wurde bereits im letzten Abschnitt vorgestellt. Sämtliche Anwendungen, die

in dieses Verzeichnis kopiert werden, erkennt JBoss automatisch und stellt diese dynamisch zur Verfügung. Zum Entfernen einer Anwendung ist diese einfach aus dem deploy-Verzeichnis zu löschen oder besser in ein undeploy-Verzeichnis zu verschieben.

- **deployers-Verzeichnis:** Enthält Services zum Erkennen der verschiedenen Anwendungen- und Archivtypen aus dem deploy-Verzeichnis.
- **lib-Verzeichnis:** Enthält Bibliotheken, die von sämtlichen JEE Services einer gemeinsamen Serverkonfiguration verwendet werden. Spezielle Bibliotheken, die nur zu einer einzelnen Anwendung gehören, stellen Sie lieber über die Anwendung selbst zur Verfügung – beispielsweise als Teil eines Webarchives.

Neben diesen Standard-Verzeichnissen erzeugt JBoss noch weitere Ordner zur Laufzeit. Hiervon sind besonders diese interessant:

- **log-Verzeichnis:** Enthält die Dateien `boot.log`, `server.log` und eventuell `audit.log` (je nach Konfiguration). `boot.log` enthält alle Log-Meldungen des Start-Prozesses des Servers, bis die Kontrolle an log4j übergeben wird. Dieser Service schreibt die Meldungen dann in die Datei `server.log`. Das Sicherheits-Subsystem von JBoss verwendet die Datei `audit.log` für sicherheitsrelevante Meldungen.
- **work-Verzeichnis:** Hier hält der JBoss Webserver die übersetzten Java-Class Dateien und Servlets auf. Für die oben aufgeführte Webanwendung existieren hier beispielsweise die beiden Dateien `work/jboss.web/localhost/helloworld/org/`

`apache/jsp/hello_jsp.class` und `work/jboss.web/localhost/helloworld/org/apache/jsp/hello_jsp.java`.

Zum Anpassen des Servers sind sicherlich die Konfigurationsdateien unterhalb von `conf/` am interessantesten. Als Beispiel soll hier das Logging des JBoss-Servers etwas angepasst werden. Wie bereits erwähnt, setzt JBoss das log4j Logging-Framework ein. In der Konfigurationsdatei `conf/jboss-log4j.xml` existieren in der Standardkonfiguration zwei sogenannte Appender. Diese bestimmen, wohin die Logmeldungen der JBoss-Services oder der bereitgestellten Anwendungen zu senden sind. Der erste Appender schreibt sämtliche Meldungen aller Loglevel (TRACE, DEBUG, INFO, WARN, ERROR and FATAL) in die Datei `log/server.log` und legt dabei einmal pro Tag eine neue Datei mit einem entsprechenden Datums-Suffix an (siehe Listing "WAR-Archiv mit jar erzeugen"). Soll der Server stattdessen die Log-Datei rotieren, sobald diese eine bestimmte Größe erreicht hat, so sind die Appender-Parameter entsprechend anzupassen (siehe Listing "Anpassen der Appender-Parameter").

Der zweite Appender "CONSOLE" sorgt für eine Ausgabe auf der Konsole. Jedoch findet diese erst ab dem Log-Level INFO statt, wofür der Parameter "`<param name='Threshold' value='INFO'/>`" in der Konfiguration des Appenders zuständig ist. Somit vermeiden Sie, dass das Konsolen-Log mit zu vielen Log-Meldungen

```
<appender name="FILE" class="org.jboss.logging.ap-
pender.DailyRollingFileAppender">
  <errorHandler
    class="org.jboss.logging.util.OnlyOnceError
    Handler"/>
  <param name="File"
    value="${jboss.server.log.dir}/server.log"/>
  <param name="Append" value="true"/>
  <param name="DatePattern" value="'.'yyyy-
MM-dd"/>
  <layout class="org.apache.log4j.PatternLay
  out">
    <param name="ConversionPattern" value="%d
    %5p [%c] (%t) %m%n"/>
  </layout>
</appender>
```

Listing:
WAR-Archiv mit jar erzeugen





überflutet wird. Natürlich ist es auch möglich, für die einzelnen Dateien oder Log-Level einzelne Log-Dateien zu erzeugen. Hierfür existieren in der Kategorie "Limit categories" Einstellmöglichkeiten, die sich auf einen Appender mit einem bestimmten Namen beziehen (dieser ist hier als Referenz anzugeben) und das Logging einer bestimmten Klasse oder einer Anwendung, die von dieser Klasse abgeleitet ist, ab einem bestimmten Log-Level definieren. Die Konfigurationsdatei bietet hierfür sehr viele Beispiele.

Unnötige Dienste abschalten

In den bisherigen Beispielen wird der JBoss-Server immer mit der Konfigurationseinstellung "all" gestartet. Hierdurch stehen sämtliche Services und Komponenten des Servers zur Verfügung. Für Test- und Entwicklungssysteme mag dies sicherlich in Ordnung sein, für Systeme in der Produktion gilt dies jedoch nicht. Hier gilt der Grundsatz "Weniger ist mehr". Wieso soll der Server Dienste anbieten, die gar nicht benötigt werden? Diese stellen nur ein unnötiges Sicherheitsrisiko dar und sollten somit deaktiviert oder noch besser entfernt werden.

Mit der Konfiguration "all" startet JBoss 25 verschiedene Services, mit der Konfiguration "default" sind es dagegen lediglich 15 Services. Der Hauptunterschied zwischen den beiden Konfigurationen liegt darin, dass mit "all" sämtliche Cluster-Dienste zur Verfügung stehen, mit "default" jedoch nicht. Wenn Sie also

keinen Cluster benötigen, so reicht die Standard-Konfiguration sicherlich aus. Jedoch bietet es sich an, selbst diese Konfiguration noch etwas abzuspecken, falls Sie auf bestimmte Dienste verzichten können. Hierfür ist zuerst ein neues Konfigurationsverzeichnis auf Basis der default-Konfiguration zu erzeugen:

```
# cp -r /opt/jboss-
5.1.0.GA/server/default
/opt/jboss-5.1.0.GA/server/custom
```

In dem Verzeichnis "custom" können Sie nun sämtliche Services deaktivieren, die nicht unbedingt notwendig sind. Beispielsweise soll auf einem Produktionssystem sicherlich nicht die JBoss-Startseite sichtbar sein. Entfernen Sie diese einfach, indem Sie *custom/deploy/ROOT.war* löschen oder umbenennen. Ist der Mail-Service nicht wirklich notwendig, so löschen Sie die Dateien *custom/deploy/mail-service.xml* und *custom/lib/mail*.jar*. Ein Blick in das *deploy-* und *lib-*Verzeichnis hilft weitere unnötige Services zu identifizieren.

JBoss bietet von Haus aus einige Management-Tools an, dazu zählt beispielsweise die JMX-Console, die unter der URL <http://localhost:8080/jmx-console/> zu erreichen ist. Mit der Konsole haben Nutzer die Möglichkeit, ManagedBeans (MBeans) des Servers zu lesen und zu verändern. Die weiter oben angesprochenen Änderungen am Logging-Subsystem hätten so auch mit der JMX-Console durchgeführt werden können. Somit stellt diese Webanwendung eine mächtige, aber auch gefährliche Möglichkeit dar, den kompletten JBoss-Server zu konfigurieren. Auf einem Produktionssystem ist die Konsole somit entweder zu entfernen (*deploy/jmx-console.war*) oder aber der Zugang ist mit Hilfe einer Benutzerauthentifizierung entsprechend zu sichern.

Authentifizierung und Autorisierung

Das Sicherheitssystem von JBoss basiert auf dem Java Authentication and Authorization Service (JAAS). Über Sicherheits-Domänen legen Sie hier fest, welche Art von Login-Modulen für eine bestimmte Anwendung zum Einsatz kommen soll. Es existieren bereits vorgefertigte Login-

Module für den Zugriff auf Datenbanken, LDAP-Server oder einfache Dateien. Ist eine Webanwendung für eine bestimmte Sicherheits-Domäne konfiguriert, so muss sich ein Benutzer beim Zugriff auf diese authentifizieren und bekommt nach erfolgreicher Authentifizierung und Autorisierung eine bestimmte Rolle zugewiesen. Anhand dieser Rolle kann der Admin festlegen, auf welche Teile der Webanwendung der Benutzer zugreifen darf. Eine vordefinierte Sicherheits-Domäne für die JMX-Console finden Sie im entsprechenden Listing.

Bei diesem Login-Modul handelt es sich um eine einfache Variante, bei der die Authentifizierung und Autorisierung von Benutzern anhand von Dateien stattfindet. Komplexere Beispiele für den Zugriff auf eine Datenbank oder einen LDAP-Server befinden sich jedoch ebenfalls in der Datei *conf/login-config.xml*. Damit eine Anwendung nun weiß, welche Sicherheitsdomäne zum Einsatz kommen soll, ist diese im JBoss-eigenen Deployment-Deskriptor der Anwendung, *jboss-web.xml*, zu hinterlegen. Hier tragen Sie den Namen der Domäne ein, mit dem diese sich über das Java Naming and Directory Interface (JNDI) auf dem Server angemeldet hat. Im Falle der JMX-Console hat die Änderung also in der Datei *deploy/jmx-console.war/WEB-INF/jboss-web.xml* zu erfolgen:

```
<jboss-web>
  <security-domain>java:/jaas/jmx-
    console</security-domain>
</jboss-web>
```

```
<appender name="FILE" class="org.jboss.logging.ap-
  pender.RollingFileAppender">
  <errorHandler
    class="org.jboss.logging.util.OnlyOnceError
      Handler"/>
  <param name="File"
    value="${jboss.server.log.dir}/server.log"/>
  <param name="Append" value="false"/>
  <param name="MaxFileSize" value="10MB"/>
  <param name="MaxBackupIndex" value="20"/>
  <layout class="org.apache.log4j.PatternLay
    out">
    <param name="ConversionPattern" value="%d
      %-5p [%c] (%t) %n"/>
  </layout>
</appender>
```

**Listing: Anpassen
der Appender-Parameter**



```
<application-policy name="jmx-console">
  <authentication>
    <login-module
      code="org.jboss.security.auth.spi.UsersRoles
        LoginModule"
      flag="required">
      <module-option
        name="usersProperties">props/jmx-console-
          users.properties</module-option>
      <module-option
        name="rolesProperties">props/jmx-console-
          roles.properties</module-option>
    </login-module>
  </authentication>
</application-policy>
```

**Listing: Sicherheits-Domäne
für die JMX-Console**





Hiermit ist nun klar, welche Sicherheits-Domäne und somit welches Login-Modul für die JMX-Console zum Einsatz kommt. Es fehlt jedoch noch ein Regelwerk, welches bestimmt, wer Zugriff auf welche Ressourcen hat. Diese Information ist der Anwendung nun über den regulären Deployment-Deskriptor `deploy/jmx-console.war/WEB-INF/web.xml` mitzuteilen:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>HtmlAdap
      <description>Eine beispiel
        hafte Sicherheitseinstellung
        die nur Nutzern mit der
        Rolle JBossAdmin den Zugriff
        auf die HTML JMX-Webappli-
        kation erlaubt
      </description>
    <url-pattern>/*</url-pattern>
    <http-method>GET</http-
      method>
    <http-method>POST</http-
      method>
  </web-resource-collection>
</security-constraint>
```

```
# keytool -genkey -alias example -keystore tuxge-
ek.keystore -keyalg RSA
keytool -genkey -alias example -keystore
tuxgeek.keystore -keyalg RSA
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: tiffy.tuxgeek.de
What is the name of your organizational unit?
[Unknown]: GPS
What is the name of your organization?
[Unknown]: Red Hat
What is the name of your City or Locality?
[Unknown]: Stuttgart
What is the name of your State or Province?
[Unknown]: BW
What is the two-letter country code for this unit?
[Unknown]: DE
Is CN=tiffy.tuxgeek.de, OU=GPS, O=Red Hat,
L=Stuttgart, ST=BW, C=DE correct?
[no]: yes
```

```
Enter key password for <example>
(RETURN if same as keystore password):
Re-enter new password:
```

```
# keytool -list -keystore tuxgeek.keystore
Enter keystore password:
```

```
Keystore type: JKS
Keystore provider: SUN
```

```
Your keystore contains 1 entry
```

```
example, Mar 25, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5):
AC:D5:CB:5C:13:9D:EF:F2:85:6B:AB:89:49:F8:48:3A
```

Listing:
Zertifikatsspeicher mit keytool



```
</web-resource-collection>
<auth-constraint>
  <role-name>JBossAdmin</role-
    name>
</auth-constraint>
</security-constraint>
```

Fehlen schließlich noch Benutzeraccount-Daten. Wie im Login-Modul für die Anwendung festgelegt, kommen diese aus den beiden Dateien `props/jmx-console-users.properties` für die Benutzer-Namen und Passwörter und aus `props/jmx-console-roles.properties` für die Zuordnung einer Rolle zu einem Account. Anhand des Beispiels muss ein Benutzer nun also der Rolle "JBossAdmin" angehören, damit dieser Zugriff auf die Console bekommt. Hat alles funktioniert, sollte diesmal beim Aufruf von `http://localhost:8080/jmx-console/` ein Fenster aufgehen, welches den Benutzer zur Authentifizierung auffordert.

Andere Webanwendungen lassen sich nun auf ähnliche Art und Weise für eine Benutzer-Authentifizierung und Autorisierung konfigurieren. Wichtig dabei ist, dass die verwendete Sicherheits-Domäne sich zuvor beim JNDI registriert hat.

Sichere Kommunikation

Abschließend geht es um die Konfiguration für einen sicheren Zugriff auf eine Webanwendung. Dies ist besonders dann wichtig, wenn die Anwendung sensible Daten überträgt und selbstständig eine Benutzer-Authentifizierung durchführt, wozu dann wahrscheinlich auch die Übertragung eines Benutzer-Passwortes gehört. Für eine gesicherte https-Verbindung ist dem JBoss-Server ein zusätzlicher Web-Connector hinzuzufügen. Vor dessen Konfiguration ist jedoch erst ein Zertifikatsspeicher zu erzeugen. Dieser Speicher enthält ein X.509-Zertifikat, welches entweder selbst signiert wurde oder über die Signatur einer externen Zertifizierungsstelle (CA) verfügt. Mit Hilfe der Java-Anwendung `keytool` lässt sich ein solcher Zertifikatsspeicher anlegen.

Um schließlich den https-Port des Web-Connectors zu aktivieren, müssen Sie in der Konfigurationsdatei des JBoss Web-

Services, `deploy/jbossweb.sar/server.xml`, den soeben erzeugten Zertifikatsspeicher, inklusive des dazugehörigen Passwortes, ausführen:

```
<Connector protocol="HTTP/1.1"
  SSLEnabled="true"
  port="8443"
  address="{jboss.bind.address}"
  scheme="https"
  secure="true" clientAuth="false"

