Auf DVD: Original Microsoft-Toolkit

4 197970 309908 05

Sonderheft 5/2014 Juli/August/September
Deutschland € 9,90 Österreich, Benelux € 10,95
Schweiz sfr 19,90

PC WELT Tech

NEU: DAS WINDOWS-MAGAZIN FÜR TECHNIK-FANS

Windows 8.1 für Profis

- PCs zentral konfigurieren und steuern
- Windows 8.1 im Netzwerk nutzen
- Die besten Admin-Tools
- Profi-Tricks: Passwörter zurücksetzen, Systeme und Programme fernsteuern u.v.m

Bootfähige Rettungs-DVD

Auf DVD
Komplettes Tool-Paket für Windows 8.1

Konfigurieren, Rechte steuern, partitionieren, virtualisieren u.v.m.

Virtualisierung
- Windows-Bordmittel richtig nutzen
- Profi-Tipps für virtuelle Laufwerke

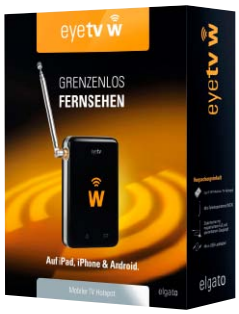
Powershell
- Alles automatisieren per Kommandozeile
- Schnelle Nutzer- und Rechtesteuerung

Windows Server
- Einrichten und verwalten
- Tricks zu den Windows Server Essentials

Christian Löbering,
stellv. Chefredakteur
cloebering@pcwelt.de

Für Profis?

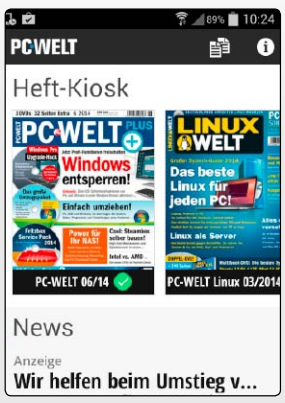
BEVOR MAN EIN MAGAZIN „Windows 8.1 für Profis“ nennt, sollte man sich überlegen, wen man damit eigentlich ansprechen will. Laut Wikipedia ist ein Profi – das Kurzwort von Professionist – jemand, der eine Tätigkeit beruflich ausübt und dafür in der Regel eine formale Qualifikation hat. Andererseits geht der Begriff aber auch darüber hinaus und zeichnet ganz allgemein jemanden mit einem erhöhten Maß an Kenntnissen und Fähigkeiten aus.
Und obwohl der Begriff Profi oft und gerne in den unterschiedlichsten Zusammenhängen verwendet wird, trifft er es hier eindeutig am besten. Denn dieses Magazin geht deutlich einen ganzen Schritt weiter als herkömmliche Windows-Magazine – und zwar in jeder Hinsicht. Egal also, ob Sie ein technisch interessierter Windows-Nutzer sind oder Windows tatsächlich beruflich einsetzen oder einsetzen werden: Hier finden Sie viele spannende Ratgeber, Tipps und Tricks, die Sie zum Windows-Profi machen.
Wie bei jedem neuen Magazin und hier ganz besonders sind wir auf Ihr Feedback angewiesen, und das soll sich natürlich auch für Sie lohnen. Füllen Sie dazu einfach den Fragebogen unter *www.pcwelt.de/profiumfrage* aus.
Als kleines Dankeschön erhalten Sie im Anschluss das PDF unseres PC-WELT-Sonderhefts „Aus für XP“ zum Windows-Umzug als Download. Außerdem verlosen wir unter allen Teilnehmern den mobilen TV-Hotspot Eye TV W von Elgato für Android, iPhone und iPad. Wir freuen uns auf Ihr Feedback.



Viel Spaß beim Lesen!

Jetzt testen! Die neue Kiosk-App von PC-WELT, LinuxWelt & Co.

Wir haben die Kiosk-App der PC-WELT komplett neu entwickelt – und die Vorteile für Sie liegen direkt auf der Hand: Alle Hefte, alle Reihen und alle Sonderhefte stehen dort für Sie bereit.
Als Abonnent – zum Beispiel der PC-WELT oder der LinuxWelt – bekommen Sie jeweils die digitale Ausgabe für Ihr Mobilgerät kostenlos dazu, auch mit speziell angepasstem Lesemodus und Vollzugriff auf die Heft-DVD. Die App läuft auf allen großen Mobil-Plattformen – iPhone, iPad, Android-Smartphone und -Tablet, Windows 8.1 und Windows Phone 8, allerdings noch nicht unter Linux.
Die erste Ausgabe, die Sie herunterladen, ist für Sie kostenlos. Um die App zu nutzen, installieren Sie die für Ihr Gerät passende Version einfach über die Download-Links unter *www.pcwelt.de/magazinapp*. Auf dieser Seite finden Sie auch alle Informationen zu den neuen Funktionen und zum schnellen Einstieg.
Übrigens: Wenn Sie eine digitale Ausgabe gekauft haben, können Sie sie auf allen Ihren Geräten lesen.



www.pcwelt.de/magazinapp

Das ist neu bei Windows 8.1

Windows 8.1 bietet mehr als die Rückkehr des Start-Buttons. Es bringt vor allem neue Enterprise- und Management-Funktionen. Ein wesentlicher Grund für kürzere Update-Intervalle ist die neue Positionierung des Betriebssystems für mobile und Touch-fähige Geräte.

8

Editionen und Lizenzierung

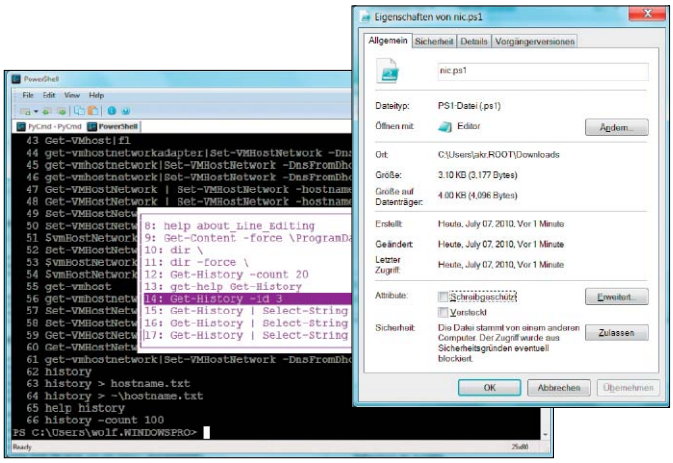
Microsoft hat bei der Einführung von Windows Server 2012 R2 überraschend ganz schön an der Preisschraube gedreht. Es gibt aber auch gute Nachrichten.

40

Windows & Netzwerk

Server

Virtualisierung



Gratis-Tools für Hyper-V

Zugegeben: Viele der kostenlosen Tools für Hyper-V sind nur Einsteigerversionen von kostenpflichtiger Software, aber es gibt auch ein paar gute Open-Source-Programme.

70

Einstieg in die Powershell

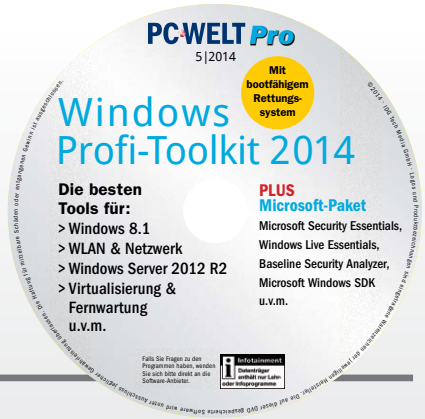
Aufgrund der strategischen Bedeutung von Powershell kommen Windows-Administratoren auf Dauer nicht umhin, sich mit dieser Kombination aus Kommandozeile und Script-Umgebung zu beschäftigen.

84

Powershell

Tools auf der Heft-DVD

6



Programme im Überblick

.NET Framework 4
.NET Framework 4.5
5nine Manager for Hyper-V Free 4.1
Active Sync 4.5
AD ACL Scanner 1.3.3
Altaro Hyper-V Backup Free Edition 4.1.26
Blat (32 Bit) 3.1.2
Blat (64 Bit) 3.1.2
Core Configurator (64 Bit) 2.0
Corefig for Windows Server 2012 Core and Hyper-V Server 2012 1.1.1
Dotnetfx Cleanup 11.11.2013
Easeus Partition Master Free Edition 10.0
Enhanced Mitigation Experience Toolkit 4.1
Excel Viewer 1
File Checksum Integrity Verifier 1.0
HV Backup 1.0.1
Inssider 3.1.2.1
Hyper V Mon 3.0.2
Linux Live USB Creator 2.8.28
Microsoft Baseline Security Analyzer (MBSA) (32 Bit) 2.3
Microsoft Baseline Security Analyzer (MBSA) (64 Bit) 2.3
Microsoft Security Essentials (XP, Vista, Win 7, Win 8,32 Bit) 4.5.216
Microsoft Security Essentials (XP, Vista, Win 7, Win 8, 64 Bit) 4.5.216
Microsoft Windows SDK for Windows 7 and .NET Framework 4 7.1
Minitool Partition Wizard Home Edition 8.1.1
Netfx Setupverifier 6.0
Nmap 6.46
NTFS Permissions Reporter Free 1.5.0
Openssl für Windows (64 Bit) 1.0.1 g
Openssl für Windows (32 Bit) 1.0.1 g
Paragon Partition Manager 2014 Free
Putty 0.63
Putty Portable 0.63
Remote App Tool 4.0.2.5
RSAT für Windows 8.1 (32 Bit)
RSAT für Windows 8.1 (64 Bit)
Starwind Native SAN for Hyper-V Free
Trilead VM Explorer Free Edition 5.0.020
Virtual Box 4.3.10
Visual C++ 2012 Redistributable Package (x64) Update 4
Visual C++ 2012 Redistributable Package (x86) Update 4
Vmware Player 6.0.2
Vmware SSL Certificate Automation Tool 5.5.0
VM Turbo Virtual Health Monitor for Microsoft Hyper-V
VM Turbo Virtual Health Monitor for Vmware ESX/Vsphere
Vmware Vsphere Hypervisor (ESXi) 5.5
Win SCP 5.5.3
Windows Live Essentials (Web-Installer) 2011
Word Viewer 1

Service

Highlights der Heft-DVD

Auf der Heft-DVD finden Sie die besten Tools für Administratoren von Windows-8-Rechnern, die wichtigsten Programme für die Virtualisierung und alles Nötige für die Festplattenverwaltung.

VON ARNE ARNOLD

WINDOWS-PROFIS FINDEN auf der DVD genau die kleinen Tools, die die Konfiguration, Wartung und Überwachung von Windows 8 einfach machen. So hilft Ihnen zum Beispiel das kostenlose Tool Blat dabei, Mails von der Kommandozeile aus zu versenden. So können Sie Überwachungsaufgaben ganz einfach automatisieren. Natürlich fehlen auch die Tools zur Partitionierung von Festplatten nicht, wenn Sie Windows auf neuen Rechnern installieren möchten. Das geht etwa mit den Gratis-Tool Easeus Partition Master Free. Zur Virtualisierung von Systemen gibt's Software von Vmware und Oracle sowie zahlreiche Zusatz-Tools.

Bootfähige Notfall-DVD: Falls bei der Konfiguration Ihrer Rechner mal etwas schiefläuft, können Sie diese mit der Heft-DVD booten und reparieren. Denn auf der DVD befindet sich ein leistungsfähiges Linux-Live-Notfall-System, mit dem Sie Daten retten oder ein vergessenes Windows-Passwort zurücksetzen können.

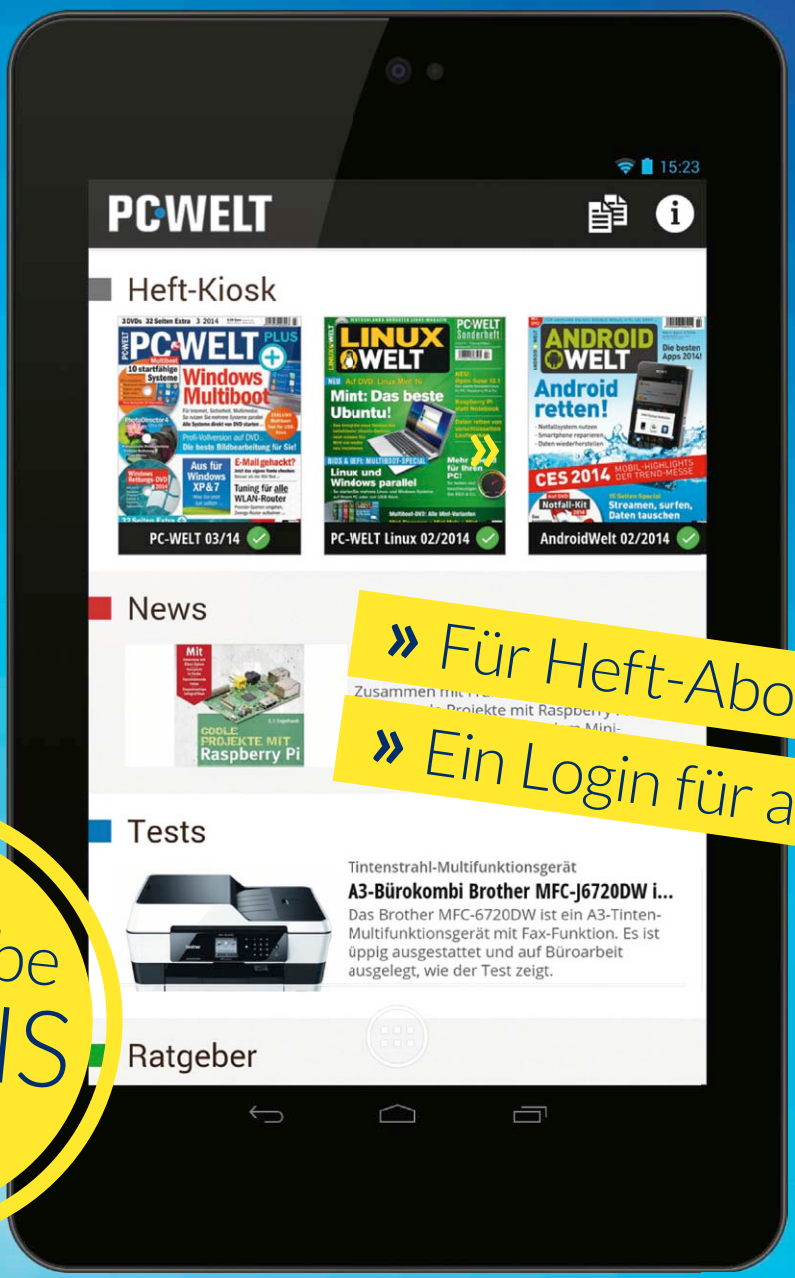
Auf Heft-DVD **Programme im Überblick**

.NET Framework 4
.NET Framework 4.5
5nine Manager for Hyper-V Free 4.1
Active Sync 4.5
AD ACL Scanner 1.3.3
Altaro Hyper-V Backup Free Edition 4.1.26
Blat (32 Bit) 3.1.2
Blat (64 Bit) 3.1.2
Core Configurator (64 Bit) 2.0
Corefig for Windows Server 2012 Core and Hyper-V Server 2012 1.1.1
Dotnetfx Cleanup 11.11.2013
Easeus Partition Master Free Edition 10.0
Enhanced Mitigation Experience Toolkit 4.1
Excel Viewer 1
File Checksum Integrity Verifier 1.0
HV Backup 1.0.1
Inssider 3.1.2.1
Hyper V Mon 3.0.2
Linux Live USB Creator 2.8.28
Microsoft Baseline Security Analyzer (MBSA) (32 Bit) 2.3
Microsoft Baseline Security Analyzer (MBSA) (64 Bit) 2.3
Microsoft Security Essentials (XP, Vista, Win 7, Win 8,32 Bit) 4.5.216
Microsoft Security Essentials (XP, Vista, Win 7, Win 8, 64 Bit) 4.5.216
Microsoft Windows SDK for Windows 7 and .NET Framework 4 7.1
Minitool Partition Wizard Home Edition 8.1.1
Netfx Setupverifier 6.0
Nmap 6.46
NTFS Permissions Reporter Free 1.5.0
Openssl für Windows (64 Bit) 1.0.1 g
Openssl für Windows (32 Bit) 1.0.1 g
Paragon Partition Manager 2014 Free
Putty 0.63
Putty Portable 0.63
Remote App Tool 4.0.2.5
RSAT für Windows 8.1 (32 Bit)
RSAT für Windows 8.1 (64 Bit)
Starwind Native SAN for Hyper-V Free
Trilead VM Explorer Free Edition 5.0.020
Virtual Box 4.3.10
Visual C++ 2012 Redistributable Package (x64) Update 4
Visual C++ 2012 Redistributable Package (x86) Update 4
VMT urbo Virtual Health Monitor for Microsoft Hyper-V
VM Turbo Virtual Health Monitor for VMware ESX/Vsphere Vmware Player 6.0.2
Vmware SSL Certificate Automation Tool 5.5.0
Vmware Vsphere Hypervisor (ESXi) 5.5
Win SCP 5.5.3
Windows Live Essentials (Web-Installer) 2011
Word Viewer 1

PC-WELT

Die **MAGAZIN-APP** für Android

Lesen Sie PC-WELT, AndroidWelt, LinuxWelt, GalaxyWelt und alle Sonderhefte digital.



» Für Heft-Abonenten gratis

» Ein Login für alle Devices

1. Ausgabe GRATIS für alle!

Kostenlos für Ihr Android Tablet oder Phone downloaden:

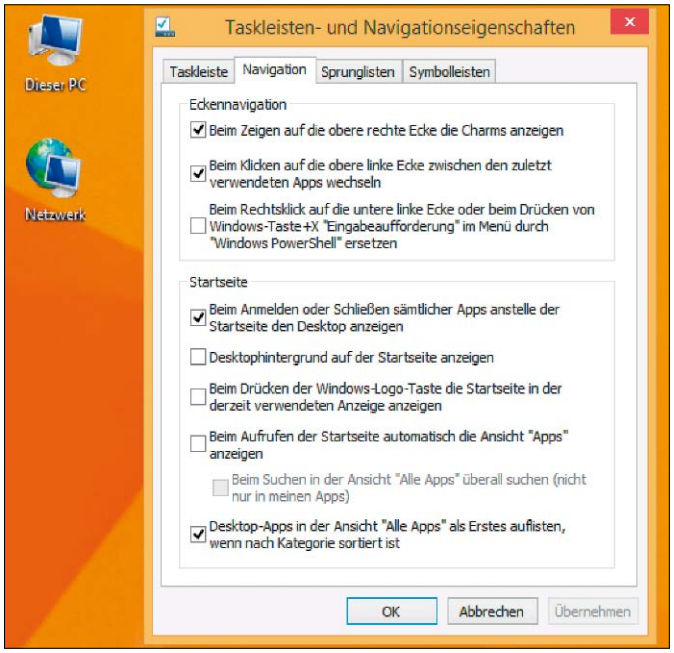
www.pcwelt.de/android

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Windows 8.1 – das ist neu

Windows 8.1 bietet mehr als die Rückkehr des Start-Buttons. Neben der verbesserten Bedienbarkeit für Desktop-Benutzer bringt es vor allem neue Enterprise- und Management-Funktionen.

VON WOLFGANG SOMMERGUT



Die Eigenschaften der Taskleiste bieten mehrere Optionen, mit denen man das Verhalten von Startseite und Desktop steuern kann.

WINDOWS 8.1 IST NICHT NUR wegen seiner Neuerungen interessant, sondern auch, weil es den Beginn einer neuen Update-Politik markiert. Es handelt sich dabei um das erste Minor Release seit Windows 3.1, also seit 1992. Microsoft möchte künftig die langen Intervalle zwischen neuen Windows-Versionen auf einen Ein-Jahres-Rhythmus verkürzen. Dabei kann es sich um Major oder ein Minor Release handeln oder wie zuletzt einfach um ein „Update".

Ein wesentlicher Grund für kürzere Update-Intervalle ist die neue Positionierung des Betriebssystems für mobile und Touch-fähige Geräte. In diesem Marktsegment ist Microsoft ein Nachzügler, der mit dem hohen Innovationstempo seiner Hauptkonkurrenten Google und Apple mithalten muss. Aber auch beim Wettlauf um Browser-Marktanteile reicht es nicht aus, den Internet Explorer wie bisher nur alle drei oder vier Jahre zusammen mit einem Update von Windows zu aktualisieren.

Windows 8 brachte wenig für Desktop-User und Firmen

Windows 8 stand ganz und gar im Zeichen der neuen Mobility- und Touch-Strategie, die sich vor allem in der neuen Kacheloberfläche und den dazugehörigen Apps manifestierte. Für traditionelle Desktop-Benutzer, die das System mit Maus und Tastatur bedienen und auf einen großen Monitor blicken, brachte dieses große Update praktisch gar nichts – im Gegenteil.

Aus der Perspektive von Unternehmen, die Windows überwiegend auf PCs und Notebooks einsetzen, kam hinzu, dass die Version 8 auch keine nennenswerten Neuerungen für Administratoren und professionelle User brachte.

Dem Update auf Windows 8.1 kam also die Aufgabe zu, die Mehrheit von Microsofts Stammkunden mit der neuen Bedienerführung zu versöhnen und Enterprise-Feature zu liefern, die einer Firma als Argumente für ein Update dienen können.

Korrekturen und Verbesserungen in der Bedienerführung

Vor allem die Entscheidung von Microsoft, Windows 8 als hybrides System zu konzipieren und neben dem klassischen Desktop eine separate Touch-Oberfläche anzubieten, stieß bei vielen PC-Nutzern auf geringe Zustimmung. Die Bedienung der Apps mit Maus und Tastatur erwies sich oft als umständlich, außerdem erforderte das gänzlich andere Bedienkonzept einigen Lernaufwand. Die diversen Spekulationen vor der offiziellen Ankündigung von Windows 8.1 drehten sich daher vor allem um die Rücknahme bestimmter Änderungen in der Bedienerführung, die Windows 8 gegenüber seinem Vorgänger brachte. Ganz oben auf der Wunschliste stand die Rückkehr des Startmenüs. Tatsächlich bringt Windows 8.1 den Start-Button zurück. Doch zur großen Enttäuschung vieler Nutzer enthält er aber kein Menü mehr, sondern er führt einfach zur Kacheloberfläche.

Eine weitere Änderung der Benutzeroberfläche erlaubt das Booten direkt auf den herkömmlichen Desktop, was vor allem bei der Nutzung auf PCs erwünscht ist. Hinzu kommen eine flexiblere Anordnung der Kacheln auf dem Startbildschirm sowie eine Aktualisierung von fast allen vorinstallierten Apps. Außerdem enthält es einige neue Anwendungen für die Kacheloberfläche, darunter zum Beispiel einen Taschenrechner, einen Wecker und eine App zur Verwaltung von Leselisten.

Mausfreundliche Kacheln

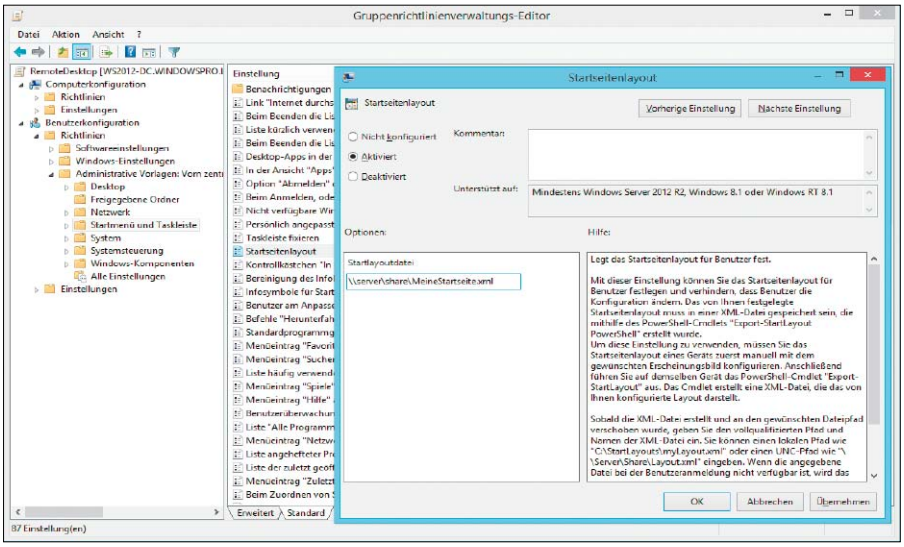
Das Update von Windows 8.1 geht in dieser Hinsicht noch weiter, indem es die neue Touch-optimierte Startseite und die darauf laufenden Apps um Bedienelemente ergänzt, die der Benutzung mit Maus und Tastatur entgegenkommen. So erhalten die Apps, die weiterhin nur im Vollbildmodus laufen, eine Titelleiste, die wie gewohnt einen Button zum Schließen der Anwendung enthält.

Hinzu kommt das ebenfalls vom Desktop her bekannte Kontextmenü, das sich durch einen Rechtsklick auf eine Kachel öffnen lässt. Es enthält jene Einträge, die bisher ausschließlich am unteren Bildschirmrand in einer Charms-Bar angezeigt wurden. Auch die rechte Leiste muss einige Icons abtreten, die künftig direkt auf der Startseite zu finden sind. Dazu zählen solche für die Suche und das Herunterfahren des Systems. Eine engere Integration der zwei Oberflächen möchte Microsoft dadurch erreichen, dass sich jetzt auch Modern Apps auf der Taskleiste festpinnen lassen. Man kann sie so auf die gleiche Weise starten wie herkömmliche Windows-Anwendungen und auf diesem Weg zwischen den Anwendungen umschalten.

Eine häufige Kritik an Windows 8 galt der Suchfunktion, die ihre Ergebnisse automatisch in die Kategorien Apps, Einstellungen und Dateien aufteilt. Eine gesamte Übersicht über sämtliche Treffer bietet sie jedoch nicht. Eine solche kommt nun in Windows 8.1, ergänzt um Ergebnisse der Websuche von Bing und von Dateien auf Onedrive. Letzteres erhält zudem einen prominenten Platz unter „Dieser PC“.

App als Alternative zur Systemsteuerung

Ebenfalls in vielen Kommentaren bemängelt wurde die inkonsistente Verwaltung von Windows 8. Sie entspringt in erster Linie den unvollständigen Funktionen der App PC-Einstellungen, so dass man immer wieder zur Systemsteuerung des Desktops wechseln muss, um das System anzupassen. Windows 8.1 beendet diesen besonders auf Touch-Geräten unerfreulichen Zustand, indem die Kachel-Anwendung nun die gängigsten Aufgaben der Systemsteuerung übernehmen kann.



Die Einstellung „Start Screen Layout“ legt fest, welche Startseite per GPO vorgegeben wird.

Explorer ohne Bibliotheken

Während Microsoft den Desktop-Benutzern mit der Rückkehr des Start-Buttons entgegenkommt, räumt es andererseits weitere Windows-7-Merkmale ab. Nachdem Windows 8 bereits Aero zugunsten einer 2D-Oberfläche eliminierte, opfert Windows 8.1 nun auch das Konzept der Bibliotheken. Die von „Windows Explorer“ auf „Explorer“ umbenannte Shell blendet Standard-Bibliotheken wie Dokumente, Bilder oder Musik nicht mehr ein.

Diese lassen sich aber auf Wunsch weiterhin anzeigen, indem man in „Ordneroptionen“ unter der Registerkarte „Allgemein“ die entsprechende Einstellung aktiviert. Darüber hinaus kann man auch wie gewohnt neue Ordner den Bibliotheken hinzufügen oder neue Bibliotheken anlegen.

Internet Explorer 11

Windows 8.1 bringt ein Major Release des Internet Explorer, wobei der Versionssprung durch die neuen Funktionen im IE 11 kaum gerechtfertigt ist. Sie betreffen primär die Usability in der App-Version des Browsers, beispielsweise durch die Unterstützung der Screen Orientation API. Hinzu kommen generelle Performance-Verbesserungen sowie die Implementierung weiterer HTML-5-Elemente, darunter ein verbesserter Editor.

Für Webentwickler bringt der IE 11 vollständig überarbeitete Developer Tools, darunter ein DOM-Inspektor und Profiler für die Performance von Webseiten sowie für den Speicherverbrauch. Der Internet Explorer 11 ist kein exklusives Feature von Windows 8.1, sondern steht in seiner Desktop-Ausprägung auch für Windows 7 zur Verfügung.

Enterprise-Modus für den IE 11

Ein weiteres Entgegenkommen gegenüber Firmenkunden stellt in Windows 8.1 Update der sogenannte Enterprise Mode für den Internet Explorer 11 dar. Er emuliert die Rendering Engine des älteren IE 8, so dass Seiten, die für diese Version des Browsers entwickelt wurden, im neuesten IE ohne größere Kompatibilitätsprobleme angezeigt werden.

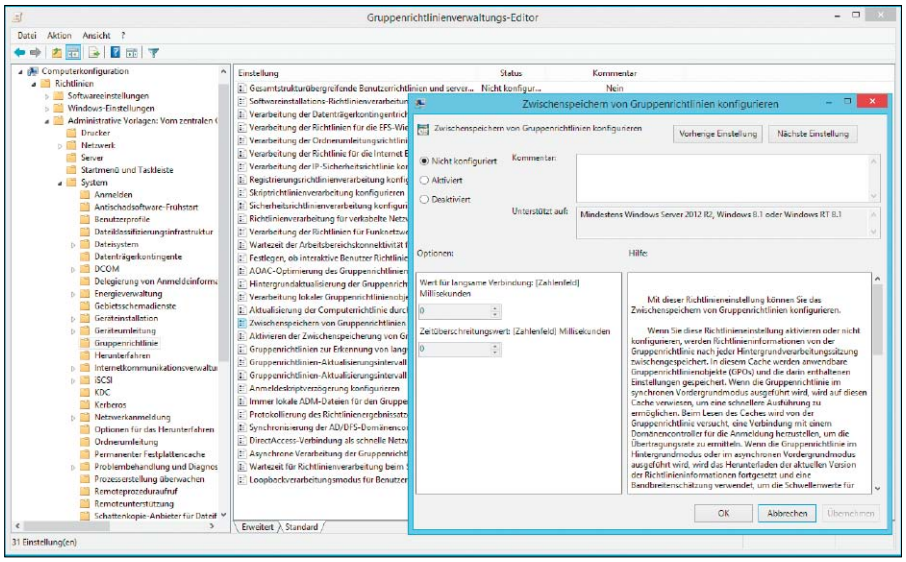
Der Name des Features verweist darauf, dass es hauptsächlich für die Ausführung von Webanwendungen benötigt wird, die Firmen intern entwickelt haben und die sie an einem Upgrade des Browsers hindern. Ein solches ist unausweichlich, weil unter Windows 8.x nur die IE-Versionen 10 und 11 zur Verfügung stehen. Unverzichtbare Webapplikationen, die für den IE8 optimiert wurden, würden sich daher in vielen Firmen als Hürde für die Migration auf Windows 8.1 erweisen.

Außerdem sieht der Enterprise-Modus ein zentrales Management über Gruppenrichtlinien vor, das eine Liste von URLs definiert, die eine Darstellung nach Art des IE8 benötigen.

Neue Business-Funktionen

Windows 8 war wie erwähnt primär ein Consumer-Release mit Schwerpunkt auf mobile Geräte, das relativ wenige Verbesserungen für den Firmen-Desktop brachte. Aber auch die neue Touch-Oberfläche wies für den Einsatz im professionellen Umfeld vor allem Defizite beim zentralen Management auf. Windows 8.1 schließt nun einige dieser Lücken und bringt Fortschritte bei Mechanismen zur Systemverwaltung, etwa den Gruppenrichtlinien.

Die Konfiguration des zugewiesenen Zugriffs erfolgt über die PC-Einstellungen und benötigt ein lokales Konto.



Über eine eigene Einstellung lässt sich das GPO-Caching konfigurieren oder abschalten.

Beitritt zu Domäne über Workplace Join

Der normale Beitritt zu einer Domäne ist wie in der Vergangenheit nur über die Systemsteuerung oder die Kommandozeile möglich und für Windows RT gänzlich ausgeschlossen. Die Mitgliedschaft in einer Domäne ist normalerweise firmeneigenen PCs vorbehalten und bedarf eines autorisierten Benutzers, der zum Beitritt befugt ist. Windows 8.1 bietet mit Workplace Join einen alternativen Weg, der über eine eigene App führt. Er sieht vor, dass Benutzer alle die von ihnen verwendeten, auch privaten Geräte im Active Directory (AD) registrieren. Dies erfolgt über eine Zwei-Faktor-Authentifizierung, bei der sich die User über ihre Mailadresse anmelden und anschließend ein Token zur Anmeldung bekommen.

Für die Nutzung von privaten Geräten am Arbeitsplatz (BYOD – Bring Your Own Device) kündigte Microsoft eine Funktion für das „Mobile Information Management" an. So lassen sich Firmendaten in einem gesicherten Bereich auf mobilen Geräten speichern und auch remote löschen., so dass sie sich auch ohne Zugriff auf das Unternehmensnetz nutzen lassen. Sie können von der IT bei Bedarf remote entfernt werden, ohne andere Daten auf einem privaten Gerät des Mitarbeiters zu löschen.

Startbildschirm über Gruppenrichtlinien verwalten

Eine Schwachstelle bei der Verwaltung von Windows 8 besteht darin, dass man zwar vor dem Deployment den Startbildschirm anpassen und damit für alle Benutzer vorgeben kann, aber sich dieser anschließend nicht einfach mit Bordmitteln zentral auf einen Standard festlegen lässt.

Windows 8.1 sieht nun vor, dass man die Konfiguration des Startbildschirms in einer Referenzinstallation per Powershell exportieren (mit dem Cmdlet *export-startlayout*) und anschließend per Gruppenrichtlinie verteilen kann. Die betreffenden User erhalten dann nach dem nächsten Log-on die vom Administrator vorgegebene Kacheloberfläche. Dabei besteht die Möglichkeit, den Startbildschirm gegen Veränderungen zu sperren. Die extreme Form einer solchen abgesperrten Konfiguration nennt sich in Windows 8.1 Assigned Access, bei dem es sich im Prinzip um einen Kiosk-Modus handelt. Er beschränkt das System auf die Ausführung einer einzigen Modern App, der Zugriff auf Systemdateien und andere Apps wird verhindert.

Zu diesem Zweck muss man ein lokales Benutzerkonto festlegen, das mit dem Kiosk-Modus assoziiert wird. Eine Verwendung von Domänen-Konten ist in diesem Zusammenhang nicht möglich, entsprechend sieht Microsoft auch keine zentrale Verwaltung des Assigned Access, etwa über GPOs, vor.

Mobile Device Management

Microsoft verbessert die Management-Fähigkeiten von Windows 8.1 zusätzlich durch die Implementierung von Open MDM. Es handelt sich dabei um standardisierte APIs für das Mobile Device Management, die von der Open Mobile Alliance verabschiedet wurden.Microsoft nennt im Blog Windows for your Business *(http://blogs.windows.com/windows/b/business)* als Hauptvorteil von Open MDM, dass Anbieter von Lösungen für das Mobile Device Management nun Windows 8.1 ohne zusätzlichen Agent verwalten könnten. Gemeint ist, dass sie Geräte mit unterschiedlichen Betriebssystemen über eine einzige Schnittstellte ansprechen können, vorausgesetzt, diese verfügen ebenfalls über die Standard-APIs.

Neue Netzwerkfunktionen

Zu den weiteren Verbesserungen von Windows 8.1 zählt eine Reihe neuer Netzwerkfunktionen. Darunter fällt die einfachere Nutzung von Netzwerkdruckern, weil Windows 8.1 nun Tap-to-pair beherrscht, wenn ein Drucker mit einem NFC-Tag ausgestattet ist. Eine manuelle Konfiguration des Druckers auf dem Gerät entfällt damit. Zusätzlich unterstützt das Betriebssystem Wi-Fi Direct Printing, so dass man einen Drucker drahtlos ansprechen kann, ohne dafür eigens einen Treiber zu installieren.

Broadband Tethering verwandelt einen PC oder ein Tablet unter Windows 8.1, das über ein 3G- oder 4G-Netzwerk verbunden ist, in einen WLAN-Hotspot für bis zu zehn andere Geräte. Außerdem erlaubt die Unterstützung von Miracast das drahtlose Übertragen von Bildschirminhalten auf Projektoren oder Fernseher, so dass sich etwa Tablets für die Präsentation von Powerpoint-Folien einsetzen lassen.

Sicherheits-Features

In puncto Sicherheit bringt Windows 8.1 Auto-triggered VPN, so dass der Zugriff auf eine

Ressource, die eine VPN-Verbindung benötigt, den Benutzer automatisch zur Anmeldung am VPN auffordert. Dies soll nicht nur mit dem Windows-eigenen Client, sondern auch mit solchen von anderen Anbietern funktionieren. Schließlich erweitert Microsoft die integrierte Antiviren-Software Defender um Network Behavior Monitoring, mit dem es versucht, die Verbreitung bis dato unbekannter Malware zu verhindern. Der Internet Explorer wird den Defender nutzen, um Add-ons vor der Ausführung zu untersuchen.

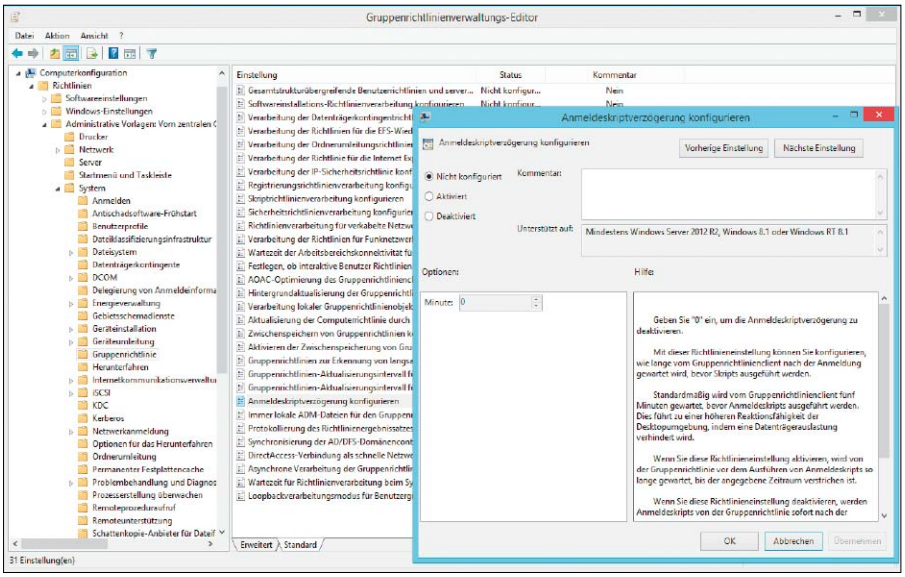
Caching von Group Policy Objects bei langsamen Netzwerken

Wie praktisch alle Windows-Updates führte auch die Version 8.1 zusätzliche Einstellungen für Gruppenrichtlinien ein, mit denen sich neue Features konfigurieren lassen. Dazu zählte etwa die Verwaltung von Boot to Desktop oder Start Screen Control, mit dem sich die Startseite zentral für alle User vorgeben lässt. Sämtliche neuen Einstellungen für Windows 8 und Server 2012 R2 sind in Microsofts GPO-Tabelle (*http://www.microsoft.com/en-us/download/details.aspx?id=25250*) dokumentiert.

Windows 8.1 erweitert nicht nur den Richtlinienumfang, sondern ändert auch das Verhalten der GPO-Engine selbst in einigen wichtigen Punkten. Sie verfolgen den Zweck, den Anmeldevorgang zu verkürzen oder zusätzliche Aktionen während der periodischen Aktualisierung von GPOs abzuarbeiten. Auch die am häufigsten erwähnte Neuerung, das Group Policy Caching, dient der Zwischenspeicherung von GPOs auf lokalen Laufwerken. Es ist allerdings auf langsame Netzwerke beschränkt, wo die Client Side Extensions auf das Herunterladen von GPOs vom Domänen-Controller verzichten und stattdessen lokale Kopien verwenden.

Das Caching greift allerdings nicht bei der Abarbeitung von allen GPOs, sondern nur dann, wenn beim Starten von Windows und beim Anmelden eines Benutzers ein Vordergrundprozess läuft. Dagegen erfolgt die periodische Ausführung von GPOs während einer User-Session im Hintergrund. Als weitere Bedingung gilt, dass eine Aktion den synchronen Modus erzwingt. Das trifft etwa auf die Software-Installation oder die Ordnerumleitung zu.

Aufgrund dieser Einschränkungen ist der Nutzen für das GPO Caching klar umrissen: Es soll das Booten von PCs oder das Anmelden von Benutzern beschleunigen, wenn der Domain Controller (DC) nur über ein langsames Netz erreichbar ist und eine Aktion ausgeführt werden soll, die nur synchron ablaufen kann. Entgegen mancher Erwartung dient das Feature keinesfalls dazu, GPOs dann anzuwenden, wenn der Client offline ist beziehungsweise keine Verbindung mit einem DC hat. Wer dieses Feature deaktivieren möchte, kann es über die folgende Einstellung abschalten: „Computerkonfiguration → Richtlinien → Administrative Vorlagen → System → Gruppenrichtlinie → Zwischenspeichern von Gruppenrichtlinien konfigurieren".



Die Anmeldescript-Verzögerung von 8.1 lässt sich über eine eigene Einstellung konfigurieren oder abschalten.

Zeitverzögerte Log-in-Scripts unter Windows 8.1

Eine weitere Neuerung von Windows 8.1, die den Anmeldevorgang beschleunigen soll, besteht in der zeitversetzten Ausführung von Log-in-Scripts. Sie starten per Voreinstellung erst fünf Minuten, nachdem der Benutzer bereits den Desktop angezeigt bekommt.

Bei der Einführung dieses Features ist Microsoft wohl davon ausgegangen, dass die meisten Anwender das Mapping von Laufwerken und Druckern über Group Policy Preferences realisieren. Tun sie das nicht und setzen dafür weiterhin auf Log-in-Scripts, dann stehen Netzwerklaufwerke nach dem Anmelden noch nicht zur Verfügung. Möchte man diesen Zustand vermeiden, dann kann man die Wartefrist bis zum Start der Scripts reduzieren oder komplett eliminieren. Für diesen Zweck ist eine neue Einstellung unter „Computerkonfiguration → Richtlinien → Administrative Vorlagen → System → Gruppenrichtlinie → Anmeldeskriptverzögerung zuständig".

Netzlaufwerke im Hintergrund verbinden

Group Policy Preferences können fast alle Aufgaben übernehmen, für die traditionell Log-in-Scripts verwendet werden. Sie ersparen dem Admin nicht nur die Programmierung von Batch-Dateien oder sonstigen Scripts, sondern lassen sich über das Item „Level Targeting" (Zielgruppenadressierung) genauer bestimmten Computern oder Benutzern zuordnen.

Windows 8.1 bringt eine weitere Verbesserung beim Verbinden von Netzlaufwerken über Group Policy Preferences, indem dieser Vorgang als Hintergrundprozess läuft. Das Drive-Mapping erfolgt nicht nur beim Anmelden des Benutzers, sondern bei der periodischen Ausführung von GPOs während einer User-Session oder nach dem Aufruf von *gpupdate*.

In der Praxis kann also der Administrator die Laufwerkszuordnungen ändern, ohne dass sich die betroffenen User ab- und anmelden müssen. Seit Windows 8 lassen sich GPOs auch remote über die Gruppenrichtlinienverwaltung aktualisieren, so dass man in dringenden Fällen die Netzlaufwerke sofort verändern kann.

Group Policy Preferences mit Support für IPv6

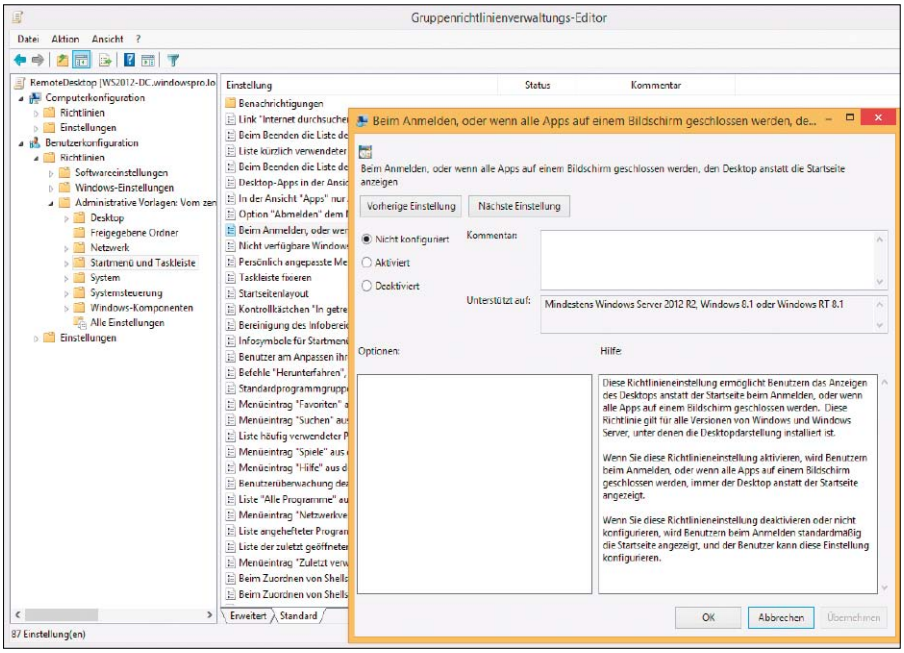
Eine Neuerung bringt Windows 8.1 schließlich mit der Unterstützung für IPv6 in den Group Policy Preferences. Diese erscheint in verschiedenen Kontexten. So kann man zum Beispiel die Geltung von GPOs über das Item „Level Targeting" auf bestimmte IPv6-Adressbereiche eingrenzen. Der IPv6-Support zeigt sich auch beim Konfigurieren eines TCP/IP-Druckers. Denn nun kann man alternativ zu IPv4 eine IPv6-Adresse vergeben.

Die entsprechende Option „Verwenden Sie eine IPv6-Adresse" unter „Einstellungen → Systemsteuerungseinstellungen → Drucker" ist aufgrund eines Darstellungsfehlers des lokalisierten Textes aber kaum zu entziffern. ■

Windows 8.1 zentral verwalten

Windows 8 brachte tiefgreifende Veränderungen für das Betriebssystem, ließ aber das zentrale Management vieler Neuerungen vermissen. Die Version 8.1 holt dies in einigen wichtigen Punkten nach.

VON WOLFGANG SOMMERGUT



Die meisten Einstellungen aus der Taskleiste gibt es auch für GPOs, darunter auch Boot to Desktop.

DIE AUFFÄLLIGSTE und bahnbrechende Änderung von Windows 8 bestand bekanntermaßen darin, dass es neben dem traditionellen Desktop eine zusätzliche Touch-optimierte Oberfläche einführte, die vor allem für den Einsatz auf mobilen Geräten gedacht ist.

Die erste Inkarnation dieses hybriden Systems hatte aus der Sicht von professionellen Anwender zwei wesentliche Defizite: Zum einen ließ sich das neue Subsystem nur sehr eingeschränkt zentral administrieren, und zum anderen benachteiligte das neue Design jene, die ihr Endgerät mit Maus und Tastatur bedienen. Microsoft reagierte mit Windows 8.1 auf das Feedback der Kunden, indem es Management-Funktionen für die Kacheloberfläche nachlieferte und mehr Rücksicht auf traditionelle PC-Nutzer nahm. Letzteres äußerte sich unter anderem darin, dass der Bootvorgang nicht mehr zwangsläufig auf der neuen Startseite enden muss. Die Option lässt sich erfreulicherweise auch noch zentral über GPOs steuern.

Die Gruppenrichtlinien als das wesentliche Instrument der zentralen Windows-Administration dehnen damit ihren Wirkungsbereich auf das neue Gesicht von Windows 8.x aus. Sie erfahren zusätzlich eine Aufwertung dadurch, dass noch mehr Aktionen als bisher asynchron ausgeführt werden. Das gilt besonders für die Verbindung von Netzlaufwerken.

Boot to Desktop

Neben der Wiederherstellung des Start-Buttons wünschten sich viele Benutzer von Windows 8, dass der herkömmliche Desktop anstelle der neuen Startseite nach dem Booten des Betriebssystems angezeigt wird. Microsoft reagierte darauf in Windows 8.1 mit der Funktion „Boot to Desktop“. Diese bietet die Möglichkeit, Windows so zu konfigurieren, dass es nach dem Start oder nach dem erneuten Logon den Desktop anzeigt. Diese Einstellung bewirkt außerdem, dass man nach dem Beenden der letzten App automatisch auf der herkömmlichen Oberfläche landet.

Boot to Desktop aktiviert man in den Einstellungen der Taskleiste, wo man zur Registerkarte „Navigation“ wechselt. Dort ist im Abschnitt „Startseite“ gleich die erste Option dafür zuständig. Zusätzlich kann man noch dafür sorgen, dass die neue Startseite in der Kategorienansicht zuerst die herkömmlichen Windows-Anwendungen zeigt. Auch dies kommt dem Desktop-Benutzer entgegen, dem die Startseite ja als Ersatz für das Startmenü dienen soll.

Per GPOs zum Desktop starten

Für zentral verwaltete PCs führte Microsoft mit Windows 8.1 eine Gruppenrichtlinie ein, mit der man den Desktop als Standardoberfläche

nach dem Booten des Rechners festlegen kann. Sie heißt „Beim Anmelden oder Schließen sämtlicher Apps anstelle der Startseite den Desktop anzeigen“ und findet sich unter „Benutzerkonfiguration → Administrative Vorlagen → Startmenü und Taskleiste“. Als weitere Einstellungen finden sich dort andere Optionen aus den Eigenschaften der Taskleiste, nämlich die, die sich dort unter „Navigation → Startseite“ befinden. Dazu zählen die erwähnte „Desktop-Apps in der Ansicht ‚Apps‘ als Erste auflisten“ sowie „Ansicht ‚Apps‘ automatisch anzeigen, wenn der Benutzer zur Startseite wechselt“.

So geben Sie die Startseite für alle Benutzer vor

Der Wunsch vieler Anwender, direkt nach dem Booten des Systems auf dem herkömmlichen Desktop zu landen, spiegelt die relativ geringe Akzeptanz der neuen Oberfläche wider. Diese wird auch von Umfragen bestätigt, denen zufolge eine Mehrheit der PC-Nutzer nur selten oder gar nie eine der neuen Apps verwendet. Wenn allerdings Unternehmen der neuen Kacheloberfläche größere Aufmerksamkeit schenken, etwa weil sie Windows 8.x auf mobilen Geräten einsetzen möchten, dann erwarten sie auch, dass sie die Startseite wie vom Desktop gewohnt zentral verwalten können.
Windows 8 erlaubte zwar die individuelle Anpassung der Startseite vor dem Deployment des Betriebssystems, aber sie ließ sich nicht gegen unerwünschte nachträgliche Änderungen schützen. Das Verteilen einer zentralen Konfigurationsdatei wirkte sich zudem nur auf neue Profile aus und blieb für vorhandene Konten ohne Folgen.
Zu den Neuerungen von Windows 8.1 zählt die Möglichkeit, die Einstellungen für den Startbildschirm aus einer Referenzinstallation zu exportieren und unternehmensweit über Gruppenrichtlinien zu verteilen. Hinzu kommen Einstellungen, die Benutzer am Ändern der vorgegebenen Startseite hindern oder die für eine neue App auf dem Startbildschirm automatisch eine Kachel einrichten.

Musterhafte Startseite mit Powershell exportieren

Windows 8.1 beseitigt nun in der Enterprise Edition die größten Defizite beim Management der Startseite, so dass diese zentral angepasst und für einzelne Benutzergruppe vorgegeben werden kann. Die Konfiguration der Kacheloberfläche wird dazu im ersten Schritt bei einer Musterinstallation mit Hilfe von Powershell exportiert. Zuständig ist für diese Aufgabe ist das neue Cmdlet *Export-StartLayout:*

Desktop-Anwendungen als Standardansicht der Startseite lassen den Verlust des Startmenüs leichter verschmerzen.

```
Export-StartLayout -Path \\server
 \share\MyStartLayout.xml -As XML
```

Dieser Beispielaufruf zeigt im Wesentlichen alle Möglichkeiten des Befehls, der nur die Konfiguration des aktuellen Benutzers erfassen kann. Zur Auswahl stehen ein XML- und ein binäres Format, wobei man Letzteres mit dem Parameter *-As BIN* erzeugen kann. Es ist etwas kompakter als das XML-Pendant, lässt sich aber nicht für die Gruppenrichtlinie verwenden. Die exportierten Daten beschränken sich auf die Namen der Apps, die als Kacheln auf der Oberfläche präsent sind, ihre Größe und Anordnung. Man speichert die Datei am besten auf einer Netzfreigabe, damit sie bei der Verteilung mittels Gruppenrichtlinie von allen PCs gefunden werden kann.

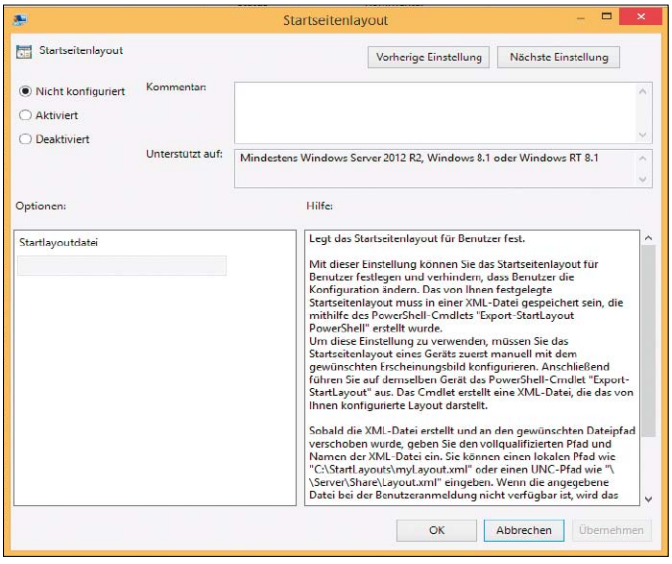
Neue Einstellung Startseitenlayout

Die Durchsetzung der Standardoberfläche übernimmt die neue Einstellung „Startseitenlayout“. Man findet sie unter „Benutzerkonfiguration → Richtlinien → Administrative Vorlagen → Startmenü und Taskleiste“.

Da es sich um eine für Windows 8.1 und Server 2012 R2 neu eingeführte Richtlinie handelt, muss man sie entweder unter Windows 8.1 mit installiertem RSAT verwalten oder die ADMX-Vorlagen von dort auf einen PC mit Windows 7/8 oder in einen zentralen Speicher kopieren. Wenn man die Einstellung „Startseitenlayout“ aktiviert, dann muss man im GPO-Editor den (UNC-)Pfad zu jener Datei angeben, in der die exportierte Konfiguration der Startseite gespeichert ist. Alle User, auf die das GPO angewandt wird, erhalten bei der nächsten Anmeldung eine Startseite nach den Vorgaben der Musterinstallation, aus der ihr Layout exportiert wurde.

Vorgegebene Startseite lässt sich nicht ändern

Ein Nebeneffekt dieser Richtlinie besteht darin, dass die User nach Anwendung des GPO keine Möglichkeit mehr haben, die Startseite zu verändern. Eine solche Sperre kann man auch unabhängig vom einheitlichen Startseiten-Layout erreichen. Für diesen Zweck exis-



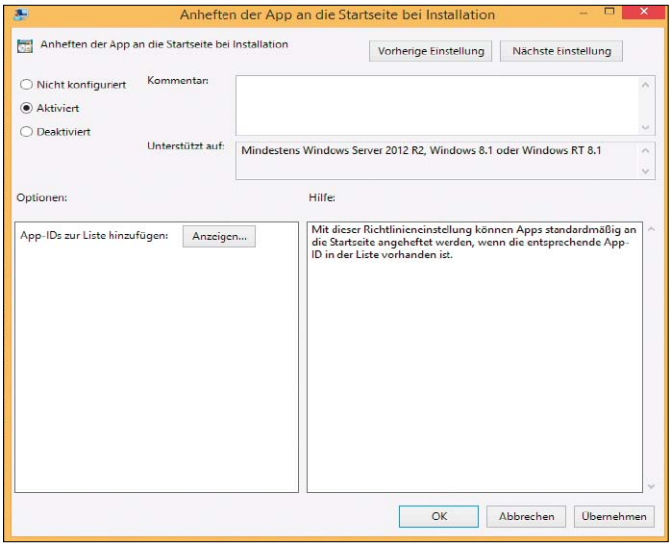
Die exportierten Einstellungen der Startseite sind überschaubar und lassen sich für GPOs nur im XML-Format nutzen.

tiert nämlich die neue Einstellung „Benutzer am Anpassen ihrer Startseite hindern“. Mit ihr lässt sich eine standardisierte Startseite schützen, die bereits vor dem Deployment des Betriebssystems definiert wurde.
Die Überschneidung zwischen den beiden Einstellungen ist ungünstig, weil ohne Not verhindert wird, einen Standard vorzugeben, der von den Benutzern angepasst werden kann. Sinnvoller wäre es, wenn „Startseitenlayout“ die Startseite nicht gegen Anpassungen abschotten würde.
Benötigt man jedoch einen solchen Schutz, dann könnte man die Richtlinie mit der Einstellung „Benutzer am Anpassen ihrer Startseite hindern“ kombinieren.

Apps automatisch an die Startseite pinnen

Neben den beiden genannten Einstellungen gibt es noch die weniger rigide Variante, installierte Apps automatisch an die Startseite anzuheften. Zu diesem Zweck muss man in der Einstellung „Anheften der App an die Startseite bei Installation“ eine Liste von IDs jener Apps eintragen, für die diese Richtlinie gelten soll.

Auch das lässt sich per GPO ändern: Wenn man in der betreffenden Einstellung die ID der gewünschten Apps eingibt, werden sie automatisch an die Startseite angeheftet.

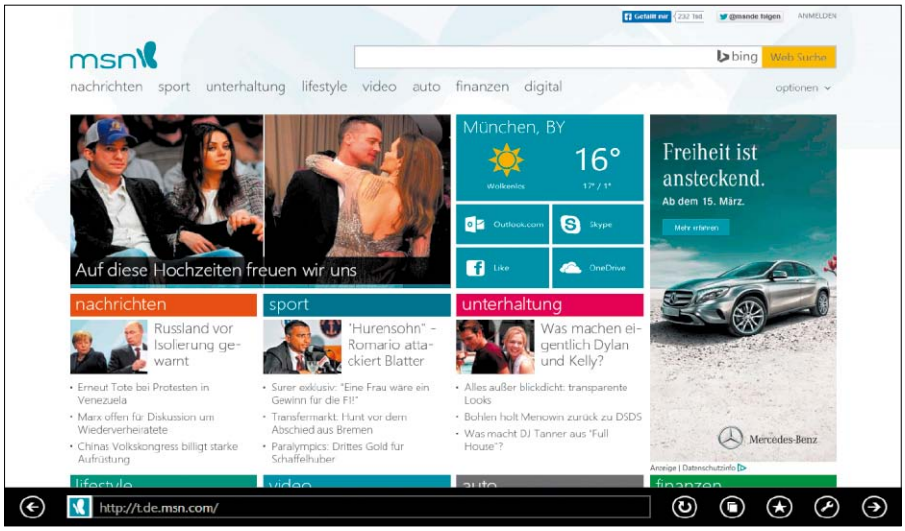


So bringen Sie Windows 8.1 in den Kiosk-Modus

Eine weitere Neuerung von Windows 8.1 öffnet Apps für Nutzungsszenarien jenseits von mobilen Geräten und PCs. Sie ist in erster Linie gedacht für Touch-befähigte stationäre Geräte, also vornehmlich für Info-Terminals.
Auf öffentlich zugänglichen Informationskiosken und ähnlichen Geräten sollen die Rechte der User weitgehend eingeschränkt bleiben, so dass sie das System nicht verändern können. Das wichtigste Merkmal dieser Betriebsart besteht somit darin, dass Anwender nur mit einem Programm arbeiten können, das beim Start automatisch lädt und das ein Benutzer nicht beenden kann.
Während man in der Windows-Frühzeit den Explorer über einen INI-Eintrag relativ leicht durch ein anderes Programm ersetzen konnte, lassen sich herkömmliche Anwendungen weiterhin über GPOs als Shell festlegen. Der zugewiesene Zugriff in Windows 8.1 ändert in dieser Hinsicht nichts, weil er nur die exklusive Ausführung von Store Apps vorsieht.

Konto in den PC-Einstellungen administrieren

Der zugewiesene Zugriff ist an lokale Benutzerkonten gebunden. Meldet sich jemand unter einer solchen Kennung an, dann erhält er nur die App, die dem Konto vorher zugeteilt wurde. Aufgrund der Bindung an lokale Accounts ist eine Konfiguration des Kiosk-Modus über GPOs nicht vorgesehen. Das einzige Tool für diesen Zweck ist die App PC-Einstellungen.
Diese Kachelalternative zur Systemsteuerung kann lokale Konten verwalten. Im entsprechenden Abschnitt findet sich der Eintrag „Weitere Konten“ und dort wiederum der Link „Konto für zugewiesenen Zugriff einrichten.“
Bevor man diesen Befehl ausführt, muss man zwei Voraussetzungen schaffen. Zum einen ist dafür zu sorgen, dass ein lokaler User als Mitglied der Gruppe „Standardbenutzer“ existiert. Zum anderen muss sich dieser schon vorher zumindest einmal angemeldet haben, damit die für ihn vorgesehenen Apps installiert sind. Wenn man anschließend den zugewiesenen Zugriff einrichtet, dann wählt man das dafür angelegt Konto aus und weist ihm eine bestimmte App zu, etwa den Internet Explorer für eine Surf-Station.

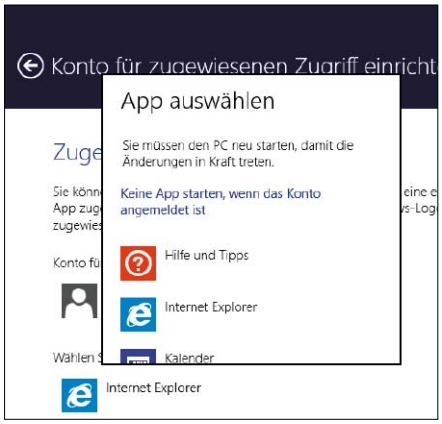


Der zugewiesene Zugriff eignet sich etwa zur Einrichtung einer Surf-Station, auf der die App-Version des IE läuft.

Bei der Konfiguration des Kiosk-Modus wäre noch zu bedenken, dass man die Kennwortregeln für den Rechner mit „secpol.msc“ ändern muss, wenn man den Anwendern den Zugang ohne Eingabe eines Passworts gewähren möchte. Zusätzlich wird man auf diesem Weg verhindern wollen, dass die Benutzer sich abmelden oder den Rechner herunterfahren.

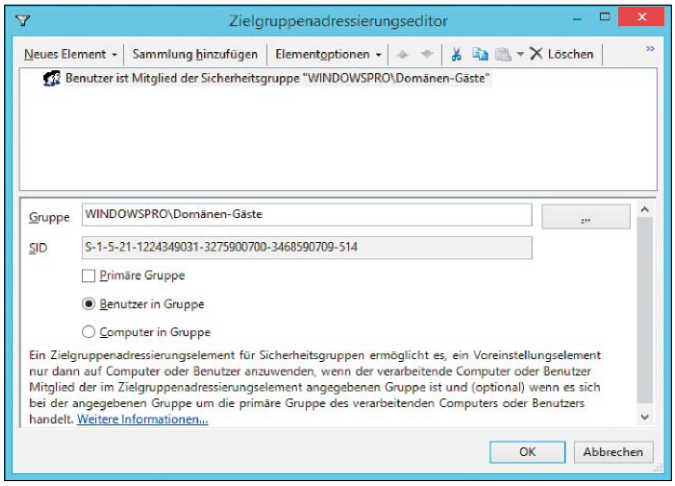
Netzlaufwerke über Group Policy Preferences zuweisen

Zu den wesentlichen Anforderungen an Benutzerumgebungen gehört, dass ihnen alle erforderlichen Netzwerkressourcen zur Verfügung stehen. Dazu zählen neben Druckern vor allem Freigaben auf Fileservern.
Traditionell stellten Administratoren die Verbindung zu Shares über Log-in-Scripts her, in denen das Kommandozeilen-Tool net use meistens diese Aufgabe übernimmt. Wenn man die Zuordnung von Laufwerksbuchstaben zu Netz-



Das Konto für den Kiosk-Modus hat nur das Recht, eine einzige App ausführen.

Damit die Einschränkung des GPO auf bestimmte Gruppen funktioniert, muss ihre SID eingetragen werden.



freigaben von bestimmten Kriterien abhängig machen will, dann kann dies in erheblichen Programmieraufwand ausarten.

Seit Vista bietet Windows mit den Group Policy Preferences (GPP) eine mächtigere, elegantere und flexiblere Alternative an. Trotz der Vorzüge dieser Technik ist sie vielen Admins noch unbekannt, etwa wenn noch viele PCs unter XP laufen.

Exaktere Auswahl von Benutzern

Durch das sogenannte Item Level Targeting lassen sich fast alle Parameter einer Benutzerumgebung abfragen, um diesen gezielt Freigaben zuzuordnen. Dies funktioniert übrigens auch noch mit Windows XP, wenn man dort die erforderlichen Client Side Extensions installiert. Die Administration muss allerdings unter einer neueren Windows-Version erfolgen.

Windows 8.1 liefert ein weiteres Argument für den Einsatz von GPP für das Laufwerks-Mapping, indem es die Zuordnung vom Log-in der Benutzer entkoppelt. Daher lassen sich Netzlaufwerke auch während einer User-Session ändern. Im ersten Schritt legt man über die Gruppenrichtlinienverwaltung ein neues GPO an und öffnet es zur Bearbeitung mit dem Gruppenrichtlinienverwaltungs-Editor. Dort navigiert man zu „Benutzerkonfiguration → Einstellungen → Windows-Einstellungen → Laufwerkzuordnungen“. Anschließend führt man aus dem Menü den Befehl „Aktion → Neu → Zugeordnetes Laufwerk“ aus.

Bestehende Zuordnungen ersetzen oder aktualisieren

Der folgende Dialog bietet meist selbsterklärende Einstellungen. Auf Anhieb nicht ganz klar ist die Entscheidung zwischen „Erstellen“, „Ersetzen“ und „Aktualisieren (default)“:

- **Erstellen** bedeutet, dass eine Zuordnung eingerichtet wird, wenn eine Freigabe „\\server\share“ noch nicht verbunden wurde, andernfalls passiert nichts.
- **Ersetzen** löscht eine vorhandene Verbindung mit einem Share und richtet sie gemäß den GPP-Einstellungen neu ein. Wurde jedoch eine Freigabe noch nicht verbunden, dann erzeugen die Client Side Extensions eine neue Zuordnung.
- **Aktualisieren** verändert eine bestehende Zuordnung, indem die Einstellungen aus dem GPO übernommen werden, wenn eine Verbindung für die Freigabe bereits besteht. Beispielweise würde dadurch der Laufwerksbuchstabe geändert. Existiert für ein Share keine Zuordnung, dann wird sie eingerichtet.

In der Regel wird man die Option „Ersetzen“ wählen, um sicherzustellen, dass eventuell vom Benutzer angelegte Zuordnungen beseitigt und zentrale Vorgaben durchgesetzt werden. Wenn man möchte, dass die Verbindung mit einer Freigabe entfernt wird, sobald die Kriterien für die Zuordnung nicht mehr zutreffen, etwa weil ein Benutzer aus einer Organisationseinheit (OU) entfernt wurde, dann muss man ohnehin „Ersetzen“ wählen. Die Einstellung für das Entfernen einer Verbindung mit einem Netzlaufwerk findet sich auf der Registerkarte „Gemeinsame Optionen“, sie lässt sich nur in Kombination mit „Ersetzen“ aktivieren.

Sichtbarkeit im Explorer steuern

Etwas rätselhaft wirken auf der ersten Seite des Dialogs die Abschnitte „Laufwerk aus-/einblenden“ sowie „Alle Laufwerke aus-/einblenden“. Sie entscheiden darüber, ob die zugeordneten Laufwerke im Explorer angezeigt werden. Dabei setzt sich „Laufwerk aus-/einblenden“ durch, wenn aus beiden Abschnitten sich widersprechende Einstellungen gewählt wurden. Die bis zu diesem Punkt verfügbaren Einstellungen führen dazu, dass die damit definierten Laufwerkzuordnungen für alle User eines AD-Containers (Domäne, OU) gelten, mit dem das GPO verknüpft wurde.

Kriterien für Zielgruppe festlegen

Die passgenaue Einschränkung auf bestimmte User erfolgt erst über die Zielgruppenadressierung auf Elementebene (Registerkarte „Gemeinsame Optionen“). In den meisten Fällen wird man hier die Zuordnung eines Share von der Gruppenzugehörigkeit eines Benutzers abhängig machen (Option „Sicherheitsgruppe“). Beim folgenden Dialog zur Festlegung der Gruppe sollte man den Auswahldialog benutzen, weil nur so die SID der Gruppe eingetragen wird. Das Eintippen des Gruppennamens alleine reicht nicht.

Standardmäßig legt man mit der Auswahl einer oder mehrerer Gruppen fest, dass die User ihr angehören müssen, damit die Regel greift. Allerdings besteht auch die Möglichkeit, die Bedingung umzudrehen und das Laufwerk nur zuzuordnen, wenn User nicht Mitglied einer oder mehrerer Gruppen sind. Zu diesem Zweck unterstützt das Item „Level Targeting“ die Operatoren „nicht“, „und“, „oder“.

Einfachere Regeln durch Negation

Sinnvoll ist die Negation dann, wenn ein Netzlaufwerk für die meisten Benutzer verbunden werden soll, während wenige Gruppen außen vorbleiben. Diese Ausnahmen lassen sich innerhalb einer Regel mit dem Operator „oder“ verketten und anschließend negieren. Das GPO kann man dann einer Domäne oder einer übergeordneten OU zuordnen.

Umgekehrt gilt natürlich auch, dass man die Mitgliedschaft als Kriterium dann wählt, wenn nur eine Minderheit ein Netzlaufwerk erhalten soll. Andernfalls müssten mehr Gruppen in die Liste aufgenommen werden, als draußen bleiben, was auch die Abarbeitung der Bedingung verlangsamt. ■

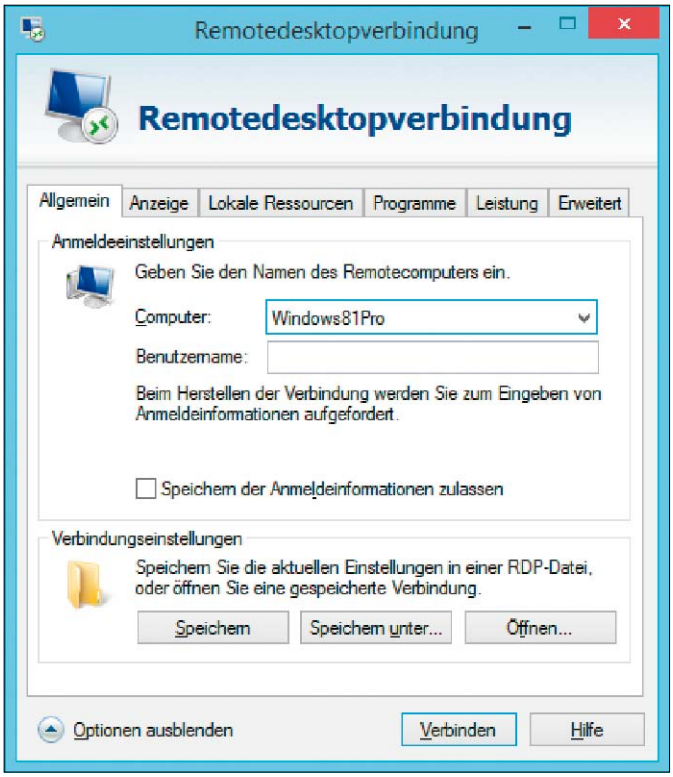
Remote-Zugriff auf Windows 8.1

Windows bietet Ihnen gleich mehrere Optionen, um von entfernten Rechnern aus mit dem Desktop, einzelnen Anwendungen oder dem Dateisystem zu interagieren. Zu den gängigsten zählen RDP und FTP.

VON WOLFGANG SOMMERGUT

DIE TERMINAL-DIENSTE wurden ursprünglich als Technologie für den Server entwickelt, damit mehrere Benutzer eine Instanz des Betriebssystems gemeinsam nutzen können. Mit dem Remote-Desktop-Protokoll (RDP) greifen Sie auf Programme zu, die auf einem entfernten Rechner ausgeführt werden, und Ihr Client ist dabei nur für die Bildschirmausgabe und Ihre Eingaben zuständig. Die Ressourcen des Servers sind für die darauf laufenden Applikationen lokal, und da, wo der Benutzer sitzt, ist für sie remote. Microsoft hat diese Technologie auch in die Client-Systeme integriert, die allerdings auf eine einzige Session limitiert sind. Andere Vorzüge, wie ein gutes Benutzererlebnis über langsame Netzwerke oder das Mapping lokaler Peripherie in die entfernte Sitzung, stehen aber auch dort zur Verfügung.

Mit RDP 8.0 in Windows 8 und Server 2012 kamen mehrere neue Optionen hinzu, Windows 8.1 und Server 2012 R2 setzen diese Entwicklung mit zusätzlichen Features fort.



Nach dem Einblenden der Optionen lässt sich im RDP-Client eine Reihe von Einstellungen konfigurieren.

Konfiguration per RDP-Dateien

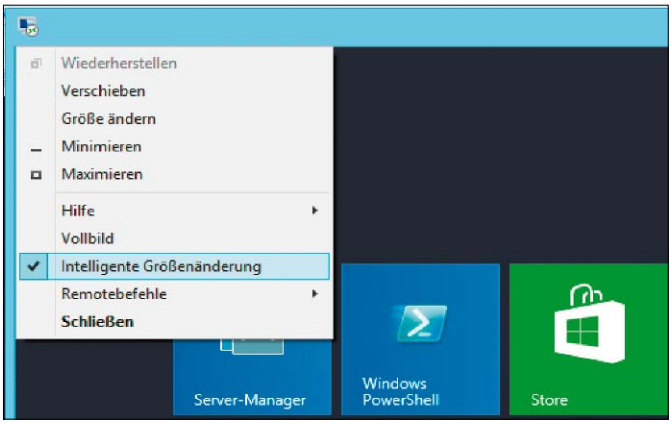
Öffnet man den RDP-Client über die Suche und Eingabe von *Remotedesktopverbindung*, dann kann man sich auf Basis der Standardeinstellungen sofort mit dem Remote-PC verbinden. Als Hosts kommen neben einem vollwertigen Remote Desktop Session Host auch normale Server und Desktops (ausgenommen die Home-Editionen) unter Windows in Frage. Möchte man eine Sitzung nicht mit der vorgegebenen Konfiguration starten, dann kann man über die Schaltfläche „Optionen“ eine Reihe von Einstellungen anpassen. Der RDP-Client merkt sich diese Änderungen bis zum nächsten Aufruf. Man kann aber auch spezifische Konfigurationen in einer Datei mit der Endung RDP speichern, beispielsweise um sie auf andere Rechner zu übertragen. Diese liegt im Klartextformat vor und kann bei Bedarf mit einem Editor bearbeitet werden. Die Optionen für diese Konfigurationsdateien finden sich im Technet (*http://bit.ly/1hHk1SR*).

Intelligente Größenänderung konfigurieren

In den meisten Fällen wird man eine Remote-Desktop-Session jedoch über die Oberfläche des RDP-Clients anpassen. Die erste Registerkarte nach den allgemeinen Einstellungen betrifft die Konfiguration der Anzeige, nämlich die Auflösung, die Farbtiefe und die Anzeige der Verbindungsleiste.