  keystoreFile="{jboss.server.home.
    dir}/conf/tuxgeek.keystore"
  keystorePass="redhat"
  sslProtocol = "TLS"
/>
```

Ab nun stehen sämtliche Webanwendungen auch über den gesicherten https-Port 8443 zur Verfügung und bieten somit eine verschlüsselte Übertragung der Daten an.

Fazit

Natürlich kann dieser Artikel nicht sämtliche Konfigurationsmöglichkeiten des JBoss-Applikationsservers vorstellen, dafür ist die Thematik zu umfangreich. Interessante Themen, die bisher nicht angesprochen wurden, sind beispielsweise die Enterprise Java Beans (EJBs) und das JBoss-Clustering. Mit EJBs ist es möglich, komplexe Anwendungen zu modularisieren und somit die eigentliche Geschäftslogik aus der Anwendung herauszutrennen. Das JBoss-Clustering sorgt für eine hochverfügbare Konfiguration des Servers. Weitere Informationen zu diesen und weiteren Themen bietet die ausführliche Dokumentationsseite des JBoss-Projektes [5]. (dr)



- [1] Java EE-Spezifikation
B7P61
- [2] Java EJB-Technologie
B7P62
- [3] JBoss Community Seite
B7P63
- [4] log4j Projektseite
B7P64
- [5] JBoss Dokumentation
B7P65

Link-Codes



Bleiben Sie in Verbindung!



Folgen Sie uns auf Twitter

twitter.com/ita_blog



Werden Sie ein Fan auf Facebook

www.facebook.de/itanet



Treten Sie unserer Xing-Gruppe bei

www.xing.com/net/itanet



Lesen Sie unseren RSS-Feed

www.it-administrator.de/rss.xml

Social Networks sind auch beim IT-Administrator angekommen!

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

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

Ausfallsicherheit der DHCP-Infrastruktur unter Windows Server 2008 R2

Solides Netzwerk-Fundament

von Thomas Gronenwald

In den wenigsten Fällen machen sich Systemverantwortliche über eine ausreichende Redundanz ihres DHCP-Servers Gedanken. Dabei hat ein Ausfall des DHCP für ein Unternehmen oft erhebliche Auswirkungen. Fällt der einzige DHCP-Server im Netzwerk aus und kommen Leasetimes von mehr als fünf Tagen zum Einsatz, ist das Problem in den meisten Unternehmen höchstwahrscheinlich nicht allzu groß. Anders verhält es sich, wenn Technologien wie VPN, Provisioning und viele andere vom DHCP-Server abhängige Dienste genutzt werden.

Dieser Workshop zeigt vier Maßnahmen zur Erhöhung der DHCP-Verfügbarkeit auf und wirft einen detaillierten Blick auf die Konfiguration von DHCP-Split-Scope unter Windows Server 2008 R2.

Kommt es zum Ausfall des DHCP-Servers, erhält der DHCP-Client üblicherweise eine Auto-IP-Konfiguration (APIPA) aus dem 169.254.x.x Bereich – ein geregeltes Arbeiten innerhalb einer Domäne oder des Netzwerkes ist damit jedoch nicht möglich. Doch sinnvollerweise verfallen bei einem Bootvorgang die DHCP-Leases nicht. Der Client versucht lediglich, seinen Lease bei seinem zuständigen DHCP-Server zu erneuern (DHCP-Request). Erhält er keine Antwort vom Server, so sendet er einen entsprechenden ARP-Request, um zu prüfen, ob seine IP-Adresse bereits im Netzwerk verwendet wird. Erhält er darauf keine Antwort, nutzt er seine IP-Adresse bis zum Ablauf seiner Leasetime.

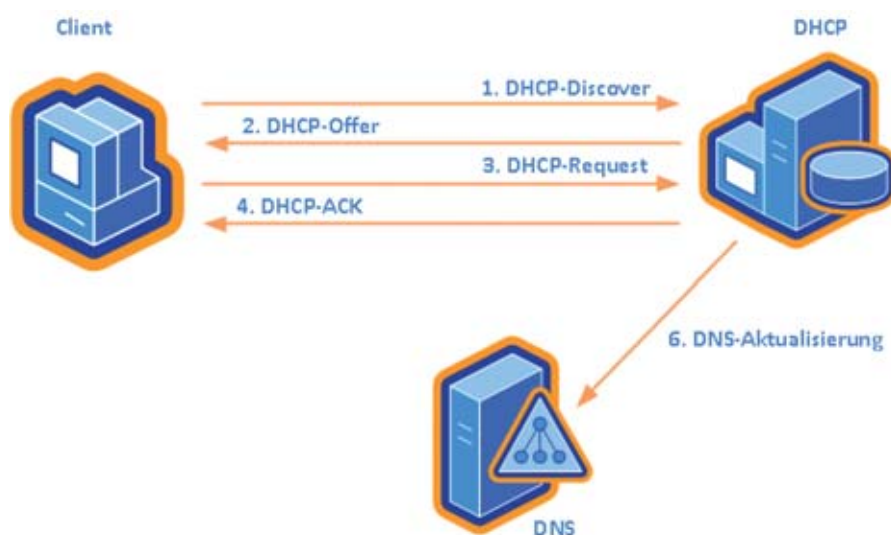


Bild 1: Ablauf eines DHCP-Requests

Probleme bei nicht verfügbarem DHCP-Server

Das heißt in der Regel, dass Probleme nur entstehen, wenn der DHCP-Server nicht verfügbar ist, und:

1. ein neuer DHCP-Client integriert wird
2. ein Client-Computer neugestartet wird und ein DHCP-Client das Ende seiner Leasetime erreicht hat
3. eine neue Verbindung zum Netzwerk hergestellt (Netzwerkkabel, Dockingstation oder Standby) wird
4. ein DHCP-Client mit Reservierung diese nicht validieren kann und eine andere Adresse erhält.

Ebenso kommt es zu Problemen, wenn der DHCP-Server zwar verfügbar ist, aber keine gültigen Adressen mehr verfügbar sind, spricht der Bereich erschöpft ist.

Das bedeutet: Fällt der DHCP-Server aus, bricht die Kommunikation im Netzwerk nicht sofort zusammen – es ist jedoch damit zu rechnen, dass je länger der Dienst nicht verfügbar ist, vermehrt Fehler auftreten. Um diesen Ausfällen vorzubeugen, sollte die ständige Verfügbarkeit eines DHCP-Servers mit freien IP-Adressen sichergestellt werden. Um das zu realisieren, gibt es wie so oft mehrere Wege, die ans Ziel führen.

Hochverfügbarkeit für DHCP

In der Praxis unterscheiden wir zwischen den folgenden vier Hochverfügbarkeits-Optionen:

- DHCP-Cluster
- DHCP-Hot-Standby
- DHCP-Cold-Standby
- DHCP-Split-Scope

DHCP-Cluster

Seit Windows Server 2000 gibt es die Möglichkeit, die DHCP-Dienste zu clustern. Mit der Einführung eines DHCP-Clusters im Unternehmen lässt sich eine vollumfängliche Redundanz schaffen. Nachteile hierbei sind jedoch die nicht unerheblichen Kosten für einen Cluster und eine komplexe Konfiguration und Verwaltung. Aus diesen Gründen finden sich in Unternehmen nur relativ selten DHCP-Cluster – oft wird anderen und zumeist günstigeren Lösungen der Vortritt gewährt.

DHCP-Cold-Standby

Eine der simpelsten Methoden, um die Verfügbarkeit des DHCP-Dienstes sicherzustellen, ist die eines "Cold-Standby"-Servers. Das heißt, dass es zwar nur einen



richtigen DHCP-Server im Netzwerk gibt, aber als Ersatz ein Server vorhanden ist, der diese Dienste jederzeit übernehmen könnte. Dieser Server ist jedoch in keinsten Weise dafür konfiguriert. Dabei wird lediglich die DHCP-Konfiguration in regelmäßigen Abständen gesichert und die Wiederherstellung dieser Konfiguration auf einem anderen Server getestet. Dies ist zweifellos die günstigste Variante, die DHCP-Verfügbarkeit zu gewährleisten, jedoch lässt sich so weder eine wirkliche Ausfallsicherheit erreichen noch sind genaue Angaben zu Ausfallzeiten möglich. Dazu kommt ein erhöhter administrativer Aufwand bei der Migration der DHCP-Dienste.

DHCP-Hot-Standby

Ein weiterer Weg zur Erhöhung der Ausfallsicherheit besteht darin, einen Standby-Server für den produktiven DHCP-Server zu konfigurieren. Dieser Weg funktioniert aber erst zuverlässig ab Windows Server 2003 oder später. Das Failover erfolgt bei dieser Methode – anders, als Sie es vielleicht vermuten – nicht automatisch, sondern manuell durch den Administrator. Ein Automatismus ist mit Bordmitteln nicht zu erreichen. Was diese Lösung jedoch für einige Administratoren wieder interessant macht, ist der günstige Preis im Vergleich zu einem Cluster.

Die Konfiguration des Standby-DHCP-Servers unter Windows Server 2003, 2008 oder 2008 R2 erfolgt mittels *netsh* in der Kommandozeile. Mit relativ wenigen Parametern lassen sich alle notwendigen Umschaltmaßnahmen in Skripten und in einer Batch-Datei zusammenfassen. Die Ausführung beziehungsweise Sicherung der DHCP-Konfiguration erfolgt in der Regel per geplanten Task. Hiermit werden sodann alle Leases und DHCP-Konfigurationen mittels *export* (von *netsh*) exportiert und auf dem Ziel-Server wieder importiert. Im Falle eines Failovers muss der Administrator dann nur noch den Backup-DHCP-Server im Active Directory autorisieren.

Auch diese Variante ist relativ günstig und bietet auch einen akzeptablen Grad der Ausfallsicherheit. Diese ist jedoch von einer manuellen Umschaltung durch den Administrator abhängig. Daher entsteht ein erhöhter administrativer Aufwand bei der Inbetriebnahme. Technisch sieht sich



Bild 2: Im Szenario mit einem Hot-Standby-DHCP-Server muss der Administrator diesen beim Ausfall des DHCP-Servers manuell aktivieren

der IT-Verantwortliche dabei möglicherweise mit IP-Adresskonflikten (Änderungen seit der letzten Sicherung und Wiederherstellung) konfrontiert.

DHCP-Split-Scope

Der häufigste und auch oft kostengünstigste Weg, um eine Ausfallsicherheit herzustellen, besteht darin, dass Administratoren den verfügbaren IP-Adressbereich auf verschiedene DHCP-Server aufteilen – unter Windows Server 2003 auch als „80/20-Regel“ bekannt (unter Windows Server 2008 R2 jedoch stark vereinfacht und mit eigenem Assistenten ausgestattet). Jeder DHCP-Server erhält dabei einen eigenen Bereich (Aufteilung 80 zu 20 Prozent) der IP-Adressen, der sich nicht überschneiden darf.

Fällt ein Server aus, kann der zweite Server zumindest übergangsweise übernehmen und die Clients versorgen, die keinen gültigen Lease haben. Im optimalen Fall ist der zweite Server so dimensioniert, dass er im Failover alle DHCP-Clients mit IP-Adressen versorgen kann. So wären auch längere Ausfallzeiten ohne Beeinflussung der IT-Prozesse möglich.

Wichtig hierbei ist allerdings, dass bei dieser Lösung auch die Reservierungen auf den DHCP-Servern berücksichtigt wer-

den. Diese lassen sich für jeden DHCP-Bereich getrennt festlegen. Wird von einem Client zum Beispiel eine bestimmte IP-Adresse (Reservierung) benötigt und erhält er diese per DHCP, spielen Reservierungen eine elementare Rolle. Hierdurch ergibt sich die Pflicht, dass auf allen DHCP-Servern auch alle nötigen Reservierungen hinterlegt sind – und das immer aktuell.

Vorteile dieser Konfiguration:

- hohe Ausfallsicherheit
- einfache Konfiguration
- bereits als Option wählbar und keine zusätzlichen Skripte oder Tools notwendig
- Reservierungen lassen sich initial auf den zweiten DHCP-Server übertragen
- einfache Administration und kein manuelles Umschalten durch den Administrator notwendig

DHCP-Split-Scope einrichten

Wir wollen nun einen tieferen Blick in die neuen Funktionalitäten von Windows Server 2008 R2 und dem DHCP-Split-Scope werfen. Als Basis für unser Szenario greifen wir auf ein funktionierendes Active Directory mit mehreren Domain Controllern, DNS-Servern und zwei DHCP-Servern zurück.

Zur Installation des DHCP-Dienstes auf



Bild 3: Beim DHCP-Split-Scope sind zwei DHCP-Server online und teilen sich die zu vergebenen IP-Adressen nach der 80/20-Regel

beiden DHCP-Servern öffnen Sie den Servermanager und installieren die Rolle "DHCP-Server". Im Assistenten wählen Sie nun den entsprechenden Netzwerkadapter aus, auf dem der DHCP-Server das Netzwerk abhört. Nun müssen Sie noch die Domäne sowie den DNS-Server angeben. In unserem Beispiel deaktivieren wir die Nutzung von DHCPv6 und schließen die Installation ohne Autorisierung ab. Beide Konfigurationsschritte sind auf beiden DHCP-Servern durchzuführen.

Jetzt müssen Sie auf dem ersten der beiden DHCP-Server den IP-Adressbereich (Scope) anlegen. Wir nutzen hierfür einen IPv4-Bereich und weisen einen entsprechenden Namen zu. Im Anschluss muss eine Start- sowie eine End-IP-Adresse für den Bereich angegeben werden. In unserem Fall nutzen wir einen Bereich von 192.168.1.1 bis 192.168.1.100. Jetzt sollten Sie noch die benötigten Serveroptionen wie DNS, Gateway et cetera vornehmen. Anschließend aktivieren Sie den erstellten Bereich. Mit einem Rechtsklick auf die soeben erstellte Zone und der Auswahl des Menüpunktes "Erweitert" wählen Sie die Option "geteilter Bereich".

Mit Hilfe des Assistenten starten Sie nun die Konfiguration des Split-Scopes. Hierzu müssen Sie den zweiten, bereits installierten DHCP-Server angeben. Mittels Schieberegler lässt sich der geteilte Bereich auf beiden Servern einfach konfigurieren. Hierbei empfiehlt sich eine 80/20 Konfiguration – also 80 Prozent der Adressen werden durch den ersten

und 20 Prozent der IP-Adressen durch den zweiten Server bereitgestellt.

Im nächsten Schritt wird die Verzögerung, mit der der zweite Server antwortet, konfiguriert. Hiermit verhindern Sie das zeitgleiche Antworten der DHCP-Server auf eine Client-Anfrage. Hier empfiehlt sich eine Verzögerung zwischen 500 und 1.000 ms zu nutzen.

Abschließend konfiguriert der Assistent die beiden DHCP-Server und die Konfigurationen und Reservierungen werden auf den jeweils anderen kopiert. Unsere Empfehlung hier: Die benötigten Reservierungen sollten Sie im Vorfeld bereits auf dem ersten DHCP-Server konfigurieren, damit diese auf dem zweiten Server übernommen werden können.

Test der Konfiguration

Diese Split-Scope-Konfiguration sollten Sie nun ausführlich testen, bevor diese produktiv eingesetzt wird. Dabei sollten Sie beide Server jeweils einmal vom Netz trennen, um zu prüfen, ob der andere Server das Bereitstellen von Adressen übernimmt. Um hier valide Aussagen treffen zu können, sollten Sie mittels folgender Befehle die IP-Adresse jeweils einmal freigeben und wieder erneuern:

`ipconfig /release`

gibt die genutzte IP-Adresse vom Client wieder frei. Und

`ipconfig /renew`

fordert vom DHCP-Server eine Verlängerung des Leases oder eine neue IP-Adresse an.

Fehleranfälligkeit durch Konflikterkennung verringern

Ebenso empfiehlt es sich, die Konflikterkennung innerhalb der DHCP-Infrastruktur zu nutzen. Dadurch ermitteln Sie, ob eine IP-Adresse vor dem Verwenden der Adresse bereits im Netzwerk von einem anderen Gerät genutzt wird. Der DHCP-Dienst selber führt jedoch standardmäßig keine Konflikterkennung durch – daher muss diese erst in der DHCP-Verwaltung aktiviert werden.

Beim Verwenden der DHCP-Konflikterkennung wird die Anzahl der Konflikterkennungsversuche des DHCP-Servers auf zwei Versuche festgelegt. Hierdurch verlängert sich lediglich die Dauer der Adressvergabe – dies jedoch nur minimal, sodass hierdurch keine Probleme entstehen.

Mehr Sicherheit durch MAC-Adressfilterung

Ebenfalls neu in Windows Server 2008 R2 ist die Option "MAC-Adressfilter". Dabei können sowohl zugelassene als auch verweigerte MAC-Adressen im DHCP-Server hinterlegt werden. Mit der Liste stellen Sie sicher, dass speziell festgelegte Geräte eine DHCP-Adresse erhalten oder dass der Server bestimmte Adressen nicht mit IP-Adressen versorgt.

Die MAC-Adressen tragen Sie über die grafische Oberfläche ein – auch ganze Adressbereiche sind möglich. Zudem besteht die Möglichkeit, Adresslisten aus einer Textdatei zu importieren. Des Weiteren hat das Microsoft DHCP-Server-Team eine grafische Oberfläche (MAC Filter Import Tool) zum Importieren von MAC-Adressen veröffentlicht [1]. Sicherlich bietet diese Option keinen vollumfänglichen Netzwerkzugriffsschutz, doch jede, sei es noch so kleine Maßnahme, die zum Schutz der Infrastruktur beiträgt, erhöht die Sicherheit kontinuierlich.

Fazit

Unser Beispiel zeigt, dass mit wenig Aufwand eine funktionierende, redundante und kostengünstige DHCP-Serverlandschaft implementiert werden kann. Teure Cluster-Konstellationen sind nicht zwangsläufig notwendig. Zudem bieten kleine, aber feine Neuerungen unter Windows Server 2008 R2 erweiterte Konfigurationsmöglichkeiten. (jp)

Thomas Gronenwald ist Security Consultant bei der adMERITia GmbH. Seinen Blog finden Sie unter blog.port389.de.



Bild 4: Innerhalb des geteilten Bereichs kann der Administrator die IP-Adressen bequem mit einem Schieberegler verteilen

[1] Download MAC Filter Import Tool
B7P51

Link-Codes





Hochleistungscluster mit Windows HPC Server 2008 R2

Kräftige Schultern

von Thomas Joos

Auch mit einfachen Servern und Clients lassen sich Hochleistungscluster aufbauen. Die Grundlage hierfür stellt Microsoft mit dem Windows HPC Server 2008 R2 bereit. Hierbei handelt es sich um eine spezielle Version des Windows Server 2008 R2 beziehungsweise um eine Zusatzlösung für das Betriebssystem. Administratoren können damit einen Cluster aufbauen, der die Rechenkapazität aller angeschlossenen Knoten nutzt, um die Gesamtrechenleistung zu erhöhen. Vor allem Computer mit mehreren Kernen laufen mit dem System zu Höchstleistungen auf. Welche Neuerungen das Release 2 mitbringt, erfahren Sie in diesem Beitrag.

Quelle: 123RF

HPC Server 2008 R2 ist der direkte Nachfolger von HPC Server 2008 mit erweiterten Funktionen. Dieser wiederum hat den Windows Compute Cluster Server 2003 (CCS) abgelöst. Microsoft stellt auf seiner Internetseite verschiedene Benchmarks zur Verfügung, welche die Leistungsfähigkeit des Systems zeigen sollen. Sie finden diese Daten auf der Seite [1]. Da Sie für die Supercomputerlösung keine spezielle Hardware benötigen und sogar Rechenoperationen auf Windows 7-Computern auslagern können, haben auch mittelständische Unternehmen durchaus Vorteile von der Serverlösung, vor allem weil eine Testumgebung sehr schnell aufgebaut ist. Damit Anwendungen die HPC-Techniken nutzen können, müssen sie so programmiert sein, dass sie parallele Rechenoperationen unterstützen. Beispiele für die Entwicklung finden Sie zum Beispiel auch über Visual Studio 2010. Viele Anwendungen, die auf Berechnungen aufbauen, wie zum Beispiel Excel 2010, sind für HPC optimiert.

Supercomputer-Cluster mit einfachen Servern

Der Vorteil von Windows HPC Server 2008 R2 ist, dass Sie diesen auf herkömmlichen Servern installieren können, die dadurch ihre Rechenkraft bündeln. Die Computer müssen allerdings als 64-

Bit-System zur Verfügung stehen, Windows HPC Server 2008 R2 unterstützt keine 32-Bit-Systeme mehr. Eine neue Funktion in HPC Server 2008 R2 ist die Möglichkeit, Excel-Tabellen, die extreme Rechenleistung benötigen, schnell auf HPC-Clustern berechnen zu lassen. Excel User-Defined Functions (UDFs) in Excel 2010 können Sie mit dieser Technik auf einen HPC-Cluster berechnen lassen. Rechenoperationen, die auf normalen Computern Stunden dauern, lassen sich mit dieser Technik in wenigen Minuten berechnen.

Eine wesentliche Neuerung in Windows HPC Server 2008 R2 ist die Möglichkeit, Windows 7-Computer im Cluster zu betreiben. Diese neue Technik heißt "Cluster of Workstation" (CoW). Mit ihr lassen sich Rechenoperationen an Windows 7-Rechner auslagern, die Bestandteil des Clusters sind. Ebenfalls neu ist die Möglichkeit, HPC-Knoten in Windows Azure einzubinden, dem Cloudsystem von Microsoft. Dies ermöglicht ein Auslagern von komplexen Rechenoperationen in die Cloud. Die Knoten lassen sich parallel zu den HPC-Clusterknoten im internen Netzwerk betreiben oder als kompletter Ersatz. Die Übergabe der Berechnungen steuert dazu der Broker Node im Cluster, der parallel auch in-

terne Server verwalten kann. Sie müssen zur Unterstützung von Azure das SP1 des HPC Pack 2008 R2 installieren. Dieses finden Sie auf der Seite [2]. Alle Neuerungen des SP1 im Detail finden Sie unter [3]. Insbesondere, wenn Sie Excel-Berechnungen durchführen oder den internen HPC-Cluster an Windows Azure anbinden möchten, sollten Sie das SP1 installieren. Dieses Service Pack hat aber nichts mit dem SP1 für Windows Server 2008 R2 zu tun, sondern aktualisiert lediglich die HPC-Komponente des Betriebssystems.

Viele Aufgaben lassen sich in der neuen Version über die PowerShell auch als Skript durchführen. Dazu steht die neue HCP PowerShell zur Verfügung. Starten Sie diese und geben

```
get-command *-hpc*
```

ein, zeigt die Shell alle verfügbaren Befehle an. Verbessert hat Microsoft zudem die Java-Unterstützung und die Verwaltung des Clusters. Auch die Zusammenarbeit der Knoten läuft jetzt wesentlich stabiler und leistungsfähiger ab. Vor allem beim Einsatz mehrerer Knoten bietet HPC Server 2008

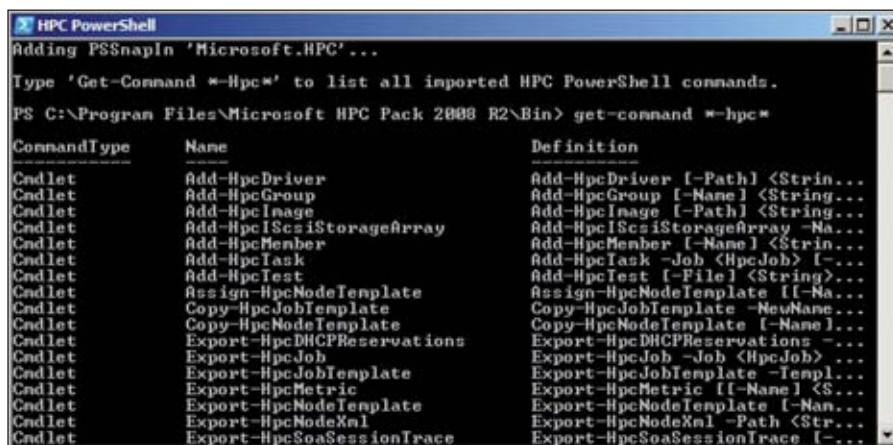


Bild 1: Das Verwalten von HPC-Clustern ist auch über die PowerShell möglich

R2 die Möglichkeit, über Diskless-Boot das Betriebssystem von einem gemeinsamen zentralen System zu booten. Eine Möglichkeit dazu ist iSCSI. Microsoft bietet die Möglichkeit an, von Clustern mit HPC Server 2008 zu 2008 R2 zu migrieren. Die entsprechenden Anleitungen zu diesem Thema finden Sie in der TechNet auf den Seiten [4,5].

Head Node, Compute Node und Broker Node

In den Vorgängerversionen konnten Sie den Verwaltungsknoten des Clusters (Head Node) nicht vor einem Ausfall schützen. Diese Möglichkeit gibt es nun in Windows HPC Server 2008 R2, da Sie den Head Node jetzt auch clustern können. Auf diesem Node läuft zum Beispiel der Job Scheduler, der die Berechnungen aller Knoten steuert. Wollen Sie diesen ausfallsicher installieren, müssen Sie HPC Pack 2008 R2 auf der Enterprise- oder Datacenter-Edition von Windows Server 2008 R2 installieren.

Die Verwaltungsaufgaben des Clusters und der Job Scheduler laufen auf diesem zentralen Element des HPC-Clusters. Die einzelnen Knoten des Clusters, welche die Berechnungen ausführen, die der Job Scheduler auf dem Head Node angibt, tragen die Bezeichnung "Compute Node". Rechner, die Anwendungen von externen Anwendungen an den Cluster zur Berechnung übergeben und die Endergebnisse wieder den Anwendern zur Verfügung stellen, sind die "Broker Nodes". Ein Glossar der Fachbegriffe finden Sie in der Microsoft-TechNet un-

ter [6]. Was die Sprachunterstützung angeht, ist Windows HPC Server 2008 R2 in Englisch, Chinesisch und Japanisch verfügbar. Sie können HPC Pack 2008 R2 aber auch auf anderen Sprachen installieren. In diesem Fall ist die Oberfläche der Verwaltung in Englisch. Die Knoten müssen Bestandteil der gleichen Active Directory-Gesamtstruktur sein, ohne Active Directory können Sie keinen HPC-Cluster betreiben.

Technik hinter dem HPC-Server

Die eigentliche Technik hinter dem HPC-Server ist das HPC-Pack, das auf den Knoten läuft und die Rechenoperationen der angebundenen Knoten steuert. Das HPC Pack 2008 R2 unterstützt bis zu 64 Kerne auf einem Server, egal auf welcher

Serverversion Sie das Pack nutzen. Installieren Sie das Pack auf einem Server mit Windows Server 2008 R2 HPC oder Windows Server 2008 R2 Standard, können Sie bis zu vier Prozessoren verwenden. Das HPC-Pack lässt sich aber auch auf Servern mit Windows Server 2008 R2 Enterprise oder Datacenter verwenden. In diesem Fall können Sie bis zu acht Prozessoren pro Server einsetzen, die Datacenter Edition unterstützt bis zu 64 Prozessoren pro Server. Microsoft stellt drei verschiedene Editionen von HPC Pack 2008 R2 zur Verfügung:

1. HPC Pack 2008 R2 Express: Die kostenlose Express-Version laden Sie über das Downloadcenter von Microsoft herunter [7]. Diese enthält nur die Funktionalitäten des HPC Server 2008 (nicht R2), zum Beispiel den Job Scheduler, SOA, MPI und die Clusterverwaltung. Der Installationsassistent ermöglicht auch die Installation der HPC Pack 2008 R2 Enterprise Edition.
2. HPC Pack 2008 R2 Enterprise: Diese Version unterstützt alle Neuerungen in HPC Server 2008 R2 und zusätzlich die Funktionen der Express-Edition. Sie benötigen diese Edition zum Beispiel für die Anbindung von Windows 7-Computern oder für Excel-Berechnungen.
3. HPC Pack 2008 R2 für Workstations: Hierbei handelt es sich um die Erweiterungen für Windows 7, um Clients

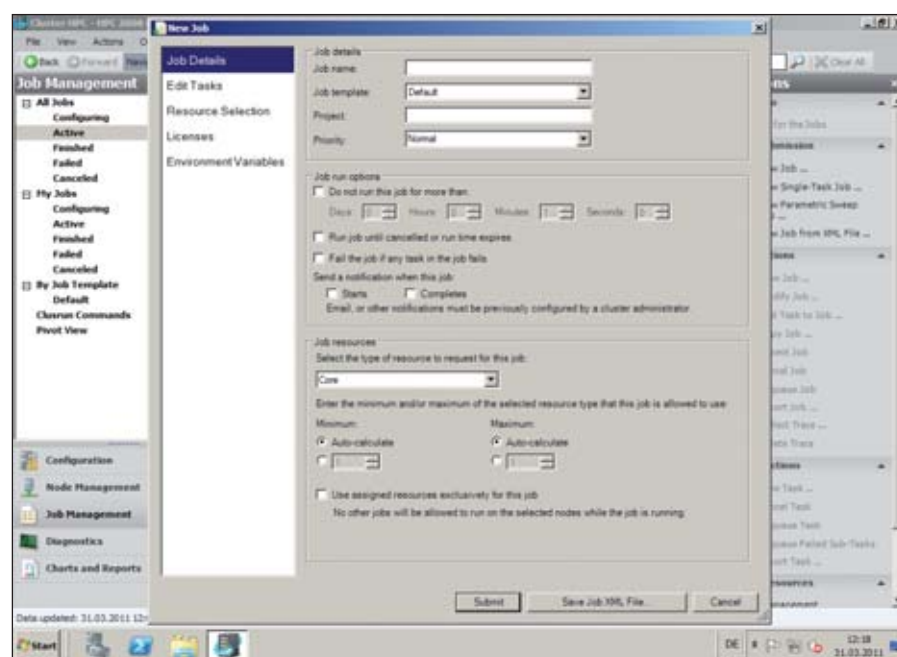


Bild 2: Rechenaufgaben im HPC-Cluster steuern Sie über Jobs



an den Server anzubinden (Workstation Node). Damit können auch Windows 7-Computer Rechenoperationen für den Cluster durchführen. Voraussetzung ist die Verwendung einer 64-Bit-Version von Windows 7 Professional oder Enterprise.

Installieren Sie das HPC Pack 2008 R2, ermittelt es auch, welche Anwendungen und Zusatztools Sie auf dem Server benötigen. Die notwendigen Erweiterungen installiert das Pack automatisch. Auf dem ersten Server, auf dem Sie das HPC Pack installieren, richtet der Assistent auch den Cluster ein und definiert den Computer als Head Node. Der oberste Knoten des HPC-Clusters (Head Node) speichert seine Daten in einer SQL-Datenbank. Hierbei unterstützt der Server auch die kostenlose Edition SQL Server 2008 (R2) Express Edition. Steht dem Server keine Datenbank zur Verfügung, installiert das HPC Pack automatisch

SQL Server 2008 Express Edition auf dem Server. Nach der Installation des HPC Pack können Sie über Assistenten die Konfiguration des Clusters vornehmen und mit dem HPC 2008 R2 Cluster Manager den Cluster erstellen und verwalten. Die Oberfläche erinnert an die Verwaltungskonsolle von System Center-Produkten und hat nichts mit der Failover-Clusterverwaltung in Windows Server 2008 R2 gemeinsam.

Ein wichtiger Punkt in diesem Pack ist das Message Passing Interface (MPI). Dieses steuert die Kommunikation zwischen den Clusterknoten. Im Cluster können Sie über tausend Knoten parallel betreiben und deren Rechenleistung gemeinsam nutzen. Die Rechenaufgaben verteilt der Job Scheduler auf den verschiedenen Knoten. Dieser überwacht die Rechenoperationen auch und synchronisiert die Systeme. Mit dieser Technik können Sie zum Beispiel bestimmte Windows 7-Computer im Netzwerk zu bestimmten Zeiten, beispielsweise nachts, an den Cluster anbinden und Rechenoperationen durchführen lassen.

Die Computer sind dann keine vollwertigen Compute Nodes, sondern stehen tagsüber Anwendern als normale Rechner zur Verfügung. Nachts oder an Wochenenden können diese Computer durch den Job Scheduler im HPC-Cluster

ter Aufgaben erhalten und Berechnungen für den Cluster durchführen. Microsoft stellt in der TechNet dazu umfangreiche Anleitungen und Informationen zur Verfügung. Diese finden Sie auf der Seite [8]. Den Blog der Entwickler erreichen Sie über die Seite [9].

In der TechNet stellt Microsoft außerdem ein Forum für HPC zur Verfügung. Dieses erreichen Sie über [10]. Umfangreiche Informationen erhalten Sie auch direkt auf der amerikanischen HPC-Seite [11], die deutschen Informationen in diesem Bereich sind aktuell mehr als spärlich. Microsoft stellt Testversionen zur Verfügung, sodass interessierte Administratoren ohne großen Aufwand einen Cluster aufbauen können. Diese finden Sie unter [12].

Vor allem Unternehmen, die häufig große und langwierige Berechnungen durchführen müssen, profitieren von der Lösung, da Ergebnisse schneller vorliegen und Anwender deutlich Arbeitszeiten sparen. Allerdings ergibt der Einsatz nur dann Sinn, wenn solche Berechnungen regelmäßig anstehen. Beispiele für Berechnungen von Excel-Tabellen in HPC-Clustern finden Sie auch in den Webcasts auf den Seiten [13] und [14]. Ein Whitepaper zu den technischen Möglichkeiten des Servers steht schließlich unter [15] zum Download bereit. (dr)



[1] Microsoft Cluster Performance-Benchmarks
B7P91

[2] SP1 des HPC Pack 2008 R2
B7P92

[3] Neuerungen des SP1 im Detail
B7P93

[4,5] Cluster mit HPC Server 2008 zu R2 migrieren
B7P94, B7P95

[6] Glossar der Fachbegriffe in TechNet
B7P96

[7] Kostenlose Express-Version herunterladen
B7P97

[8] Job Scheduler im HPC-Cluster
B7P98

[9] Blog der HPC-Entwickler
B7P99

[10] TechNet-Forum zu HPC
B7P90

[11] US-amerikanische HPC-Seite
B7P9A

[12] HPC-Testversionen
B7P9B

[13,14] Berechnungsbeispiele von
Excel-Tabellen in HPC-Clustern
B7P9C, B7P9D

[15] Whitepaper zu den technischen
Möglichkeiten des Servers
B7P9E

Link-Codes

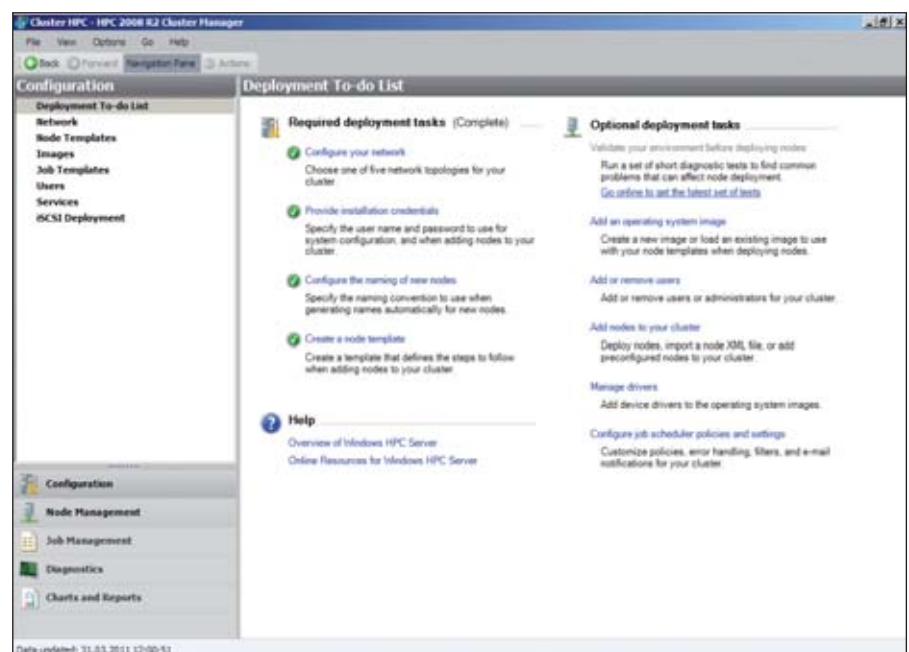


Bild 3: Die Verwaltung des HPC-Clusters erfolgt über den Cluster-Manager



Zuverlässigkeit von Reputationsdiensten unter der Lupe Zutritt verboten?

von Ralph Dombach

Eine der größten Bedrohungen in der IT-Sicherheit resultiert aus dem Web und dem Surfen der Mitarbeiter darin. Hierbei öffnen sich zahlreiche Einfallswegen für Malware. Eine bekannte Tatsache, auf die Unternehmen und die Sicherheitsindustrie mit verschiedenen Mitteln reagieren. Eine etablierte Methode besteht darin, Webseiten anhand ihrer Reputation zu filtern. Doch dabei stellt sich die Frage, wie zuverlässig der genutzte Reputationsdienst böswärtige Webseiten findet. Dieser Artikel zeigt unterschiedliche Technologien von Reputationsdiensten auf. Gleichzeitig haben wir untersucht, wie zuverlässig schädliche URLs identifiziert werden, die der Angreifer verschleiert.

Hinter einen Reputationsdienst verbirgt sich eine Datenbank, die Webadressen mit einem Bewertungskriterium verknüpft. Dieses gibt darüber Auskunft, ob eine Webadresse/URL sicher ist oder nicht. Dieses Prinzip der Bewertung funktioniert schon seit langem sehr zuverlässig bei der SPAM-Überprüfung von E-Mails, so dass der Gedanke naheliegt, dieses erfolgreiche System auch auf URLs zu übertragen.

Die Bewertung einer Webseite erfolgt dabei anhand unterschiedlicher Kriterien: Üblicherweise sind Browser-Exploits, die den Browser des besuchenden Users attackieren, ein klares Risiko. Ebenso Malware, die zum Beispiel als Datei zum Download bereitsteht. Aber auch eine Nutzung der Webseite für SPAM oder als Phishing-Hoster sind eindeutige Risikofaktoren. Die Risikoeinschätzung wird dabei üblicherweise durch Virens Scanner oder andere analysierende Verfahren ermittelt und abgespeichert. Mitunter bedienen sich die Systeme dabei aber auch öffentlichen Ressourcen [1] oder vertrauen auf die menschliche Einschätzung, wie beispielsweise bei der WOT-Community, die hinter dem Web Of Trust steht [2].

Ein Reputationsdienst ist durchaus geeignet, die Sicherheit nachhaltig zu verbessern und den Anwender davor zu bewahren, eine maliziöse Webseite zu besuchen. Doch wie so oft gibt es Situa-



Bild 1: Der McAfee SiteAdvisor findet auf der Webseite des URL-Verkürzungsdienstes goo.gl keine Security-Probleme

tionen, die den Anwender gehörig ins Straucheln bringen können.

Einsatzorte des Reputationsdienstes

Wir unterscheiden zwischen verschiedenen Arten der Service-Implementierung bei den Reputationsdiensten. Um den Anwender zu schützen, bieten sich die folgenden Methoden an:

- PC: Der Service wird auf dem jeweiligen PC installiert (zum Beispiel McAfee SiteAdvisor).
- Gateway: Der Service wird auf einem (eigenen) Gateway-System erbracht (wie etwa bei SECURE Web Gateway, Clearswift).
- WWW: Der Service wird online im Web zur Verfügung gestellt (etwa M86). M86, einer der Pioniere im Umfeld Web-Security, bietet die Nutzung seines "URL Analysis Tools" umsonst an. McAfee offeriert eine Online-Version (analog zu M86), hat aber auch eine Browser-Erweiterung im

Portfolio, die als Gratis-Version angeboten wird, und eine funktionserweiterte Browser-Kaufversion.

In einer anderen Liga spielt das Produkt von Clearswift, welches nicht für den einzelnen User gedacht ist, sondern als Gateway-System ganze Unternehmen schützt. Wer sich auf dem Markt umsieht, wird funktionstechnisch identische Lösungen von den namhaften Anbietern finden. Die hier aufgeführten Produkte sind lediglich exemplarisch zu sehen und stellen keine Wertung dar.

Generell dürfte ein zentral implementierter Reputationsservice einfacher zu administrieren sein als eine Vielzahl von Insel-Installationen. Andererseits ist aber auch eine PC-Lösung nicht zu unterschätzen, wenn aktuell kein Budget verfügbar ist. Denn generell gilt: Jede Schutzkomponente stellt einen wichtigen Baustein bei der Abwehr des immer ausgefeilteren Cybercrimes dar.



Stolpersteine

Ein Reputationsdienst ist ein nützlicher Service, aber es gibt auch einige Hürden zu überwinden, die unter Umständen den Dienst stolpern lassen.

Problem der unbekannten URL

Die Wirksamkeit eines Reputationsdienstes steht und fällt mit der Aktualität der Daten. In einer Zeit, da tagtäglich hunderttausende von Webseiten online geschaltet werden, ist es eine logistische und technische Herausforderung, auch nur annähernd einen aktuellen Datenbestand vorzuhalten. Es ist daher durchaus nachvollziehbar, dass nicht jede URL im Datenbestand des Service vorhanden ist. Dies kann dazu führen, dass für eine URL keine Reputation ausgesprochen werden kann und der Anwender auf eigenes Risiko die Seite besucht (alternativ wird auch angeboten, die Webadresse demnächst zu überprüfen). Im günstigsten Fall ist dies nach einigen Minuten erledigt. Aber welcher Anwender hat schon die Geduld, mehrere Minuten auf ein Reputationsergebnis zu warten?

Problem der Risikoeinschätzung

Ein ausgezeichnetes Tool zur Risikobewertung einer Adresse ist URLVoid [3]. Dieses Tool analysiert auf Anfrage eine Webadresse mit verschiedenen Produkten hinsichtlich ihrer Gefährdung. Im Idealfall zeigen alle Resultate einen identischen Zustand an. Aber wie in Bild 2 ersichtlich, gibt es auch verschiedene Ansichten über die Gefährdung einer Webseite. Welcher Status (CLEAN/DETECTED) wird in der Reputationsdatenbank festgeschrieben? Oder ist es gegebenenfalls besser einen Prozentwert zu speichern? Wobei Letzteres unsinnig ist, denn "Die Webseite ist ein wenig mit Malware infiziert" gibt es nicht. Also auch hier keine leichte Entscheidung für einen Reputationsdienst.

Problem der URL Obfuscation

Obfuscation ist, vereinfacht gesagt, eine Art der Verschleierung. Dabei wird ein beliebiger Text so verändert, dass er für das menschliche Auge nicht mehr lesbar ist. Obfuscation wird zum Beispiel dazu verwendet, um den Diebstahl von Sourcecode zu erschweren. Aber es ist nicht nur möglich, so den Programmcode zu verschleiern, sondern auch URLs. Die einfachste Form besteht darin,

Scanning site with:	AMaDa	DETECTED