Eine mit RDP 7 eingeführte wichtige Neuerung, das sogenannte „Smart Sizing“, lässt sich hier

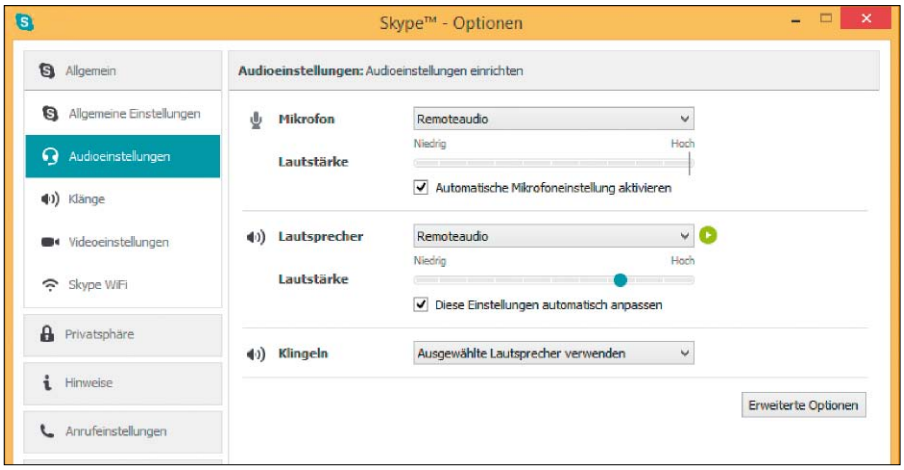
jedoch nicht festlegen. Es handelt sich dabei um die Fähigkeit des RDP-Clients, den Remote-Desktop automatisch an die Größe des Fensters anzupassen.
Die Skalierung erfolgt allerdings nicht proportional, so dass man selbst auf ein vernünftiges Seitenverhältnis des Desktops achten muss. Außerdem können vorher die im Client festgelegten Dimensionen des Bildschirms nicht überschritten werden, so dass man dafür unbedingt gleich großzügige Werte wählen soll, wenn man die Größe des Fensters nachher beliebig ändern möchte.
Der RDP-Client in Windows 8.x bietet nach dem Aufbau der Verbindung die Möglichkeit, dieses Feature über den Menüeintrag „Intelligente Größenänderung“ zu aktivieren. Unter Windows 7 muss man zu diesem Zweck dagegen die RDP-Datei für diese Verbindung bearbeiten und dort den Eintrag *smart sizing:i:1* einfügen.



Die intelligente Größenänderung lässt sich unter Windows 8.x über die GUI aktivieren.

Umleitung von Mikrofon und Audioausgabe

Die meisten Einstellungen, die für die Integration der Remote-Session in den Client relevant sind, finden sich unter dem Reiter „Lokale Ressourcen“. Dort bestimmt man, wo Ein- und Ausgaben des Audiosystems erfolgen, wie sich bestimmte Tastenkombinationen auswirken und welche lokalen Geräte im entfernten Desktop verfügbar sein sollen.
Die Standardeinstellungen sehen zwar vor, dass die Audiosignale des Remote-PCs auf dem Client auszugeben sind, aber die Umleitung des lokalen Mikrofons auf den entfernten Desktop ist deaktiviert.
Für Letzteres ist der unglücklich übersetzte Abschnitt „Remoteaudioaufzeichnung“ zuständig. Möchte man in der Remote-Session zum Beispiel Skype nutzen, dann muss man das am Client vorhandene Mikrofon dorthin durchreichen, und zwar über die Option „Von diesem Computer aufzeichnen“. Das Eingabegerät heißt dann dort einfach „Remoteaudio“.



Entfernte Anwendungen können das lokale Mikrofon nutzen und Audio über den Client ausgeben.

Lokale Drucker ansteuern

Bei der Umleitung von lokalen Geräten in die Remote-Session finden sich „Drucker“ und „Zwischenablage“ direkt auf der Registerkarte, weitere lokale Ressourcen müssen in einem Folgedialog unter „Weitere“ konfiguriert werden. Damit man aus entfernten Anwendungen auf lokalen Printern drucken kann, müssen auf dem Host die entsprechenden Treiber für die Drucker installiert sein.
Im angesprochenen Dialog unter „Weitere“ stehen zum einen „Smartcards“ und „Ports“ zur Auswahl. Erstere eignen sich somit auch zur Anmeldung am Remote-Host, wenn man den Reader dorthin durchreicht. Bei „Ports“ sind sowohl serielle als auch parallele Anschlüsse gemeint.

Umleitung von Laufwerken

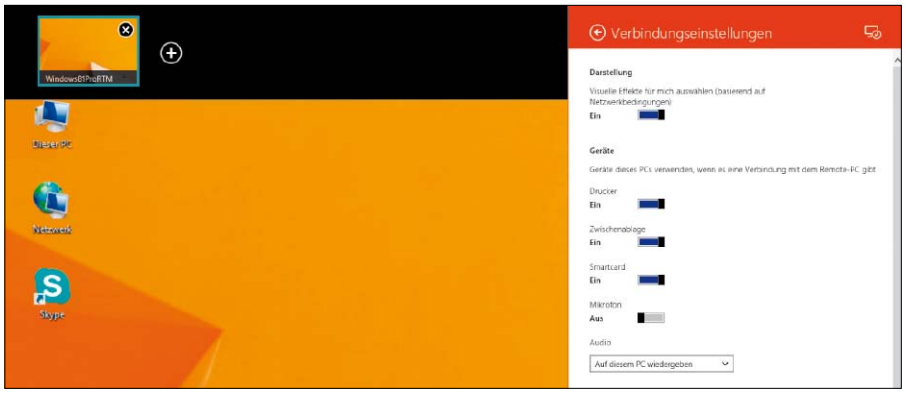
Zum anderen findet sich in diesem Dialog die vollständige Liste der lokalen Laufwerke. Bereits angeschlossene Festplatten und DVD-Laufwerke kann man über den Laufwerksbuchstaben explizit auswählen, so dass sie sofort nach dem Aufbau zu Verfügung stehen. Zu beachten ist, dass die darauf befindlichen Dateien gleichzeitig von lokalen und entfernten Anwendungen geöffnet werden können, ohne dass ein Zugriffskonflikt auftritt. Entsprechend droht in solchen Situationen ein Datenverlust. Für USB-Geräte gibt es eine Plug-and-Play-Unterstützung, so dass man bei Bedarf Wechseldatenträger oder Webcams, die man nach dem Start der Session anschließt, ebenfalls im Remote-Desktop nutzen kann.

Automatische Erkennung der Verbindungsqualität

Ein neues Feature von RDP 8.0 besteht darin, dass der Client selbständig die Verbindungsqualität erkennt. Daher muss man auf der Registerkarte „Erweitert“ nicht mehr explizit „Modem“, „LAN“ oder dergleichen auswählen. Voreingestellt ist nun „Verbindungsqualität automatisch erkennen“. Wenn man nach dem Aufbau der Session diese in den Vollbildmodus schaltet (Strg-Alt-Unterbr), dann findet sich in der Verbindungsleiste nun ein Icon, hinter dem sich ein Dialog für die Übertragungsqualität verbirgt.

Remote-Desktop-App für Win 8.x

Für Windows 8.x gibt es neben dem integrierten Client für RDP zusätzlich eine App für Remote-Desktop. Sie ist nicht vorinstalliert, sondern muss über den Store bezogen werden. Allerdings fehlen ihr eine ganze Reihe der hier beschriebenen Einstellungsmöglichkeiten.
So ist es beispielsweise nicht möglich, lokale Laufwerke und USB-Geräte auf den Host umzuleiten. Die Wahl der Bildschirmgröße ist zwar auch nicht vorgesehen, aber nachdem eine App ohnehin im Vollbildmodus läuft, ist dieser Mangel leicht zu verkraften.
Die Ausführung für Windows 8.1 brachte bei der Darstellung einige Verbesserungen. Dazu gehört etwa die automatische Anpassung der Bildschirmauflösung, wenn sich die Größe der



Der Remote-Desktop-App aus dem Store fehlen im Vergleich zum herkömmlichen RDP-Client wichtige Features.

App verändert. Dies kann etwa eintreten, wenn die Darstellung auf einem Tablet zwischen Hoch- und Breitformat umschaltet. Das Feature greift aber auch in einer Multi-Monitor-Konfiguration, wenn die Bildschirme unterschiedliche Auflösungen haben und die Remote-Desktop-App zwischen ihnen verschoben wird. Naturgemäß bietet eine App für Windows 8 Support für die Touch-Bedienung, der allerdings recht wenig bringt, wenn man es remote mit dem klassischen Desktop zu tun hat (und darin besteht eigentlich eine wesentliche Aufgabe des neuen Clients, indem er Windows RT den Zugriff auf herkömmliche Windows-Anwendungen erlaubt).

Umgekehrt bietet der normale Client für RDP 8.0 einige Eingabehilfen, wenn man von Desktop mit Maus und Tastatur remote auf die Startseite von Windows 8 zugreift. Die entsprechenden Befehle finden sich unter dem Menüpunkt „Remotebefehle“ und erlauben das Wechseln zum Startbildschirm, das Öffnen von Charms oder das Andocken von Apps.

Neu in RDP 8.1

Der RDP-Client „Mstsc.exe“ erhält in Windows 8.1 neue Parameter, über die man das Spiegeln von Sitzungen sowie den Restricted Admin Mode aktivieren kann. Derzeit ist noch unklar, ob diese Erweiterungen auf ältere Versionen des Betriebssystems portiert werden.

Als Vorbeugung gegen „Pass the Hash“-Angriffe, die eine Schwachstelle der NTLM-Authentifizierung nutzen, führt Microsoft mit Windows 8.1 und Server 2012 R2 den „Restricted Admin Mode“ ein. Er verhindert, dass die Anmeldedaten des Benutzers an den Remote-PC übertragen werden.

Restricted Admin Mode mit reduzierten Rechten

Der Start einer solchen Verbindung erfolgt, indem man „Mstsc.exe“ mit dem Schalter */restrictedAdmin* und optional einer RDP-Datei als zweites Argument aufruft. Eine entsprechende Einstellung auf der grafischen Oberfläche gibt es nicht. Läuft die Session im Vollbildmodus, dann erkennt man den eingeschränkten Admin-Modus am eingeblendeten Vorhängeschloss-Icon.

Der Restricted Admin Mode führt indes zu beschränkten Rechten, wenn man von der Session auf dem Remote-PC andere Ressourcen im Netz verwenden möchte. In diesem Fall erfolgt der Zugriff im Kontext des aktuellen Computer-Kontos.

Sitzungen spiegeln mit /shadow

Die zweite wesentliche Neuerung reflektiert die Tatsache, dass die Remote Desktop Services in Windows Server 2012 R2 wieder die Spiegelung von Sessions einführen, nachdem dieses bewährte Feature in Server 2012 fehlte.

Um sich auf eine bestehende Sitzung aufzuschalten, muss man erst ihre ID ermitteln. Dies erfolgt mit Hilfe des Powershell-Cmdlets *Get-RDUserSession*, das Bestandteil des Remote-Desktop-Moduls ist:

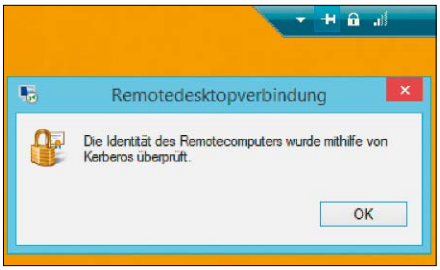
```
Get-RDUserSession -CollectionName
 <Name der Sammlung> | select
 UserName, UnifiedSessionId
```

Anschließend übergibt man die ermittelte ID an den Parameter */shadow* nach dem folgenden Muster:

```
mstsc.exe /shadow:<SessionID>
 /v:<Server>
```

Schaltet man sich in dieser Form auf eine Sitzung eines Benutzers auf, dann kann man nur dessen Aktivitäten beobachten. Möchte man die Kontrolle über die Session übernehmen, dann muss man zusätzlich den Schalter */control* angeben.

Beide Formen der Spiegelung erfordern die Zustimmung des betreffenden Benutzers. Möchte man diese umgehen, dann gibt man zusätzlich */noConsentPrompt* an. Allerdings muss diese Option erst über eine Gruppenrichtlinie freigeschaltet werden.



Das Symbol mit dem Vorhängeschloss zeigt, dass die Authentifizierung über Kerberos erfolgt ist.

Anmeldedialog anzeigen

Neu ist auch der Schalter */prompt*, der das Anzeigen des Anmeldedialogs erzwingt. Dies ist dann sinnvoll, wenn man in der RDP-Datei das Speichern der Anmeldeinformationen zugelassen hat, so dass man sie nicht bei jedem Verbindungsaufbau neu eingeben muss.

Hat man das Passwort geändert, dann würde aber das automatische Anmelden scheitern. In diesem Fall erlaubt der Schalter */prompt*, dass man sich mit seinem neuen Kennwort anmeldet und dieses gleich speichert.

Einzelne Programme auf Windows 7, 8 über RDP öffnen

Microsoft führte mit Windows Server 2008 unter der Bezeichnung „Remoteapp“ ein Feature ein, das die Darstellung einzelner entfernter Anwendungen auf dem lokalen Desktop erlaubt. Dieses funktioniert grundsätzlich auch dann, wenn der Host unter Windows 7, 8 läuft. Wenn man nur eine Anwendung auf einem Remote-PC nutzen möchte, dann bietet Remoteapp einen größeren Benutzerkomfort, weil das betreffende Programm nahtlos in die lokale Umgebung eingebettet ist. Der komplette Desktop des RDP-Hosts ist in solchen Fällen eher hinderlich.

Keine Remoteapp-Konfiguration im RDP-Client

Auf den ersten Blick sieht es so aus, als ließe sich dieses Feature auch dann ganz einfach nutzen, wenn der Remote-PC unter Windows 7, 8 läuft. Schließlich gibt es bei der Konfiguration von Remote-Desktop unter dem Reiter „Programme“ die Möglichkeit, eine Anwendung einzutragen, die anstelle des gesamten Desktops angezeigt wird. Diese Option steht aber nur für Terminal-Server zur Verfügung und bleibt ohne Wirkung, wenn es sich beim Remote-PC um einen Rechner mit Windows 7 oder Windows 8 handelt.

Dabei sind die Client-Versionen von Windows aber durchaus in der Lage, nur einzelne Anwendungen über RDP bereitzustellen. Allerdings erfordert dies, dass man die Konfigura-

tionsdaten für jede Verbindung manuell in die Registry unter „HKLM\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\TSAppAllowList\Applications“ einträgt.

Konfiguration mit Remoteapp Tool

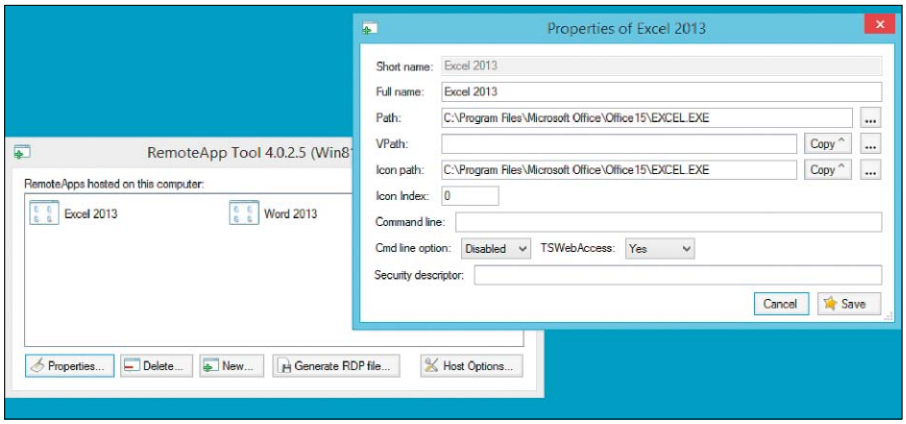
Das kostenlose Remoteapp Tool von Kim Knight (auf Heft-DVD, *www.kimknight.net/Remoteapptool*) dient dem Zweck, diese Prozedur zu vereinfachen. Über ein simples Interface kann man auf dem Host-Rechner jene Anwendungen konfigurieren, die remote im Seamless-Modus zur Verfügung stehen sollen. Es zeigt für jede Remoteapp ein Icon an, so dass man schnell überblicken kann, welche man bereits eingerichtet hat. Dort kann man die Einstellungen auch nachträglich leicht verändern. Die Eingabefelder im Konfigurationsdialog sind nur teilweise selbsterklärend, eine Online-Hilfe existiert nicht. So gibt es zum Beispiel neben dem Feld „Path“ ein weiteres mit der Bezeichnung „Vpath“, das automatisch mit dem Wert von Path gefüllt wird. Hier bestünde etwa die Möglichkeit, einen alternativen Pfad ohne Laufwerksbuchstaben zu hinterlegen und stattdessen Umgebungsvariablen oder die UNC-Notation zu verwenden.

Weitere Verbindungsdaten

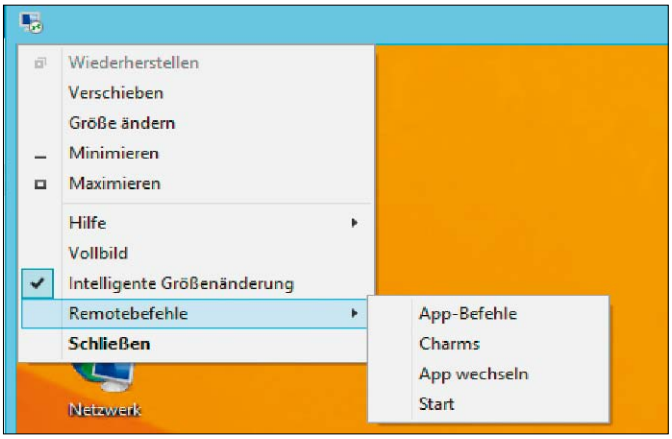
Der Icon „Path“ gibt an, aus welcher Datei das Programmsymbol entnommen werden soll. In der Regel ist dies ebenfalls die ausführbare Datei. Wenn sie mehr als ein Icon enthält, kann man über den Icon „Index“ angeben, welches man haben möchte. Über das Feld „Command Line“ legt man die Parameter fest, die man an das Programm übergeben will. Über das Dropdown-Menü „Cmd line option“ lässt sich zudem bestimmen, ob Parameter zulässig oder sogar erforderlich sind. Der „Security Descriptor“ dient am Terminal-Server dazu, Programme aus RD Web Access auszublenden, die der User nicht ausführen darf. In Windows 7, 8 wird man ihn für Remoteapp alleine nicht benötigen.

RDP-Datei erzeugen

Nach der Konfiguration der Verbindung bietet das Remoteapp Tool die Möglichkeit, die RDP-Datei für den Aufruf des Programms automatisch zu generieren. Im einfachsten Fall wird man diese auf die PCs verteilen, von denen aus man die Anwendung remote nutzen möchte.
Alternativ bietet Kim Knight ein ebenfalls kostenloses Zusatzprogramm namens Raweb (*http://bit.ly/1gKN8a5*) an, das ein simples RD Web Access unter Windows 7, 8 implementiert. Es setzt voraus, dass die IIS auf dem Host aktiviert wurden. Anwender auf den Clients können dann über ein Webinterface alle veröffentlichten Programme anzeigen und von dort starten. Das Tool erzeugt zusätzlich sogar einen Webfeed, über den sich die Remoteapp-Anwendungen in das Startmenü von Clients integrieren lassen.



Das Remoteapp Tool erstellt eine RDP-Datei, die eine einzelne Anwendung nahtlos in den lokalen Desktop einbettet.



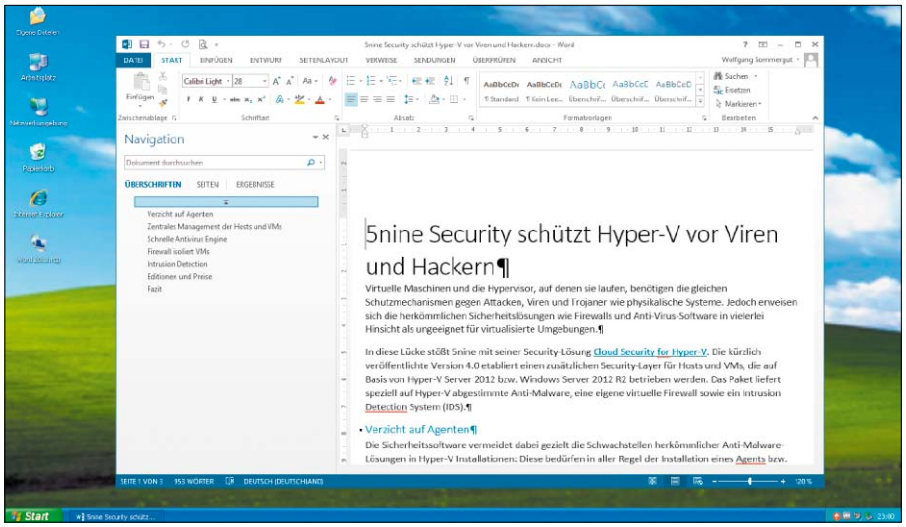
Das Steuern von entfernten Windows-8-Desktops wird durch die Remote-Befehle in RDP 8 vereinfacht.

Systemvoraussetzungen und Verfügbarkeit

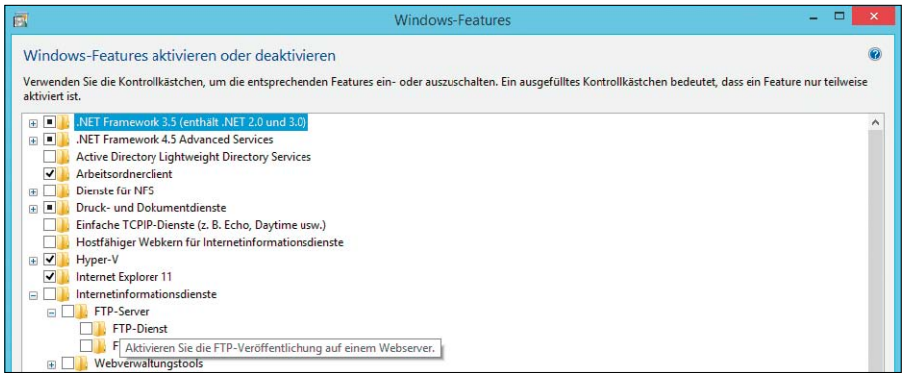
Neben Windows 7 und Windows 8, auf denen sich Remoteapp ohne Modifikationen einrichten lässt, kommt für diesen Zweck auch XP SP3 in Frage. Allerdings muss dort erst RDP 7 installiert werden. Nachdem Microsoft den XP Modus in Windows 8 nicht mehr unterstützt, ließen sich alternativ über Remoteapp einzelne Programme von XP-VMs nahtlos auf dem Desktop des Host-Systems einblenden.
Der Einsatz des Remoteapp Tool setzt voraus, dass auf dem Host-PC das Remote-Desktop-Feature (*http://bit.ly/PU74Om*) aktiviert wurde. Es wird ab der Professional Edition unterstützt. Dabei gilt die gleiche lizenzrechtliche Einschränkung wie bei der Bereitstellung eines kompletten Desktops, so dass nur eine Verbindung aufgebaut werden darf und die Sitzung eines lokal angemeldeten Benutzers unterbrochen wird. Das Remoteapp Tool benötigt zu seiner Ausführung die .NET Runtime 4. Eine Installation der Software ist nicht erforderlich. Sie kann kostenlos von der Website des Autors heruntergeladen werden (*http://bit.ly/1j7VTOH*).

Dateien über FTP-Server tauschen

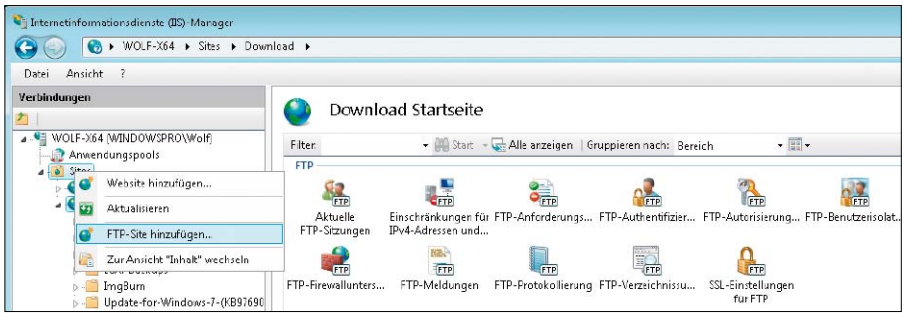
Grundsätzlich erlaubt eine Remote-Desktop-Verbindung das Kopieren von Dateien zwischen Host und Client. Oft erweist sich aber das gute alte File Transfer Protocol (FTP) als einfachste Möglichkeit, um Dateien zwischen PCs auszutauschen – vor allem dann, wenn diese unter verschiedenen Betriebssystemen laufen. Windows 7, 8 bringt einen eigenen FTP-Server mit, der im Vergleich zu einigen freien Produkten recht mächtig ist. Der Preis dafür ist eine umständliche Konfiguration.
Wenn man einen FTP-Server unter Windows nur gelegentlich für Ad-hoc-Transfers benötigt, dann sollte man eher zu unkomplizierten Lösungen wie Quick ’n Easy oder Filezilla greifen. Damit ist man schnell startklar, um die gewünschten Dateien hinauf- oder herunterzuladen. Der in die Internet Information Services eingebaute FTP-Server hat seine Stärken vor allem in der Integration mit der Benutzer- und Berechtigungsverwaltung von Windows. Dafür muss man aber mehr konfigurieren.



Word 2013, das normalerweise nicht unter Windows XP läuft, hier als Remoteapp.



Der FTP-Server wird als Teil der IIS über „Systemsteuerung/Programme“ hinzugefügt.



Mit dem Internetinformationsdienste(IIS)-Manager lassen sich neben der Default-Site weitere FTP-Sites hinzufügen.

FTP-Server als Teil der Internetinformationsdienste

Die eigentliche Installation des FTP-Servers ist noch recht einfach. Sie erfolgt in der Systemsteuerung unter „Programme → Windows-Funktionen aktivieren oder deaktivieren“. Dort klappt man die Struktur unterhalb von „Internetinformationsdienste“ auf und aktiviert unter „FTP-Server“ die Checkbox für FTP-Dienst und unter „Webverwaltungstools“ jene für die IIS-Verwaltungskonsole. Nach Abschluss der Installation startet man „Internetinformationsdienste (IIS)-Manager unter Systemsteuerung → System und Sicherheit → Verwaltung“. Dort findet man eine Konfiguration vor, die nur die Default-Website enthält. Sie verweist per Voreinstellung auf „C:\inetpub\ftproot“ und ist nicht als FTP-Site aktiviert.

Default-Site anpassen

Wenn man die Default-Site nutzen möchte, dann kann man die Einstellung beim genannten Verzeichnis belassen oder sie auf einen anderen Ordner umpolen, den man als FTP-Root verwenden möchte. Um Letzteres zu bewerkstelligen, führt man in der Aktionsleiste den Befehl „Grundeinstellungen“ aus. Er bietet die Möglichkeit, ein anderes Verzeichnis auszuwählen. Alternativ zu „Default“ kann man über das Kontextmenü von „Sites“ seine eigene FTP-Site hinzufügen.

Egal, ob man die vorgegebene Site nimmt oder eine eigene hinzufügt, beide sind erst nur angelegt und so nicht über FTP erreichbar. Vielmehr ist es notwendig, dass man sie über den Befehl „FTP-Publishing hinzufügen“ dafür konfiguriert. In diesem Prozess bindet man den Dienst bei Bedarf an eine bestimmte IP-Adresse, weist ihm einen virtuellen Host-Namen zu (wie zum Beispiel *ftp.contoso.com*) und bestimmt, ob die Kommunikation über SSL verschlüsselt werden soll. Wenn man mehrere FTP-Sites anlegt, dann benötigt jede eine eigene IP-Adresse, an die sie gebunden werden kann. Virtual Hosts sind dagegen dann interessant, wenn man mehrere FTP-Server über eine IP-Adresse bereitstellen möchte.

Will man FTP über SSL (FTPS) verwenden, dann kann man im Wizard zum Veröffentlichen einer neuen Site nur die entsprechende Option an- oder abwählen. Das für die SSL-Verschlüsselung nötige Zertifikat wird im Pull-down-Menü nur angezeigt, wenn zuvor ein solches importiert oder selbst ausgestellt hat.

Authentifizierung, Autorisierung, Berechtigungen

Im zweiten Dialog des Wizards legt man fest, wie sich Benutzer authentifizieren müssen und welche Berechtigungen sie bekommen. Aktiviert man „Anonym“, dann reicht es, wenn sich User mit der Kennung FTP oder Anonymous und ihrer Mailadresse als Passwort anmelden. In diesem Fall wird man im Abschnitt „Autorisierung“ für „Anonyme Benutzer“ den Zugriff gewähren.

Erzwingt man die Anmeldung über Benutzername und Passwort, dann kann man die Zugriffsrechte für bestimmte Konten beziehungsweise Gruppen von Windows erteilen. Zu diesem Zweck trägt man entweder bestehende User ein, oder man legt eine eigene Gruppe für FTP an. In diese könnte man nicht nur lokale, sondern auch AD-Konten aufnehmen. Zu beachten ist, dass diese auf NTFS-Ebene die nötigen Rechte in den festgelegten Verzeichnissen haben. Für den anonymen Zugriff muss man diese dem Benutzer IUSR erteilen.

Rechte-Management nach dem Anlegen der Site

Man kann zwar innerhalb des Wizards zum Publishing von FTP-Sites beide Formen der Authentifizierung auswählen, aber benannte und anonyme User lassen sich nicht gleichzeitig im Abschnitt „Autorisierung“ eintragen. Die abschließende Gewährung von Lese- und

Schreibrechten gilt daher nur für eine Sorte der zugelassenen Benutzer. Daher wird man in der Regel das differenzierte Rechte-Management auf die anschließende Konfiguration der FTP-Site verlegen. Bevor man sich an diese machen kann, muss man die Site aktualisieren und gegebenenfalls manuell starten. Danach steht im Hauptfenster das Applet „FTP-Authentifizierung“ zur Verfügung, über das man die beiden Anmeldetypen verwalten kann. Die detaillierte Rechtevergabe erfolgt indes über „FTP-Autorisierung“. Hier kann man beliebig viele Zulassungs- und Ablehnungsregeln für User und Gruppen hinzufügen, um Lese- und Schreibrechte zu steuern.

SSL-Verbindungen konfigurieren

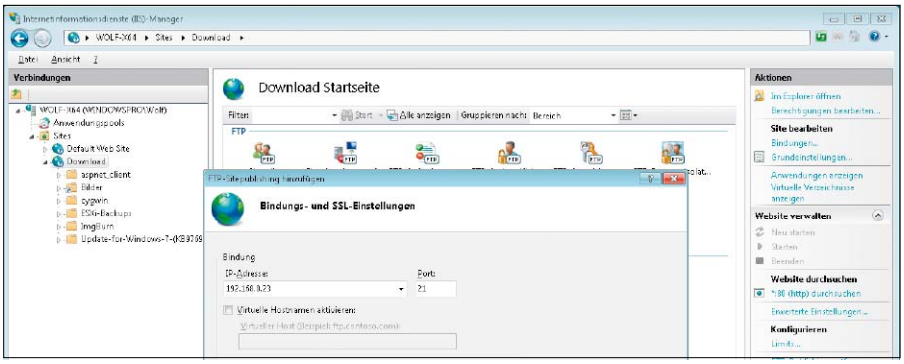
Auch die beim Anlegen einer FTP-Site getroffene Entscheidung für oder gegen SSL ist nur vorläufig und fällt relativ undifferenziert aus. Über die nachträgliche Konfiguration mit Hilfe des Applets „SSL-Einstellungen für FTP“ kann man die Security-Anforderungen feiner abstufen. Die Option „SSL-Verbindungen erforderlich“ lässt keine unverschlüsselte Kommunikation zu, während „SSL-Verbindung zulassen“ dem Client die Möglichkeit einräumt, alle Daten inklusive der Anmeldeinformationen im Klartext zu übertragen. Zwischen diesen beiden Varianten existiert noch eine benutzerdefinierte Einstellung, bei der man beispielsweise erzwingen kann, dass Passwörter codiert werden, aber der Client für alle anderen Daten eine unverschlüsselte Verbindung nutzt.

Zertifikat ausstellen

Für die Konfiguration einer SSL-Verbindung benötigt man ein Zertifikat, wobei der Internetinformationsdienste(IIS)-Manager eine Funktion zum Erstellen eines selbst signierten Zertifikats bietet. Ein solches eignet sich primär für den internen Gebrauch oder für Tests.
Zu diesem Zweck wechselt man im Fenster „Verbindungen“ zum Wurzelverzeichnis (also zum Namen des Servers) und wählt im Hauptfenster die Feature-Ansicht. Dort öffnet man das Applet für Server-Zertifikate und kann dann im Aktionsfenster den entsprechenden Befehl ausführen.

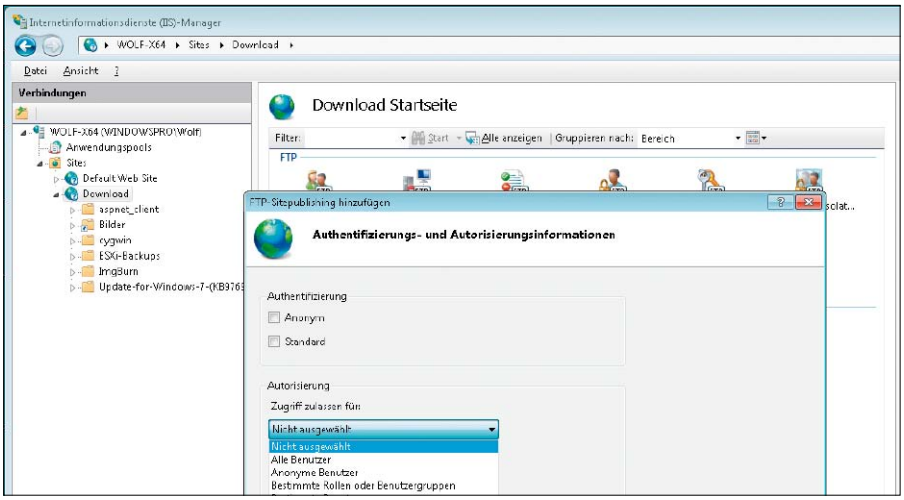
Virtuelle Verzeichnisse und Filter

Nach dieser Basiskonfiguration kann man noch einige fortgeschrittene Funktionen des FTP-Servers in Anspruch nehmen, um die Site auf die individuellen Anforderungen anzupassen. Dazu zählt etwa die Definition von virtuellen Verzeichnissen. Sie dienen dazu, um Ordner außerhalb des festgelegten FTP-Verzeichnisbaumes in diesen einzuhängen. Zum Beispiel könnte man „c:\users\public\bilder“ für Clients unter „/bilder“ zugänglich machen, auch wenn das Stammverzeichnis der FTP-Site unter „c:\inetpub\ftproot“ liegt.
Ein weitere Funktion für die Anpassung des FTP-Servers sind die sogenannten Anforderungsfilter. Mit ihrer Hilfe lässt sich festlegen, welche Dateitypen er übertragen soll und welche er blockiert.
Weitere Filter lassen sich anwenden, um bestimmte IP-Adressen oder Domänen explizit zuzulassen oder auszuschließen.



Der Wizard für das FTP-Publishing bietet im ersten Dialog die Optionen für die IP-Bindung und für SSL.

Die Feinabstimmung des FTP-Servers erfolgt nach dem Durchlauf des Wizards mit den Applets des IIS-Managers.



Die Konfiguration von Authentifizierung und Autorisierung braucht nach dem Ende des Wizards oft weitere Anpassungen.

Firewall-Blockade überwinden

Grundsätzlich stünde einer Verbindung einer solcherart eingerichteten FTP-Site nichts mehr im Wege. Als Spielverderber könnte sich jedoch wieder einmal die Windows-Firewall erweisen. Dabei treten Probleme gar nicht bevorzugt auf der Server-Seite auf, wo die Installation des FTP-Servers die nötigen Firewall-Regeln automatisch erzeugt.
Aufgrund der Charakteristik von FTP, wo Client und Server erst einen Port für die Datenübertragung aushandeln und der Server schließlich die Verbindung initiiert, hakt es häufig auf der Client-Seite. Microsoft hat unter *http://bit.ly/1ml3nhA* Infos zusammengestellt, die bei der Beseitigung von Verbindungsproblemen helfen, die von der Firewall verursacht werden. Die Konfiguration der Regeln erfolgt dort über das Kommandozeilen-Tool *netsh*. ■

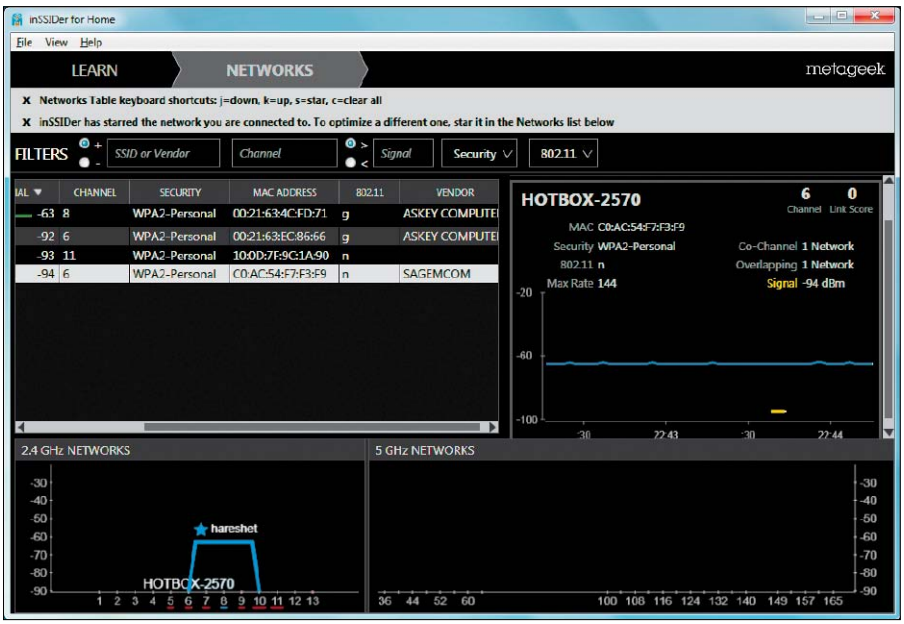
So sichern Sie das Netzwerk ab

Testen Sie von innen und von außen, was die WLAN-Router in Ihrem Netzwerk alles verraten und welche Schwachpunkte sie haben. Der Schwerpunkt liegt hier auf kleinen Netzen und Heimnetzwerken.

VON DAVID WOLSKI

DER ZUGANGSPUNKT ZUM INTERNET ist heutzutage der eigene oder der vom Internet-Provider zur Verfügung gestellte (WLAN-)Router. Damit dieser Zugangspunkt nicht zum Einfallstor wird, ist es wichtig, den Router einigen Checks zu unterziehen und abzusichern. Viele Anwender nehmen den Router jedoch ohne große Änderungen mit der Standardkonfiguration in Betrieb.

Die Voreinstellungen sind längst nicht immer optimal und schlimmstenfalls sogar unsicher. Testen Sie deshalb, was Ihr Router über sich und das Netzwerk preisgibt. Von außen, ohne Teilnehmer im Netzwerk zu sein, sowie von innen aus dem eigenen (W)LAN.



Zeigt auch Drahtlosnetzwerke ohne SSID: Das Freeware-Programm Inssider analysiert empfangene Netzwerkpakete und spürt damit ebenfalls vermeintlich unsichtbare WLANs auf.

Check von außen

An einen WLAN-Router müssen Sie hohe Anforderungen stellen und für eine weitgehend sichere Konfiguration sorgen, da Sie nur schwer kontrollieren können, wer das Signal des Drahtlosnetzwerks empfängt. Es gibt einige Informationen, die Sie über einen WLAN-Router herausfinden können, ohne am Netzwerk angemeldet zu sein und ohne das Passwort für die WLAN-Verschlüsselung oder die SSID des Netzwerks zu kennen.

Broadcast-Pakete: Das WLAN stellt sich vor

Damit WLAN-fähige Geräte überhaupt in der Lage sind, ein Drahtlosnetzwerk zu erkennen, macht sich der WLAN-Router oder Access Point durch einen „Beacon“ bekannt. Diese Broadcast-Datenpakete sind der Herzschlag des Netzwerks und informieren alle Geräte in Reichweite über Anbindungsgeschwindigkeit, MAC-Adresse des Routers, Kanal und die verwendete Verschlüsselung. Der Router schickt diese Pakete etwa zehnmal pro Sekunde über das Netzwerk heraus.

Um das Netzwerk sicherer zu machen, greifen viele Nutzer immer noch auf einen alten Trick zurück: Die SSID, also der Netzwerkname, wird im Router abgeschaltet und das WLAN damit vermeintlich unsichtbar. Abgesehen von einem höheren Konfigurationsaufwand bringt dieser Schritt aber nichts. Denn eine versteckte SSID verhindert nur, dass der Router in den Broadcast-Paketen den Netzwerknamen öffentlich bekannt macht, die Pakete werden jedoch trotzdem verschickt und identifizieren das WLAN. Die Freeware Inssider 3 (auf DVD, Download unter *www.pcwelt.de/306569*) zeigt alle verfügbaren WLANs in der Umgebung an, egal ob die SSID aktiviert ist oder nicht.

Es macht also keinen Unterschied, ob Sie die SSID in der WLAN-Konfiguration des Routers anzeigen lassen oder verstecken. Bei der SSID ist lediglich darauf zu achten, dass damit keine internen Infos preisgegeben werden: Tabu ist ein WPA2/WPA-Passwort, das identisch mit der SSID ist oder einfach nur aus einer Abwandlung der SSID besteht. Ebenfalls sollte die SSID keine Typenbezeichnung des Routers enthal-

ten. Einige Router sind ab Werk so eingestellt, dass sie den kompletten Modellnamen in der SSID ausposaunen. Da es niemand etwas angeht, welcher Router bei Ihnen steht, und eine genaue Typenbezeichnung bei der Suche nach herstellerspezifischen Sicherheitslücken hilft, sollte hier immer etwas Unverfängliches und für Fremde Uneindeutiges stehen.

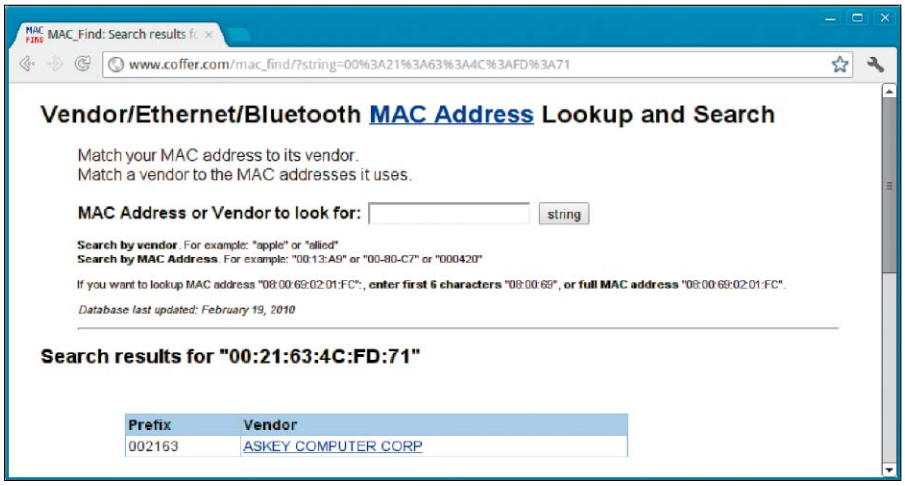
MAC-Adresse: Hersteller entschlüsseln

Eine weitere Information, die der Router aller Welt in den Broadcast-Paketen mitteilt, ist die eigene MAC-Adresse. Die MAC-Adresse steht auch bei WLANs, die über eine Verschlüsselung verfügen, im Klartext in den Netzwerkpaketen und wird hier auch BSSID genannt. Diese Adresse ist für jedes Gerät einmalig und enthält in den ersten sechs Stellen den Herstellernamen des Routers oder des Netzwerkchips. Sie haben ebenfalls die Möglichkeit, sich die MAC-Adresse des Routers mit dem Freeware-Programm Inssider anzeigen zu lassen. In der Übersicht der Netzwerke klicken Sie zu diesem Zweck mit Hilfe der rechten Maustaste die Tabellenüberschrift an und wählen im Anschluss daran im Menü „Vendor".

Auf eigene Faust können Sie MAC-Adressen darüber hinaus auf der englischsprachigen Webseite *www.coffer.com/mac_find* nach den enthaltenen Infos entschlüsseln.

Sicherheitslücken in der Router-Firmware

Die Kombination aus MAC und den verfügbaren WLAN-Standards (a/b/g/n) ist immer ein Hinweis auf das Router-Modell. Eine übersehene Gefahr sind die Router selbst. Hier schlummern in der Firmware oft Sicherheitslücken, die nie durch Hersteller-Updates behoben wurden. Eine umfangreiche, recht aktuelle Datenbank mit bekannten Schwachstellen bietet die englischsprachige Open Source Vulnerability Database unter *http://osvdb.org*. Hier können Sie im Feld „General Search" mit einer Volltextsuche nach Sicherheitslücken von Routern forschen – etwa, indem Sie den Herstellernamen eingeben.



MAC-Adresse: In der Hardware-Adresse jedes Netzwerkgeräts ist der Hersteller in den ersten drei Bytes codiert, die sich auf www.coffer.com/mac_find entschlüsseln lassen.

Dauerthema: Die WPS-Lücke

Ein hartnäckiges Problem ist die oft unsichere Implementierung von WPS (Wi-Fi Protected Setup) in Routern. WPS möchte die Konfiguration der WLAN-Clients über ein PIN-Verfahren vereinfachen. Seit Anfang 2012 sind aber bereits Sicherheitslücken bekannt: Oft lässt sich die PIN von WPS einfach per Ausprobieren knacken. Durch die verräterischen Antworten vieler Router reichen bereits 11 000 Anmeldeversuche aus, um eine PIN zu erraten und darüber ins WLAN zu kommen. Bei den meisten Routern ist WPS außerdem standardmäßig eingeschaltet. Das Ausnutzen dieser Sicherheitslücke ist derzeit noch versierten Linux-Anwendern vorbehalten, denn das dazu nötige Tool Reaver-WPS (Download unter *http://code.google.com/p/reaver-wps*) lässt sich nur unter Linux kompilieren. Mit dem Live-System Kali Linux (ISO-Datei unter *www.kali.org*) kann man sich den Aufwand sparen, denn hier ist Reaver bereits einsatzfertig vorinstalliert. Bevor Reaver-WPS in Aktion treten kann, müssen Sie allerdings noch den WLAN-Chip in den Monitormodus umschalten. Dies gelingt am einfachsten mit dem Programm Aircrack-ng. In Kali Linux schalten Sie in einem Terminal-Fenster mit

```
airmon-ng start wlan0
```

die Netzwerkkarte um. Anschließend steht die WLAN-Schnittstelle unter einer neuen Kennung bereit, in den meisten Fällen lautet diese „mon0". Wenn Sie den Namen der eigenen WLAN-Schnittstelle und die MAC-Adresse des Routers haben, können Sie Reaver-WPS nach folgendem Schema einsetzen:

```
reaver -i mon0 -b [Router-MAC]
  -vv
```

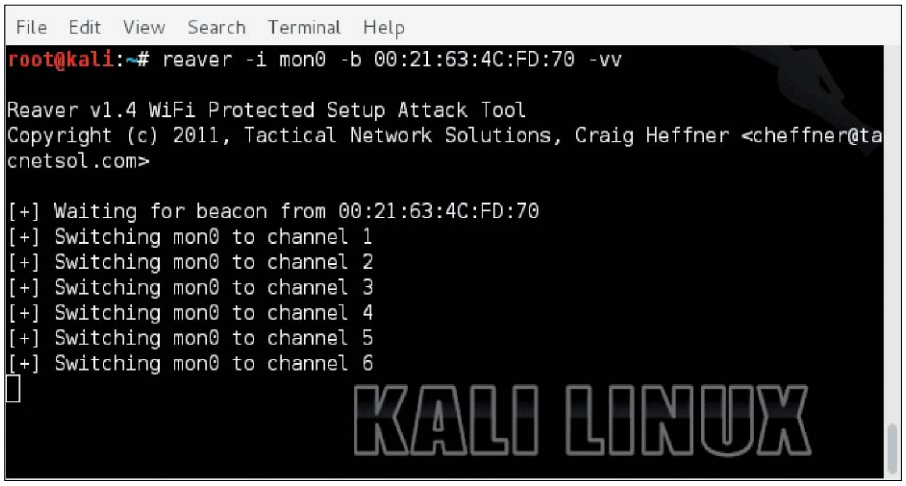
Da es sich hierbei jedoch um einen Brute-Force-Angriff handelt, kann der Check bis zu mehreren Stunden dauern. Für den Fall, dass der Angriff gelingt, erhalten Sie im Terminal die Ausgabe mit dem gefundenen WPA-Schlüssel. Auch wenn der Angriff für Sie wegen mangelndem Linux-Know-how nicht in Frage kommen sollte: Schalten Sie die WPS-Funktionalität im Router vorsichtshalber ab, wenn Sie sich nicht absolut sicher sind, dass der Hersteller diese weit verbreitete Sicherheitslücke behoben hat. Anwender, die AVM-Geräte im Einsatz haben, können dagegen beruhigt sein, denn die Fritzbox ist nicht verwundbar.

Check von innen

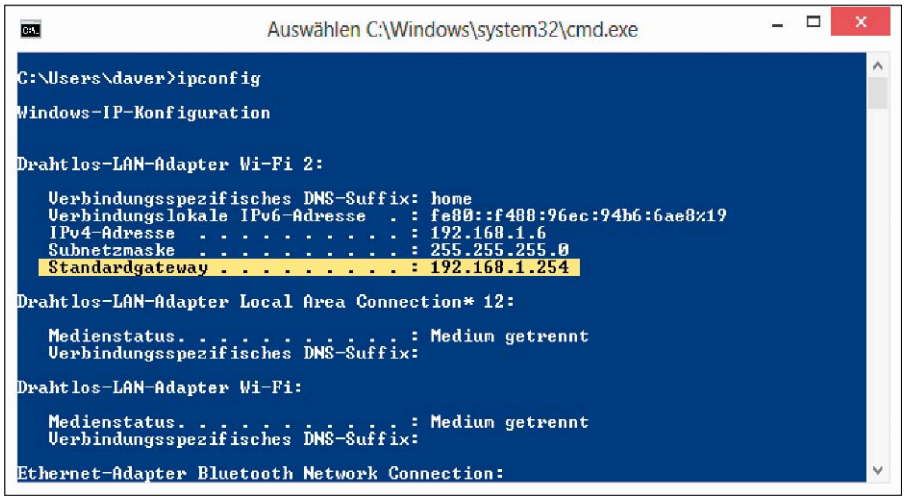
Wenn Sie mit dem Netzwerk verbunden sind, gibt der Router bereitwillig Auskunft über seine interne Netzwerkadresse, Ports, Dienste und eventuell sogar seine Konfiguration. Die

Übersicht Tools für Sicherheits-Checks

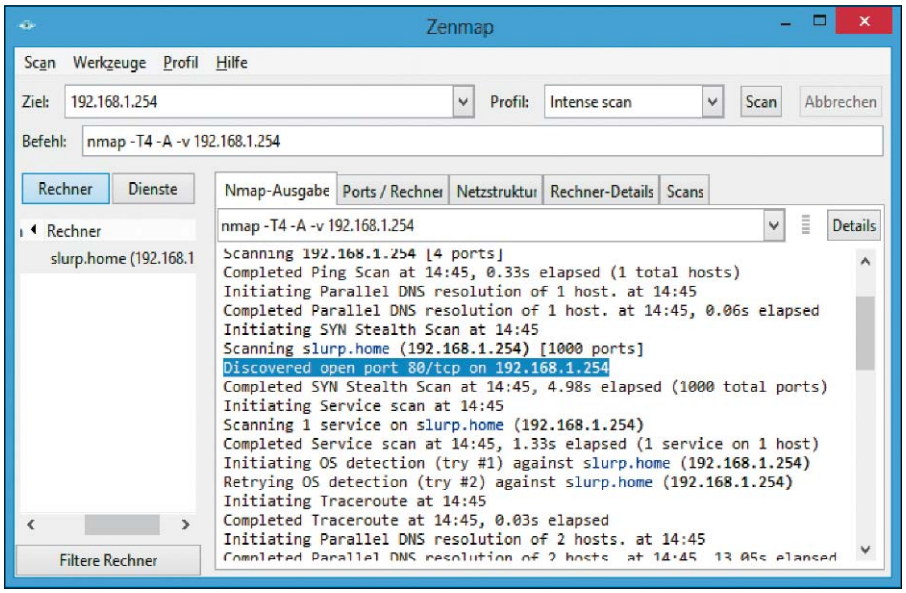
Programm	Beschreibung	Geeignet für	Internet	Sprache	Seite
Inssider 3.0.7	WLAN-Monitor	Windows Vista, 7, 8	*www.pcwelt.de/306569*	Englisch	22
Kali Linux 1.0	Linux-Live-System	Linux	*www.kali.org*	Englisch	23
Nmap 6.25	Portscanner	Windows Vista, 7, 8	*http://nmap.org/download.html*	Deutsch	24
Putty 0.62	SSH-Client	Windows Vista, 7, (8)	*www.pcwelt.de/729799*	Englisch	25
Reaver-WPS 1.4	WPS-Test	Linux	*http://code.google.com/p/reaver-wps/*	Englisch	23
THC-Hydra 7.4.2	Passworttest	Linux	*www.thc.org/thc-hydra*	Englisch	25



WPS knacken: Das Tool Reaver-WPS, hier unter Kali Linux, bietet eine Brute-Force-Attacke gegen Router mit einer bekannten Schwachstelle in Wi-Fi Protected Setup.



IP-Adresse des Routers: In Windows zeigt dieser Befehl in der Eingabeaufforderung die Gateway-Adresse an, die in Heimnetzwerken auch die Adresse des (WLAN-)Routers ist.



Portscanner Zenmap unter Windows: Eines der wichtigsten Tools bei der Suche nach Lücken ist Nmap, das hier über sein Frontend Zenmap einen Router auf offene Ports hin überprüfen kann.

Suche nach Sicherheitslücken beginnt ab hier, im eigenen Netzwerk. Besonders wichtig ist dieser Punkt, wenn Sie ein öffentliches WLAN anbieten oder viele Nutzer haben.

Die IP-Adresse des Routers finden

Im lokalen Netzwerk ist die IP-Adresse des Routers gleichzeitig die Gateway-Adresse, an die der Netzwerkverkehr für die Internetverbindung geht. Außerdem ist dies bei den meisten Routern mit integriertem DNS-Server auch die Adresse für DNS-Anfragen aus dem eigenen Netzwerk. Bei der Verbindungsaufnahme im LAN/WLAN erhält jeder Netzwerkteilnehmer über DHCP automatisch die Adresse des Routers für DNS und Gateway ins Internet. Um die Router-Adresse unter Windows herauszufinden, öffnen Sie nun ein Fenster der Eingabeaufforderung (Cmd.exe) und geben dort den Befehl *ipconfig* ein.

Die Ausgabe zeigt dann die Verbindungsinformationen aller Netzwerkschnittstellen. Interessant ist jedoch nur die aktive Schnittstelle, die mit dem Router verbunden ist. Hier erscheint die IP-Adresse des Routers in der Zeile „Standardgateway". Typische IP-Adressen von Routern sind 192.168.0.254 oder 192.168.1.254 in einem privaten C-Klasse-Subnetz. Einige Router verwenden gemäß Herstellereinstellungen ein A-Klasse-Netz nach dem Schema 10.0.0.0 bis 10.255.255.255. Die übliche Router-Adresse ist dann 10.0.0.138.

So setzen Sie den Portscan auf den eigenen Router an

Welche Dienste der Router im lokalen Netzwerk anbietet, lässt sich mit einem Portscanner herausfinden. Die mit Abstand bekannteste Anwendung für diesen Zweck ist der „Portscanner Network Mapper", auch kurz Nmap.

Das Programm steht unter GNU Public License für eine Vielzahl verschiedener Plattformen bereit und bringt für Windows das grafische Frontend Zenmap mit. Nmap lässt sich damit nicht nur von der Kommandozeile aus starten, sondern auch einfacher mit einer grafischen Bedienoberfläche. Nmap mit Zenmap finden Sie in Form der Setup-Datei „Nmap-6.25-setup.exe" als Download unter *http://nmap.org/download.html*.

In Zenmap geben Sie als Ziel die IP-Adresse des Routers ein. Wählen Sie im Auswahlmenü hinter Profil die gewünschte Scan-Methode, beispielsweise „Intense Scan", was für die gängigsten TCP-Ports ausreichen sollte. Unter „Nmap-Ausgabe" sehen Sie die detaillierten Ergebnisse des Scans. Auf der Seite „Ports/Rechner" sind die offenen Ports auf der untersuchten IP-Adresse aufgelistet.

Wichtiger, rechtlicher Hinweis: Scannen Sie nur eigene PCs und Netzwerke. Das Scannen fremder PCs oder Netzwerke kann eine Straftat sein und erheblichen Ärger mit den Administratoren einbringen.

Auf das Web-Frontend zugreifen

Wenn ein Portscan auf dem Router einen Webserver gefunden hat, etwa auf dem Port 80 (http) oder auf dem Port 443 (https), können Sie versuchen, sich mit dem Browser einfach mal zu verbinden. Geben Sie dazu die Adresse *http://[IP des Routers]:80* oder *https://[IP des Routers]*:443 im Adressfeld des Browsers ein. Meldet sich eine Anmeldemaske zur Eingabe von Log-in und Passwort, ist dies eine Einladung, hier sämtliche bekannte Standard-Anmeldeinformationen verschiedener Hersteller auszuprobieren. Die meisten Router haben in den Standardeinstellungen recht einfache Log-ins. Üblicherweise melden sich Router hier auch gleich mit der kompletten Typenbezeichnung. Diese können Sie dazu verwenden, um im Handbuch des Routers, das Sie zumeist über die Hersteller-Webseite bekommen, nach den Standard-Log-ins zu suchen. Einige Router bieten im Web-Frontend auch sehr einfach zu findende Sicherheitslücken. So erlaubt zum Beispiel der verbreitete Router 3COM Office Connect den Zugriff auf das interne Script „SaveCfgFile.cgi“ ganz ohne Anmeldung, um die komplette Konfiguration mit unverschlüsselten Passwörtern im Browser anzuzeigen.

Hintertür: Telnet-Verbindungen zum Router

Einige Router erlauben den Zugang für deren Konfiguration nicht nur über ein Web-Frontend, sondern auch über Telnet. Dies ist ein altes Protokoll zum Aufbauen einer Terminal-basierten Verbindung zu einem Host, um eine dort bereitgestellte Befehlszeile über das Netzwerk zu nutzen. Der Telnet-Port ist üblicherweise 23, es lohnt sich aber, auch andere Portnummern offener Ports auszuprobieren, um zu sehen, ob der Router dort antwortet. Unter Windows nutzen Sie Telnet in der Eingabeaufforderung mit dem Befehl *telnet [IP-Nummer]*. Es erfolgt üblicherweise auch hier die Abfrage von Anmeldeinformationen, und es lohnt sich, die Standard-Log-ins der Werkseinstellungen des Routers auszuprobieren. Geräte für den professionellen Einsatz, etwa von Cisco, bieten auch einen Zugang über SSH auf dem Port 22 an. Um sich unter Windows mit dem SSH-Server des Routers zu verbinden, reichen die Bordmittel jedoch nicht aus. Sie brauchen einen SSH-Client wie Putty (auf DVD, Download unter *www.pcwelt.de/729799*).

Mit roher Gewalt: THC-Hydra ist ein Brute-Force-Tool, das Anmeldeinformationen aus einer vorbereiteten Liste auf Formulare im Web anwenden kann. Das Tool müssen Sie selbst kompilieren oder unter Kali Linux einsetzen.

Passwort durch Brute-Force-Angriffe ermitteln

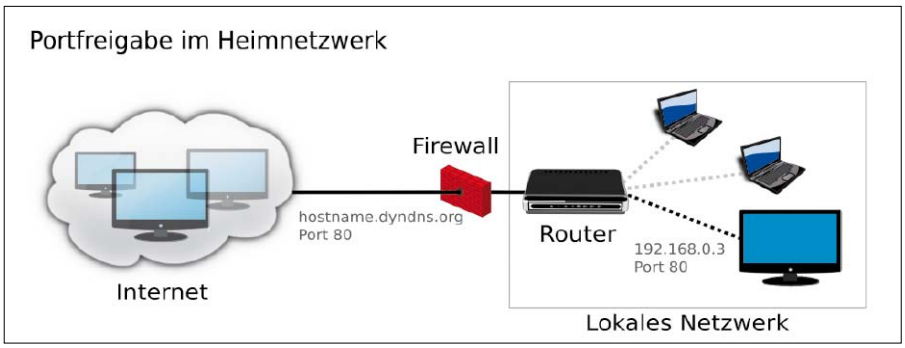
Auch wenn der Router sich keine Blöße gibt, lässt sich noch eine Methode einsetzen, um den Router anzugreifen: Man kann Router mittels Brute Force, also durch Ausprobieren, auf schwache Passwörter hin überprüfen. Eines der mächtigsten Tools dafür ist das Open-Source-Programm THC-Hydra. Das Tool stammt aus der Linux-Ecke und steht im Quellcode unter *www.thc.org/thc-hydra* zum Download. Es ist auch im erwähnten Live-System Kali Linux vorinstalliert. THC-Hydra wird über die Befehlszeile bedient und spielt seine Stärke mit Regular Expressions aus, um Log-in-Dialoge und Formulare auf Webseiten mit Anmeldeversuchen zu bombardieren. Es unterstützt GET- und POST-Requests sowie mehrere Threads und ist daher auch bei langsamer Netzwerkverbindung noch flott. Log-ins und Passwörter übergeben als Textdateien.

Sie können eine laufende Überprüfung darüber hinaus unterbrechen und später fortsetzen, falls das Tool mehrere Stunden lang zugange sein sollte. Allerdings darf hier wiederum der rechtliche Hinweis nicht fehlen: Setzen Sie THC-Hydra ausschließlich in Ihrem eigenen Netzwerk ein.

Von außen ins Netzwerk

Netzwerkverkehr von außen durch die Firewall zu erlauben, ist die Voraussetzung für den Fernzugriff aus dem Internet auf eigene Server-Dienste. Dies gelingt mit Portfreigaben und dynamischen Host-Namen.

Das eigene lokale Netzwerk und die dort angemeldeten Teilnehmer müssen vor unerwünschten Anfragen oder Zugriff aus dem Internet gut abgeschottet sein. Diese Aufgabe übernimmt im Heimnetzwerk der (WLAN-)Router, der mit einem Paketfilter ausgestattet ist, um unerwünschten Netzwerkverkehr von draußen zu blockieren. Mittels Network Address Translation (NAT) sorgt der Router außerdem dafür, dass die Teilnehmer im lokalen Netz nicht direkt erreichbar sind, sondern nur gesammelt über die IP des Routers online gehen. Denn NAT reicht die Datenpakete aus dem Internet an die Privatadressen der einzelnen Clients weiter.



Schema einer Portfreigabe im Heimnetzwerk: Der Router agiert als Firewall, bekommt einen dynamischen Host-Namen und leitet Anfragen auf einen Port an einen Server im Netzwerk weiter.

Darf das Programm seine Dienste anbieten: Ab Windows 7 meldet sich die Firewall von Windows automatisch, wenn eine Anwendung einen Port öffnen will.

Wohldosierte Portfreigaben durch die Firewall

Steht dagegen im eigenen lokalen Netzwerk ein PC, der über das Internet erreichbar sein soll, dann ist die rigorose Abschottung mit Paketfilter und NAT kontraproduktiv. Etwa, wenn ein FTP-Server von außen Verbindungen annehmen muss oder ein Bittorrent-Client im Server-Modus eingehende Verbindungen akzeptieren soll. Damit ein Rechner und der darauf laufende Server-Dienst im Netzwerk gezielt von außen erreichbar ist, müssen Sie von innen ein wohldefiniertes Loch durch die Firewall bohren. Dies gelingt mit einer Portfreigabe und Portweiterleitung auf dem Router, der dann dafür sorgt, dass die Anfragen an den offenen Port intern zum richtigen PC gelangen, ohne das Netzwerk zu gefährden.

Den Ziel-Server vorbereiten

Die Konfiguration beginnt auf jenem PC im eigenen Netzwerk, der den Server-Dienst für Zugriffe aus dem Internet beherbergen soll. Der Einfachheit halber geht der Beitrag davon aus, dass es sich dabei um ein Windows-System handelt. Notieren Sie sich auch gleich die LAN-IP-Adresse des PCs, denn die benötigen Sie später. Diese IP ermitteln Sie, indem Sie in den Ausführen-Dialog von Windows, den Sie mithilfe der Tastenkombination Windows-Taste-R aufrufen, den Befehl

```
cmd /k ipconfig
```

eingeben. In der Ausgabe findet sich die IP-Nummer in der Zeile „IPv4-Adresse“.

Installieren Sie das Server-Programm und lassen Sie zu, dass dieses Programm seine Dienste auf dem genutzten Port durch die Windows-Firewall hindurch anbietet. Diese Erlaubnis müssen Sie manuell erteilen. Mit ihren Voreinstellungen erlaubt die Windows-Firewall von Vista/7/8 nämlich auch bei den freizügigen Netzwerkprofilen „Heimnetzwerk“ und „Arbeitsplatznetzwerk“ nur wenige vordefinierte Ports für die Datei- und Druckerfreigabe. Um hier ganz gezielt mehr zu ermöglichen, gehen Sie in der Systemsteuerung auf „System und Sicherheit → Windows-Firewall → Ein Programm oder Feature durch die Windows-Firewall zulassen“.

Dort angekommen, können Sie nun über die Schaltfläche „Einstellungen ändern“ mittels „Anderes Programm zulassen“ das Server-Programm auswählen, das durch die Firewall Netzwerkpakete empfangen darf.

Ab Windows 7 warnt die Firewall Sie übrigens selbständig, wenn eine Anwendung durch den Paketfilter hindurch Verbindungen akzeptieren will. Sie können die Erlaubnis direkt im Meldungsfenster der Windows-Firewall erteilen. Ausflüge in die Systemsteuerung dienen dann lediglich der Kontrolle sowie zum Löschen von Ausnahmeregeln.

Einen Port auf dem Router freigeben

Die Portweiterleitung richten Sie jetzt auf der Administrationsoberfläche des Routers ein. Kommt die weitverbreitete Fritzbox zum Einsatz, dann gehen Sie dafür auf der Administrationsoberfläche von *http://fritz.box* zunächst auf „Einstellungen → System → Ansicht“. Stellen Sie hier die „Expertenansicht“ ein. Anschließend können Sie über „Internet → Portfreigabe → „Neue Portfreigabe“ einen Port auf dem Router öffnen und zu einem Rechner im Netzwerk weiterleiten.

Dazu ein praktisches Beispiel: Steht im Netzwerk ein FTP-Server, der Verbindungen auf dem Port 21 entgegennimmt, wählen Sie im Konfigurationsdialog der Fritzbox unter „Portfreigabe aktiv für“ die Option „Andere Anwendungen“. Als „Bezeichnung“ geben Sie als Notiz einen Namen für diese Portfreigaben an, etwa „FTP-Server“, und wählen unter „Protokoll“ die erforderliche Protokollart aus. Ein FTP-Server nutzt das übliche TCP-Protokoll und nicht etwa UDP. Im Feld „von Port“ geben Sie den Port an, auf dem Anfragen aus dem Internet auf dem Router eingehen sollen, beispielsweise Port 21 für FTP.

Die Angabe „bis Port“ ist optional und nur notwendig, wenn Sie den gesamten Portbereich freigeben möchten. Ansonsten tragen Sie hier bei einem Einzelport nur nochmal die Portnummer 21 ein. Nun teilen Sie der Fritzbox mit, wohin diese Anfragen im lokalen Netz gehen sollen. Dazu geben Sie für „an IP-Adresse“ die lokale IP-Adresse des Rechners ein, der den Server-Dienst zur Verfügung stellt. Abschließend geben Sie unter „an Port“ noch die Portnummer ein, auf welcher der Server-Dienst auf dem PC lauscht. Bei FTP ist das auch wieder der Port 21.

Tabu Zugangsdaten unverschlüsselt übertragen

Die im Home-Office häufig für den Zugriff auf eigene Server eingesetzten Protokolle HTTP, FTP und Web DAV haben ein Problem gemeinsam: Die Zugangsdateien für die Anmeldung an Servern werden unverschlüsselt übertragen. Unterwegs, beim Zugriff auf das heimische Netzwerk über öffentliche WLAN-Verbindungen, ist die Anmeldung über diese Protokolle deshalb tabu. Denn es besteht immer ein erhöhtes Risiko, dass die Zugangsdaten in falsche Hände gelangen. Verwenden Sie daher von unterwegs immer verschlüsselnde Protokolle, auch wenn dies Server-seitig mehr Administrationsaufwand ist: HTTPS anstatt HTTP sowie SFTP oder FTPS anstatt des einfachen FTP.

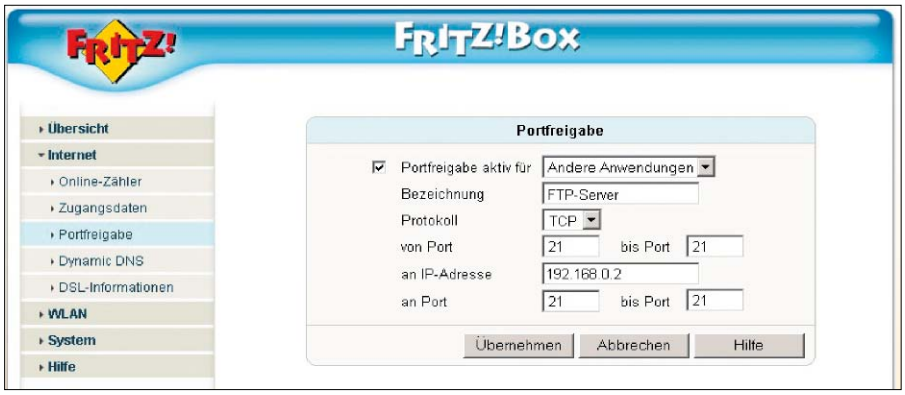
Bei den Routern anderer Hersteller funktioniert die Portfreigabe auf ähnliche Weise, die Menüpunkte unterscheiden sich jedoch deutlich. Zumeist ist ein Menüpunkt namens „Portforwarding“, „Portmapping“, „Forward“ „Custom Service“ oder „Virtual Server“ vorhanden. Bei der Detaileinstellung der Portfreigaben erscheinen dann häufig die folgenden Bezeichnungen:

Public Port / External Port / Inbound Service: Damit legen Sie die Portnummer auf dem Router fest, die vom Internet aus erreichbar sein soll.

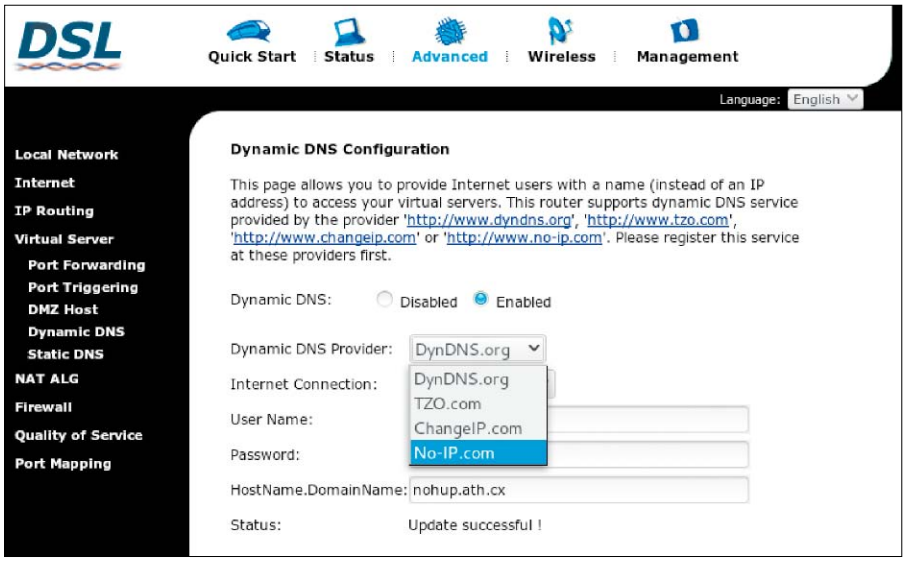
Private IP / Internal IP: Tragen Sie in dieses Eingabefeld die IP-Adresse des PCs im lokalen Netzwerk ein, an den die Datenpakete weitergeleitet werden sollen.

Private Port / Internal Port: Hier geben Sie die Portnummer für den PC mit dem Server-Dienst im lokalen Netzwerk ein. Üblicherweise ist dies der gleiche Port, den Sie auch bei „Public Port“, „External Port“ oder „Inbound Service“ eintragen.

Type / Protocol: Hier wählen Sie den Protokolltyp TCP oder UDP aus.



Eine Portfreigabe (Portweiterleitung) auf der Fritzbox definieren: Hier ist beispielsweise ein FTP-Server auf dem Port 21 und der internen LAN-IP 192.168.0.2 definiert.



Dynamischer Host-Name: Viele Router unterstützen mehrere DNS-Anbieter, etwa den hier gewählten kostenlosen Dienst von www.noip.com. Dyn DNS ist für Neukunden jedoch nicht mehr kostenlos.

Host-Name: Den Router erreichbar machen

Wenn die Portweiterleitung steht und der Server-Dienst im eigenen Netz läuft, ist dieses bereits aus dem Internet erreichbar. Allerdings bleibt noch ein Problem: Der DSL- oder Kabel-Provider vergibt bei jedem Verbindungsaufbau eine neue IP-Adresse. Diese Adresse müssten Sie jedes Mal herausfinden, beispielsweise über die Webseite *http://ifcon fig.me*, und das ist zu umständlich.

Für Abhilfe sorgt in diesem Fall der Dienst von DNS-Anbietern, die bei der Einwahl des Routers die Internet-IP-Adresse einem dynamischen Host-Namen zuordnen. Dynamisch deshalb, weil der Router seine neue Internet-IP-Adresse bei jeder Einwahl automatisch dem DNS-Dienst mitteilt. In den letzten Jahren war Dyn DNS (*www.dyndns.org*) die erste Wahl. Mittlerweile akzeptiert dieser Service aber keine kostenlosen Neuanmeldungen mehr, sondern bietet nur noch kostenpflichtige Konten ab 25 US-Dollar an sowie befristete Test-Accounts, für die Sie aber eine Kreditkartennummer angeben müssen. Wer einen Router von D-Link betreibt, erhält weiterhin unter *www.dlinkddns.com* einen Gratis-Account für Dyn DNS. Im Prinzip kann sich hier jeder anmelden. Beachten Sie jedoch, dass der Anbieter den Zugang löscht, wenn Sie auf Nachfrage keine Seriennummer für einen D-Link-Router liefern.

Eine kostenlose Alternative, die von der Firmware vieler Router unterstützt wird, ist bei *www.noip.com* erhältlich. Ob Ihr Router mitspielt, können Sie in dessen Administrationsoberfläche überprüfen. Die Fritzbox bietet den Dienst in jedem Fall an.

Nach der kostenlosen Registrierung auf *www.noip.com* über die Mailadresse erhalten Sie die Zugangsdaten per Mail und definieren dann nach einer Anmeldung den eigenen Host-Namen als Subdomain über einen A-Record auf der Webseite. Die erhaltenen Kontodaten und den eingerichteten Host-Namen geben Sie in die dafür vorgesehenen Eingabefelder des Routers ein. Bei der Fritzbox finden Sie diese unter „Internet → Freigabe → Dynamic DNS“. Im Feld „Dynamic-DNS-Anbieter“ wählen Sie „No-IP.com“ aus und tragen darunter die Nutzerdaten ein.