Scanning site with:	BrowserDefender	UNRATED
Scanning site with:	DNS-BH	CLEAN
Scanning site with:	Google Diagnostic	CLEAN
Scanning site with:	hpHosts	UNRATED
Scanning site with:	joewein.de LLC	CLEAN
Scanning site with:	Malware Domain List	DETECTED
Scanning site with:	Malware Patrol	CLEAN
Scanning site with:	MyWOT	DETECTED
Scanning site with:	Norton SafeWeb	UNRATED
Scanning site with:	ParetoLogic URL Clearing House	CLEAN
Scanning site with:	PhishTank	CLEAN
Scanning site with:	SURBL	DETECTED

Bild 2: Beim Test einer URL durch URLVoid mit verschiedenen Malware-Scannern ist das Problem, dass keine einheitliche Aussage vorliegt. Einige Produkte stufen die URL als "CLEAN/Ungefährlich" ein, andere entdecken ein Risiko.

die Domainadresse von <http://www.it-administrator.de> als IP-Adresse anzugeben. Das Ergebnis <http://82.197.146.28> ist für einen Anwender wesentlich schwerer zu identifizieren – nicht aber für den Computer. Trickreicher ist es dagegen schon, wenn eine URL mit einem URL-Verkürzungsdienst, wie etwa <http://goo.gl>, ersetzt wird. Denn <http://goo.gl/hLxxx> zeigt ja zuerst auf den URL-Verkürzer selbst und wird von dort erst weitergeleitet auf die verkürzte Zieladresse.

Leider erfreut sich URL-Obfuscation gerade in Kreisen der Cyberkriminalität steigender Beliebtheit. Denn eine verschleierte URL ist schwieriger zu analysieren als eine normale URL und verschafft den Cyberkriminellen einen Vorteil. Die Möglichkeiten, eine URL zu verschleiern, sind dabei durchaus vielfältig. Manche Methoden setzen ein detailliertes Wissen und Programmiererfahrung voraus, bei anderen genügt es vorhandene Tools im Web zu nutzen und zu kombinieren.

URL-Prüfung im Praxistest

Unter diesen Voraussetzungen haben wir uns angesehen, was die Reputationsdienste in der Praxis leisten. Da eine möglichst große Anzahl von Lesern von den Ergebnissen der Untersuchung und

den sich daraus gegebenenfalls ergebenden Produktüberlegungen profitieren sollte, verzichten wir auf den Test einer Gateway-Lösung.

Damit bleiben zwei Kategorien von Lösungsansätzen übrig: Zum einen die Webdienste, wie von M86 [4], Trend Micro [5], McAfee [6] oder auch F-Secure [7] und anderen Anbietern. Die zweite Gruppe sind Browser-Erweiterungen wie von McAfee [8], Web Of Trust [9] oder Trend Micro [10] und anderen Anbietern.

In unseren Untersuchungen verschleierten wir eine anerkannt "böse URL", die von allen getesteten Security-Produkten als solche eingestuft wird:

1. Böse Original-URL im Klartext
2. Original-URL verkürzt mit URL-Verkürzer goo.gl
3. Verkürzte URL aus 2. erneut mit einem anderen URL-Verkürzer bearbeitet
4. Original-URL in Octale-Schreibweise umgewandelt
5. Original-URL als IP-Adresse in Hex-Schreibweise
6. Original-URL mit einem unbekannten URL-Verkürzer verkürzt
7. Verkürzte URL aus 2. mit Obfuscator-Tool aus dem Web verschleiert
8. Original-URL mit Kombi-Tool verkürzt und verschleiert



Ergebnisse der Prüfung einer verschleierte URL durch Reputationsdienste

URL	McAfee Siteadvisor	M86 URL-Analyse	Trend Micro Web Reputation Query
URL 1	Warnung	Warnung	Warnung
URL 2		Warnung	
URL 3			
URL 4	Warnung	Warnung	
URL 5	Warnung	Warnung	
URL 6			
URL 7		FEHLER	
URL 8		FEHLER	

Bei McAfee verwendeten wir die Direktprüfung von www.siteadvisor.de (am rechten Bildschirmrand unter "Site-Bericht anzeigen").

Unerwartet schlecht fielen die Ergebnisse bei den Online-Services aus (siehe Tabelle "Ergebnisse der Prüfung..."). Obwohl die Reputationsdatenbanken aller Hersteller ausgezeichnet gepflegt sind, mangelt es doch an der Interaktion zwischen Web-GUI und dem eigentlichen Service. Anscheinend schlagen bei der Annahme der URL Filtermechanismen zu, welche die eingegebene URL abschneiden und nicht komplett an den Reputations-Service weiterleiten. Bei verkürzten URLs wird beispielsweise nicht die Zieladresse geprüft, sondern der Verkürzungsdienst. Die verkürzte URL wird einfach aus der URL gestrichen.

Alle Services erkannten die verwendete URL als gefährlich, tun sich aber schwer mit der Erkennung, wenn diese verschleiert ist. Wobei aus unserer Sicht ein besseres Ergebnis durch etwas mehr Intelligenz in der Schnittstelle erreicht würde. Allerdings sollte den Anbietern hier kein Vorwurf gemacht

werden, denn wenn heute fünf URL-Verkürzungsdienste implementiert werden, kommen morgen zehn neue hinzu, die alle Erweiterungen umgehen. Web-Reputationsdienste, die eine eingegebene URL bewerten, sind also nur bedingt geeignet, da sie verschleierte URLs teilweise nicht korrekt erkennen.

Wesentlich besser sieht es dagegen bei den Browser-Erweiterungen aus. Hier erkannten die Tools alle URL-Verschleierungen und blockierten diese entsprechend beziehungsweise warnten vor Besuch der Webseite. Dies liegt daran, dass die URL-Obfuscation durchlaufen wird und erst, wenn am Ende eine entsprechend "entschleierte" URL auftaucht, diese dann in der Reputationsdatenbank überprüft wird. Die Klartext-URL wird dann auch gefunden und davor gewarnt. Browser-Erweiterungen sind nicht für URL-Verschleierung anfällig und erkennen gefährliche Seiten besser.

Fazit

Wie eingangs erwähnt, ist ein Web-Reputationsdienst ein zusätzlicher Schutz vor gefährlichen Webseiten. Wer keinen auf seinen Gateway-Systemen betreibt, sollte bevorzugt eine Browser-Erweiterung nutzen, da diese gegen URL-Obfuscation weitestgehend immun ist. Durch die Integration in den Browser ergibt sich zusätzlich der Vorteil, dass Ergebnisse einer Websuche mit Suchmaschinen bei der Anzeige sofort bewertet werden. Die im Web angebotenen URL-Reputationstools funktionieren nur zuverlässig bei einer unverschleierte URL. Wobei dies nicht an einer mangelhaften Reputationsdatenbank liegt, sondern an der technischen Funktionsweise derartiger "Vorschau-Reputationsservices".

Die Technik der Reputation, die sich so wunderbar gegen SPAM bewährt, wirkt also auch im Web. Generell genügt aber ein URL-Reputationsservice allein nicht zur Erkennung und Abwehr der Bedrohungen aus dem Web (nicht jede Webseite hat eine Reputation). Erst im Zusammenspiel von Virens Scanner, AdWare-Plugins und Phishing-Filtern ergibt sich ein akzeptabler Grundschutz. (jp) 

- [1] Malware Domain List
B7P71
- [2] Web Of Trust
B7P72
- [3] URLVoid
B7P73
- [4] M86 (Dieser Dienst wird aktuell überarbeitet und steht daher unter Umständen nicht zur Verfügung)
B7P74
- [5] Trend Micro Site Safety Center
B7P75
- [6] McAfee Check Single URL
B7P76
- [7] F-Secure Browsing Protection
B7P77
- [8] McAfee SiteAdvisor
B7P78
- [9] Web Of Trust Browser Add-on Download
B7P79
- [10] Trend Micro Download TrendProtect
B7P70

Link-Codes

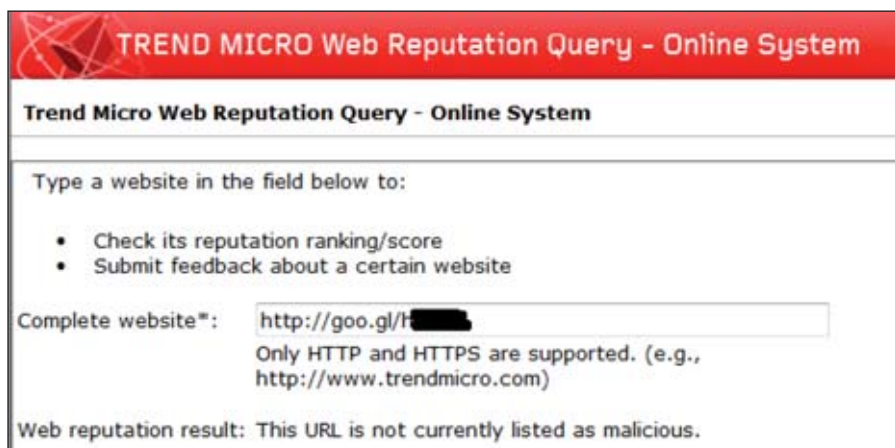



Bild 3: Der Reputationsdienst von Trend Micro findet bei der überprüften URL keinen "Malicious"-Eintrag in der eigenen Reputations-Datenbank

Exchange Server 2010

Verteilerlisten absichern

von Robert Lindermeier

Erfahrene Administratoren wissen, dass es bereits in früheren Versionen des Exchange Server möglich war, die Benutzung von Verteilerlisten einzuschränken. Nehmen wir als Beispiel den Exchange Server 2003. Hier bestand die Möglichkeit, den Versand an eine Liste einzuschränken. So war der Versand nur durch authentifizierte Benutzer möglich (authenticated users only). Dies bedeutet, dass an die Mitglieder der Verteilerliste die Nachrichten nur weitergeleitet werden, wenn der Absender sich korrekt am Exchange Server angemeldet hat, also etwa über Outlook an die Verteilerliste schickt. Kommt die E-Mail an den Verteiler jedoch beispielsweise von extern per SMTP, dann findet keine Zustellung an die Mitglieder der Verteilerliste statt. Dies ist wichtig, falls beispielsweise die SMTP-Adresse in eine Spammer-Datenbank geraten ist.

Mit Exchange Server 2010 haben Sie dieselben Möglichkeiten des Versands nur durch bestimmte Benutzer (Only from oder From everyone except), allerdings noch er-

gänzt durch eine neue Möglichkeit der "Moderation". Dies bedeutet, dass eine Nachricht an eine entsprechend konfigurierte Verteilerliste zuerst zu einem Moderator (ein bestimmtes angegebenes Postfach) gesandt wird, der dann diese Nachricht freigibt.

Sehen wir uns die Verteilerliste (VL) "Alle Mitarbeiter" im Detail an. Dazu öffnen wir die Eigenschaften der Verteilerliste und wechseln auf die Registerkarte "Nachrichtenübermittlungseinstellungen".

Die Eigenschaften "Einschränkungen für die Nachrichtenzustellung" (siehe Bild 2) stehen für sich und sind mit den Einstellungen bei Exchange Server 2003 direkt vergleichbar. Öffnen wir nun die Eigenschaft "Nachrichtenmoderation" (siehe Bild 3) können wir nun einen Empfänger als Moderator einsetzen, der dann beim Versand an diese Verteilerliste eine spezielle E-Mail er-

hält, in der er dem Versand der angehängten Nachricht zustimmt oder diesen gegebenenfalls ablehnt.

Wird nun eine Nachricht an die Verteilerliste erstellt, wird dem Absender bereits im Outlook-Tipp angezeigt, dass die VL moderiert ist und möglicherweise zurückgewiesen wird. Auszuwählen ist auch, ob der ursprüngliche Absender der Mail an die Verteilerliste über eine Ablehnung benachrichtigt werden soll, auch abhängig davon, ob es sich um einen organisationsinternen Empfänger handelt oder nicht. (dr)

Robert Lindermeier ist Inhaber und Senior Managing Consultant bei YOUR-ADMIN.

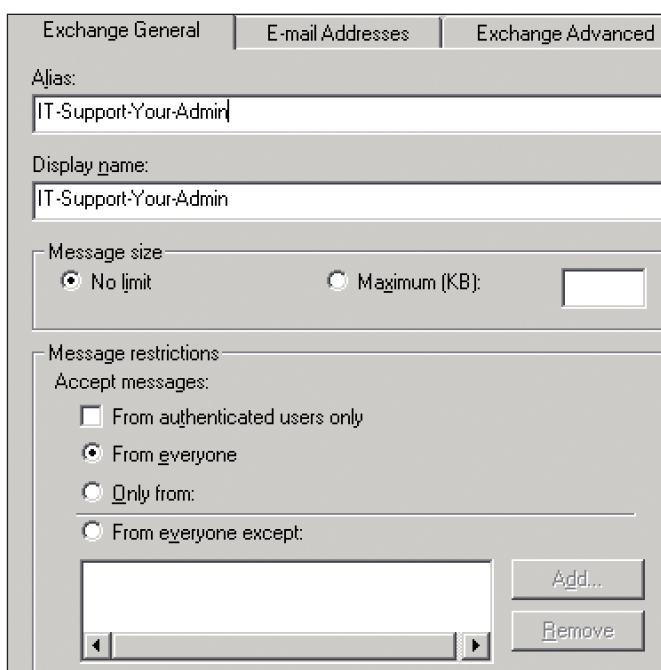


Bild 1: In Exchange 2010 lässt sich der Versand von Verteilerliste einschränken

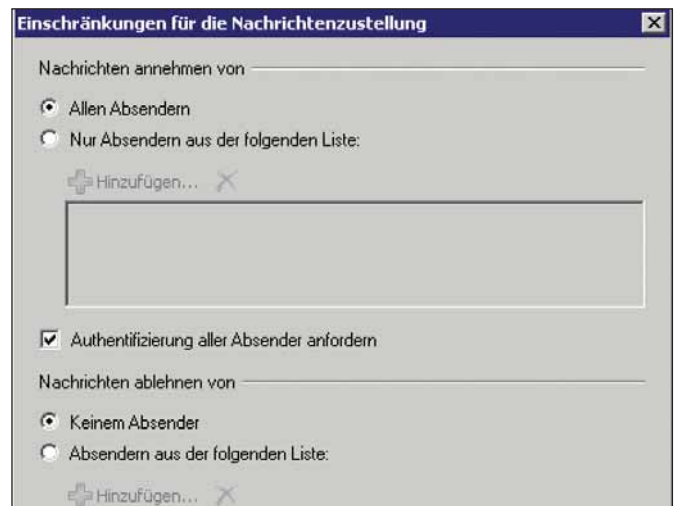


Bild 2: Auch Exchange 2010 bietet Einschränkungen für die Nachrichtenzustellung

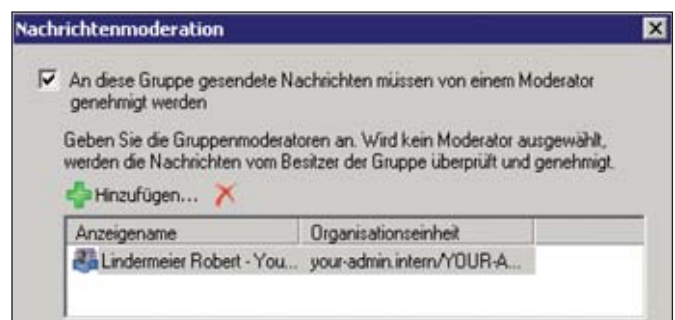


Bild 3: In der Eigenschaft "Nachrichtenmoderation" lässt sich ein Empfänger als Moderator einsetzen



Tipps & Tricks ohne Gewähr

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



Nach einiger Zeit des Testens wollen wir in unserem Unternehmen nun auf Basis von Microsofts **Hyper-V** ein Host zur Virtualisierung aufbauen. Nun haben wir unsere IT bisher jahrelang auf physikalischen Windows-Servern betrieben und dabei ist die **Auslagerungsdatei** ja ein wichtiger Faktor für die Performance der Systeme. Als Leitspruch aus der physikalischen Welt habe ich verinnerlicht, dass pro GByte RAM etwa 2 GByte Plattenplatz für die Auslagerungsdatei zur Verfügung stehen sollten. Heißt das nun, dass ein Hyper-V-Host mit 64 GByte Speicher mit zusätzlich 128 GByte Plattenplatz ausgestattet werden muss?

Sie haben recht, die Dimensionierung der Auslagerungsdatei (Virtual Memory, Pagefile) ist ein wichtiger Performance-Faktor. Aber zu Ihrer Beruhigung lässt sich sagen, dass Sie in einem Hyper-V-Host nicht so viel Plattenplatz benötigen wie Ihre Faustregel errechnet. Um dies zu erläutern, sollten Sie wissen, dass heutzutage Windows automatisch die benötigte Größe des Virtual Memory (*pagefile.sys*) festlegt. Dieser Wert entspricht mindestens dem installierten RAM, maximal dem doppelten Wert. Sollte dieser zur Neige gehen, kann Windows Daten in die Pagefile auslagern. Zwar verfügt auch ein Hyper-V-Host über eine Pagefile, allerdings geht es in diesem Fall rein um die Hyper-V Parent Partition. Da bereits beim Start einer virtuellen Maschine der physikalische Spei-

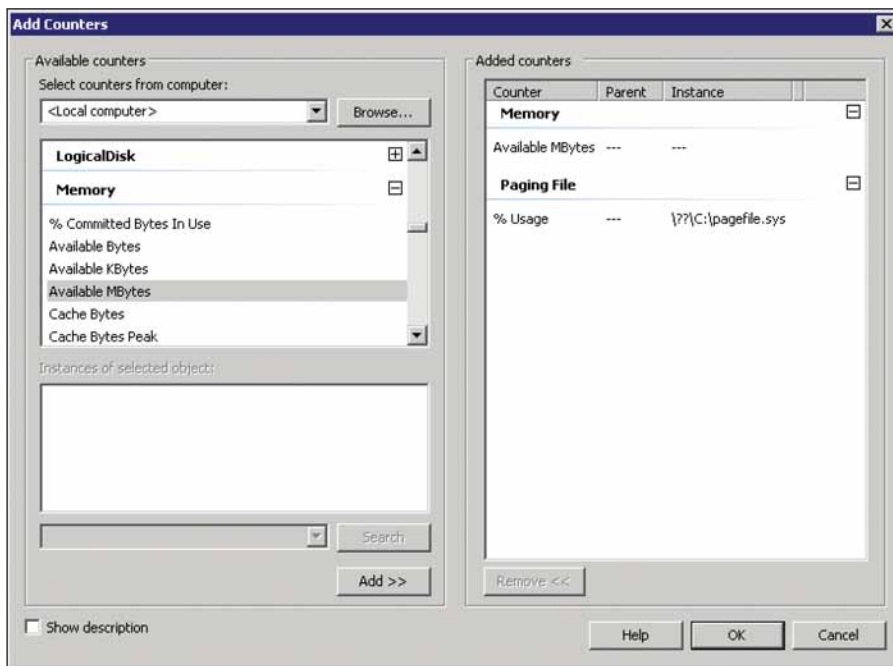
cher zugewiesen wird, steht der Parent Partition jeweils nur der Rest zur Verfügung. Bevor Sie also über den virtuellen Speicher nachdenken, sollten Sie ermitteln, wie viel physikalischen Speicher die Parent Partition benötigt. Dies kann durch verschiedenste Faktoren beeinflusst werden. Daher ist es von großer Wichtigkeit, dass Sie auf einem solchen System nur qualifizierte und effektiv benötigte Management-Software installieren (etwa Management-Agents von SCOM, SCCM, SCVMM oder ähnlichem, Backup-Software, Anti-Virus und nicht viel mehr). Bei der Ermittlung gibt der Windows Task Manager einen ersten Anhaltspunkt (viel mehr Details zu der Auslastung lassen sich allerdings mit dem Sysinternals Process Explorer ermitteln). Im Unterschied zu einem Windows-Server muss bei einem Hyper-V-Host zusätzlich auch ein Overhead für den Hypervisor (300 MByte) und die virtuellen Maschinen berücksichtigt werden. Der Overhead einer VM richtet sich nach dessen Hardware-Konfiguration, konkret nach dem zugewiesenen Memory. Für das erste GByte virtuellen Speichers werden 32 MByte und für jedes zusätzliche nochmals je 8 MByte benötigt. Dies lässt sich anhand der folgenden Beispiele besser veranschaulichen:

- Guest mit 2 GByte RAM = 40 MByte an Overhead
- Guest mit 4 GByte RAM = 56 MByte an Overhead
- Guest mit 8 GByte RAM = 88 MByte an Overhead

Damit die Parent Partition auch über die benötigten Ressourcen verfügen kann,

sollte eine "Memory Reserve" konfiguriert werden. Dort wird der physikalische Speicher für die Parent Partition reserviert. In der Regel liegt der Bedarf bei einem Hyper-V-Host bei etwa 2 GByte. Diese Konfiguration wird in der Registry vorgenommen. Bei einem Hyper-V Failover Cluster kann dies auch mittels PowerShell konfiguriert werden: (*Get-Cluster MyCluster*).*RootMemoryReserved=2048* (mit SP1 wird diese Einstellung allerdings hinfällig). In der Registry von Windows Server 2008 und 2008 R2 öffnen Sie dazu den Schlüssel HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Virtualization und setzen den DWORD-Wert "RootMemoryReserve" auf "2048". Unter Windows Server 2008 R2 SP1 setzen Sie den selben Wert unter HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Virtualization beim Schlüssel "MemoryReserve". Um nun die Größe der Pagefile zu ermitteln, ist es notwendig, das Paging-Verhalten eines Servers mit dem Performance Monitor zu analysieren. Dazu benötigen Sie die beiden Werte "Pagefile - % Usage" und "Memory - Available Mbytes". Dies kann auch mit *logman.exe* in der Kommandozeile, zum Beispiel bei Server Core, durchgeführt werden:

```
logman.exe create counter Pagefile-Counter-Log -o "c:\perflogs\Page-File_Sizing.blg" -f bincirc -v mmdhmm -max 250 -c "\Memory\*" "\Paging File(*)\*" "\Process(*)\*" -si 00:00:15C:\> logman.exe start Pagefile-Counter-Log
```



Zur Ermittlung der richtigen Größe der Auslagerungsdatei sind im Performance Monitor zwei Counter zu überwachen

Die Daten sollten Sie über einen Zeitraum von mindestens einer Woche sammeln. Danach kann mit *logman.exe stop Pagefile-Counter-Log* die Analyse wieder gestoppt werden. Die Einstellungen der Pagefile nehmen Sie bei einer normalen Installation über die GUI wie gewohnt in den System-Eigenschaften vor. Nur bei Server Core muss dabei auf WMI zurückgegriffen werden. Zunächst muss allerdings die automatisch verwaltete Pagefile deaktiviert werden, da sonst die neue Pagefile nicht angelegt werden kann. Der Befehl würde mit "No Instance(s) available" fehlschlagen.

```
wmic computersystem set AutomaticManagedPagefile=False
```

Um eine Pagefile von zum Beispiel 10 GByte zu konfigurieren, nutzen Sie folgenden Befehl:

```
wmic pagefileset where name="C:\\pagefile.sys" set InitialSize=10240,MaximumSize=10240
```

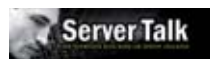
Viele weitere Tipps & Tricks sowie konkrete Hilfe bei akuten Problemen bekommen Sie auch im Internet bei unserem exklusiven Foren-Partner administrator.de. Über 60.000 registrierte Benutzer tauschen dort in über 100 Kategorien ihre Erfahrungen aus und leisten Hilfestellung. So wie der IT-Administrator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

www.administrator.de



Bei Hosts mit wenig Memory (< 32 GByte) kann, sofern genügend Plattenplatz vorhanden ist, auch bedenkenlos die Einstellung des Virtual Memory auf "System Managed" belassen werden. In der Vergangenheit hat sich ein Pagefile von 10 GByte sehr gut bewährt, was auch als Standard zu empfehlen ist. (Michel Lüscher/jp)

Link-Code:: B7PE1



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

Wenn ich unter **Windows 7** einen Ordner per Drag&Drop in die Taskleiste ziehe, wird dieser ja automatisch dem Explorer-Symbol als "Angeheftet" hinzugefügt. Mit einem Klick mit der rechten Maustaste auf das Explorer-Symbol greife ich so über die Sprungliste auf die häufigsten Ordner und die angehefteten Ordner zu. Das ist alles recht praktisch, nur fehlt mir dabei die Möglichkeit, eigene Symbole in die Taskleiste aufzunehmen. Haben Sie dazu einen Tipp für mich?

Ja, es gibt eine Möglichkeit, für einzelne Ordner eigene Symbole in der Taskleiste aufzunehmen. Der Vorteil ist, dass Sie diese Ordner dann nicht über das Explorer-Symbol aufrufen müssen, sondern ein eigenes Symbol für den Ordner mit eige-

nem Icon erstellen können. Dazu erstellen Sie über das Kontextmenü des Desktops eine neue Textdatei und geben dieser Datei die Bezeichnung, unter der der Ordner später in der Taskleiste erscheinen soll (und die Endung *.exe). Achten Sie darauf, dass die Datei auch ausführbar sein muss. Klicken Sie die neue ausführbare Datei mit der rechten Maustaste an und wählen Sie "An Taskleiste anheften". Öffnen Sie als Nächstes den übergeordneten Ordner des Verzeichnisses im Explorer, den Sie über das neue erstellte Symbol in der Taskleiste öffnen wollen. Handelt es sich dabei um ein Verzeichnis innerhalb des Benutzerprofils, klicken Sie im Startmenü auf Ihren Benutzernamen. Halten Sie dann die Shift-Taste gedrückt und klicken Sie mit der rechten Maustaste den Ordner an, den Sie mit dem Symbol in der Taskleiste öffnen wollen und wählen "Als Pfad kopieren". Im Grunde genommen geht es bei den letzten beiden Punkten darum, den Pfad des Verzeichnisses, das Sie mit dem Symbol in der Taskleiste öffnen wollen, in die Zwischenablage zu kopieren. Den echten Pfad eines Verzeichnisses im Explorer sehen Sie auch, wenn Sie in der Adressleiste ganz links auf das Symbol des Ordners klicken. Klicken Sie als Nächstes das neu erstellte Symbol in der Taskleiste mit der rechten Maustaste an, um dessen Sprungliste aufzurufen. Klicken Sie dann den Namen des Programmes mit der rechten Maustaste an und rufen Sie Eigenschaften auf. Geben Sie auf der Registerkarte "Verknüpfung" im Feld "Ziel" den Pfad des Ordners an, den Sie öffnen wollen. Wichtig ist, dass es sich um den physischen Pfad des Verzeichnisses handelt, nicht den Anzeigenamen im Explorer. Über die Schaltfläche "Anderes Symbol" wählen Sie noch ein passendes Icon für den Ordner aus. Das neue Icon erscheint aber erst nach dem Neustart des Rechners. Wollen Sie die Anzeige beschleunigen, öffnen Sie den Taskmanager, wechseln auf die Registerkarte "Prozesse" und beenden den Prozess Explorer. Anschließend startet das System den Explorer neu und verwendet dann auch das neue Symbol. Die ausführbare Datei auf dem Desktop können Sie löschen, diese benötigen Sie nicht mehr. Klicken Sie zukünftig auf das Icon in der Taskleiste, öffnet sich das Verzeichnis, das in den Eigenschaften festge-

legt ist. Das kann wesentlich sinnvoller sein, als über angeheftete Ordner im Explorer zu arbeiten. (jp)



Bei unserer routinemäßigen, quartalsweisen Überprüfung der **Software-Lizenzen** in unserem Unternehmen stießen wir bei **XenDesktop** auf Probleme. Nach mehrmaliger Überprüfung der in XenDesktop angegebenen Zahlen sind wir sicher, dass das Programm einen falschen Wert bei der Anzahl der überschrittenen Lizenzen zeigt. Woran liegt das und wie lässt sich das Problem beheben?

Das Problem tritt ausschließlich bei Kunden auf, die das so genannte Citrix Subscription Advantage-Abonnement vor dem 2. März 2011 erneuert haben. Hier kommt es vereinzelt zu fehlerhaften Werten in der Lizenzierungsdatei. Im Normalfall sollten im Rahmen des Abos allen Kunden 10 Prozent mehr Lizenzen zur Verfügung stehen als gekauft wurden. In der "License Administration Console" können Anwender die Lizenzen dahingehend überprüfen. Sollte die Zahl der zugewiesenen Lizenzen nicht übereinstimmen, schafft das My Citrix-Portal Abhilfe. Hier kann die Zahl der Lizenzen neu berechnet und gegebenenfalls eine aktualisierte Lizenzierungsdatei zugeteilt werden. Dazu sind folgende Schritte nötig: Nach dem Login bei My Citrix ist in der Toolbox zunächst die Rubrik "Activation System/Manage Assets" auszuwählen. Im "Reallocate"-Tab geben Sie im Anschluss nur noch die abgefragten Informationen ein. Danach steht Ihnen die neue Lizenzierungsdatei direkt zum Download zur Verfügung. Im letzten Schritt muss lediglich die alte Lizenz-Datei auf dem Lizenz-Server durch die neu erstellte Version ersetzt werden. (Citrix/jp)



Linux

Ich arbeite sehr viel auf der Linux-Kommandozeile, wechsele dabei jedoch oft in einen Browser, um bestimmte Begriffe in der Wikipedia nachzuschlagen. Gibt es hierfür nicht auch einen bequemeren Weg?

Hierfür gibt es eine einfache Lösung: Da Wikipedia einen XML-Dump aller Einträge ermöglicht, hat David Leadbeater diese Dumps in eine SQL-Datenbank importiert, die als Backend von seinem DNS-Server verwendet wird. Dieser stellt nun sämtliche Einträge als DNS TXT-Records zur Verfügung. Durch eine einfache DNS-Abfrage können Sie nun sämtliche Wikipedia-Einträge von der Kommandozeile aus abfragen:

```
# dig -t txt +short redhat.wp.dg.cx
"In computing, Red Hat, Inc. is a
company in the free and open source
software sector, and a major
Linux distribution vendor. Founded
in 1995 ...
/a.vu/w:Red_Hat"
```

Über eine einfache Bash-Funktion funktioniert die Abfrage noch eleganter:

```
wiki () { dig +short txt
$1.wp.dg.cx }
```

Um eine Abfrage zu starten, ist der Funktion einfach der gesuchte Begriff als Argument zu übergeben: `# wiki redhat.` (Thorsten Scherf/jp)

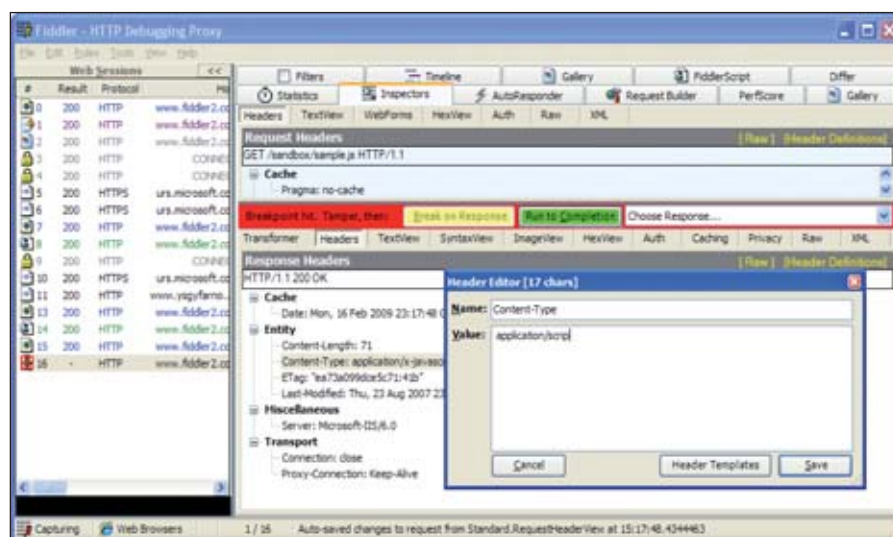


Tools

Viele IT-Abteilungen scheuen den Einsatz von **Netzwerk-analyse-Tools**, da diese oft komplex zu bedienen sind und in ihren Ergebnissen eine wahre Lawine von Daten liefern. Denn deren Auswertung und somit die zielgerichtete Fehlersuche sind extrem zeitaufwändig. Wenn jedoch das Netzwerkprotokoll, auf dem der Fehler vermutet wird, **HTTP** beziehungsweise **HTTPS** ist,

kann es sinnvoll sein, ein hierauf spezialisiertes Werkzeug einzusetzen. Dies macht Sinn, wenn der IT-Verantwortliche Probleme mit der Firmenwebsite untersucht – und auch für **Outlook**.

Die Suche nach **Fehlern im Netzwerk** kann bei der Verwendung eines umfassenden Netzanalyse-Tools wie beispielsweise Wireshark insofern sehr zeitaufwändig sein, als dass ein solches Tool den kompletten Datenverkehr mitschneidet und dem Administrator entsprechend umfangreiche Daten präsentiert. Ist jedoch bekannt, dass sich die Fehlerquelle im **HTTP/HTTPS-Protokoll** abspielt, ist das kostenlose Tool **Fiddler** ein sehr hilfreiches Werkzeug. Fiddler platziert sich als **lokaler Proxy-Server** zwischen dem Browser und dem Internet, um alle HTTP(S)-Pakete aufzuzeichnen und sie dem Administrator zur Analyse zur Verfügung zu stellen. Und Fiddler kann Pakete auch modifizieren oder komplett neue erstellen. Besonders Exchange-Admins sollten dieses Tool in ihre Werkzeugsammlung aufnehmen, da es erlaubt, auch Anfragen von Outlook-Clients an den Server zu monitoren. Darüber hinaus stehen für Fiddler eine ganze Reihe von Add-Ons für Spezialaufgaben bereit. Dabei ist die Arbeit mit Fiddler schnell erlernt: das Tool zeigt in einem Fenster alle mitgeschnittenen Pakete an. Wählt der Anwender eines aus, erscheinen alle Details dazu in einem zweiten Fenster. Interessant ist der Reiter "Inspectors", der erlaubt, den Inhalt des Datenpakets in verschiedenen Ansichten



Virtuos wie ein meisterhafter Geigenspieler: Fiddler überwacht den HTTP-Verkehr und kann so unter anderem Outlook-Problemen auf die Spur kommen



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

zu analysieren (etwa als Rohdaten, als Webformular oder als XML). Werden mehrere Pakete ausgewählt, zeigt der Reiter "Statistic" eine Übersicht der Datenmenge und Timing-Details. Fiddler ist mit 600 KByte erfreulich klein und unterstützt Windows 2000 bis Windows 7. Das Tool setzt das .NET Framework 2.0 oder höher voraus. Bei den Browsern Internet Explorer, Google Chrome, Apple Safari und Opera sind nach der Installation keine weiteren Einstellungen nötig. Lediglich bei Firefox müssen unter "Einstellungen / Erweitert / Netzwerk" die Verbindungseinstellungen manuell auf den HTTP-Proxy unter der lokalen IP-Adresse 127.0.0.1 und Port 8888 umgestellt werden. Allerdings erhält Firefox dann nur noch eine Verbindung, wenn Fiddler läuft. (jp)

Link-Code: B7PE2

Stark ausgelastete Windows-Computer, auf denen mehrere Applikationen gleichzeitig um die verfügbare CPU-Zeit ringen, sind nichts Besonderes. Auf der einzelnen Workstation ringen Videosoftware, Brennerprogramm und Desktopsuche-Lösungen um die wertvolle Prozessorzeit. Auf Windows-Terminalservern sind es die verschiedenen Applikationen wie Microsoft Access, Excel oder im Hintergrund gestartete Backup-Tasks, die um eine zügige Abarbeitung kämpfen. Die Zuweisung der CPU-Zeiten übernimmt das Betriebssystem – hier Windows 2000 und höher.

Process Arbiter heißt ein kostenloses Tool aus dem Hause SINN GmbH. Das kleine Programm **beschleunigt messbar die Reaktionsgeschwindigkeit** von stark frequentierten Windows-Com-

putern und besticht durch eine administrationslose Oberfläche. Um die Reaktionszeiten von Programmen zu beschleunigen, verwendet der Process Arbiter einen einfachen wie genialen Mechanismus des Betriebssystems: die Prozesspriorität. Üblicherweise stellen Administratoren diese für einzelne Programme zur Laufzeit herunter, um die Reaktionsgeschwindigkeit einer Windows-Maschine zu erhöhen. Der Process Arbiter übernimmt diesen Vorgang vollautomatisch. Das als Windows-Dienst mit der Microsoft .NET Managed API erstellte Werkzeug benötigt nicht einmal Einstellungen von Seiten des Benutzers oder des Administrators. (jp)

Link-Code: B7PE3

Für Administratoren, die kleine Außenstellen betreuen, oder Berater, die spontan einen Überblick über die IT-Landschaft ihres Kunden benötigen, bietet sich die Nutzung eines Smartphones geradezu an. Denn wer eigentlich nur einen Routinebesuch vor Augen hatte und nun mehr Daten als erwartet über die Systeme benötigt, ist mit einem kleinen Helfer gut bedient.

Für mobile Admins bietet sich die kostenlose App "FCS Scanner" der FCS Fair Computer Systems GmbH an. Diese steht für Smartphones und Tablets mit Android-Betriebssystemen (ab Version 2.2) zur Verfügung. Die App ermöglicht das Auslesen wichtiger Informationen zum mobilen Kommunikator, wie zum Beispiel Hersteller, Modell, Seriennummer, CPU, Betriebssystem, Speichergröße, Telefondaten, Kamera et cetera. Der FCS Scanner ist zweisprachig verfügbar und passt sich automatisch an die Culture des Geräts an. Die gesammelten Daten lassen sich in einer Ergebnisdatei (XML) per E-Mail an eine hinterlegte Adresse versenden. Der FCS Scanner kann nach einer Registrierung beim Hersteller über unseren Link-Code bezogen werden und steht als kostenfreie App im Android Market von Google zur Verfügung. (jp)

Link-Code: B7PE4

Bei manchem Administrator steht öfter, als ihm lieb ist, die Analyse von Log-Dateien auf der Tagesordnung. Unbeliebt ist diese Tätigkeit auch deshalb, weil eine struktu-

rierte Suche in derlei Dateien oft mühsam ist. Zudem wäre es oft hilfreich, wenn der IT-Verantwortliche auch während der Logfile-Analyse neu eintreffende Log-Einträge sehen und so in seine Analyse einbeziehen könnte.

Das kostenlose Werkzeug BareTail hilft bei diesem altbekannten Problem. BareTail ermöglicht dem Administrator, Log-Files in Echtzeit zu überwachen – selbst, wenn diese zum Zeitpunkt der Betrachtung in BareTail noch wachsen. Darüber hinaus bringt das Werkzeug einige äußerst hilfreiche Features für das Auswerten von Log-Dateien mit:

- Ansicht von Dateien beliebiger Größe (> 2 GByte)
- Blättern zu einem beliebigen Punkt in der Datei
- Dateiansicht im Netzwerk
- Konfigurierbare Zeilenumbrüche, Tab-Erweiterungen und Schriftarten

Im "Follow The Tail"-Modus kann der Administrator die neu hinzukommenden Einträge einer Datei in Echtzeit betrachten – egal, wie schnell die Datei wächst. Zudem erlaubt BareTail dies auch für mehrere Dateien simultan. Zur verbesserten Übersichtlichkeit der eigenen Auswertung stehen dem Anwender frei konfigurierbare Hervorhebungen zur Verfügung, um wichtige Textpassagen zu kennzeichnen und nachzuverfolgen. Zu den unterstützten Dateiformaten zählen Windows-/DOS-Textdateien, UNIX-Textdateien und Microsoft IIS-Logfiles. Bei dem Werkzeug handelt es sich um eine kleine ausführbare Datei, die keine Installation erfordert. (jp)

Link-Code: B7PE5



BareTail erlaubt die Echtzeit-Analyse von Log-Dateien

Stratus Avance bei Röchling Automotive in Wolfsburg

Der Hochverfügbarkeit Tür und Tor geöffnet

von Dr. Rainer Doh



Quelle: Vistry - Fotolia.com

Gerade einmal 120 bis 210 Minuten hat Röchling Automotive als Automobilzulieferer in Wolfsburg Zeit, um einen kompletten Satz von Türverkleidungen für die VW-Modelle Touran, Tiguan und Golf zu produzieren – vom Spritzen des Kunststoffrahmens über das Einbauen von Ausstattungsvarianten wie Fensterheber und Lautsprecher bis zur Abnahme. Auf diese Weise produziert Röchling in seinem Werk in Wolfsburg im Drei-Schicht-Betrieb rund um die Uhr Türverkleidungen für rund 2.000 Fahrzeuge. Diesem engen Zeitrahmen folgend, ist Röchling auf die Verfügbarkeit seiner IT-Infrastruktur und insbesondere der Server essentiell angewiesen. Mit Stratus Avance hat das Unternehmen nun eine hochverfügbare Virtualisierungslösung mit zwei synchronen Servern implementiert, die nur geringen Administrationsaufwand erfordert.

Im benachbarten VW-Werk gibt es für Komponenten, wie sie Röchling herstellt, so gut wie keine Lagerhaltung mehr. Die benötigten Stückzahlen der Türverkleidungen werden in wechselnden Konfigurationen abgerufen und müssen dann sofort produziert werden. Nach der vorgegebenen Produktionszeit steht schon ein LKW bereit, der sie zum VW-Werk fährt, wo sie verbaut werden. Dabei kommt es nicht nur auf die zeitgenaue Herstellung an, die Komponenten müssen auch in einer genau vorgegebenen Reihenfolge bereitgestellt werden. Nicht nur die drei Fahrzeugmodelle sind dabei zu unterscheiden, sondern für jedes Modell auch rechte und linke Türen, Vorder- und Hintertüren sowie diverse Farb- und Ausstattungsvarianten. Eine Produktion auf Vorrat ist daher nicht möglich. Die fertigen Teile

müssen für die Lieferung so zusammengestellt werden, dass die Arbeiter, die die Fahrzeuge bei VW am Band zusammenbauen, ohne nochmalige Überprüfung mit einem Griff in den von Röchling gelieferten Container immer die richtigen Bauteile in der Hand halten.

Röchling Automotive muss also nicht nur just in time, sondern auch just in sequence produzieren – Teile unterschiedlicher Art in einer exakt vorgeschriebenen Reihenfolge. Im VW-Werk läuft die Produktion der Fahrzeuge nur dann reibungslos, wenn der Zulieferer die passenden Komponenten entsprechend der Produktionsplanung bereitstellt. Hätte Röchling Automotive einen Bandstillstand bei VW zu verantworten, so würden Konventionalstrafen und Imageverlust drohen.

Stunden für den Abgleich der Datenbank

Entsprechend unternehmenskritisch sind die IT-Prozesse, mit denen Röchling die Produktion steuert. Die Übernahme der Aufträge von VW per EDI (Electronic Data Interchange), die Weitergabe an die Produktion, die Überwachung des Produktionsablaufs und die Zusammenstellung der Komponenten in Racks bis zur Übergabe der fertigen Bauteile am Warenausgangspunkt und der Rückmeldung an das SAP-System wird von einem Datenstrom begleitet, der nicht unterbrochen werden darf. Durch laufendes Einscannen von Barcodes, die sich auf allen Teilen, Behältern und Maschinen befinden, wird sichergestellt, dass sich Daten und physische Bauteile entsprechen.

Von der Verfügbarkeit der IT hängt die Arbeitsfähigkeit des gesamten Werks ab.

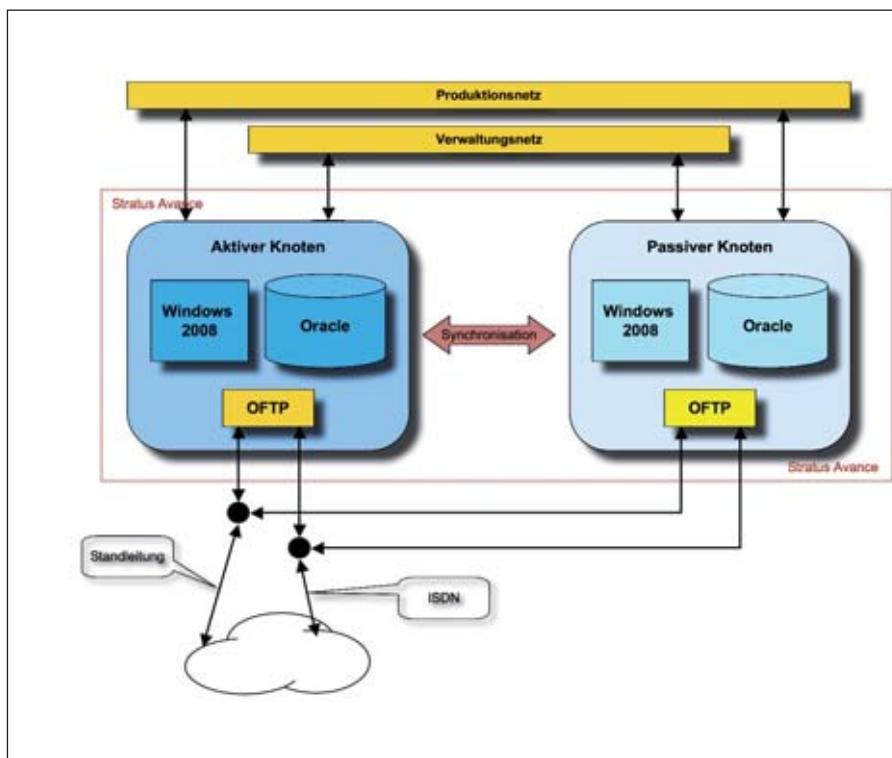


Bild 1: Schematische Darstellung der Röchling IT-Infrastruktur nach der Einführung des Hochverfügbarkeits-Werkzeugs

“Kommt es zu einer Unterbrechung, zu einem Stillstand oder Ausfall des Servers, dann sind wir praktisch blind”, sagt Atila Güner, Systemverantwortlicher bei Röchling Automotive in Wolfsburg. “Wir können nur noch das abarbeiten, was bereits auf den Arbeitspapieren aus-

gedruckt ist.” Auch nach einer kurzzeitigen Unterbrechung müssten die Systeme manuell nachgeführt und auf den aktuellen Stand gebracht werden – ein überaus aufwändiges und auch fehlerträchtiges Unterfangen.

Administration und Fehlerbehebung sind ohnehin kritische Punkte: Da die Systeme 7x24 Stunden verfügbar sein müssen, besteht lediglich am Sonntag zwischen 14 und 18 Uhr ein Wartungsfenster, in dem dann sämtliche administrativen Aufgaben wie Softwarepflege oder Datenbereinigungen erledigt werden müssen. Viel Zeit für die Beseitigung eventueller Fehler oder Inkonsistenzen bleibt da nicht mehr. “Wir sind essentiell darauf angewiesen, dass unsere IT störungsfrei läuft”, erklärt Güner. Bisher hatte Röchling Automotive seine IT durch ein Stand-by-System abgesichert – ein Server stand in Reserve und wurde im Störfall zugeschaltet.

Allerdings dauerte es viel zu lange, bis das Ersatzsystem produktiv arbeitete, so dass von einem reibungslosen Umschalten auf den Notbetrieb nicht die Rede sein konnte. Da die Daten des passiven Systems nur in größeren Abständen ab-

Die weltweit operierende Röchling-Gruppe steht mit 6.000 Mitarbeitern an 54 Standorten in 20 Ländern für “Kompetenz in Kunststoff”. Mit ihren beiden Geschäftsbereichen Hochleistungs-Kunststoffe und Automobil-Kunststoffe konzentriert sie sich auf die Verarbeitung hochwertiger Kunststoffe zu Halbzeugen, Teilen und Systemen für eine Vielzahl industrieller Anwendungen.

Die Röchling Automotive-Gruppe mit Hauptsitz in Mannheim ist mit 3.200 Mitarbeitern weltweit Partner von Automobilherstellern und Systemlieferanten. Das Unternehmen verfügt über vier Entwicklungsstandorte und 21 Fertigungsstätten auf vier Kontinenten. Weitere deutsche Standorte sind Worms, Gernsbach, Wackersdorf, Peine und Wolfsburg. Zu den Kernkompetenzen von Röchling Automotive gehören die Aerodynamik und Akustik in jedem Segment eines Fahrzeugs sowie Fluidkomponenten und Interieursanwendungen, bei denen es neben einem hohen Maß an Funktionsintegration um Kosteneffizienz und um das Thema Leichtbau geht.

Die Röchling-Gruppe



Worüber Administratoren morgen reden

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

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

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

Jetzt einfach und kostenlos bestellen unter:



www.it-administrator.de/newsletter

geglichen wurden, waren bei Störungen Datenverluste unvermeidlich. "Der Abgleich einer Oracle-Datenbank, bei dem die Datenbanken auf den beteiligten Rechnern wieder in Übereinstimmung gebracht werden, kann viel Zeit in Anspruch nehmen", führt Güner dazu aus. "Auch wenn wir unterdessen wieder auf die aktuell hereinkommenden Informationen zugreifen und somit weiterarbeiten konnten, so bedeutete das, dass die Datenbank nicht mehr synchron war. Wir mussten dann mit großem Aufwand die Daten abstimmen und dafür sorgen, dass der Betrieb wieder komplett rund lief."

Der passende Weg zur Hochverfügbarkeit

Mitte 2010 ersetzte Röchling Automotive diese Konfiguration im Rahmen einer Runderneuerung seiner IT-Systeme durch eine hochverfügbare Lösung. Auf zwei High-Performance-Servern von HP wurde vom Braunschweiger Systemhaus MTS die Hochverfügbarkeits- und Virtualisierungslösung Stratus Avance implementiert. MTS hat als Implementierungspartner außerdem die Migration des Altsystems und seiner Anbindungen übernommen und das Projekt von der umfangreichen Beratung bis zur vollständigen Abnahme des Gesamtsystems mit allen zugehörigen Failover-Tests betreut.

Die beiden Server befinden sich in weit auseinanderliegenden Räumen und sind damit auch gegen Havarie-Fälle abgesichert. Die Avance-Software synchronisiert die beiden technisch gleich aufgebauten Server permanent, so dass das aktive und das passive System immer auf dem gleichen Stand sind, sowohl hinsichtlich des jeweiligen Status der Anwendungen als auch hinsichtlich der Datenbank selbst.

Die Koppelung erfolgt durch eine dedizierte Verbindung, beide Server arbeiten daher trotz ständiger Synchronisation mit hoher Performance. Stellt Avance eine Störung – beispielsweise in einem Speicherbaustein oder auf einer Platte – oder den Ausfall eines Systems fest, so wird der Workload automatisch

vom anderen System übernommen. Der Betrieb wird dabei ohne nennenswerte Unterbrechung fortgeführt, die Nutzer merken von der Störung in der Regel nichts; der Administrator erhält eine automatische Benachrichtigung über den Fehler und kann sich dann stressfrei um dessen Behebung kümmern.

Avance erlaubt das Anlegen virtueller Server, beispielsweise für die Applikationen und die Datenbank. Auf diese Weise konnte Röchling Automotive seine Systeme gegen etwaige Ausfälle schützen und hochverfügbar machen. "Wir haben es ausprobiert und bei einem System einfach mal den Stecker gezogen", berichtet Güner. "Der Schwenk zum anderen Server ging automatisch und reibungslos. Der Partner-Server hat die Prozesse übernommen und die Anwendungen waren auch während des Wechsels verfügbar. Wir haben hinterher in der Datenbank keinen einzigen Fehler gefunden."

Da Avance die Datenbanken ständig synchronisiert und beide bis zum Augenblick des Fehlers auf demselben Stand sind, dauert auch der Abgleich der Datenbanken nach dem Wiederanlaufen des ausgefallenen Systems nicht lange. "Spätestens nach einer halben Stunde laufen die beiden Server wieder synchron", führt Güner weiter aus. Damit kehrt das Gesamtsystem schneller wieder in den hochverfügbaren Zustand zurück, denn während der Phase des Hochfahrens und der Rekonstruktion der zweiten Maschine ist ja nur ein Server voll verfügbar.

Erleichterungen bei der Administration

Obwohl die Konfiguration zwei physisch getrennte Maschinen umfasst, ist nach außen nur ein einziges System sichtbar, was die Administration erheblich vereinfacht. "Mit Avance hat sich die Arbeit mit unserem System erheblich entspannt", stellt Güner fest. "Avance bietet uns eine ganz einfache Verwaltungsoberfläche sowohl für die Verfügbarkeit als auch für die Virtualisierung. Das erlaubt es uns, das ganze System auch remote zu administrieren. Ich kann beispielsweise bei Störungen von zu Hause aus nachsehen, was passiert ist. Da die Sys-

teme vollständig doppelt implementiert wurden, muss auch nichts umgesetzt oder manuell eingestellt werden. Früher musste ich mich in solchen Fällen auf den Weg ins Werk machen, was nicht nur umständlich ist, sondern auch wertvolle Zeit kostete." Vor allem im Dreischicht-Betrieb ist die Remote-Administration ein wichtiger Vorteil und trägt nicht unwesentlich zur Sicherung der Betriebsbereitschaft bei.

Auch das enge Wartungsfenster stellt nun kein Problem mehr dar. Zum einen ist die Gesamtperformance durch die leistungsfähigeren 64-Bit-Quad-Core-Server und eine sorgfältige Konfiguration aller Komponenten, insbesondere der Festplatten, deutlich gestiegen, so dass grundsätzlich alle Vorgänge schneller ablaufen, zum anderen kann durch die einfachere Administration die verfügbare Wartungszeit besser genutzt werden.

Natürlich wurden bei Röchling Automotive in Wolfsburg auch Alternativen zu Stratus Avance geprüft. Ein Cluster-System, das das Unternehmen bereits früher im Einsatz hatte, schied wegen der aufwändigen Administration aus. Auch eine Lösung auf Basis der Virtualisierungs-Software VMware hätte einen deutlich höheren Betreuungsaufwand verlangt. Vor allem aber hätte Röchling Automotive hier mit erheblich höheren Kosten rechnen müssen. "Sowohl bei einem Cluster-System als auch bei VMware hätten wir ein SAN implementieren müssen", erläutert Güner.

"Aus Gründen der Hochverfügbarkeit hätten wir dieses SAN spiegeln, also zwei SANs implementieren müssen. Unterm Strich wären damit unsere Investitionen für dieses Projekt etwa doppelt so hoch ausgefallen, denn mit Avance können wir das lokale RAID-System nutzen." So hat Röchling Automotive eine sehr leistungsstarke, hoch verfügbare Virtualisierungslösung erhalten, die sich mit geringem Aufwand verwalten lässt. "Eigentlich genau das, was wir uns immer gewünscht hatten", resümiert Güner. (jp)

Dr. Rainer Doh ist freier Redakteur in München.



Liefertermin:
Ende Oktober 2011

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

180 Seiten Praxis-Know-how rund um das Thema

SharePoint 2010 für Administratoren

zum Abonnenten-Vorzugspreis* von

nur € 24,90!

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

Mehr Informationen und ein Onlinebestellformular finden Sie auch hier

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



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

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

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

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

Ich zahle ☐ per Bankeinzug

Geldinstitut: _____

Kto.: _____

BLZ: _____

oder ☐ per Rechnung

Datum: _____

Unterschrift: _____

Firma: _____

Name, Vorname: _____

Straße: _____

Land, PLZ, Ort: _____

Tel: _____

E-Mail: _____

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

So erreichen Sie unseren
Vertrieb, Abo- und
Leserservice:

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

Tel: 06123/9238-251

Fax: 06123/9238-252

leserservice@it-administrator.de

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



Heinemann Verlag

Leopoldstraße 85

D-80802 München

Tel: 089-4445408-0

Fax: 089-4445408-99

Geschäftsführung:

Anne Kathrin Heinemann

Matthias Heinemann

Amtsgericht München HRB 151585

ITA 0711

Hochverfügbarkeit in komplexen Storage-Architekturen

Doppelt hält besser

von Johannes Wagmüller



Quelle: 123RF

Immer mehr Applikationen, Workloads und Unternehmensdaten werden virtualisiert und auf gemeinsam genutzten (shared) Speicherinfrastrukturen konsolidiert. Größere User- und Applikationsgruppen benötigen eine genaue Koordination der Downtime für Upgrades oder Erneuerungen der Hardware, um ungewollte Ausfälle zu vermeiden. Darüber hinaus steigt die Auswirkung eines potenziellen Ausfalls bei erhöhter Applikations- und Servicekonzentration auf den Systemen enorm. Die zunehmende Verfügbarkeitsanforderung erhöht dabei die Kosten für das Aufrechterhalten der Service-Level. Die Komplexität der IT-Infrastruktur wächst, und es treten mehr potenzielle Fehlerquellen auf. Bedienungs- und Applikationsfehler gelten als häufigste Gründe für Betriebsunterbrechungen.

Zentrale Voraussetzung für die Vereinfachung der Produktivumgebung, aber auch der Disaster-Recovery-Struktur ist die Konsolidierung der Daten auf einer möglichst einheitlichen Storage-Architektur. Networked Storage in Verbindung mit Server-Virtualisierung ist eine Investition, die sich sehr schnell amortisiert. Der Vorteil einer einheitlichen Architektur, wie sie der Unified Storage-Ansatz bietet, liegt nicht nur in der protokoll-unabhängigen Datenkonsolidierung für FC SAN, IP SAN und NAS, sondern

auch in einheitlichen, einfachen und automatisierbaren Management-Tools und Prozessen, die menschliche Irrtümer auf ein Minimum reduzieren.