Die Portweiterleitung von außen überprüfen

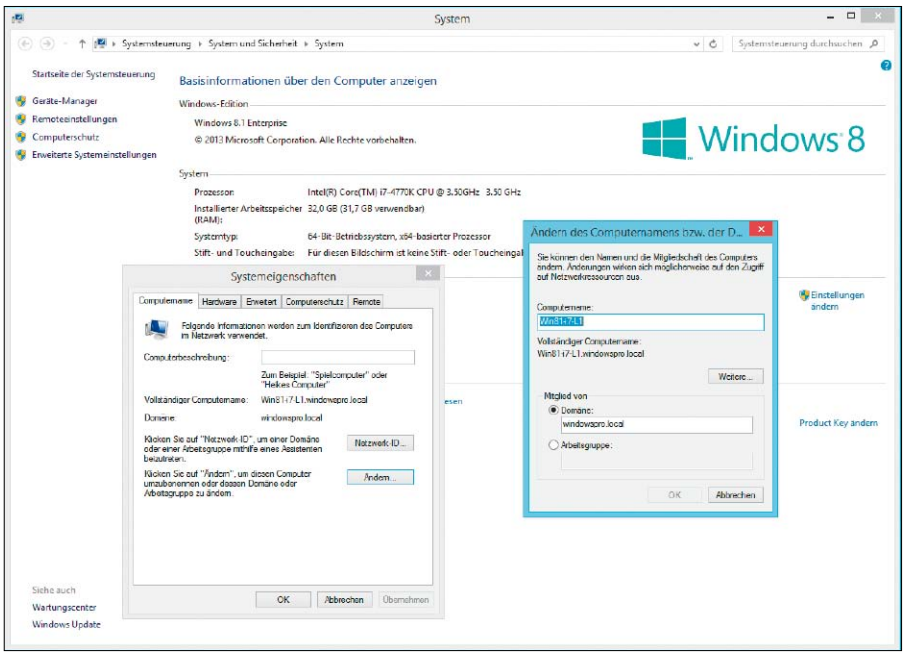
Ob alles wie gewünscht funktioniert, müssen Sie von außen unter realen Bedingungen prüfen. Dazu benötigen Sie Zugriff auf einen anderen PC, der über einen anderen Router mit dem Internet verbunden ist und nicht im eigenen Netzwerk hängt. Einen Test, ob der Router Verbindungen auf dem freigeschalteten Port akzeptiert, können Sie allerdings auch aus dem eigenen Netzwerk heraus ausführen: Der PC-WELT Browser-Check auf *http://browser-check.pcwelt.de* offeriert über den Menüpunkt „Firewall-Check“ eine Portscanner-Funktion. Geben Sie dazu im Feld „Zusätzlichen Port überprüfen“ die Nummer des freigeschalteten Ports ein. Geöffnete Ports zeigt der Check mit einem roten Warnsymbol an.

Beachten Sie, dass viele Router Portscans dieser Art blockieren. Um einen hartnäckigen Scan auf den Host-Namen zu starten, ist daher der Service von *http://port-scan.e-dns.org* empfehlenswert. Den gewählten, dynamischen Host-Namen des Routers müssen Sie hier manuell eingeben, allein mit IP-Adresse funktioniert der Scan nicht. ■

Windows-Tricks für IT-Profis

Tipps zum Management von Benutzern, Passwörtern und Speicher auf Windows-PCs, die einer AD-Domäne oder einer Workgroup angehören.

VON WOLFGANG SOMMERGUT



Der Beitritt eines PCs zu einer Active-Directory-Domäne über die „Systemsteuerung“ erfolgt in Windows 8.1 wie in früheren Versionen des Betriebssystems. Allerdings muss ein PC mit 8.1 andere Voraussetzungen erfüllen.

MUSS MAN EINE GRÖSSERE ZAHL von Windows-Rechnern effizient verwalten, dann führt kein Weg am Active Directory (AD) vorbei. Sind PCs Mitglied in einer Domäne, lassen sich viele Einstellungen zentral über Gruppenrichtlinien festlegen, und die Verwaltung der Benutzer erfolgt an einer Stelle.

Aber selbst wenn alle Rechner einer AD-Domäne beigetreten sind, bleiben gelegentlich noch Aufgaben, die sich nur lokal erledigen lassen. Dazu zählen etwa bestimmte Aspekte bei der Verwaltung lokaler Benutzer oder das Management von Laufwerken und Volumes.

Mit Windows 8.1 einer Domäne beitreten

Auf den ersten Blick mag es aussehen, als ändere sich die Prozedur für einen Domain Join von Windows 8.x nicht wesentlich gegenüber Windows 7. Ein PC muss jedoch andere Voraussetzungen erfüllen, und die Mitgliedschaft in einer Domäne hat geringere Auswirkungen auf das Management der Geräte. Neben dem bekannten Dialog „Systemeigenschaften“ empfehlen sich die App PC-Einstellungen und Powershell für den Beitritt in eine Domäne.

Zu den veränderten Systemvoraussetzungen zählt, dass der Domain Join nicht nur Home-Editionen von Windows verwehrt bleibt, sondern auch der ARM-Ausführung des Betriebssystems namens Windows RT. Mitgliedschaft in einer AD-Domäne bleibt somit den Editionen Pro und Enterprise vorenthalten.

Name des PCs beim Domain Join ändern

Als Voraussetzung für den Beitritt zu einer Domäne gilt wie gewohnt, dass man über ein Domänenkonto verfügt, das dazu berechtigt, einen Rechner ins Active Directory aufzunehmen. Außerdem sollte der Client einen DNS-Server nutzen, der ihm über einen SVR-Eintrag (Service Resource Records) den Weg zum Domain Controller weist. Dies ist typischerweise bei einem DNS der Fall, der auf einem DC läuft. Die eigentliche Aufnahme eines PCs in eine Domäne erfolgt auf die gleiche Weise wie unter Windows 7, wenn man den Weg über die grafische Oberfläche nehmen will. Der kürzeste Weg zu „Systemsteuerung → System und Sicherheit → System“ führt über die Suchfunktion der Startseite, wo man über den Begriff „Domäne“ fündig wird.

In den Dialog trägt man den Namen der Domäne und bei Bedarf die neue Bezeichnung für den Rechner ein. Wie bisher ist es hier nicht möglich, die OU (Organisation Unit, Organisations-Einheit) festzulegen, der das Computer-Konto zugeordnet werden soll. Daher landet es standardmäßig im Container „Computer“. Das lässt sich nur verhindern, wenn man für den Namen des Rechners schon vorab ein Konto in der gewünschten OU anlegt. Seit Windows 8.1 ist auch die Modern App PC-Einstellungen in der Lage, Rechner einer AD-Domäne anzuschließen. Die zuständigen Optionen finden sich unter „PC und Geräte → PC-Info“ und entsprechend weitgehend jenen in der Systemsteuerung.

Alle Schritte in einem Powershell-Kommando

Im Gegensatz zu den GUI-Tools kann Powershell mit dem Cmdlet Add-Computer alle Schritte für den Beitritt zu einer Domäne in einem Befehl erledigen. Dazu zählen neben dem Anschluss an die Domain auch eine etwaige Umbenennung des Rechners sowie sein Neustart.

Damit ist Add-Computer faktisch der Nachfolger von *netdom*, das nicht zum Lieferumfang des Betriebssystems gehört, das sich aber über RSAT für Windows 8.x installieren lässt (*http://goo.gl/SPWai3*).

In der einfachsten Form erfolgt der Aufruf des Powershell-Befehls in der Form

```
Add-Computer -DomainName <Name
 DerDomain>
```

Er nimmt nach Eingabe der Anmeldedaten für das berechtigte Konto den lokalen Rechner in die gewünschte Domäne auf. Möchte man die Prozedur für einen Remote-PC ausführen, muss man dessen Namen über den Parameter *-ComputerName* mitteilen.

Will man den Computer auch noch gleich umbenennen, dann kann man dies mit Hilfe des Parameters *-NewName* tun. Für die Zuordnung des neu erstellten Kontos zu einer bestimmten OU ist *-OUPath* zuständig, wobei man sie als Distinguished Name angeben muss, also zum Beispiel *OU=Marketing,DC=contoso,DC=de*. Soll der Rechner nach dem Domain Join neu starten, dann fügt man noch den Parameter *-restart* an:

```
Add-Computer -DomainName contoso.
 de -NewName W8Mar33 -OUPath
 OU=Marketing,DC= cont
 oso,DC=de -Restart
```

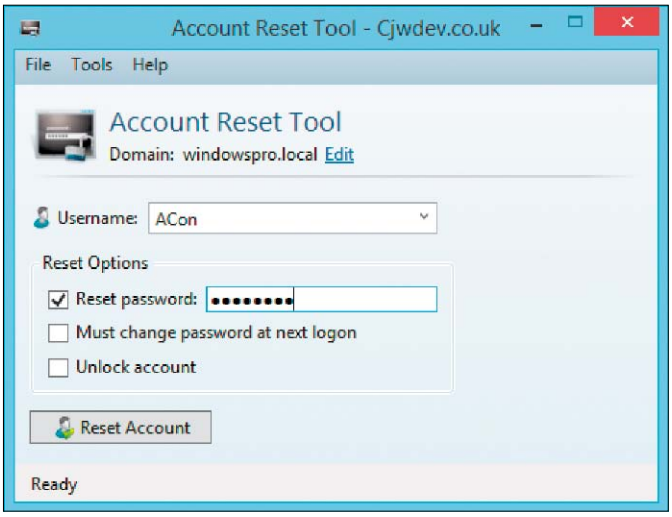
Wenn man einen bestimmten Domänen-Controller ansprechen möchte, gibt man diesen über den Parameter *-Server* an. Will man schließlich auf die interaktive Eingabe der Anmeldedaten verzichten, dann kann man *Add-Computer* stattdessen ein *Credentials*-Objekt mitgeben. Eine Anleitung dazu gibt's über *http://goo.gl/5mWfQ4*.

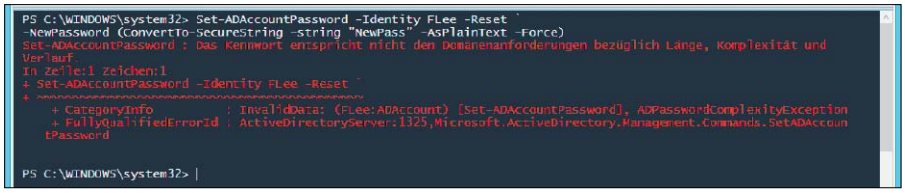
Passwörter zurücksetzen

Ist ein Windows-PC Mitglied einer AD-Domäne, dann melden sich die Benutzer dort meistens über AD-Konten an. Diese werden über die entsprechenden Tools zentral verwaltet, so dass ein Administrator auch für das Passwort-Management nicht mehr zu einzelnen Rechnern gehen muss.

Fehlgeschlagene Anmeldeversuche aufgrund vergessener Passwörter gehören zu den alltäglichen Problemen, mit denen der Helpdesk konfrontiert ist. Neben den gängigen GUI-Tools aus dem RSAT-Fundus und kostenlosen Programmen, die auf diesen Zweck zugeschnitten sind, kann auch die Kommandozeile oder Powershell Passwörter zurücksetzen.

Das kostenlose Account Reset Tool ist eine von mehreren GUI-Optionen, aber häufig ist die Kommandozeile eine gute Alternative.





Powershell gibt klar Auskunft darüber, warum das Zurücksetzen eines Passworts gescheitert ist.

Unter den Kommandozeilen-Tools für das AD-Management ist *dsmod* für das Passwort-Reset zuständig. Die Syntax dafür ist etwas umständlich, weil man die Art des AD-Objekts spezifizieren und den Benutzernamen als Distinguished Name angeben muss:

```
dsmod user "CN=Bseidl,OU=Sales,DC
 =contoso,DC=com" -pwd NewPass
```

Bei Bedarf kann man für den Parameter *user* mehrere Konten angeben, die jeweils in Anführungszeichen stehen und nicht durch Kommata getrennt werden. Fügt man noch *-mustchpwd yes* an, dann muss der User beim nächsten Anmelden sein Kennwort ändern.

Ein alternatives Vorgehen für den Aufruf von *dsmod* besteht darin, dass man *dsquery* nutzt, um den Distinguished Name für einen User Principal Name zu ermitteln und diesen über eine Pipe an *dsmod* zu übergeben:

```
dsquery user -name bseidl | dsmod
 user -pwd NewPass
```

Passwort-Reset mit Powershell

Das Active-Directory-Modul von Powershell enthält das Cmdlet *Set-ADAccountPassword*, mit dem sich Passwörter ändern oder zurücksetzen lassen. Wenn man ihm mit dem Parameter *-Identity* nur den Benutzernamen übergibt, kann man das Passwort interaktiv ändern:

```
Set-ADAccountPassword -Identity
 FLee
```

Diese Variante eignet sich nur für den Inhaber des Kontos, weil man zuerst nach dem alten Passwort gefragt wird. Ein Administrator, der das Passwort für andere Benutzer zurücksetzen soll, muss den Aufruf um weitere Angaben ergänzen. Dazu zählen das neue Passwort sowie der Schalter *-Reset*:

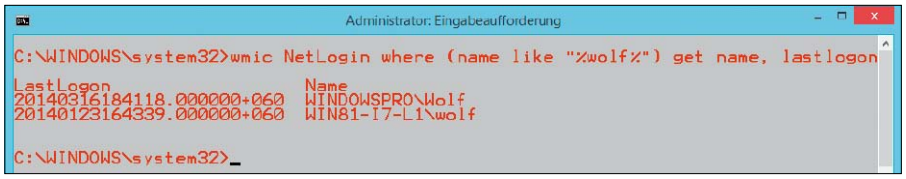
```
Set-ADAccountPassword -Identity
 FLee -Reset -NewPassword (Con
 vertTo-SecureString -string
 "NewPass" -AsPlainText -Force)
```

Zu beachten ist hier, dass das neue Passwort (*NewPass* in diesem Beispiel) als Secure String übergeben werden muss, was sich durch die Verwendung der Funktion *ConvertTo-SecureString* bewerkstelligen lässt.

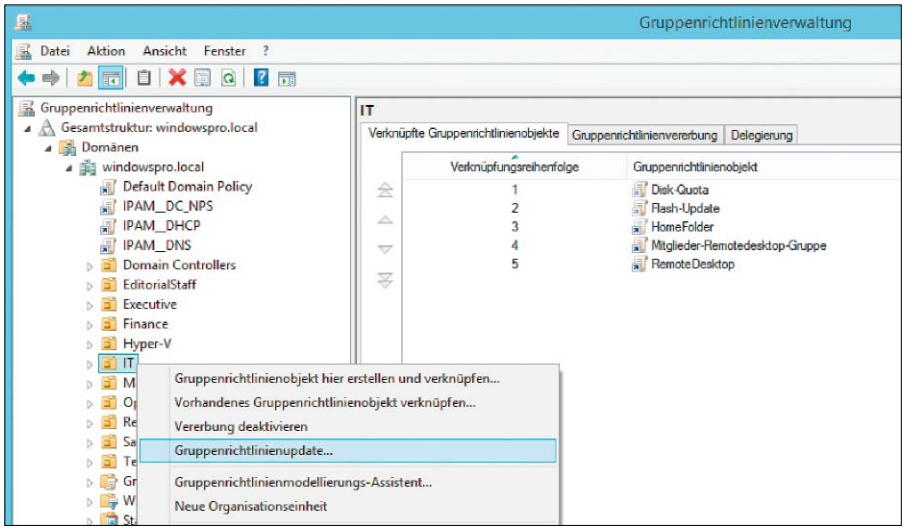
Soll das Passwort für eine größere Zahl von Benutzern zurückgesetzt werden, dann findet sich dafür auf Microsofts Technet-Galerie ein Script (Download über *http://goo.gl/VN3SA1*). Es kann Listen von User-Namen und Kennwörtern aus einer Excel-Datei importieren und in einem Durchgang abarbeiten.

Wann war ein Benutzer das letzte Mal angemeldet?

Zu einem häufigen Anliegen beim Benutzer-Management gehört neben dem Passwort-Reset, dass man wissen möchte, ob User noch aktiv sind. Dies lässt sich am ehesten über das letzte Log-on ermitteln. Wenn man herausfin-



Die Datumsausgabe von wmic erfolgt im schlecht lesbaren Format Jahr + Monat + Tag.



Über die Gruppenrichtlinienverwaltung lassen sich alle GPOs auf den PCs einer OU remote ausführen.

den möchte, wann sich ein lokaler Benutzer das letzte Mal an einem Rechner angemeldet hat, dann bekommt man diese Information über Windows Management Instrumentation (WMI). Als Tools dafür eignen sich *wmic* oder Powershell. Möchte man das letzte Log-in eines Domänen-Users erfahren, dann erschließt sich dieses über eine Anfrage an das AD.

Für die Auskunft über die letzte Anmeldung eines Benutzers an einem bestimmten Rechner ist das WMI-Objekt „Win32_NetworkLoginProfile" zuständig, das unter anderem den Benutzernamen und den Zeitpunkt des Logins vorhält. In *wmic* existiert dafür ein Alias namens *netlogin*, das die Abfrage vereinfacht. Um detaillierte Angaben zu anderen Benutzern zu erhalten, muss man zum Beispiel diesen Befehl in einer Eingabeaufforderung mit administrativen Rechten eingeben:

```
wmic NetLogin where (name like
 "%admin%") get name, lastlogon
```

Der Aufruf von *wmic* in dieser Form gibt den Benutzernamen und die Zeit des letzten Logins aus, und zwar für alle User, deren Name die Zeichenkette „admin" enthält. Lässt man die Einschränkung mittels *where*-Klausel weg, dann erhält man die Informationen für sämtliche lokale Konten. Wie generell üblich bei Windows Management Instrumentation (WMI) lässt sich die *wmic*-Anfrage auch an entfernte Rechner stellen, indem man den Parameter */node:<Name des PCs>* hinzufügt.

Konvertiertes Datumsformat mit Powershell

Das Ergebnis von *wmic* hat den Schönheitsfehler, dass es Zeit und Datum in einer einzigen Zeichenkette ausgibt, die mit dem Jahr beginnt. Möchte man hier eine besser lesbare Form, empfiehlt sich der Einsatz von Powershell:

```
Get-WmiObject -class Win32_Networ
 kLoginProfile -Filter "name like
 '%admin%'" | select Name, @{Name
 ="Letzter Login";Expression={$_.
 ConvertToDateTime($_.LastLogon)}}
```

Der Powershell-Aufruf fällt etwas länger aus, weil er die von WMI gelieferte Datumsangabe in einer Calculated Property mit Hilfe der dafür vorhandenen Konvertierungsfunktion in ein angenehmeres Format bringt.

Letztes Login eines Domänen-Users erfragen

Wenn man das letzte Log-in eines Domänen-Users ermitteln will, muss man das Active Directory konsultieren. Auch da empfiehlt sich Powershell, in der man diese drei Befehle absetzt, um zum Beispiel die Informationen zum User „Administrator" zu ermitteln:

```
Import-Module ActiveDirectory
$user = Get-ADUser "Administra
 tor" | Get-ADObject -Properties
 lastLogon
[DateTime]::FromFileTime($user.
 lastlogon)
```

Dabei handelt es sich um die absolute Minimalvariante, die etwa keinen Domain Controller (DC) explizit auswählt, sondern den Standard-DC nimmt. Außerdem fängt es keine Fehler ab, die auftreten können, wenn ein User nicht existiert oder sich nie angemeldet hat.

Gruppenrichtlinien remote aktualisieren

GPOs sind das wichtigste Werkzeug in der zentralen Verwaltung von Windows-Rechnern. Ihre Ausführung erfolgt nach dem Pull-Prinzip in vorgegebenen Intervallen (Standard: 90 Minuten). Möchte man einen Refresh ohne Verzögerung anstoßen, dann kann man dies auf den Zielrechnern lokal mittels *gpupdate* tun (Infos über *http://goo.gl/KdDQeJ*). Windows 8.x und Server 2012 (R2) bieten darüber hinaus die Möglichkeit, Gruppenrichtlinien remote zu aktualisieren. Der lokale Aufruf von *gpupdate* eignet sich primär dazu, auf einzelnen Rechnern zu testen, wie sich die Änderungen an einem GPO auswirken. Wer jedoch eine modifizierte Gruppenrichtlinie auf vielen Rechnern sofort umsetzen möchte, musste bisher auf Scripts oder Tools von Drittherstellern ausweichen, beispielsweise auf Remote GPO Refresh (*http://sdmsoftware.com/gpoguy*).

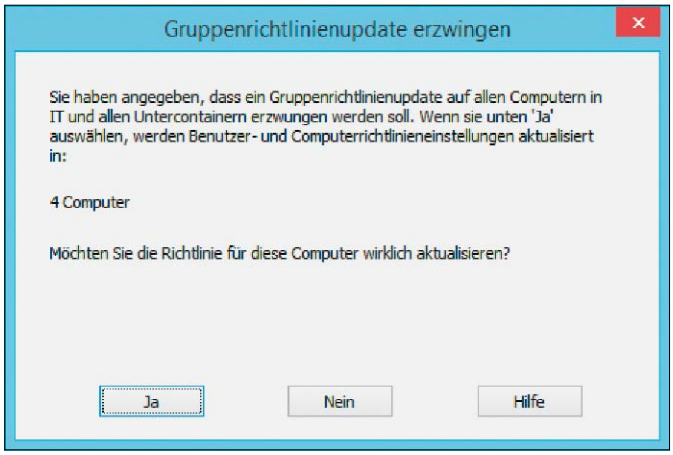
Refresh-Befehl in der Gruppenrichtlinienverwaltung

Die Gruppenrichtlinienverwaltung enthält seit Windows Server 2012 und RSAT für Windows 8 eine Option zur Remote-Aktualisierung von GPOs auf allen Computern einer Organisationseinheit. Zu diesem Zweck öffnet man in der Baumstruktur das Kontextmenü einer OU und führt dort den Befehl „Gruppenrichtlinienupdate" aus. Er bewirkt, dass in der Aufgabenplanung aller Rechner in dieser Organisationseinheit eine Task für den Refresh der Gruppenrichtlinie eingerichtet wird. Die Aufgaben werden nach Zufallsprinzip über einen Zeitraum von zehn Minuten verteilt, um ein gleichzeitiges Update vieler Clients zu vermeiden.

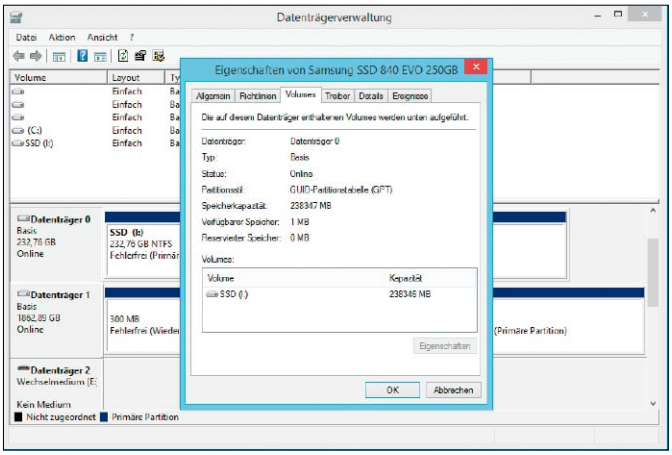
Die Planung eines zeitgesteuerten Tasks auf einem entfernten Rechner erfolgt über WMI und Remote Procedure Calls (RPCs), so dass sichergestellt sein muss, dass die Firewall auf den Zielrechnern ein solches Management zulässt. Sonst muss mit der berüchtigten Fehlermeldung „Der RPC-Server ist nicht verfügbar" (*http://goo.gl/IPHGT0*) gerechnet werden.

Alternative: Powershell-Cmdlet Invoke-Gpupdate

Wie bei fast allen Administrationsaufgaben unter Windows 8.x und Server 2012 (R2) gibt es als Alternative zu den GUI-Tools stets eine



Vor dem Update wird der Admin informiert, wie viele Rechner davon betroffen sind.



Das Partitionierungsschema lässt sich in der Datenträgerverwaltung auslesen.

Powershell-Option. Für den GPO-Refresh bringt die neuen Versionen des Betriebssystems das Cmdlet *Invoke-GPUpdate* mit. Wie in den meisten Fällen bietet die Powershell nicht nur mehr Möglichkeiten, den Vorgang durch zusätzliche Schalter genauer zu steuern, sondern ist insgesamt auch flexibler.

Dazu gehört, dass sich *Invoke-GPUpdate* nicht wie der neue Befehl in der Gruppenrichtlinienverwaltung bloß auf bestimmte OUs anwenden lässt. Vielmehr kann ihm eine mehr oder weniger beliebige Liste von Computern übergeben werden, die zuvor über diverse Filter und Kriterien aufbereitet wurde.

Partitionierungsschema auslesen

Neuere PCs sind zumeist nicht mehr mit einem Bios, sondern mit der moderneren Firmware UEFI ausgestattet. Sie bringt ein neues Partitionierungsschema namens GUID Partition Table (GPT), mit dem sich das 2-TB-Limit von MBR überwinden lässt. Gerade unter Windows gibt es einige Zwänge bei der Verwendung von GPT, so dass man wissen muss, nach welchem Schema ein Datenträger aufgeteilt wurde.

Möchte man die Partitionierungsdaten über die grafische Oberfläche auslesen, dann kann man dies in der „Datenträgerverwaltung“ tun. Dieses Vorgehen eignet sich, wenn man Informationen über die lokalen Platten einzelner PCs haben möchte. Die Auskunft über das verwendete Schema findet man im Kontextmenü eines Laufwerks (nicht eines Volumes), und dort unter „Eigenschaften → Volumes“.

Ebenfalls nur den lokalen Rechnern untersuchen kann *diskpart*. Nach dem Aufruf des Kommandozeilenprogramms gibt man *list disk* ein. Die tabellarische Ausgabe dieses Befehls enthält in der rechten Spalte die Überschrift „GPT“. Wird ein Datenträger dort mit einem „*“ markiert, dann wurde er mit GUID Partition Table (GPT) initialisiert.

GPT und MBR über WMI abfragen

Für die Untersuchung mehrerer Rechner, und zwar über Scripts und remote, empfehlen sich WMI oder die neuen Powershell-Cmdlets in Windows 8.x und Server 2012 (R2).

WMI kann man, wie oben schon gezeigt, entweder über das Dienstprogramm *wmic* oder in älteren Windows-Versionen über Powershell nutzen, wo die neuen Storage-Cmdlets noch nicht zur Verfügung stehen.

Um alle lokalen GPT-Laufwerke zu ermitteln, würde man *wmic* zum Beispiel so aufrufen:

```
wmic partition get name, type |
 findstr "GPT"
```

Möchte man damit einen entfernten Rechner untersuchen, gibt man dessen Namen über den Parameter */node* an.

Für WMI-Abfragen existiert in Powershell das Cmdlet *Get-WMIObject* (Alias *gwmi*). Das Äquivalent zum obigen *wmic*-Aufruf würde dort so aussehen:

```
gwmi Win32_DiskPartition | select
 deviceID, @
 {Name="GPT";Expression={$_.Type.
 StartsWith("GPT")}}
```

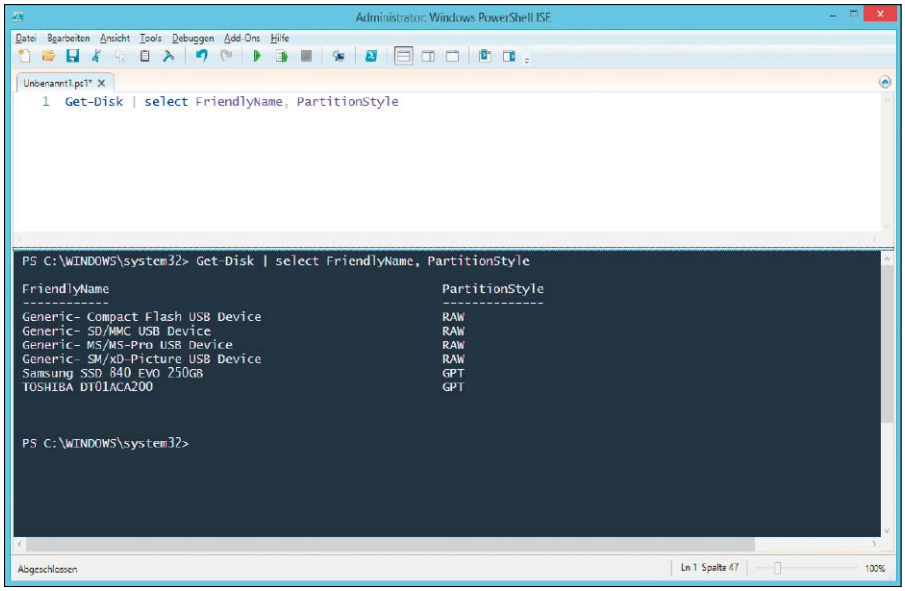
Dieses Kommando verwendet eine Calculated Property, um eine Eigenschaft GPT zu definieren, die ermittelt wird, indem man den Anfang von Type auf die Zeichenkette „GPT“ prüft. Eine Remote-Abfrage ließe sich hier über den Parameter *-Computer* ausführen.

Get-Disk in Windows 8.x

Deutlich einfacher lässt sich die Aufgabe unter Windows 8.x und Server 2012 (R2) lösen:

```
Get-Disk | select FriendlyName,
 PartitionStyle
```

Dieser Aufruf in einer Powershell mit Admin-Rechten zeigt für jedes Laufwerk das Partitionierungsschema an, während alle vorigen Varianten nur GPT ausdrücklich erkennen. MBR ist dort einfach alles, was nicht GPT ist. ■



Das Powershell-Cmdlet Get-Disk liest unter Windows 8.x das Partitionierungsschema aus.

Modern Apps für Administratoren

Mittlerweile gibt es eine Reihe einfacher Tools für die neue Oberfläche Modern UI von Windows. Die meisten anspruchsvollen Management-Werkzeuge laufen aber unter dem herkömmlichen Desktop.

VON WOLFGANG SOMMERGUT

Die Store App für Ping kann die Erreichbarkeit von mehreren Zielrechnern gleichzeitig prüfen.

WIE BEI ALLEN NEUEN SYSTEMEN üblich, erschienen auch für die Touch-Oberfläche von Windows 8.x zuerst relativ triviale Apps sowie einige Referenzprogramme des Plattform-Anbieters. Diese Situation spiegelte sich zunächst auch bei den Tools für Administratoren wider, für die es aber mittlerweile ein Handvoll nützlicher Programme gibt.

Die derzeit verfügbaren Tools stellen durch die Bank keine vollwertige Alternative zu etablierten Desktop-Programmen dar. Und schon gar nicht finden sich irgendwelche Store-Apps, zu denen es kein Gegenstück unter den herkömmlichen Windows-Anwendungen gäbe. Auf einem Windows-8-PC wird man daher wenig Bedarf an diesen Apps der ersten Generation haben. Ihr wesentlicher Nutzen besteht darin, Tablets (mit Windows RT) eine Basisausstattung zu verleihen, so dass man von diesen Geräten aus wenigstens einige administrative Aufgaben erledigen kann.

Weniger Funktionen, aber optimiert für Touch

Die meisten der verfügbaren Tools für die neue Oberfläche fallen in einer der drei folgenden Kategorien:

- kostenlose Clients für gängige Cloud-Dienste und Server-Anwendungen sowie Programme für die Konfiguration von PC-Peripherie und Netzwerkgeräten
- eigenständige Apps mit relativ geringem Funktionsumfang
- kostenlose Programme von Microsoft, die neue Geräte mit Windows 8.x attraktiver machen sollen

Apps für Windows 8.1 kommen in der Regel über den Windows Store, wenn es sich nicht um Eigenentwicklungen handelt, die man über das Sideloading (*http://bit.ly/1dNwB0I*) selbst installieren kann. Daher wird man normalerweise mit der Store-Anwendung nach passenden Apps schauen und sie von dort installieren. Die meisten der hier aufgelisteten Apps sind gratis oder kosten weniger als 10 Euro. Die kostenpflichtigen Anwendungen können in der Regel für einen bestimmten Zeitraum ausprobiert werden.

Ein Schwachpunkt der Store-App ist die integrierte Suche. Zum Teil findet sie manche App nicht einmal dann, wenn sich diese schon länger im Store befinden. Umso schwieriger ist daher die allgemeine Recherche nach einem Programm, um damit ein bestimmtes Problem zu lösen. Daher kommt man oft besser ans Ziel, wenn man in Google mit den Zusatz *site:apps.microsoft.com* nach einer Anwendung sucht. Vor diesem Zusatz geben Sie in Google die Stichwörter ein, nach denen Sie suchen. Die am meisten fortgeschrittenen Anwendungen kommen von Microsoft selbst. Sie sind überwiegend kostenlos, um damit Windows 8.x zu promoten. Zu den bekanntesten gehören die Clients für Mail, Kalender, Skype, Onedrive oder Lync sowie eine neue Implementierung für Onenote. Für IT-Pros besonders interessant sind Remote-Desktop und My Server.

Remote-Desktop & Citrix Xenapp

Bei der App Remote-Desktop (*http://bit.ly/1eT8D9W*) handelt es sich um keine Admin-App im engeren Sinn, aber da das Management von Windows häufig über eine Remote-Desktop-Session erfolgt, kommt sie besonders Admins entgegen. Der RDP-Client für die Touch-Oberfläche unterstützt jedoch nur einen Teil der Funktionen von RDP 8.1. So fehlt etwa die Möglichkeit, lokale Laufwerke und Geräte in die entfernte Session umzuleiten. Die Remote-Desktop-App erlaubt den Aufbau von mehreren gleichzeitigen Verbindungen, wobei sie für jede aktive oder kürzlich genutzte Session einen Thumbnail auf ihrer Startseite ablegt, was diese unübersichtlich machen kann.

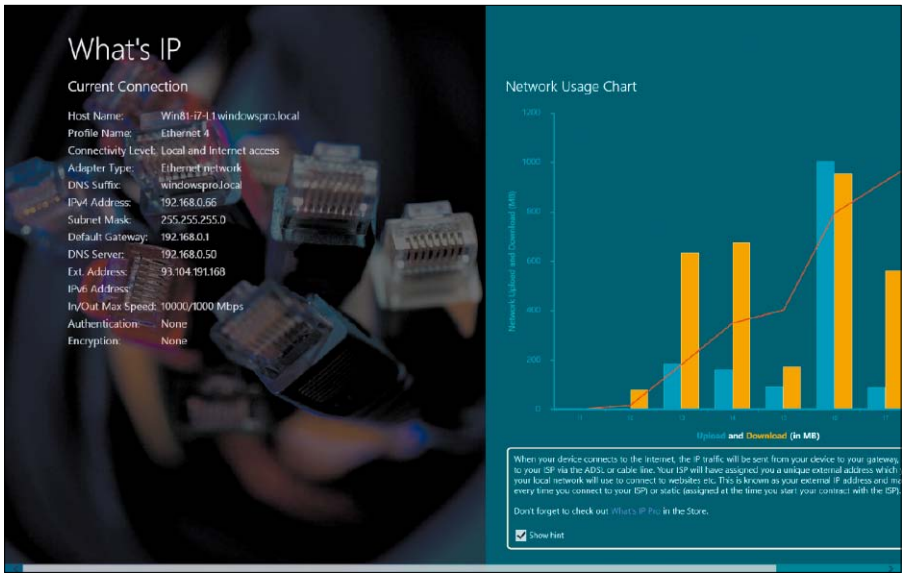
Citrix bietet mit Xenapp Manager (*http://bit.ly/1m6eDM3*) eine kostenlose App an, mit der sich einige administrative Aufgaben erledigen lassen. Dazu zählen das Suchen, Browsen, Trennen und Zurücksetzen von Sessions. Die Software setzt Xenapp 6.5 voraus.
Citrix hat darüber hinaus bereits den Receiver (*http://bit.ly/1l4eYyJ*) als App für Windows 8.x implementiert, so dass man mit seiner Hilfe Xenapp-Sessions öffnen oder auf virtuelle Desktops unter Xendesktop oder VDI-in-a-Box zugreifen kann.

My Server

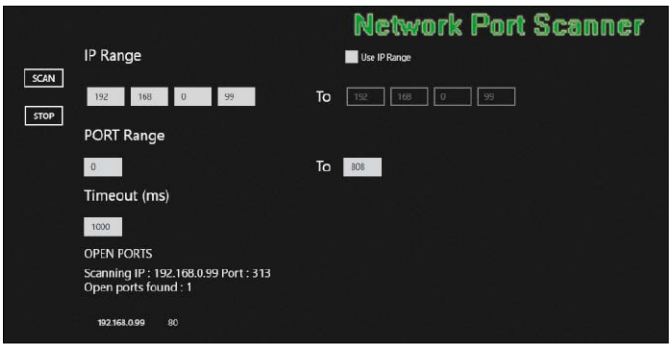
Die App My Server (*http://bit.ly/1l4fnRQ*) dient als Client für Windows Server 2012 (R2) Essentials. Sie ersetzt zum einen das Launchpad für den Desktop, zum anderen bietet es Zugriff auf freigegebene Ordner und unterstützt einige administrative Aufgaben. So zeigt es wichtige Systemmeldungen und Warnungen in einer eigenen Kachel an.
Darüber hinaus kann man die Liste der eingerichteten Benutzer und Geräte öffnen und dort die Passwörter ändern oder Konten deaktivieren. Bei Computer-Konten sieht My Server vor, dass man für Client-Maschinen außerhalb der geplanten Backup-Zyklen eine manuelle Sicherung anstößt.

Einfache Netzwerk-Tools

Eine ganze Reihe simpler Anwendungen dienen dazu, die wichtigsten Netzwerkinformationen darzustellen. Die von ihnen gelieferten Daten entsprechen meist jenen, die man mit dem Befehlszeilen-Tool *ipconfig* ebnfalls erhält, eventuell ergänzt um Traffic-Statistiken. Ein Vorteil der Apps besteht darin, dass sie einige Daten mittels Live Tile anzeigen können, ohne dass man sie dafür extra starten muss. Denn Live Tiles zeigen ihren Inhalt laufend auf der Modern UI an.
In diese Kategorie fallen Network Usage (*http://bit.ly/1dvvzMl*), What's IP (*http://bit.ly/1pyEQTv*) oder das minimalistische IP Address (*http://bit.ly/1jJdPeA*).
Wer nur ein Ping benötigt, kann dieses als eigenständige App haben. Diese heißt ebenfalls Ping und lässt sich im Store über *http://bit.ly/1hs0C74* herunterladen. Anstatt ICMP zu verwenden, misst das Tool die Roundtrip-Zeit einer TCP-Verbindung.
Zu diesem Zweck benötigt die App einen offenen Port, standardmäßig versucht es sich an Kandidaten wie Port 80. Man kann aber explizit einen anderen angeben. Die Software erlaubt das gleichzeitige Ping mehrerer Adressen, wobei die Ergebnisse animiert in grafischer Form dargestellt werden.



What's IP kann man als grafische Alternative zu ipconfig verwenden. Es informiert in einem Balkendiagramm.



Der Network Port Scanner prüft Geräte auf offene Ports. Bei Bedarf kann er dabei einen ganzen Adressbereich untersuchen.

Port- und Netzwerk-Scanner, WOL

Ein einfacher Port- und Netzwerk-Scanner ist Network Port Scanner (*http://bit.ly/1m6g652*). Er erlaubt die Eingabe einzelner IP-Adressen oder eines Adressbereichs, wo er nach offenen Ports suchen soll. Der IP Scanner dient dazu, (unbekannte) Geräte innerhalb eines definierbaren Adressbereichs aufzuspüren. Die vorgegeben Ports kann man ergänzen.
Kostenlose Apps für Wake-on-LAN (WOL) sind Pcwakeup (*http://bit.ly/1l4hpRX*) oder Wake on LAN (http://bit.ly/1l4hpRX). Ersteres erlaubt die Eingabe von IP-oder MAC-Adresse, Zweiteres der MAC-Adresse oder des Gerätenamens. Ansonsten beschränken sich beide auf das Versenden des Magic Packet.

FTP, Telnet und SSH

Ein kostenloser FTP-Client als App für Windows 8.x ist Mftp (*http://bit.ly/1g12m6f*). Er beherrscht die gängigen Funktionen wie den Up- und Download sowie das Löschen und Umbenennen von Dateien. Außerdem kann man damit Verzeichnisse anlegen und Berechtigungen ändern – alles über die Modern UI. Ein Telnet-Client liegt mit >t (*http://bit.ly/1drkFXr*) vor, der beim Start einer Session auf Wunsch gleich ein Script ausführen kann. Einen SSH-Terminal-Emulator gibt es für 1,69 Euro von Devfluid unter *http://bit.ly/1gY25kH*.

Ortung von Geräten

Verlorene oder gestohlene Geräte wiederfinden kann die App Neutracker (*http://bit.ly/1p6kAKP*). Sie macht in Abständen Aufnahmen, wenn eine eingebaute Webcam vorhanden ist, und lädt die Bilder auf Onedrive. Darüber hinaus meldet es den Standort des Geräts. Das funktioniert natürlich nur, solange der Akku Saft hat und das Tablet online ist.

Packer und Komprimierer

Wenn man Archive in diversen Formaten nur entpacken möchte, dann reicht dafür Mzip (*http://bit.ly/1hYbRFQ*). Es kennt ZIP, RAR, 7Z, TAR und TGZ. Dem gleichen Zweck dient Unpacker App (*http://bit.ly/1j3TqlO*), das ebenfalls die gängigsten Formate für Archive unterstützt. Komplette Packer sind die App-Versionen von Winzip (*http://bit.ly/1ha0Q6y*) und 8 Zip (*http://bit.ly/1o1dsSF*). Sie bieten Ähnliches wie ihre Pendants vom Desktop. ■

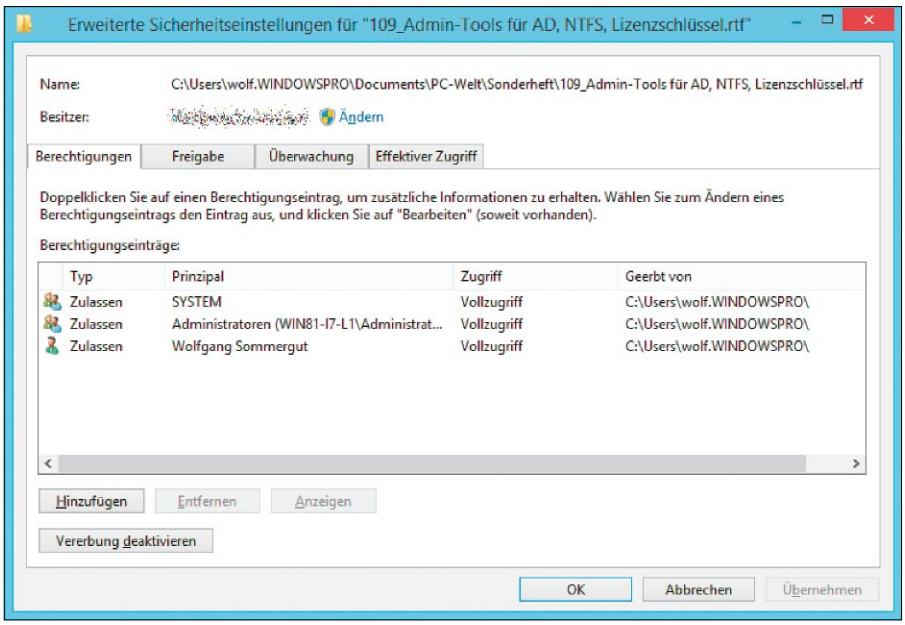
Tools für AD und Storage

Das Management von Zugriffsrechten sowie das Anlegen von Benutzerkonten gehört zum Kerngeschäft der Systemverwaltung. Mehrere kostenlose Tools helfen bei dieser Aufgabe.

VON WOLFGANG SOMMERGUT

DAS MANAGEMENT VON DATEIRECHTEN unter Windows ist relativ kompliziert, weil im Fall von Netzfreigaben die im Dateisystem erteilten Privilegien mit jenen der Shares kombiniert werden. Beide kennen eine Vielzahl von Rechten, die obendrein über Verzeichnisstrukturen vererbt werden können.

Wenn mehrere Administratoren über einen längeren Zeitraum die Verzeichnisrechte auf einem Fileserver pflegen, dann sind daher Inkonsistenzen und zu großzügige Rechte für bestimmte User eine häufige Folge. Der kostenlose NTFS Permissions Reporter (auf Heft-DVD) hilft dabei, den Überblick zu behalten.



Der Windows Explorer liefert nur Rechteinformationen zu einzelnen Dateien und Verzeichnissen.

Verzeichnisrechte anzeigen mit dem NTFS Permissions Reporter

Verschiedene Bordmittel von Windows sind in der Lage, die Rechte von Benutzern und Gruppen für Verzeichnisse zu ermitteln. Dazu zählt der Explorer, der im Kontextmenü eines Verzeichnisses oder einer Datei die vorhandenen Berechtigungen anzeigt. Außerdem stehen mit icacls (*http://bit.ly/1j43Ba5*) und Powershell auch Tools für die Kommandozeile zur Verfügung. Die größte Schwäche dieser Werkzeuge besteht jedoch darin, dass die Informationen entweder über mehrere Orte verstreut sind oder dass die Darstellung unübersichtlich ist.

Hier setzt das Programm NTFS Permission Reporter (*http://bit.ly/1hYgvUv*) an, das schon den Einstieg in die Analyse der Berechtigungen erleichtert. Wenn man den Pfad zu einer Netzfreigabe nicht auswendig weiß, dann bietet das Tool ein Feld zur Eingabe eines Server-Namens, für den es dann alle Shares anzeigt und aus denen man die gewünschten auswählen kann. Insgesamt kann man eine ganze Liste von Verzeichnissen zusammenstellen, bevor man das Reporting startet.

Die Übersicht über die vorhandenen Berechtigungen einer Verzeichnisstruktur, die man als Baum oder als Tabelle darstellen kann, zeigt an, ob die jeweiligen Rechte explizit für dieses Verzeichnis vergeben oder ob sie vererbt wurden. Außerdem offenbart das Tool, wenn Rechte für User oder Gruppen eingetragen sind, die gar nicht mehr existieren.

Die Software liegt in einer Free- und einer Standard Edition vor. Die kostenlose Ausführung liefert vollständige Reports, ihr fehlen aber die Filter- und Exportmöglichkeiten der kostenpflichtigen Version. Diese kann außerdem Berichte zeitgesteuert erstellen und per Mail verschicken.

NTFS Permission Reporter setzt das .NET Framework 4 voraus. Die Free Edition gibt's auf der Website des Entwicklers Chris Wright zum Herunterladen: *http://bit.ly/1hYgvUv*. Die Lizenz der Standard Edition kostet 149 Dollar.

AD-Zugriffsrechte analysieren mit dem AD ACL Scanner

Eine gewissenhafte Verwaltung von Zugriffsrechten ist nicht nur im Dateisystem erforderlich, damit sensible Informationen nicht in die falschen Hände geraten. Mindestens genauso

kritisch ist das Privilegien-Management für einen zentralen Netzwerkdienst wie das Active Directory (AD).

Aufgrund seiner Komplexität wird es bei größeren Installationen nicht nur von einem Admin verwaltet. Aus diesem Grund bietet es die Möglichkeit, bestimmte Aufgaben an verschiedene Benutzer oder Gruppen zu delegieren. Das kann über einen längeren Zeitraum zu einem Rechte-Wildwuchs mit entsprechenden Sicherheitsproblemen führen.

Die Bordmittel von Windows konzentrieren sich vor allem darauf, Privilegien auf bestimmte Objekte zu vergeben. „Active Directory-Benutzer und -Computer" bietet zu diesem Zweck einen eigenen Wizard (Befehl „Objektverwaltung zuweisen"), der AD-Rechte in Form von Aufgaben darstellt und diese in einer verständlichen Form beschreibt.

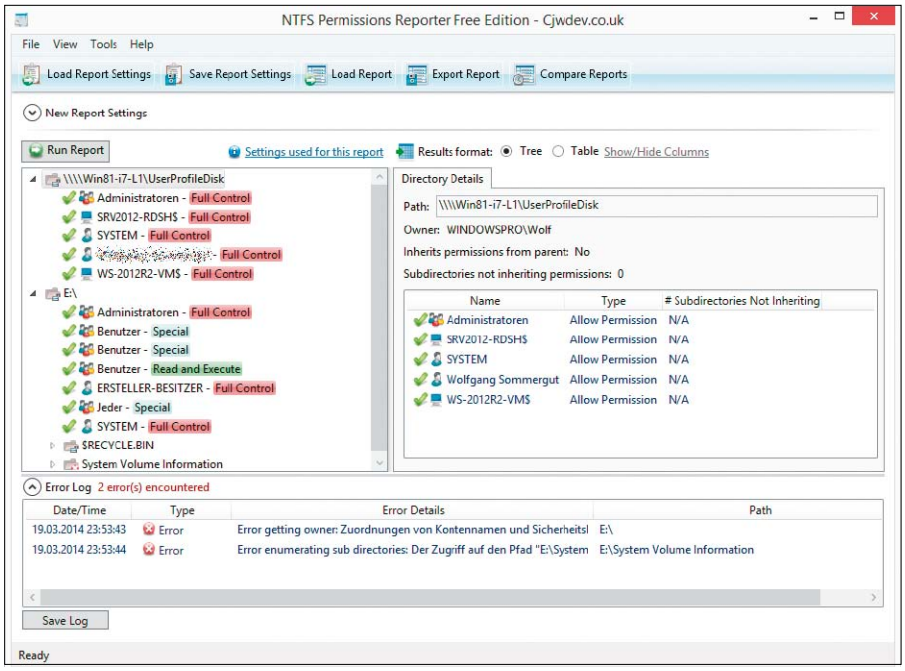
Möchte man dagegen einen Überblick über die Berechtigungsstruktur einer Domäne oder eine OU gewinnen, dann muss man diese Informationen aus den Eigenschaften eines jeden Objekts unter „Sicherheit → Erweitert" separat auslesen.

Diese Aufgabe vereinfachen zahlreiche kommerzielle Reporting-Tools für das Active Directory. Wer keine zu hohen Ansprüche hat, kann auch mit dem kostenlosen AD ACL Scanner (auf Heft-DVD, *http://bit.ly/1o1mWgM*) die wichtigsten Informationen über die vergebenen Rechte auswerten. Er liest alle Berechtigungen aus und zeigt anhand von Reports, wer wo was im AD darf. Dabei sollen mögliche Inkonsistenzen, zu großzügige Privilegien oder verwaiste Einträge aufgespürt werden.

Beispielsweise könnte man der Frage nachgehen, ob bestimmten Benutzern irgendwann Rechte für bestimmte Tätigkeiten zugeteilt wurden, sie aber für diese nicht mehr zuständig sind. Um das AD nicht mit ungültigen Einträgen zu überfrachten, kann man mit diesem Tool nach Berechtigungen für User oder Gruppen suchen, die nicht mehr existieren.

Die Bedienung des AD ACL Scanners ist aufgrund des überschaubaren Funktionsumfangs relativ einfach. Bevor man sich mit einer Domäne verbindet, wählt man aus, ob man nur die Hierarchie der OUs oder alle Objekte sehen möchte. In der angezeigten Struktur markiert man die Ebene, für die man einen Report erzeugen möchte.

Prinzipiell kann man jetzt schon den Scan-Befehl ausführen. In der Regel möchte man aber nicht die zahlreichen Standardrechte für die eingebauten User und Gruppen sehen, weil sie normalerweise keine Probleme darstellen. Diese lassen sich über eine entsprechende Option ausblenden. Zusätzlich bietet das Tool



Die Free Edition des NTFS Permission Reporter ist ein vollwertiges Reporting-Tool für Zugriffsrechte auf Dateien.

einfache Filteroptionen, zum Beispiel um nur explizit verweigerte Rechte anzuzeigen.

Berichte lassen sich im HTML-Format erzeugen oder als CSV-Datei für eine Weiterverarbeitung in Excel oder anderen Programmen exportieren. Die CSV-Option dient auch dazu, gespeicherte Reports mit dem Ist-Zustand des Active Directory zu vergleichen. Auf diese Weise kann man Änderungen in den Active-Directory-Zugriffsrechten nachverfolgen.

Beim AD ACL Scanner handelt es sich um ein Powershell-Script mit einer grafischen Oberfläche. Eine Installation ist daher nicht erforderlich, Voraussetzung ist nur Powershell 2.0. Außerdem muss sichergestellt sein, dass unsignierte Scripts ausgeführt werden dürfen.

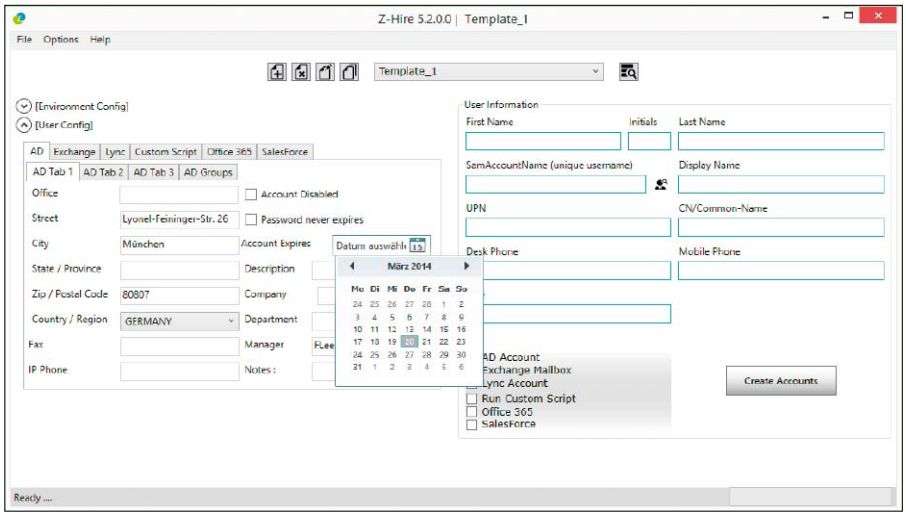
Das Tool wurde vom schwedischen Microsoft-Mitarbeiter Robin Granberg geschrieben. Es kann kostenlos von Microsofts Open-Source-Plattform Codeplex heruntergeladen werden: *http://bit.ly/1o1mWgM*.

Active-Directory-Konten anlegen mit Z-Hire

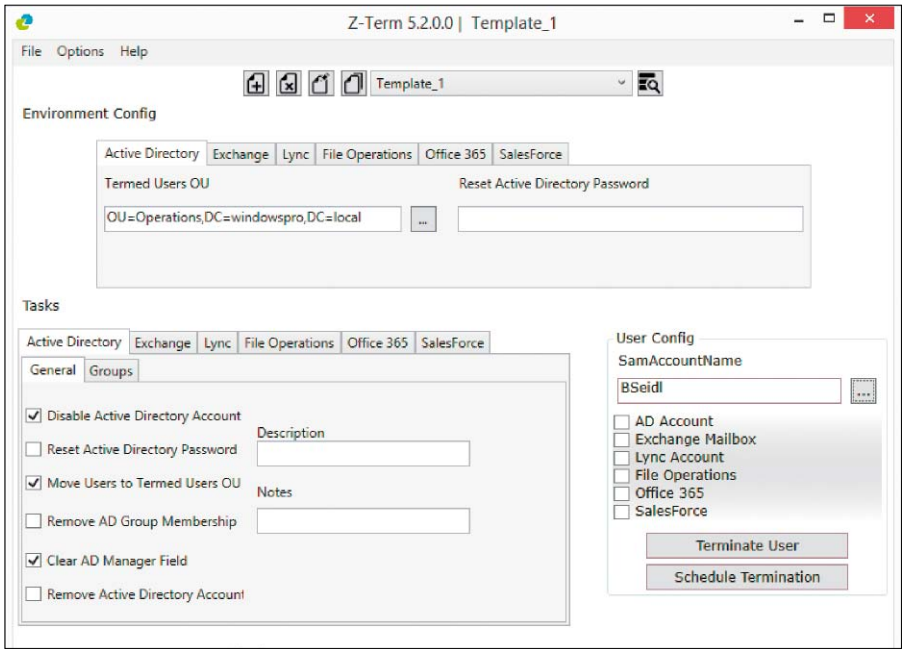
Wenn man häufig neue Mitarbeiter im Active Directory anlegen und zusätzlich ihre Konten für Exchange, Lync oder Office 365 konfigurieren muss, dann kann dies in mühselige Handarbeit ausarten – es sei denn, man automatisiert diese Tätigkeit durch entsprechende Tools. Das kostenlose Z-Hire (*http://bit.ly/1m6no8M*) erspart wiederkehrende Eingaben beim Einrichten neuer User, sein Gegenstück Z-Term (*http://bit.ly/1gYa94S*) hilft dabei, die Konten wieder abzuräumen, wenn ein Mitarbeiter die Firma verlässt. Das wesentliche Feature von Z-Hire zur Rationalisierung der Benutzerverwaltung sind Templates. Sie erlauben es, die wiederkehrenden Informationen für bestimmte User zu speichern und bei Bedarf in einem Rutsch zu laden. So kann man etwa Vorlagen für Abteilungen, Standorte oder OUs anlegen und so das Erstellen neuer Konten für diese Umgebungen beschleunigen.

In einem Template lassen sich unter anderem die Werte für Standort, Adresse, Telefon oder den Vorgesetzten speichern. Außerdem kann das Tool die im AD vorhandenen Sicherheitsgruppen auslesen, so dass man diese auch gleich auswählen und mit den restlichen Informationen speichern kann. Zu den Einstellungen, die sich auch in einer Vorlage hinterlegen lassen, gehören das Standardpasswort sowie dazu gehörige Regeln („muss beim nächsten Login geändert werden", „läuft nie ab").

Nach dem gleichen Muster kann man Templates für Exchange-, Lync- und Office-365-Konten erstellen, wobei sich die Einstellungsmöglichkeiten dort natürlich an den Eigenheiten dieser Systeme orientieren. So sehen Vorlagen für Exchange vor, dass man dort die Datenbank für die Mailbox, Activesync-Policies, Quotas oder zusätzliche SMTP-Server eintragen kann. Die früheren Versionen von Z-Hire waren auf maximal sechs Templates beschränkt, die in größeren Umgebungen jedoch nicht ausreichen. Mit der Version 5 legt das Tool hier keine Grenzen mehr fest. Außerdem enthält es einen Passwort-Generator, mit dem man ein Kennwort für die erste Anmeldung vorgeben kann.



Mit Templates automatisiert Z-Hire beim Anlegen neuer Benutzerkonten die Eingabe von wiederkehrenden Infos.



Z-Term rationalisiert als Gegenspieler von Z-Hire das Deaktivieren von nicht mehr benötigten Benutzerkonten.

Neu ist zudem die Möglichkeit, ein Ablaufdatum für Konten im Template zu speichern. Darüber hinaus kann Z-Hire eine Zusammenfassung der Benutzerdaten generieren, die sich in sich über Copy & Paste in Dokumente übernehmen lässt.

Z-Term zur Deaktivierung von Konten

Der Gegenspieler von Z-Hire heißt Z-Term und dient erwartungsgemäß dazu, Konten zu deaktivieren, wenn Mitarbeiter das Unternehmen verlassen. Es kann für AD-Accounts Passwörter zurücksetzen, die Mitgliedschaft in bestimmten Gruppen beenden, deaktivierte User in eine eigens dafür vorgesehene OU verschieben oder das Manager-Feld löschen.

Nützlich ist zudem die Möglichkeit, das Home-Verzeichnis, das sich in Z-Hire konfigurieren und auf einen bestimmten Laufwerksbuchstaben festlegen lässt, mit Z-Term an einen bestimmten Speicherort zu verschieben. Bei Exchange-Konten besteht zudem die Option, Mailboxen als PST-Dateien zu exportieren, eine Out-of-Office-Nachricht zu bestimmen und ein Konto zu benennen, an das alle Nachrichten weitergeleitet werden sollen.

Z-Term arbeitet wie Z-Hire auf Basis von Templates, in denen man die Einstellungen für das Deaktivieren von Konten speichern kann. Dazu zählen etwa die OU, in die solche User standardmäßig verschoben werden, oder der Pfad, an dem die Heimatverzeichnisse oder die PST-Dateien abgelegt werden sollen.

Z-Hire und Z-Term sind kostenlose Programme, die von Microsofts Technet Gallery heruntergeladen werden können. Der Download unter *http://bit.ly/1m6no8M* in Form eines ZIP-Archivs enthält beide Programme. Sie erfordern keine Installation und lassen sich nach dem Entpacken direkt ausführen.

Kostenlose Partitionierungs-Tools

Die Entwicklung des legendären Partition Magic wurde 2010 von Symantec eingestellt, und die auf vielen Download-Sites noch verfügbare Version 8 eignet sich nicht für Windows-Versionen nach XP. Die Lücke füllen einige Anbieter auch mit Gratis-Tools, die sich jedoch beim Funktionsumfang erheblich unterscheiden.

Das von Powerquest entwickelte Partition Magic machte in den 90er-Jahren Furore, weil man damit die Partitionen aus einer benutzerfreundlichen grafischen Oberfläche fast nach Belieben vergrößern, verkleinern oder verschieben konnte. Die Betriebssysteme boten damals keine Möglichkeit, die Partitionierung von Laufwerken ohne Datenverlust zu ändern. Mittlerweile können die Bordmittel von Windows die wichtigsten Aufgaben bei der Verwaltung von Partitionen selbst übernehmen. Dazu gehören das Vergrößern und Verkleinern sowie die Konvertierung von Dateisystemen. Einzelne Funktionen für das Diskmanagement sind jedoch so rudimentär, dass etwa die Konvertierung zwischen MBR und GPT das Löschen und das erneute Anlegen aller Partitionen erfordert. Daher besteht weiterhin Bedarf an Tools, die mehr leisten als die Windows-eigenen Basisfunktionen. Zu den fortgeschritten Features zählen unter anderem das Verschieben, Zusammenführen oder Teilen von Partitionen, außerdem wäre eine Konvertierung zwischen MBR und GPT ohne Datenverluste wünschenswert. Auch scheinbar einfache Aufgaben wie die Umwandlung von logischen in primäre Partitionen und vice versa bleibt solchen Werkzeugen überlassen, weil Windows das nicht selbst kann.

Easeus Partition Master

Ein populäres Tool mit einem großen Funktionsumfang ist Easeus Partition Master (auf Heft-DVD, *http://www.easeus.com*). Es liegt in Ausführungen für Workstation und Server vor, wobei von der PC-Variante auch eine Free Edition existiert. Sie ist allerdings auf den Gebrauch durch private Anwender beschränkt. Ein weiteres Limit besteht darin, dass sie die Größe von Volumes auf dynamischen Datenträgern nicht ändert. Ansonsten bietet es alle wesentlichen Features eines vollwertigen Diskmanagers, darunter das Zusammenführen

und Verschieben von Partitionen, die Konvertierung von dynamischen in Basisdatenträger oder das Kopieren von Partitionen und Laufwerken auf andere Disks. Hinzu kommt die Möglichkeit, gelöschte Partitionen wiederherzustellen. Neben den unmittelbaren Funktionen für das Management von Partitionen bietet Easeus noch solche für das sichere Löschen von Daten oder zur Wiederherstellung des Master Boot Record (MBR). Neben den Dateisystemen von Windows unterstützt es auch solche von Linux, so dass es unter Windows Partitionen mit Ext2 und Ext3 formatieren, löschen oder wiederherstellen kann.

Bei der Installation des Tools ist darauf zu achten, dass es nebenbei eine Vielzahl von Crapware aufspielen möchte. Dies lässt sich durch die Abwahl der entsprechenden Optionen verhindern. Benötigt man die Software nur kurzfristig, dann kann man auf die Trial-Version ausweichen, die keinen solchen unterwünschten Code auf die Platte spülen möchte.

Minitool Partition Wizard

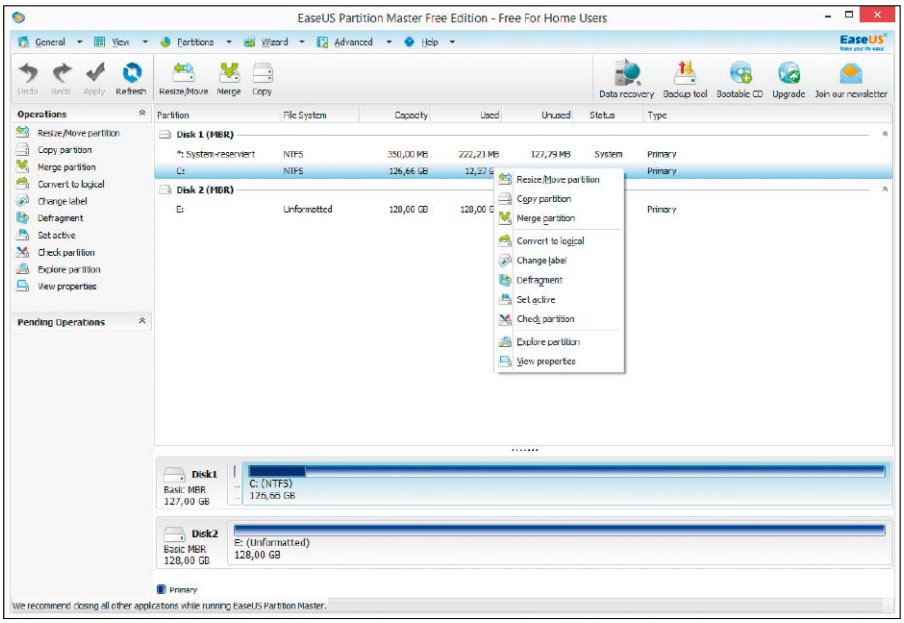
Dieser Hersteller verfolgt einen ganz ähnlichen Ansatz wie Easeus, indem er seine Software kostenlos für den privaten Gebrauch zur Verfügung stellt (auf Heft-DVD, *http://www.partitionwizard.com*). Die Professional Edition für den Einsatz in Unternehmen kostet in einer Einzellizenz moderate 39 Dollar.

Auch in Hinblick auf den Funktionsumfang gibt es eine weitgehende Überschneidung mit Easeus. Allerdings eignet sich Partition Wizard zusätzlich für ein paar Aufgaben, die der Partition Master nicht schafft.

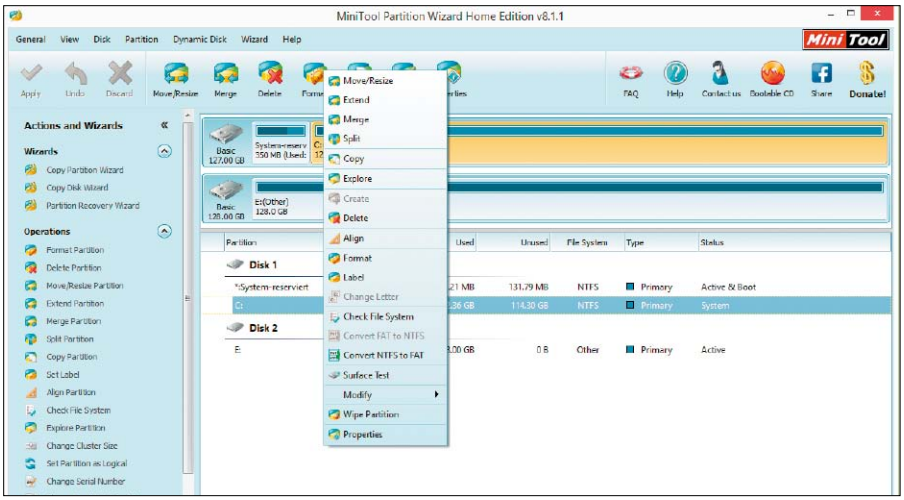
Dazu gehört die verlustfreie Konvertierung von Laufwerken zwischen MBR und GPT oder von Volumes zwischen NTFS und FAT in beiden Richtungen. Es kann bestehende Partitionen in einem Durchgang teilen, eine Funktion, die auch Easeus für sich reklamiert, die sich aber zumindest in der Free Edition nicht finden lässt. Minitool unterstützt ebenfalls Linux-Dateisysteme, und zwar im Gegensatz zu Easeus auch Ext4.

Paragon Partition Manager Free

Paragon (*www.paragon-software.de*) vertreibt mit der Harddisk Manager Suite ein mächtiges Tool für die Verwaltung von Disks und Partitionen, die einen ähnlichen Funktionsumfang bietet wie die beiden oben genannten Produkte. Einen kleinen Teil davon koppelt der Hersteller in Partition Manager Free (auf Heft-DVD) aus, das ebenfalls auf die private Nutzung beschränkt ist. Die kostenlose Ausführung eignet sich für einfache Aufgaben wie das Anlegen, Vergrößern, Verkleinern und Löschen von Partitionen. Zusätzlich ist es in der Lage, das Dateisystem von Volumes zwischen NTFS, FAT32 und Apples HFS zu konvertieren. Die wenigen Features benötigen nicht unbedingt die Benutzeroberfläche der Vollversion. Daher öffnet das Tool standardmäßig eine GUI nach dem Vorbild der Startseite von Windows 8, die für jede Funktion eine eigene Kachel bereitstellt. ■



Easeus Partition Master ist ein mächtiges Tool fürs Diskmanagement, das für die private Nutzung kostenlos ist.



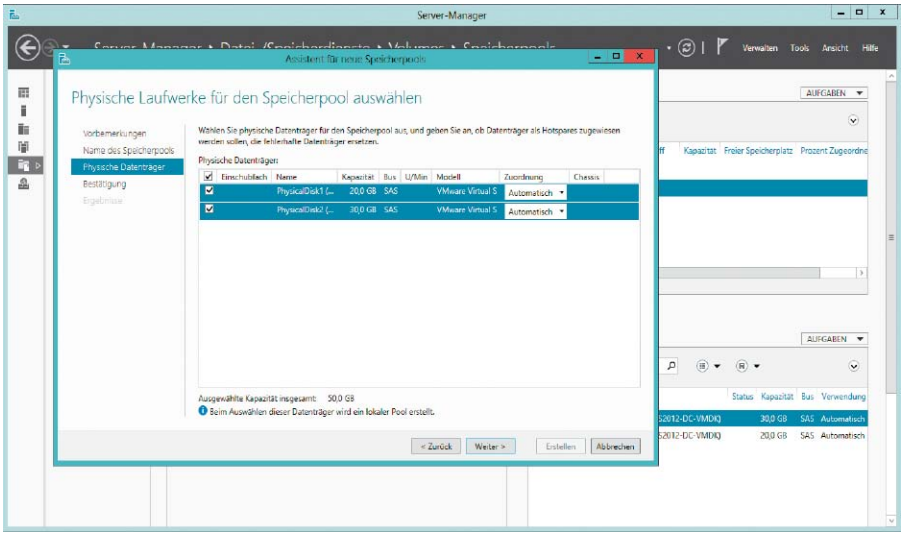
Das vielseitige Programm Minitool Partition Wizard konvertiert verlustfrei zwischen MBR und GPT.

Die kostenlose Version von Paragon Partition Manager bietet einen überschaubaren Funktionsumfang, der sich über eine Kacheloberfläche im Windows-8-Stil abrufen lässt.

Neu in Windows Server 2012 R2

Parallel zu Windows 8.1 veröffentlicht Microsoft das Release 2 von Windows Server 2012. Es bringt wesentliche Neuerungen bei Storage, Networking und der Automatisierung des Server-Managements.

VON WOLFGANG SOMMERGUT



Die mit Windows Server 2012 neuen „Speicherplätze“ richten virtuelle Volumes auf Basis von Laufwerk-Pools ein.

DIE KÜRZEREN RELEASE-ZYKLEN erlauben Microsoft eine schnellere Entwicklung jener Features, die im Wettbewerb mit anderen Herstellern besonders wichtig sind und wo Windows Server noch Nachholbedarf hat.
Das gilt vor allem für den Hypervisor, der in Server 2012 R2 eine ganze Reihe von Verbesserungen erhält, oder bei Storage, das durch die Virtualisierung dramatische Veränderungen erlebt.

Auto-Tiering für Storage Spaces

Eine dieser Neuerungen beim Storage-Management ist das Auto-Tiering für „Speicherplätze“ (*http://bit.ly/OXbkM7*), die mit Windows Server 2012 eingeführt wurden. Sie dienen dazu, SATA- oder SAS-Disks (Serial Attached SCSI) zu Pools zusammenzufassen, auf denen sie virtuelle Volumes einrichten und für die sie Funktionen wie Thin Provisioning oder Mirroring bereitstellen.
Windows Server 2012 R2 erlaubt die Einrichtung von Storage Spaces, die sowohl Plattenlaufwerke als auch SSDs umspannen. Das System analysiert in regelmäßigen Abständen die Nutzung der darauf gespeicherten Daten und verlagert sie nach Bedarf auf die schnelleren oder langsameren Speichermedien. Administratoren können aber eigene Prioritäten setzen, indem sie Dateien explizit einem bestimmten Storage-Tier zuordnen.
Der schnellere Storage-Tier wird zudem für das Caching von Schreiboperationen genutzt, wenn beispielsweise virtuelle Festplatten (VHDs) auf einem Storage Space liegen. Falls die Zugriffsmuster nicht erfordern, dass ein solches virtuelles Laufwerk dauerhaft auf einem SSD platziert wird, dann schichtet es das Auto-Tiering später automatisch auf ein langsameres Medium um.
Eine weitere Storage-Neuerung wertet Windows Server auf, wenn man ihn als blockorientiertes Speichersystem einsetzen möchte. Das integrierte iSCSI-Target nutzt unter Server 2012 für die Bereitstellung von iSCSI LUNs noch virtuelle Laufwerke im alten VHD-Format, so dass die maximale Größe 2 TB pro LUN beträgt. Windows Server 2012 R2 setzt dafür das neue VHDX ein, wodurch die Beschränkung der Kapazität auf 64 TB steigt.

File-Synchronisierung mit Work Folders

Eine andere Neuerung erweitert die Fileserver-Rolle um sogenannte Sync Shares. Dateien, die dort gespeichert werden, repliziert Server 2012 R2 auf die Clients von berechtigten Benutzern. Ausgewählte Verzeichnisse lassen sich gleichzeitig als normale SMB-Shares freigeben und als Work Folders definieren. Man kann sie dann wie gewohnt als Netzlaufwerke nutzen, deren Inhalt den Clients aber auch offline zur Verfügung steht.
Microsoft reagiert mit der neuen Synchronisierungsfunktion darauf, dass Benutzer immer häufiger über mehrere Endgeräte verfügen und diese verstärkt mobil nutzen. Ein Fileserver, der nur vom Desktop-PC über das Firmen-LAN erreichbar ist, verwandelt sich nicht nur in das viel zitierte Datengrab, sondern provo-

ziert auch den unautorisierten Einsatz von Consumer-Tools wie Dropbox, um ein flexibleres Arbeiten zu ermöglichen.

Wie andere Anbieter von Synchronisierungs-Tools (etwa Enterprise-Dropbox, weitere Informationen über *http://bit.ly/1hwhYQq*) verzichtet Microsoft auf die Replizierung von Daten in die Cloud und grenzt das Server-Feature daher explizit von Onedrive for Business (*http://bit.ly/1j7PVuF*) ab. Work Folders übertragen die Dateien in verschlüsselter Form, zudem lassen sich Berechtigungen zentral verwalten. Im Prinzip handelt es sich dabei um den überfälligen Nachfolger der Offline-Dateien. Weitere Infos dazu gibt's über *http://bit.ly/1l6JMil*.

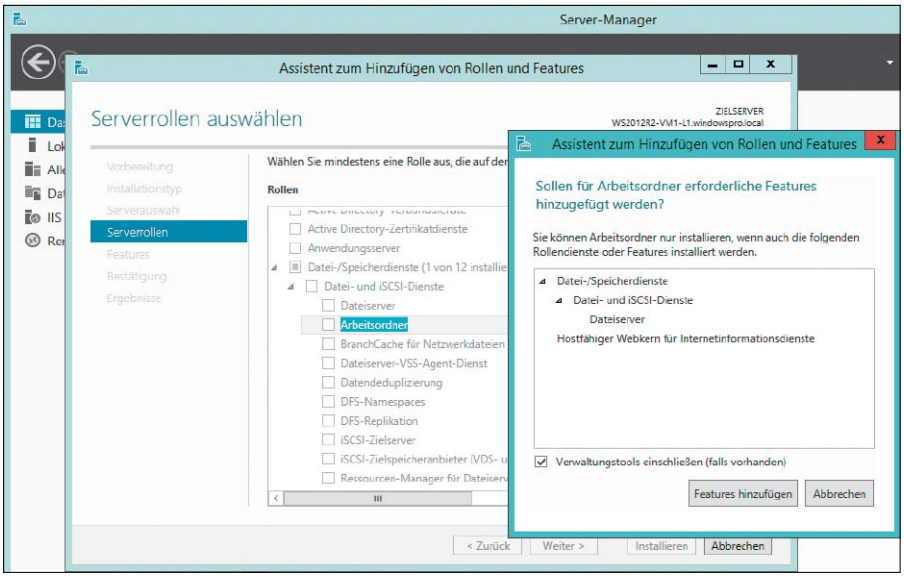
In Zeiten heterogener mobiler Endgeräte hängt der Nutzen von solchen Synchronisierungs-Tools wesentlich davon ab, welche Clients sie unterstützen. Für das erste Release beschränkt sich der Support auf Windows, wobei auch ältere Versionen wie Windows 7 berücksichtigt werden. Microsoft kündigte aber an, künftig auch andere Plattformen wie Mac-OS, iOS oder Android zu berücksichtigen.

Powershell 4.0 mit Desired State Configuration

Powershell wurde bereits in Windows 8 und Server 2012 als Tool zur Automatisierung der Systemverwaltung deutlich aufgewertet, indem Hunderte neue Cmdlets das Scripting weiterer Komponenten ermöglichen. Windows Server 2012 R2 erhält eine Reihe weiterer Cmdlets, darunter solche für das Management von VPNs, des Startbildschirms oder des Trusted Platform Module (TPM).

Die einzige größere Änderung in der Sprache, die den Versionssprung auf Powershell 4.0 rechtfertigt, ist die Einführung einer deklarativen Syntax. Sie dient dazu, die Konfiguration eines Servers zu beschreiben, also in erster Linie, welche Rollen und Features aktiviert werden und welche Einstellungen sie erhalten sollen. Grundsätzlich ließe sich dieses Ziel auch über die imperativen Sprachmittel in Powershell 3.0 erreichen, aber die neuen Spracherweiterungen in der Version 4 erleichterten diese Aufgabe deutlich.

Diese „Desired State Configuration" lässt sich nicht nur nutzen, um einen frischen Windows-Server für den geplanten Einsatz in einem Aufwasch einzurichten. Vielmehr realisiert sie auch das Konzept des „kontinuierlichen Deployments", so dass Server regelmäßig auf Abweichungen von der gewünschten Konfiguration (Configuration Drift) geprüft und bei Bedarf auf diese zurückgesetzt werden können. Einen Überblicksbeitrag zum Thema gibt es über *http://bit.ly/1iDeRcF*.



Arbeitsordner erweitern die Dateidienste und erlauben die Synchronisierung auch auf Nicht-Windows-Clients.

Neuerungen in den Remote Desktop Services

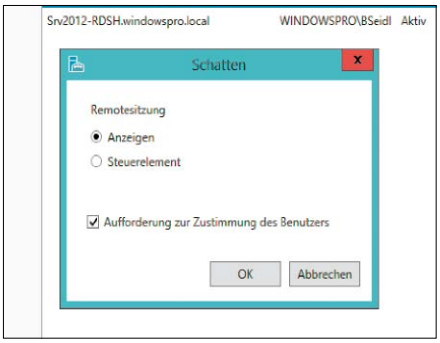
Die weitreichende Umstellung des RDS-Managements in Windows Server 2012 bewirkte auch Veränderungen, die einige Anwender nicht unbedingt als Fortschritt wahrnehmen. Dazu zählen der Wegfall von Session Shadowing und der Zwang, dass Session Hosts Mitglied in einer AD-Domäne sein müssen.

Windows Server 2012 R2 korrigiert nun einige dieser zweifelhaften Fortschritte. Zum einen ist das Spiegeln von Sitzungen künftig wieder möglich, so dass sich ein Administrator auf die Session eines Users aufschalten kann.

Zum anderen können die RDS zwar weiterhin nicht in einer Workgroup eingerichtet werden, aber dafür unterstützt Microsoft zumindest wieder die gemeinsame Installation der AD-Verzeichnisdienste und des RD Connection Broker auf einem Server. Diese Konfiguration vereinfacht das Deployment in kleinen Umgebungen, etwa in Außenstellen.

Eine weitere Erleichterung bei der Einrichtung der RDS besteht darin, dass ein direktes Update von Server 2012 auf das Release 2 möglich ist (In-Place-Update). Schließlich erhält das RD Gateway eine Plug-in-Schnittstelle für Module zur User-Authentifizierung, um mehr Flexibilität bei der Anmeldung von Benutzern aus dem Internet zu bieten.

Einige Verbesserungen der Remote Desktop Services gehen auf die Weiterentwicklung von RDP und Remote FX zurück. So soll der Bandbreitenverbrauch beim Media-Streaming über Remote FX um 50 Prozent geringer sein als unter Server 2012. Überarbeitete Codecs reduzieren laut Microsoft die Netzwerkbelastung auch für Nicht-Video-Inhalte, hinzu kommen



Die Remote Desktop Services von Windows Server 2012 R2 führen das Session Shadowing wieder ein, mit dem man sich auf eine Sitzung aufschalten kann.

Möglichkeiten, das Decodieren der Daten an spezifische H.264-Hardware zu delegieren.

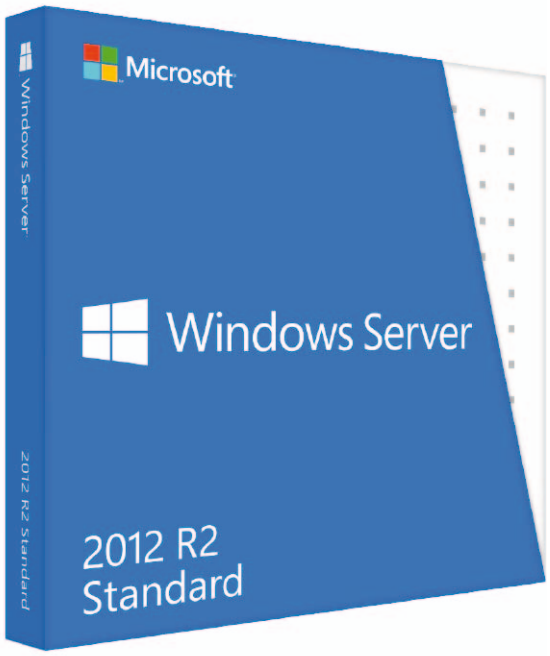
Die erst mit Windows Server 2008 eingeführte Option, einzelne entfernte Anwendungen als Remote App nahtlos in den lokalen Desktop zu integrieren, wird in puncto Benutzererlebnis aufgewertet. Sie reagieren nun wie lokale Programme auf die Änderung der Desktop-Auflösung und auf Aero Peek, sie sind in der Thumbnail-Vorschau der Taskleiste zu sehen und sollen insgesamt mit weniger Verzögerung auf das Vergrößern oder Verkleinern der Fensters ansprechen.

Zu den weiteren Neuerungen für die Remote Desktop Services zählen die Unterstützung für transparente Fenster oder Ränder wie in Office 2013 sowie „Quick Reconnect". Dieses stellt eine Verbindung mit einer Session oder einem zentralen Desktop, die etwa durch Netzwerkprobleme unterbrochen wurde, in weniger als zehn Sekunden wieder her, während dieser Vorgang bisher über eine Minute in Anspruch nehmen konnte. ■

Server-Editionen: Lizenzen & CALs

Microsoft hat bei der Einführung von Windows Server 2012 R2 überraschend ganz schön an der Preisschraube gedreht. Es gibt aber auch gute Nachrichten.

VON WOLFGANG SOMMERGUT



Windows Server 2012 R2 gibt es in vier Editionen, wobei Standard und Datacenter die zwei wichtigsten Varianten sind.

BEI DEN LIZENZBEDINGUNGEN von Windows Server 2012 R2 steht einer saftigen Preiserhöhung für die Datacenter Edition eine liberale Regelung bei den CALs gegenüber. Neu ist Server and Cloud Enrollment im Rahmen von Enterprise Agreements, das Rabatte und zusätzliche Rechte bei der Nutzung von Azure einräumt. Nachdem Microsoft die Lizenzierung von Windows Server anlässlich der Version 2012 neu geregelt (*http://bit.ly/1dQbFGc*) und die Zahl der Editionen eingedampft hatte, war beim Release 2 nicht erneut mit tiefgreifenden Änderungen zu rechnen. Tatsächlich bleibt die Aufteilung in vier Editionen gleich, aber dafür ändern sich das Preisgefüge und einige Nutzungsrechte.

Datacenter Edition und Essentials werden teurer

Am auffälligsten ist die Preiserhöhung von circa 30 Prozent für die Datacenter Edition. In Server 2012 belief sich eine Lizenz auf 4809 Dollar, beim Release 2 sind es dagegen 6155 Dollar. Teurer wird auch Windows Server 2012 R2 Essentials, dessen Preis von 425 Dollar auf 501 Dollar steigt. Unverändert bleiben indes die Konditionen für die Standard Edition.

Die wesentlichen Lizenzbedingungen für die Editionen Standard und Datacenter lauten:

- Beide Editionen haben den genau gleichen Funktionsumfang
- Lizenzen sind grundsätzlich an physikalische Server gebunden
- eine Lizenz deckt zwei Prozessoren ab, unabhängig von der Zahl der Kerne
- Lizenzen können nicht auf mehrere Rechner aufgeteilt werden, beispielsweise eine Lizenz auf zwei Server mit je einer CPU
- Eine Lizenz der Standard Edition erlaubt die Ausführung von bis zu zwei Instanzen von Windows Server in virtuellen Maschinen (im Microsoft-Jargon „Virtual Operating System Environments“ genannt, VOSEs)
- Die Datacenter Edition lässt unbegrenzt viele VOSEs zu

Bei der Entscheidung zwischen Standard und Datacenter kommt es ausschließlich darauf an, wie viele Instanzen des Betriebssystems in VMs auf einem Server ausgeführt werden sollen. Trotz der Bindung von Lizenzen an die Hardware dürfen VOSEs etwa mittels Live Migration auf einen anderen Hyper-V-Host umziehen. Allerdings wandert die Lizenz nicht mit, so dass der Ziel-Server für die Ausführung aller VMs voll lizenziert werden muss.

Kalkulation für Standard versus Datacenter

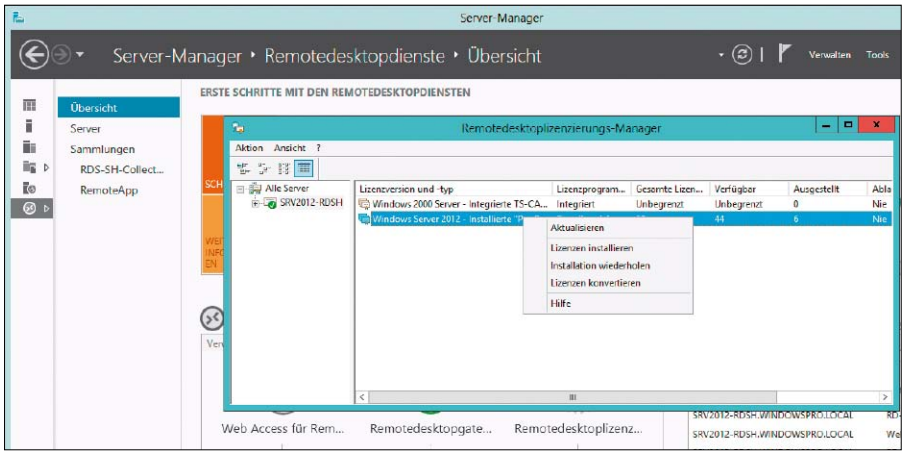
Aufgrund der kräftigen Preiserhöhung für die Datacenter Edition ändert sich nun die Formel für die Kalkulation, ab wann es günstiger ist, die große Ausführung zu kaufen. Bisher galt abhängig vom gewählten Lizenzprogramm die Regel, dass sich ab ungefähr 12 VOSEs für zwei Prozessoren die Anschaffung der Datacenter Edition rechnet. Denn für 12 VMs mit Windows Server benötigt man sechs Lizenzen der Standard Edition, auch wenn die Maschine nur zwei Sockel hat. Ausschlaggebend ist hier das Limit von zwei VOSEs pro Lizenz.

Beim neuen Preisgefüge dagegen ist die Datacenter Edition circa sieben Mal so teuer wie die Standard Edition. Daher wird erst bei 14 VOSEs pro Lizenz der Punkt erreicht, an dem alle benötigten Lizenzen der Standard Edition zusammen gleich viel kosten wie eine Datacenter Edition. Microsoft rechtfertigt die kräftige Preiserhöhung mit den zahlreichen neuen Funktionen in Hyper-V 2012 R2. Infos gibt's dazu in einer FAQ (Download als PDF über

Edition	Feature comparison	Licensing model	Server Pricing*
Datacenter	Unlimited virtual OSE All features	Processor + CAL**	$6,155
Standard	Two virtual OSE All features	Processor + CAL**	$882
Essentials	2 processor One OSE Limited features	Server 25 user limit	$501
Foundation	1 processor Limited features	Server 15 user limit	OEM Only

OSE: Operating System Environment

Im Vergleich zu Windows Server 2012 zieht der Preis der Datacenter Edition von Release 2 deutlich an.



Terminaldienste erfordern zusätzliche CALs, zu deren Verwaltung man einen eigenen Lizenz-Server installieren muss.

http://bit.ly/1bm96xp). Diese sind jedoch nicht der Datacenter Edition vorbehalten, vielmehr kommen alle Ausführungen in ihren Genuss. Wahrscheinlicher ist es wohl, dass Microsoft aufgrund der typischen Nutzungsmuster von Server 2012 errechnet hat, wie weit es die Preisdifferenz zwischen den Editionen dehnen kann, um höhere Einnahmen zu erzielen.

Neue Virtualisierungsrechte für Essentials

Bei den Editionen für kleinere Firmen bleibt es wie bisher bei Windows Server Essentials und Foundation. Beide sind in ihrem Funktionsumfang und der Zahl der möglichen User (25 bei Essentials, 15 bei Foundation) eingeschränkt. Windows Server 2012 R2 Foundation richtet sich zudem nur an OEMs, die das System auf ihrer Hardware vorinstallieren und dann an ihre Kunden verkaufen.

Bei Windows Server 2012 R2 Essentials erhöht sich nicht nur der Preis pro Lizenz, zusätzlich ändern sich auch die Nutzungsrechte. Bisher war diese Edition nur für die Installation auf physikalischer Hardware ausgelegt, auch wenn es keine lizenzrechtlichen Hindernisse für die Ausführung in einer VM gab.

Das Release 2 des Servers unterstützt nun explizit die Installation in einer virtuellen Maschine, indem Hyper-V nun zu seinem Lieferumfang gehört und ein gemeinsames Setup das gesamte System einrichtet. Nachdem die Installation in der Parent Partition technischen und lizenzrechtlichen Einschränkungen unterliegt, darf eine weitere Kopie des Betriebssystems als VOSE eingerichtet werden.

Die bisher exklusiven Funktionen von Windows Server Essentials, darunter ein Backup für die angeschlossenen Clients oder Remote-Webzugriff, sind nun als eigene Rolle in den Editionen Standard und Datacenter enthalten und werden dort Essentials Experience genannt. Infos dazu finden Sie über *http://bit.ly/OXrlli* und direkt bei Microsoft über *http://bit.ly/1gZUL8n*). Als solche ist sie ein Feature dieser größeren Ausführungen und damit über deren Lizenz abgedeckt.

CALs für Windows Server, RDS und RMS

Für die Nutzung von Diensten auf einem Windows Server sind bekanntlich Client Access Licenses (CALs) erforderlich (Ausnahme: Essentials und Foundation). Grundsätzlich gilt die Regel, dass für jeden Benutzer oder jedes Gerät eine CAL zu erwerben ist, wenn er beziehungsweise es direkt oder indirekt auf eine Server-Software zugreift. Dabei ist zu berücksichtigen, dass die CAL in einer gemischten Umgebung für die neueste verwendete Version der Server-Komponente gültig sein muss. Windows Server 2012 R2 benötigt indes keine neue CAL-Version, es reicht jene für Server 2012.

Zusätzlich kompliziert wird Microsofts Lizenzmodell dadurch, dass einzelne Features von Windows Server eigene CALs erfordern, etwa die Remote Desktop Services oder die Rights Management Services, während andere wie die Authentifizierung über das AD mit einer CAL für das Betriebssystem abgedeckt sind. Die relativ liberale Regelung, wonach CALs von Windows Server 2012 auch für R2 weiterverwendet werden dürfen, gilt auch für die Remote Desktop Services und die Rights Management Services.

Dem RDS-Lizenzdatenblatt (Download als PDF über *http://bit.ly/1eU4EYN*) zufolge berechtigen RDS-CALs nun auch dazu, auf Sessions auf Microsofts Cloud-Service Azure zuzugreifen. Eine bisher vorgeschriebene zusätzliche Subscriber Access License ist dafür nicht mehr nötig, allerdings wird vorausgesetzt, dass man über eine aktive Software Assurance verfügt.

Es gibt nicht nur Szenarien wie RDS, die zusätzliche CALs erfordern, sondern auch einige, für die man gar keine braucht. Das trifft zum Beispiel auf Windows Server zu, wenn er ausschließlich als öffentlich zugänglicher Webserver im Internet verwendet wird. Sobald sich die Benutzer in irgendeiner Form gegenüber der Webanwendung identifizieren müssen, dann brauchen sie eine CAL oder einen externen Connector.

Eine Ausnahme vom CAL-Zwang gibt es auch für Administratoren. Jede Server-Software erlaubt den Zugriff von bis zu zwei Geräten oder Benutzern für rein administrative Aufgaben. Erledigt der Systemverwalter nebenbei auch andere Tätigkeiten, wie das Abrufen von Mails, dann sind auch für ihn Client-Lizenzen nötig.

Server and Cloud Enrollment für Enterprise Agreement

Seit der Freigabe von Windows Server 2012 R2 bietet Microsoft seinen Kunden eine weitere Möglichkeit an, um Infrastruktur-Software sowie Cloud-Dienste von Azure zu erwerben. Es handelt sich dabei um Server and Cloud Enrollment (SCE), das sich an Kunden mit Enterprise Agreement richtet. Ziel dieses Programms ist eine unternehmensweite Festlegung von Anwendern auf bestimmte Microsoft-Produkte für einen Zeitraum von drei Jahren.

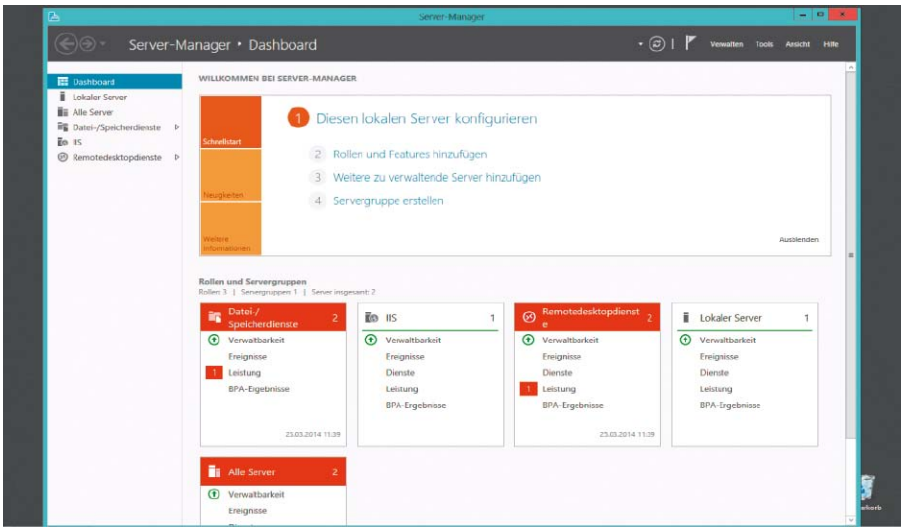
Das Angebot besteht aus den vier Komponenten Core Infrastructure, Application Platform, Developer Platform und Windows Azure. Entscheidet man sich für eine der ersten drei, dann erhält man als Kunde bestmögliche Konditionen für Azure.

Zu den weiteren Vorteilen von Server and Cloud Enrollment (SCE) zählen laut Microsoft Preisnachlässe für Lizenzen und Software Assurance im Bereich von 5 bis 15 Prozent, neue Abo-basierte Lizenzmodelle und License Mobility für viele Anwendungen, so dass diese unter Verwendung der vorhandenen Lizenzen auch in der Cloud genutzt werden können. ■

Server 2012 R2 verwalten

Der mit Windows Server 2008 eingeführte Server Manager wird in Server 2012 (R2) zur zentralen Schaltstelle für den Administrator. Für das Remote-Management gibt es die aktualisierten RSAT.

VON WOLFGANG SOMMERGUT



Das Dashboard der Server Managers bietet Befehle für gängige Aufgaben und zeigt den Server-Status.

WIE SCHON IN FRÜHEREN Versionen startet der Server Manager automatisch nach dem Anmelden am System, denn Windows Server 2012 R2 bootet nämlich im Gegensatz zu Windows 8.x nicht standardmäßig in den neuen Startbildschirm.

Während es sich bei den verbliebenen sonstigen Tools weitgehend um altbekannte MMC-Snap-ins wie die Dienste- oder Gruppenrichtlinienverwaltung handelt, präsentiert sich der Server Manager in neuer Optik. Diese ist mit ihrem Kachel-Design an das Aussehen des neuen Windows-Startbildschirms angelehnt.

Die Startseite des Management-Tools ist nun ein Dashboard, das eine eigene Kachel für jede installierte Rolle sowie für einzelne oder Gruppen von Servern anzeigt. Sie enthält Links auf Übersichten zu aufgetretenen Ereignissen, zu Leistungsdaten und zu Ergebnissen des für die Rolle zuständigen Best Practice Analyzer.

Treten Probleme auf, zeigt das Dashboard diese an, indem es die entsprechende Kachel mit einem roten Balken versieht. Wie andere Daten präsentiert der Server Manager diese Health-Indikatoren nach wie vor nicht in Echtzeit, sondern aktualisiert sie per Voreinstellung alle zehn Minuten. Dieses Intervall lässt aber sich über „Verwalten → Server-Manager-Eigenschaften“ anpassen.

Keine Trennung mehr zwischen Rollen und Features

Eine zentrale Aufgabe des Server Manger bestand schon in Windows Server 2008 R2 darin, Rollen und Features hinzuzufügen oder zu entfernen. Allerdings war dafür jeweils ein eigener Wizard zuständig, so dass man wissen musste, ob Microsoft eine Funktion unter Rollen oder unter Features einsortiert hat. Diese Trennung entfällt unter Windows Server 2012, so dass sich alle Komponenten des Betriebssystems über einen einzigen Wizard einrichten oder deinstallieren lassen.

Als weitere Änderung im Vergleich zu Server 2008 R2 fällt auf, dass der Wizard beim Hinzufügen von Rollen eine eigene Option für die Remote Desktop Services bietet. Sie startet die sogenannte Szenario-basierte Installation, mit der sich alle Komponenten einrichten lassen, die für Terminal-Server oder virtuelle Desktops benötigt werden. Die wohl wichtigste Neuerung besteht darin, dass der Server Manager sich nicht mehr bloß dafür eignet, einzelne Server, sondern Gruppen von Servern zu verwalten. Dabei steht es dem Administrator frei, Maschinen unter verschiedenen Kriterien zusammenzufassen, sei es, weil sie sich an einem gemeinsamen Standort befinden oder die gleiche Anwendung ausführen.

Die Mitglieder einer solchen Server-Gruppe lassen sich nicht nur gemeinsam überwachen, indem der Server Manager etwa die Einträge aus den Server-Logs aller Maschinen konsolidiert und beim Auftreten von Problemen die Kachel für die ganze Gruppe rot markiert.

Vielmehr bietet er die Möglichkeit, bestimmte Aktionen auf ausgewählte oder alle Server einer Gruppe anzuwenden. Dazu zählt etwa das das Öffnen einer Powershell-Sitzung, der Computerverwaltung oder die Konfiguration von

NIC-Teaming (Network Interface Card, Netzwerkkarte). Dieses Remote-Management beschränkt sich nicht auf Maschinen unter Windows Server 2012 (R2), sondern lässt sich für einige Aufgaben auch auf Windows Server 2008 (R2) anwenden. Voraussetzung dafür ist aber, dass man dort das Windows Management Framework 3.0 installiert. Dieses enthält neben Powershell 3.0 auch den erforderlichen CIM-Provider (Common Information Model) für den Server Manager.

Die Basis des Multi-Server-Managements sind WMI, Powershell und die darin enthaltenen Workflow-Funktionen. Aus diesem Grund lassen sich praktisch alle Aktionen, die der Server Manager über die GUI anbietet, auch über die Kommandozeile beziehungsweise über Scripts durchführen. Dies erlaubt gerade bei einer größeren Zahl von Servern die Automatisierung vieler Abläufe.

Tools-Menü konfigurieren

Der Server Manager in Windows Server 2012 (R2) bringt nicht nur Neuerungen durch Multi-Server-Management und die Integration der Best Practice Analyzer, sondern er dient auch als Schaltzentrale für die verbliebenen (MMC-) Verwaltungswerkzeuge. Sie finden sich fast vollständig im „Tools"-Menü, wo sich auch eigenen Programme einbinden lassen.

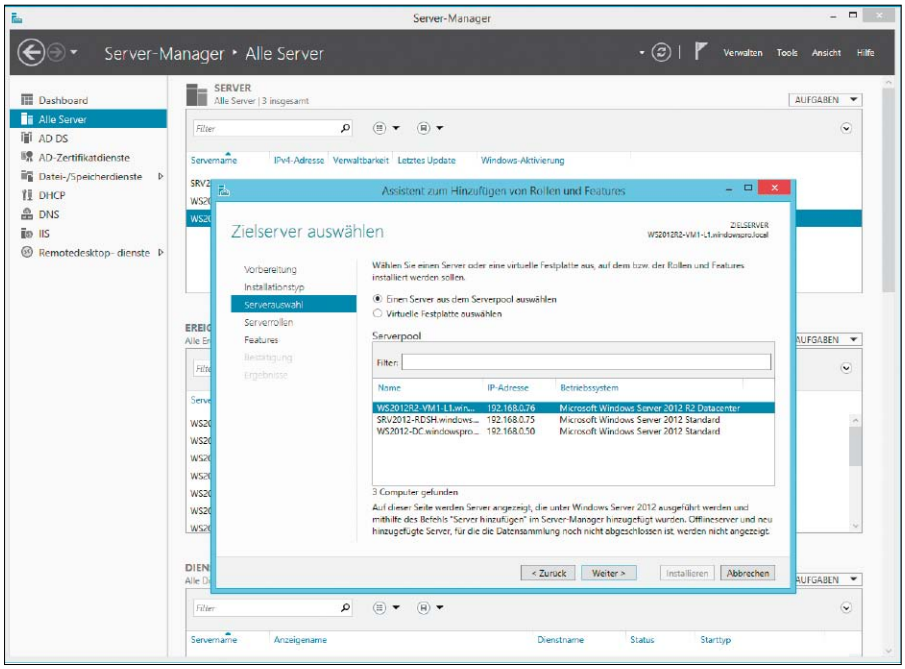
Die Möglichkeit, verschiedene Admin-Tools direkt aus dem Server Manager zu starten, kompensiert unter Windows 8.x und Server 2012 (R2) den Wegfall des Startmenüs. Anstatt für den Aufruf eines Management-Werkzeugs zur neuen Startseite zu wechseln oder dafür das rudimentäre Menü hinter dem Start-Button (Tastenkombination Win-X) zu nutzen, kann man die gewünschten Programme also direkt aus dem Server Manager aufrufen.

Die vorgegebene Liste der Anwendungen im Menü „Tools" ist nicht nur ellenlang, sie weist zudem eine flache Struktur auf, die mit Ausnahme von „Terminal-Services" keine Ordner enthält. Wenn man eigene Programme in dieses Menü hinzufügen möchte, dann empfiehlt es sich, dafür eine hierarchische Gliederung mit Hilfe von Ordnern zu nutzen.

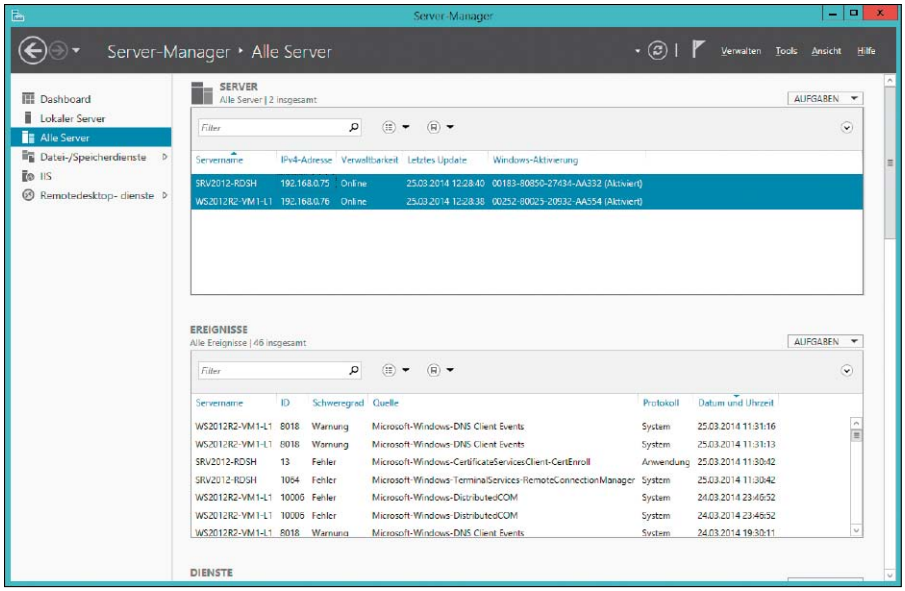
Verknüpfungen in die Systemsteuerung kopieren

Das Tools-Menü lässt sich nicht im Server Manager konfigurieren. Vielmehr spiegelt es nur die Programme wider, die in der Systemsteuerung unter „System und Sicherheit → Verwaltung" als Verknüpfungen vorliegen. Man legt am einfachsten neue an, indem man die gewünschten Verzeichnisse inklusive der Programm-Verknüpfungen auf dem Desktop erstellt und per Drag & Drop in die Systemsteuerung verschiebt.

Alternativ kann man nach „%ProgramData%\Microsoft\Windows\Start Menu\Programs\Administrative Tools" wechseln und in diesem Verzeichnis eigene Ordner und Verknüpfungen anlegen. Die Struktur unter diesem Pfad ist die Basis für „Verwaltung" in der Systemsteuerung und für das Tools-Menü im Server Manager.



Der Wizard zum Hinzufügen und Entfernen von Rollen und Features verwaltet nun alle Funktionen.

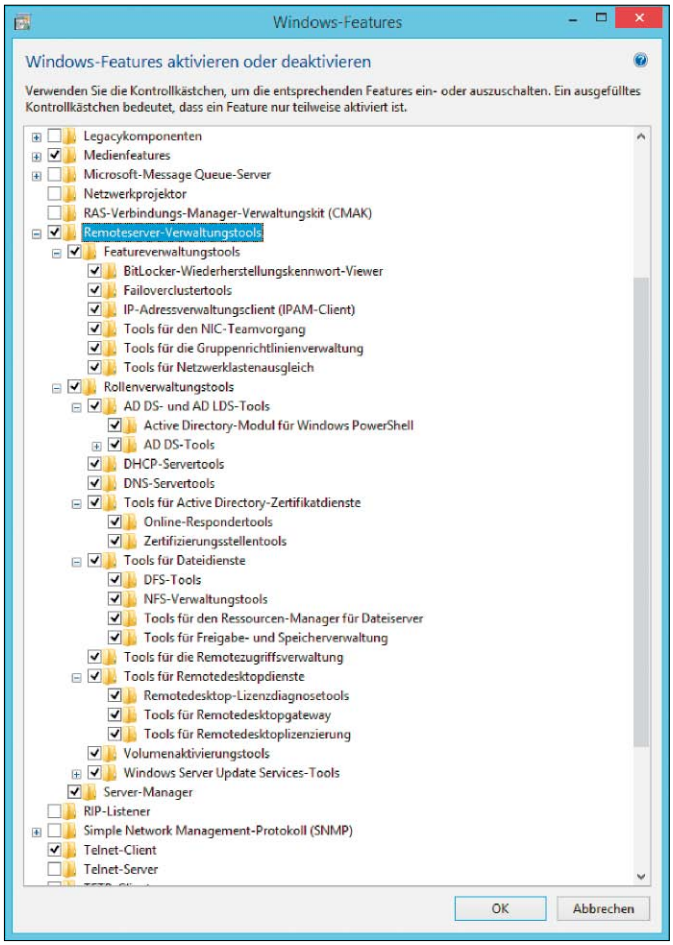


Das Multi-Server-Management wendet Befehle auf eine Gruppe von Servern an und liefert auch ihre Infos.

Management-Optionen für die Konsole

Die beschriebenen neuen Möglichkeiten für die Server-Administration stehen nicht immer zu Verfügung, sondern hängen davon ab, welche Installationsoptionen für das System gewählt wurden. Neben der spartanischen Variante Server Core, die Microsoft schon in Server 2008 einführte, und einer vollen grafischen Benutzerführung (GUI) brachte Windows Server 2012 noch das Minimal Server Interface.

Es handelt sich dabei um eine Konfiguration, die zwischen der kompletten und der mageren Ausstattung angesiedelt ist. Anders als ihre dürre Optik vermuten lässt, die sich kaum von Core unterscheidet, bietet sie eine Reihe grafischer Management-Tools, darunter auch den Server Manager. Dieser fehlt indes unter Ser-



Das Setup von RSAT richtet die umfangreiche Tools-Sammlung standardmäßig komplett ein.

ver Core, das man jedoch mit Hilfe von Remote Server Administration Tools (RSAT, auf Heft-DVD, Download über *http://bit.ly/1iDMUS3*) remote von einer Workstation und einem anderen Server aus verwalten kann. Lokal stehen dort im Wesentlichen nur Powershell und die alte Kommandozeile zur Verfügung.

Im Unterschied zu Windows Server 2008 (R2) können die neuen Versionen des Servers zwischen diesen drei Modi umschalten, ohne dass man das System neu installieren muss. Der Umstieg von einer reichhaltigeren auf eine magere Oberfläche erfolgt über den Server Manager. Zu diesem Zweck führt man im Menü „Verwalten" den Befehl „Rollen und Funktionen entfernen" aus. Im folgenden Assistenten wählt man, nachdem auch das Remote-Management von Rollen möglich ist, den betreffenden Server aus und geht im linken Teil des Fensters auf „Features".

Unter „Benutzeroberfläche und Infrastruktur" finden sich drei Einträge, wobei nur „Grafische Servershell" und „Grafische Verwaltungstools und Infrastruktur" für das Umschalten zwischen den Installationsmodi interessant sind. Für die vollständige GUI sind beide Optionen aktiviert, während für das Minimal Server Interface nur „Grafische Verwaltungstools und Infrastruktur" erforderlich ist. Wählt man auch das ab, landet man bei „Server Core".

Hat man alle grafischen Tools entfernt und damit die Core-Variante aktiviert, dann führt der Weg zurück nur mehr über Powershell. Mit Hilfe des Cmdlets *Install-WindowsFeature* kann man die benötigten Komponenten wieder nachrüsten.

Will man nur das Minimal Server Interface, dann reicht der Aufruf von

```
Install-WindowsFeature Server-
  Gui-Mgmt-Infra
```

Möchte man dagegen die volle grafische Oberfläche haben, dann muss man zusätzlich folgenden Parameter aufrufen:

```
Install-WindowsFeature Server-
  Gui-Shell
```

Administration mit dem Remote Server Administration Tools (RSAT)

Windows Server lässt sich nicht nur über seine eigene Konsole verwalten, sondern weitgehend auch remote von einer Windows-Workstation aus. Zuständig sind dafür die Remote Server Administration Tools (RSAT), die in der deutschen Version „Remoteserver-Verwaltungstools" heißen. Diese Werkzeuge deckten in der Vergangenheit nicht alle Features von Windows Server ab und unterstützten ältere Server-Versionen nur eingeschränkt. Die RSAT für Windows 8.x nähern sich weiter dem Ziel einer vollständigen Server-Verwaltung, lassen aber noch Lücken und bringen keine größeren Fortschritte für Windows Server 2008 (R2).

Die meisten Änderungen der neuesten RSAT entspringen zum einen der neuen Bedienerführung des Client-Betriebssystems, zum anderen den erweiterten Features von Windows Server 2012 (R2). Ihre Installation setzt wie gewohnt immer die passende Version von Windows voraus, so dass man die neueste Ausführung zur Verwaltung von Server 2012 R2 nicht unter Windows 7 oder gar XP nutzen kann.

Im Unterschied zu früheren Versionen richtet die Installation von RSAT für Windows 8.x sämtliche Tools ein. Wenn man einzelne davon nicht benötigt, dann kann man sie wie gewohnt in der Systemsteuerung unter „Programme → Windows-Funktionen aktivieren oder deaktivieren" abwählen.

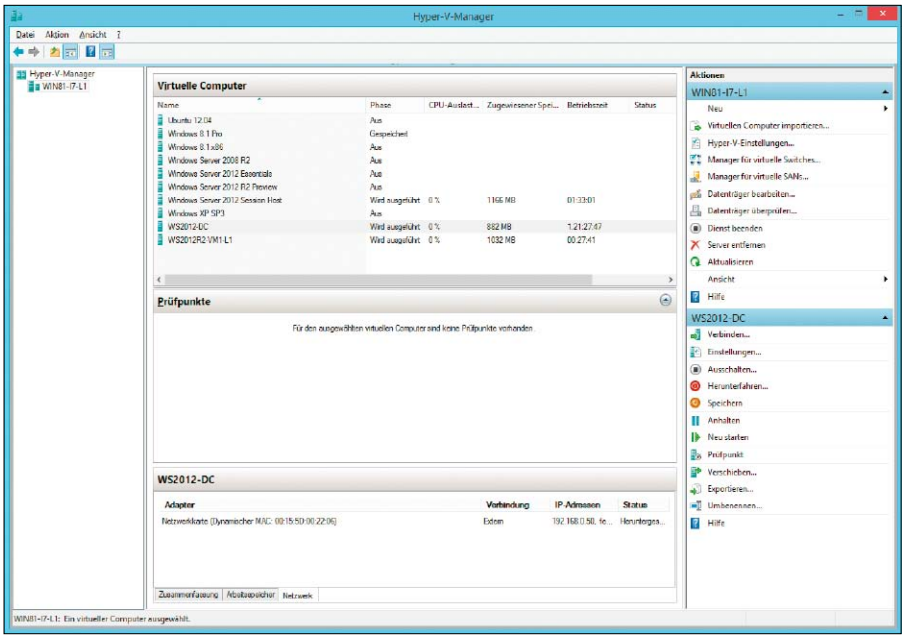
Nach vollendetem Setup stellt sich für alle, die sich noch nicht mit dem Verschwinden des Startmenüs abgefunden haben, die Frage, wo man die Tools nun aufrufen kann. Ein Weg führt erwartungsgemäß über die neue Startseite, wo man durch Tippen des Programm-Namens automatisch die Suchfunktion auslöst. Dies setzt allerdings voraus, dass man die teilweise eigenwillig lokalisierten Bezeichnungen der Tools im Kopf hat.

Wer bevorzugt die Kacheloberfläche nutzt, wird daher eher die Symbole für RSAT und andere Verwaltungswerkzeuge neben den vorhandenen Apps einblenden. Zu diesem Zweck öffnet man die Charms-Leiste am rechten Bildschirmrand und wählt dort „Einstellungen → Kacheln" und aktiviert die Option „Verwaltungstools anzeigen".

Wer lieber vom Desktop aus arbeitet, wird dort im abgespeckten Win-X-Startmenü zwar einige Links zu den integrierten Management-Tools finden. Allerdings zeigt es nach der Installation von RSAT keines der darin enthaltenen Programme. Als Alternative für ein Desktop-zentrisches Arbeiten empfiehlt sich daher der Server Manager, der auch am Client als Schaltzentrale für alle RSAT-Tools dient.

Dort kann man aus dem Tools-Menü alle RSAT-Anwendungen starten, außerdem enthält auch das Kontextmenü der verwalteten Server entsprechende Links. Während sich unter „Tools" fast nur GUI-Anwendungen befinden, bietet das Kontextmenü eines Servers auch direkten Zugriff auf eine Reihe von Kommandozeilen-Tools.

Die Remote Server Administration Tools lassen sich über eine einzige Einstellung auf der Startseite anzeigen.



Der Hyper-V Manager ist seit Windows 8 nicht mehr Teil der RSAT, sondern kommt mit dem Betriebssystem.

Mittlerweile ist der Server Manager schlau genug, in diesem Kontextmenü nur die Befehle anzuzeigen, die auf die installierten Features und die OS-Version des Zielrechners tatsächlich passen – natürlich vorausgesetzt, die entsprechenden Tools sind lokal installiert. So blendet er auch den Befehl „Rollen und Funktionen hinzufügen“ aus, wenn ein Rechner unter Server 2008 (R2) läuft.

Eine wichtige Einschränkung besteht somit darin, dass der Server Manager nur bei Windows Server 2012 (R2) Rollen und Features remote hinzufügen und entfernen kann. Für ältere Versionen des Betriebssystems ändert sich damit nichts zum Besseren, nachdem auch schon der Server Manager in RSAT für Windows 7 diese Limitierung hatte.

Neue Tools für neue Features

In der Sammlung der „Remote Server Administration Tools“ kommen unter Windows 8.x neue Werkzeuge hinzu. Sie verwalten neue oder erweiterte Funktionen von Windows Server 2012 (R2), dagegen bleiben die in der Vergangenheit nicht berücksichtigten Features wie „Windows Server Backup“, die „Windows Deployment Services“ oder die „Rights Management Services“ weiterhin außen vor.

Unter den Neuzugängen von RSAT für Windows 8.x finden sich Verwaltungs-Tools für „Cluster-Aware Updating“, „IP Address Management“ (IPAM) und „NIC-Teaming“, die als Module von Server Manager implementiert sind. Weitere Tools bieten eine neue Verwaltungssicht auf Features, die auch schon unter Server 2008 (R2) vorhanden waren.

Dazu zählt die „Remotezugriff-Verwaltungskonsole“, die das Management von Direct Access und VPN unter einer Oberfläche zusammenführt, während für Routing und RAS weiterhin das alte Programm zuständig ist. Mit von der Partie ist zudem die WSUS-Konsole (Windows Server Update Services), die bisher separat zu installieren war. Abwesend sind in RSAT für Windows 8.x die „SMTP Server Tools“, der „Storage Explorer“ und der „Storage Manager for SAN.

Hyper-V-Manager für Windows 8 nicht abwärtskompatibel

Ebenfalls aus den RSAT verschwunden ist der Hyper-V-Manager, der seit Windows 8 als Teil des Betriebssystems ausgeliefert wird. Da es die Client-Version von Hyper-V umfasst, bringt es die erforderlichen Management-Werkzeuge gleich selbst mit. Sie lassen sich auch dann installieren, wenn der lokale Hypervisor nicht verwendet wird, weil man damit auch Hyper-V remote auf dem Server verwalten kann.

Ärgerlich ist dabei jedoch, dass die in Windows 8.x enthaltene Version des Hyper-V-Managers nicht in der Lage ist, ältere Versionen von Hyper-V unter Server 2008 oder 2008 R2 zu administrieren. Da erwartungsgemäß auch der Hyper-V Manager aus RSAT für Windows 7 nicht mit Windows Server 2012 (R2) kompatibel ist, benötigt man zum entfernten Management von Hyper-V eine jeweils passende, komplette Umgebung aus Windows plus das dazu gehörige Programm.

Besser ist jedoch die Kompatibilität zwischen RSAT für Windows 8 und 8.1. Die Version aus Windows 8 kann sich mit Hyper-V 2012 R2 verbinden und viele Einstellungen von virtuellen Maschinen (VMs) verwalten. Natürlich ist er nicht in der Lage, neue Features wie VMs der Generation 2 zu bearbeiten (Infos über *http://bit.ly/1fntc9k*). Umgekehrt passt der Hyper-V-Manager in Windows 8.1 seinen Assistenten für neue VMs so an, dass er die vom Hypervisor in Windows 8 und Server 2012 nicht unterstützten Optionen ausblendet.

Diese unkomplizierte Zusammenarbeit zwischen den Versionen von Windows 8.x und Server 2012 beziehungsweise 2012 R2 trifft indes nicht auf andere Tools zu. Beispielsweise wurde IP Address Management (IPAM) in der neuesten Version stark erweitert, so dass das betreffende RSAT-Tool in Windows 8.1 nicht für Windows Server 2012 geeignet ist.

Außerdem wird mit dem Release 2 der „Windows System Resource Manager“ ausgemustert, womit nun in RSAT das dazugehörige Werkzeug fehlt. Das Gleiche gilt für „Identity Management for UNIX“, das man unter Windows 8.1 ebenfalls nicht mehr verwalten kann.

Powershell-Cmdlets für Server-Management

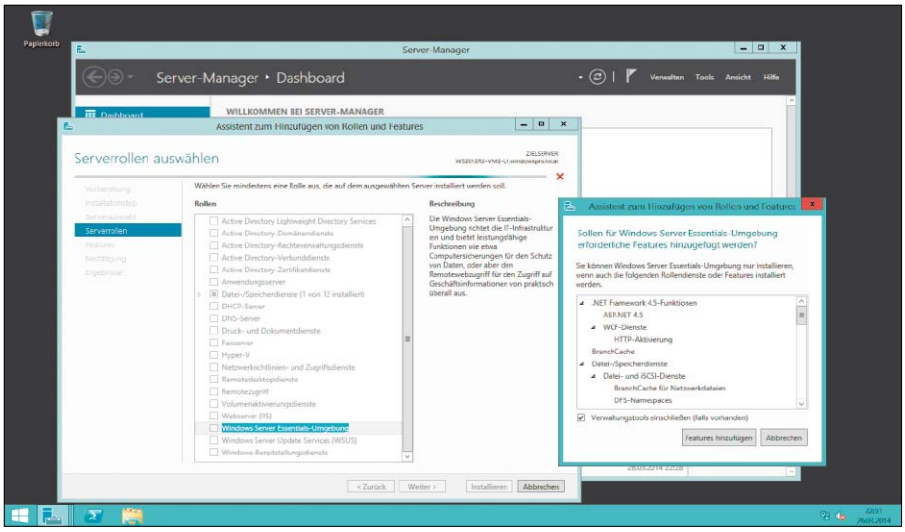
Neben der Verwaltung über GUI-Tools spielt unter Windows Server 2012 (R2) die Administration mittels Powershell eine zentrale Rolle. Er umfasst daher zahlreiche neue Cmdlets für diesen Zweck, von denen ein großer Teil auch mit RSAT für Windows 8.x installiert wird.

Um ihre Verwendung zu erleichtern, bietet der Server Manager Befehle zum Aufruf der Powershell auf dem Remote-Computer sowie für eine lokale Session, die beim Start alle Cmdlets des Active-Directory-Moduls lädt. RSAT für Windows 8.1 liegen wie gewohnt in einer 32- und einer 64-Bit-Ausführung vor. Sie können kostenlos von Microsofts Website heruntergeladen werden (*http://bit.ly/1iDMUS3*). ■

Neu in Server Essentials

Mit dem Release 2 von Windows Server 2012 steht auch ein Upgrade der Small-Business-Variante an. Das neue Essentials lässt sich auch in einer VM unter Hyper-V oder als Rolle in anderen Server-Edition installieren.

VON WOLFGANG SOMMERGUT



Features von Server Essentials stehen nun als Rolle auch in den Editionen Standard und Datacenter zur Verfügung.

WINDOWS SERVER 2012 ESSENTIALS wurde als gemeinsamer Nachfolger für den Small Business Server und für den Home Server eingeführt. Er bietet einige exklusive Features für kleine Firmen und Privatanwender, die nicht die technische Expertise von IT-Profis besitzen. Dazu zählen die einfache Administration über ein Dashboard, der Remote-Webzugriff auf freigegebene Ordner oder das Backup für alle angeschlossenen Client-PCs.

Dem einfachen Management sowie den exklusiven Funktionen standen bisher einige Beschränkungen gegenüber, die Unternehmen unnötig einengten. Dazu zählen das Limit von maximal 25 Benutzern und die Anforderung, dass Server 2012 Essentials der erste Domänen-Controller im Netz sein muss und keiner bestehenden Active-Directory-Struktur (AD-Struktur) beitreten kann.

Wenn Firmen aus dem Lizenzkorsett entwachsen, weil sie mehr als 25 User haben, dann gab es bisher keine überzeugenden Optionen zur Weiternutzung. Um den Wegfall des Small Business Server 2011 zu kompensieren, der bis zu 75 Benutzer erlaubte, bot Microsoft nur ein In-Place-Update auf die Standard Edition an. Danach konnten die exklusiven Features von Server Essentials ebenfalls für bis zu 75 User genutzt werden.

Die genannten Limitierungen verbauten dem kleinsten Windows-Server oft die Möglichkeit, von größeren Firmen in Zweigstellen und Niederlassungen eingesetzt zu werden. Dort wären beispielsweise das integrierte Client-Backup oder das einfache Management häufig gefragt, aber die fehlende Integration mit einem vorhandenen AD spricht dort meistens gegen Server Essentials.

Mehr Flexibilität durch Essentials Experience

Die neue Deployment-Option als installierbare Rolle der Standard und Datacenter Edition („Windows Server Essentials Experience“, WSEE) soll Windows Server 2012 R2 Essentials nun neue Einsatzgebiete erschließen.

Zum einen fällt damit das Limit von 25 Benutzern, weil die Client-Lizenzen als CALs separat erworben werden müssen und nicht mehr Bestandteil der Server-Lizenz sind. Zum anderen können die größeren Server-Editionen einer bestehenden Domäne beitreten. Für die Essentials Experience gilt jedoch die Einschränkung, dass im AD nur eine einzige Domäne vorhanden sein darf. Dafür lässt sich die WSEE-Rolle auf mehreren Servern innerhalb eines Netzwerks installieren, beispielsweise um das Client-Backup besser zu bewältigen.

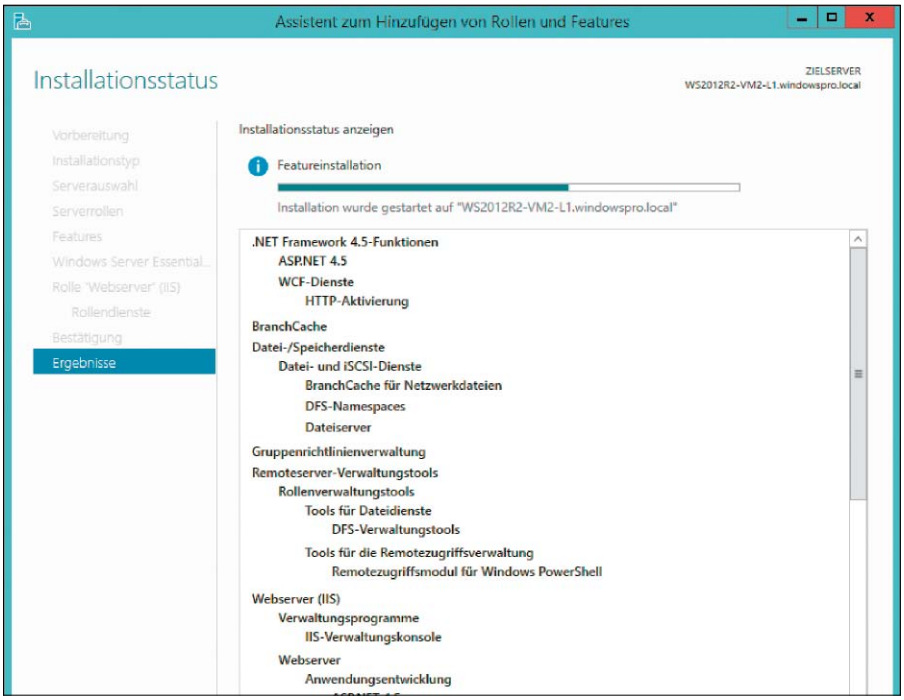
Das Hinzufügen der WSEE-Rolle erfolgt über eine einzige Checkbox im zuständigen Wizard des Server Managers, aber es bewirkt die Installation mehrerer Rollen und Features. Dazu zählen unter anderem das .NET Framework 4.5, Branchcache, Dateiserver, RSAT, IIS oder das Backup-Programm.

Gemeinsames Setup für Hyper-V und Server Essentials

Wenn man dagegen Windows Server 2012 R2 Essentials wie bisher als eigenständiges Pro-

dukt einsetzen möchte, dann gelten die genannten Einschränkungen weiterhin. Neu ist hingegen beim Stand-alone-Produkt, dass Microsoft die Installation in einer Virtuellen Maschine (VM) unter Hyper-V als bevorzugte Deployment-Variante empfiehlt. Die Virtualisierung von Server Essentials war lizenzrechtlich auch schon in der Vergangenheit möglich, allerdings musste man dafür den Hypervisor selbst bereitstellen. Microsoft sah dafür den kostenlosen Hyper-V Server 2012 vor, der nur Server Core mit der Hyper-V-Rolle umfasst und für die Zielgruppe des kleinen Windows-Servers nicht einfach zu verwalten ist. Die Installation von Server Essentials in einer VM hielt bisher zudem einige Hürden bereit.

Auch hier schafft Windows Server 2012 R2 Essentials Abhilfe, indem es nun mit integriertem Hyper-V 2012 R2 (*http://bit.ly/1ebX2xb*) ausgeliefert wird. Eine erweiterte Setup-Routine kümmert sich um den kompletten Vorgang vom Einrichten des Hypervisors und dem Anlegen der VM bis zur Installation des Betriebssystems in der virtuellen Maschine.



Die Installation der WSEE-Rolle erfolgt über den Server Manager und lädt zahlreiche Komponenten.

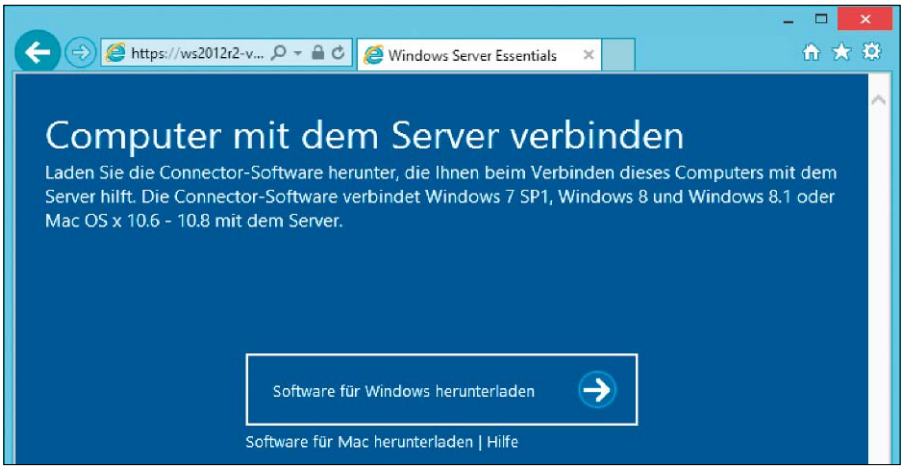
Installation von virtuellem Operating System Environments

Diese neue Konfiguration spiegelt sich nun auch in einer lizenzrechtlichen Änderung wider, die neben der Installation von Server Essentials in der Parent Partition eine zusätzliche virtuelle Instanz erlaubt.

Die Installation als Konsolenbetriebssystem für Hyper-V unterliegt aber wie gewohnt erheblichen Beschränkungen, so dass sie nicht für die Ausführung von produktiven Anwendungen in Frage kommt. Der Betrieb von Server 2012 R2 Essentials unter Hyper-V bietet den Vorteil, dass sich parallel dazu auf dem gleichen Rechner virtuelle Maschinen mit Datenbanken, Exchange oder Sharepoint ausführen lassen, also weitere Operating System Environment (OSE). Auch wenn Microsoft bei Server Essentials für E-Mail und Collaboration die Cloud-Services von Office 365 vorsieht, so werden viele Firmen weiterhin diese Dienste lieber intern bereitstellen wollen.

Verbinden von Clients mit Windows Server Essentials

Das Setup von Windows Server 2012 R2 Essentials bietet zum Abschluss an, mehrere Benutzerkonten einzurichten, mit denen von den angeschlossenen PCs auf den Server zugegriffen werden kann. Danach besteht die Möglichkeit, weitere Konten über das Dashboard anzulegen. Die maximal zulässige User-Zahl liegt bei 25. Wenn ein Benutzer seine Anmeldedaten vom Administrator erhalten hat, dann kann er



Die Verbindung eines Clients mit Server Essentials geschieht über den Download der Connector-Software.

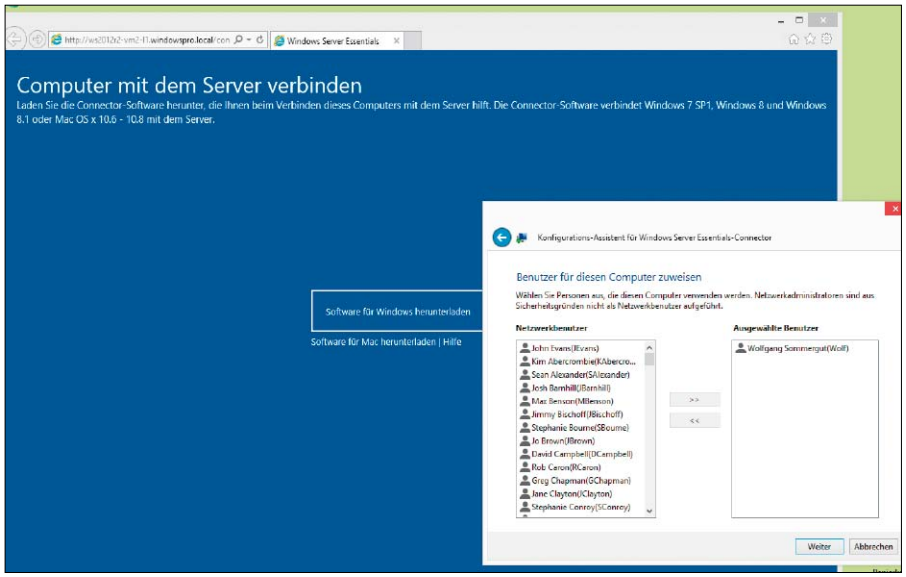
im nächsten Schritt mit seinem Rechner der Domäne des Essentials-Servers beitreten. Dies erfolgt nicht über den vom großen Server gewohnten Weg, sei es über die Systemsteuerung oder über die dafür Kommandozeilen-Tools.

Obwohl der kleinste Windows-Server die Rolle als Domänen-Controller übernimmt, gehört es nämlich zu seinem Konzept, dass weder Benutzer noch Systemverwalter mit dem AD direkt in Berührung kommen.

Client-Software per Browser

Aus diesem Grund lädt der Anwender eine eigene Client-Komponente von Server 2012 Essentials auf den PC herunter. Dafür verbindet er sich via Internet-Browser mit *http://<Win 2012R2-Essentials>/connect*, wobei sichergestellt sein muss, dass der Server über DNS gefunden wird. Andernfalls reicht auch die Eingabe der IP-Adresse. Die anschließende Installation des Connectors schließt den PC an die Domäne an und richtet ein Programmsymbol für das Dashboard ein, über das der Server weitgehend verwaltet wird. Dafür verwendet Microsoft ein neues lokales Administratorkonto namens „__clientsetup__$".

Nach dem Reboot des Systems, der durch den Domänenbeitritt erzwungen wird, muss die Anbindung an den Server unter dieser Kennung fortgesetzt werden. Dabei kann es im Fall der WSEE-Rolle passieren, dass der Prozess nicht einfach durchläuft, sondern eine Benutzeranmeldung erfordert. Da man das Passwort von „__clientsetup__$" jedoch nicht kennt, kann



Bei der Nutzung von Server Essentials als Rolle kann man die bestehenden Domänen-Konten übernehmen.

Das Dashboard ist für die meisten Administrationsaufgaben zuständig, so auch für die Funktion „Zugriff überall".

man sich damit behelfen, dass man sich unter einem anderen Administratorkonto anmeldet, das Passwort von „__clientsetup__$" zurücksetzt und sich anschließend unter diesem Namen einloggt. Danach setzt Windows die Connector-Installation automatisch fort. Wenn Server Essentials als Rolle auf einer Standard- oder Datacenter Edition installiert wird, verläuft das Anbinden von Clients nach dem gleichen Prinzip. In diesem Fall wird man indes mit der Benutzerverwaltung nicht auf der grünen Wiese beginnen, sondern die User aus der bestehenden Domäne verwenden. Zu bedenken ist nur, dass die vom System verlangten Anmeldedaten solche von einem Domänen-Konto sein müssen, selbst wenn der PC dieser noch nicht beigetreten ist. Auf der Download-Seite des Servers findet sich die Client-Software für Windows 7, 8 und Mac-OS X ab der Version 10.5. Windows XP wird nicht unterstützt. Hat man noch alte XP-Rechner im Netz, dann können sie der Domäne des Essentials-Servers auf die übliche Weise beitreten und auch wie gewohnt über „Active Directory-Benutzer und -Computer" verwaltet werden. Der kleine Server bringt nämlich alle gängigen Tools für das Management von Active Directory und Gruppenrichtlinien mit.

Zugriff überall

Zu den exklusiven Funktionen von Windows Server 2012 R2 Essentials, die seinen Einsatz in kleinen Firmen und bei privaten Anwendern vereinfachen sollen, zählt „Remote Web Access" (auch „Zugriff überall" genannt). Es kombiniert den Webzugang zu freigegebenen Ordnern mit der Einrichtung eines VPN, der Registrierung einer Internet-Domäne und der automatischen Konfiguration eines Routers. Remote Web Access erlaubt somit die Nutzung des kleinsten Windows-Servers von außerhalb der Firewall. Das Konzept von Server 2012 R2 Essentials, die Benutzer von komplexer Technik mittels Assistenten und Tools abzuschirmen, klappt bei einigen Funktionen gut, zum Beispiel bei der Benutzerverwaltung oder der Konfiguration des Client-Backups. Dagegen sind die Dinge bei „Zugriff überall" komplizierter, als der Wizard glauben machen möchte. Ohne Kenntnisse dessen, was hinter den Kulissen passiert, kann die Einrichtung des VPN daher leicht scheitern, während dagegen die Konfiguration des reinen Browser-Zugriffs auf die Dateien völlig unproblematisch ist.

Wie die meisten Aufgaben der Administration erfolgt auch die Aktivierung des „Remotewebzugriff" über das Dashboard. Nach der Auswahl des Menüpunkts „Zugriff überall einrichten" kann man über den Link in der rechten Fensterhälfte den zuständigen Wizard zur Konfiguration des Features starten.

Die Kombination des SSTP VPN mit dem eigentlichen Remote Web Access, den man ja auch innerhalb des LANs nutzen kann, führt dazu, dass man in den ersten Schritten die nötige Netzkonfiguration durchlaufen muss. Sie beginnt damit, dass man den Namen der Domäne eingibt, über die Windows Server 2012 R2 Essentials von außen erreichbar sein soll.

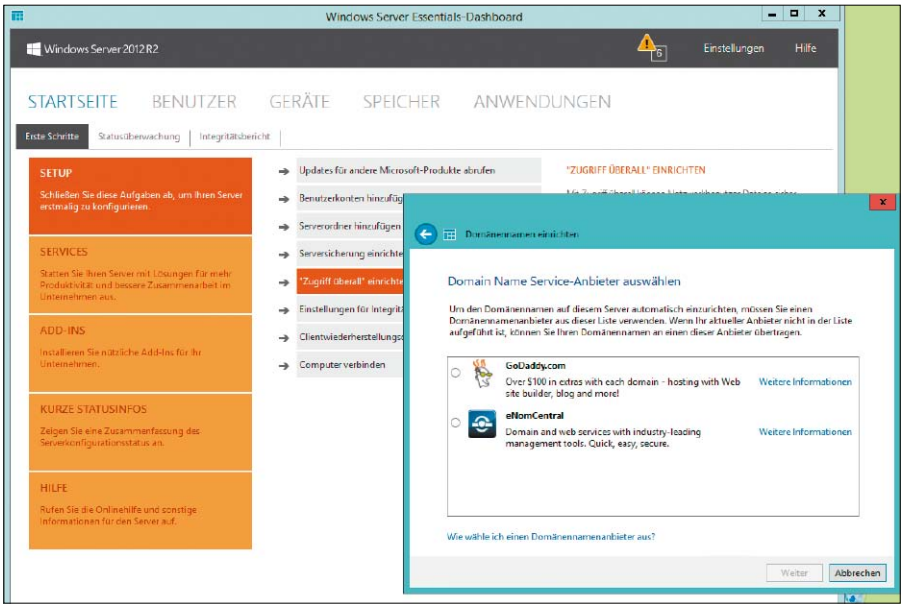
Bestehende Domäne verwenden

Die erste Option dabei lautet: „Ich möchte einen Domänennamen verwenden, den ich bereits besitze". Hier liegt es nahe, gleich eine Internet-Domäne zu verwenden, die man bereits registriert hat. So einfach geht das in den meisten Fällen aber nicht, weil kleine Unternehmen und private Anwender in der Regel keine festen, sondern dynamisch zugeteilte IP-Adressen verwenden.

Wenn man unter diesen Bedingungen von unterwegs auf den Server in der Firma zugreifen möchte, dann muss der Domänenname stets in die gerade aktuelle IP-Adresse des DSL-Anschlusses aufgelöst werden. Daher ist es notwendig, dass der Provider, der die Domäne hostet, dynamisches DNS (*http://bit.ly/1jAzCXy*) unterstützt und dass man diesen Service gebucht und konfiguriert hat. Besitzt man eine feste IP-Adresse, dann sollte man sie vor der Konfiguration des Remote-Webzugriffs zusammen mit dem Host-Namen des Essentials-Servers im DNS des Providers eintragen. Die

Eingabe einer bestehenden Domäne führt unweigerlich zum schnellen Ende der Wizard-geführten Konfiguration, weil es im nächsten Dialog nur noch die Auswahl zwischen manueller und automatischer Einrichtung der Domäne gibt. Die automatische Option besteht nur bei Providern, die einen auf Windows Server Essentials abgestimmten Mechanismus implementiert haben. Er ist für die Registrierung der Domäne, die Konfiguration des DNS sowie das Ausstellen und den Import eines Zertifikats zuständig. In der vom Wizard angebotenen Auswahl von ISPs befinden sich bis dato jedoch nur zwei US-amerikanische Firmen (Godaddy und Enomcentral).

Daher muss man als europäischer Anwender alle Schritte zur Konfiguration einer bestehenden oder für die Anmeldung einer neuen Domäne zu Fuß absolvieren. Microsoft fasst die dabei anfallenden Aufgaben in einem Hilfedokument (*http://bit.ly/1fMKCw8*) zusammen, allerdings nur in einer sehr allgemeinen Form. Wer etwa eine genaue Anleitung benötigt, wie man selbst ein Zertifikat ausstellt und in den Wizard für „Zugriff überall" übernimmt, dem sollte dieser Blog-Beitrag von Cesare Auteri helfen: *http://bit.ly/1fMKCw8*.



Für die automatische Einrichtung einer Domäne und des DNS kennt Server Essentials nur zwei US-Provider.

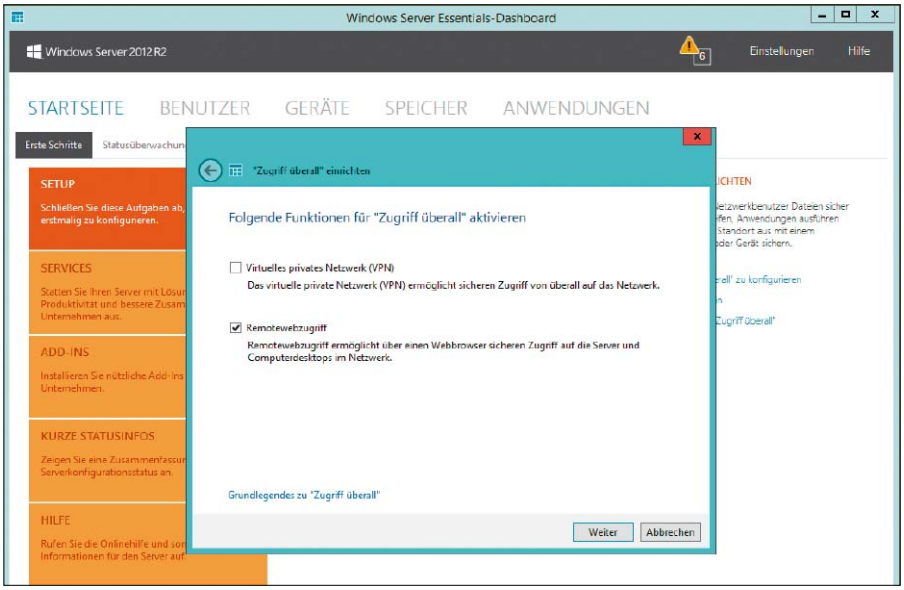
Neuen Domänennamen verwenden

Alternativ zur Verwendung einer bestehenden Domäne bietet der Wizard an, einen neuen Domänennamen einzurichten. Entscheidet man sich für diese Option, dann besteht beim nächsten Dialog die Auswahl zwischen der Registrierung der Domäne bei einem unterstützten Provider und einem Domänennamen von Microsoft.

Entscheidet man sich für die Option „Professionellen Domänennamen von einem unterstützten Provider erwerben", dann landet man derzeit wieder bei der Auswahl zwischen den beiden genannten US-Providern.

Alternativ springt Microsoft mit einem eigenen kostenlosen Angebot ein, das primär für private Anwender gedacht ist (Option „Persönlichen Domänennamen abrufen"). In der Praxis erhält man so eine Subdomäne unter *remotewebaccess.com*, wobei man gleich innerhalb des Dialogs prüfen kann, ob der gewählte Name noch verfügbar ist.

Erst nach Festlegung der Domäne, egal auf welchem Weg, gelangt der Wizard zur eigentlichen Konfiguration des Remote-Webzugriffs und des VPN. Der Browser-Zugang zu den freigegebenen Dateien auf dem Server bereitet keinerlei Kopfzerbrechen, denn nach Aktivierung der entsprechenden Checkbox wird er automatisch eingerichtet.



Der eigentliche Remote-Webzugriff lässt sich sehr einfach über eine einzige Checkbox aktivieren.

Router-Konfiguration

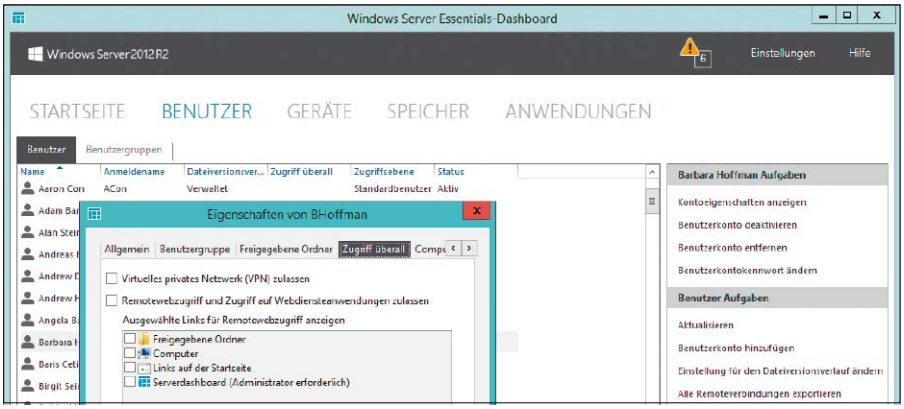
Mehr Aufmerksamkeit erfordert dagegen das VPN, weil dafür auch die Konfiguration des Routers erforderlich ist. Genau genommen geht es darum, ein Port-Forwarding für HTTPS einzurichten. Es bewirkt, dass der Router die Anfragen auf Port 443 an Server 2012 Essentials durchreicht. Für Geräte, die UPnP (Universal Plug and Play) unterstützen, übernimmt der Wizard diese Aufgabe.

Wenn man gleich beim Start des Wizards die Option zur automatischen Konfiguration des Routers abgewählt hat oder ein älteres Gerät besitzt, dann muss man das Port-Forwarding selbst einrichten. Microsoft veröffentlichte ein umfangreiches Hilfedokument, das für mehrere im Soho-Bereich populäre Router beschreibt, wie man dabei vorgehen muss. Sie finden das Dokument über *http://bit.ly/1myV3bm.*

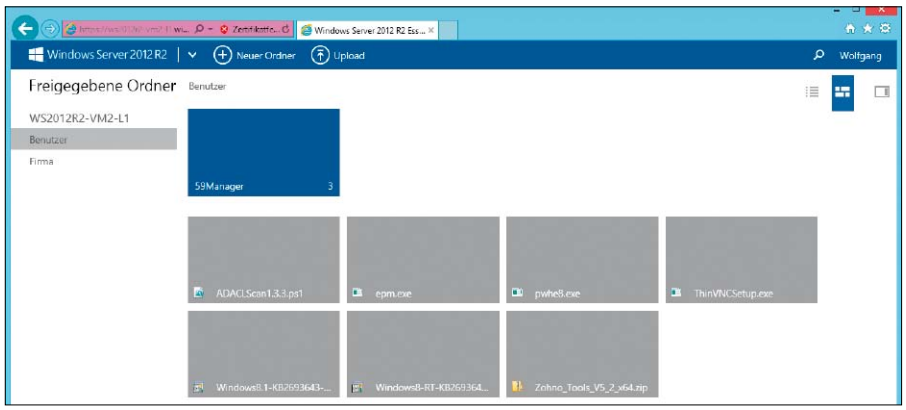
Benutzerrechte für Zugriff überall

Der Wizard fragt danach, ob allen vorhandenen und künftig angelegten Usern das Recht eingeräumt werden soll, dieses Feature zu nutzen. Wenn man darauf verzichtet, ist es später allerdings relativ leicht, einzelnen Benutzern dieses Privileg ganz oder teilweise zu erteilen. Zu diesem Zweck öffnet man im Dashboard die Benutzerverwaltung und wechselt in den Kontoeigenschaften zur Registerkarte „Zugriff überall". Hier besteht die Möglichkeit, die Rech-

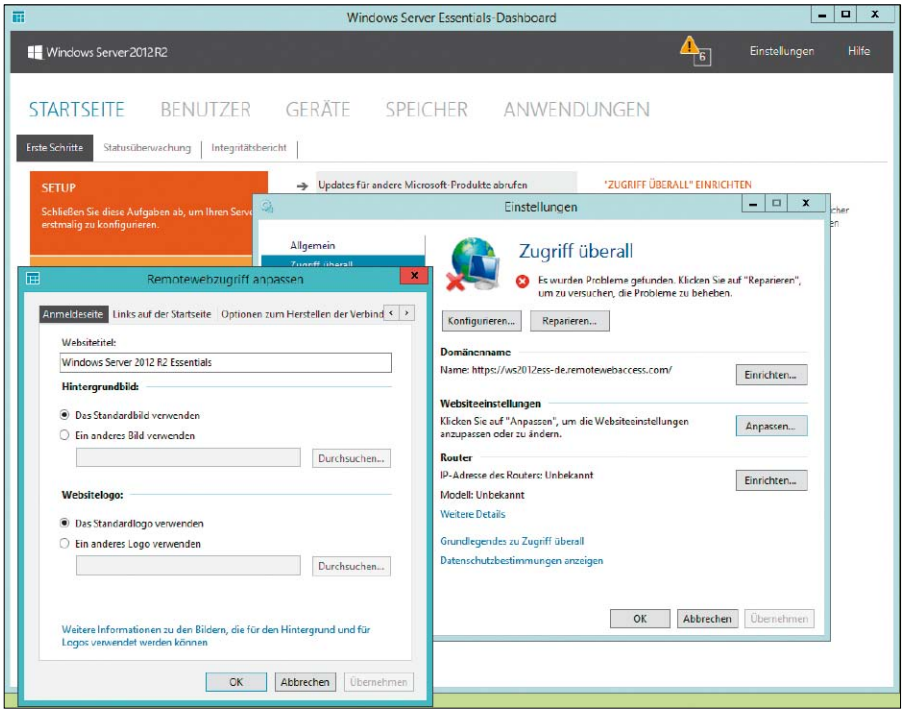
te für die VPN-Nutzung und Remote-Webzugriff separat zu verwalten. Außerdem lässt sich hier steuern, auf welche Ressourcen ein Benutzer remote zugreifen darf.