Vor diesem Hintergrund sind hochverfügbare und gleichzeitig kosteneffiziente Storage-Plattformen ein Muss. Der erste Schritt in diese Richtung ist die Beseitigung so genannter Single-Points-of-Failure, die in erster Linie die Komponentenausstattung betreffen. Defekte Lüfter, Netzteile oder auch Fehler im Hauptspeicher können zu ungeplanter Downtime führen. Um diese zu vermeiden, müssen Komponenten redundant ausgelegt sein. Im Störfall eines Storage-Controllers sollte ein automatisches und möglichst transparentes Failover auf eine zweite Komponente erfolgen können. Darüber hinaus sollten die im Einsatz befindlichen Storage-Lösungen grundsätzlich ein hohes Maß an erprobter Stabilität, erhöhten Schutz vor Datenverlust und proaktives Monitoring bieten. Vor allem Features wie RAID 6-Schutz gegen doppelte Plattenausfälle, Spiegel- und Multipath-Optionen, hochverfügbare Controller-Hardware und integrierte Monitoring-Funktionen helfen, die Hochverfügbarkeit der Storage-Infrastruktur zu sichern.

Doppelter RAID-Schutz

RAID-Technik ist die Basis, was Datenintegrität und Datensicherheit betrifft.

Um Hochverfügbarkeitsanforderungen zu erfüllen, muss allerdings mehr als RAID 5 möglich sein. Das gilt besonders, wenn SATA-Disks eingesetzt werden. SATA-Disks zeichnen sich im Vergleich zu FC- und SAS-Disks durch niedrigere Kosten und eine höhere Kapazität pro Laufwerk aus. Letzteres führt zusammen mit der ursprünglich für den Consumer-Bereich konzipierten Verfügbarkeit zu einem statistisch höheren Ausfallrisiko einzelner Datenblöcke. Besonders ernst zu nehmen ist dieses statistisch erhöhte Risiko dann, wenn bereits ein Block oder eine ganze Disk rekonstruiert wird – bei RAID 5 ein Zustand ohne weiteren Ausfallschutz.

Funktionen wie RAID-DP von NetApp – eine hoch performante RAID 6-Implementierung – bieten Double-Parity RAID 6-Schutz gegen doppelte Festplattenausfälle, ohne die Performance zu beeinträchtigen. Dies ist besonders bei einer hohen Datendichte auf großen 2-TByte-Platten und den bei Ausfällen damit verbundenen Rekonstruktionszeiten wichtig.

Doppelte Wege für Stabilität im Rechenzentrum

Der Einsatz von Multipath-Optionen, also redundanter Pfade zu Disk, Switch und Host, ist essenziell, um Hochverfügbarkeit in einem dynamischen Rechenzentrums-



betrieb zu erzielen. Software-Updates einzelner Komponenten lassen sich so unterbrechungsfrei durchführen. Zusätzlich besteht damit eine zuverlässige Absicherung gegen Konfigurations- oder Komponentenfehler. Zur Betriebssicherheit in komplexen Umgebungen trägt auch das End-to-End Monitoring der Datenpfade bei. NetApp bietet im Rahmen seiner OnCommand Management-Produkte agentenloses und damit einfach zu implementierendes und zu betreibendes Monitoring für heterogene Rechenzentrums-umgebungen.

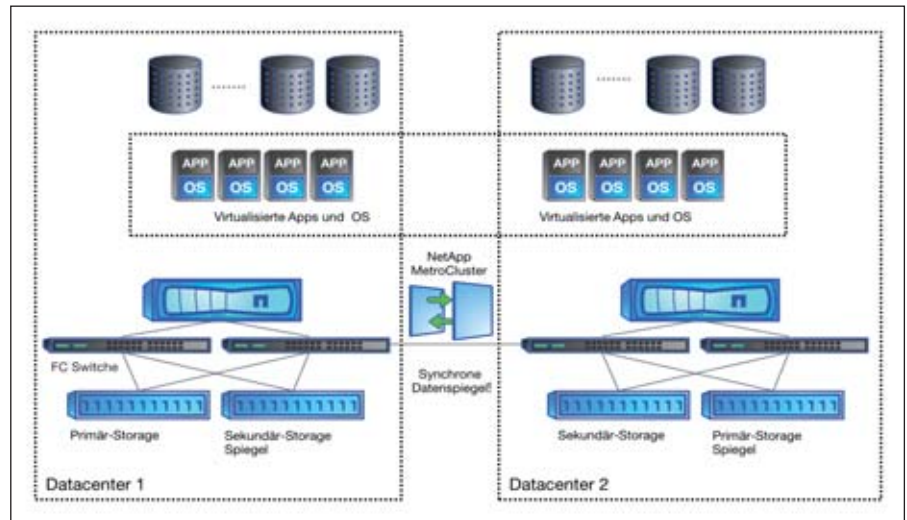
Doppelte Daten: asynchron repliziert

Um geschäftskritische Daten und Anwendungen zusätzlich zu schützen und hochverfügbar zu halten, sind Optionen für das Spiegeln von Daten notwendig. Sowohl asynchrone als auch synchrone Möglichkeiten sind dabei von Bedeutung. Bei der asynchronen Spiegelung etwa wird erst der Schreibvorgang auf dem Primärsystem beendet, bevor der Schreibvorgang auf dem Spiegelsystem zeitverzögert durchgeführt wird. Diese Art der Spiegelung ist – bei gegebener Bandbreitenverfügbarkeit – sehr gut geeignet, Disasterschutz auch über sehr weite Distanzen abbilden zu können. NetApp kombiniert Snapshot-basierende Replikation, Deduplizierung und Kompression, um die zu replizierende Datenmenge auf ein absolutes Minimum zu reduzieren und damit die möglichen Intervalle und Durchsatzraten zu maximieren. Je größer die Entfernung zwischen Quell- und Zielsystem wird, desto eher empfiehlt sich asynchrones Spiegeln.

Asynchrone Datenspiegelung kann jedoch noch eine weitere Option bieten: Daten lassen sich von einem Fibre Channel-Primärspeicher auf kostengünstigeren SATA-Storage replizieren. Snapshot-Technologie, die nur blockbasierte inkrementelle Änderungen über das Netz überträgt, reduziert zusätzlich die Anforderungen an die Netzwerkbandbreite – und auch deren Kosten.

Doppelte Daten: synchron repliziert

Definitionsgemäß kann asynchrone Spiegelung keine hundertprozentige Datenverfügbarkeit im Recoveryfall bieten, da die Replikationsintervalle zeitverzögert sind. Die sicherere Alternative dazu ist die syn-



Voneinander getrennte und dennoch synchrone Rechenzentren sind eine Maßnahme gegen Standortausfälle

chrone Spiegelung, bei der der Schreibvorgang erst beendet wird, wenn die Daten sowohl auf dem Primär- als auch auf dem Spiegelsystem geschrieben wurden. Die Methode der synchronen Spiegelung ist optimal für hochverfügbare, desastertolerante Speicherarchitekturen, wie sie mit der NetApp MetroCluster Technologie aufgebaut werden. Auf Systemebene sind Cluster die Standardmaßnahme für Hochverfügbarkeit und Ausfallsicherheit. Hochverfügbarkeitscluster werden vor allem in kritischen Umgebungen eingesetzt.

Als Maßnahme gegen Standortausfälle werden die Systeme eines Hochverfügbarkeitsclusters räumlich getrennt auf zwei Rechenzentren aufgeteilt, die auch über 100 Kilometer voneinander entfernt sein können. Die synchrone Replikierung kombiniert dabei die Fähigkeiten eines Hochverfügbarkeitsclusters mit dem automatisierbaren Failover des kompletten Standorts. Im Ernstfall ist die gespiegelte Datenkopie sofort verfügbar. So bleibt die betriebliche Kontinuität erhalten, und Datenverluste werden vermieden.

Ein System mit zwei Storage-Controllern ist zudem eine einfache und verlässliche Methode zum Upgrade von Hard- und Software oder für Wartungsarbeiten. Während ein Controller aktualisiert wird, übernimmt der zweite den Datenservice und umgekehrt. So lassen sich ausfallfrei Hardware-Komponenten erweitern oder austauschen und Software mit minimaler Unterbrechung auf den neuesten Stand setzen.

Integrierte Datensicherung Pflicht

Hochverfügbarkeit und Monitoring sind wichtige Komponenten für die Vermeidung ungeplanter Downtime und den Schutz vor Datenverlust. Backup und Disaster Recovery müssen jedoch ebenso in Betracht gezogen werden. Integrierte Datensicherungsoptionen auf Snapshot-Basis bieten den Vorteil hoher Effizienz und Betriebssicherheit bei einfachem Management. Sie sind die Mittel der Wahl, wenn es darum geht, in kürzester Zeit gelöschte Daten oder ältere Versionen wiederherzustellen.

In diesem Zusammenhang spielt die Festlegung individueller Richtwerte für zeitliche und inhaltliche Wiederanlaufpunkte nach einem Systemausfall eine entscheidende Rolle für die Passgenauigkeit des Konzepts. Die Recovery Time Objective (RTO) definiert die Zeit, die zur Wiederherstellung verlorener oder beschädigter Daten benötigt wird. Mit Recovery Point Objectives (RPO) wird bestimmt, wie viel Datenverlust maximal in Kauf genommen wird. Das Maß dafür ist der Zeitabstand zwischen zwei Backups oder Replikierungen. Je nach dessen Länge ist im schlimmsten Fall mit mehr oder weniger großem Datenverlust zu rechnen. Für Datenbankapplikationen beispielsweise ist Replikierung oft zwingend. Je höher der Verfügbarkeitsanspruch an die Applikation ist, desto eher wird ein Synchronverfahren zum Einsatz kommen. (dr)



Johannes Wagmüller ist Director Systems Engineering bei NetApp.

Berechnung der Kosten von IT-Ausfällen

Der Preis ist heiß

von Sven Wolf

Eine IT völlig ohne Ausfallzeiten – das ist natürlich die Idealvorstellung jedes Administrators. Eine maximale Verfügbarkeit hat allerdings auch ihren Preis. Für eine vernünftige Investitionsentscheidung gilt es daher, den richtigen Mittelweg zwischen Ausfallrisiko und Kosten der Backup-Infrastruktur zu finden. Wie Sie diesen für Ihr Unternehmen berechnen können, lesen Sie in diesem Beitrag.



Quelle: 123rf

Geschäftsführer und Controlling-Mitarbeiter denken gerne in Euro und Cent. Das gilt auch – und ganz besonders – bei der Anschaffung von Backup-Infrastrukturen. Denn Investitionen in die Sicherheit bringen ja zunächst keinen höheren Umsatz oder ein besseres Ergebnis. Eine unzureichende Datenabsicherung kann allerdings zu enormen Schäden führen – und diese sind klar bezifferbar. Doch wie viel Hochverfügbarkeit braucht ein Unternehmen? Wer diese Frage beantworten will, muss das individuelle Risiko quantifizieren und in Beziehung zu den Kosten der Backup-Infrastruktur setzen. Ein Disaster-Recovery-Plan soll schließlich nicht nur technisch, sondern auch betriebswirtschaftlich sinnvoll sein. Nur so lässt sich vermeiden,

mit der dicksten synchronen Replikationskanone auf einen Risiko-Spatzen zu schießen – oder sehr viel Geld für eine Downtime auszugeben, die mit relativ wenig Geld zu verhindern gewesen wäre.

Mehr oder weniger genaue Schadensprognosen für den Fall des Ausfalls sind oft schon vorhanden, aber oft auch veraltet. Daher empfiehlt sich eine grundlegend neue Bewertung. Denn die Risiko-Verteilung hat sich in den meisten Rechenzentren in den vergangenen Jahren stark verändert. Grund hierfür ist die Virtualisierung. Programme, die früher allein schon aus Inkompatibilitätsgründen auf mehrere physische Server verteilt waren, laufen nun auf einem. Insgesamt sind also meist weniger Server am Netz – und wo

weniger Hardware ist, kann logischerweise auch weniger kaputt gehen. Andererseits kumuliert sich das Risiko natürlich auf den konsolidierten Servern. Fällt ein virtualisierter und maximal ausgelasteter Server einmal aus, ist gleich eine ganze Reihe von Diensten nicht mehr am Netz. Eine realistische Einschätzung muss daher nicht den Server, sondern den einzelnen Workload untersuchen.

Ausfallfolgen pro Workload

Was der Ausfall genau kostet, lässt sich nach einer recht einfachen Formel ausrechnen: $\text{Ausfallkosten} = (\text{To} + \text{Td}) \times (\text{Rp} + \text{Lr})$. „To“ steht für die tatsächliche Dauer des Ausfalls in Zeiteinheiten, „Td“ bezeichnet die so genannte Delta Time – sprich die seit dem letzten Backup verstrichenen Zeiteinheiten. „Rp“ (Rate of Personnel) bildet Kosten ab, die durch die untätig herumsitzende Belegschaft entstehen. Dieser Wert errechnet sich aus den Personalkosten des betroffenen Bereichs, geteilt durch die geleisteten Zeiteinheiten. „Lr“ (Lost Revenue) schließlich gibt den entgangenen Profit an. Hier nehmen Sie am besten einen Durchschnittswert aus mehreren Monaten an und dividieren ihn durch die betrachteten Zeiteinheiten.

Nach dieser Formel lässt sich jedem Workload ein monetäres Risiko zuordnen. Dies ist auch notwendig, da in einigen virtuellen Infrastrukturen die Workloads je nach Auslastung von einem Server zum anderen verlagert werden. Die Addition aller auf dem Server installierten Workload-Risiken ergibt letztlich das Gesamtrisiko eines Servers. Die Risikoeinschätzung nach Workloads ist nicht zuletzt auch deswegen sinnvoll, weil moderne Host-basierende Replikation auch die Absicherung bestimmter Server-Bereiche zulässt. Außerdem lassen sich Konstellationen vermeiden, die eine unnötig hohe Risikoakkumulation auf einem physischen Server bedeuten würden.

Wie bereits erwähnt, nimmt die Ausfallhäufigkeit mit der Anzahl der in Betrieb befindlichen Komponenten ab. Für eine Kosten-Nutzen-Abschätzung bei der Anschaffung einer Hochverfügbarkeitslösung ist dieser Faktor aber weniger von Belang, da die Risikoanalyse grundsätzlich

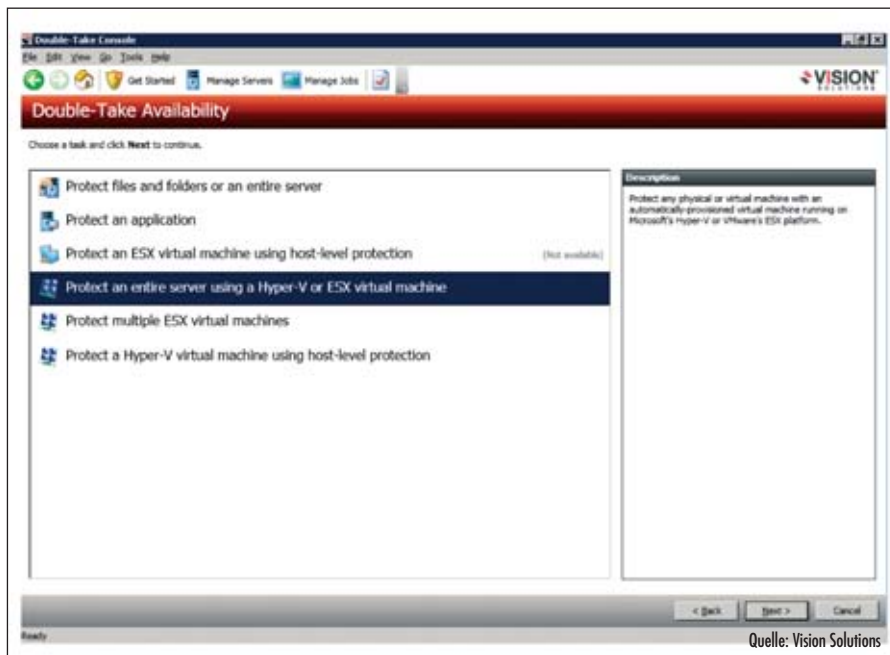


Bild 1: Mit moderner Hochverfügbarkeits-Software kann die Absicherung individuell auf das Risikopotenzial abgestimmt werden – zum Beispiel die Replikation physisch nach virtuell

vom Schadensfall ausgeht – und der kann schließlich auch gleich morgen eintreten. Statistiker mögen außerdem einwenden, dass eine Risikoabschätzung nach dieser relativ einfachen Formel keine Parameter wie Varianz oder Standardabweichung mit einbezieht. Die Ergebnisse sind aber dennoch ein klar quantifiziertes Argument gegenüber der Controlling-Abteilung – zeigen sie doch, dass auch ein relativ kurzer Ausfall oft viel, viel teurer kommt als ein richtig dimensioniertes Hochverfügbarkeits-System. Was aber ist ein richtig dimensioniertes Hochverfügbarkeits-System?

Die Kosten-Risiko-Analyse

Betrachten wir die Formel $(To + Td) \times (Rp + Lr)$ genauer, zeigt sich deutlich, warum reine Band-Backups heute nicht mehr ausreichen. In der Regel werden sie einmal pro Nacht gezogen. Und streng nach Murphys Law fällt der Server bestimmt nächsten Tag um 17:00 Uhr aus. Dann wird der Td-Wert mit mindestens acht Stunden zu einem gewichtigen Multiplikator. Da hilft es auch wenig, wenn der Support die Anlage schnell wieder am Laufen hat und damit die tatsächliche Ausfallzeit (To) gering hält.

Auf der anderen Seite der Multiplikation schlägt zunächst einmal der Personalkosten-Ausfallwert Rp zu Buche. Ausgespro-

chen kritisch sind dabei die Kommunikationssysteme. Fällt der Mail- oder VoIP-Server aus, sinkt die Produktivität bereits dramatisch, erwischt es beide, geht in der Regel nichts mehr – und dann wird es schnell teuer. Diese beiden Services sollten daher auch keinesfalls auf derselben Hardware laufen. Der entgangene Umsatz Lr hängt ebenfalls stark von der jeweiligen Applikation ab. Besonders teuer kommt ein Ausfall bei unmittelbar am Verkauf beteiligten Prozessen wie etwa e-Shops oder Warenwirtschaftssystemen. Wichtig bei der Risikoabschätzung ist allerdings der Gewinn – nicht der Umsatz.

Synchrone Replikation

Downtime und seit dem letzten Backup verstrichene Zeit addieren sich in ihren Auswirkungen. Ist der Rp- oder Lr-Wert hoch (oder auch beide), dann müssen die To und Td möglichst niedrig gehalten werden. So kann zum Beispiel in der Finanzbranche der Lr-Faktor schnell gegen plus unendlich tendieren. Deshalb werden die beiden andern Multiplikatoren durch synchrone Replikation praktisch bei null gehalten.

Dabei fängt die Software Schreibzugriffe ab und sendet sie gleichzeitig an das primäre und sekundäre Array. Erst wenn beide den Empfang bestätigt haben, akzeptiert das Programm den nächsten Write

Request. Beide Speicher haben also immer exakt denselben Stand, Datenverluste sind praktisch ausgeschlossen. Synchrone Replikation markiert allerdings einen Extrempunkt in der Replikationspyramide. Sie lässt den Traffic im Netz stark ansteigen und erfordert daher oft schnelle und teure Fibre Channel-Verbindungen. Eine derartige Maximallösung ist in den meisten Fällen überdimensioniert.

Asynchrone Replikation

Akzeptieren wir einen Td-Wert, also ein Recovery Point Objective, im Bereich weniger Minuten, ist asynchrone Replikation die bessere, weil preiswertere Wahl. Dabei werden Write Requests des Betriebssystems zunächst an das lokale Ziel weitergereicht und erst nach dem Schreibvorgang auf das sekundäre, entfernte Backup-System kopiert. Dabei wartet die Anwendung nicht auf Bestätigungen, sondern fährt unmittelbar mit den nächsten Daten fort. Zeitgemäße asynchrone Replikations-Software fängt die Schreibzugriffe auf Low-Level-Ebene ab, repliziert werden also nur die tatsächlich geänderten Bytes. Dies beansprucht kaum Bandbreite und funktioniert auch über WAN-Verbindungen. Asynchrone Replikation ist prinzipiell nicht ganz verlustfrei wie die synchrone Variante. Die Ausfallformel zeigt aber, dass sie in den allermeisten Fällen das beste Preis-Leistungs-Verhältnis bietet.

Recovery – automatisch oder manuell

Für den To-Wert, also das Recovery Time Objective, gilt wie beim Parameter Td: Er muss umso niedriger sein, je geschäftskritischer ein Service ist, also je höher die Werte Rp oder Lr sind. Auch Performance und Kapazitäten der Backup-Hardware müssen dem Risiko angepasst werden. Denn entscheidend ist nicht nur die schnelle Wiederherstellung, sondern auch eine bedarfsgerechte Quality of Service (QoS) nach dem Failover.

Das Warenwirtschaftssystem zum Beispiel muss nach einem Ausfall binnen weniger Minuten wieder verfügbar sein, sonst kann der Einkauf nicht weiterarbeiten und auch die Verkäufer sitzen untätig herum. Zu den Personal-Ausfallkosten gesellt sich dann auch noch der entgangene Gewinn. Eine derart



hohe Rp- und Lr-Prognose verlangt die permanente Bereitstellung eines Backup-Servers, der mit dem Produktionssystem bei der Leistung weitgehend identisch ist. Schließlich muss bei derart kritischen Servern die QoS auch nach dem Recovery in etwa gleich bleiben, sonst bremsen lange Antwortzeiten die Produktivität zu stark aus. Das Recovery muss automatisch erfolgen und auch alle Applikationen auf dem neuesten Stand wiederherstellen, mit allen Service Packs oder Updates. Hier brauchen Sie ein asynchrones Replikationsprogramm mit Full-Server-Failover. Der Backup-Server übernimmt vollautomatisch oder nach wenigen Mausklicks den Posten seines ausgefallenen Kollegen.

Haben Sie einen mittleren Rp- und Lr-Wert ermittelt, bietet sich zum Beispiel eine preiswertere Many-to-one-Datenreplikation mit automatischem Failover an. Dabei werden mehrere Server permanent auf ein Backup-System repliziert. Die automatische Server-Umschaltung sorgt auch hier dafür, dass nach wenigen Minuten alle wieder weiterarbeiten. Bedenken sollten Sie, dass je nach Backup-Hardware die QoS nach dem Recovery niedriger ist und dieses Konzept bei Mehrfach-Ausfällen möglicherweise nicht mehr greift. Durch eine geschickte Aufteilung lässt sich das Risiko aber gut eingrenzen.

Daneben gibt es auch noch so genannte Sekundär-Server, wie sie zum Beispiel für Archivierungszwecke zum Einsatz kommen. Die Risikoabschätzung liefert hier meist geringe Rp- oder Lr-Werte. Auch ein mehrstündiger Ausfall verursacht keine allzu hohen Kosten. Hier wird wieder Many-to-one-Replikation eingesetzt, da eine niedrigere QoS nach der Wiederherstellung durchaus akzeptabel ist. Ein automatisches Recovery ist hier zwar praktisch, aber betriebswirtschaftlich nicht erforderlich. Die Wiederherstellung wird in diesem Fall vom Administrator per Image-Mounting durchgeführt. Die permanente Replikation hat aber dafür gesorgt, dass der Td-Wert niedrig bleibt. Damit bleibt auch der Schaden geringer als bei einem Recovery von Bandsicherungen – die sich oft auch noch als unzuverlässig erweisen.

Moderne Replikations-Software bietet eine Fülle von Replikations- und Recovery-Optionen, die den Rahmen dieses Beitrags sprengen würden. Wer sich hier qualifiziert beraten lässt, findet sicher eine Lösung, die optimal zu seinem Risikopotenzial passt.

Räumliche Trennung

Ein tragfähiger Disaster-Recovery-Plan sollte allerdings nicht nur Replikation und Wiederherstellung betrachten, sondern auch die geografische Verteilung. Die Tsunami-Katastrophe in Japan hat gezeigt, wie anfällig moderne Technik gegen großflächige Impacts sein kann. Dass ein Backup-System im selben Raum bei einem Feuer wenig bringt, ist wohl offensichtlich. Dennoch zeigt die Statistik, dass auch in puncto räumlicher Risikoverteilung noch Nachholbedarf besteht: Nach einer Brandkatastrophe müssen 70 Prozent der betroffenen Firmen Konkurs anmelden – trotz Entschädigung. Oft vergessen: Auch die beste Versicherung zahlt nur für unmittelbare Schäden, etwa die zerstörte Hardware, nicht aber für entgangenen Umsatz.

Steigt die Temperatur in den Speichermedien über den Curie-Punkt, ab dem Metalle ihre magnetischen Eigenschaften verlieren, sind alle Daten physikalisch gelöscht. Einen solchen Totalausfall sollten Sie nicht einfach dem Restrisiko zuordnen. Server mit sehr hohem Rp- und Lr-Wert müssen an einen entfernten Standort repliziert werden, zum Beispiel in einer Filiale. Ein räumlich aufgeteiltes Sicherheitskonzept muss dabei nicht zwangsläufig mit höheren Kosten einhergehen. Hier erweist sich die Entscheidung für ein asynchrones Sicherungsmodell wieder als richtig. Moderne Hochverfügbarkeits-Software, zum Beispiel Double-Take Availability, schickt, nach der einmaligen Vollsicherung zu Beginn, nur noch die Bytes über die WAN-Verbindung, die auf dem Primärsystem modifiziert wurden. Bei geringer zur Verfügung stehender Bandbreite kann die Initialspiegelung auch durch Datenimport erfolgen. Je nach Situation und Auslastung funktioniert die Replikation sogar über ganz gewöhnliche Internet-Verbindungen wie SDSL oder sogar ADSL. Die Absicherung gegen unbefugte Zugriffe erfolgt dabei per VPN-Tunnel.

Cloud als Sekundär-Standort

Haben Sie selbst keinen ausreichend entfernten Replikationsstandort zur Verfügung, bietet sich eine Cloud-Lösung an. Die Cloud-Replikation kann sich dabei auf die zuverlässigen Server-Farmen des Projektpartners Amazon stützen. Cloud-Replikation bietet maximale Freiheitsgrade beim Recovery. Bei Bedarf werden kritische Applikationen einfach im Internet gestartet. Dann kann der Geschäftsbetrieb prinzipiell an jedem Ort der Welt weitergehen. Grundsätzlich gilt: je flexibler die Replikation, desto geringer die Kosten. Eine generische Replikation, wie sie bei zeitgemäßen Produkten Standard ist, fängt lediglich I/O Requests ab und leitet sie asynchron weiter. Das Zielsystem muss also mit dem produktiven System nicht identisch oder typgleich sein. Für die Low-Level-Replikation sind sogar offene Dateien kein Problem. Damit lassen sich zum Beispiel Exchange Server oder SQL-Datenbanken in das Sicherheitskonzept einbeziehen.

Host-basierende Replikation

In der Praxis lässt sich feststellen, dass die Host-basierende Replikation gegenüber der Array-basierenden immer mehr an Boden gewinnt. Die Replikation von Server zu Server hat eine Reihe von Vorteilen. Neben der Hardware-Unabhängigkeit ist dabei auch die Granularität zu nennen: Absicherungen können über komplette Server vorgenommen werden, aber auch für bestimmte Applikationen. Angesichts der breiten Risikostreuung auf virtualisierten Systemen ist das oft von Vorteil. Host-basierende Replikation kommt zudem ohne ein SAN aus, das sich nicht selten als Kostentreiber erweist. Kostendämpfend kann sich dagegen eine gute Integration der Replikation in das Administrationskonzept auswirken. Dies gilt insbesondere bei den meist stark ausgelasteten virtualisierten Systemen. Hier setzt sich immer mehr Hyper-V durch. Microsoft bietet für seinen Hypervisor einen SCVMM (System Center Virtual Machine Manager) an, der alle Arten von virtuellen Maschinen zentral verwaltet. Wer eine solche zentrale Konsole nutzt, sollte darauf achten, dass sich auch die Replikations-Software nahtlos einbinden lässt. (dr)