Die Rechte für die Nutzung des VPN und freigegebenen Ordner lassen sich auch einfach nachträglich vergeben.



Über die Weboberfläche können auch Windows-Vista- und 7-Clients Funktionen von Server Essentials nutzen.



Das Web-Interface ist gleich aufgebaut wie die App My Server 2012 R2 und lässt sich teilweise anpassen.

Remote Web Access starten

Wenn bisher alle Schritte erfolgreich absolviert wurden, dann sollte dem Browser-Zugriff auf die freigegebenen Ordner auf dem Server 2012 R2 Essentials nichts mehr im Wege stehen. Der schnellste Zugang führte bisher über das Launchpad, das einen eigenen Eintrag für Remote-Webzugriff enthielt. Dieses bleibt nun standardmäßig geschlossen und tritt im Release 2 hinter die Modern App „My Server 2012 R2“ zurück. Die im Kachel-Design gehaltene Anwendung ist in die Bereiche „Status“ (für Statusmeldungen des Servers), „Freigegebene Ordner“, „Benutzer“ und „Geräte“ unterteilt. Unter „Geräte“ findet sich eine Liste aller Server und Clients, die über die Installation des Connectors mit Server 2012 R2 Essentials verbunden wurden. Klickt man dort auf die Kachel für einen Rechner, dann gelangt man auf eine Übersichtseite, die neben einigen Statusinformationen einen Link zum Aufbau einer Remote-Desktop-Verbindung enthält.

Der eigentliche Remote Web Access verbirgt sich hinter den Kacheln im Abschnitt „Freigegebene Ordner“, durch die man navigieren kann. Standardmäßig finden sich dort nach der Installation bereits zwei Exemplare mit der Bezeichnung „Benutzer“ und „Firma“. Die App unterstützt einfache Operationen wie das Löschen oder das Hinauf- und Herunterladen von Dateien.

Für Clients, die nicht unter Windows 8.1 laufen, steht auch weiterhin eine reine Weboberfläche zur Verfügung. Ihr Aussehen hat sich seit Windows Server 2012 Essentials allerdings gründlich verändert und ist nun weitgehend ein Abbild von „My Server 2012 R2“. Die Eingabe von *http://<Name-von-Server-2012R2-Essentials>* öffnet die Homepage, deren Kacheln in die gleichen Bereiche unterteilt sind wie in der App.

Falls man die schon bestehende Internet-Domäne der Firma verwendet, dann ist der voll qualifizierte Host-Name (FQHN) normalerweise innerhalb und außerhalb des LAN ohnehin gleich. Nutzt man aber zum Beispiel eine Subdomäne von remotewebaccess.com, dann kann man Server 2012 R2 Essentials im Firmennetz über den internen FQHN ansprechen.

Konfiguration der Weboberfläche

Unter den Einstellungen für „Zugriff überall“, die man über das Dashboard öffnen kann, lässt sich das Aussehen der Browser-Oberfläche für Remote Web Access zu einem gewissen Grad an die eigenen Bedürfnisse anpassen. Zuviel darf man hier aber nicht erwarten.

So kann man unter „Websiteeinstellungen“ das Hintergrundbild und das Logo ändern. Außerdem lassen sich unter der Registerkarte „Links auf der Startseite“ die Verweise auf diverse Microsoft-Seiten durch eigene URLs ersetzen beziehungsweise ergänzen. ■

Kurz erklärt
Abkürzungen in diesem Heft

VON ARNE ARNOLD

Glossar Das bedeuten die Abkürzungen in der Welt der IT

AD = **Active Directory** heißt der Verzeichnisdienst von Microsoft Windows Server.

Bios = **Basic Input Output System** ist die Firmware bei x86-PCs, die den PC startet und anschließend das Betriebssystem lädt.

CAL = **Client Access License** (Client-Zugriffslizenz) ist eine besondere Form des Lizenzierung, die hauptsächlich bei Microsoft-Produkten verbreitet ist.

CIM = **Common Information Model** ist ein offener Standard, der in einer IT-Umgebung Objekte und ihre Beziehungen zueinander beschreibt.

DAS = **Direct Attached Storage** bezeichnet an einen Host angeschlossene Festplatten oder anderen Massenspeicher, die sich in einem separaten Gehäuse befinden.

DC = **Domain Controller** (Bereichs-Steuerung) ist ein Server zur zentralen Authentifizierung und Autorisierung von Computern und Benutzern in einem Netzwerk.

DHCP = **Dynamic Host Configuration Protocol** ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.

DISM = **Deployment Image Servicing and Management** (Abbildverwaltung und Bereitstellung von Images). Es handelt sich um ein Befehlszeilen-Tool zum Einbinden und Warten von Windows-Images.

DOM = **Document Object Model** ist ein Standard, der festlegt, wie eine Programmiersprache, etwa HTML, mit einem Dokument umgeht.

ESXi Free = **Vmware Vsphere Hypervisor** ist eine kostenlose Version der Virtualisierungs-Software von Vmware.

FTP = **File Transfer Protocol** dient der zuverlässigen Datenübertragung in Netzwerken.

GPO = **Group Policy Object** (Gruppenrichtlinienobjekt) setzt in einer Windows-Active-Directory-Domain Richtlinien für Benutzer und Computer.

GPP = **Group Policy Preferences** stellt eine Alternative zu Log-in-Scripts bei der Windows-Anmeldung bereit.

Hyper-V = **Hypervisor** ist die Virtualisierungs-Software unter Windows Server und Windows 8.x.

IIS = **Internet Information Server** ist eine Diensteplattform von Microsoft für PCs und Server. Über sie werden Dokumente und Dateien im Netzwerk zugänglich gemacht.

ISCSI = **Internet Small Computer System Interface** ist ein Verfahren, welches die Nutzung des SCSI-Protokolls über TCP ermöglicht.

LUN = **Logical Unit Number** wird zur Zuordnung für die Ansteuerung von Geräten im SCSI-Bus verwendet.

MMC = **Microsoft Management Console** ist eine grafische Benutzeroberfläche zur Verwaltung von Computern unter Microsoft Windows und Windows Server.

NIC-Teaming = **Network Interface Card Teaming** ist eine logische Netzwerkkarte (NIC), die mehrere physikalische Netzwerkkarten zu einer Gruppe zusammenfasst.

OSE = **Operating System Environment** stellt eine Umgebung dar, in der sich Programme nutzen lassen.

OU = **Organisation Unit**, Organisationseinheit ist in einer AD ein Container-Objekt, das Objekte und andere OUs enthalten kann.

PXE = **Preboot Execution Environment** startet einen PC über das Netzwerk und installiert dann ebenfalls über das Netz ein neues Betriebssystem. So lassen sich Rechner auch von der Ferne einrichten.

QoS = **Quality of Service** (Dienstequalität) stellt sicher, dass die vereinbarte Qualität einer Datenübertragung eingehalten wird.

RDP = **Remote Desktop Protocol** ermöglicht den Zugriff auf Programme, die auf entfernten Windows-Rechnern laufen.

RDS = **Remote Desktop Services** beschreibt die Fähigkeit von Windows Server, Terminal-Sessions und virtuelle Desktops bereitzustellen.

Regex = **Regular Expression** (regulärer Ausdruck) ist eine Zeichenkette, die der Beschreibung von Mengen von Zeichenketten mit Hilfe bestimmter syntaktischer Regeln dient. Sie werden unter anderem in der Suchen-Ersetzen-Funktion von Texteditoren gebraucht.

RSAT = **Remote Server Administration Tools** ist eine Sammlung von Microsoft-Tools für die Fernwartung.

Scopes = **Bereiche**, die man beim Einrichten eines DHCP-Servers unter Windows Server 2012 R2 festlegt.

Slat = **Second Level Address Translation** hilft bei der Virtualisierung mittels Hyper-V unter Windows.

SRV = **Service Resource Records** gibt in einem Netzwerk bekannt, welche IP-basierten Dienste zur Verfügung stehen.

SSTP = **Secure Socket Tunneling Protocol** ist ein Protokoll von Microsoft, das eine VPN-Verbindung aufbaut.

Uefi = **Unified Extensible Firmware Interface** ist der Nachfolger des Bios und bietet mehr Funktionen als dieser.

VHD = **Virtual-Hard-Disk** ist eine virtuelle Festplatte, also in der Regel eine Container-Datei für die Virtualisierungs-Software von Microsoft.

VHDX = **Virtual-Hard-Disk (enhanced)** ist eine Verbesserung des virtuellen Festplattenformats VHD.

VM = **Virtuelle Maschine** ist ein virtueller Rechner, der auf einem Hypervisor läuft.

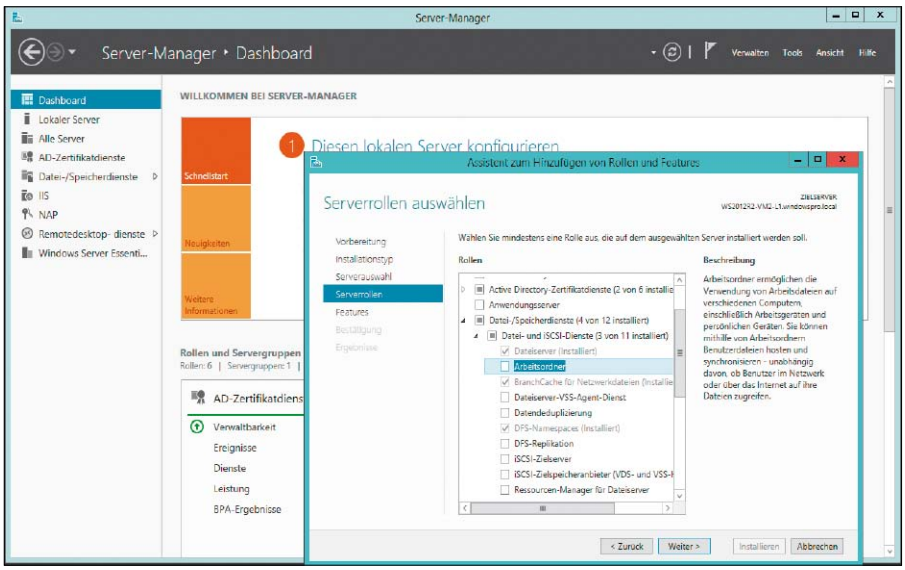
WMI = **Windows Management Instrumentation** ist eine Programm-Schnittstelle zur Administration und Wartung von Windows-Rechnern.

VPN = **Virtual Private Network** ist ein privates Netzwerk, das meist auch eine Verbindung über das Internet hat, aber dank Verschlüsselung als abhörsicher gilt.

Arbeitsordner in Windows 2012

Eine wichtige Neuerung von Windows Server 2012 R2 sind die Work Folder genannten Arbeitsordner. Sie ergänzen die File-Server-Dienste um die Synchronisierung von Dateien auch für mobile Geräte.

VON WOLFGANG SOMMERGUT



Arbeitsordner sind eine Erweiterung der Datei-/Speicherdienste und werden über den Server Manager hinzugefügt.

MICROSOFT LIESS DEN DATEIDIENSTEN im Lauf der letzten Updates zwar einige Neuerungen angedeihen, darunter die Classification Infrastructure oder Dynamic Access Control (*http://bit.ly/1gbo10b*), aber in wesentlichen Punkten gab es kaum Fortschritte. Bis heute beschränkt sich deshalb die Nutzung der File-Services weitgehend darauf, dass PCs über SMB freigegebene Ordner im Firmennetzwerk als gemeinsamen Speicher nutzen.

Dieses Szenario repräsentiert aber immer weniger die Anforderungen von Firmen, deren Mitarbeiter vermehrt von unterwegs mit diversen Endgeräten auf ihre Daten zugreifen möchten. Daher nimmt in vielen Unternehmen der unautorisierte Einsatz von Dropbox und anderen Consumer-Services zu. Wer eine Enterprise-taugliche Alternative (Beispiele über *http://bit.ly/1hwhYQq*)haben will, kann eine solche von verschiedenen Herstellern beziehen. Nur die Microsoft-Plattform selbst hatte bis dato kaum etwas zu bieten.

Zwar entwickelte Microsoft in der Vergangenheit eine Reihe von Produkten und Services zur Synchronisierung von Dateien. Genannt seien etwa Live Mesh, Live Sync oder zuletzt Onedrive. Diese Dienste richten sich jedoch nicht an professionelle Anwender, sondern an Privatanwender. Für professionelle Nutzer ist nur Onedrive Pro verfügbar. Dabei handelt es sich aber um einen Service in der Cloud, in die viele Firmen keine Daten übertragen möchten. Zudem ist es primär für die Synchronisierung von Sharepoint-Dokumenten gedacht.

Work Folders, also Arbeitsordner, benötigen keine Cloud

Work Folders (auch Arbeitsordner genannt) sind eine Lösung, die von Firmen selbst installiert wird (on premise) und keine Cloud-Services nutzen muss. Sie basieren auf einem eigens entwickelten Sync-Protokoll, das über verschlüsselte HTTP-Verbindungen mit Clients auch außerhalb des LANs kommuniziert. SMB ist hier also nicht im Spiel, und die Notwendigkeit für den Aufbau eines VPN-Tunnels entfällt. Als Dreh- und Angelpunkt für Work Folders dient ein neues Feature der Rolle „Datei/Speicherdienste“ namens „Arbeitsordner“. Sobald ein Benutzer in einem lokalen Work Folder eine Datei neu anlegt oder ändert, wird sie auf den Fileserver repliziert und dort als Kopie gespeichert. Dieser verteilt sie umgehend auf alle Endgeräte des jeweiligen Users, vorausgesetzt, auf ihnen wurde eine Partnerschaft mit dem Server eingerichtet.

Limitierungen der Version 1.0

In der ersten Ausführung der Work Folders kann pro Gerät und Benutzer nur eine Partnerschaft, also nur eine Verbindung, zum Server festgelegt werden. Außerdem beschränken sich Work Folders auf die Synchronisierung von Dateien individueller User. Team- oder Projektordner sind nicht vorgesehen, zudem bietet Microsoft derzeit noch keine Collaboration- und Sharing-Funktionen, wie sie etwa Novell in Filr (*http://bit.ly/1kN7yyW*) unterstützt. Eine weitere Limitierung besteht darin, dass ein Server 2012 R2 derzeit nur lokale Laufwerke für Work Folders nutzen kann. Obendrein ist

der Client-Support derzeit noch mager und beschränkt sich auf die Editionen von Windows 8.1. Allerdings kündigte Microsoft die Unterstützung für Windows 7 und das iPad an. Darüber hinaus gibt es bereits Erklärungen des Herstellers, wonach weitere Plattformen folgen sollen. Work Folder sind für andere Betriebssysteme relativ offen, weil die Mitgliedschaft der Geräte in einer AD-Domäne keine Bedingung ist. Sie gilt nur für den Server und die Benutzer.

Integration externer Endgeräte

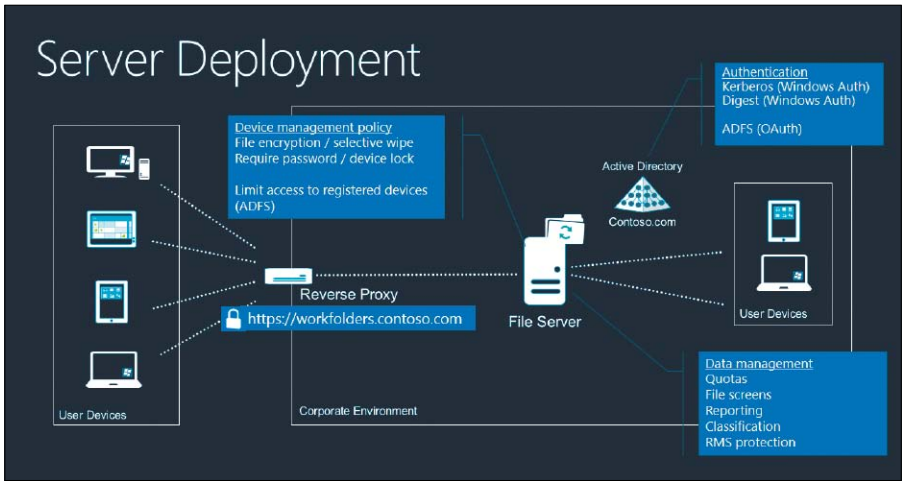
Sollen Endgeräte von außerhalb der Firewall ihre Daten über den Fileserver mit anderen Clients austauschen, dann geht das mit üblichen Mechanismen wie Reverse Proxy oder einfach über Port Forwarding in der Firewall. Eine weitere Voraussetzung ist eine entsprechende DNS-Konfiguration, so dass der Proxy- oder der Fileserver über eine im öffentlichen Internet gültige Adresse erreichbar ist.

Work Folders können auf mehrere Fileserver verteilt werden, beispielsweise wenn dezentrale Unternehmen den Sync-Dienst in verschiedenen Niederlassungen betreiben möchten. Nachdem jeder User nur eine Instanz der Arbeitsordner nutzen kann, muss sichergestellt sein, dass er dem richtigen Server zugeordnet wird. Diese Aufgabe lässt sich manuell durch die Vergabe von individuellen URLs an verschiedene Benutzergruppen erledigen.

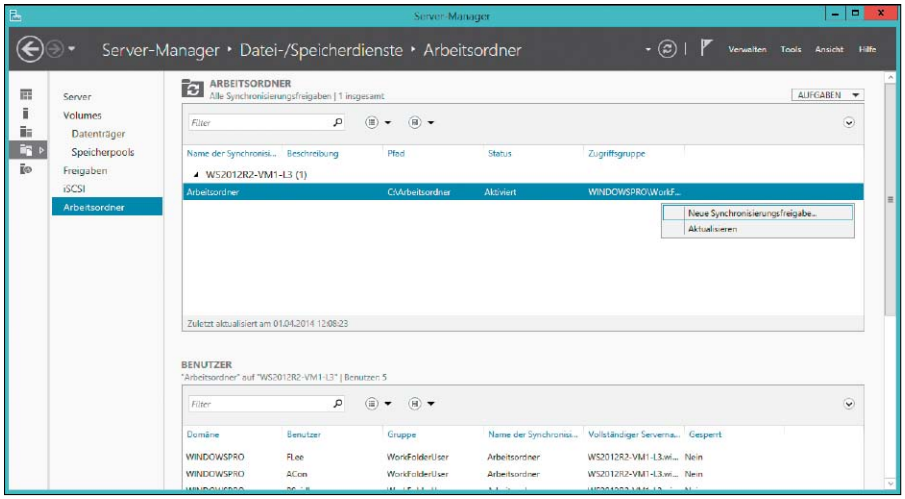
Deployment mehrerer Work-Folder-Server

Alternativ dient „Auto Discovery“ der selbstständigen Zuteilung von Benutzern zu Arbeitsordnern. Microsoft empfiehlt, den Zugriff auf Work Folders über eine jeweils eigene Security Group im AD zu regeln. Wenn ein Benutzer beim ersten Sync-Vorgang mit einem Work Folder verbunden wird, für die er keine Berechtigung besitzt, dann liest der Server im Rahmen des „Auto Discovery“ die korrekte URL aus einem eigens dafür angelegten AD-Attribut und gibt sie an den Client zurück. Der kann nun seine Daten mit dem zuständigen Server abgleichen. Dieser Mechanismus greift auch dann, wenn der Administrator bestimmten Benutzern die Rechte für einen Arbeitsordner entzieht, weil er sie auf einen anderen Work Folder migrieren möchte.

Die Zuordnung von Anwendern zu verschiedenen Work Folders kann erfolgen, um die Last auf mehrere Fileserver zu verteilen oder um eine dezentrale Firmenstruktur abzubilden. Ein weiterer Grund besteht darin, dass Richtlinien auf der Ebene der Arbeitsordner definiert werden. Wenn man beispielsweise für die Abteilung Finanzbuchhaltung die Verschlüsselung aller Dateien erzwingen möchte, dann würde man für sie einen eigenen Work Folder mit den entsprechenden Policies einrichten.



Die Dateien in Work Folders können auch mit Geräten außerhalb der Firmen-Firewall abgeglichen werden.



Nach der Installation der Arbeitsordner-Rolle legt man im nächsten Schritt eine Synchronisierungsfreigabe an.

Alle Zugriffsregeln des File-Servers gelten

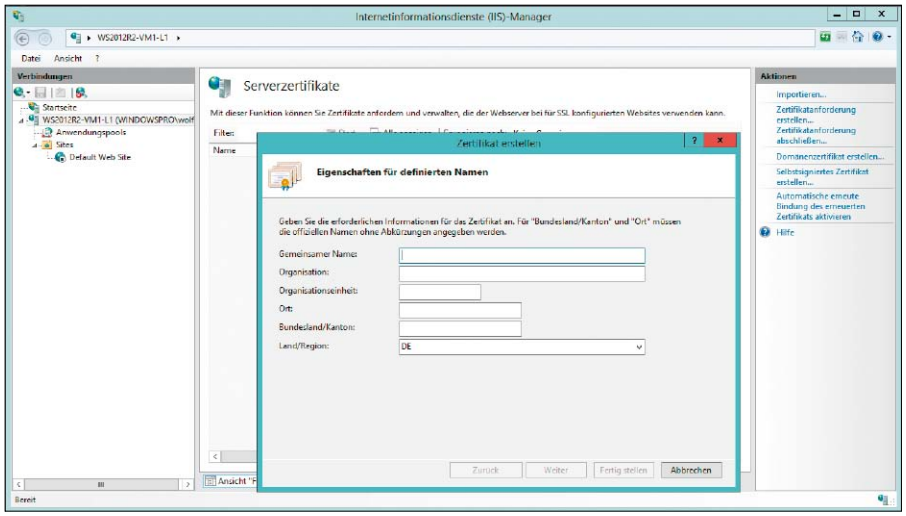
Neben den Richtlinien, die über die Arbeitsordner selbst vorgegeben werden, gelten weiterhin uneingeschränkt alle Restriktionen des Fileservers. So regeln die NTFS-Berechtigungen (*http://bit.ly/1i43cnQ*) die Zugriffsrechte auf die Dateien, und eventuelle Disk-Quotas (*http://bit.ly/1i43BGO*) beschränken den für Benutzer verfügbaren Plattenplatz auch dann, wenn die Dateien nicht über SMB, sondern via Synchronisierung auf den Server gelangen.

Nachdem Work Folders auf die bestehende Infrastruktur für Fileserver aufsetzen, stehen ihnen auch andere ergänzende Dienste zur Verfügung. So lassen sich die Rights Management Services (RMS) nutzen, um die Weitergabe von vertraulichen Dateien an Unbefugte zu verhindern, etwa wenn sie auf private Geräte von Mitarbeitern synchronisiert werden.

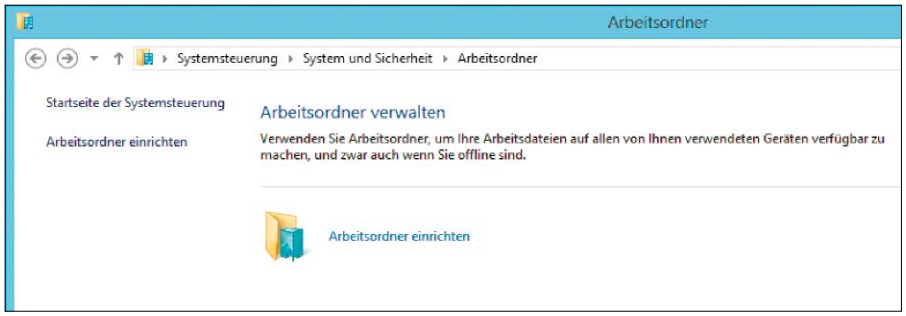
Eine weitere Konsequenz aus der Integration der neuen Sync-Funktionen mit herkömmlichen Netzfreigaben besteht darin, dass der Inhalt von Arbeitsordnern entweder auf Clients repliziert oder von diesen über SMB genutzt werden kann. Ältere Windows-PCs, die Work Folders nicht unterstützen, können daher auf herkömmliche Weise Dateien lesen und schreiben, die von Kollegen auf den Server synchronisiert wurden.

Versionskonflikte und Replikationsprobleme

Im Vergleich zum traditionellen Zugriff auf File-Shares via SMB konfrontiert die Synchronisierung sowohl User als auch Administratoren mit spezifischen Eigenheiten. Dazu gehören Replikationskonflikte, wenn eine Datei auf mehreren Geräten gleichzeitig verändert wird. In diesem Fall setzt sich der letzte Schreibzugriff durch und andere Versionen des Doku-



Wenn alle Clients Mitglied in der Domäne sind, dann reicht ein SSL-Zertifikat, das man mit der CA des AD ausstellt.



Die Systemsteuerung von Windows 8.1 enthält ein Applet zur Client-seitigen Konfiguration der Arbeitsordner.

ments (bis zu 100) werden beibehalten (und markiert). Der Benutzer muss dann selbst entscheiden, wie er den Konflikt auflöst.

Aus der Sicht von Administratoren gilt es zu bedenken, dass ein Sync-Mechanismus wie jener von Work Folders genau Buch darüber führt, wann welche Version einer Datei auf welche Geräte übertragen wurde. Microsoft verwendet zu diesem Zweck wie in AD oder Exchange eine (angepasste) Jet-Datenbank (auf den Clients und auf dem Server).

Und genau wie bei der AD-Replikation droht Chaos, wenn man durch einen Restore des gesamten Systems das Rad der Zeit zurückdreht oder alte Versionen von Dateien aus externen Quellen einspielt.

Work Folders als Ersatz von Offline-Files

Es liegt auf der Hand, dass Arbeitsordner als (überfällige) Nachfolger von Offline-Dateien zu betrachten sind. Letztere bieten nichts, was Work Folders nicht besser könnten. Aber auch die beiden anderen in die Jahre gekommenen Techniken, die Microsoft unter User State Virtualization (*http://bit.ly/1hjLBJ1*) zusammenfasst, stehen zu Disposition. Es handelt sich dabei um die Ordnerumleitung und Roaming Profiles. Rein technisch lassen sich Work Folders und Ordnerumleitung miteinander kombinieren, aber Microsoft rät davon ab, dies zu tun. Tatsächlich gibt es dafür keinen vernünftigen Grund, denn Arbeitsordner lösen das Problem der dezentralen Datenhaltung, indem sie alle Änderungen auf den Server replizieren. Gleichzeitig erlauben sie ein (Offline-)Arbeiten mit lokalen Kopien der Dateien und die Integration von Plattformen anderer Hersteller.

Ablöse von Roaming Profiles zusammen mit UE-V

Roaming Profiles dagegen gleichen nicht nur die Benutzerdaten zwischen dem Server und Windows-PCs ab, sondern übertragen als Teil des Profils auch die individuellen Einstellungen. Diese Aufgabe können Work Folders zwar nicht übernehmen, aber Microsoft bietet zu diesem Zweck eine eigene Software namens UE-V. Diese wurde erst kürzlich in der stark erweiterten Version 2.0 veröffentlicht.

Während jedoch alle unterstützten Clients Work Folders nutzen können, sobald ein Server 2012 R2 im Netz ist, bleibt UE-V 2.0 als Teil des MDOP 2013 R2 (*http://bit.ly/1k7tqGX*) jenen Kunden vorbehalten, die eine Software Assurance abgeschlossen haben.

Praxis: Arbeitsordner installieren

Nachdem Arbeitsordner herkömmliche Fileserver in die Lage versetzen sollen, sowohl firmeneigenen als auch privaten Geräten innerhalb und außerhalb der Firewall Zugriff auf Dateien zu gewähren, sieht dieses Feature auch komplexe Deployment-Varianten vor. Dazu zählen Multi-Site- und Multi-Server-Konfigurationen, Autodetect von Arbeitsordnern oder die Nutzung eines Reverse Proxy inklusive ADFS (*http://bit.ly/1izIMB1*).

Für die Evaluierung von Work Folders und für kleinere Umgebungen reicht indes ein Setup, das nur PCs unter Windows 8.1 bedient, die Mitglied einer Domäne sind, und das mit einem einzelnen Fileserver auskommt. Die folgende Beschreibung orientiert sich an solchen bescheidenen Anforderungen und beschränkt sich daher etwa auf die Verwendung eines SSL-Zertifikats, das von den AD-Zertifikatsdiensten ausgestellt wurde.

Der einfachste Teil bei der Einrichtung von Work Folders ist die Installation der benötigten Server-Komponenten. Sie erfolgt erwartungsgemäß über den Server Manager, wo man im Wizard zum „Hinzufügen von Rollen und Features“ im Zweig unterhalb von „Datei-/Speicherdienste“ die Option „Arbeitsordner“ wählt. Bei dieser Gelegenheit wird auch „IIS Hostable Web Core“ („Hostfähiger Webkern für Internetinformationsdienste“) installiert.

Synchronisierungsfreigaben: So legen Sie sie an

Im nächsten Schritt legt man eine neue Synchronisierungsfreigabe an, unterhalb der später die Ordner der für die einzelnen Benutzer liegen. Auch diese Aufgabe erledigt man im Server Manager, und zwar indem man über die linke Navigationsleiste die Seite für Datei-/Speicherdienste öffnet und dort zu „Arbeitsordner“ wechselt. Aus dem Menü „Aufgaben“ startet man anschließend den Wizard „Neue Synchronisierungsfreigabe“.

Dieser belehrt auf der Seite „Vorbereitung“ darüber, dass man den Speicher für Work Folders auf einem NTFS-Volume bereitstellen muss und bevorzugt AD-Sicherheitsgruppen nutzen sollte, um die Zugriffsrechte für Work Folders zu verwalten. Letzteres ist besonders dann empfehlenswert, wenn man mehrere Arbeitsordner anlegt. Dies kann man bei Bedarf nun nachholen, bevor man den Wizard fortsetzt.

Speicherort und Namen für die Synchronisierungsordner

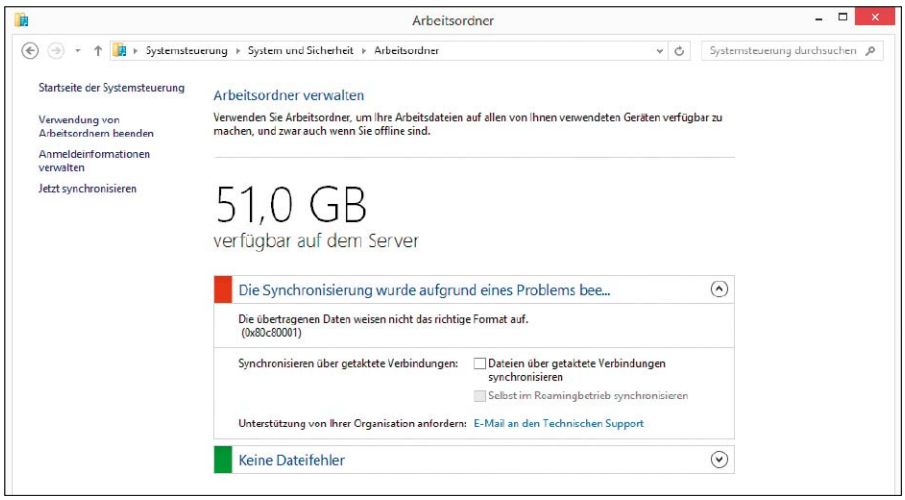
In den folgenden Schritten wählt man erst den Server und Pfad für die Synchronisierungsfreigabe (entweder ein bestehendes SMB-Share

oder ein lokales Laufwerk) und danach die Namenskonvention für die Benutzerverzeichnisse. Diese werden automatisch unterhalb des Arbeitsordners angelegt und bestehen entweder nur aus dem Benutzernamen alleine (Option „Benutzeralias“) oder aus Benutzername plus „@<Domäne>“.

Die zweite Variante wird man dann wählen, wenn Benutzer aus mehreren Domänen die Sync-Freigabe nutzen, weil auf diese Weise keine Namenskonflikte auftreten können. In diesem Dialog kann man zusätzlich bestimmen, dass nicht alle Verzeichnisse unterhalb des Benutzerordners synchronisiert werden, sondern nur die angegebenen.

Nach der Vergabe eines Namens für den Arbeitsordner legt man fest, wer darauf zugreifen darf. Zu diesem Zweck wählt man die AD-Benutzergruppe aus, die man dafür zuvor angelegt hat. Zum Abschluss aktiviert man noch die gewünschten Geräterichtlinien, über die man etwa die Verschlüsselung der synchronisierten Daten erzwingen kann.

Bei der interaktiven Client-Konfiguration kann man den Speicherort für den Sync-Ordner ändern.



Beim Synchronisierungs-Fehler 0x808001 sollte man das Update KB2887595 auf dem Server installieren.

SSL-Zertifikat anfordern und an Port 443 binden

Die Server-seitige Konfiguration erfordert schließlich noch die Installation eines SSL-Zertifikats, weil die Kommunikation zwischen Clients und Server durchgängig über HTTPS erfolgt. Aus diesem Grund wird „IIS Hostable Web Core“ zusammen mit der Arbeitsordner-Rolle installiert.

Verschiedene Anleitungen wie jene auf diesem Technet-Blog (*http://bit.ly/1lM8J3a*) bewältigen diese Aufgabe mit Powershell oder mit Kommandozeilen-Tools wie „netsh.exe“, weil der IIS Manager mit Web Core nicht eingerichtet wird. Im Allgemeinen ist es aber einfacher, dieses grafische Tool am Workfolder-Server nachzuinstallieren und die Zertifikatsverwaltung damit zu erledigen. Zu diesem Zweck öffnet man ein Powershell-Fenster mit administrativen Rechten und gibt diesen Befehl ein:

```
Install-WindowsFeature Web-Mgmt-
  Console
```

Im IIS Manager kann man sowohl Zertifikate einbinden, die man von externen CAs erworben hat, als auch selbst signierte Zertifikate ausstellen. Eine weitere Option besteht darin, ein Zertifikat von den AD-Zertifikatsdiensten anzufordern. Ein solches reicht aus, wenn alle Clients Mitglied der Domäne sind.

Domänenzertifikat ausstellen

Dazu wählt man in der linken Strukturdarstellung den Server aus und startet anschließend das Applet „Serverzertifikate“. Im rechten Fenster taucht dann unter anderem die Option „Domänenzertifikat erstellen“ auf. Sie öffnet einen Dialog, in den man alle nötigen Angaben für das Zertifikat eingeben muss.

Nach dem erfolgreichen Ausstellen des Zertifikats wird es automatisch in den lokalen Speicher importiert. Nun muss es noch an den SSL-Port 443 gebunden werden. Dazu wählt man in der Baumstruktur „Default Web Site“ aus, worauf dann rechts der Menüpunkt „Bindungen“ auftaucht. Über ihn öffnet man einen Dialog, in dem man über Pull-down-Menüs den Port 443 und das installierte Zertifikat auswählen kann.

Clients für Synchronisierung einrichten

Der letzte Schritt besteht darin, die Clients für die Synchronisierung zu vorzubereiten. Neben der zentralen Konfiguration über Gruppenrichtlinien gibt es die Möglichkeit, diese Aufgabe den Benutzern selbst zu überlassen. Für diesen Zweck existiert in der Systemsteuerung von Windows 8.1 unter „System und Sicherheit → Arbeitsordner“ ein Applet namens „Arbeitsordner einrichten“.

Führt man dieses aus, dann verlangt es im ersten Dialog die Eingabe einer Mailadresse. Aus dieser entnimmt es den Namen der Domäne und sucht im DNS einen Eintrag in der Form „workfolders.<meine-domain.com>“, der auf die IP des Workfolder-Servers verweist. Will man den Client auf diesem Weg einrichten, dann muss man daher im DNS erst ein entsprechendes Alias (CNAME) für den Server anlegen, der die Arbeitsordner bereitstellt. Alternativ kann man statt der Mailadresse direkt die URL eingeben, die man den Benutzern zuvor etwa per Mail zuschickt.

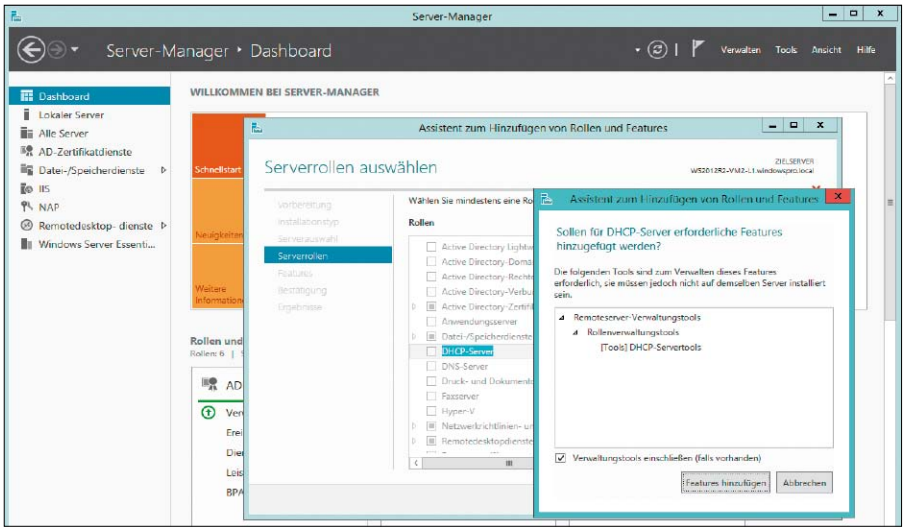
Nach der erfolgreichen Verbindung mit dem Server bietet der Wizard die Möglichkeit an, das lokale Verzeichnis für den Arbeitsordner zu verändern. Der Vorgabewert ist „%USERPROFILE%\Work Folders“. Nach Abschluss der Konfiguration versucht Windows sofort, die Dateien im betreffenden Verzeichnis mit dem Server abzugleichen.

Dabei kann jedoch der Fehler 0x80c80001 auftreten, wonach die übertragenen Daten nicht das richtige Format aufweisen. In diesem Fall liegt das Problem nicht bei den Dateien, vielmehr handelt es sich um einen Bug des Systems, den man durch Einspielen von KB2887595 (Infos über *http://bit.ly/1lM8J3a*) auf dem Server beheben kann. ■

DHCP-Dienst in Server 2012 (R2)

Ein DHCP-Server gehört schon lange zum Lieferumfang von Windows Server. Die Version 2012 (R2) bringt nun wichtige Neuerungen für die Verwaltung der IP-Konfiguration, aber auch ein verändertes Setup.

VON WOLFGANG SOMMERGUT



Die Installation des DHCP-Servers erfolgt als Hinzufügen einer Rolle im Server Manager.

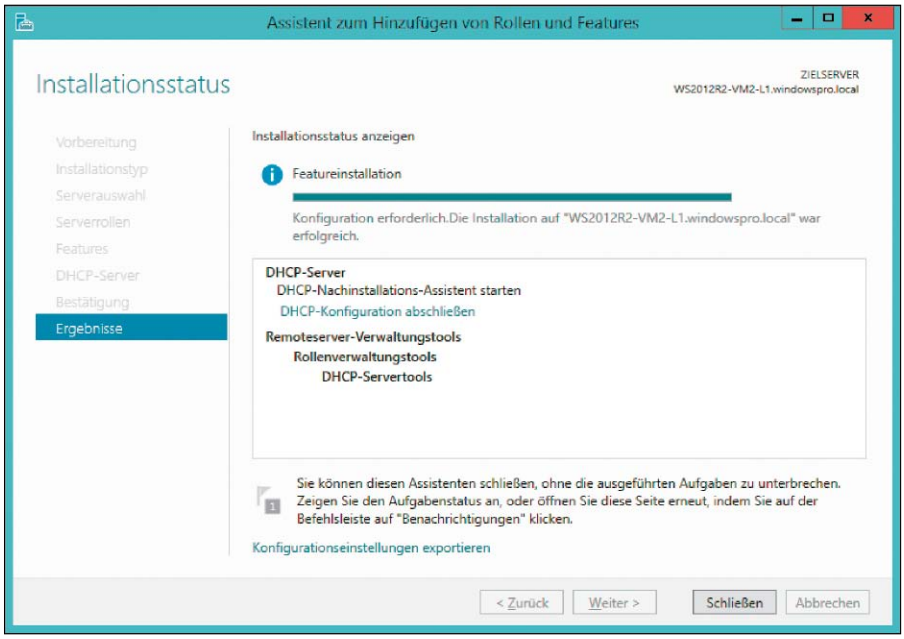
SERVER FÜR DAS Dynamic Host Configuration Protocol (DHCP) gelten als Allerweltsprodukte, weil diverse Netzwerkgeräte oder verschiedene kostenlose Implementierungen diesen Dienst erbringen können. Dennoch spricht einiges dafür, Windows Server für diesen Zweck einzusetzen. Vor allem die einfache Integration mit dem DNS von Active Directory empfiehlt die Nutzung vom Windows Server. Sie sorgt dafür, dass ein DHCP-Client automatisch seinen DNS-Eintrag aktualisiert, wenn sich die IP-Konfiguration ändert. Zudem gibt es zwei weitere wichtige Enterprise-Features: die Zuweisung von Adressen auf Basis von Richtlinien sowie die Failover-Konfiguration.
Bevor man den DHCP-Server auf einem Windows-Server aktiviert, sollte dieser zumindest über eine statische IP-Adresse verfügen. Darüber hinaus empfiehlt Microsoft, dass er in Umgebungen, die über ein Active Directory (AD) verwaltet werden, Mitglied in einer Domäne sein sollte. Prinzipiell lässt sich zwar auch ein Workgroup-Server nutzen, dieser stellt aber seine Arbeit ein, sobald ein im AD autorisierter DHCP-Server im gleichen Subnet auftaucht.

Einfache und schnelle Installation über Server Manager

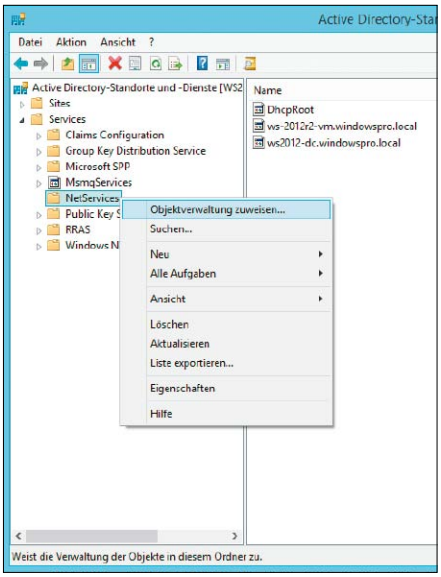
Wie bei vielen anderen Rollen, beispielsweise den Terminaldiensten, weicht in Windows Server 2012 das vormals eigenständige Setup dem neuen Server Manager, der als zentrales Tool für das Hinzufügen von Rollen und Features dient. Die eigentliche Installation des DHCP-Servers ist trivial und besteht darin, dass man aus dem Menüpunkt „Verwalten“ den Befehl „Rollen und Features hinzufügen“ ausführt. Im anschließenden Wizard wählt man die Serverrolle „DHCP“ und durchläuft die restlichen Schritte bis zur Installation. Da der Server Manager auch entfernte Rechner konfigurieren kann, lässt sich zum Beispiel ein Server mit einer Core-Installation von einer Workstation aus mit Hilfe der Remote Server Administration Tools (RSAT) einrichten.
Der Wizard endet mit dem Hinweis, dass die Konfiguration der eben installierten Rolle erforderlich sei, und enthält einen entsprechenden Link, um einen weiteren Assistenten zu starten. Bei der noch ausstehenden Konfiguration geht es nicht um die weitere Einrichtung des DHCP-Servers durch das Anlegen von Adressbereichen oder dergleichen, vielmehr steht nur die Autorisierung des DHCP-Servers im Active Directory an.

Autorisieren des DHCP-Servers im Active Directory

Der für diese Aufgabe zuständige Wizard bietet die Möglichkeit, alternativ zum aktuellen Benutzer die Anmeldedaten eines anderen Kontos einzugeben. Für das Autorisieren des DHCP-Servers sind nicht unbedingt jene eines Administrators erforderlich, vielmehr lässt sich diese Aufgabe delegieren, indem man in „Active Directory-Standorte und -Dienste“ das Kontextmenü von „Netservices“ öffnet und den Befehl „Objektverwaltung zuweisen“ ausführt. Das Autorisieren eines DHCP-Servers kann



Nach Abschluss der Installation kann man direkt mit dem Wizard zur Autorisierung des DHCP-Servers fortfahren.



Das Autorisieren eines DHCP-Servers lässt sich in „Active Directory-Standorte und -Dienste“ an Benutzer delegieren. Admin-Rechte sind so nicht direkt nötig.

alternativ auch über Netsh.exe oder das MMC-Snap-in erfolgen, die beide auch in der Lage sind, eine Autorisierung aufzuheben. Um einen Server hinzuzufügen gibt man

```
netsh dhcp add server <server-
 name oder IP>
```

ein, um eine Autorisierung zu entfernen, ersetzt man *add* durch *delete*.

DHCP-Server auf einem Domänen-Controller ausführen

Es ist zwar möglich, einen DHCP-Server auf einem Domain Controller zu installieren, aber diese Konstellation entspricht nicht den Empfehlungen von Microsoft. Gerade in kleineren Umgebungen wird man sie aber trotzdem häufig wählen.

In diesem Fall findet sich in der Ereignisanzeige die Warnung (Event-ID 1056), dass der DHCP-Dienst über keine Anmeldeinformationen verfügt, die für die Verwendung mit dynamischen DNS-Registrierungen konfiguriert sind. Damit wird verhindert, dass der DHCP-Server für das DNS-Update das Computer-Konto des Domain Controllers nutzt.

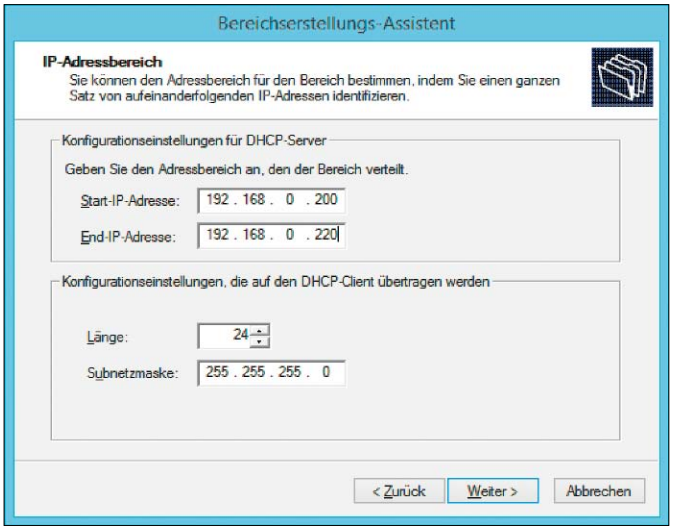
Die Lösung besteht darin, dass man ein eigenes Konto zur Ausführung des DHCP-Servers anlegt. Dieses benötigt keine besonderen Privilegien. Die „DNSCredentials“ gibt man im MMC-Snap-in für DHCP ein, indem man im Knoten „IPv4“ des betreffenden Servers das Kontextmenü öffnet und dort den Dialog „Eigenschaften“ anzeigt. Unter dem Reiter „Erweitert“ klickt man auf den Button „Anmeldeinformationen“ und gibt die Daten des gewählten Benutzerkontos ein.

Neue Bereiche einrichten

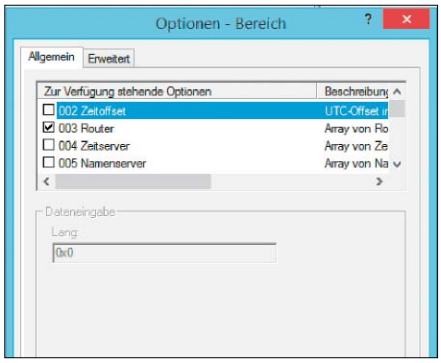
Die bisher beschriebenen Schritte haben alle wesentlichen Voraussetzungen für die Bereitstellung des DHCP-Dienstes geschaffen. Obzwar der Service nun verfügbar ist, nimmt er seine Aufgaben aber noch nicht wahr und teilt den Clients keine IP-Konfiguration zu. Zu diesem Zweck müssen zuerst Adressbereiche eingerichtet werden.

Für die Verwaltung des DHCP-Servers ist wie in der Vergangenheit das MMC-Snap-in „Dhcpmgmt.msc“ zuständig. Die Konfiguration beginnt wie üblich damit, dass man Bereiche (Scopes) definiert, für die der DHCP-Server zuständig ist. Dabei kann er mittels Multihoming (*http://bit.ly/1hEIoWx*) auch mehrere Subnets bedienen, wenn der Server mit der nötigen Zahl an Netzwerkadaptern ausgestattet ist und diese mit den jeweiligen Segmenten verbunden sind. Alternativ kann er mit Hilfe eines Relay Agents die Client-Anfragen aus mehreren Subnets beantworten.

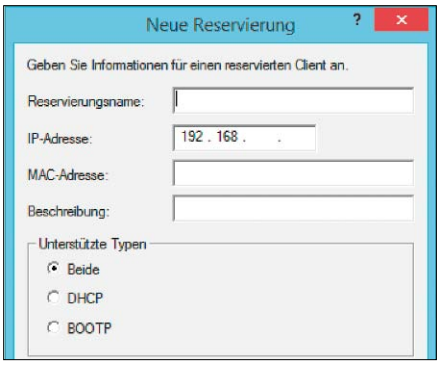
Der Befehl zum Anlegen von Bereichen findet sich im Kontextmenü des Servers. Er startet einen Wizard, der die meisten Einstellungen für einen neuen Bereich abfragt. Dabei handelt es sich nicht nur um Blöcke von Adressen, wie die unglückliche Übersetzung „Bereich“ nahelegt. Der englische Begriff „Scope“ steht vielmehr für den „Geltungsbereich“, in dem bestimmte Einstellungen wirksam sind. Dazu zählen auch die Gültigkeitsdauer von Leases oder die DNS-Konfiguration. Werte, die man innerhalb eines Bereichs festlegt, setzen jene außer Kraft, die man global für den ganzen DHCP-Server definiert hat.



Das Anlegen eines Bereichs erfolgt über den dafür zuständigen Wizard, in dem man auch Adressen ausschließen kann.



In den Bereichsoptionen kann man weitere Einstellungen der IP-Konfiguration festlegen, etwa Zertifikarte, DNS-Server oder Gateways.



DHCP-Reservierungen eignen sich besonders für Server oder Netzdrucker und stellen sicher, dass diese Geräte immer die gleiche IP erhalten.

Adressbereiche ausschließen

Das Einrichten eines neuen Bereichs beginnt mit der Eingabe einer Start- und End-IP, die den Adressraum begrenzen. Hinzu kommt noch die Festlegung der Netmask. Im nächsten Schritt kann man einen oder mehrere Adressbereiche ausschließen, weil sie beispielsweise für Server oder Netzwerkgeräte reserviert bleiben und nicht dynamisch vergeben werden sollen. Bei diesem Schritt besteht auch die Möglichkeit, eine Verzögerung festzulegen, mit der der DHCP-Server auf Client-Anfragen reagieren soll. Sie wird vor allem dann benötigt, wenn man Adressbereiche zwischen mehreren Servern aufteilt („Split Scope"), um eine höhere Ausfallsicherheit zu erzielen. Der verzögert reagierende Server kommt nur dann zum Zug, wenn der primäre Server zu langsam oder gar nicht antwortet. Durch die neue Failover-Option in Windows Server 2012 verliert diese Konfiguration aber an Bedeutung. Im dann folgenden Dialog entscheidet man sich für den Zeitraum, währenddessen ein Client eine IP-Adresse verwenden kann, bevor er den DHCP-Server erneut kontaktieren muss. Voreingestellt sind acht Tage, die man verkürzen kann, wenn man es im betreffenden Subnet vor allem mit mobilen Geräten zu tun hat. Zum Abschluss bietet der Wizard an, einen weiteren Assistenten zu starten, mit dem sich verschiedene Einstellungen wie Standard-Gateway, DNS- und WINS-Server festlegen lassen.

Reservierungen anstelle statischer IP-Adressen

Die nun abgeschlossene Basiskonfiguration eines Bereichs ignoriert zwei DHCP-Features, nämlich die Reservierungen und die bereits erwähnten, neu eingeführten Richtlinien. Erstere dienen dazu, bestimmten DHCP-Clients immer die gleiche Adresse zuzuweisen. Bevorzugte Kandidaten für diese Funktion sind Server oder Drucker. Die dauerhafte Zuordnung der IP erfolgt über die MAC-Adresse. Die Vergabe von festen IP-Adressen für Server mittels DHCP hat den Vorteil, dass sich auf diese Weise ein zentrales IP-Management realisieren lässt. Man kann unter einer Oberfläche nachvollziehen, welche Adressen an welche Clients vergeben wurden. Beim Wechsel eines Rechners oder Druckers in ein anderes Subnet reicht es zudem, die Reservierung im DHCP-Server zu ändern und das betreffende Gerät neu zu starten und über *ipconfig /renew* die aktuelle Adresse anzufordern. Das Editieren der Netzwerkeinstellungen auf jedem einzelnen Gerät mit fester Adresse entfällt damit.

Dennoch ziehen es viele Admins vor, für Server lieber statische IP-Adressen zu verwenden. Hauptgrund dafür ist die Sorge vor einem Ausfall des DHCP-Dienstes, wodurch wichtige Anwendungen nicht mehr erreichbar sein könnten. Durch die neue Failover-Funktion lässt sich aber eine hohe Ausfallsicherheit erreichen, die solche Bedenken zerstreuen sollte.

Clients über Richtlinien filtern

Die in einem Bereich definierten Adressen und Optionen gelten prinzipiell für alle Clients, die den DHCP-Server anfragen. Mit Hilfe der neuen Richtlinien kann man aber die Endgeräte nach verschiedenen Kriterien, etwa nach Hersteller- und Benutzerklasse, Client-Kennung oder MAC-Adresse filtern und für sie spezifische Konfigurationen nutzen.

Auf diese Weise kann man zum Beispiel bestimmten Gerätetypen auf Basis der Herstellerklasse einen ausgewählten Teil des gesamten Adressbereichs zuweisen. Darüber hinaus besteht die Möglichkeit, spezifischen Clients andere DNS- oder WINS-Server zuzuordnen oder für sie die Gültigkeitsdauer einer Lease im Vergleich zu jener des Scopes zu verkürzen oder zu verlängern.

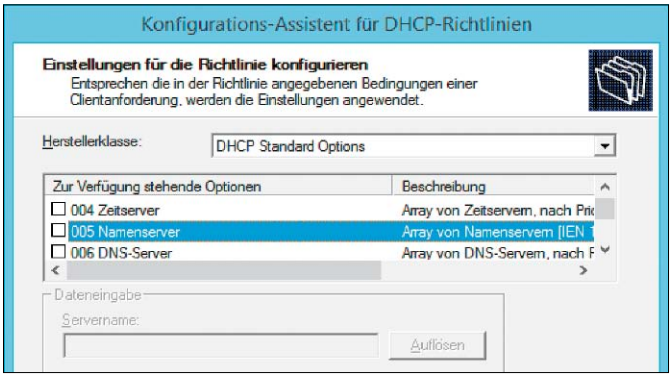
Wie für andere Optionen gilt auch für Richtlinien, dass jene innerhalb eines Bereichs Priorität haben gegenüber solchen, die auf der Ebene des Servers festgelegt wurden. Dort lassen sich zwar diverse Optionen modifizieren, aber aus naheliegenden Gründen kann man an dieser Stelle keinen eingeschränkten Adressbereich bestimmen.

Ausfallsicherheit konfigurieren

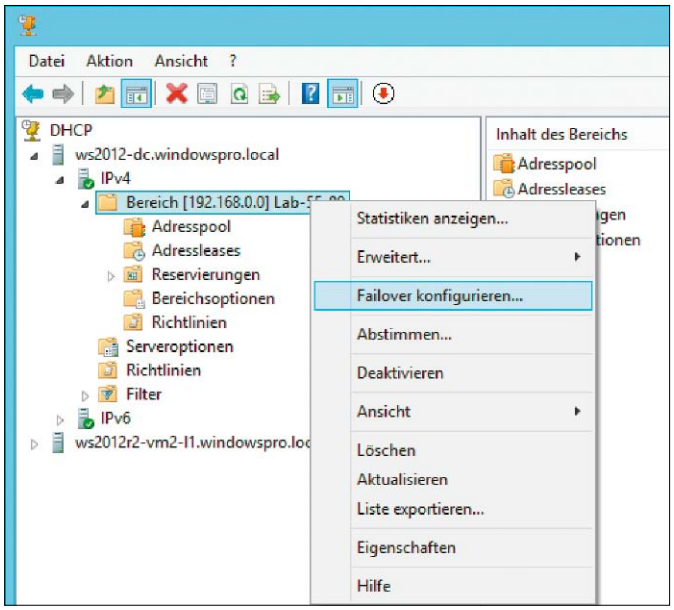
Ein DHCP-Server erbringt kritische Netzwerkdienste, deren Ausfall dazu führen kann, dass Benutzer keinen Zugriff mehr auf ihre Anwendungen und Daten haben. Es ist unangenehm genug, wenn Leases für Clients nicht verlängert werden, weil sie keinen DHCP-Server erreichen können. Hat man sich jedoch entschieden, auch die IP-Konfiguration der Server über DHCP zu verwalten, in der Regel über Reservierungen, dann sollte man seinem DHCP-Service vertrauen können.

Daher bot Windows Server schon in der Vergangenheit Mechanismen, um eine hohe Verfügbarkeit zu gewährleisten. Diese existieren weiterhin, aber sie weisen einige Defizite auf, so dass Microsoft in den aktuellsten Versionen seines Betriebssystems eine neue Failover-Option einführte.

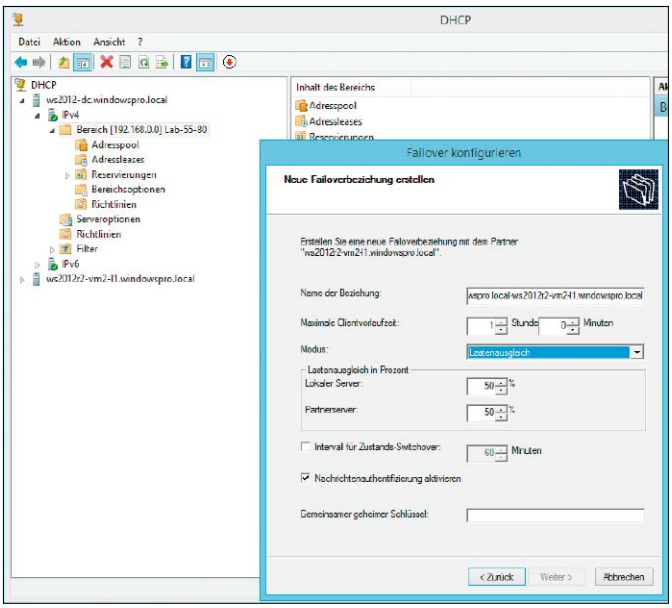
Eine der bisherigen Möglichkeiten besteht in der Einrichtung eines Failover-Clusters, so dass bei einem Defekt an einem Server ein anderer dessen DHCP-Dienst übernehmen kann. Solche Rechnerverbünde sind jedoch relativ aufwendig einzurichten und mit erheblichen (Storage-)Kosten verbunden.



Die neuen Richtlinien erlauben die Definition separater Einstellungen für Clients, die den festgelegten Kriterien entsprechen.



Die Einrichtung einer Failover-Beziehung erfolgt auf der Ebene von Bereichen, so dass ein Server mehrere Partnerschaften eingehen kann.



Die Failover-Konfiguration unterscheidet zwischen den Modi „Lastenausgleich“ und „Hot Standby“, die jeweils ihre Vor- und Nachteile haben.

Ein weiteres etabliertes Verfahren setzt direkt bei der DHCP-Rolle an und verteilt die Adressen eines Bereichs auf zwei Server („Split Scope“). Ist einer von beiden nicht mehr erreichbar, dann reagiert der andere auf Anfragen der Clients, indem er IP-Adressen aus seinem Teilbereich vergibt. Die bei Split Scope typische 70/30-Aufteilung eines Bereichs scheitert oft daran, dass Unternehmen nicht 30 Prozent der Adressen eines Subnets in Reserve halten können, nur um sich für den Ausfall des primären DHCP-Servers abzusichern.

DHCP-Synchronisierung zwischen zwei Servern

Die Nachteile der beiden Optionen bewog Microsoft dazu, mit Server 2012 einen flexibleren Failover-Mechanismus einzuführen. Dieser ist ein Feature der DHCP-Rolle und erlaubt die Kopplung von zwei DHCP-Servern in verschiedenen Konfigurationen. Dabei schöpfen beide Server aus dem gesamten Pool eines Bereichs, sie operieren also ohne Split Scope. Damit keine Konflikte auftreten und Adressen nicht doppelt vergeben werden, synchronisieren sie alle Informationen über die vergebenen Leases. Der Zusammenschluss bezieht sich auf einen oder mehrere Bereiche, so dass ein DHCP-Server, der mehrere Subnets betreut, für jedes davon eine andere Partnerschaft eingehen kann. Daher lassen sich mit diesem Feature etwa auch Hub-and-Spoke-Topologien einrichten. Die Einrichtung des DHCP-Failovers beginnt damit, dass man auf einem Server die benötigten Bereiche definiert. Auf dem Partner-Server muss man dagegen die gleichen Bereiche nicht nochmal anlegen, weil er seine Konfiguration über die Synchronisierung mit dem ersten Server erhält.

Im nächsten Schritt verbindet man sich im MMC-Snap-in für DHCP mit dem Server, dessen Bereiche durch einen zweiten Rechner abgesichert werden sollen. Dort öffnet man den Zweig unterhalb von IPv4, weil das Failover-Feature nur die alte Version des Internet-Protokolls unterstützt. Dort wählt man aus dem Kontextmenü des gewünschten Bereichs den Befehl „Failover konfigurieren“.

Er startet einen Wizard, der zuerst die erneute Auswahl von Bereichen erlaubt, die er alternativ aus dem Kontextmenü von IPv4 aufrufen kann. In diesem Fall könnte man die Entscheidung für Bereiche nicht schon vorher treffen. Im nächsten Dialog gibt man den vorgesehenen Partner-Server ein.

Einrichtung der Failover-Beziehung

Die Konfiguration der wesentlichen Parameter erfolgt dann im dritten Schritt. Dort vergibt man einen Namen für die Server-Beziehung und legt den Wert für die „Maximale Clientvorlaufzeit“ fest. Sie bestimmt, um welches Intervall die Client-Leases von einem Server vorübergehend verlängert werden dürfen, wenn der Partner nicht erreichbar ist.

Die Failover-Konfiguration für DHCP kennt zwei Modi, die sich über das entsprechende Pulldown auswählen lassen: „Lastenausgleich“ und „Hot Standby“. Beim Lastenausgleich vergeben beide Server gleichzeitig Adressen aus demselben Pool, wobei man über die Gewichtung der Server steuern kann, wie die Arbeitslast zwischen ihnen verteilt wird. „Hot Standby“ sieht sowohl einen aktiven als auch passiven Partner vor, wobei wie bei Split Scope ein bestimmter Teil des Adress-Pools für Failover reserviert werden muss. Allerdings entfällt hier die manuelle Festlegung des Standby-Bereichs, es reicht der Prozentwert für die zurückgelegten IP-Adressen.

Lastenausgleich versus Hot Standby

Microsoft empfiehlt den Lastenausgleich, wenn sich beide Server am gleichen Standort befinden. Dagegen eignet sich Hot Standby besonders dann, wenn in Niederlassungen oder Außenstellen eigene DHCP-Server vorhanden sind und diese durch einen Failover-Partner in der Zentrale abgesichert werden sollen. Aufgrund der meist beschränkten Netzwerkverbindung operieren die dezentralen Server normalerweise unabhängig vom Standby-Server, der nur im Notfall einspringt.

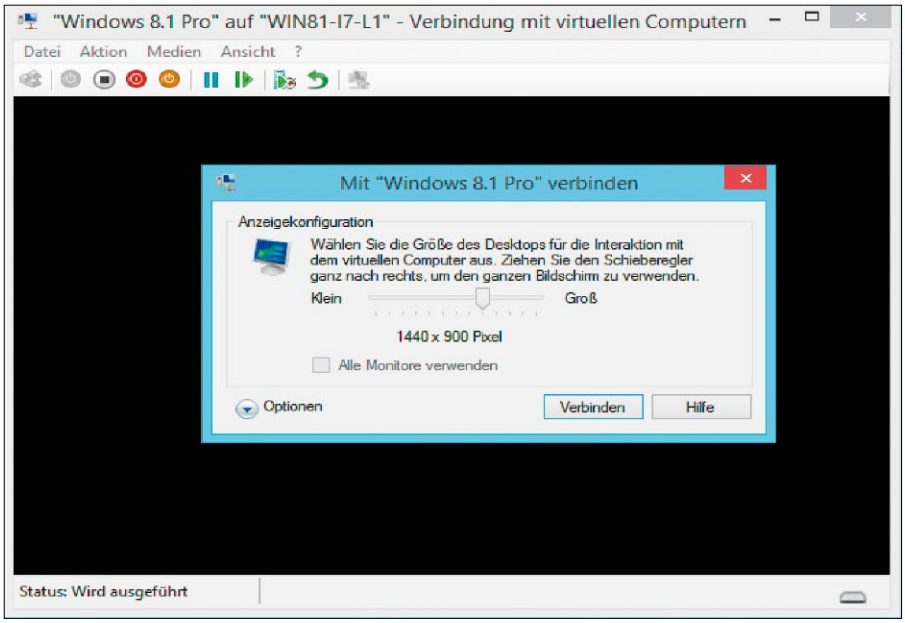
Die Einstellung „Intervall für Zustands-Switchover“ legt den Zeitraum fest, nach dessen Verstreichen ein DHCP-Server in den Zustand „Partner Down“ versetzt wird. Danach vergibt er IP-Adressen, ohne zuvor den anderen Server zu kontaktieren. Diese Option ist standardmäßig nicht aktiviert, so dass man den Server manuell in diesen Status versetzen muss.

Schließlich kann man die Failover-Partnerschaft so konfigurieren, dass sich beide Server für die Synchronisierung authentifizieren müssen. Wenn man das möchte, wählt man die zuständige Option aus und gibt zusätzlich ein Passwort ein, das beide Seiten verwenden. ■

Hyper-V: Besser als die anderen?

Windows 8.1 bringt eine neue Version von Hyper-V, der Virtualisierungs-Software von Microsoft. Hier erfahren Sie, wie gut die ebenfalls aktualisierten Tools von Vmware und Oracle im Vergleich abschneiden.

VON WOLFGANG SOMMERGUT



Der erweiterte Sitzungsmodus baut aus dem Hyper-V-Manager eine vollwertige Remote-FX-Verbindung auf.

HYPER-V FEIERTE IN WINDOWS 8 sein Debüt auf dem Client. Die Portierung des Hypervisors vom Server auf den Client ging zwar mit einigen Anpassungen einher, um den dortigen Anforderungen gerecht zu werden (etwa die Unterstützung des Energiesparmodus). Während Hyper-V bei der rohen Leistungsfähigkeit führend war, erwiesen sich aber Vmware Workstation (auf der Heft-DVD und unter *www.vmware.com*) und Virtualbox (auf der Heft-DVD und unter *www.virtualbox.com*) beim ersten Vergleichstest (*http://bit.ly/1iMy7In*) als ausgereifter und benutzerfreundlicher.

Microsoft versucht, in Windows 8.1 die Defizite von Hyper-V in puncto Bedienung und Komfort zu reduzieren. Deshalb ist der sogenannte Enhanced Session Mode (*http://bit.ly/1iMyMDb*) eine wesentliche Neuerung von Hyper-V, weil er den Aufbau einer vollwertigen RDP-Verbindung via Vmconnect aus dem Hyper-V Manager erlaubt – jedoch nur, wenn in der virtuellen Maschine (VM) die neuesten Versionen von Windows und Windows Server laufen. Das beseitigt zwar nicht die grundlegenden Einschränkungen, die duch die Interaktion mit dem Gast über Remote Desktop entstehen (kein Drag & Drop, limitierter Support für USB). Aber das neue Feature erspart zumindest den umständlicheren Aufbau einer direkten RDP-Verbindung mit dem Gast.

Eingeschränkter UEFI- und SCSI-Support von Hyper-V

Windows 8 Hyper-V bot als einziges der drei Tools keine UEFI-Unterstützung für virtuelle Maschinen. Auch in dieser Hinsicht bringt die Version 8.1 Fortschritte, auch wenn sich diese auf VMs der Generation 2 (*http://bit.ly/1fntc9k*) und damit auf Windows 8.x (64 Bit) und Server 2012 (R2) als Gäste beschränken. Dagegen lassen die beiden anderen Produkte für jede VM die Wahl zwischen Bios oder UEFI.

Neu in VMs der Generation 2 ist auch die Unterstützung für das Booten von SCSI-Laufwerken, so dass die Notwendigkeit für IDE entfällt. Auch Virtualbox 4.3 erlaubt nun den Start der VMs von SCSI-CD/DVD, und zwar anders als Hyper-V unabhängig vom Gast.

Auch wenn Linux nicht VMs der Generation 2 nutzen kann, so dehnt Hyper-V zumindest Dynamic Memory auf Linux aus, nachdem es bisher Windows-Gästen vorbehalten war. Bei der Unterstützung heterogener Gastsysteme sind die beiden Wettbewerber aber nach wie vor besser als Microsoft.

Dies zeigt sich nicht alleine an der Zahl der zulässigen Betriebssysteme, sondern auch an der Wizard-geführten Einrichtung von VMs, die bei Vmware Workstation und Virtualbox automatisch auf die Gäste zugeschnitten wird.

Vmware Workstation mit höherer Skalierbarkeit

Die Vmware Workstation Vmware bot zuletzt deutlich geringere Maximalwerte bei der Aus-

stattung von VMs als die beiden Wettbewerber. Die Version 10 kann mit ihnen immer noch nicht gleichziehen, erhöht aber immerhin das Limit von acht auf 16 vCPUs pro virtueller Maschnine. Außerdem fällt mit der Virtual Hardware 10 die Beschränkung von VMDKs auf die Größe von 2 TB, die Obergrenze liegt nun bei 8 TB. Keine Veränderung gab es durch die Updates bei der Fähigkeit, Intel VT-x oder AMD-V zu virtualisieren. Sie ist die Voraussetzung dafür, dass man einen Hypervisor in einer VM installieren kann, beispielsweise um Vsphere mit mehreren virtuellen Hosts auf einem Rechner testen zu können. Dieses Feature bietet weiterhin nur die Vmware Workstation.

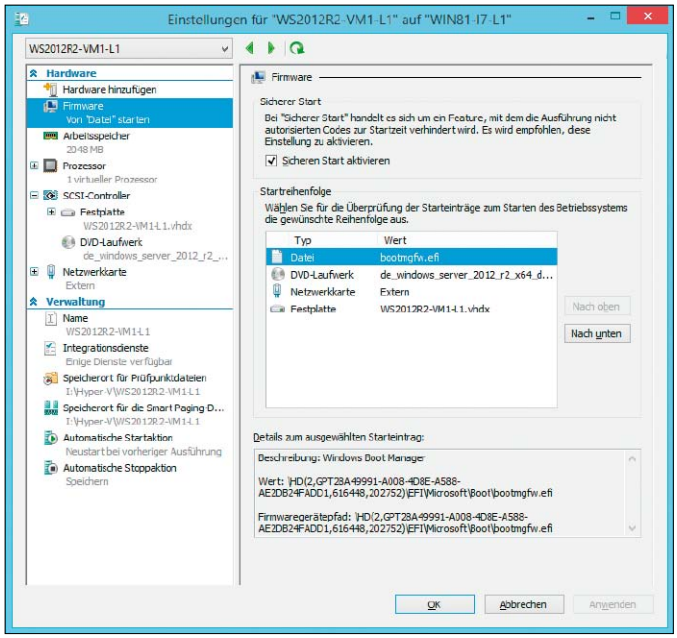
In einer solchen Lab-Konfiguration erweist es sich zudem als nützlich, wenn der Virtualisierer SSDs emulieren (*http://bit.ly/1iMD2Tb*) kann. In diesem Fall würde jeder Hypervisor, der in einer VM läuft, einen solchen schnellen Speicher vorfinden, obwohl der Rechner gar keine derartige Hardware besitzt. SSDs werden zum Beispiel benötigt, wenn man Vmware Vsan oder Vsphere Flash Read Cache testen möchte. Aktuell ist nur die Vmware Workstation in der Lage, SSDs zu simulieren.

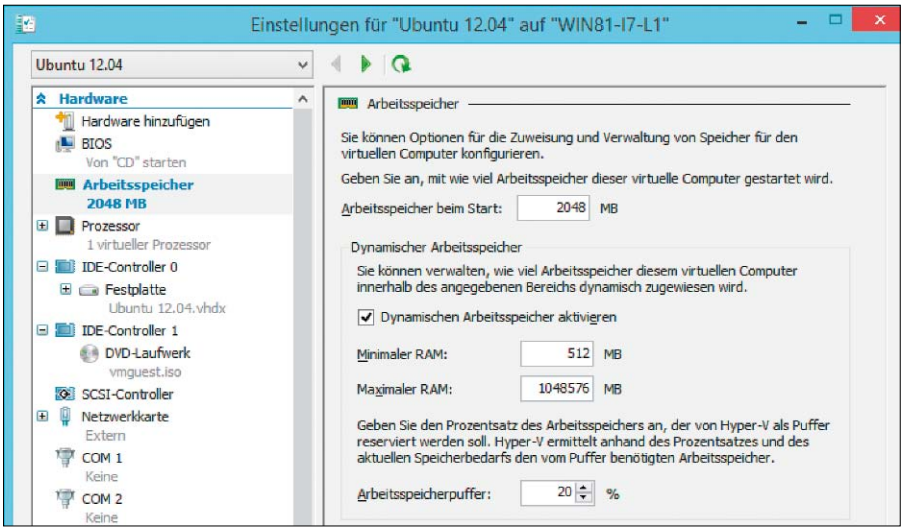
Die aktuellen Updates bieten noch eine weitere Form der SSD-Unterstützung. Wenn Gastbetriebssysteme in der Lage sind, ihre Konfiguration automatisch auf diese Speichermedien einzustellen, dann müssen sie darüber informiert werden, dass sich ihre virtuellen Laufwerke auf einer SSD befinden. Es ist Aufgabe des Hypervisors, diese Information an die VM durchzureichen („SSD Passthrough"). Vmware Workstation 10 tut dies automatisch, und in Virtualbox 4.3 kann man diese Eigenschaft setzen.

Neue Sicherheitsfunktionen

Die Vmware Workstation 10 erweiterte die Möglichkeiten zur Kontrolle von VMs, indem man sie nun mit einem Ablaufdatum versehen kann. Dies erlaubt die zeitlich befristete Weitergabe von Anwendungen. Diese Neuerung ergänzt schon länger vorhandene Sicherheitsfunktionen wie die Verschlüsselung von VMs oder den Passwortschutz für die Einstellungen einer virtuellen Maschine, die den Konkurrenten bis dato fehlen.

Natürlich kann man argumentieren, dass es nicht Aufgabe der Virtualisierungs-Software sein muss, VMs zu verschlüsseln, weil man das auch mit den Bordmitteln des Hosts oder des Gasts machen kann. Aber nicht alle Betriebssysteme bieten derartige Funktionen, und außerdem verbessert es die Portabilität von VMs, wenn die Vmware Workstation auf Windows und auf Linux die gleichen Mechanismen verwendet wie Vmware Fusion auf dem Mac. Für Windows 8.1 Hyper-V bietet UEFI-Unterstützung nur in VMs der zweiten Generation, die dem neuesten Windows vorbehalten sind.





Die Integrationsdienste von Windows 8.1 Hyper-V unterstützen auch dynamischen Arbeitsspeicher für Linux.

Hyper-V ist dieses Thema weniger relevant, weil es auf Windows beschränkt ist.

Multimedia-Funktionen

Alle drei Produkte erlauben schon seit längerer Zeit, Screenshots der Gäste zu erfassen. Im Fall von Hyper-V gibt es dafür nur im einfachen Sitzungsmodus eine explizite Funktion. Hat man eine direkte RDP-Verbindung mit dem Gast aufgebaut, kopiert Alt-Druck das aktive Sitzungsfenster in die Zwischenablage.

Während die beiden Typ-2-Hypervisors in den virtuellen Maschinen Hardware-beschleunigtes DirectX bereitstellen, bietet Hyper-V eine leistungsfähige Grafik nur über den Umweg von Remote FX.

Die Vmware Workstation 9 hatte im Vergleich mit Windows 8 Hyper-V und Virtualbox 4.2 ein weiteres exklusives Feature, indem sie alle Aktionen in einer VM als Video mitschneiden konnte. In der Workstation 10 wurde dieses Feature entfernt, weil der Hersteller nach eigenen Angaben die schon in der Vorversion aufgetretenen technischen Probleme nicht in den Griff bekam. Virtualbox rüstet dagegen eine solche Aufzeichnungsfunktion nun nach, wogegen sie bei Hyper-V weiterhin fehlt.

Tabellarischer Funktionsvergleich

Die Tabelle auf der nächsten Seite zeigt Ihnen die Funktionen der aktullen Versionen von Hyper-V, Vmware und Virtualbox. So können Sie selbst entscheiden, welches Tool für Sie passt. Der Vergleich zwischen Windows 8 Hyper-V, Vmware 9 und Virtualbox 4.2. ist weiterhin über *http://bit.ly/1iMy7In* verfügbar.

Virtualisierungs-Software im Vergleich Hyper-V, Vmware und Virtualbox

	WINDOWS 8.1 HYPER-V	VMWARE WORKSTATION 10	VIRTUALBOX 4.3.
Typ	Bare Metal (Typ 1)	Hosted (Typ 2)	Hosted (Typ 2)
CPU-Voraussetzungen	64-Bit-CPU mit Second Level Address Translation (SLAT)	64-Bit-CPU, Intel VT-x oder AMD-V für 64-Bit-Gäste	64-Bit-CPU, Intel VT-x oder AMD-V für 64-Bit-Gäste
Max. vCPU pro VM	64	16	128
Max. RAM pro VM	1 TB	64 GB	1 TB
Max. vNICs pro VM	12	10	36
Gastzugriff auf USB-Geräte	sehr eingeschränkt (Weitere Informationen dazu finden Sie über *http://bit.ly/1qWGFu9*)	ja (inkl. USB 3.0)	ja
Virtuelle Audiogeräte	nein (Sound über Audioumleitung von RDP)	ja	ja
UEFI-Emulation	Nur in VMs der Generation 2 mit Windows 8.x bzw. Server 2012 (R2) als Gästen.	ja	ja
Memory Overcommit	Dynamic Memory, in 8.1 auch für Linux-Gäste	Page Sharing, Ballooning	Memory Ballooning über Kommandozeile
Verschachtelte Virtualisierung (Nested Virtualization)	nein	ja (ESXi, Hyper-V)	nein
Virtuelle Netzwerke	Extern, Intern, Privat (Weitere Informationen dazu finden Sie über *http://bit.ly/Q6tBax*)	NAT, Bridged, Host-only, Custom	NAT, Bridged, Intern, Host-only
Zuordnung von vNICs zu VLANs	ja	nein	nein
Scripting	Powershell	VXI/vmrun	Vboxmanage,Vboxtool (Linux-Hosts)
Unterstützte Host-Betriebssysteme	Feature von Windows 8.1 x64 Pro und Enterprise	Windows, Linux (VMware Fusion als eigenes Produkt für Mac-OS)	Windows, Linux, Mac OS X, Solaris
Unterstützte Gäste	Windows, Cent-OS, Redhat, Suse	Windows, Linux, Free BSD, Mac-OS X, Netware, Solaris (vollständige Liste: *http://partnerweb.vmware.com/GOSIG/home.html*)	Windows, Linux, Solaris, Mac-OS X, OS/2 (vollständige Liste* *https://www.virtualbox.org/wiki/Guest_OSes*)
64-Bit-Gäste	ja	ja	ja
Formate für virtuelle Laufwerke	VHD, VHDX	VMDK, VHD	VHD, VMDK, VDI, HDD (Parallels), QED (Qemu), QCOW (Qemu)
Max. Größe für virt. Laufwerke	64 TB (VHDX)	8 TB (mit Virtual Hardware 10)	2 TB über GUI
Verschlüsselung von VMs	nein	ja	nein
Emulation von SSDs	nein	ja	nein
Virtuelle Floppy	ja	ja	ja
SSD Passthrough	nein	ja	ja
Boot von SCSI	Nur VMs der Generation 2	Ja	Ja
OVF-Import von Virtual Appliances	nein	ja	ja
Import physikalischer Systeme (P2V)	über separate Tools	ja	manueller Prozess (Infos über *http://bit.ly/1qxZbdX*)
Support für XP-Modus	nicht zutreffend, da kein XP-Modus unter Windows 8.x	ja	manueller Import der VHD in neue VM, Vmlite
Migration von VMs	Cold Migration von/zu Hyper-V Server	Cold Migration von/zu ESXi und Vcenter, HTTP-Streaming zu VMware Workstation	Live-Migration zwischen Virtualbox-Hosts
Live Storage Migration	ja	nein	nein
Snapshots	ja	ja	ja
Online Snapshot Merging	ja	ja	ja
Full Clones	Über Live Storage Move	ja	ja
Linked Clones	Mittels differenzierender VHDs	ja (eine Anleitung dazu finden Sie über *http://bit.ly/1p312dy*)	ja (eine Anleitung dazu finden Sie über *http://bit.ly/1jEiTSL*)
Fernzugriff	RDP	VNC, VM-Sharing, HTTPS/HTML5	RDP
VMs ohne GUI starten (Headless Mode)	ja	ja (über Kommandozeile)	ja (über Kommandozeile)
Copy & Paste zwischen VMs und Host	über RDP-Client, in VMConnect eingeschränkt	ja	ja
Shared Folder	über RDP-Client	ja	ja
Drag & Drop zwischen Host und Gast	nein	ja	experimentell, nur für Linux-Gäste
Stufenloses Verkleinern und Vergrößern des Gastfensters	über RDP 8.x	ja	ja
Nahtlose Integration von VM-Anwendungen in den Host	manuell über Remote-App von Microsoft	ja	ja
Video-Mitschnitt der VM-Session	nein	nein	ja

Einen Vergleich der Vorversionen dieser drei Virtualisierungsprogramme finden Sie über *http://bit.ly/1iMy7ln*.

PC-WELT

Die **MAGAZIN-APP** für Ihren Windows 8.1 PC oder Tablet

Lesen Sie PC-WELT, AndroidWelt, LinuxWelt, GalaxyWelt und alle Sonderhefte digital.

1. Ausgabe GRATIS für alle!

» Mehr als 40 Hefte pro Jahr

» Volltextsuche über alle Hefte

Kostenlos für Ihren Windows 8.1 PC oder Tablet downloaden:

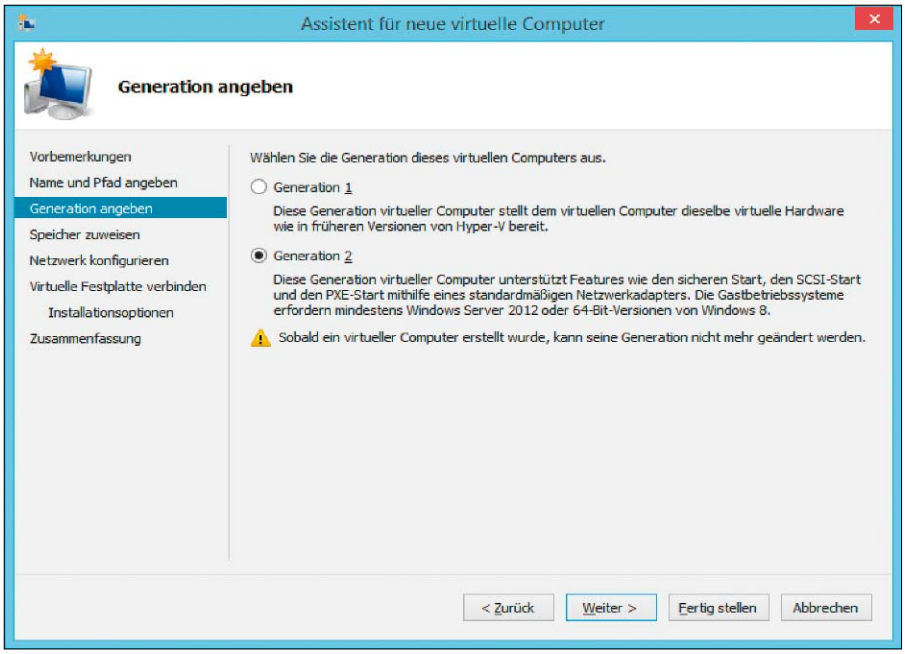
www.pcwelt.de/win8

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Neu in Hyper-V und VM Manager

Viele Neuerungen von Windows Server 2012 R2 betreffen den integrierten Hypervisor. Dazu zählen VMs der zweiten Generation, Live Migration Compression und Fortschritte beim Virtual Machine Manager.

VON WOLFGANG SOMMERGUT



Der Wizard für neue VMs bietet unter 8.x und Server 2012 (R2) die Auswahl zwischen erster und zweiter Generation.

WIE AUF DEM CLIENT stellt Microsoft auch bei Windows Server auf Updates im Jahres-Rhythmus um. Diese kürzeren Release-Zyklen erlauben dem Hersteller, vor allem jene Komponenten schneller zu aktualisieren, die aufgrund des Wettbewerbs einem stärkeren Innovationsdruck unterliegen. Auf dem Server betrifft dies besonders das Subsystem für die Virtualisierung. Wegen ihres vielversprechenden Namens dürften die virtuellen Maschinen der zweiten Generation (*http://bit.ly/1fntc9k*) auf besonderes Interesse stoßen. Ihr wichtigstes Feature ist der UEFI-Support, so dass davon abhängige Funktionen wie Secure Boot für Windows-Gäste zur Verfügung steht. UEFI-Firmware in VMs bieten Vmware und VirtualBox schon länger, Microsoft schließt nun zu den Wettbewerbern auf. Ein weiteres Merkmal von VMs der zweiten Generation ist der Verzicht auf emulierte Geräte, die ein Performance-Problem darstellen. Solche VMs ohne Altlasten können von virtuellen SCSI-Laufwerken oder von einer synthetischen NIC booten. Die Gäste müssen aber mindestens unter Windows 8 (64 Bit) oder Server 2012 laufen.

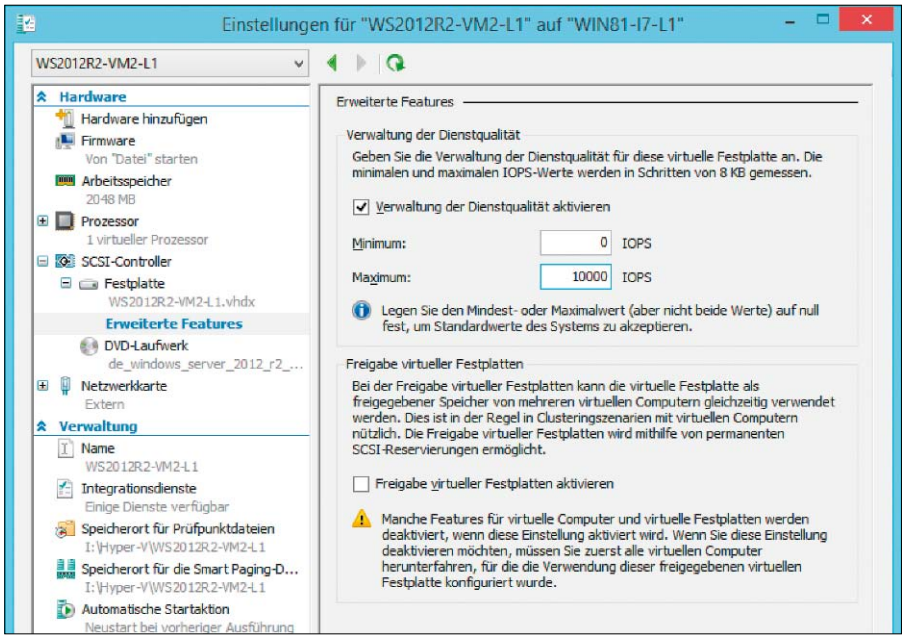
Erweiterte Nutzung von VHDX seit Windows Server 2012

Eine ganze Reihe von Fortschritten betrifft das Storage-Management von Hyper-V. Das mit Windows Server 2012 eingeführte VHDX-Format lässt mit einer Obergrenze von 64 TB wesentlich größere virtuelle Laufwerke zu als VHD. Es erhält weitere Verbesserungen, die einen flexibleren Betrieb von Hyper-V erlauben. So kann man künftig die Größe von VHDX ändern, während die VM eingeschaltet bleibt. Wie bisher kann man eine virtuelle Festplatte nur verkleinern, wenn sie einen unpartitionierten Bereich enthält.

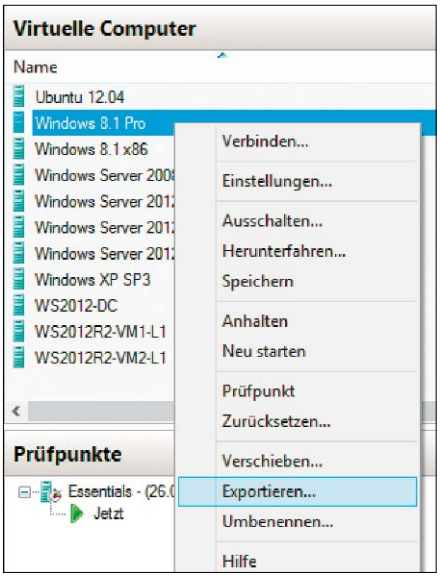
Hyper-V Server 2012 R2 führt außerdem „Shared VHDX“ ein, so dass bis zu 64 VMs gemeinsam auf ein virtuelles Laufwerk zugreifen können. Ein solches dient nicht der Einrichtung von Disks, von denen die VMs booten können, sondern für Daten-Volumes.

Shared VHDX sollen damit vor allem die Konfiguration von Clustern auf Ebene der Gastbetriebssysteme vereinfachen, weil sie eine Alternative zur Zuordnung von physikalischen LUNs zu bestimmten VMs darstellen. Shared VHDX können entweder auf einem Fileserver mit SMB 3.0 oder auf einem CSV-Volume eines Block-orientierten Storage-Systems (SAN) abgelegt werden. Weitere Informationen zu CSV-Volumen gibt es über *http://bit.ly/1gAlWaH*.

Das neue VHDX-Feature ist kompatibel mit Live Migration, so dass virtuelle Maschinen auch dann auf einen anderen Host umziehen können, wenn sie eine Shared VHDX nutzen. Storage Live Migration für Shared VHDX wird jedoch nicht unterstützt.



Hyper-V 2012 R2: Quality of Service (Dienstqualität) und Shared VDHX sind die auffälligsten Storage-Neuerungen.



Virtuelle Maschinen lassen sich nun exportieren. Das funktioniert auch dann, wenn sie eingeschaltet sind oder über Snapshots verfügen.

Storage Quality of Service und Deduplizierung

Eine weiteres neues Feature namens „Storage Quality of Service" (QoS) erlaubt es dem Administrator, den Datendurchsatz für einzelne virtuelle Maschinen zu begrenzen. Ein solches Limit soll überaktive VMs daran hindern, zu viele Ressourcen auf Kosten anderer Workloads zu konsumieren. Solche Grenzwerte lassen sich auch während der Laufzeit einer virtuellen Maschine festlegen.

Vmware bietet mit Storage IO Control bereits seit Vsphere 4.1 in der Enterprise Plus Edition ein derartiges QoS-Feature. Allerdings basiert es nicht wie bei Hyper-V 2012 R2 auf festen IOPS-Limits, sondern es verteilt die Bandbreite dynamisch, abhängig davon, wie der Administrator VMs gewichtet.

Windows Server 2012 führte die Deduplizierung von Daten (*http://bit.ly/1iZ2pRO*) auf NTFS-Volumes ein, um Speicherplatz zu sparen. Das Feature war explizit nicht für VHDs von laufenden virtuellen Maschinen ausgelegt, weil sich ihr Inhalt zu häufig ändert.

Im Release 2 des Betriebssystems fällt diese Beschränkung für virtuelle Desktops, die auf Basis der Remote Desktop Services eingerichtet werden. Ihre Images können nun während des laufenden Betriebs dedupliziert werden, wenn die VHD(X)-Dateien auf einem Cluster Shared Volume liegen.

Schnellere Live Migration

Gleich mehrere Verbesserungen erhöhen die Mobilität von virtuellen Maschinen. Dazu gehört „Live Migration Compression", das den Umzug von VMs zwischen Hosts beschleunigt und laut Microsoft die dafür nötige Zeit bei den meisten Workloads auf die Hälfte verringert. Wie die Bezeichnung nahelegt, wird dies durch die Kompression von VHD(X)-Dateien und damit durch die Reduktion der zu übertragenden Datenmengen erreicht.

Ebenfalls einem beschleunigten Umzug von VMs dient „Live Migration with RDMA" (Remote Direct Memory Access). Sie macht sich besonders in sehr schnellen Netzwerken (10 GBit) bemerkbar, weil sie Transfers von bis zu 56 GB/s zulässt. Diese Performance wird erreicht, indem der Hypervisor den Datentransfer direkt auf die RDMA-Hardware auslagert.

Das Update von Hosts auf Windows Server 2012 R2 sowie der gemischte Betrieb von Server 2012 mit dem Release 2 wird dadurch erleichtert, dass Microsoft die Live Migration zwischen beiden Versionen des Hypervisors unterstützt.

Klonen und Export von aktiven virtuellen Maschinen

Fortschritte beim Management von virtuellen Maschinen bringt die neue Cloning-Funktion, die eine Duplizierung von VMs im laufenden Betrieb unterstützt. Bisher war für diesen Zweck der System Center Virtual Machine Manager notwendig, der Hyper-V Manager bot nur eine Behelfslösung über den Export und Reimport einer VM (Informationen dazu über *http://bit.ly/1ePBgji*). Außerdem musste die VM dabei ausgeschaltet sein.

In Windows Server 2012 R2 ist die Exportfunktion nun in der Lage, auch eingeschaltete virtuelle Maschinen zu kopieren. Außerdem fällt die Beschränkung, dass nur VMs ohne Snapshots exportiert werden dürfen. Daher ist es künftig nicht mehr erforderlich, vor dem Export Snapshots zu löschen.

Flexibleres Hyper-V Replica

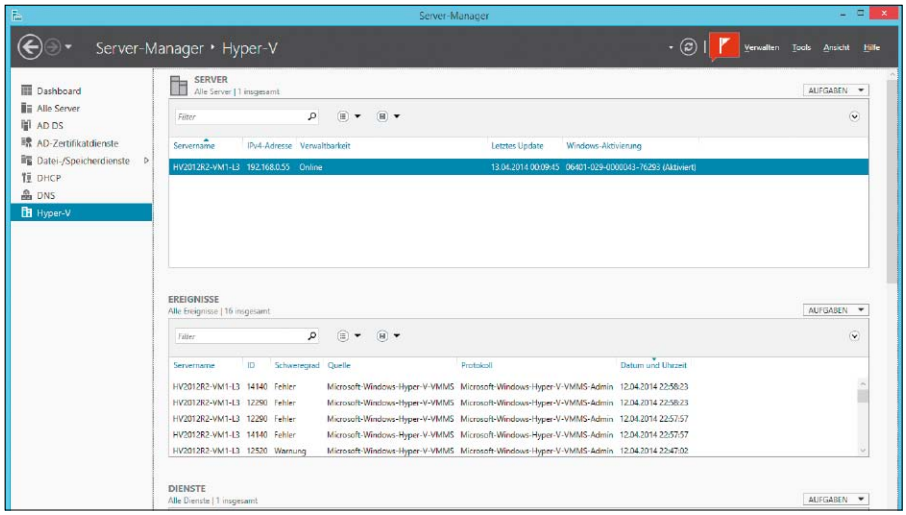
Zu den Neuerungen von Server 2012 zählte eine einfache Funktion für das Desaster Recovery namens Hyper-V Replica. Es überträgt VMs zeitgesteuert auf andere Hosts, typischerweise in externe Rechenzentren oder zu einem Cloud-Provider.

Das Release 2 bietet mehr Flexibilität bei der Replikation von virtuellen Maschinen, indem es verschiedene Zeitintervalle zulässt, nach denen Änderungen einer VM übertragen werden. Diese bewegen sich zwischen 30 Sekunden und 15 Minuten. Außerdem lassen sich virtuelle Maschinen künftig nicht nur auf einen Ziel-Host replizieren, sondern hintereinander auch auf einen dritten Host.

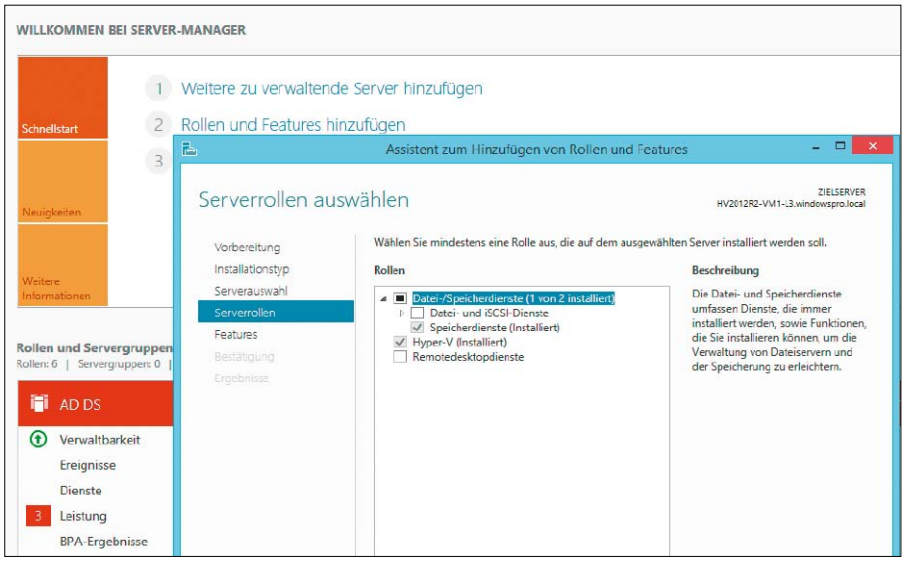
Dynamic Memory für Linux-Gäste

Hyper-V 2012 R2 erweitert auch den Support von Gastbetriebssystemen, indem es nun auch Dynamic Memory für Linux anbietet. Microsoft führte dieses Feature, mit sich der verfügbare Arbeitsspeicher besser zwischen den VMs verteilen lässt, bereits mit Hyper-V 2008 R2 SP1 ein. Bis dato war es aber Windows-Gästen vorbehalten.

Die mit Windows gleichwertige Unterstützung von Dynamic Memory in Linux erfordert aktualisierte „Linux Integration Components". Diese werden laut Microsoft künftig zum Liefer-



Der Hyper-V Server 2012 R2 lässt sich Remote mit den RSAT und den darin enthaltenen Server Manager verwalten.



Der Hyper-V Server 2012 R2 unterstützt nicht die Hyper-V-Rolle, einige Storage-Dienste und Remote Desktop.

umfang der wichtigsten Distributionen gehören. Eine Neuerung für Windows-Gäste ist das so genannte „Zero Touch Activation". Windows-Installationen innerhalb von virtuellen Maschinen werden automatisch aktiviert, wenn sie auf einer Datacenter Edition von Windows Server läuft. Eine Lizenz dieser Ausführung erlaubt beliebig viele Instanzen von Windows Server in virtuellen Maschinen.

Erweiterte RDP-Funktionen für VM Connect

Eine Verbesserung bei der Interaktion mit den Gastbetriebssystemen bringt das überarbeitete VM Connect. Dieses kommt immer dann zum Einsatz, wenn man im Hyper-V Manager eine Verbindung zu einer VM aufbaut. Sein Vorteil besteht darin, dass die RDP-Session über den Host läuft und die Gastbetriebssysteme für eine Remote-Desktop-Verbindung nicht konfiguriert werden müssen. Der Nachteil von VM Connect bestand bisher in einem schlechten Benutzererlebnis, so dass man für einen vollwertigen Zugriff auf das Gastsystem eine direkte RDP-Verbindung mit demselben aufbauen musste.

Hyper-V 2012 R2 unterstützt nun auch in VM Connect erweiterte RDP-Funktionen wie Datenaustausch über die Zwischenablage sowie Audio-, Ordner- und USB-Umleitung. Dieses Feature ist auch in Windows 8.1 Hyper-V vorhanden, wo es aufgrund der dort intensiveren Interaktion mit Gastsystemen von besonderem Nutzen ist.

Features des kostenlosen Hyper-V Server 2012 R2

Microsoft koppelte auch aus Windows Server 2012 R2 den Hypervisor in ein kostenloses Produkt aus. Während es aus dem Vollprodukt alle Funktionen von Hyper-V erbt, enthält die Parent Partition nur einen abgespeckten Windows Server. Hyper-V Server 2012 R2 bietet nicht nur die gleichen Kernfunktionen für die Virtualisierung, beispielsweise die vom Vollprodukt bekannten Maximalwerte bei der Ausstattung von Hosts und virtuellen Maschinen. Dazu gesellen sich seit der Vorversion die Unterstützung für Live Migration, Netzwerk-Virtualisierung inklusive Extensible Switch oder das VHDX-Format.

Windows Server 2012 R2 Hyper-V fügt wie oben beschrieben eine ganze Reihe von Funktionen hinzu, von UEFI-Support für VMs über diverse Storage-Features bis zu einer optimierten Live Migration. Die kostenlose Ausführung kommt mit allen dieser Fortschritte.

Zu den wichtigsten Neuerungen des Hypervisors, die auch in der kostenlosen Variante enthalten sind, zählen:

- Virtuelle Maschinen der Generation 2
- Shared VHDX
- Storage Quality of Service (QoS) für VMs
- Live Migration Compression
- Hyper-V Replica mit flexiblen Zeitintervallen
- Dynamic Memory für Linux-Gäste

Alle diese Features lassen sich mit den gleichen Management-Tools verwalten wie beim Vollprodukt. Dazu zählen vor allem der Hyper-V Manager und der System Center Virtual Machine Manager.

Neue Features neben der Virtualisierungsfunktion

Hyper-V Server 2012 R2 besteht aber nicht nur aus dem Hypervisor, sondern basiert auf einem Windows Server Core, aus dem die meisten Rollen und Features entfernt wurden. Aus diesem Grund kann man die kostenlose Version ebenfalls mit dem Server Manager, RSAT oder SCCM administrieren. Darüber hinaus kann (und soll) er Mitglied in einer AD-Domäne werden, so dass auch Gruppenrichtlinien für ihn wirksam sind.

Vom vollwertigen Windows Server erbt Hyper-V Server 2012 R2 die Unterstützung für Clustering, wobei die Obergrenze bei 64 Knoten liegt. Mit an Bord ist zudem Powershell 4.0, für die sich das Hyper-V-Modul als Feature installieren lässt, so dass man VMs über die Kommandozeile oder über Scripts verwalten kann.

Unterstützung für Storage Spaces über den Server Manager

Fügt man Hyper-V Server 2012 R2 im Server Manager zur Liste der verwalteten Rechner hinzu, dann sieht man, dass neben der Hyper-V-Rolle auch jene für Datei- und Speicherdienste vorhanden ist. Sie erlaubt auch das Einrich-

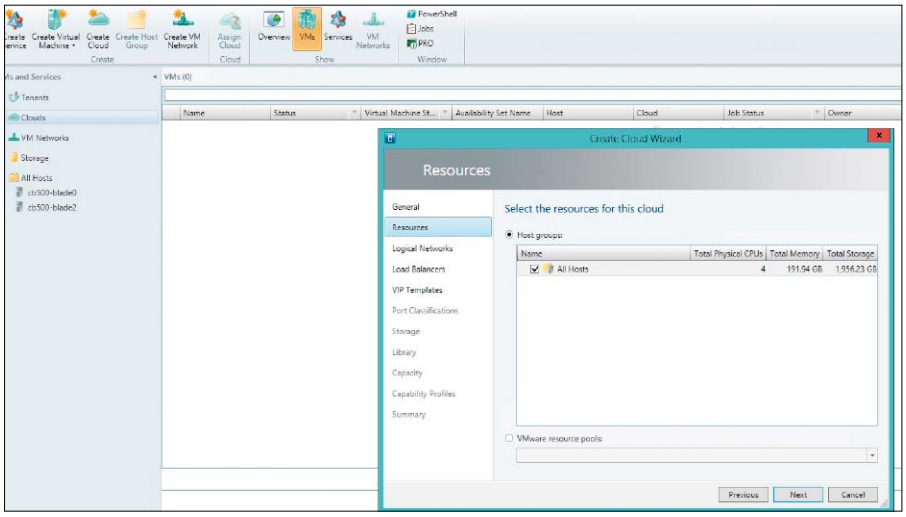
ten von Storage Spaces (*http://bit.ly/OXbkM7*) auf Basis von Direct Attached Storage (DAS). Vorhanden ist auch die Unterstützung für Multipath-I/O und NIC-Teaming.
Startet man an dieser Stelle den Wizard zum Hinzufügen von Rollen und Features, dann zeigt sich, dass mit den Remote-Desktop-Diensten eine weitere Rolle zur Verfügung steht, die standardmäßig nicht aktiviert ist. Sie reduziert sich jedoch auf die Funktion des Virtualisierungs-Hosts, der dem Bereitstellen von virtuellen Desktops dient.

Einsatzmöglichkeiten des kostenlosen Hyper-V

Angesichts der erheblichen Funktionsfülle des kostenlosen Hyper-V Server 2012 R2 eignet dieser sich für eine Reihe von Einsatzgebieten. Der Virtualisierung von Windows Server steht indes Microsofts Lizenzmodell entgegen, das keinen Grund zum Einsatz der kostenlosen Version liefert. Schließlich enthält Windows Server 2012 R2 nicht nur Hyper-V, sondern räumt auch das Recht auf ein vollwertiges Windows in der Parent Partition nur zum Betrieb der Hyper-V-Rolle ein.
Daher bleibt die Verwendung von Hyper-V Server 2012 R2 wie die seiner Vorgänger auf die Virtualisierung von Desktops, älteren Versionen von Windows Server und Linux beschränkt. Letzteres ist mit der aktuellen Ausführung des Microsoft-Hypervisors eine reelle Option, nachdem er nun auch Dynamic Memory für Linux-Gäste bietet. Darüber hinaus bieten sich noch eher exotische Anwendungen, wie etwa die Einrichtung eines kostengünstigen Storage-Systems mit Tools wie Starwind iSCSI SAN.
Hyper-V Server 2012 R2 kann nach Anmeldung mit einem Microsoft-Konto von Technet heruntergeladen werden (Infos und Download über *http://bit.ly/1hlREXL*).

Verbesserungen von System Center Virtual Machine Manager

Wenn man Hyper-V-Hosts nicht nur einzeln verwalten, sondern ihre Ressourcen zu einem Pool zusammenschließen möchte, dann sieht Microsoft dafür den „ System Center Virtual Machine Manager“ (SCVMM) vor. Wie gewohnt steht mit dem Update des Hypervisors auch ein solches für den SCVMM an, so dass sich damit die neuen Funktionen von Windows Server 2012 R2 Hyper-V nutzen lassen.
System Center Virtual Machine Manager spielt in der Microsoft-Welt weitgehend die gleiche Rolle wie Vcenter unter Vmware. Viele der fortgeschrittenen Features von Hyper-V sowie die Automatisierung virtueller Infrastrukturen setzen dieses Tool voraus.



Wenn man Hyper-V-Hosts nicht einzeln, sondern als Ressourcen-Pool verwalten möchte, dann führt kein Weg am Virtual Machine Manager 2012 R2 vorbei.

Erweitertes Management von VMs

Die meisten Neuerungen betreffen die Verwaltung von VMs. So können nun virtuelle Datenträger im VHDX-Format während der Laufzeit vergrößert oder verkleinert werden, außerdem lässt sich Dynamic Memory ebenfalls unterbrechungsfrei konfigurieren. SCVMM unterstützt diese Features von Hyper-V 2012 R2 ebenso wie das Live Cloning von VMs.
In puncto Administration bringt Virtual Machine Manager 2012 R2 weitere Verbesserungen, die nicht direkt Veränderungen des Hypervisors reflektieren. Dazu zählt ein flexibleres Delegieren von Rechten an Administratoren, indem einem User oder einer Rolle bestimmte Privilegien pro Cloud erteilt werden können (Cloud ist eine administrative Einheit in SCVMM). Damit entfällt die Notwendigkeit, für bestimmte Rechte in jeder Cloud einen eigenen Benutzer und eine eigene Rolle anzulegen.

Schnelle Konfiguration von VMs durch XML-Dateien

Eine weitere neue Funktion erlaubt die Konfiguration von VMs durch Einspielen von XML-Dateien in das entsprechende Verzeichnis noch vor dem ersten Start einer virtuellen Maschine. Zusätzlich lassen sich Einstellungen über Suchen und Ersetzen von Einträgen in der Konfigurationsdatei ändern.
Wenn eine VM keine Verbindung zu einem Library-Server hat, dann kann man Dateien in das Gastsystem transferieren, etwa um dieses oder darin enthaltene Anwendungen individuell anzupassen. Allerdings muss dafür in der VM ebenfalls Windows Server 2012 R2 laufen. Der Support für Linux verbessert sich nicht nur dadurch, dass Hyper-V 2012 R2 auch für dieses Betriebssystem Dynamic Memory ermöglicht. SCVMM 2012 R2 steuert die Möglichkeit bei, Multi-VM-Konfigurationen für mehrschichtige Anwendungen auch mit Linux-Gästen aus einer Template-Gallery zu erzeugen.

Support für Scale-out File-Server

Die wichtigste Neuerung in puncto Storage besteht in der erweiterten Unterstützung für Scale-out File-Server. Es handelt sich dabei um eine mit Windows Server 2012 eingeführte Rolle, die eine File-basierte Alternative zu Block-orientierten SANs bieten soll.
Sie erlaubt das Einrichten von Server-Clustern mit einer Active/Active-Konfiguration, um bei Ausfall eines Knotens einen transparenten Storage-Failover für Applikations-Server oder Hyper-V-Hosts zu erreichen. Die Kommunikation mit dem Windows-basierten Speichersystem erfolgt dabei über SMB 3, das bei Bedarf Multichannel und RDMA unterstützt.
Die Positionierung von Windows Server als System für Shared Storage macht sich in SCVMM 2012 R2 dadurch bemerkbar, dass es das komplette Management der Scale-out File-Server übernehmen kann. Dies beginnt mit der Bare-Metal-Installation des Clusters und reicht bis zum Monitoring während des Betriebs.

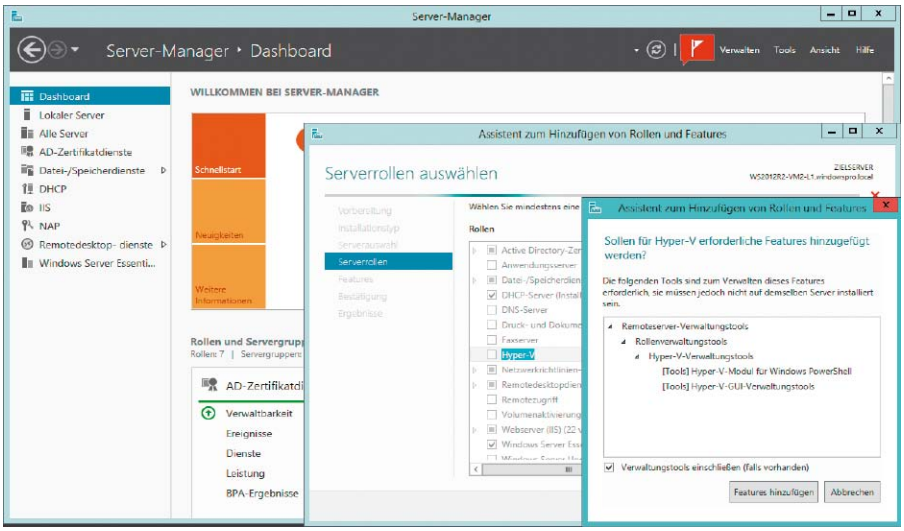
Neue Netzwerkfunktionen

Beim Networking unterstützt SCVMM die erweiterten Site-to-Site-VPNs von Windows Server 2012 R2, dessen VPN-Gateway mandantenfähig ist und sich besonders für Hybrid Clouds eignet. Neu ist auch die Möglichkeit, die IP-Einstellungen von Gästen aus dem Virtual Machine Manager zu konfigurieren. Hinzu kommt dabei noch die Unterstützung für das erweiterte IP Address Management (IPAM) von Windows Server 2012 R2. ■

Hyper-V remote installieren

Um aus Windows einen Virtualisierungs-Host zu machen, fügen Sie Hyper-V als Rolle hinzu. Wir zeigen, wie das am Client und am Server geht. Dank Powershell lässt sich Hyper-V sogar remote installieren.

VON WOLFGANG SOMMERGUT



Die komfortabelste Installation von Hyper-V bietet der Server Manager, der den Hypervisor einrichten kann.

BEVORZUGT MAN EINE GUI-geführte Installation der Hyper-V-Rolle, dann ist der Server Manager das Tool der Wahl. Er steht am Server selbst zur Verfügung, es sei denn, man hat sich für die Installationsvariante Server Core entschieden. In diesem Fall hilft Powershell beziehungsweise Deployment Image Servicing and Management (DISM). Unter Windows Server 2008 R2 konnte nur der lokal installierte Server Manager Rollen hinzufügen, die mit RSAT für Windows 7 gelieferte Version war dazu nicht in der Lage. Der neue Server Manager in Windows Server 2012 (R2) und in RSAT für Windows 8 kann dagegen Rollen und Features auch remote installieren oder entfernen. Die Aktivierung von Hyper-V erfolgt mit Hilfe des Wizards, den man im Menü unter „Verwalten → Rollen und Funktionen hinzufügen" startet. In der Liste der verfügbaren Rollen bietet sich die Möglichkeit, neben dem Hypervisor auch noch die dazugehörigen Verwaltungs-Tools zu installieren. Dazu zählen der GUI-basierte Hyper-V Manager sowie die Powershell-Module.

So fragen Sie bereits installierte Rollen mit Powershell ab

Das Powershell-Modul „Servermanager" umfasst Cmdlets, die installierte Rollen und Features anzeigen, installieren und entfernen können. Sie stehen unter Windows Server 2008 R2 und 2012 sowie unter Windows 8.x zur Verfügung, wenn man dort die RSAT installiert hat. Möchte man wissen, ob Hyper-V auf einem Server eingerichtet wurde, dann kann man dies mit dem folgenden Befehl erfragen:

```
Get-WindowsFeature Hyper-V
```

Übergibt man als Argument *Hyper-V**, dann zeigt das Cmdlet unter Windows 8 und Server 2012 auch an, ob die Management-Tools installiert wurden. Außerdem bietet die neue Version des Cmdlets die Möglichkeit, die Ausstattung eines Servers mit dem Parameter *-ComputerName* remote abzufragen.

Unter Server 2008 R2 finden sich die Tools für Hyper-V unter RSAT, so dass man dort mittels

```
Get-WindowsFeature RSAT-Hyper-V*
```

herausfinden muss, ob sie installiert sind.

Hyper-V per Powershell

Um Hyper-V zu installieren, gibt es unter Windows Server 2008 R2 das Cmdlet Add-WindowsFeature, unter Server 2012 (R2) heißt es Install-WindowsFeature (und ist aus Kompatibilitätsgründen auch über das vordefinierte Alias Add-WindowsFeature ansprechbar).

Im einfachsten Fall installiert man auf beiden Server-Versionen die Hyper-V-Rolle, indem man den folgenden Befehl aufruft:

```
Add-WindowsFeature Hyper-V
```

Es ist sinnvoll, vorab zu simulieren, wie der Vorgang ablaufen würde, indem man den Parameter *-WhatIf* anfügt.

Unter Windows 8.x und Server 2012 akzeptiert das Cmdlet zudem die Option *-IncludeManagementTools*, um den Hyper-V Manager zu installieren. Eine Verbesserung in der neuen Version besteht darin, dass man durch Angabe von *-ComputerName* die Hyper-V-Rolle auch auf einem entfernten Server installieren kann.

Nachdem die Aktivierung von Hyper-V einen Neustart erfordert, kann man diesen schließlich über den Schalter *-restart* veranlassen. Er ist bereits unter Server 2008 R2 verfügbar.

Hyper-V mit DISM aktivieren

Das Deployment Image Servicing and Management (DISM) ist nicht nur Bestandteil von WAIK und dem Windows ADK, sondern ein in Windows integriertes Dienstprogramm. Es kann Packages nicht bloß zu Windows-Images im WIM-Format hinzufügen, sondern auch zu einem aktiven Betriebssystem. Um herauszufinden, ob Hyper-V installiert ist, gibt man

```
dism /online /Get-FeatureInfo /
  FeatureName:Microsoft-Hyper-V
```

ein. Sollen die Virtualisierungsfähigkeiten hinzugefügt werden, dann erledigt man das mit

```
dism /online /enable-feature /
  FeatureName:Microsoft-Hyper-V
```

DISM lässt sich nur auf die lokale Maschine anwenden, eine Remote-Installation von Rollen ist nicht möglich.

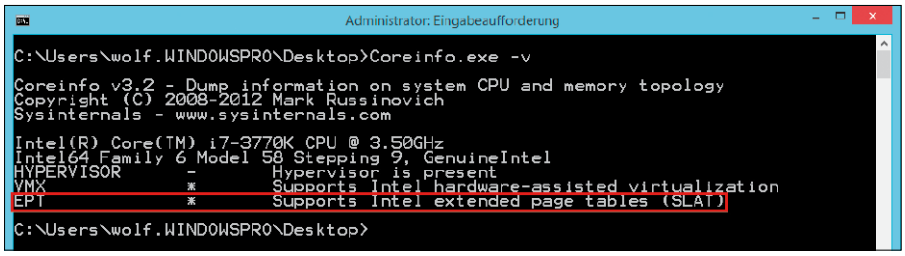
Virtual-PC-Nachfolger: Client-Version von Hyper-V einrichten

Zum Lieferumfang der 64-Bit-Ausführung von Windows 8 und 8.1 ab der „Pro"-Edition gehört die Client-Version von Hyper-V, die dem bisherigen Desktop-Virtualisierer Virtual PC nachfolgt. Allerdings unterscheiden sich die beiden Produkte grundlegend in ihrer Architektur, so dass die Installation von Hyper-V nicht nur anders erfolgt, sondern auch deutlich höhere Anforderungen an die Hardware stellt.
Windows 8.x Hyper-V stimmt nicht nur im Namen mit seinem Gegenstück unter Windows Server überein, vielmehr beruht er auf der gleichen Technik und ist somit ein Bare-Metal-Hypervisor. Im Unterschied zu Vmware Workstation, Virtualbox oder zu Virtual PC übernimmt er die Kontrolle über die Hardware, bevor ein Betriebssystem startet. Die anderen Produkte benötigen dagegen als Grundlage ein Host-Betriebssystem.

Kompatibilität von VMs zwischen Client und Server

Die Portierung einer Server-Komponente auf den Client hat Vor- und Nachteile. Letztere bestehen vor allem im Benutzererlebnis, weil eine so enge Integration von VMs wie beim Seamless-Modus von Virtual PC nicht gegeben ist. Dafür erbt Windows 8.x die Skalierbarkeit des Server-Hypervisors und ist mit diesem kompatibel, so dass sich virtuelle Maschinen zwischen Client und Server migrieren lassen.
Ein wesentlicher Unterschied zwischen der Client- und Server-Implementierung besteht

Mit Powershell lässt sich herausfinden, ob Hyper-V und die zugehörigen Verwaltungs-Tools installiert sind.



Dieser PC erfüllt die Hardware-Voraussetzungen für die Installation von Windows 8.1 Hyper-V.

darin, dass Windows 8.1 Hyper-V eine CPU voraussetzt, die Second Level Address Translation (SLAT) beherrscht, manchmal auch mit Extended Page Table (EPT) bezeichnet. Am Server ist eine solche nur erforderlich, wenn Remote FX genutzt werden soll. Diese Bedingung erfüllen die neuesten Baureihen der Intel -Prozessoren (i5, i7) oder aktuellere AMD-CPUs.

SLAT-Fähigkeit prüfen

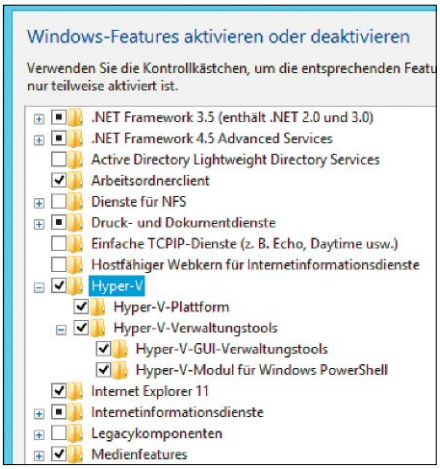
Vor der Installation von Windows 8.x Hyper-V ist es daher sinnvoll zu prüfen, ob das System die Hardware-Anforderungen erfüllt. Zu diesen gehören eine Ausstattung mit mindestens 4 GB RAM sowie die erwähnte SLAT-fähige CPU. Letztere lässt sich am einfachsten mit Hilfe des kostenlosen Tool Coreinfo (auf der Heft-DVD und über *http://bit.ly/1npSuZH*) von Sysinternals ermitteln. Der Aufruf von

```
coreinfo -v
```

zeigt an, ob ein Hypervisor installiert ist, ob die CPU Unterstützung für Hardware-basierte Virtualisierung bietet und ob sie SLAT beherrscht. Ist das jeweilige Feature mit einem „*" markiert, dann ist es vorhanden, bei einem „-„ nicht.

Hyper-V über Systemsteuerung

Wenn die Systemvoraussetzungen gegeben sind, dann kann die Installation erfolgen. Der Hypervisor ist ein Windows-Feature, das sich unter „Systemsteuerung → Programme" hinzufügen lässt. Hat man zuvor auf die Prüfung der Hardware verzichtet, dann kann man hier leicht in die Irre geführt werden, weil Hyper-V auch dann in der Liste auftaucht, wenn der Rechner dafür gar nicht geeignet ist.
Das liegt daran, dass man zwar das Kästchen mit der Beschriftung „Hyper-V" auswählen kann, aber im daran anschließenden Zweig der Feature-Liste nur die Verwaltungs-Tools untergebracht sind, also der Hyper-V Manager und das Hyper-V-Modul für Powershell. Beide sind für die Remote-Administration von VMs geeignet, so dass sie sich auch auf PCs installieren lassen, die nicht die Voraussetzungen für den Hypervisor erfüllen. Das gilt auch für die 32-Bit-Version von Windows 8, die entsprechende Ausführungen der Admin-Tools mitbringt.



Über die Systemsteuerung lassen sich die Verwaltungs-Tools getrennt vom Hypervisor installieren, etwa um andere Hosts remote zu administrieren.

Hyper-V über die Kommandozeile

Wer Hyper-V lieber über die Kommandozeile einrichtet, dem stehen dort die bekannten Mechanismen zur Paketverwaltung zur Verfügung. Dazu zählt einerseits DISM, das man auf die gleiche Weise aufruft wie am Server.
Die Entsprechung dazu in Powershell ist

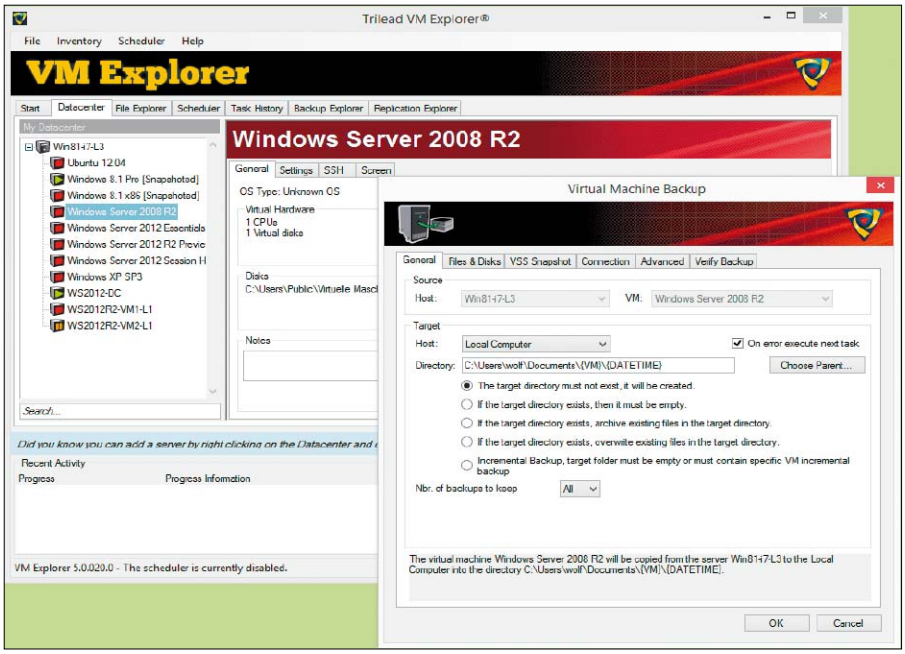
```
Enable-WindowsOptionalFeature
  -Online -FeatureName Microsoft-
  Hyper-V -All
```

In beiden Fällen benötigt man eine Kommandozeile mit Administratorrechten. ■

Kostenlose Tools für Hyper-V

Mit dem steigenden Interesse an Microsofts Hypervisor nimmt auch die Zahl der Drittanbieter zu, die Tools für das Management von Hyper-V entwickeln. Hier finden Sie die nützlichsten kostenlosen Programme.

VON WOLFGANG SOMMERGUT



Die Free Edition des Trilead Explorer sichert unbegrenzt viele VMs auf maximal zwei Hosts.

ZUGEGEBEN: Viele der kostenlosen Tools für Hyper-V sind nur Einsteigerversionen von kostenpflichtiger Software, aber es gibt auch ein paar gute Open-Source-Programme.

Während die zahlreichen Freeware-Tools für Vmware ESXi (*http://bit.ly/1hcb9ar*) nur dem Management des Hypervisors oder virtueller Maschinen dienen, besteht aufgrund der Architektur von Hyper-V dort ein Bedarf an Programmen, die ein größeres Spektrum abdecken. Nachdem bei Hyper-V immer zumindest eine Core-Variante von Windows in der Parent Partition läuft, sind auch Tools für die Verwaltung dieser spartanischen Version des Betriebssystems von Nutzen.

Aufgrund der Vorreiterrolle von Vmware bei der x86-Virtualisierung gibt es für ESXi und Vsphere mehr Tools als für Hyper-V. Das verstärkte Engagement von Microsoft führt nun aber dazu, dass viele Hersteller aus dem Vmware-Umfeld mit ihren Werkzeugen nun auch Hyper-V unterstützen.

Backup und Replikation

Hyper-V in Windows Server 2012 R2 bringt eine Basisausstattung für die Datensicherung und das Desaster Recovery mit. So ist Windows Server Backup nun in der Lage, ausgewählte VMs zu sichern oder wiederherzustellen, während sie vorher nur im Rahmen eines Volume-Backups gesichert wurden (und obendrein war ein Registry-Eingriff nötig). Für ein einfaches Desaster Recovery ist Hyper-V Replica vorgesehen. Dieses kann für kleine Umgebungen reichen, dagegen wird man bei Windows Server Backup aufgrund seiner Beschränkungen (kein Support für SMB 3 und Cluster Shared Volumes) selbst bei der Sicherung einzelner Hosts Alternativen in Erwägung ziehen.

Veeam Backup Free Edition

Wie das Vollprodukt Backup & Replication unterstützt die Free Edition (Infos über *http://bit.ly/1hcb9ar*) sowohl Vmware ESXi als auch Hyper-V. Sie eignet sich für das Sichern oder das Migrieren einzelner VMs. Zu den Features zählen das Wiederherstellen ganzer VMs oder einzelner darin enthaltener Dateien (File Level Restore). Durch die Integration des ehedem eigenständigen Fastscp lässt sich die Free Edition auch nutzen, um VMs zwischen Hosts zu kopieren. Komprimierung und Deduplizierung sorgen für kompakte Backup-Archive. Die in Version 7 neue Tape-Unterstützung kann Backups wiederherstellen, die von NT Backup auf Band geschrieben wurden.

Download: *http://bit.ly/1i5U8PZ*

Altaro Hyper-V Backup Free

Altaro, ein relativ neuer Hersteller von Backup-Software für virtuelle Umgebungen, bietet

ebenfalls eine kostenlose Einsteigerversion von Hyper-V Backup (auf Heft-DVD, Infos über *http://bit.ly/1jDD15E*). Diese ist auf die Sicherung von zwei VMs beschränkt und bietet weniger Funktionen als die Pro-Version. So lässt sie keine Wiederherstellung einzelner Dateien aus einer VM zu und gestattet keinen Restore von VHDs unter einem anderen Dateinamen. Sie unterstützt jedoch das Backup laufender VMs und eine inkrementelle Sicherung.
Download: *http://bit.ly/1reHr82*

Trilead Explorer

Die Software der Schweizer Trilead AG sichert sowohl Vmware Vsphere als auch Hyper-V. Die kostenlose Ausführung (auf Heft-DVD) hat durchaus praktischen Nutzen, auch wenn ihr einige Features der kostenpflichtigen Version fehlen. Sie kann Backups von beliebig vielen (eingeschalteten) VMs auf maximal zwei Hosts erstellen, die sie in komprimierter Form speichert. Sie kopiert Dateien zwischen verschiedenen Gastsystemen per Drag & Drop.
Die Free Edition unterstützt aber keine inkrementelle Datensicherung, keine Wiederherstellung einzelner Dateien und keine zeitgesteuerte Datensicherung.
Download: *http://bit.ly/1muNdjI*

HV Backup

HV Backup (auf Heft-DVD) ist ein Open-Source-Tool für die Kommandozeile, das ein .NET Framework 3.5 voraussetzt. Die Software nutzt den VSS Writer für Hyper-V, um VMs in einem konsistenten Zustand zu sichern. Sie unterstützt zudem das Backup von VMs auf Cluster Shared Volumes (*http://bit.ly/1gAlWaH*). Das Tool erzeugt für jede VM ein eigenes ZIP-Archiv.
Download: *http://bit.ly/1txtlAx*

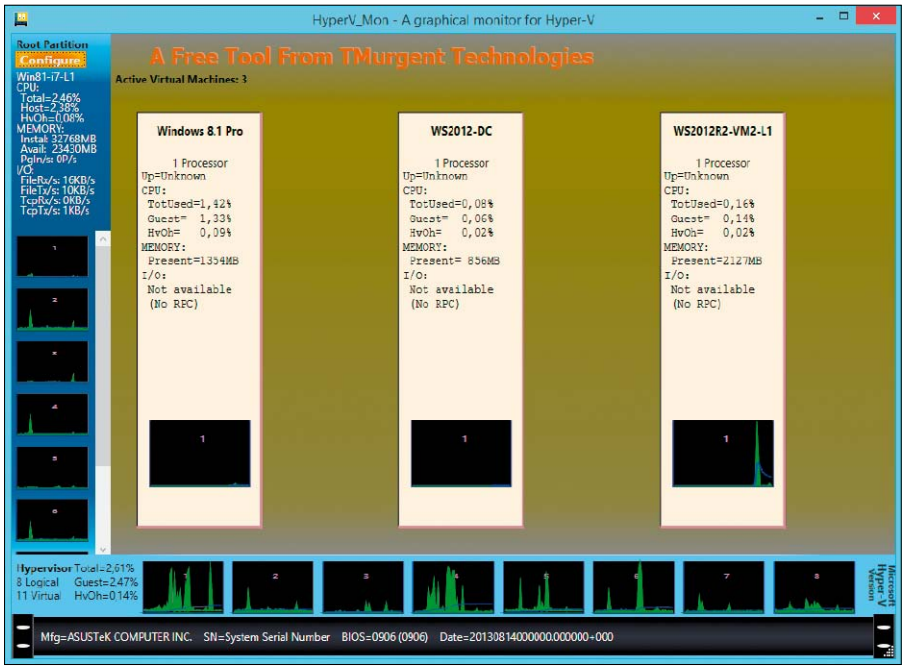
Monitoring und Reporting

Vmturbo Virtual Health Monitor

Dabei handelt es sich um ein Tool, das einige Features des mächtigen Hauptprodukts für das Virtualisierungs-Management bietet. Die kostenlose Version erfasst Leistungsdaten, sie benachrichtigt beim Auftreten von Kapazitäts- und Performance-Problemen und erlaubt das Erstellen von Berichten. Die Nutzung ist nicht auf eine bestimmte Zahl von CPUs oder Servern eingeschränkt. Der Virtual Health Monitor unterstützt neben Hyper-V auch Vmware, KVM und Xenserver.
Download: *http://bit.ly/1rjTuii*

Veeam ONE Free Edition

Wie das kostenlose Backup Veeam One (auf Heft-DVD) unterstützt sowohl Vmware als auch Hyper-V. Die Software sammelt Performance-Daten von den Servern, zeigt die Prozesse auf dem Host und in den VMs an und versendet Alarmmeldungen bei Auftreten kritischer Ereignisse. Die Free Edition kennt keine Einschränkungen hinsichtlich der Zahl an Servern oder Benutzern, es fehlen ihr aber eine Reihe von fortgeschrittenen Funktionen der Vollversion. Ein Update ist ohne Neuinstallation durch bloße Eingabe eines Lizenzschlüssels möglich.
Download: *http://bit.ly/1fkCAL9*



Hypervmon ist ein leichtgewichtiges Monitoring-Tool, das Auskunft über die wichtigsten Systemparameter gibt.

Solarwinds Free VM Monitor

Die Software dient vor allem dem Health-Monitoring von VMs und Hosts. Sie liefert dabei Daten in Echtzeit zur Auslastung von CPU, Arbeitsspeicher oder zur Zahl aktiver VMs. Zusätzlich ist es möglich, für bestimmte Metriken Grenzwerte festzulegen, bei deren Überschreiten der Free VM Monitor den Administrator benachrichtigt. Die Software eignet sich nur zur Überwachung einzelner Hosts und liegt in separaten Ausführungen für Hyper-V und Vmware vor.
Download: *http://bit.ly/1k3EiEQ*

Manage Engine Free Hyper-V SM

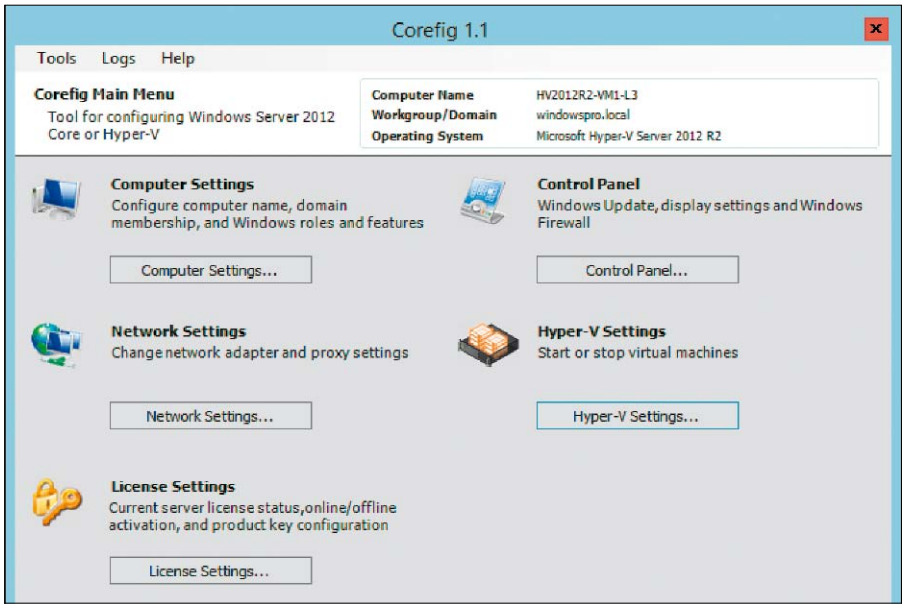
Der Free Hyper-V Monitor (auf Heft-DVD) überwacht ebenfalls einige wesentliche Systemparameter wie CPU-Last, RAM-Auslastung, Festplattennutzung und Netzwerk-Traffic. Darüber hinaus listet das Tool alle konfigurierten VMs auf, sowohl aktive als auch inaktive. Der Ressourcen-Verbrauch von Hosts lässt sich nach virtuellen Maschinen aufschlüsseln. Auch Manage Engine sieht die Definition von Grenzwerten vor, bei deren Überschreiten eine Warnung erzeugt wird. Das Tool ist auf die Überwachung von zwei Hyper-V-Hosts beschränkt.
Download: *http://bit.ly/1eZY9Gu*

Hypervmon

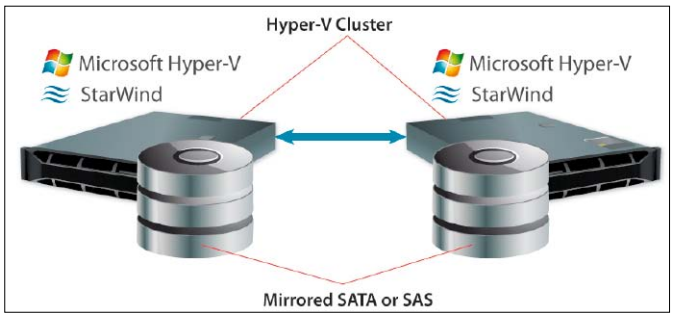
Der Hersteller Tmurgent empfiehlt seine Software nicht für das permanente Monitoring von Hyper-V, sondern sieht ihren Nutzen primär in stichprobenartigen Überprüfungen der Systemauslastung. Zu diesem Zweck liefert das Tool die grundlegenden Daten wie die CPU-Nutzung, aufgeschlüsselt nach Host und Gastsystemen. Zusätzlich gibt es Auskunft über den gesamten und den verfügbaren Speicher sowie über File- und Netzwerk-I/O. Hypervmon erfordert die .NET Runtime 4.0 und muss nicht installiert werden.
Download: *http://bit.ly/1txw1OD*

VM Migration Test Wizard

Dieses Open-Source-Tool Virtual Machine Migration Test Wizard (auf Heft-DVD) berichtet nur über einen bestimmten Aspekt von Hyper-V, nämlich über die Chancen für eine erfolgreiche Migration von VMs auf andere Hosts. Dabei gibt es Auskunft darüber, ob sich eine VM per Live Migration, also der empfindlichsten Variante, auf einen anderen Server übertragen lässt. Es berücksichtigt auch manuelle Formen der Migration wie Export/Import oder die Wiederherstellung von Backups.
Das Tool eignet sich nicht nur dazu, um unmittelbar vor einer Migration zu prüfen, ob diese



Corefig eignet sich in erster Linie für grundlegende Management-Aufgaben in Server Core und Hyper-V Server.



Starwind Native SAN for Hyper-V Free Edition erlaubt die Einrichtung von hochverfügbarem Shared Storage.

gelingen kann. Vielmehr lässt es sich schon einsetzen, um beim Hinzufügen eines Hosts zu einem Cluster herauszufinden, ob Inkompatibilitäten drohen.
Download: *http://bit.ly/1reMXHL*

Management: Server Core

Die Architektur von Hyper-V erfordert ein vollwertiges Betriebssystem in der Parent Partition, das im Vergleich zu den Gästen in den VMs eine privilegierte Position einnimmt. Microsoft empfiehlt für diese Aufgabe die Installationsoption Server Core, wo keine weiteren Server-Rollen oder Anwendungen laufen sollen.
Dann lassen sich der Hypervisor und die virtuelle Maschinen aber trotzdem noch mit Powershell mit ihren neuen Cmdlets für Hyper-V verwalten. Wenn man dagegen grafische Tools bevorzugt, hilft die folgende Software.

Core Configurator 2.0

Das Open-Source-Programm Core Configurator (auf Heft-DVD und über *http://bit.ly/1lzFT4S*) war eines der ersten Tools, das für die wichtigsten Aufgaben unter Server Core eine GUI bereitstellte. Es besteht aus einer Reihe von Powershell-Scripts. Beim Management von Hyper-V beschränkt es sich auf wenige und einfache Funktionen, nämlich das Starten und Stoppen von virtuellen Maschinen. Darüber hinaus bietet es eine Thumbnail-Ansicht von aktiven VMs.
Die Software läuft unter Server 2008 und 2008 R2, jedoch nicht unter Server 2012 (R2). Für die neuen Ausführungen des OS ist der Nachfolger Corefig (auf Heft-DVD) zuständig.
Download: Corefig, *http://bit.ly/1mzZmX1*

5nine Manager for Hyper-V

Beim 5nine Manager (auf Heft-DVD) handelt es sich um ein Tool, das die meisten Aspekte bei der Konfiguration von Hyper-V-Hosts und VMs abdeckt. Es kann VMs anlegen, starten und herunterfahren, Snapshots erstellen und zu solchen wieder zurückkehren. Außerdem lässt es sich einsetzen, um die Einstellungen einer VM zu bearbeiten oder virtuelle Netzwerke zu konfigurieren. Nur RDP-Verbindung zu Gastsystemen kann das Tool nicht aufbauen.
Aufgrund seines Funktionsumfangs eignet sich der 5nine Manager als Ersatz für den Hyper-V Manager von Microsoft. Gerade in gemischten Umgebungen aus Server 2008 (R2) und Server 2012 (R2) ist der 5nine Manager die bessere Wahl, weil er mehrere Versionen des Hypervisors verwalten kann.
5nine Manager kann wahlweise auf einem Client, auf einer Vollinstallation von Windows Server oder auf der Core-Variante installiert werden. Es setzt .NET Framework 4.0. voraus.
Download: *http://bit.ly/1rjXuQ7*

Storage-Management

Starwind iSCSI SAN Free Edition

Bei Starwind iSCSI SAN Free (auf der Heft-DVD) handelt es sich nicht direkt um ein Management-Tool für Hyper-V, sondern um ein iSCSI-Target mit einer Reihe von Zusatzfunktionen. Dazu zählen ein kontinuierliches Backup, Deduplizierung, Snapshots und Thin Provisioning. Man kann die kostenlose Version von Starwind iSCSI SAN nutzen, um einen Windows-Rechner als Shared Storage für Hyper-V (SAN oder NAS) einzusetzen. Darüber hinaus lässt sich die Software dem Hersteller zufolge in der Parent Partition des kostenlosen Hyper-V Server installieren. Die beiden Freeware-Produkte könnte man daher zu einem Billig-SAN kombinieren, beispielsweise für Testumgebungen.
Download: *http://bit.ly/1hcu70x*

VHD(X)-Konvertierung

Die Hersteller von Virtualisierungssystemen implementieren aus naheliegenden Gründen nur Funktionen für den Import, aber nicht für den Export in Fremdformate. Hier springen Drittanbieter mit kostenlosen Tools ein, die eine Umwandlung in beiden Richtungen ermöglichen. Siehe dazu unsere ausführliche Übersicht für Konvertierungs-Tools (Infos über *http://bit.ly/1jvx8q0*).
In Windows Server 2012 Hyper-V führte Microsoft mit VHDX ein weiteres Format für virtuelle Festplatten ein. Für die Konvertierung zwischen VHD und VHDX benötigt man jedoch keine Zusatzprogramme, das lässt sich mit Bordmitteln erledigen (*http://bit.ly/1gP8ikb*).
VHDs vergrößern, verkleinern, kompaktieren – aufgrund der spartanischen Mittel, die Windows 7 und Server 2008 (R2) für diese Zwecke bieten, entstanden mehrere kostenlose Tools, um diese Lücke zu füllen. Dazu zählen etwa VHD Resizer oder VHD Tool (beide auf DVD)
Download: *http://bit.ly/1k3L9OF*
Unter Windows Server 2012 entfällt zunehmend die Notwendigkeit für solche Produkte, weil Powershell dank vieler neuer Cmdlets für das Management von Hyper-V diesen Job selbst übernehmen kann. ■

PC-WELT

Die **MAGAZIN-APP** für iPad & iPhone

Lesen Sie PC-WELT, AndroidWelt, LinuxWelt, GalaxyWelt und alle Sonderhefte digital.

» Alle Ausgaben immer dabei

» Alle DVD-Inhalte inkl. Vollversionen

1. Ausgabe GRATIS für alle!

Kostenlos für Ihr iPad oder iPhone downloaden:

www.pcwelt.de/ios7

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Tipps für virtuelle Laufwerke

VHD(X) ist nicht nur das Format für virtuelle Laufwerke in Hyper-V, sondern wird von Windows auch für andere Zwecke genutzt. Bordmittel erlauben daher ein umfassendes Management dieser virtuellen Disks.

VON WOLFGANG SOMMERGUT

MICROSOFT FÜHRTE MIT WINDOWS 8 unter der Bezeichnung VHDX ein neues Format für virtuelle Festplatten ein. Es sprengt einige Limits des bisherigen VHD-Formats und unterstützt gleichzeitig alle Features des alten Formats wie das Booten des Betriebssystems von einem virtuellen Datenträger.

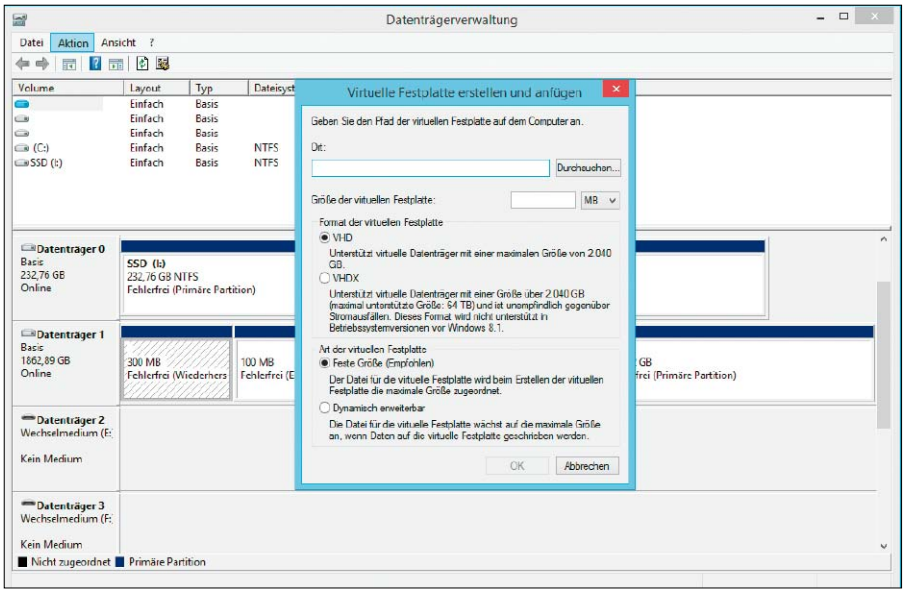
Das für Virtual PC und Virtual Server entwickelte Virtual Hard Disk (VHD) ist auf eine Größe von 2 TB begrenzt, so dass für VMs mit Bedarf an viel Plattenplatz bisher nur der Einsatz einer Pass-Through-Disk übrig blieb. Diese hat aber beispielsweise den Nachteil, dass sie die Live-Migration von VMs beeinträchtigt und keine Snapshots zulässt. Mit VHDX erhöht sich die Größenbeschränkung virtueller Disks von 2 auf 64 TB, so dass die meisten VMs damit ihr Auskommen haben sollten.

Standardmäßig hat VHDX größere Blöcke als VHD (32 MB für fixe und dynamische Laufwerke, 2 MB für differenzielle). Außerdem harmoniert VHDX besser mit Advanced Format Disks, weil es sich an 4 KB großen Sektoren ausrichten kann (Alignment).

Zu den weiteren Vorteilen gehören:

- Das VHDX-Format führt ein Journal über Änderungen der Metadaten, so dass es robuster gegenüber Hardware-Ausfällen ist.
- Es sieht die Möglichkeit vor, benutzerspezifische Metadaten zu hinterlegen.
- Die Performance von VHDX soll zumindest gleich gut oder höher sein als jene von VHD.

Windows 8.x und Server 2012 (R2) bieten eine Reihe neuer Techniken, um VHD- und VHDX-Laufwerke zu erstellen, anzufügen oder zu trennen. Dazu zählt besonders die Unterstützung für Powershell, aber auch die engere Integration in den Explorer.



In der Datenträgerverwaltung kann man unabhängig von Hyper-V virtuelle Laufwerke im VHD(X)-Format erzeugen.

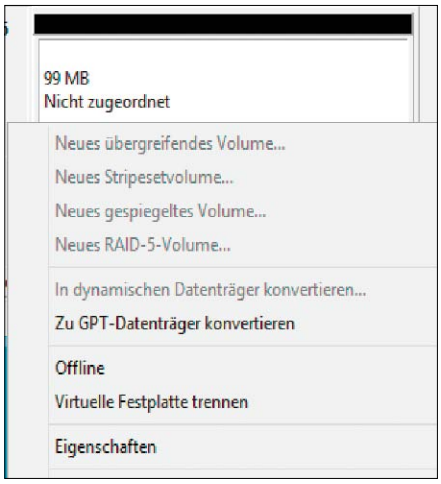
Erzeugen von VHDX über Tools mit einer grafischen Bedienerführung

Virtuelle Datenträger lassen sich nicht nur mit den Management-Tools für Hyper-V-Manager erstellen, um sie einer VM zuzuordnen. Vielmehr ist das Betriebssystem dazu selbst in der Lage und das auch dann, wenn der Hypervisor gar nicht installiert wurde.

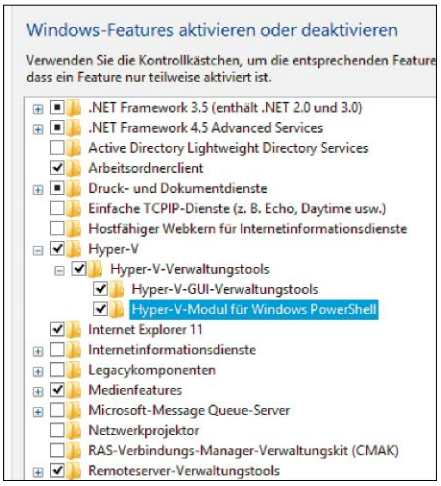
In den meisten Fällen wird man jedoch eine virtuelle Festplatte im Hyper-V-Manager erstellen, wenn man eine neue VM anlegt. Alternativ lässt sich dort auch für eine vorhandene VM nachträglich eine VHDX erzeugen und dieser zuordnen. In beiden Fällen bietet der zuständige Dialog die Wahl zwischen dem alten VHD- und dem neuen VHDX-Format.

Um eine neue VHDX unabhängig von Hyper-V zu erstellen, kann man den Weg über die GUI beschreiten oder Powershell nutzen. Wer die grafische Oberfläche bevorzugt, kann wie bisher für VHDs die Datenträgerverwaltung verwenden, wo der Menüpunkt „Aktion → Virtuelle Festplatte erstellen“ für diesen Zweck zuständig ist. Der anschließende Dialog bietet die Wahl zwischen VHD und VHDX.