Sven Wolf ist Technical Manager bei Vision Solutions.

Linux Hochverfügbarkeit



Hochverfügbarkeits-szenarien waren vor ein paar Jahren nur den Administratoren sehr großer Rechenzentren vorbehalten, sind aber mittlerweile auch in mittleren und kleineren Netzwerken relevant. Linux-Experte Oliver

Liebel widmet sich diesem Thema und das primär auf seiner Open Source-Plattform. Die Motivation dahinter entspringt den praxisnahen Admin-Anforderungen: maximale Ausfallsicherheit bei relativ moderaten Hardware-Voraussetzungen. Dabei berücksichtigt der Autor keine spezielle Hardware-Konstellation, sondern stellt Ansätze mit bereits bewährten Standard-Tools vor. Die kurze, aber ausreichende Einführung in die The-

matik soll den Leser sensibilisieren, bevor er sich den Komponenten lokaler Hochverfügbarkeit widmet.

Den Kernpunkt der Publikation bildet die freie Software-Clusterlösung, die aus den Komponenten Pacemaker, OpenAIS und Heartbeat besteht. Natürlich werden die verschiedenen Clustertypen erläutert und eine konzeptionelle Übersicht geboten. Im Abschnitt "Management von Cluster-Ressourcen" wird der Praktiker besonders fündig. Ausfallsichere Replikationslösungen (DRBD) dürften zudem den Storage-Admin erfreuen, da der Autor sich dieser Thematik besonders ausführlich widmet. Erfreulich, dass die gewählten Beispiele auch Neulingen auf diesem Gebiet einen guten Einblick in ein funktionierendes Cluster-Setup gewähren. Den aktuellen Trends folgend ist dem Thema "Virtualisierung im Cluster" ein Kapitel gewidmet, wo sich XEN und KVM/qemu wiederfinden. Abgeschlossen wird das Buch durch einen Abschnitt zum oft vernachlässigten Thema Backup und Disaster Recovery.

Fazit: Der Untertitel "Einsatzszenarien und Praxislösungen" lässt vermuten, dass der Autor keine akademisch-theoretischen Absichten hegt. Untermauert wird dies durch den Faktor der sorgfältigen Planung, die das Fundament jeder Hochverfügbarkeitslösung ist. Der Autor lässt sein Know-how in die detailliert aufgeschlüsselte Arbeit auf 350 Seiten einfließen und präsentiert eine gelungene Mischung aus relevanter Theorie gepaart mit praktischen Beispielen. Einziges Manko: Kommerziell verfügbare Systeme werden in keiner Weise erwähnt. Dennoch ist der Administrator nach dieser Lektüre Garant für den unterbrechungsfreien Geschäftsablauf.

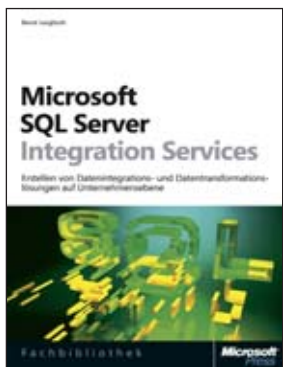
Frank Große

Autor	Oliver Liebel
Verlag	Galileo Computing
Preis	49,90 Euro
ISBN	978-3-8362-1339-4

Bewertung (max. 10 Punkte) 9



Microsoft SQL Server Integration Services



Analyse und Auswertung von Unternehmensdaten sind der Grundstein im Bereich Business Intelligence. Die Microsoft SQL Server Integration Services (SSIS) sind in der Lage, Daten unterschiedlichster Quel-

len zu verarbeiten, um jenen Anforderungen gerecht zu werden. Der Autor Bernd Jungbluth, ein renommierter SQL-Experte, beschreibt in diesem Buch die einzelnen Komponenten mit ihren Eigenschaften detailliert und erarbeitet Beispiele, Praxistipps sowie relevante Hinweise. Doch der Reihe nach: Der Inhalt ist in fünf Teile aufgesplittet, wobei der Chronologie entsprechend sich der Einstiegsteil dem Sinn und Zweck von SSIS widmet. Neben einem Blick in die Vergan-

genheit wird dem Leser die Architektur und Struktur von Paketen erläutert, sodass auch bis dato mit dem Thema unbedarfte Nutzer einen Kenntnisstand erreichen können, der für die fortlaufenden Kapitel nötig ist.

Für einen sicheren Umgang in der Arbeit mit der Entwicklungsumgebung sorgt der zweite Teil, der sich dem Business Intelligence Development Studio, Paketvariablen, Ausdrücken und dem Verbindungs-Manager widmet. Mit diesem Rüstzeug gewappnet gelangt der Leser an das Eingemachte der Daten: die Konfiguration der Ablaufsteuerung. Die einzelnen Elemente werden detailliert vorgestellt und deren Einsatzmöglichkeiten beschrieben. Zahlreiche Screenshots lockern die Materie auf und erleichtern das Wiederfinden in der IDE. Der Einsatz des Ereignis-Handlers schließt den dritten Teil ab. Der Datenfluss, seine Quellen, zahlreiche Transformationsmöglichkeiten und Datenflussziele liefern umfangreiches technisches Material, dem der Autor gerecht wird. Developer dürften sich über den finalen Teil freuen, der sich der Entwick-

lung, Bereitstellung und dem Betrieb widmet. Nach Lektüre dieser Passage sollten in Zukunft keine Schwierigkeiten mit der Bearbeitung von Daten vorhanden sein.

Fazit: Wer ist die Zielgruppe dieser 774 Seiten starken Dokumentation? (SQL)-Datenbank-Administratoren auf jeden Fall, aber letztlich jeder, der Daten importieren, exportieren, aufbereiten, transformieren, konsolidieren und integrieren muss. Unterschiedlich komplexe Lösungen werden demonstriert, sodass kaum eine Frage offenbleibt. Der Fokus liegt auf SSIS 2008 und SSIS 2008 R2. Die Schriftgröße ist relativ klein, was die Seiten sehr gepresst wirken lässt und beim Lesen anstrengend werden kann.

Frank Große

Autoren	Bernd Jungbluth
Verlag	Microsoft Press
Preis	49,90 Euro
ISBN	978-3-86645-654-9

Bewertung (max. 10 Punkte) 9



<http://itproblogs.de/> **Geballtes Wissen**

Stets technisch auf dem Laufenden zu sein, ist in einer so dynamischen Welt wie der aktuellen IT für Administratoren und IT-Verantwortliche ein Muss. So erscheint beispielsweise praktisch jede Woche ein neues Produkt rund um die Virtualisierung und in noch höherer Frequenz werden Sicherheitslücken veröffentlicht. Da ist aktuelles Wissen gefragt, sei es, um jederzeit korrekt auf Probleme in der eigenen Infrastruktur vorbereitet zu sein oder bei der Anschaffung neuer Geräte nicht auf eine veraltete Technik zu setzen. Ein beliebtes Mittel, um in Sachen Know-how auf dem aktuellsten Stand zu bleiben sind – neben der Lektüre dieses Fachmagazins – Blogs.

Doch auch hier stellen sich der gezielten Wissensbeschaffung noch einige Fragen und Anforderungen in den Weg: Welche Blogs soll ich lesen? Wo finde ich die besten Blogs für mein Tätigkeitsfeld? Hat der Blog tatsächlich die fachliche Qualität, die ich benötige? Sind all diese Frage geklärt, bleibt natürlich immer noch die Herausforderung, die Zeit zu finden, sich möglichst täglich durch all die neuen Blogposts zu lesen.

Und genau hier setzt unsere Website des Monats – itproblogs.de – an, indem die Seite als eine Art "Meta-Blog" fungiert

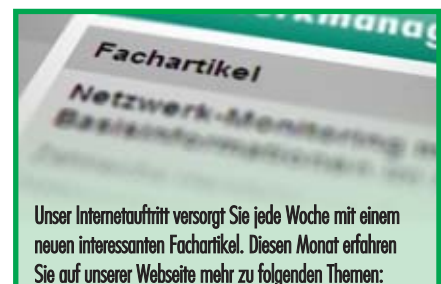
und die Posts einer ganzen Reihe namhafter Experten in einem Blog kumuliert. So bleibt Ihnen viel Zeit bei der Suche nach den passenden Blogs erspart.

Thematisch setzt itproblogs.de einen Schwerpunkt bei Microsoft-Technologien. So finden sich die Blog-Einträge des deutschen Active Directory-Blogs hier ebenso wie des Windows Server-Teams und diverser wichtiger Microsoft-Mitarbeiter – allesamt deutschsprachig. Und auch eine ganze Reihe von Autoren des IT-Administrator von Niels Kaczenskis faq-o-matic.net über Marc Grote und Walter Steinsdorfer bis zum Blog-Port 389 von Thomas Gronenwald und Florian Thiessenhusen sind hier eingebunden. In Sachen Hochverfügbarkeit und Windows-Cluster hält Sie Nail Own auf dem Laufenden, Reiner Ganser informiert über Sharepoint und Informationen zum MS Forefront/TMG fehlen ebenso wenig wie die Themen Virtualisierung und Sicherheit. Und auch wer sich über die beliebteste Veranstaltung der IT-Community, der ice in Lingen, auf dem Laufenden halten will, wird über den Blog von Nicki Wruck bedient.

Insgesamt bündelt itproblogs.de über vierzig Blogs. Von diesen sind zwar einige schon nicht mehr aktiv, dennoch stellt die Sammlung einen wirklich empfehlenswerten Pool an Tipps, Tricks und Know-How für den Netz- und Systemadministrator bereit. (jp)



Unter itproblogs.de findet sich eine Sammlung zahlreicher exzellenter Blogs



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

Effizientes Log-Management gegen Sicherheitsrisiken

Ob bösartige Cyber-Attacke oder Malware in allen Varianten – Risiken für die Unternehmens-IT gibt es zuhauf. Menschen sind dabei meist das schwächste Glied in der Kette und anfällig für Fehler und trickreiche Social Engineering-Techniken. Unser Online-Fachartikel zeigt, wie Sie Security-Lücken durch ein effizientes Log- und Security Event-Management stopfen – gerade weil Anwender und oft auch Administratoren nicht selten das Kernproblem der Sicherheit sind.

www.it-administrator.de/themen/sicherheit/fachartikel/98733.html

Management von mobilen Devices und iOS4-Geräten

Die Verbreitung von iOS4-Geräten lässt sich nicht mehr verhindern. Administratoren stoßen mit den Apple-eigenen Tools zum Management der mobilen Geräte jedoch schnell an Grenzen. Unser Fachbeitrag im Web führt auf, wie es trotzdem gelingt, iOS4-Devices aus der Ferne zu konfigurieren und Anwender mit Software zu versorgen. Sie erfahren, welche Fallstricke es dabei gibt, welche Voraussetzungen Sie erfüllen müssen und wie Sie das Thema Sicherheit abdecken.

www.it-administrator.de/themen/netzwerkmanagement/fachartikel/98734.html

Sichere Systemverwaltung trotz externer Datenträger

Spektakuläre Datenverluste veranlassen viele Administratoren, USB-Sticks komplett aus dem Unternehmen zu verbannen. Dabei müssen die Flash-Speicher kein Risiko sein. Denn wer auf Verschlüsselung und zentrale Administration aller USB-Sticks setzt, kann die Vorteile der Technik nutzen, ohne ihre Risiken in Kauf nehmen zu müssen. Unser Webartikel beschreibt, wie verschlüsselte Speicherriegel sogar ein höheres Sicherheitsniveau bieten können als konventionelle Datenträger.

www.it-administrator.de/themen/sicherheit/fachartikel/98735.html

Open Source-Virtualisierungslösungen im Überblick

Schlank und flexibel: So präsentiert sich KVM im Vergleich zu anderen Virtualisierungs-Tools und hält damit auch den hohen Anforderungen im Enterprise-Umfeld stand. In unserem Online-Beitrag veranschaulichen wir neben einer Gegenüberstellung aktueller Virtualisierungslösungen den Aufbau einer offenen Virtualisierungsumgebung auf Basis von KVM. Ergänzend dazu werfen wir einen Blick auf die Open Source-Lösung openQRM als zentrales Management-Werkzeug.

www.it-administrator.de/themen/virtualisierung/fachartikel/98736.html

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

»Mathematik und Informatik habe ich im Blut«

Claudia Eggert (38) betreut als Systemadministratorin in Leverkusen den Unix-Bereich der umfangreichen IT-Landschaft bei Bayer Business Services – dem globalen Kompetenz-Zentrum des Bayer-Konzerns für IT- und Business Services. Als weltweit tätiger Dienstleister für die Geschäftsprozesse von Bayer verantwortet der Bereich die IT-Services, entwirft, vollzieht und betreibt Lösungen für Personal, Einkauf, Logistik und Finanzen und bietet Rechts- und Unternehmensberatung.

Warum sind Sie IT-Administratorin geworden?

Für mich war klar, dass meine beruflichen Schwerpunkte auf Mathematik und Informatik liegen sollten – das hab ich einfach im Blut. Die Ausbildung hat Spaß gemacht und die damals noch als Spartenorganisation aufgestellte Bayer AG hatte ein so großes Spektrum an EDV-Anforderungen, dass es nicht schwer war, einen für mich interessanten Einstieg zu finden. Warum würden Sie einem jungen Menschen raten, Administrator zu werden?

Die Arbeit als Systemadministrator ist unheimlich vielseitig, so dass man im Laufe der Jahre eigene Vorlieben berücksichtigen kann. Die IT-Branche ist ein so schnelllebiges Geschäft, dass man immer wieder neu gefordert wird. Das ist meiner Meinung nach eine Voraussetzung dafür, sich in diesem Umfeld nicht vor weit über 35 abzuleisten den Dienstjahren fürchten zu müssen.

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

Ich finde es großartig, dass ich schon so viele verschiedene Aufgabengebiete kennen gelernt habe und bin immer noch neugierig. Ich verstehe sowohl die Client Seite, habe aber auch Erfahrung im Bereich Windowsserver-Betrieb, Lotus Notes Server und Applikationen bis hinein in die UNIX-Welt, in der ich aktuell arbeite. Und ich finde es toll, dass ich trotz all der EDV so viel mit Menschen zu tun habe.

Nehmen Sie Ihre Arbeit auch ins Wochenende mit?

Früher sehr oft, auch dadurch bedingt, dass ich oft Bereitschaft für Nacht- und Wo-

chenendzeiten hatte. Da war die Arbeit immer präsent. Mittlerweile arbeite ich nur noch Teilzeit und weil ich nicht immer ansprechbar sein möchte, habe ich es viel besser im Griff, an Kollegen zu delegieren.

Wie denken Sie, arbeitet ein Administrator in 10 Jahren?

Ich habe jetzt schon festgestellt, wie problemlos ich von wechselnden Schreibtischen aus arbeiten kann. Dank Tools wie Lync oder Skype bin ich immer auch telefonisch erreichbar. Ich glaube diese Situation wird sich noch verstärken. Außerdem werden wir es noch stärker nutzen, mit Kollegen in unterschiedlichen Zeitzeonen zu arbeiten, so dass wir unsere Wartungstermine noch kundenfreundlicher planen können.

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

Eine Excel-Tabelle bereitet mir immer wieder Kopfzerbrechen. Sie stellt unsere AIX-basierte Hardware dar, zeigt die installierten Instanzen mit all ihren Ressourcen, berechnet freie Kapazitäten und macht allerlei Auswertungen. Die Tabelle ist ziemlich gewaltig, von mehreren Händen weiterentwickelt worden und es schleicht sich immer mal wieder ein Fehler ein. Meine Programmierzeiten sind schon länger vorbei und hier stoße ich immer wieder an meine Grenzen. Hier könnte ich ein Tool brauchen, das alles klar darstellt und völlig fehlerfrei läuft.

Setzen Sie eine Hochverfügbarkeitslösung ein?

Wir nutzen im Bereich AIX für alle 53 Cluster HACMP/ Power HA. In der Linux und VMware-Landschaft nutzen wir HA für alle 40 Cluster, die aus bis zu acht Servern bestehen.

Wie hoch muss die Verfügbarkeit dieser Systeme sein und wird diese auch erreicht?

Die geforderte Verfügbarkeit der Business Critical-Systeme liegt bei 99,5 Prozent und wird auch erreicht.



Geburtstag: 19.01.1973
Familienstand: verheiratet, eine Tochter
Hobbys: Patchwork, Singen und Heimelektronik

Claudia Eggert, IT-Administratorin

Ausbildung und Tätigkeit

- Ausbildung zur Mathematisch-technischen Assistentin
- Technischer Support für 1st level Support-Anfragen
- Danach Wechsel in den Ingenieur-Bereich
- Heute in der zentralen Informatik als Teilzeit-Systemadministratorin

Betreute Umgebung

- UNIX-Systeme als Grundlage für Webserver, Oracle DB Server, TSM-Server und diverse SAP-Systeme
- Mischung aus Linux RHEL 4- und 5- sowie AIX-Maschinen
- IBM P570, IBM P595 und IBM 350, 3850, 3950 sowie HP DL 380, DL 570 und DL 580

Aus Ihrer Erfahrung: welche Komponenten der IT sind besonders ausfallgefährdet?

Festplatten und Hauptspeichermodule sind meiner Erfahrung nach die größten Problemzonen einer IT-Landschaft.

Viele IT-Abteilungen setzen eher auf schnelles Recovery mit virtualisierten Servern als auf eine dedizierte Hochverfügbarkeitslösung – wie sehen Sie das?

Wegen der großen Datenmengen können wir uns nicht auf ein schnelles Recovery verlassen. Seit vielen Jahren haben wir auch Standorte in Ländern, die sehr langsam angebunden sind, so dass die überschaubare Datenmenge in der Wiederherstellung zu lange brauchen würde. Wir haben da "nur" die Möglichkeit des sogenannten continuous access, was uns ein Anlaufen der Übernahme-Seite im Cluster mit dem erstellten Spiegel erlaubt.

Das Interview führte Petra Adamik.

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

Was haben Sie zu sagen?

Die Ausgabe 8/11 erscheint am 2. August 2011

Schwerpunktthema:

Systemmanagement

Im Test: Eye of the Storm Network Professional Edition

Im Test: Systemüberwachung mit openITCOCKPIT

Workshop: GPOs mit der Advanced Group Policy Management Console verwalten

Systeme: Windows Intune – PC-Management aus der Cloud

Die Redaktion behält sich Themenänderungen aus aktuellem Anlass vor.

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

Die Ausgabe im September hat sich zum Schwerpunkt das Thema **E-Mailmanagement und Collaboration** gesetzt. In unseren Tests werfen wir unter anderem einen Blick auf Zimbra 7.0. In den Workshops lesen Sie, wie Sie den Lync Server 2010 im Netzwerk integrieren.

Als Schwerpunkt im Oktober folgt dann das Thema **Netzwerksicherheit**.

IMPRESSUM

Redaktion

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

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

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

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

Autoren dieser Ausgabe

Petra Adamik, Thomas Bär, Dr. Rainer Doh,
Ralph Dornbach, Thomas Drilling, Thomas Gronenwald,
Frank Große, Marc Grote, Jürgen Heyer, Thomas Joas,
Robert Lindermeier, Thorsten Scherf, Johannes Wagnmüller,
Sven Wolf

Anzeigen

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

Es gilt die Anzeigenpreisliste
Nr. 8 vom 01.01.2011

LAG/2008



Produktion / Anzeigendisposition

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

Druck

Konrad Tritsch
Print und digitale Medien GmbH
Johannes-Gutenberg-Straße 1-3
97199 Ochsenfurt-Hahestadt

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

Vertriebsbetreuung

SI special interest Pressevertrieb GmbH,
www.specialinterest.com

Erscheinungsweise

monatlich

Bezugspreise

Einzelheftpreis: € 12,60
Jahresabonnement Inland: € 135,-
Studentenabonnement Inland: € 67,50
Jahresabonnement Ausland: € 150,-
Studentenabonnement Ausland: € 75,-

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

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

Verlag / Herausgeber

Heinemann Verlag GmbH
Leopoldstraße 85
80802 München
Tel.: 089/4445408-0
Fax: 089/4445408-99

(zugleich Anschrift aller Verantwortlichen)

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

Eingetragen im Handelsregister des
Amtsgerichts München unter
HRB 151585.

Geschäftsführung / Anteilsverhältnisse

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

ISSN

1614-2888

Urheberrecht

Alle in IT-Administrator erschienenen Beiträge sind
urheberrechtlich geschützt. Alle Rechte, einschließlich
Übersetzung, Zweitverwertung, Lizenzierung vorbe-
halten. Reproduktionen und Verbreitung, gleich wel-
cher Art, ob auf digitalen oder analogen Medien, nur
mit schriftlicher Genehmigung des Verlags. Aus der
Veröffentlichung kann nicht geschlossen werden, dass
die beschriebenen Lösungen oder verwendeten Be-
zeichnungen frei von gewerblichen Schutzrechten sind.

Haftung

Für den Fall, dass in IT-Administrator unzutreffende
Informationen oder in veröffentlichten Programmen,
Zeichnungen, Plänen oder Diagrammen Fehler en-
thalten sein sollten, kommt eine Haftung nur bei
grober Fahrlässigkeit des Verlags oder seiner Mit-
arbeiter in Betracht. Für unverlangt eingesandte
Manuskripte, Produkte oder sonstige Waren über-
nimmt der Verlag keine Haftung.

Manuskripteneinsendungen

Die Redaktion nimmt gerne Manuskripte an. Diese
müssen frei von Rechten Dritter sein. Mit der Ein-
sendung gibt der Verfasser die Zustimmung zur Ver-
wertung durch die Heinemann Verlag GmbH. Sollten
die Manuskripte Dritten ebenfalls zur Verwertung
angeboten worden sein, so ist dies anzugeben.
Die Redaktion behält sich vor, die Manuskripte
nach eigenem Ermessen zu bearbeiten. Honorare
nach Vereinbarung.

So erreichen Sie den Leserservice

Leserservice IT-Administrator
Stephan Orgel
65341 Elfvile
Tel.: 06123/9238-251
Fax: 06123/9238-252
E-Mail: leserservice@it-administrator.de

Bankverbindung für Abonnenten

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

So erreichen Sie die Redaktion

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

So erreichen Sie die Anzeigenabteilung

Anzeigenverkauf IT-Administrator
Anne Kathrin Heinemann
Heinemann Verlag GmbH
Leopoldstr. 85
80802 München
Tel.: 089/4445408-20
Fax: 089/4445408-99
E-Mail: kathrin@it-administrator.de

1 und 1 S. 12, S. 13, S. 23
Devicelock S. 17
ExperTeach S. 05

Galileo
IBM
IIR Deutschland

S. 25
S. 84
S. 31

Libelle
Paessler
Strato

S. 41
S. 27
S. 02

INSERENTENVERZEICHNIS

Das IT-Administrator Komplettprogramm!!!

Sichern Sie sich jetzt das **IT-Administrator
Jahresabo All-Inclusive** mit allen Monats-
ausgaben, Sonderheften und der Jahres-CD.

Statt Euro 29,90 zahlen Sie dabei für jedes
Sonderheft nur Euro 19,90 – und müssen
keine zusätzliche Bestellung mehr tätigen.

Automatisch bekommen Sie im März
und Oktober jeden Jahres das jeweilige
IT-Administrator Sonderheft und mit
Ihrer Dezemberausgabe die jeweilige
Jahres-CD mit allen Monatsausgaben
des Jahres im PDF-Format zugestellt.



Als bestehender Jahresabonnent
können Sie hier upgraden:

[www.it-administrator.de/
abonnements/aboupgrade/](http://www.it-administrator.de/abonnements/aboupgrade/)

Oder Sie sind Neukunde? Hier können Sie bestellen:

[www.it-administrator.de/
abonnements/jahresabo/](http://www.it-administrator.de/abonnements/jahresabo/)

www.it-administrator.de



Heinemann Verlag
Im Dialog mit Spezialisten.

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

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

Vertrieb, Abo- und Leserservice IT-Administrator

vertriebsunion meynen
Herr Stephan Orgel
D-65341 Eltville

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

Vernetzen statt verzetteln.

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



Überzeugen Sie sich ... in nur 10 Minuten.

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

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