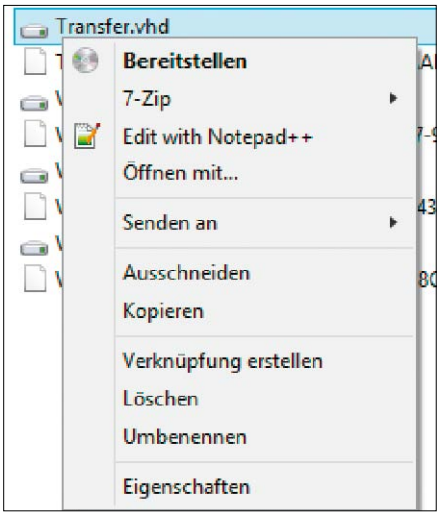
Die frisch angelegte VHDX lässt sich in der Datenträgerverwaltung gleich partitionieren und formatieren, wobei sich der entsprechen-



Angehängte VHDX lassen sich in der Datenträgerverwaltung von Windows ganz einfach wie physikalische Datenträger partitionieren und formatieren.



Das Hyper-V-Modul für Powershell zur Verwaltung von VHDs kann man auch dann installieren, wenn der Hypervisor auf dem System nicht vorhanden ist.



Unter Windows 8.x lassen sich VHDX-Laufwerke über den Befehl „Bereitstellen“ direkt im Explorer mounten.

de Befehl nicht im Kontextmenü des Datenträgerabbilds befindet, sondern in jenem der dazugehörigen Beschriftung.

Virtuelle Festplatte mittels Powershell erstellen

Eine zusätzliche Option zum Erzeugen von virtuellen Festplatten bieten Windows 8.x und Server 2012 (R2) durch das neue Hyper-V-Modul für Powershell. Am Server installiert man dieses über den Server Manager, und zwar über „Rollen und Features hinzufügen“. Im Dialog für die Auswahl von Features muss man unter „Rollenverwaltungstools → Hyper-V-Verwaltungstools“ das „Hyper-V-Modul für Windows Powershell“ aktivieren. Am Client geht man dagegen über „Systemsteuerung → Programme → Windows-Funktionen aktivieren oder deaktivieren“. Dort findet sich das Powershell-Modul unter „Hyper-V → Hyper-V-Verwaltungstools“. Wenn das Powershell-Modul installiert ist, kann man dessen Cmdlets sofort und ohne Aufruf der Import-Anweisung verwenden. Um eine VHDX zu erstellen, gibt man einen Befehl nach folgendem Muster ein:

```
New-VHD -VHDFormat VHDX -Path
 Test.vhdx -Dynamic -SizeBytes
 50MB
```

Möchte man statt einer dynamischen VHDX eine fixe anlegen, dann ersetzt man *-Dynamic* durch *-Fixed*.

VHDX über Bedienerführung und Powershell mounten

Virtuelle Festplatten vom Typ VHDX kann man wie von VHDs gewohnt über die Datenträgerverwaltung mounten, die Rede ist dabei von „Anfügen“. Dort lassen sie sich auch wieder trennen. Einfacher geht es jedoch, indem man eine VHD oder VHDX im Explorer nur doppelt anklickt. Dadurch wird die virtuelle Festplatte automatisch angefügt, und sie erhält standardmäßig gleich einen Laufwerksbuchstaben. Sie lässt sich wieder trennen, indem man im Explorer unter „Computer“ das Kontextmenü des Laufwerks öffnet, das der virtuellen Festplatte zugeordnet ist, und dort den Befehl „Auswerfen“ ausführt.

Unter den zahllosen Cmdlets des Powershell-Moduls für Hyper-V finden sich natürlich auch welche, die für das Mounten und Trennen von virtuellen Festplatten zuständig sind. Ersteres übernimmt Mount-VHD, Zweiteres Dismount-VHD. Zum Beispiel würde

```
Mount-VHD -Path c:\test\test.vhdx
 -ReadOnly
```

die virtuelle Festplatte „Test.vhdx“ im Nur-Lesen-Modus anfügen.

Vorsicht beim Verkleinern von VHDX-Laufwerke

Das mit Windows 8 und Server 2012 eingeführte VHDX-Format für virtuelle Laufwerke erlaubt nicht nur Disks mit einer größeren Kapazität, sondern es vereinfacht auch das Verkleinern und Komprimieren von Datenträgern. Dank der neuen Powershell-Cmdlets kann man solche Aktionen gleich auf mehrere VHDX-Dateien anwenden.

Bei allen Operationen, die ein virtuelles Laufwerk verändern, ist zu bedenken, dass diese wie physikalische Datenträger normalerweise Partitionen, Volumes und Dateisysteme enthalten, die vom Gastbetriebssystem verwaltet werden. Unkontrollierte Eingriffe von außen können hier schnell Chaos stiften, etwa wenn man eine VHD(X) direkt unter Windows mountet und bearbeitet. Aus diesem Grund hat Vmware die Funktionen zum Verkleinern von VMDKs aus seinen Produkten entfernt.

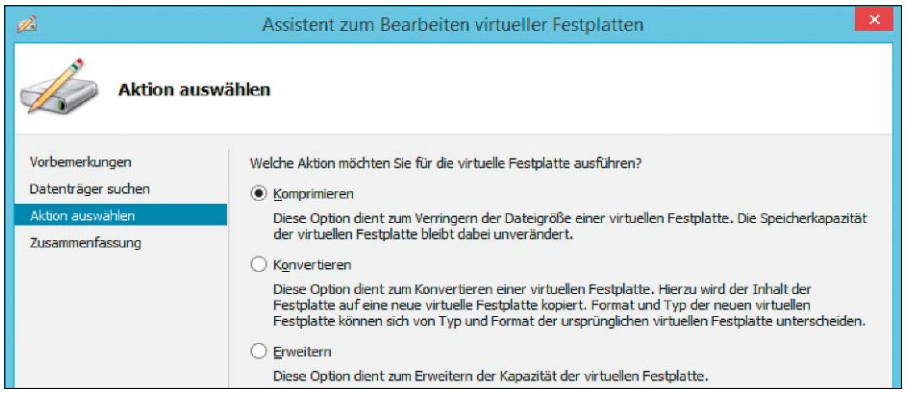
Optimierung nur von Offline-VHDX

Abhängig von den File-Systemen, die eine VM intern verwendet, können externe Tools virtuelle Datenträger nur eingeschränkt warten. Beispielsweise ist das Zurückgewinnen unbenutzter Blöcke in vielen Fällen unmöglich, wenn das Gastbetriebssystem sie nicht mit Nullen überschreibt.

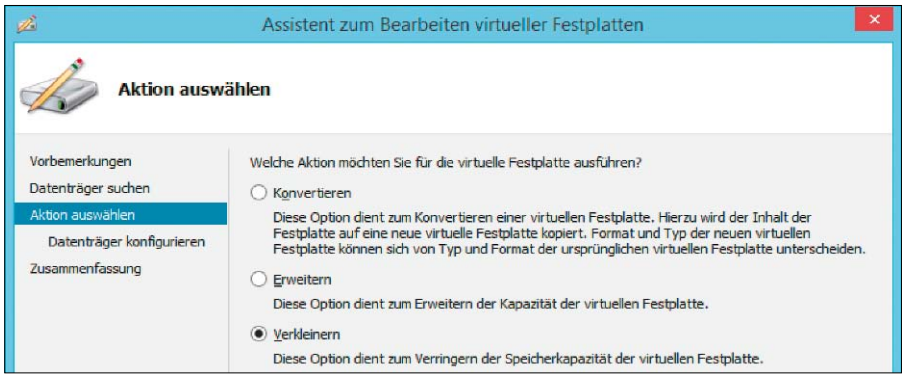
Das Verkleinern von Datenträgern setzt voraus, dass die Partitionen erst von innen geschrumpft werden, so dass anschließend die VHDX von außen den frei gewordenen Platz abgeben kann.

Auch die Verwaltung von virtuellen Laufwerken durch den Hypervisor droht durch externe Manipulation von VHDX-Dateien in Unordnung zu geraten. Das kann vor allem dann passieren, wenn Snapshots von einer VM angelegt wurden. An sich harmlose Veränderungen der übergeordneten VDHX haben dann unangenehme Folgen. Daher sollte man virtuelle Datenträger nicht konvertieren, vergrößern oder verkleinern, ehe man nicht die Snapshots gelöscht hat. Außerdem dürfen virtuelle Datenträger während solcher Operationen nicht genutzt werden.

Unter Windows 8.x und Server 2012 (R2) bietet der Hyper-V Manager für VHDX-Laufwerke zwei Optionen zur Reduktion des Platzverbrauchs. Zum einen handelt es sich dabei um das Komprimieren, das auch schon Hyper-V 2008 R2 für VHDs angeboten hat. Hinzu kommt nun das Wizard-geführte Verkleinern von VHDX-Dateien, das für VHDs nicht unterstützt wird. Wenn man sich daher beim alten Format das umständliche manuelle Umkopieren ersparen



Der Assistenz zum Bearbeiten virtueller Festplatten kann VHDX je nach Typ komprimieren oder verkleinern.



Eine VHDX lässt sich nur verkleinern, wenn die enthaltenen Partitionen nicht den gesamten Speicherplatz belegen.

möchte, um Plattenplatz zu sparen, dann sollte man es in VHDX konvertieren und dann dessen neue Funktion in Anspruch nehmen.

Komprimieren dynamischer Laufwerke

Das Komprimieren eines virtuellen Laufwerks ist nur für dynamische VHDX-Laufwerke möglich. Es soll der Tendenz der Datenträger entgegenwirken, ständig zu wachsen, auch wenn die Menge der enthaltenen Daten kaum zunimmt. Der Hypervisor kann nämlich den Platz von gelöschten Dateien nicht freigeben, wenn er ihn nicht als ungenutzten Bereich erkennt. Beim Komprimieren wird eine VHDX mit der Partition verbunden, auf der sie abgelegt ist, und Windows kann dann das virtuelle Laufwerk untersuchen. Dies funktioniert jedoch nur für Partitionen, die mit NTFS formatiert wurden, weil es dort je nach verwendeter Methode erkennt, welche Blöcke tatsächlich von Dateien belegt sind. Bei anderen File-Systemen muss man geeignete Tools verwenden, die ungenutzte Bereiche mit Nullen überschreiben.

Das Komprimieren ordnet dann die verwendeten Blöcke ähnlich wie beim Defragmentieren neu an und gibt die nicht genutzten frei. Im Hyper-V Manager findet man dieses Feature wie die anderen Operationen für VHDX-Dateien unter „Aktionen → Datenträger bearbeiten“. Der Vorgang ist Wizard-geführt und startet nach dem Auswählen der gewünschten VHD beziehungsweise VHDX.

So komprimieren Sie VHDX mit Hilfe von Powershell

Während das grafische Tool nur das Komprimieren einzelner virtueller Laufwerke erlaubt und dabei bloß die Standardmethode für einen bestimmten Typ ausführt, kann man in Powershell diesen Vorgang besser steuern.

Bevor man mit der Rückgewinnung von Speicherplatz beginnt, will man sich wahrscheinlich einen Überblick über die Größe der VHDX-Dateien verschaffen, damit man nachher den Erfolg der Komprimierung messen kann. Folgender Befehl ermittelt den Platzverbrauch sämtlicher VHDX-Dateien in einem Verzeichnis:

```
$len=0; gci *.vhdx | foreach{$len
 += $_.length}; $len/1GB
```

Im nächsten Schritt startet man die Komprimierung der virtuellen Laufwerke mit Hilfe des Cmdlets Optimize-VHD. Dieses unterstützt den Parameter *-mode*, über den man eine der fünf zulässigen Methoden für die Komprimierung (Infos über *http://bit.ly/1gQtbLZ*) auswählen kann. Die besten Ergebnisse erzielt *full*, dafür dauert sie am längsten. Sie ist Standard bei VHDs, während bei VHDX die Variante *quick* zum Einsatz kommt, wenn man *-mode* nicht angibt. Möchte man alle VHDX in einem Verzeichnis optimieren, dann kann man dies zum Beispiel mit folgendem Aufruf tun:

```
Get-VHD *.vhdx | where {$_.VhdTy-
 pe -eq "Dynamic"} | Optimize-VHD
 -mode full
```

Über die Verwendung von *Get-VHD* kann man die virtuellen Laufwerke vom Typ dynamisch herausfiltern, denn nur sie lassen sich komprimieren. Wenn man anschließend den Gewinn an Speicherplatz sehen möchte, dann hilft dieser Befehl:

```
$olen=0; gci *.vhdx |
 foreach{$olen += $_.length};
 ($len - $olen)/1GB
```

Voraussetzung für ein vernünftiges Ergebnis ist natürlich, dass die Variable *$len* aus dem ersten Befehl noch unverändert vorhanden ist.

Komprimieren versus Verkleinern

Das Komprimieren einer VHDX ändert die Einstellungen eines virtuellen Datenträgers nicht. Der beim Anlegen definierte Höchstwert, den das Gastbetriebssystem als Kapazität des Laufwerks erkennt, bleibt unangetastet. Dagegen schränkt das Verkleinern den Speicherplatz aus der Sicht des Gastes ein, so dass Partitionen erst geschrumpft werden müssen, um die Dimensionen des Laufwerks reduzieren zu können. Diese Operation ist für VHDX mit fester Größe vorgesehen. Die Größe der Partitionen und Volumes muss man von innerhalb der VM anpassen, wo man die Mittel des Gastbetriebssystems nutzt. Im Fall von Windows wären dies die Datenträgerverwaltung oder „diskpart“.

Die anschließende Verkleinerung, die den Platz freigibt, der nicht durch Partitionen belegt ist, erfolgt wieder über den Hyper-V Manager oder mittels Powershell. Dort ist für diese Aufgabe das Cmdlet Resize-VHD zuständig, das VHDX-Dateien vergrößern und verkleinern kann. Im Normalfall wird man sämtlichen Platz zurückfordern, den man durch die Reduktion von Partitionen gewonnen hat. Der entsprechende Aufruf würde so aussehen:

```
Resize-VHD -Path <vDisk.vhdx>
 -ToMinimumSize
```

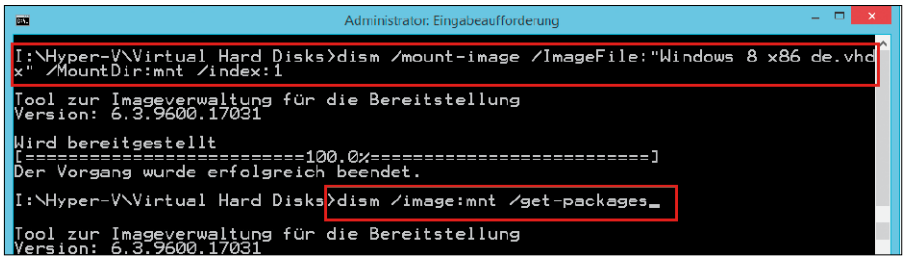
Möchte man das virtuelle Laufwerk um eine bestimmte Größe reduzieren, dann gibt man diese über den Parameter *-SizeBytes* an, also beispielsweise *-SizeBytes 256MB*.

Konvertieren von VHD und VHDX

Seit Windows 8 und Server 2012 verwendet Hyper-V das neue VHDX-Format als Vorgabe beim Erzeugen neuer virtueller Laufwerke. Gleichzeitig unterstützen die neuen Betriebssysteme weiterhin VHDs. Umgekehrt lassen sich aber VHDX-Dateien unter älteren Win-

dows-Versionen nicht nutzen, so dass man virtuelle Festplatten immer wieder zwischen den beiden Formaten konvertieren muss.
Konvertierungen werden nicht nur aufgrund der fehlenden Abwärtskompatibilität von VHDX zu VHD erforderlich sein, sondern beim Upgrade auf Windows 8 und Server 2012 auch in die umgekehrte Richtung, um die Vorteile des neuen Formats nutzen zu können. Entsprechend unterstützt Microsoft die bidirektionale Umwandlung. Bei der Koexistenz von VHD und VHDX gilt jedoch, dass es nicht möglich ist, ein Elternlaufwerk in dem einen Format mit einer davon abhängigen differenziellen Disk in dem anderen Format zu kombinieren.
Wie bei den meisten Operationen unter Windows Server 2012 gibt es für die Konversion zwischen VHD und VHDX sowohl eine GUI- als auch eine Powershell-Variante. Als grafisches Tool für diesen Zweck dient der Hyper-V-Manager, bei dem der „Assistent zum Bearbeiten virtueller Festplatten" für die Konvertierung zuständig ist. Er wird über den Befehl „Datenträger bearbeiten" gestartet und ist weitgehend selbsterklärend. Beim Konvertierungsvorgang bleibt die alte virtuelle Festplatte erhalten, und jene im ausgewählten Zielformat wird zusätzlich erstellt.

Die Konvertierung funktioniert zwischen VHD und VHDX sowie zwischen dynamisch und fest des gleichen Formats.



VHD(X) lassen sich in DISM nun mounten wie WIM-Archive, so dass man offline Updates einspielen kann.

Variante mit Convert-VHD

Um VHD- beziehungsweise VHDX-Dateien in das jeweils andere Format per Powershell zu überführen, muss das Hyper-V-Modul für Powershell installiert sein. Anschließend steht das Cmdlet Convert-VHD zur Verfügung, um die gewünschte Umwandlung zu erledigen. Es bietet mehr Kontrolle über die Eigenschaften der Zieldatei als der Hyper-V-Manager, zum Beispiel kann man dort auch die Blockgröße festlegen. Um eine VHD in eine VHDX zu konvertieren, könnte der Aufruf folgendermaßen aussehen:

```
Convert-VHD -Path test.vhd –Des
 tinationPath test.vhdx -VHDType
 Dynamic
```

Wie der Hyper-V-Manager belässt auch Convert-VHD die Quelldatei, man kann sie aber durch Angabe des Parameters *-DeleteSource* entfernen.

VHD(X) offline aktualisieren

Die in Windows 8.x, Server 2012 (R2) und im Windows ADK (Informationen dazu finden Sie über *http://bit.ly/1iepmpb*) enthaltene Version von DISM (Deployment Image Servicing and Management) kann nicht nur WIM-Images mounten und aktualisieren, sondern auch virtuelle Festplatten in den Formaten VHD und VHDX. Mit DISM kann man daher nun Updates oder Services Packs in ausgeschaltete VMs einspielen. Die Erweiterung des Funktionsumfangs schlägt sich bei DISM erwartungsgemäß in einer Reihe neuer Parameter nieder, mit denen man das Kommandozeilen-Tool ausführen kann. Dazu gehören zum einen solche zur Erstellung und Bearbeitung von WIM-Dateien, mit denen es die Aufgaben des ausgemusterten Imagex übernehmen kann. Zum anderen kommt eine Liste von Befehlen dazu, die sich auf WIM- und auf VHD(X)-Images anwenden lassen.
Diese Optionen erwarten in der Praxis noch weitere Angaben, die man teilweise über die Online-Hilfe abrufen kann, etwa durch

```
dism /Mount-Image /?
```

VHDs mounten

Ein Aufruf, mit dem man eine VHD(X)-Datei mounten kann, sieht beispielsweise so aus:

```
dism /mount-image /ImageFile:"d:\
 Virtual Machines\Windows7.vhd" /
 MountDir:mnt /index:1
```

Das Mount-Verzeichnis muss wie gewohnt leer sein und bereits existieren, die Pfadangaben dürfen auch relativ sein. Der Schalter */index* ist im Zusammenhang mit VHDs eigentlich nutzlos, weil sie im Gegensatz zu WIMs immer nur ein Abbild enthalten. Er muss aber dennoch verwendet werden.

Installierte Packages erfragen

Ist ein virtuelles Laufwerk gemountet, dann kann man mit all jenen Befehlen, die DISM mit dem Schalter */online* für das gerade ausgeführte Windows schon bisher anbot, auch Offline-VHDs bearbeiten. So lassen sich die installierten Packages beispielsweise mit

```
dism /image:mnt /get-packages
```

abfragen, wenn das Image in das Verzeichnis „.\mnt" gemountet wurde.

Package entfernen

Anschließend besteht die Möglichkeit, eines der über */Get-Packages* aufgelisteten Pakete mit */Remove-Package* zu entfernen:

```
dism /image:mnt /Remove-Package /
 PackageName: Package_for_KB98359
 0~31bf3856ad364e35~x86~~6.1.1.0
```

Packages installieren

Analog funktioniert das Hinzufügen von Paketen, dafür ist der Parameter */Add-Package* zuständig:

```
dism /image:mnt /Add-Package /
 PackagePath:c:\MeinPackage.cab
```

Für das Installieren von Packages sind Dateien im Format CAB und MSU zulässig, wobei bei einem Aufruf gleich mehrere davon angegeben werden können. In diesem Fall muss man dem Namen jeder Datei ein eigenes */PackagePath* voranstellen.

Unmount von VHDs

Nach getaner Arbeit muss man das Image explizit aushängen, um die Änderungen zu übernehmen oder zu verwerfen. Ein entsprechender Aufruf sieht beispielsweise so aus:

```
dism /unmount-image /mountdir:mnt
 /commit
```

Möchte man die Änderungen nicht behalten, dann verwendet man anstelle von */commit* die Option */discard*. ■

ESXi Preiswerte Virtualisierung

Für Einsteiger bietet Vmware einen funktionsreduzierten kostenlosen Hypervisor. Bei kleineren Installationen von Vsphere spart das Vcenter Server Appliance Geld. Die beiden Tools haben aber Grenzen.

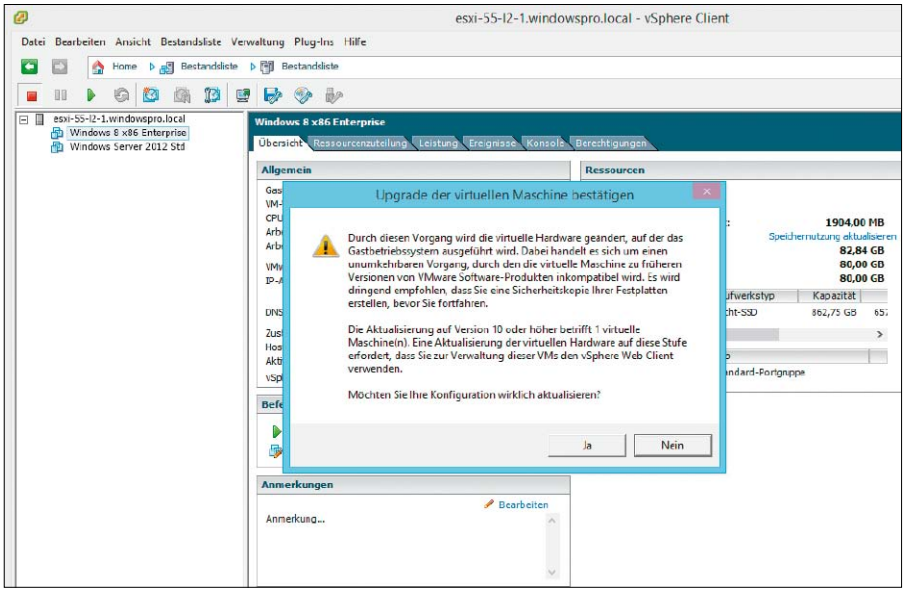
VON WOLFGANG SOMMERGUT

GLEICHZEITIG MIT DER FREIGABE von Vsphere 5.5 veröffentlichte Vmware wieder eine kostenlose Version des Hypervisors, die viele technische Neuerungen des Vollprodukts erbt. Gleichzeitig beseitigte der Hersteller das bisherige RAM-Limit. Diese Freude wird allerdings getrübt durch fehlende Management-Tools, mit denen sich die neuen Features vollständig nutzen ließen. Die kostenlose Version des Vmware Vsphere Hypervisor, so sein offizieller Name, eignet sich primär für Testumgebungen und kleine Installationen.

Keine 32-GB-RAM-Schranke mehr

Trotzdem profitiert jede neue Version von ESXi Free von den Fortschritten des Vollprodukts, die höchstens durch künstliche Limitierungen oder lizenzrechtliche Einschränkungen beschnitten werden. So galt bis ESXi 5.1 eine Obergrenze von 32 GB RAM, die im Host installiert sein durften. Diese fällt nun vollständig, so dass die gestiegene Leistungsfähigkeit des Hypervisors besser ausgenutzt werden kann.

Die höhere Skalierbarkeit von ESXi, eine der wichtigen Neuerungen von Vsphere 5.5, können die Benutzer der Gratisversion aber auch ohne 32-GB-Limit nicht voll ausschöpfen. Es bleibt nämlich weiterhin bei der Beschränkung des Servers auf zwei Prozessoren und einer VM auf maximal acht vCPUs. Letztere galt bisher auch für die Essentials Editions, wurde dort aber beseitigt. Die gesteigerten Fähigkeiten von ESXi 5.5 (siehe dazu PDF unter *http://bit.ly/1fpptbF*) sind zu einem erheblichen Teil eine Folge der Virtual Hardware 10, die auch in der Workstation 10 zum Einsatz kommt.



Der Vsphere Client kann zwar eine VM nicht auf die neueste virtuelle Hardware aktualisieren, sie dann aber verwalten.

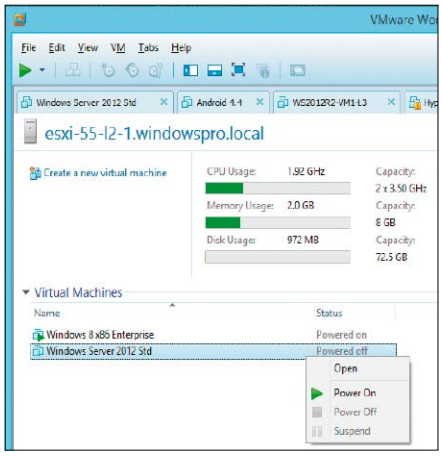
Vsphere Client inkompatibel mit Virtual Hardware 10

Der als Management-Tool für ESXi vorgesehene Vsphere Client kann indes neue VMs maximal mit Virtual Hardware 8 ausstatten, weil der dafür zuständige Wizard nicht aktualisiert wurde. Als Workaround bleibt das nachträgliche Update über den Befehl „Bestandsliste → Virtuelle Maschine → Upgrade virtueller Hardware durchführen“.

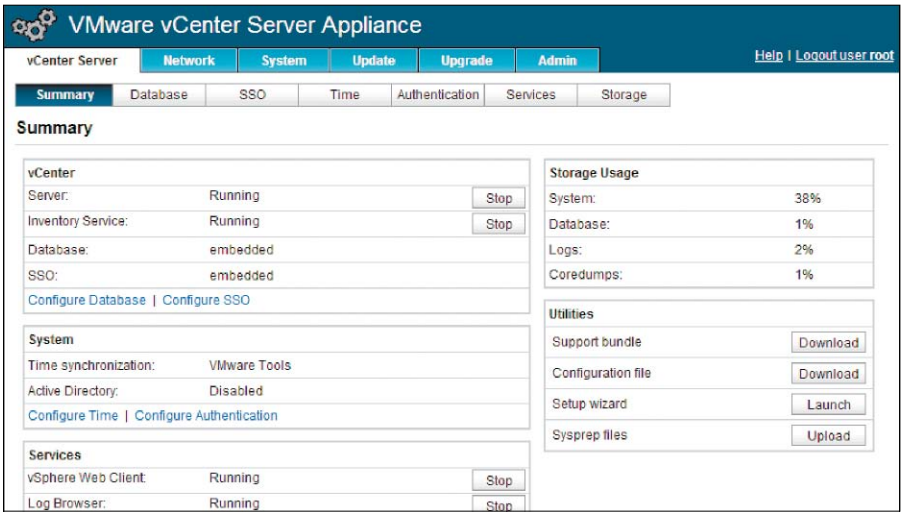
Anschließend lassen sich die Einstellungen der betreffenden VM aber nie wieder mit dem Vsphere Client bearbeiten. Versucht man es, dann rät die angezeigte Fehlermeldung, für diesen Zweck den Vsphere Web-Client zu verwenden. Tatsächlich eignet sich der Web-Client aber nicht zur Verwaltung von ESXi Free, weil er Bestandteil von Vcenter ist, und zwar entweder einer herkömmlichen Installation unter Windows oder des Vcenter Server Appliance. Beide dienen der zentralen Verwaltung von voll lizenzierten ESXi-Hosts.

Die Tools-Misere des kostenlosen Hypervisors entspringt der Entscheidung von Vmware, strategisch ganz auf das Web-Interface zu setzen und den Windows-Client nicht mehr weiterzuentwickeln. Er unterstützt daher keines der neuen Features, die ESXi 5.5 beziehungsweise Vcenter 5.5 bringen.

Gleichzeitig bleibt er aber das einzige Tool, mit dem sich Stand-alone-Hosts verwalten lassen, jedoch mit zunehmenden Einschränkungen. Für das nächste größere Release von ESXi arbeitet Vmware offenbar an einer Light-Version



Die Vmware Workstation 10 kann virtuelle Maschinen unter ESXi 5.5 verwalten, selbst wenn diese auf dem Stand der Virtual Hardware 10 sind.



Das Vcenter Server Appliance ist eine vorkonfigurierte virtuelle Maschine auf Basis von Linux und Vpostgres.

des Web-Clients, der den kostenlosen Hypervisor administrieren kann.

Vmware Workstation verwaltet VMs auf ESXi

In der Zwischenzeit kann die Vmware Workstation 10 einige Lücken füllen, die der veraltete Vsphere Client offenlässt. Allerdings ist sie nicht in der Lage, den Host selbst, dessen Datastores oder seine Netzwerkkonfiguration zu verwalten. Dafür bietet sie aber durchgängige Unterstützung für das Management von VMs. Diese lassen sich nicht nur ein- oder ausschalten, vielmehr kann man neue VMs auf Basis der Virtual Hardware 10 erstellen und nachträglich ihre Konfiguration bearbeiten. Entsprechend ist es auch möglich, virtuelle SATA-Controller hinzuzufügen oder VMDKs mit mehr als 2 TB anzulegen. Hinzu kommen weitergehende Management-Funktionen wie das Anlegen von Snapshots, Cloning oder die Verwaltung von Benutzerrechten.

Es stellt sich indes die Frage, ob die Zielgruppe für ESXi Free mehrheitlich bereit ist, ein kostenpflichtiges Produkt wie die Workstation zu erwerben, um VMs auf einem funktionsreduzierten Hypervisor zu verwalten. Der für den Privatgebrauch ebenfalls kostenlose Vmware Player besitzt nicht die Fähigkeit, sich mit einem ESXi-Server zu verbinden.

VCSA für kleine Vsphere-Installationen

Wenn die Fähigkeiten des kostenlosen ESXi nicht ausreichen und man daher eine der kleinen Editionen von Vsphere anschafft, dann muss man zu ihrer Verwaltung keinen Vcenter-Server unter Windows einrichten. Vmware bietet dafür das Vcenter Server Appliance (VCSA) als kostengünstige und einfache Alternative.

Das Vcenter Server Appliance ist eine vorkonfigurierte virtuelle Maschine auf Basis von Linux, die fast alle Komponenten eines Vcenter-Servers enthält. Das Appliance-Konzept bietet gleich zwei Vorteile: Zum einen entfällt die relativ aufwendige Installation, weil sich die Inbetriebnahme auf den Import einer OVA-Datei und die Konfiguration mittels Weboberfläche beschränkt. Zum anderen sparen sich Anwender damit die Lizenzkosten für Windows Server und je nach Setup auch für SQL Server. Zum Lieferumfang des VCSA gehört nämlich die integrierte Vpostgres-Datenbank, so dass die gesamte Vsphere-Konfiguration innerhalb des Appliance gespeichert wird. Gleichzeitig ist die eingebettete Datenbank aber der Flaschenhals beim Management einer größeren Umgebung. Sie beschränkt die maximale Zahl der ESXi-Hosts auf 100 und jene der VMs auf 1000. Im Vergleich zu den bisherigen Obergrenzen von fünf Hosts und 50 VMs ist das jedoch ein großer Fortschritt. Das Appliance selbst erreicht die gleichen Maximalwerte wie eine Vcenter-Installation auf Windows Server, wenn man eine externe Oracle-Datenbank verwendet. In dieser Konfiguration sind dann bis zu 1000 Hosts und 10 000 VMs möglich.

Unvollständiger Funktionsumfang

Auch wenn VCSA zusammen mit einer externen Datenbank gleich leistungsfähig ist wie Vcenter unter Windows, so hinkt es beim Funktionsumfang noch hinterher. Die fehlenden Features werden in der Praxis häufig darüber entscheiden, ob das VCSA für eine bestimmte Umgebung geeignet ist.

Was nicht unterstützt wird

Vcenter Linked Mode: Dieser verbindet mehrere Vcenter-Server, um ihnen den Austausch von Informationen zu erlauben. So kann ein Administrator, der an einem Vcenter-Server angemeldet ist, sich mit einem weiteren verbinden und dessen Inventar verwalten.

Vcenter Heartbeat: Dabei handelt es sich um einen Windows-Service, der Hochverfügbarkeit und Disaster Recovery für Vcenter gewährleisten soll. Er wird in LANs für HA und in WANs für DR konfiguriert, um Vcenter-Server, View Composer und MS SQL Server zu schützen.

Security Support Provider Interface (SSPI): Es ist Teil von Vcenter SSO und implementiert ein Windows-API, das für die Authentifizierung über Kerberos und NTLM benötigt wird.

Vmware Update Manager (VUM) und View Composer: Sie lassen sich nicht im VCSA installieren und müssen separat auf einer (virtuellen) Maschine unter Windows Server eingerichtet werden. Für jeden Vcenter-Server ist eine eigene Instanz von VUM erforderlich, der obendrein SQL Server benötigt. So kommen die durch das VCSA vermiedenen Lizenzkosten für Microsoft doch wieder ins Spiel.

Vcenter-Plug-ins von Drittanbietern: Möglicherweise sind einzelne von ihnen nicht mit dem VCSA kompatibel. Das muss im Einzelfall geprüft werden.

SQL Server: Als externe Datenbank kommt nur Oracle in Frage, der sonst von Vcenter bevorzugte MS SQL Server wird vom VCSA schlichtweg nicht unterstützt.

Mit der Version 5.5 des Vcenter Server Appliance macht Vmware einen großen Schritt in Richtung Unabhängigkeit der Vsphere-Administration von Windows.

Für (größere) Umgebungen wird es eine echte Alternative zum herkömmlichen Vcenter-Server, wenn Vmware künftig auch den Linked Mode sowie Heartbeat unterstützt und VUM auf Linux portiert. ■

ESXi installieren & konfigurieren

Wenn man einen Server auf Basis des kostenlosen Vmware Hypervisors virtualisieren möchte, dann sind nach der Installation die folgenden Konfigurationsschritte erforderlich, bis der Host voll einsatzbereit ist.

VON WOLFGANG SOMMERGUT

VMWARE BIETET FÜR GRÖSSERE Vsphere-Installationen geeignete Techniken an, um den Hypervisor auf eine Vielzahl von Hosts zu verteilen und zentral zu konfigurieren. Eine zentrale Rolle spielt das mit Version 5 eingeführte „Auto Deploy" im Zusammenspiel mit einem PXE-Boot des Hosts. Verwendet man den kostenlosen Vsphere Hypervisor (ESXi), dann steht diese Möglichkeit nicht zur Verfügung, so dass man ein Installationsmedium benötigt. Hier bietet ein USB-Speicher Vorteile gegenüber einer CD. Auch als Ziel für die ESXi-Installation ist ein Memory-Stick eine gängige und von Vmware unterstützte Konfiguration.

Der Download des kostenlosen ESXi (auf Heft-DVD und über *http://bit.ly/1ihiCXE*) erfolgt als ISO-Image, so dass der normale Weg zur Installation darin bestünde, eine CD/DVD zu brennen, den Server davon zu booten und den Hypervisor auf ein lokales Laufwerk oder einen Speicher im Netz zu installieren. Will man mehrere Server einrichten und den relativ langsamen Brenn- und Bootvorgang von CD vermeiden, dann sollte man einen USB-Stick als Installationsquelle vorbereiten.

Medium mit diskpart präparieren

Vmware bietet für diese Aufgabe in der Vsphere-Dokumentation eine Anleitung (*http://bit.ly/1ihjc7A*), die jedoch unter Linux umgesetzt werden muss. Das Erstellen eines bootfähigen USB-Sticks mit den Installationsdateien von ESXi 5.5 funktioniert jedoch auch unter Windows, und zwar relativ einfach. Das Speichermedium sollte so wie beim Zusammenstellen eines Win-PE-Mediums erst mit diskpart vorbereitet werden. Um folgende Anweisungen mit diskpart ausführen zu können, muss man das Programm in einer Eingabeaufforderung mit Administratorrechten starten. Die Texte nach REM werden hier zur Info mit aufgeführt:

```
REM  In der Ausgabe des 1. Befehls die Nummer des USB-Sticks merken
list disk
select disk [Nummer der Disk]
REM  Vorsicht, alle Daten werden entfernt
clean
create partition primary
select partition 1
active
format fs=fat32 quick
assign
exit
```

Übertragen der Dateien mit Linux Live USB Creator

Um den USB-Stick startfähig zu machen und die Installationsdateien zu übertragen, verwendet man den Linux Live USB Creator (*http://bit.ly/1giOB53*). Diesem teilt man in Schritt eins mit, welchen Speicherstick er als Ziel verwenden soll, und weist ihm in Schritt zwei die ISO-Installationsdatei zu, die man von Vmware heruntergeladen hat. In Schritt drei belässt man die Einstellung „Install only", und in vier wählt man alle aktivierten Checkboxen ab. Nun kann man den Vorgang starten, der den Memory-Stick als Installationsmedium einrichtet. Weitere Nachbearbeitungen wie die in der Vmware-Anleitung beschriebene Umbenennung der Datei „isolinux.cfg" oder die andernorts empfohlene Anpassung von „boot.cfg" erwiesen sich in meinem Test mit dem ESXi 5.5 als nicht notwendig.

Mit dem Open-Source-Tools Linux Live USB Creator lässt sich ein ESXi-Installationsmedium auf einem USB-Stick erzeugen. Das Tool läuft unter Windows.

ESXi 5.5 auf USB-Stick installieren

Eine gängige Konfiguration besteht darin, ESXi auf einer SD-Card oder einem Memory-Stick zu installieren. Diese Variante empfiehlt sich besonders dann, wenn ein Server über keine lokalen Platten verfügt. Der Installation auf einen solchen externen Speicher kommt entgegen, dass der Hypervisor von Vmware nur circa 300 MB benötigt. Nutzt man diese Konstellation, die offiziell unterstützt wird, im produktiven Betrieb, dann sollte man ein Medium

wählen, das dafür zertifiziert ist. Eine solche Installation des Hypervisors erfolgt auf einem physikalischen System nach dem gleichen Muster wie auf ein Plattenlaufwerk. Nach dem Booten von CD oder USB-Stick wählt man als Ziel einfach den Memory-Stick und lässt das Setup durchlaufen.

ESXi in Vmware Workstation installieren

Noch einfacher funktioniert die Installation von ESXi auf einen USB-Stick in Vmware Workstation oder einem anderen Typ-2-Hypervisor wie Virtualbox. Dort ordnet man einer bestehenden VM, die über mindestens 4 GB RAM verfügen sollte, die Installations-ISO von ESXi als DVD-Laufwerk zu und stellt sicher, dass die virtuelle Maschine davon startet. Zu diesem Zweck ändert man die Bootreihenfolge, ab der Workstation 8 kann man das über den Befehl „Power on to BIOS“ bewerkstelligen.

Wenn die VM vom ISO-Image startet, sorgt man dafür, dass der USB-Stick, auf den ESXi installiert werden soll, vom Host getrennt und der virtuellen Maschine zugeordnet wird. Falls die Installationsroutine bereits die Auswahl der Speichermedien präsentiert und der USB-Stick dort noch nicht angezeigt wird, dann kann man dort die lokalen Speicher durch Drücken der Taste mit F5 neu einlesen.

Nach der Installation des Hypervisors auf dem Memory-Stick kann man diesen verwenden, um einen Server davon zu booten. Lädt dieser die virtuellen Maschinen von einem SAN oder NAS, dann muss man ihm dieses mit Hilfe des Vsphere Client zuordnen.

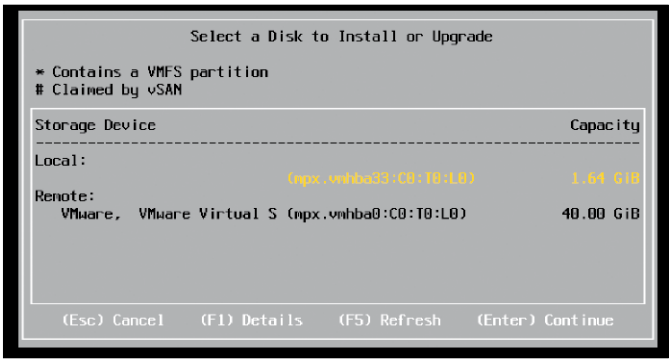
Lizenzschlüssel für ESXi eingeben

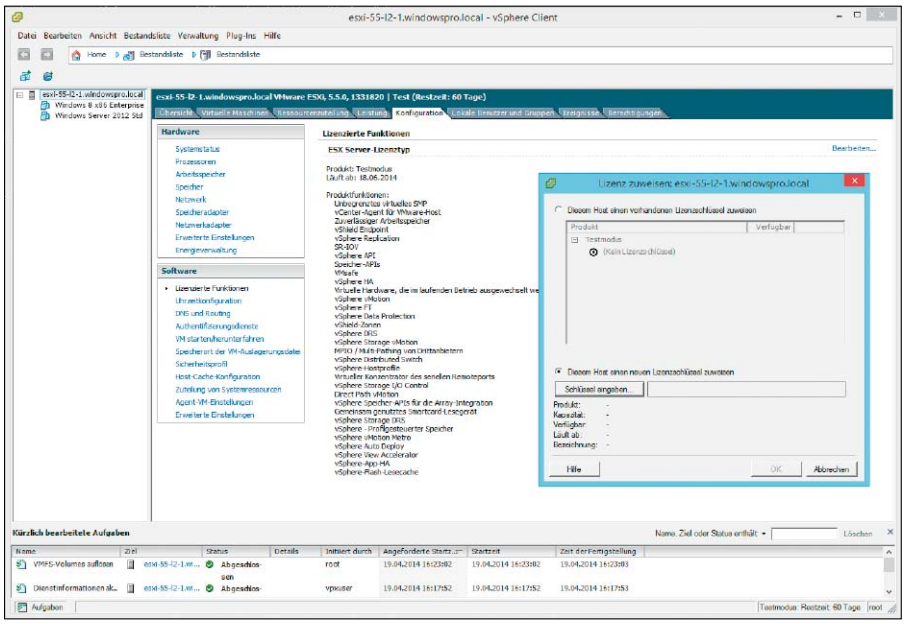
Vmware gibt die Basisversion seines ESXi unter der Bezeichnung „Vmware Hypervisor“ zwar kostenlos ab, aber er muss dennoch durch Eingabe eines Lizenzschlüssels freigeschaltet werden. Diesen erhält man beim Download der Software, und er muss relativ umständlich über den Vsphere Client eingegeben werden.

Verbindet man sich nach der Installation aus dem Vsphere Client mit einem ESXi-Server, dann erhält man den Hinweis „Ihre Testlizenz läuft in 60 Tagen ab!“. Dieser Dialog enthält einen Link mit dem Text „Dem ESXi-Host eine Lizenz zuweisen“. Wie schon unter älteren Versionen von ESXi führt dieser jedoch nur auf die Download-Seite von Vmware, von der man ESXi inklusive Vsphere Client und Lizenzschlüssel bereits heruntergeladen hat.

Das gewünschte Ergebnis erreichen Sie, indem Sie im Vsphere Client die Registerkarte „Konfiguration“ öffnen und dort „Software → Lizenzierte Funktionen“ anklicken. Auf dieser Seite findet man den Eintrag „Produkt: Testmodus“ sowie das Ablaufdatum. Rechts oben kann man über den Befehl „Bearbeiten“ einen Dialog öffnen, wo man jenen Lizenzschlüssel eingeben kann, den man beim Download von ESXi erhalten hat. Anschließend ist das Produkt unbegrenzt freigeschaltet.

Der Vmware-Hypervisor lässt sich auf ein Wechselmedium wie USB-Stick oder SD-Card installieren, indem man das Setup in der Workstation ausführt.





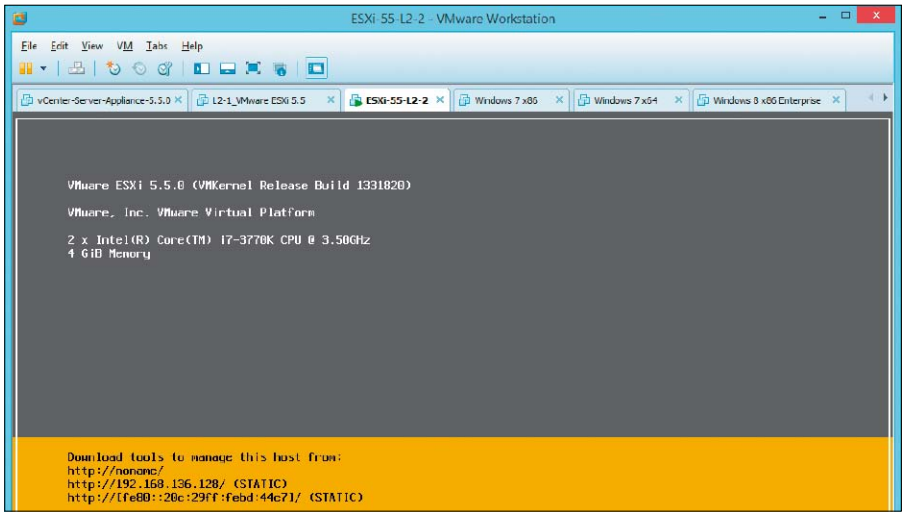
Der kostenlose Vsphere Hypervisor wird durch Eingabe eines Schlüssels in den Vsphere Client freigeschaltet.

Netzwerk konfigurieren

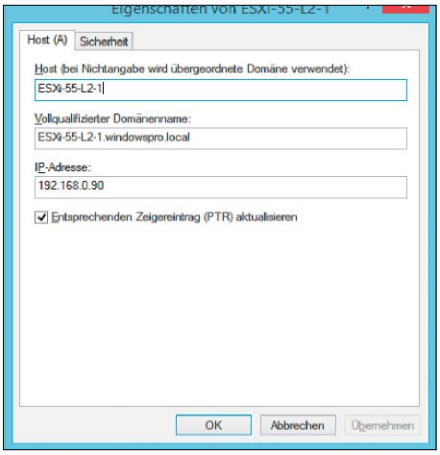
Wenn man ESXi frisch installiert, dann bezieht es standardmäßig seine IP-Adresse über DHCP. Liegt dort keine Reservierung vor, dann erhält der Host eine beliebige freie Adresse, und der Hostname lautet auf „localhost“ und „noname“, die Domäne auf „localdomain“. Nun könnte man im nächsten Schritt die Netzwerkeinstellungen manuell konfigurieren, indem man über die Konsole (DCUI) oder den Vsphere Client die IP-Adresse, das Standard-Gateway, den Host-Namen und die DNS-Server einträgt. Dieses Verfahren ist jedoch bei einer größeren Zahl von Hosts zu umständlich und unflexibel, so dass man alternativ eine Kombination aus statischen DNS-Einträgen und DHCP-Reservierungen nutzen kann. Damit erreicht man ebenfalls, dass alle Hosts eine feste IP-Adresse erhalten, aber die Administration erfolgt an zentraler Stelle. Die folgende Anleitung geht davon aus, dass der DNS- und DHCP-Dienst über Windows Server im Netzwerk bereitgestellt wird.

Im ersten Schritt legt man im DNS-Manager einen neuen Host-Eintrag (A oder AAAA) für den ESXi-Server an. Im entsprechenden Dialog gibt man den Host-Namen und die IP-Adresse ein. Hat man eine Reverse-Lookupzone für das betreffende Netzwerk definiert, dann kann man die Option „Verknüpften PTR-Eintrag erstellen“ aktiviert lassen, andernfalls führt der Versuch, einen solchen Zeiger anzulegen, zu einer Fehlermeldung.

Der PTR-Eintrag dient ESXi dazu, den Host-Namen über Reverse Lookup zu ermitteln, sobald er die IP-Adresse über DHCP bezogen hat. Bei der dynamischen IP-Konfiguration sieht Vmware nämlich nicht vor, dass man den Host-Namen manuell festlegt (man kann sich dazu aber des Tricks bedienen, temporär auf



Ein frisch installierter ESXi-Host hört auf den Namen „localhost“ oder „noname“ und gehört der „localdomain“ an.



Der PTR-Eintrag erlaubt dem ESXi-Server, den Host-Namen mit dem Befehlszeilen-Tool nslookup abzufragen und dynamisch zuzuweisen.

die manuelle Konfiguration umzustellen, dann bleibt der Host-Name nach Rückkehr zu DHCP erhalten).

DHCP-Reservierung einrichten

Hat man keine Reverse-Lookupzone und will auch keine anlegen, dann kann man den Host-Namen alternativ über DHCP an ESXi zuweisen. Der erste Schritt besteht jedoch darin, dass man eine Reservierung für den Host einrichtet. Dies erfolgt im MMC-Snap-in für DHCP, indem man den gewünschten Bereich öffnet und im Kontextmenü des Abschnitts „Reservierungen“ den Befehl „Neue Reservierung“ ausführt.
Im anschließenden Dialog gibt man die im DNS festgelegte IP-Adresse und den Host-Namen ein, darüber hinaus benötigt man die MAC-Adresse des ESXi-Servers. Diese lässt sich über die Konsole unter „Configure Management Network → Network Adapters“ ermitteln. Alternativ findet man sie im Vsphere-Client unter dem Reiter „Konfiguration → Netzwerk → Eigenschaften“. Für die Eingabe in den DHCP-Client muss man für die MAC-Adresse eine Notation ohne Doppelpunkte verwenden.
Möchte man nun auch den Host-Namen über DHCP zuteilen, dann führt man aus dem Kontextmenü der betreffenden Reservierung den Befehl „Optionen konfigurieren“ aus. Im darauf folgenden Dialog wechselt man zur Registerkarte „Erweitert“, aktiviert in der Liste den Eintrag „012 Hostname“ und gibt den gewünschten Namen ein. Erhält ESXi den Host-Namen auf diesem Weg, dann verzichtet es auf einen Reverse Lookup.

Troubleshooting

Startet man nun den Hypervisor neu oder setzt das Management Network über die DCUI zurück, dann sollte der Host die korrekte IP-Konfiguration erhalten. Ist dies nicht der Fall, etwa weil der Host-Name weiterhin auf „localhost“ lautet, dann sollte man bei Verwendung eines PTR-Eintrags zuerst mit nslookup prüfen, ob sich die über DHCP zugewiesene IP-Adresse in den Host-Namen auflösen lässt.
Funktioniert das Reverse Lookup oder erhält ESXi den Host-Namen über DHCP, kann die Verwendung unerlaubter Zeichen, etwa „_“ im Host-Namen eine weitere Ursache für Probleme sein. ESXi lässt nämlich nur alphanumerische Zeichen und den Bindestrich zu (der nicht am Anfang stehen darf). Den nach RFC 2181 erweiterten Zeichensatz unterstützt es nicht.
Bei der Fehlersuche kann sich ein Blick in die Log-Datei des DHCP-Clients als hilfreich erweisen. Sie findet man unter „/var/logs“, wo man sich etwa mit dem Befehl

```
tail -25 dhclient.log
```

die letzten 25 Einträge ausgeben lassen kann.

SSL-Zertifikat ausstellen und zuweisen

Die Komponenten einer Vsphere-Installation benötigen Zertifikate für die sichere Kommunikation untereinander. Das gilt auch für ESXi-Server, die nach ihrer Installation nur selbst signierte Zertifikate besitzen. Nachdem Vmware-Hosts normalerweise keine Verbindung zum Internet haben, bietet es sich an, die benötigten SSL-Zertifikate über die Zertifizierungsstelle des Active Directory auszustellen, anstatt sie von einer externen Authority zu kaufen.
Nicht nur Vcenter und ESXi brauchen Zertifikate, um sichere Verbindungen aufzubauen, sondern auch Vcenter Inventory Service, Vcenter Single Sign-on, Vcenter Update Manager, Vcenter Orchestrator, Vsphere Web Client oder Vcenter Log Browser. Angesichts des damit verbundenen Aufwands fällt die Tools-Unterstützung durch Vmware schwach aus, so dass man letztlich auf manuelle und damit fehleranfällige Abläufe angewiesen ist. Aber selbst dafür gibt es nur eine über zahlreiche PDFs und KB-Artikel verstreute Dokumentation, die häufig nicht mehr aktuell ist oder nicht den gesamten Prozess beschreibt. Ähnliches gilt für die zahlreichen Anleitungen im Internet, die in der Praxis oft nicht so funktionieren, wie es die Beschreibung angibt.

Automatisierung durch CLI-Tool und Script

Wer beim Ausstellen oder Erneuern von Zertifikaten eine Unterstützung durch Tools haben möchte, dem bietet Vmware ein solches als separaten Download an. Es handelt sich dabei um ein Kommandozeilenprogramm namens SSL Certificate Automation Tool (*http://bit.ly/1psNet4*), das in eigenen Ausführungen für Vsphere 5.1 und 5.5 existiert. Angesichts der relativ umständlichen Inbetriebnahme des Werkzeugs muss jeder für sich entscheiden, ob sich dessen Einsatz in einer bestimmten Umgebung lohnt. Ein weiteres Hilfsmittel für diese Aufgabe ist ein Powershell-Script von Derek Seaman (*http://bit.ly/1rof5rN*), das der Autor zwar nicht als Alternative zum Vmware-Tool versteht, aber das viele (der gleichen) Schritte automatisieren kann.

Selbst signiertes Zertifikat auf ESXi ausstellen

Wenn man ESXi installiert, dann erzeugt das Setup-Programm ein selbst signiertes Zertifikat, das auf „localhost“ ausgestellt ist. Nachdem man den Host-Namen aber entweder schon geändert hat oder im weiteren Verlauf ändern wird, stimmen die Namen schließlich nicht überein. Dies führt zu einer entsprechen-

den Warnung, wenn man mit dem Vsphere Client oder einem Internet-Browser eine Verbindung zum ESXi-Host herstellen will.
Allerdings provozieren Zertifikate, die durch ESXi selbst ausgestellt sind, grundsätzlich solche Sicherheitshinweise, so dass ein neues Zertifikat mit einem bloß korrekten Host-Namen keine Fortschritte bringt. Wer allerdings mit der reinen Namensübereinstimmung zufrieden ist, der kann auf dem ESXi-Host relativ einfach ein neues Zertifikat erstellen, das den tatsächlichen Namen des Servers enthält.
Dazu erstellt man eine Datei namens „openssl.cnf“ mit folgendem Inhalt und lädt sie über SSH auf den Host, beispielsweise mit dem kostenlosen Win SCP:

```
[req]
default_bits = 1024
default_keyfile = rui.key
distinguished_name = req_disti
guished_name
encrypt_key = no
prompt = no
string_mask = nombstr

[ req_distinguished_name ]
countryName = US
stateOrProvinceName = California
localityName = Palo Alto
0.organizationName = Vmware, Inc.
emailAddress = ssl-certificates
Vmware.com
commonName = FQDN-DES-SERVERS
```

Das Zielverzeichnis „/etc/pki/tls“ ist standardmäßig nicht vorhanden und muss erst angelegt werden. Anschließend führt man das Python-Script „generate_certificates” aus, das sich in „/sbin“ befindet. Es ruft Open SSL auf und speichert das neue Zertifikat sowie die Key-Datei im korrekten Verzeichnis unter „/etc/Vmware/ssl“. Nach einem Reboot von ESXi sollte das neue Zertifikat wirksam sein.

Active Directory als CA nutzen

Wenn man den in vielen Firmen geltenden Sicherheitsstandards entsprechen und obendrein die Warnungen der Client-Software vermeiden will, dann muss das Server-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle stammen. Dieses braucht man nicht unbedingt von einem einschlägigen Anbieter zu erwerben, vielmehr genügt in den meisten Fällen eines, das von einer internen CA, zum Beispiel jener des AD, ausgestellt wurde.
Für diesen Vorgang reichen den Anleitungen von Vmware zufolge die reinen Windows-Bordmittel jedoch nicht aus. Vielmehr muss die Zertifikatanforderung über Open SSL erfolgen. Dieses existiert auch in einer Ausführung für Windows, vor dessen Setup man das „Visual C++ 2008 Redistributable Package“ installieren muss (auf Heft-DVD und *http://bit.ly/1psRpoA*). Anschließend wechselt man in einer Eingabeaufforderung mit administrativen Rechten in das „bin“-Verzeichnis von Open SSL und gibt folgenden Befehl ein:

```
openssl req -new -nodes -out rui.
 csr -keyout rui-orig.key -config
 openssl.cfg
```

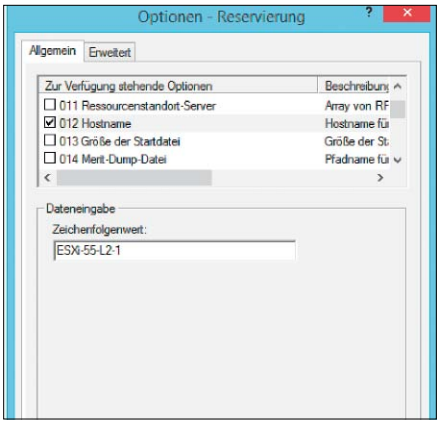
Wenn man die erforderlichen Angaben nicht zuvor in die „openssl.cfg“ eingetragen hat, dann werden diese vom Programm interaktiv abgefragt. Dazu zählen der Ländercode, die Stadt, der Firmenname, die OU oder der Name des Servers, den man meistens als vollqualifizierten Domänennamen angeben wird.
Anschließend konvertiert man den Schlüssel in das RSA-Format:

```
openssl rsa -in rui-orig.key -out
 rui.key
```

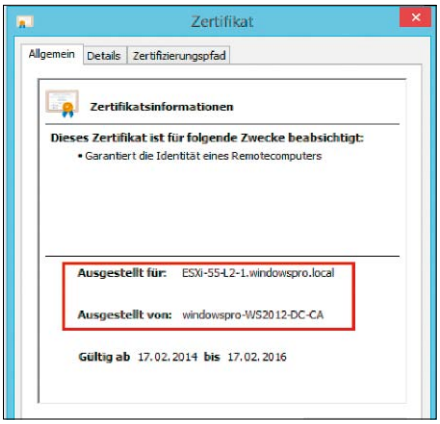
Im nächsten Schritt leitet man die von Open SSL generierte Anforderung an die AD-Zertifizierungsstelle weiter. Die meisten Anleitungen empfehlen an dieser Stelle, den Inhalt der Datei „rui.csr“ in das Web-Interface der CA zu kopieren. Dieses ist aber möglicherweise gar nicht installiert, außerdem erfordert es anschließend einen weiteren Aufruf von Open SSL. Einfacher ist in diesem Fall die Verwendung von Certreq.exe, da man ohnehin schon die Eingabeaufforderung geöffnet hat:

```
certreq -submit -attrib
 "CertificateTemplate:WebServer"
 rui.csr
```

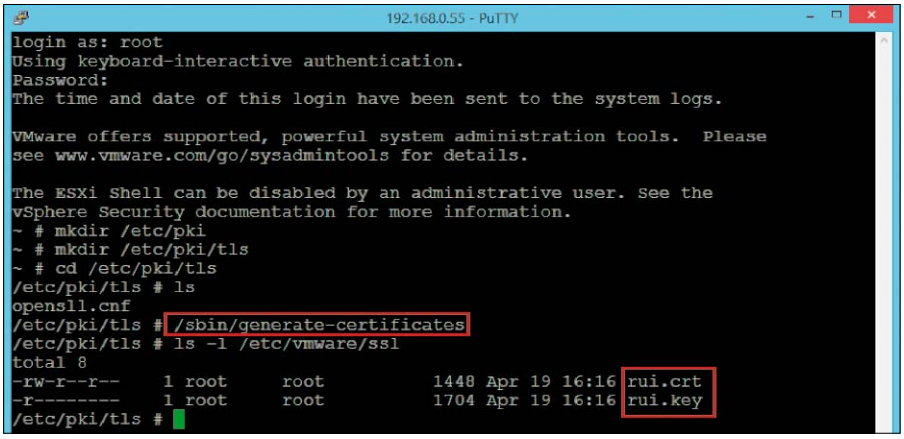
Das Kommandozeilen-Tool erlaubt die Spezifizierung der erforderlichen Zertifikatvorlage, so dass man gleich das Webserver-Template angeben kann. Versucht man dagegen die mit Open SSL erstellte Anforderung in das MMC-Snap-in „Zertifizierungsstelle“ zu importieren, dann scheitert dieser Vorgang an der fehlenden Auswahl einer Vorlage.
Nach dem Ausstellen des Zertifikats öffnet certreq einen Dialog, der den Export im X509-Format anbietet. Hier gibt man als Dateinamen „rui.crt“ an. Nun kann man die Dateien „rui.key“ und „rui.crt“ über SSH in das Verzeichnis „/etc/Vmware/ssl“ auf den ESXi-Host hochladen und den Server neu starten. ■



Eine DHCP-Reservierung sorgt dafür, dass der ESXi-Host immer die gleiche IP-Adresse erhält. Man kann ihm damit auch den Host-Namen zuweisen.



Nach der Installation eines von der Enterprise-CA ausgestellten Zertifikats unterbleiben die Sicherheitswarnungen der Clients.

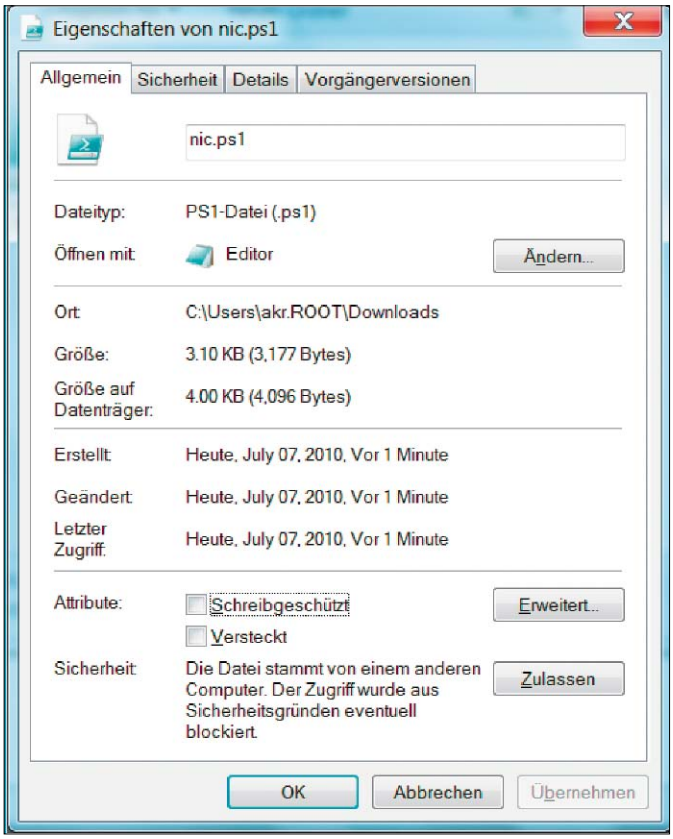


Das Script „generate_certificates“ ändert den Host-Namen eines selbst signierten Zertifikats aus einem ESXi-Server.

Einstieg in Powershell

Powershell ist ein mächtiger Nachfolger für den alten Kommando-Interpreter Cmd.exe und für Batch-Dateien. Für Microsoft hat Powershell strategischen Charakter, so dass Admins den Umstieg ernsthaft erwägen sollten.

VON WOLFGANG SOMMERGUT



Scripts, die man aus dem Internet heruntergeladen hat, kann man über das Kontextmenü der Datei freischalten.

AUFGRUND DIESER BEDEUTUNG von Powershell kommen Windows-Administratoren auf Dauer nicht umhin, sich mit dieser Kombination aus Kommandozeile und Script-Umgebung zu beschäftigen. Sei es die Automatisierung der AD-Verwaltung, von Hyper-V oder von Server-Software wie Exchange, Powershell ist das Werkzeug der Wahl. Powershell bietet vollen Zugriff auf COM und WMI, um administrative Arbeiten am lokalen und an entfernten Rechnern zu ermöglichen. Wer sich über die Jahre an Cmd.exe und VB-Script gewöhnt hat, wird sich aber erst mit dem Konzept der objektorientierten Powershell vertraut machen müssen. Die aktuelle Version von Powershell ist 4.0. Sie ist Bestandteil von Windows 8.1 und Windows Server 2012 R2, lässt sich aber für Windows 7,8, Server 2008 R2 und 2012 über das Windows Management Framework 4.0 (auf Heft-DVD und *http://bit.ly/1mI4g4v*) nachrüsten. Dieses umfasst auch WMI, Winrm sowie Server Manager CIM Provider, die jedoch weitgehend unverändert blieben.

Powershell-Scripts zulassen

Unmittelbar nach dem Speichern seines ersten Scripts wird der neue Powershell-Anwender feststellen, dass es sich nicht ausführen lässt. Powershell ist per Voreinstellung sicher und führt nur direkt eingegebene Befehle, aber keine Scripts aus. Dies muss man erst ermöglichen, indem man innerhalb einer Powershell-Sitzung mit administrativen Rechten die Execution-Policy mit Hilfe des Befehls

```
Set-ExecutionPolicy <policy>
```

festlegt. Der Wert für „<policy>“ ist per Voreinstellung „Restricted“, das heißt Powershell führt Scripts nicht aus. Weitere Parameter, mit denen man die Ausführung zulassen kann, sind:

Allsigned: Führt alle Scripts mit einer digitalen Signatur aus. Wenn die signierende Stelle nicht bekannt ist, fragt Powershell nach, ob dem Herausgeber vertraut werden soll.

Remotesigned: Erfordert eine digitale Signatur für aus dem Internet heruntergeladene Scripts, lokal erstellte Scripts werden immer und ohne Nachfrage ausgeführt.

Unrestricted: Führt alle Scripts aus; für nicht signierte, aus dem Internet heruntergeladene Scripts wird eine Warnung ausgegeben.

Den gegenwärtigen Status erfährt man über den Aufruf von

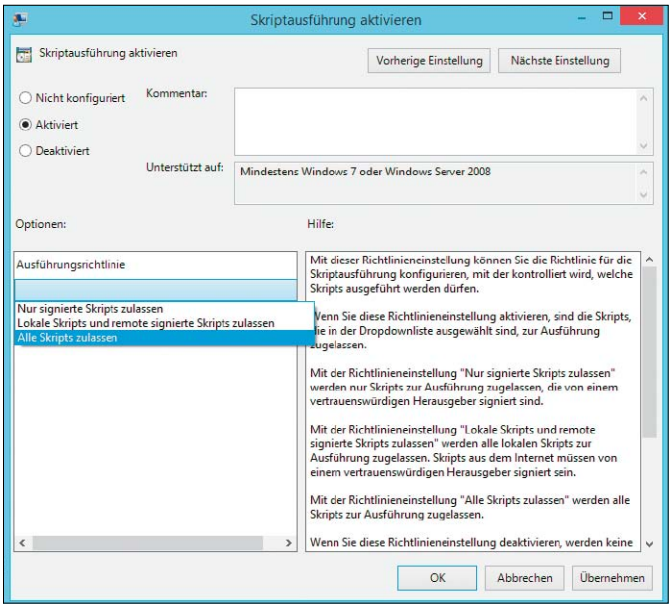
```
Get-ExecutionPolicy
```

Um zu unterscheiden, welche Scripts aus dem Internet stammen, bedient sich Powershell der NTFS-Streams, die auch über die Herkunft anderer heruntergeladener ausführbarer Dateien Auskunft geben. Man kann diesen Stream von einer Datei entfernen, indem man per Kontextmenü ihre Eigenschaften aufruft und auf der Registerkarte „Allgemein“ die Schaltfläche „Zulassen“ betätigt.

Powershell mit Hilfe von Gruppenrichtlinien zulassen

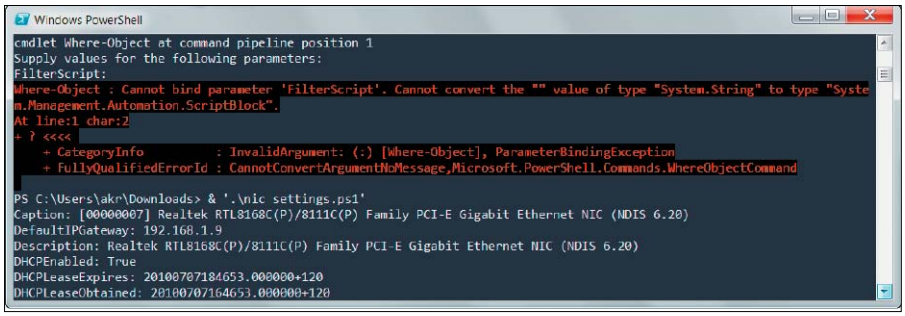
Wenn man die Ausführungsrichtlinien nicht nur auf einzelnen, sondern auf einer größeren Zahl von PCs ändern möchte, dann empfiehlt sich der Einsatz von GPOs. Unter „Computer- sowie Benutzerkonfiguration → Richtlinien → Administrative Vorlagen → Windows-Komponenten → Windows-Powershell" findet sich die Einstellung „Scriptausführung aktivieren".
Sie bietet die drei oben beschriebenen Ausführungsrichtlinien zur Auswahl, die man bei „Set-ExecutionPolicy" als Argument angibt. Im deutschen Windows sind die drei möglichen Werte lokalisiert. Sie heißen „Nur signierte Scripts zulassen", „Lokale Scripts und remote signierte Scripts zulassen" und „Alle Scripts zulassen".

Wenn man die Ausführungsrichtlinien für Powershell auf einer größeren Zahl von Rechnern ändern will, dann empfiehlt sich dafür ein GPO.



Powershell-Scripts starten

Gegenüber dem Ausführen eines Scripts etwa in Cmd.exe gibt es bei Powershell noch zwei weitere wichtige Unterschiede:
1. Powershell führt nur Scripts aus, die sich in der Umgebungsvariablen PATH befinden. Im aktuellen Verzeichnis befindliche Scripts fallen normalerweise nicht darunter und müssen gegebenenfalls in der Form *.\script.ps1* aufgerufen werden.
2. Leerzeichen in Datei- und Verzeichnisnamen können nicht einfach in Anführungszeichen eingeschlossen werden, Powershell interpretiert dies dann als String und gibt den Script-Aufruf einfach als Ausgabe zurück. Vor Datei- und Verzeichnisnamen, die wegen der enthaltenen Leerzeichen in Anführungszeichen gesetzt wurden, muss deshalb stets der Ausführungsoperator *&*, damit Powershell weiß, dass der nun folgende String ausgeführt werden soll (zum Beispiel: *&".\Mein erstes Script.ps1"*). Die Shell hilft hier allerdings mit und setzt bei der Tab-Vervollständigung von Datei- und Verzeichnisnamen bei Bedarf sowohl die Anführungszeichen als auch das *„&"*.



Wenn der Dateiname eines Scripts Leerzeichen enthält, muss man fürs Ausführen den &-Operator voranstellen.

Powershell mit Profilen konfigurieren

Fast jeder Kommando-Interpreter bietet die Möglichkeit, gleich beim Start eine vom Benutzer gewünschte Konfiguration zu laden und sich somit an individuelle Vorgaben anzupassen. Das gilt auch für die Powershell, die gleich mehrere Profildateien ausliest, um Einstellungen für verschiedene Geltungsbereiche zu übernehmen. Zulässig ist praktisch alles, was die Powershell ausführen kann.
Voraussetzung dafür, dass die Powershell beim Start eine der Profildateien lädt, ist allerdings, dass man die Ausführung von Scripts auf dem System zulässt. Sind diese Voraussetzungen geschaffen, dann können eine oder mehrere Profildateien angelegt werden. Unterstützt werden dabei vier Typen mit folgenden Gültigkeitsbereichen:

- alle Benutzer, alle Shells
- alle Benutzer, aktuelle Shell
- aktueller Benutzer, alle Shells
- aktueller Benutzer, aktuelle Shell

Mit „alle Shells" sind nicht mehrere Instanzen von Powershell.exe gemeint, sondern verschiedene Programme, die als Schnittstelle zur Script-Engine dienen. Die Rede ist hier auch häufig von Hosts. So lassen sich etwa verschiedene Profile für Powershell.exe, die grafische Powershell_ISE oder ein Produkt eines Drittanbieters definieren.
Welche Datei konkret für eine bestimmte Shell oder einen Benutzer zuständig ist, kann man den dafür vorgegebenen selbsterklärenden Variablen entnehmen. Sie lauten:

- $Profile.AllUsersAllHosts
- $Profile.AllUsersCurrentHost
- $Profile.CurrentUserAllHosts
- $Profile.CurrentUserCurrentHost

Falls alle zulässigen Profile vorhanden sind, werden sie samt und sonders beim Start einer neuen Shell ausgeführt, und zwar in der Reihenfolge vom größten zum geringsten Gültigkeitsbereich. Die Datei für „alle Benutzer und alle Shells" läuft also zuerst, die für den „aktuellen Benutzer und Host" zuletzt. Das hat zur Folge, dass Definitionen oder Aliase in der Datei, die am genauesten auf einen Benutzer und eine Shell zugeschnitten ist, bei Namensgleichheit jene aus anderen Profilen überschreiben.

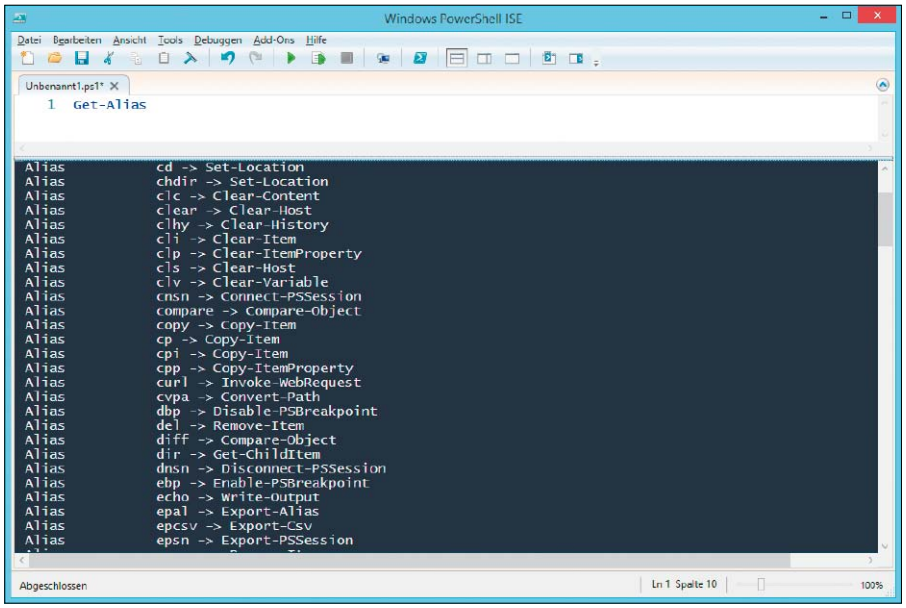
Anlegen von Profilen

Powershell bringt standardmäßig keine Profile mit. Um festzustellen, ob eine bestimmte Profildatei existiert, empfiehlt sich die Kombination aus *Test-Path* und der Umgebungsvariable für die betreffende Datei, also etwa:

```
Test-Path $Profile.Current
  UserAllHosts
```

Ist das Ergebnis des Befehls „false", dann kann man bei Bedarf eine neue Profildatei anlegen. Hilfreich ist dabei *New-item*, weil es zusammen mit dem Schalter *-force* nicht vorhandene Verzeichnisse gleich mit anlegt:

```
New-Item -path $profile -type
  file -force
```



Verbieten die Ausführungsrichtlinien Scripts, dann bringt Powershell beim Laden von Profilen eine Fehlermeldung.

```
PS C:\Users\wolf.WINDOWSPRO> dir /ad
Get-ChildItem : Der Pfad "C:\ad" kann nicht gefunden werden, da er nicht vorhanden ist.
Bei Zeile:1 Zeichen:4
+ dir <<<<  /ad
    + CategoryInfo          : ObjectNotFound: (C:\ad:String) [Get-ChildItem], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

PS C:\Users\wolf.WINDOWSPRO> cd /d c:\windows
Set-Location : Es wurde kein Positionsparameter gefunden, der das Argument "c:\windows" akzeptiert.
Bei Zeile:1 Zeichen:3
+ cd <<<<  /d c:\windows
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetLocationComma
   nd

PS C:\Users\wolf.WINDOWSPRO> del *.tmp /s
Remove-Item : Es wurde kein Positionsparameter gefunden, der das Argument "/s" akzeptiert.
Bei Zeile:1 Zeichen:4
+ del <<<<  *.tmp /s
    + CategoryInfo          : InvalidArgument: (:) [Remove-Item], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.RemoveItemComman
   d

PS C:\Users\wolf.WINDOWSPRO>
```

Die vordefinierten Aliase für cmd-Kommandos scheitern, wenn man die gewohnten Schalter verwenden möchte.

Um die Profildatei zu editieren, kann man sie etwa mit *notepad.exe $profile* öffnen.

Anwendungen für Profile

Wie sich schon aus den Namensendung „PS1" der Profildateien erkennen lässt, handelt es sich bei ihnen um normale Powershell-Scripts, deren Besonderheit nur in ihrem Speicherort und in ihrem Namen besteht. Diese beiden Faktoren sind verantwortlich, dass sie beim Start von Powershell automatisch ausgeführt werden. Daher können sie grundsätzlich alle Möglichkeiten der Powershell ausschöpfen.

In der Praxis wird man jedoch Profile primär dafür nutzen, um die Umgebung der Shell anzupassen, sei es, indem man Standardeinstellungen überschreibt oder Features hinzufügt. Zur häufigsten Anwendungen der Profile zählt die Definition von Alias-Namen für Cmdlets oder von Funktionen. Erzeugt man sie nur auf der Kommandozeile, dann beschränkt sich ihre Gültigkeit auf die aktuelle Sitzung. Sollen sie permanent verfügbar sein, müssen sie in eine Profildatei aufgenommen werden. Das Gleiche gilt auch für das Laden von Modulen, das bei jedem Start einer Powershell-Instanz wiederholt werden muss. Hier würde man einen Befehl nach dem Muster

```
import-module <Module-Name>
```

in das Profil eintragen, wenn man das Eintippen des Befehls nicht in jeder Sitzung wiederholen möchte. Weitere Anwendungsmöglichkeiten für die Profile bestehen typischerweise darin, das Aussehen oder das Verhalten der Shell zu verändern.

So könnte man etwa die Funktion „prompt" neu definieren, Farben von Schrift und Hintergrund verändern oder die Befehlshistorie speichern (*http://bit.ly/1gTDw9J*).

Hilfsmittel für Umsteiger

Statt auf Dauer am veralteten Konzept von Cmd.exe und Batch-Dateien herumzudoktern, hat Microsoft mit der Powershell einen von Grund auf neuen Nachfolger entwickelt. Um den Umstieg zu erleichtern, lassen sich in einem gewissen Rahmen die alten Befehle in der neuen Umgebung weiterverwenden.

Die Powershell ist gleichzeitig eine Scripting-Umgebung und eine Kommandozeile, die man interaktiv für die Eingabe von Befehlen verwenden kann. Damit unterscheidet sie sich von VB-Script, dessen Befehle man nicht auf der Kommandozeile eingeben kann und die zur Ausführung den Scripting Host benötigen. Aufgrund ihrer doppelten Rolle könnte man also Powershell als Standard für die Eingabeaufforderung wählen und damit Cmd.exe ersetzen.

Im Gegensatz zum alten Kommando-Interpreter setzt Powershell durchgängig eine konsistente Konvention für Befehlsnamen um, die durch die Übernahme der cmd-Befehle durchbrochen würde. Allerdings bietet die Powershell eine Alias-Funktion, mit der sich Cmdlets oder Parameternamen unter einer anderen Bezeichnung ansprechen lassen. Genau diesen Weg hat Microsoft gewählt, um die internen cmd-Befehle in Powershell bereitzustellen. Aufgrund der verschiedenen Syntax der Powershell-Pendants lassen sich die alten Kommandos aber nur sehr eingeschränkt weiternutzen.

Aliase bilden inkompatible Befehle nur teilweise ab

Wenn man *Get-Alias* ausführt, dann findet man viele cmd-Befehle als vordefinierte Aliase wieder. Sie verweisen auf neue Cmdlets, etwa *dir* auf *Get-ChildItem* oder *cd* auf *Set-Location*. Jedoch unterscheiden sich die zulässigen Schalter und Optionen der alten und neuen Befehle schon syntaktisch, so dass man einem Alias nur das übergeben kann, was der Powershell-Befehl kennt. Eine Nutzung eines Alias nach dem Muster eines gleichnamigen cmd-Befehls scheitert, sobald man zusätzlich zu Zeichenketten für Dateinamen oder Pfadangaben einen Schalter hinzufügt. Deswegen lassen sich die kurzen und praktischen Befehle wie *dir /ad* oder *del *.tmp /s* nicht ausführen, sie verursachen eine Fehlermeldung.

Aliase durch eigene Funktionen ersetzen

Eine Möglichkeit, die Kompatibilität von Powershell mit dem alten Kommando-Interpreter zu verbessern, bestünde darin, die vordefinierten Aliase zu löschen und sie durch eigene Funktionen zu ersetzen, die zur Ausführung der Befehle eine temporäre Kopie von cmd.exe aufrufen:

```
Remove-Item alias:dir
function dir {cmd /c dir $args}
```

```
8: help about_Line_Editing
9: Get-Content -force \ProgramData
10: dir \
11: dir -force \
12: Get-History -count 20
13: get-help Get-History
14: Get-History -id 3
15: Get-History | Select-String "WMI"
16: Get-History | Select-String "hist"
17: Get-History | Select-String "HIST"
```

Viele der vordefinierten Powershell-Aliase sollen Nutzern von cmd.exe oder bash den Umstieg erleichtern. Zum Beispiel der Befehl Get-Alias listet sie auf.

```
Size                    : 136364163072
MinimumSize             : 136364163072
LogicalSectorSize       : 512
PhysicalSectorSize      : 4096
BlockSize               : 33554432
ParentPath              :
DiskIdentifier          : 81859e6e-69bf-41c
FragmentationPercentage : 9
Alignment               : 1
Attached                : False
DiskNumber              :
Key                     :
IsDeleted               : False
Number                  :

PS I:\Hyper-V\Virtual Hard Disks> Get-VHD *.vhdx | where {$_.VhdType -eq "fixed"}
PS I:\Hyper-V\Virtual Hard Disks> Get-VHD *.vhdx | where {$_.VhdType -eq
```

Kopieren bis Zeichen:

Taste F2 stellt den vorhergehenden Befehl bis zum ersten Auftreten eines bestimmten Zeichens wieder her.

Diese Lösung funktioniert aus naheliegenden Gründen nicht mit Befehlen, die nur die Umgebung des aktuellen Kommando-Interpreters verändern, beispielsweise das Arbeitsverzeichnis wechseln, eine Umgebungsvariable setzen oder den Prompt neu festlegen. Außerdem muss bedacht werden, dass die Umstellung von einem vordefinierten Alias auf eine selbstdefinierte Funktion nur während der aktuellen Sitzung wirksam ist. Will man sie dauerhaft etablieren, muss man die entsprechenden Befehle in das Powershell-Profil aufnehmen.

Powershell-Befehle aus Cmd.exe aufrufen

Wer sich primär im alten Kommando-Interpreter zu Hause fühlt und von dort die Möglichkeiten der mächtigeren Powershell in Anspruch nehmen möchte, kann den umgekehrten Weg wählen und von Cmd.exe aus eine temporäre Kopie von Powershell aufrufen, um Cmdlets oder Scripts auszuführen. Das geht mit:

```
Powershell -command "Befehl"
```

Zu beachten ist hier, dass weitere Optionen für den Aufruf der Powershell (etwa *-NoProfile*) vor dem Parameter *-command* stehen müssen, weil sie sonst als Argumente an den Befehl weitergereicht werden. Bei Bedarf kann man getrennt durch Semikolon auch mehrere Befehle auf einmal übergeben

Befehlshistorie verwalten

Wie jeder ordentliche Kommando-Interpreter merkt sich auch Powershell die während einer Sitzung eingegebenen Befehle, so dass man diese bei Bedarf zurückholen kann, ohne sie erneut eintippen zu müssen. Neben mehreren Funktionstasten helfen dabei einige Cmdlets, um die Befehlshistorie zu nutzen. Die einfachste Möglichkeit, bereits abgesetzte Powershell-Befehle auf die Kommandozeile zurückzuholen, bieten wie bei cmd.exe die Cursor-Tasten. Allerdings wird die Suche auf diese Weise schnell mühselig, wenn man weiter zurück muss als zu den letzten zwei oder drei Eingaben. Man kann daher die Historie für die Navigation eingrenzen, indem man die ersten Zeichen eines bereits ausgeführten Kommandos eingibt und dann durch mehrfaches Drücken von F8 durch die gefilterte Liste iteriert. Obwohl Powershell bei Befehlen nicht zwischen Groß- und Kleinschreibung unterscheidet, tut das die History-Funktion hinter der Taste F8. Sie findet also nur Eingaben, wenn sie exakt mit den Zeichen beginnen, die man für die Suche eingegeben hat.

Eine weitere Option, die Befehlshistorie zu durchlaufen, liegt wie bei cmd.exe hinter der „F7"-Taste. Ihre Ausgabe entspricht jener des Cmdlets „Get-History", nur mit dem Unterschied, dass man sich mit den Pfeiltasten durch die Liste bewegen und von dort ein bestimmtes Kommando starten kann. Dagegen ist das Eingabefeld, das man durch Drücken von F9 erhält, nur dann von Nutzen, wenn man die ID des gesuchten Befehls kennt (was oft auch nichts hilft, weil die Zählweise nicht mit jener von „Get-History" übereinstimmt).

Editieren des letzten Kommandos in der Powershell

Einfache Editiermöglichkeiten für den zuletzt ausgeführten Befehl bieten die Tasten F2 und F4. Erstere präsentiert ein Fenster mit der Anweisung „Kopieren bis". Hier gibt man das Zeichen ein, bis zu dem der letzte Befehl übernommen werden soll. Wenn dieser zum Beispiel *Get-Content -force \ProgramData* lautet und man gibt \ ein, dann kopiert die Funktion *Get-Content -force* in die Eingabezeile. F4 („Löschen bis Zeichen") dagegen würde „ProgramData" übernehmen, weil diese Funktion das Kommando bis zum ersten Auftreten des eingegebenen Zeichens löscht.

Eine weitergehende Bearbeitung der Befehlshistorie erlauben mehrere dafür zuständige Cmdlets. Get-History (Alias history) zeigt die gesamte Liste von maximal 64 Befehlen an, die Powershell per Voreinstellung speichert. Mit dem Schalter *-count* kann man die Ausgabe auf die letzten x Befehle reduzieren:

```
Get-History -count 20
```

Kennt man die ID eines Kommandos, dann kann man es mit *history - ID <id>* anzeigen. In der Regel wird dies nicht der Fall sein, vielmehr wird man in der Historie nach einem bestimmten Befehl suchen. Dabei hilft das Cmdlet Select-String:

```
Get-History | Select-String "WMI"
```

zeigt alle ausgeführten Befehle an, die „WMI" enthalten. Möchte man die Befehlshistorie löschen, dann übernimmt *Clear-History* diese Aufgabe. Ohne Parameter entfernt es alle Einträge, der Schalter *-count <x>* räumt die x ältesten Befehle ab. Praktisch ist die Option *-CommandLine <String>*, die alle Kommandos tilgt, in denen die angegebene Zeichenfolge vorkommt.

Keine persistente Speicherung der Befehle

Im Gegensatz zu Unix-Shells wie der „bash" speichert Powershell die Historie nicht dauerhaft, so dass nach dem Ende einer Sitzung alle dort eingegebenen Kommandos verloren gehen. Man kann sich dadurch behelfen, dass man die Ausgabe von *Get-History* in eine Datei schreibt und sie von dort später mit *Add-History* wieder in die Befehlshistorie übernimmt.

Historie in CSV-Datei zwischenspeichern

Allerdings reicht es nicht, wenn man zu diesem Zweck eine reine Textdatei verwendet. Vielmehr erwartet *Add-History* den Input in Form von History-Info-Objekten, die man mit *Get-History*, *Import-Clixml* oder *Import-Csv* erzeugen kann. Daher muss man die History in einer CSV- oder XML-Datei ablegen, um sie nachher wieder importieren zu können:

```
Get-History | Select -unique |
  Convertto-Csv > hist.csv
```

Dieses Beispiel entfernt doppelte Einträge und schreibt die gesamte Historie in die Datei „hist.csv". Aus dieser kann man sie dann später wiederherstellen:

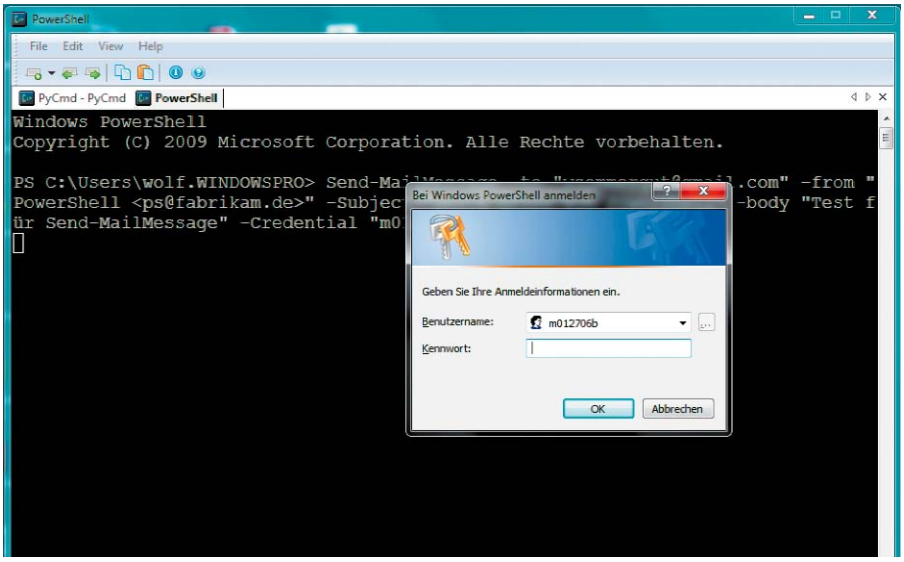
```
Get-Content hist.csv | Convert
  From-Csv | Add-History
```

Sind bereits Kommandos in der Historie vorhanden, hängt die obige Befehlszeile die Einträge aus der CSV-Datei am Ende an. ■

Mails aus Scripts versenden

Monitoring-Tools können beim Auftreten von Ereignissen Mails senden. Möchten Sie Nachrichten aus eigenen Scripts verschicken, bietet die Powershell dafür ein Cmdlet, für Batch-Dateien brauchen Sie ein Tool.

VON WOLFGANG SOMMERGUT



Im interaktiven Betrieb authentifiziert sich der User einfach mit Benutzernamen und Passwort am SMTP-Server.

SEIT DER VERSION 2.0 besitzt Powershell ein eigenes Cmdlet zum Versand von E-Mails. Es ist relativ einfach, ihm die Elemente einer Nachricht als Parameter zu übergeben und sich interaktiv am SMTP-Server zu authentifizieren. Trickreicher wird die Sache jedoch, wenn man Mails ohne Intervention eines Benutzers aus einem Script versenden möchte. Der Aufruf von *Send-MailMessage* erfolgt mit all jenen Parametern, die man von einem Mail-Client erwartet. Meistens wird man jedoch zum einen nicht alle Angaben benötigen, zum anderen sie nicht samt und sonders als Argumente übergeben. Je nach Anwendungsfall kann der Inhalt der Mail beispielsweise aus einer Logdatei stammen, die man mit Hilfe anderer Powershell-Cmdlets analysiert, oder man bestimmt die Anhänge, indem man den Inhalt eines Verzeichnisses ausliest.

Minimal-Aufruf von Send-Mailmessage

Ein einfacher Aufruf, der alle nötigen Angaben als Parameter übermittelt, könnte so aussehen:

```
Send-MailMessage -to "billg@con
 toso.com" -from "Powershell <ps@
 fabrikam.de>" -Subject "Test"
 -body "Test für Send-Mail
 Message"
```

Damit dieser Befehl erfolgreich sein kann, muss man zuvor den SMTP-Server als Vorgabewert in der Variable *$PSEmailServer* gespeichert haben, also nach dem Muster

```
$PSEmailServer = "smtp.fabrikam.
 de"
```

Andernfalls ist es notwendig, dass man den Ausgangs-Server über den Parameter *-SmtpServer* bestimmt. Wenn man öfter Mails auf diesem Weg versendet, dann empfiehlt es sich, $PSEmailServer schon im Powershell-Profil mit dem Standard-SMTP-Server vorzubelegen, damit dass man sich die manuelle Eingabe spart.

Anmeldung am SMTP-Server

Das Cmdlet im obigen Beispiel würde versuchen, sich gegenüber dem SMTP-Server mit den Windows-Anmeldedaten des aktuellen Benutzers zu authentifizieren. Wenn das jedoch nicht möglich ist, dann muss man zusätzlich ein PSCredential-Objekt für die Anmeldung mitliefern (es sei denn, der SMTP-Server verlangt keine Authentifizierung). Die einfachste Variante dafür ist, den Benutzernamen zusammen mit dem Parameter *-Credential* zu übergeben. Powershell öffnet dann einen Anmeldedialog (siehe Abbildung oben), in den man sein Passwort eintippen kann:

```
Send-MailMessage -to "billg@con
 toso.com" -from "Powershell <ps@
 fabrikam.de>" -Subject "Test"
 -body "Test für Send-Mail
 Message" -Credential "MailUser"
```

SMTP-Authentifizierung ohne Benutzereingriff

Diese interaktive Authentifizierung ist indes nicht ideal, wenn ein Script unter bestimmten Bedingungen selbständig Mails verschicken soll. Für diesen Fall muss man einen Weg finden, um die Anmeldung zu automatisieren.Die in anderen Umgebungen praktizierte unsiche-

re Methode, Passwörter an Send-MailMessage im Klartext zu übergeben, lässt Powershell nicht zu. Andererseits ist es aber auch nicht möglich, PSCredential-Objekte komplett in einer Datei zu speichern, um sie von dort bei Bedarf einzulesen.

Aus diesem Grund muss man das erforderliche PSCredential-Objekt vor dem Versand einer Mail erzeugen, indem man dafür einen Benutzernamen angibt und das Passwort aus einer Datei einliest, in der man es zuvor verschlüsselt gespeichert hat. Letzteres lässt sich auf folgende Weise bewerkstelligen:

```
(Get-Credential).password | Con
 vertFrom-SecureString > MailPW.
 txt
```

Das Cmdlet Get-Credential fordert den Benutzer dazu auf, seinen Namen und sein Passwort einzugeben. Es erzeugt daraus ein PSCredential-Objekt, aus dem der obige Befehl dann wieder das Kennwort als Secure String extrahiert und dieses verschlüsselt in der Datei „Mailpw.txt“ abspeichert.

PSCredential-Objekt vor dem Mail-Versand erzeugen

Vor dem Aufruf von *Send-MailMessage* erzeugt man das erforderliche PSCredential-Objekt, indem man für den betreffenden User das Passwort aus dieser Datei ausliest und wieder zurück in einen Secure String verwandelt:

```
$pw = Get-Content .\MailPW.txt |
 ConvertTo-SecureString
$cred = New-Object System.Manage
 ment.Automation.PSCredential
 "MailUser", $pw
```

Die Variable *$cred* kann man anschließend Send-MailMessage über den Parameter *-Credential* mitgeben, um den Benutzer zu authentifizieren:

```
Send-MailMessage -Credential
 $cred -to "billg@contoso.com"
 -from "Powershell <ps@fabrikam.
 de>" -Subject "Test" -body "Test
 für Send-MailMessage"
```

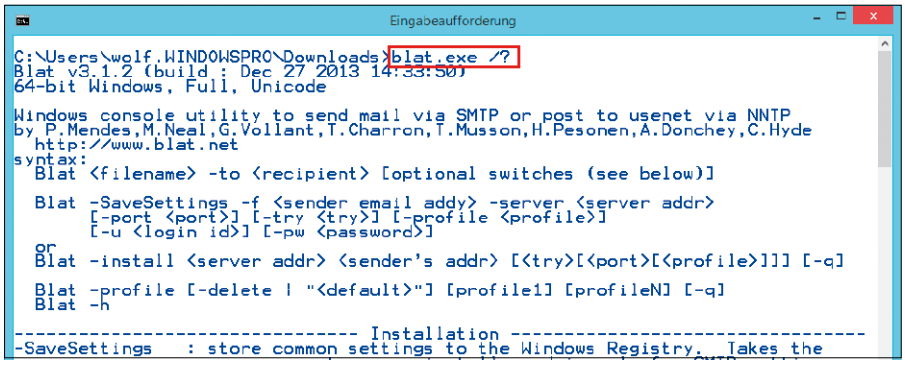
Auch für diese Prozedur kann man überlegen, ob man das PSCredential-Objekt bereits beim Start von Powershell über das Profil anlegt.

So bewahren Sie Umlaute und Sonderzeichen

Eine letzte Hürde stellt der verwendete Zeichensatz dar. Lässt man den Parameter *-Encoding* weg, dann lautet die Voreinstellung auf Ascii. Enthält der Betreff oder die Nachricht Umlaute oder andere Sonderzeichen, dann kommen diese verstümmelt beim Empfänger an. Daher wird man in der Regel UTF8 verwenden, um den Inhalt unbeschadet zu übertragen. Dies teilt man dem Cmdlet mit, indem man den Parameter

```
-encoding ([System.Text.
 Encoding]::UTF8)
```

hinzufügt.



Ruft man „blat.exe“ mit /? auf, dann zeigt sich die Mächtigkeit des Tools anhand zahlloser Optionen.

Anhänge über eine Pipe einfügen

Möchte man Anhänge nicht als eine Liste von Dateinamen für den Parameter *-Attachments* eintippen, sondern beispielsweise aus dem Inhalt eines Verzeichnisses auslesen, dann kann man sie über eine Pipe an *S*end-MailMessage schicken:

```
Get-ChildItem f*.jpg | Send-Mail
 Message -Credential $cred -to
 "billg@contoso.com" -from "Pow
 ershell <ps@fabrikam.de>" -Sub
 ject „"Test" -body "Test für
 Send-MailMessage" -encoding
 ([System.Text.Encoding]::UTF8)
```

Send-MailMessage bietet noch einige weitere Optionen, wobei die hier gezeigten Beispiele die meisten Fälle abdecken sollten.

Zu erwähnen wären vor allem noch *-BodyAsHtml* und *-UseSSL*, wenn die man eine HTML-Mail verschickt beziehungsweise den SMTP-Server über eine SSL-Verbindung ansteuert.

Mails aus Batch-Dateien mit Blat

Wenn man Mails aus Batch-Dateien versenden möchte, dann empfiehlt sich dafür das Open-Source-Tool Blat. Wie bei Programmen für die Kommandozeile häufig der Fall, besteht Blat aus einer einzelnen EXE-Datei und muss nicht installiert werden. Allerdings besteht die Möglichkeit einer nachträglichen Konfiguration, mit der sich die Werte für SMTP- oder POP3-Server sowie die Absenderadresse mittels Profilen in der Registry speichern lassen.

Beispielsweise würde man in der Eingabeaufforderung (Cmd.exe) die Werte für den SMTP-Server und die Absenderadresse folgendermaßen im Standardprofil hinterlegen:

```
blat -install smtp.MyDomain.de
 meine@mail-adresse.de
```

Zahlreiche Schalter und Optionen

Trotz dieser Arbeitserleichterung bleiben immer noch genügend Schalter und Parameter übrig, mit der man die Ausführung des Tools steuern kann. Ruft man Blat mit dem Argument „/?“ auf, dann wird man von den mehrere Bildschirmseiten füllenden Optionen regelrecht erschlagen. Die Funktionen reichen vom Versenden von Anhängen über cc: und bcc: bis zur Spezifizierung von Signature-Dateien und Zeichensätzen oder der Codierung mit Base 64.

In der Praxis wird man jedoch in den meisten Fällen mit einer überschaubaren Zahl an Argumenten auskommen. Ein Beispielaufruf könnte so aussehen:

```
blat -body "Das ist ein Test"
 -subject Test -u User -pw Pass
 wort -to rc@gmail.com
```

Zu den unabkömmlichen Angaben zählen die Adresse des Empfängers, der Betreff und der Inhalt der Nachricht sowie der Benutzername und das Passwort, wenn man sich wie heute üblich am SMTP-Server authentifizieren muss. Der Nachrichtentext kann entweder vom Kommandozeilenargument *-body* oder aus einer Datei stammen, die man mit dem Parameter *-bodyF* übermitteln muss.

Anmeldung mittels SMTP-Auth

Für die Anmeldung verwendet Blat standardmäßig SMTP-Auth, das von den meisten SMTP-Servern akzeptiert wird. Verbindungen über SSL unterstützt die Software jedoch nicht, so dass ein Versand von Nachrichten über große Web-Mailer wie Google Mail oder Hotmail nicht funktioniert. In diesem Fall hilft der flankierende Einsatz eines SSL-Proxy wie Stunnel (Infos über *http://www.stunnel.org*). Eine Anleitung für die Konfiguration dieser Kombination gibt es über *http://bit.ly/1fxR1vp*.

Da Stunnel jedoch als Dienst installiert und konfiguriert werden muss, stellt sich vermutlich die Frage, ob sich der Aufwand lohnt. In den meisten Fällen wird es einfacher sein, einen alternativen SMTP-Server zu wählen. ■

Datum in Scripts berechnen

Zum Funktionsumfang von Powershell gehört das Cmdlet Get-Date, mit dem man alle erdenklichen Datumsberechnungen einfach erledigt. Dagegen bewältigt man solche Aufgaben in Batch-Dateien nur mühsam.

VON WOLFGANG SOMMERGUT

RUFT MAN „GET-DATE“ ohne Argumente auf, dann gibt es nur das Systemdatum aus. Daraus soll man jedoch nicht den voreiligen Schluss ziehen, dass es sich dabei nur um die Powershell-Entsprechung zum „date“-Befehl der alten Eingabeaufforderung handelt. Vielmehr beherrscht es fast beliebige Datumsberechnungen und Datumsformate.

Zu den simplen Aufgaben gehört es, die Bestandteile eines Datums zu extrahieren, sei es Monat, Jahr oder Wochentag. Sie alle sind Eigenschaften eines date-time-Objekts und lassen sich ohne umständliches Parsen einer Zeichenkette direkt ausgeben. Lädt man zum Beispiel die aktuelle Systemzeit in die Variable „$datum“

```
$datum = Get-Date
```

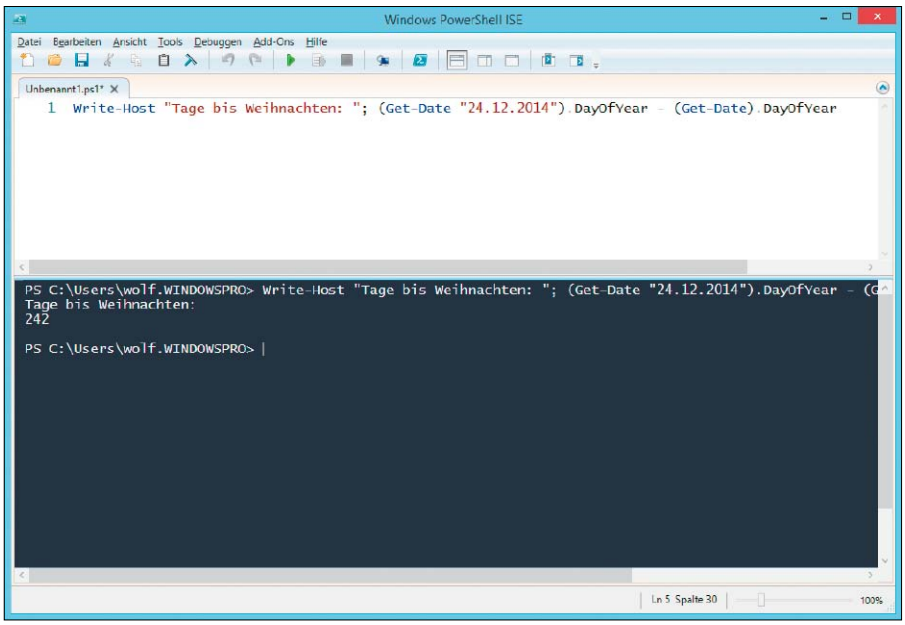
dann kann man auf einzelne Teile des Datums so zugreifen:

```
$datum.Day        # Tag des Monats
 (numerisch)
$datum.Month      # Monat (nume
 risch)
$datum.DayOfWeek # Wochentag
 (String auf Englisch, also z.B.
 "Monday")
```

Dabei werden keine Zeichenketten ausgelesen, vielmehr berechnet das date-time-Objekt die Werte der betreffenden Eigenschaften. Das erkennt man daran, dass man Get-Date mit einem beliebigen Datum laden und daraus die einzelnen Properties abrufen kann.

```
(Get-Date "24.08.2014").DayOfWeek
```

gibt wunschgemäß den Wochentag des 24. August 2014 aus.



Bei der Berechnung von Datumswerten kann man arithmetische Operatoren verwenden.

So geben Sie Wochentag auf Deutsch aus

Wie schon erwähnt, hat die DayOfWeek-Eigenschaft den Nachteil, dass man den Wert auf Englisch angezeigt erhält.

Wer die deutschen Wochentage möchte, kann sie über den Parameter „-Format“ bekommen:

```
Get-Date "24.08.2014" -Format
 dddd
```

Der Parameter „-Format“ eignet sich natürlich nicht nur, um bestimmte Werte aus dem Datum auszulesen. Vielmehr kann er die Ausgabe praktisch nach Belieben gestalten, etwa um es ohne Uhrzeit und Wochentag in Kurzform darzustellen:

```
Get-Date -Format d.M.yyyy
```

Arithmetische Operationen mit Datumsangaben

Neben den zahlreichen Eigenschaften bietet ein date-time-Objekt noch Methoden, die alle möglichen Berechnungen von Datumswerten erlauben. So kann man mit Hilfe von „AddDays“ eine bestimmte Anzahl von Tagen zu einen Datum addieren, das Gleiche funktioniert mit entsprechenden Funktionen auch mit Monaten, Stunden, Minuten und so weiter. Zum Beispiel gibt

```
(Get-Date "24.08.2014").Add-
 Days(30).DayOfWeek
```

den Wochentag jenes Datums aus, das 30 Tage nach dem 24. August 2014 liegt. Bei Berechnungen von Datumswerten ist auch der Einsatz

von arithmetischen Operatoren erlaubt. Das sieht dann so aus:

```
(Get-Date "24.12.2014").DayOfYear
  - (Get-Date).DayOfYear
```

Dieses Beispiel berechnet, wie viele Tage es noch bis Weihnachten dauert.

Nur Datum oder nur Zeit extrahieren

Interessant sind zwei weitere Methoden, wenn man aus einem date-time-Objekt nur den Datums- oder Zeitanteil extrahieren will. Es handelt sich dabei um „ToShortDateString()“ und „ToShortTimeString()“. So gibt

```
(Get-Date).ToShortTimeString()
```

nur die aktuelle Zeit ohne Datum aus.

Wer sich eine Übersicht über alle Eigenschaften und Methoden eines date-time-Objekts verschaffen will, tut dies mit diesem Befehl:

```
Get-Date|Get-Member
```

Datumsangeben analysieren in Batch-Dateien

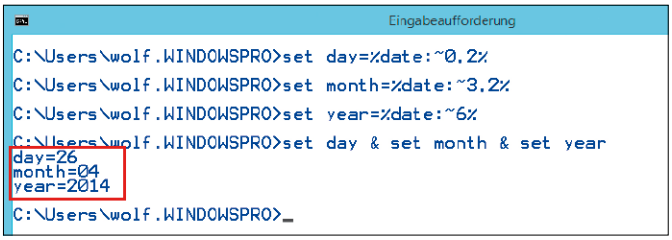
Wenn man aus irgendwelchen Gründen auf die komfortablen Möglichkeiten der Powershell verzichten will oder muss, um Datumswerte zu berechnen, dann kann man diese Aufgabe mit einigen Einschränkungen auch in herkömmlichen Batch-Dateien bewältigen.

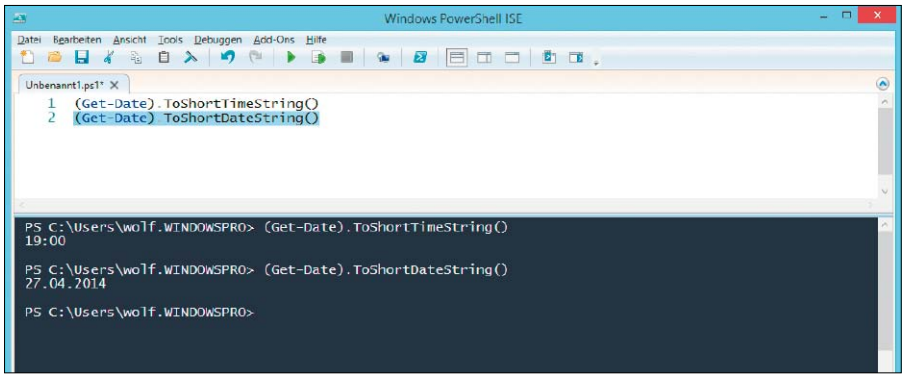
Eine typische Anwendung dafür ist das Erzeugen von Dateinamen, etwa für Backups, so dass sich ihr Erstellungsdatum aus dem Namen ablesen lässt. Während sich die numerischen Informationen relativ einfach auslesen lassen, stoßen die die reinen Batch-Mittel bei der Ermittlung des Wochentags an ihre Grenzen.Das Datumsformat gilt systemweit und ist daher unabhängig davon, aus welcher Quelle man das Datum in Batch-Dateien bezieht. Zur Auswahl stehen je nach Problem, das es zu lösen gilt, der Aufruf von „date /t“ oder die vorgegebene Umgebungsvariable „%date%“. Will man daraus Tag, Monat oder Jahr extrahieren, dann muss man sich beim Parsen des Datums darauf verlassen, dass auf allen PCs, auf denen die Batch-Datei laufen soll, die gleichen Ländereinstellungen gelten. Denn während beim deutschen Format (tt.mm.jjjj) an der zweiten Position der Monat steht, findet sich bei den US-Einstellungen (mm/tt/jjjj) dort der Tag.

Systemunabhängiges Datumsformat erzeugen

Hat man es mit verschiedenen Datumsformaten zu tun, dann besteht ein Ausweg darin, die Daten für Tag, Monat und Jahr über wmic auszulesen und selbst zu einem einheitlichen Datumsformat zusammenzufügen. Dies könnte in einer Batch-Datei so aussehen:

Mit Hilfe des SET-Befehls lassen sich die numerischen Werte für Tag, Monat und Jahr leicht aus dem Datum extrahieren.





Die Funktionen „ToShortTimeString()“ und „ToShortDateString()“ extrahieren die Zeit aus einem Date-Time-Objekt.

```
set MYDATE=
for /f "tokens=2,3,4 delims=," 
 %%g in ('wmic path win32_loca
 ltime get day^,month^,year ^/
 format:csv^|findstr /i %COMPU
 TERNAME%') do (if %%h LSS 10
 (set MYDATE=%%g.0%%h.%%i) else
 (set MYDATE=%%g.%%h.%%i))
```

In diesem Fragment werden in der Ausgabe von wmic die Spaltenüberschriften mit „findstr“ ausgefiltert und dann in der for-Schleife die Werte an den Positionen 2,3 und 4 in die Umgebungsvariable „MYDATE“ geschrieben. Die Fallunterscheidung im if/else-Statement dient dazu, den numerischen Werten der Monate Januar bis September eine Null voranzustellen.

Datum mit SET in Tag, Monat und Jahr zerlegen

Wenn man mit dem Inhalt der Umgebungsvariable „%date%“ zufrieden ist und kein eigenes Format produzieren will, dann ist das Parsen des Datums mit Hilfe von „set“ relativ einfach. Voraussetzung ist allerdings, dass wie beim deutschen Datumsformat sowohl Tag als auch Monat zweistellig sind, sonst wird es kompliziert. Der Tag, der Monat und das Jahr lassen sich beim vorgegebenen Kurzformat mit

```
set day=%date:~0,2%
set month=%date:~3,2%
set year=%date:~6%
```

auslesen.

Wochentag ermitteln

In zahlreichen Forenbeiträgen wird immer wieder danach gefragt, wie man in einer Batch-Datei den aktuellen Wochentag herausfinden kann. Und immer wieder folgt die Empfehlung, einfach die beiden ersten Zeichen von „%date%“ beziehungsweise „date /t“ zu nehmen. Allerdings funktioniert diese Lösung seit XP nicht mehr, weil Microsoft nach Windows 2000 den Wochentag aus der Datumsausgabe entfernt hat. Man könnte diesen Zustand ändern und auf die alte Darstellung zurückkehren, indem man in der Systemsteuerung unter „Region und Sprache“ das Format für „Datum (kurz)“ auf TTTT, TT.MM.JJ ändert. Allerdings stellt sich die Frage, ob man solche systemweiten Einstellungen wegen einer Batch-Datei permanent auf allen PCs verändern möchte.

Eine Alternative bietet auch hier das WMI-Tool wmic, das den aktuellen Wochentag in numerischer Form liefert, die man in eine Zeichenkette konvertieren kann. Sie wird dann in der Variablen „DOW“ gespeichert. Wie im obigen Beispiel ist es erforderlich, unerwünschten Output zu entfernen, in diesem Fall eine abschließende Leerzeile:

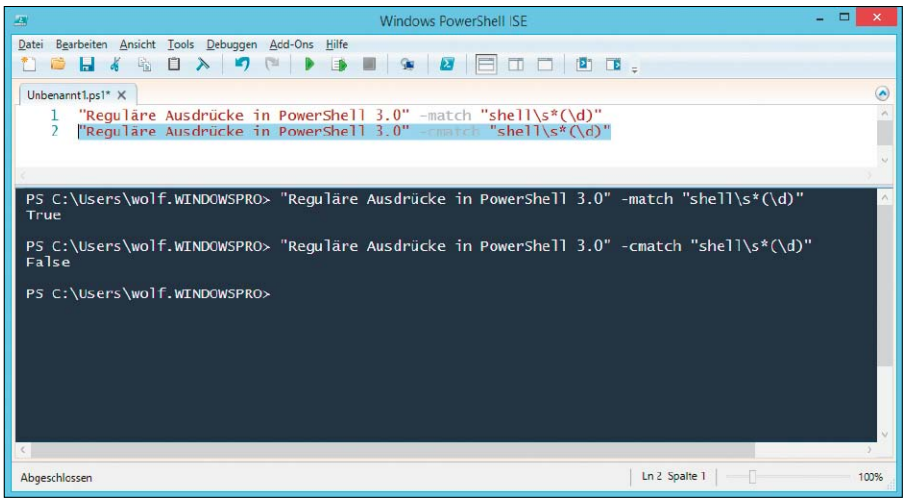
```
set DOW=
for /f %%g in ('wmic path win32_
 localtime get dayofweek^|findstr
 /v /r "^$"') do (set DOW=%%g)
if %DOW%==0 set DOW=So
 if %DOW%==1 set DOW=Mo
 if %DOW%==2 set DOW=Di
 if %DOW%==3 set DOW=Mi
 if %DOW%==4 set DOW=Do
 if %DOW%==5 set DOW=Fr
 if %DOW%==6 set DOW=Sa
```

Auch hier ist darauf zu achten, dass das Pipe-Symbol mit einem „^“ maskiert werden muss. ■

Regex in Powershell

Powershell bietet mehrere Sprachkonstrukte, die eine Verwendung von regulären Ausdrücken (Regex) zulassen. Das Tool orientiert sich an Perl, so dass die Regex-erfahrenen Nutzer damit schnell klarkommen.

VON WOLFGANG SOMMERGUT



Der Operator „-match“ unterscheidet nicht zwischen Groß- und Kleinschreibung, dafür gibt es „cmatch“.

IM VERGLEICH zu einfachen Wildcards sind reguläre Ausdrücke viel mächtiger, weil sich ihre Möglichkeiten nicht auf simple Platzhalter reduzieren. Beispielsweise lassen sich damit Bereiche festlegen (etwa [a-d]), Typen von Zeichen (numerisch, alphabetisch, Whitespace etc.), unterscheiden oder die Häufigkeit ihres Vorkommens durch verschiedene Quantifizierer beliebig bestimmen. Besonders praktisch beim Suchen und Ersetzen ist die Möglichkeit, die beim Matching ermittelten Fundstellen als Variablen im Ersetzungstext nutzen zu können. Eine gute Übersicht über die sprachlichen Mittel von Regex in Powershell gibt über *http://bit.ly/1fycv0E* ein Cheat Sheet zum Download.

Mustervergleich mit dem Operator „-match“

Powershell bietet eine Reihe von Vergleichsoperatoren (genaue Infos gibt’s etwa unter *http://bit.ly/1md7rNU*), die sich nicht nur auf numerische Werte anwenden lassen, sondern auch auf String-Objekte. Einer davon ist „-match“, dessen Besonderheit darin besteht, dass er als Vergleichsausdruck nicht nur wörtlich zu nehmende Zeichenketten akzeptiert, sondern auch Regex:

```
"Reguläre Ausdrücke in PowerShell
 3.0" -match "shell\s*(\d)"
```

Dieser Ausdruck ergibt den Wert TRUE. Das ist insofern überraschend, als bei Regex normalerweise zwischen Groß- und Kleinschreibung unterschieden wird. Im Beispiel enthält die Zeichenkette, auf die das Muster passen soll, „PowerShell“ mit einem großen „S“, während es im regulären Ausdruck klein geschrieben ist. Wenn der Mustervergleich case-sensitive sein soll, dann kann man den Operator „-cmatch“ verwenden. Zusätzlich gibt es noch „-imatch“, das genauso funktioniert wie „-match“, aber aus dessen Name explizit hervorgeht, dass es nicht zwischen Groß- und Kleinschreibung unterscheidet (und damit hilft, unerwartete Nebeneffekte zu vermeiden). Meistens will man bei komplexeren regulären Ausdrücken nicht nur wissen, ob ein Muster zutrifft, sondern auch auf welche Zeichenketten sie gepasst haben. Dies kann man über das Array „$matches“ herausfinden. Die Variable „$matches[0]“ enthält den gesamten String, auf den ein Muster passt, die folgenden Mitglieder des Arrays speichern die so genannten Group Matches. Es handelt sich dabei um Teile des Musters, die man in Klammern setzt, im obigen Beispiel wäre das „(\d)“.

Eine Eigenart von „-match“ und seinen Varianten besteht darin, dass es nur das erste Zutreffen eines Musters ermittelt, weitere Treffer werden nicht berücksichtigt.

Select-String mit den Parametern „-pattern“ und „-AllMatches“

Wenn man alle Fundstellen für einen regulären Ausdruck in einer Zeichenkette ermitteln möchte, dann eignet sich für diese Aufgabe das Cmdlet Select-String. Dieses bietet einen Parameter namens „-pattern“, dem man einen regulären Ausdruck übergibt.

Auch Select-String bricht nach dem ersten Zutreffen des Musters in einer Zeile ab. Dieses Verhalten kann man allerdings mit Hilfe des zusätzlichen Schalters „-AllMatches“ abstellen:

```
help about_regular_expressions |
 Select-String -pattern "ein.*"
 -AllMatches
```

Möchte man hier alle Fundstellen ausgeben, dann kann man über die Matches-Eigenschaft der zurückgegebenen MatchInfo-Objekte iterieren (mit „%“ als Alias für „foreach“ im folgenden Beispiel) und aus ihnen den Wert der Eigenschaft „Value“ auslesen:

```
help about_reg| Select-String
 -pattern "ein.*" -AllMatches |
 %{$_.matches}| %{$_.value}
```

Das Ergebnis dieser Anweisung besteht jedoch in der kompletten Zeile, auf die der reguläre Ausdruck irgendwo passt. Möchte man die exakten Übereinstimmungen sehen, dann hilft ein Filter, wie ihn Tobias Weltner auf Power shell.com (*http://bit.ly/1hW1iBG*) vorstellt.

Suchen und Ersetzen mit „-replace“

Möchte man bestimmte Textmuster nicht nur finden, sondern durch andere Zeichenketten ersetzen, dann dient in Powershell der Operator „-replace“ diesem Zweck. Erwartungsgemäß benötigt er als Input zwei Angaben, nämlich den regulären Ausdruck und durch ein Komma getrennt den Ersetzungstext:

```
"Einführung in Powershell 2.0"
 -replace "\d\.", "3."
```

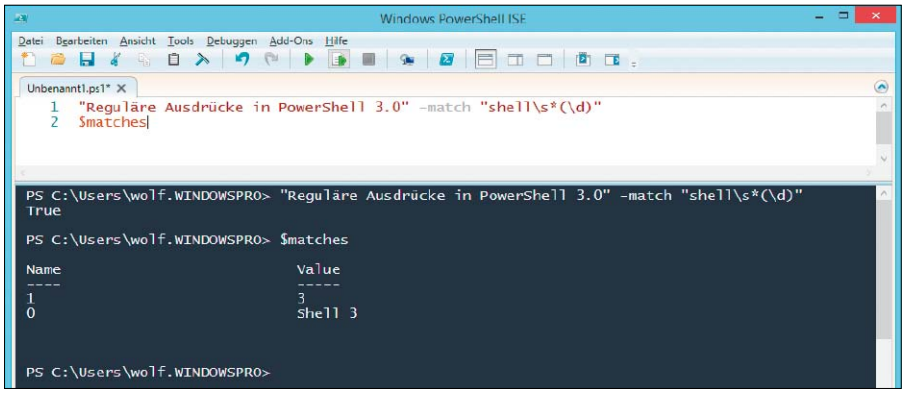
Dieser Aufruf gibt anders als „-match“ keinen boolschen Wert zurück, der über das Zutreffen des Musters informiert, sondern die geänderte Zeichenkette. Im obigen Beispiel wird aus „2.0“ ein „3.0“.

Oft möchte man einen Abschnitt, auf den ein regulärer Ausdruck zutrifft, nicht einfach durch eine feste Zeichenkette ersetzen, sondern dort Teile des ursprünglichen Textes wiederverwenden. In der Regel muss man zu diesem Zweck die Rückwärtsreferenzen mit Hilfe von Gruppierungen in den Variablen „$1“, „$2“, etc. einfangen. Bestimmte Werte, etwa „$&“ (gesamter String, auf den das Muster zugetroffen hat), sind jedoch automatisch vorhanden.

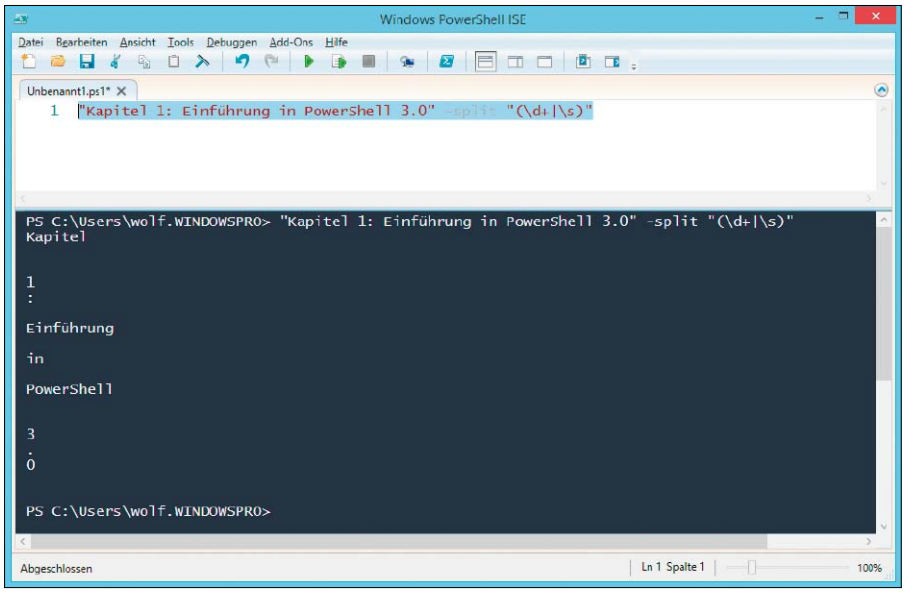
Wenn man zum Beispiel in der hosts-Datei bei allen IP-Adressen, die mit 192.168. beginnen, das dritte Oktett durch den Wert „99“ ersetzen möchte, dann kann man dies so tun:

```
$IPs = Get-Content -Path C:\Win
 dows\system32\drivers\etc\hosts
$IPs -replace "192\.168\.\d{1,3}\.
 (\d{1,3})", '192.168.99.$1'
```

Das Teilmuster, das auf das letzte Oktett der IP-Adresse zutrifft, steht als einziges in runden Klammern. Daher lässt es sich über „$1“ ansprechen und in die neue IP-Adresse übernehmen. Bei der Formulierung eines solchen Befehls ist daran zu denken, dass der Ersetzungstext in einfachen Anführungszeichen stehen sollte, weil Powershell die Variablen in doppelten Anführungszeichen schon expandiert, bevor sie an die Regex-Engine übergeben werden. Da „$1“, „$2“ und so weiter nicht vorbelegt sind, werden sie durch die leere Zeichenkette ersetzt. Der Operator „-replace“ belegt übrigens nicht wie „-match“ die Variable „$matches“ mit den Fundstellen für das angegebene Muster.



Die Elemente des Arrays „$matches“ speichern die „Group Matches“, also jene Teile, die man in Klammern setzt.



Wenn man Zeichenketten mit Hilfe von „-split“ auftrennen will, dann kann man Muster als Delimiter verwenden.

Dateien umbenennen mit Regex

Ein weiteres Anwendungsbeispiel für Suchen und Ersetzen mittels Regex ist das Umbenennen mehrerer Dateien. In diesem Fall muss man „Get-ChildItem“ zu Hilfe nehmen, das Wildcards auswerten kann und die Liste der zutreffenden Dateinamen zurückgibt.

```
Get-ChildItem *.pdf | Rename-Item
 -NewName {$_.Name -replace
 '20\d{2}','2013'}
```

In diesem Beispiel werden alle PDF-Dateien im aktuellen Verzeichnis umbenannt, wenn ihr Name die Zeichenkette „20“ plus zwei unmittelbar darauf folgende Ziffern enthält. Dann wird etwa „2010“ oder „2011“ durch „2013“ ersetzt. Angenommen, man hat mehrere Dokumente nach dem Muster „Rechnung“-<Monat>-<Jahr>“.xls“ benannt und möchte nun im Namen Monat und Jahr vertauschen, dann könnte man das mit diesem Befehl bewerkstelligen:

```
gci *.xls | Rename-Item -NewName
 {$_.Name -replace
 "Rechnung-(\d{2})-(\
 d{4})",'Rechnung-$2-$1.xls'}
```

Zeichenketten zerlegen mit „-split“

Der Operator „-split“ dient dazu, Strings an definierten Trennzeichen in mehrere Teil-Strings zu zerlegen. Meist dienen wörtlich zu interpretierende Zeichen als Delimiter, typischerweise sind das Tabulatoren, Semikolon oder Leerzeichen. Eine flexiblere Variante besteht darin, dass man die Positionen zum Auftrennen eines Strings über reguläre Ausdrücke definiert. Ein einfaches Beispiel könnte so aussehen:

```
"Kapitel 1: Einführung in Power
 shell 3.0" -split "(\d+|\s)"
```

Dieser Aufruf trennt die angegebene Zeichenkette entlang aller Zahlen und Whitespace-Zeichen auf. ■

Powershell für Webseiten

Microsoft erweiterte Powershell 3.0 um Funktionen, die Ähnliches leisten wie curl oder wget. Dazu zählen der Download von Dateien, das Parsing von HTML-Seiten und das Ausfüllen von Formularen.

VON WOLFGANG SOMMERGUT

OBWOHL ES MEHRERE CMDLETS GIBT, mit denen man eine Kommunikation über HTTP anstoßen oder Inhalte parsen kann, spielt „Invoke-WebRequest" dabei die wesentliche Rolle. Es kann nicht nur Dateien und Webseiten herunterladen, sondern es bietet auch die nötigen Methoden, um durch den DOM-Baum eines HTML-Dokuments zu navigieren oder um Formulare zu versenden.

Das Herunterladen von Dateien von der Kommandozeile oder in Scripts ist etwa dann praktisch, wenn man keinen funktionierenden Browser zur Verfügung hat. Das ist beispielsweise der Fall, wenn man auf einem Windows Server arbeitet und nicht die verstärkte Sicherheitskonfiguration des IE deaktivieren möchte. Die Nutzung von Powershell für den Download einer Datei ist sehr einfach:

```
Invoke-WebRequest "http://down
 load.pdfforge.org/download/pdf
 creator/PDFCreator-
 stable?download" -Outfile PDF
 Creator.exe
```

Dieses Beispiel lädt den kostenlosen Pdfcreator herunter und speichert ihn im aktuellen Verzeichnis als „Pdfcreator.exe". Auf die gleiche Weise könnte man eine Datei auch von einem FTP-Server herunterladen, wenn man die URI entsprechend anpasst und „http://" durch „ftp://" ersetzt.

So prüfen Sie den Return-Code und den HTTP-Header

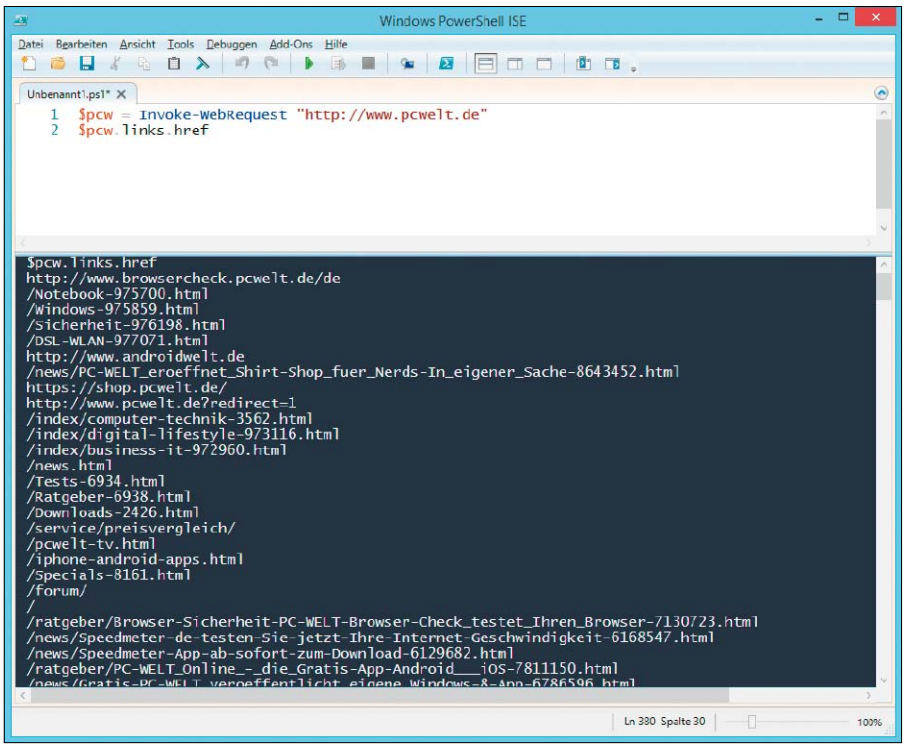
Lädt man eine binäre Datei herunter oder öffnet man eine Webseite, dann gibt „Invoke-WebRequest" Auskunft über die erfolgte HTTP-Kommunikation. Diese Informationen liegen als Eigenschaften des zurückgegebenen „HtmlWebResponseObject" vor.

Aufschlussreich für die Analyse der HTTP-Übertragung sind etwa der Statuscode sowie der HTTP-Header:

```
$wp = Invoke-WebRequest "http://
 de.wikipedia.org/"
```

Nach diesem Aufruf der Wikipedia-Homepage könnte man über „$wp.StatusCode" erfahren, ob Fehler bei der Aktion aufgetreten sind. Der verwendete Zeichensatz und der Content-Type ließe sich ermitteln über:

```
$wp.Headers["Content-Type"]
```



Das „HtmlWebResponseObject" enthält alle Links der angeforderten Seite, deren href-Attribut man ausgeben kann.

Parsing von HTML-Seiten

Bei HTML-Seiten liegen wesentliche Elemente direkt als Eigenschaften des zurückgegebenen Objekts vor. Dazu zählen alle auf der Webseite enthaltenen Links („links"), Formulare („forms"), Bilder („images") oder Scripts („scripts").

Wenn man etwa den Wikipedia-Eintrag zu „Chiemsee" abruft:

```
$cs = Invoke-WebRequest "http://
 de.wikipedia.org/wiki/Chiemsee"
```

dann erhält man eine Sammlung aller in der Seite enthaltenen Bilder mit

```
$cs.Images
```

Möchte man die Ausgabe noch filtern, etwa indem man nur Bilder wählt, die zwischen 100 und 199 Pixel breit sind, dann hilft ein Vergleich unter Verwendung eines regulären Ausdrucks:

```
$cs.Images | where {$_.width
 -match "1.{2,}"}
```

Webseiten überwachen

Eine interessante Anwendung für „Invoke-WebRequest" könnte in einem Screen Scraping bestehen, bei dem man kritische Informationen aus einer Seite ausliest, um etwa einen fehlerhaften Zustand der Website zu ermitteln. Für diese Aufgabe gibt es mehrere Möglichkeiten, ein bestimmtes Element auszuwählen. Eine davon ist die Methode „FindById", mit der man direkt auf einen Knoten zugreifen kann, der über ein „ID"-Attribut eindeutig bezeichnet wird. Der folgende Befehl würde beispielsweise zum Element „ Die Liste meiner Links " führen:

```
$cs.AllElements.
 FindById("Weblinks")
```

Deutet innerhalb eines Abschnitts eine bestimmte Zeichenkette darauf hin, dass Probleme vorliegen, dann kann man diese relativ einfach finden:

```
$cs.AllElements.
 FindById("Comments") | where
 innerhtml -like *Viagr*
```

Wenn in diesem Fall eine Sektion mit der ID „Comments" die Zeichenkette „Viagr" enthält, so wäre das wahrscheinlich ein Hinweis auf Spam. In einem Script könnte man dann eine Benachrichtigung per Mail versenden, damit der Webmaster die Site bereinigt.

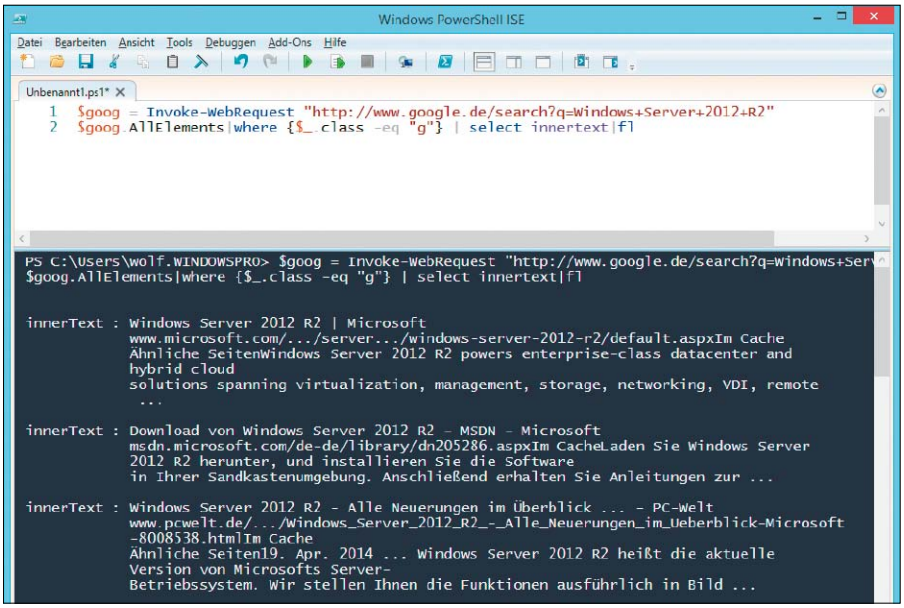
Filter anhand von Tag-Namen und Attributen

Ein alternatives Vorgehen, um bestimmte HTML-Fragmente zu extrahieren, besteht im Filtern durch Elementnamen und Attributwerte:

```
$cs.AllElements | where {$_.tag
 Name -eq "p" -and $_.class -eq
 "content"}
```

In diesem Aufruf erhält man alle Absätze (also <p>-Elemente), die mit der CSS-Klasse „content" formatiert wurden. Ein weiteres Beispiel zeigt, wie man bei einer Google-Suche nach „Windows Server 2012 R2" die reinen Textinformationen aus den Ergebnissen ausliest.

```
$goog = Invoke-WebRequest
 "http://www.google.de/search?q=W
 indows+Server+2012+R2"
```



Mit Hilfe von Powershell ließen sich relativ einfach Informationen aus den Suchergebnissen von Google auslesen.

```
$goog.AllElements|where {$_.class
 -eq "g"} | select innertext|fl
```

Der zweite Befehl filtert alle Elemente aus, deren „class"-Attribut den Wert „g" hat (und das sind bei Google die Listenelemente für die einzelnen Treffer) und extrahiert über die Eigenschaft „innertext" den Textanteil des Knotens. „innerhtml" dagegen liefert den gesamten Inhalt des Elements inklusive Markup. „outerhtml" umfasst zusätzlich das Element selbst.

Formulare ausfüllen und senden

Viele Webdienste erfordern eine Anmeldung, wobei diese in der Regel über ein HTML-Formular erfolgt. Mit Hilfe von „Invoke-WebRequest" kann man eine Anmeldeseite herunterladen, die benötigten Felder ausfüllen und danach das Formular abschicken.

Wichtig ist dabei jedoch für den Abruf von Folgeseiten, dass der HTTP-Agent Cookies speichern kann, weil sonst die Session endet. Solche Verbindungsinformationen wie Anmeldedaten, Cookies oder die Bezeichnung des User Agent speichert das Powershell-Cmdlet in einer Session-Variablen. Sie sollte man bereits beim Aufruf der Log-in-Seite verwenden:

```
$dig = Invoke-WebRequest http://
 www.diigo.com/sign-in -Session
 Variable session
```

Dieses Beispiel führt anhand des Bookmark-Dienstes Diigo vor, wie man sich über ein Formular authentifizieren kann. Zu beachten ist hier, dass der Parameter „-SessionVariable" den Namen der Variablen ohne führendes Dollarzeichen erwartet.

Im nächsten Schritt muss man herausfinden, welches Formular zuständig ist und wie seine Felder heißen. Nach der Eingabe von *$dig.forms* stellt sich heraus, dass der Name des Formulars „loginForm" lautet. Seine Felder ermittelt man mit

```
$dig.Forms["loginForm"].Fields
```

Nun kann man diese mit den gewünschten Werten belegen:

```
$dig.Forms["loginForm"].
 Fields["username"] = "Meine@
 Mail-Adresse.de"
 $dig.Forms["loginForm"].
 Fields["password"] = "P@sswort"
 $dig.Forms["loginForm"].
 Fields["referInfo"] = ""
```

Um das Formular abzuschicken, muss man jene Anwendung aufrufen, die im „action"-Attribut des Formulars angegeben ist. Diese kann man entweder selbst aus dem Quelltext auslesen, oder man verwendet die Action-Eigenschaft des Formulars. Wenn dort nur ein relativer Pfad angegeben ist, muss man die Domäne selbst voranstellen:

```
$log = Invoke-WebRequest -Method
 POST -URI ("https://www.diigo.
 com" + $dig.Forms["loginForm"].
 action) -Body $dig.
 Forms["loginForm"].Fields -Web
 Session $session
```

Zu erwähnen wäre hier, dass die Formulardaten mit dem Parameter „-Body" an den Webserver übergeben werden. Die zu verwendende HTTP-Methode hängt davon ab, welche die Webanwendung verlangt, meistens ist es POST. Schließlich leitet man die Session-Informationen, die man beim ersten Aufruf in einer Variablen gespeichert hat, über den Parameter „-WebSession" weiter. ■

Powershell für User & Computer

Mit Powershell lässt sich fast jede administrative Aufgabe im Verzeichnisdienst von Microsoft bewältigen, darunter auch das Anlegen oder Anzeigen von Benutzer- und Computerkonten.

VON WOLFGANG SOMMERGUT

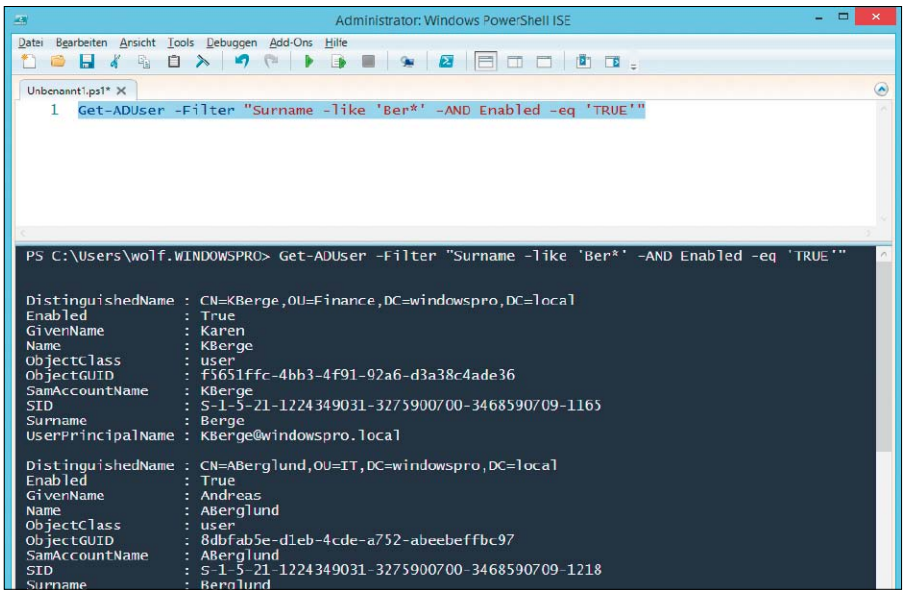
NACHDEM POWERSHELL sowohl ein interaktiver Kommandointerpreter als auch eine Script-Umgebung ist, kann man die AD-Cmdlets entweder in einzelnen Befehlen für kleinere Aufgaben einsetzen oder sie nutzen, um Scripts für komplexere Probleme zu entwickeln. Für komplexere Operationen steht jedoch eine Vielzahl an fertigen Tools und Befehlen zur Verfügung, so dass man eher selten in die Verlegenheit kommen sollte, aufwendig selbst programmieren zu müssen.

Das gilt beispielsweise beim Anlegen neuer Benutzerkonten, das Powershell mit Hilfe des Cmdlets „New-ADUser“ und mit einem ganzen Rattenschwanz von Parametern sehr gut bewerkstelligen kann.

Wenn man nur einzelne User anlegt, dann lässt sich dies über die grafischen AD-Tools einfacher erledigen. Bei einer größeren Zahl von Accounts unterstützt das kostenlose Z-Hire (→ Seite 34) den Administrator bei dieser Aufgabe durch Templates, die eine wiederholte Eingabe von bestimmten Daten vermeiden helfen.

Ähnlich ist die Lage beim Bulk-Import von Benutzern aus CSV- oder Excel-Dateien, wofür es ebenfalls mehrere, darunter auch kostenlose Tools gibt. Darüber hinaus existieren bereits zahlreiche mächtige AD-Scripts auf der „Powershell Script Gallery“, die auch immer einen Blick wert ist, wenn man Scripts für andere Zwecke benötigt.

Aus diesen Grund orientieren sich die folgenden Beispiele an Einzeilern, mit denen man auf der Kommandozeile ad hoc kleinere Aufgaben schnell bewältigen kann.



Filter für „Get-ADUser“ können komplexe Ausdrücke aus Attributen und Vergleichsoperatoren enthalten.

Benutzerkonten filtern

Häufig möchte man nur Informationen über Benutzer aus dem AD auslesen. Aber auch wenn man sie ändern will, muss man in den meisten Fällen die gewünschten User erst ermitteln. Dafür ist das Cmdlet „Get-ADUser“ zuständig, das mit Hilfe des „Parameters“ -Filter das Ergebnis gleich an der Quelle auf die benötigten Objekte einschränkt. Dies ist einem Vorgehen vorzuziehen, bei dem man alle User herunterlädt und dann lokal über eine Pipe durch ein „Where“-Objekt schickt:

```
Get-ADUser -Filter "Surname -like
  'Ber*'"
```

In diesem Beispiel gibt der Befehl alle User zurück, deren Nachname mit der Zeichenkette „Ber“ beginnt. Für Ausdrücke innerhalb des Filters kann man auch andere Vergleichsoperatoren verwenden, mit deren Hilfe man weitere Attribute prüfen kann.

Möchte man alle Konten abrufen, dann muss man den obligatorischen Parameter „-Filter „trotzdem verwenden, in diesem Fall mit dem Wert '*'.

Suche auf Domänen und OUs einschränken

Will man die Suche auf bestimmte Organisationseinheiten oder Domänen eingrenzen, dann steht dafür der Parameter „-SearchBase“ zur Verfügung:

```
Get-ADUser -Filter "Surname -like
  'Ber*'" -SearchBase
  "OU=IT,DC=contoso,DC=com"
```

Wie man an diesem Beispiel erkennen kann, erwartet „-SearchBase“ die Übergabe eines Distinguished Name.

In der Praxis möchte man User-Objekte nicht immer nur nach Namen filtern, sondern häufig auch nach anderen Eigenschaften. Standardmäßig zeigt „Get-ADUser“ aus Performance-Gründen jedoch nur wenige Attribute an. Das kann man mit dem Parameter „-Properties“ aber leicht ändern:

```
Get-ADUser -Filter "Surname -like
 'Ber*"" -Properties *
```

Anhand der Ausgabe dieses Befehls lassen sich die Namen der verschiedenen Attribute eruieren, die man dann in Filterausdrücken verwenden kann. Zum Beispiel könnte man alle Mitarbeiter, die der Niederlassung mit der Adresse „Rosenweg 1“ zugeordnet sind, auf diese Weise ermitteln:

```
Get-ADUser -Filter "StreetAddress
 -eq 'Rosenweg 1'"
```

Abfragen mit Search-ADAccount

Für bestimmte Abfragen ist indes „Search-ADAccount“ besser geeignet, weil es für eine Reihe von Eigenschaften spezifische Parameter akzeptiert. Das gilt etwa, wenn man wissen möchte, welche Benutzer sich ausgesperrt haben oder wessen Konto abgelaufen ist.

Um alle Benutzerkonten zu erfragen, deren Kennwort nie abläuft, würde man den Befehl

```
Search-ADAccount -PasswordNever
 Expires -UsersOnly
```

eingeben. Auch hier lässt sich die Abfrage mit „-SearchBase“ auf bestimmte Domänen oder OUs eingrenzen.

Weitere Parameter zur Spezifizierung von Attributen mit „Search-ADAccount“ sind unter anderem:

-AccountDisabled
-AccountExpiring <Datum>
-AccountInactive <Datum oder Zeitspanne>
(z.B.: -AccountInactive 31 für 31 Tage)
-LockedOut
-PasswordExpired

Attribute von User-Objekten per Powershell ändern

Oft ist das Abrufen von AD-Benutzern nach bestimmten Kriterien nur der erste Schritt, um anschließend ausgewählte Eigenschaften zu verändern. Letzteres lässt sich mit dem Cmdlet Set-ADUser erreichen:

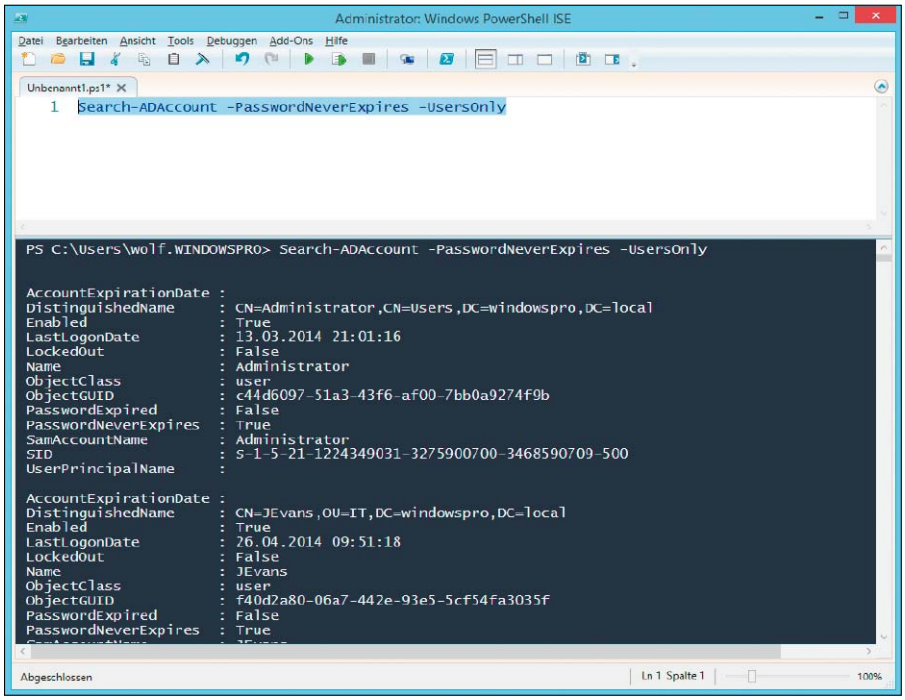
```
Get-ADUser -Filter * -SearchBase
 "OU=Marketing,DC=contoso,DC=com"
 | Set-ADUser -Manager PHuber
```

Mit diesem Befehl kann man den Vorgesetzten aller User in der OU „Marketing“ eintragen, wenn die entsprechende Abteilung einen neuen Leiter bekommen hat. Das Cmdlet akzeptiert eine Reihe von Schaltern, mit denen man jeweils einzelne Attribute mit einem neuen Wert versehen kann, im oben genannten Beispiel wäre das das Attribut „-Manager“.

Möchte man Konten mit bestimmten vorhandenen Attributwerten ändern, dann kann man in einem Kommando „Get-ADUser“ und „Set-ADUser“ kombinieren:

```
Get-ADUser -Filter "StreetAddress
 -eq 'Marsstr. 3'" | Set-ADUser
 -StreetAddress "Rosenweg 1"
```

In diesem Aufruf würde man die Anschrift in allen betroffenen Benutzerkonten ändern, wenn eine Niederlassung in eine andere Straße umgezogen ist.



Das Cmdlet „Search-ADAccount“ eignet sich etwa gut, um alle Konten anzuzeigen, deren Passwort nicht abläuft.

Computerkonten auslesen

Analog zur Abfrage und Änderung von Benutzerkonten bietet Powershell auch die entsprechenden Mittel, mit denen sich solche Operationen auf Computer-Accounts anwenden lassen. Um diese anzuzeigen und nach verschiedenen Kriterien zu filtern, gibt es das Cmdlet „Get-ADComputer“. Wie sein Gegenstück „Get-ADUser“ zum Auslesen von User-Objekten muss man ihm entweder den Namen eines Objekts oder einen Filter als Parameter übergeben. Will man sich alle Computer anzeigen lassen, dann wird man „-Filter“ mit einem Wildcard wählen:

```
Get-ADComputer -Filter *
```

Wie gewohnt kann man den Filter um Vergleichsausdrücke erweitern, um das Ergebnis einzuschränken. So würde bei Verwendung einer entsprechenden Namenskonvention im Unternehmen die Abfrage

```
Get-ADComputer -Filter "Name
 -like 'Win81*'"
```

alle PCs mit Windows 8.1 ausgeben.

Will man die Abfrage auf eine OU reduzieren, dann benötigt man zusätzlich den Parameter „-SearchBase“:

```
Get-ADComputer -Filter * -Search
 Base "OU=IT, DC=contoso, DC=com"
```

Die Suche in einer bestimmten Gruppe funktioniert nach dem gleichen Muster:

```
Get-ADComputer -Filter * -Search
 Base "CN=Workstations,
 DC=contoso, DC=com"
```

Möchte man nicht nur die standardmäßig angezeigten, sondern alle Attribute der Computerobjekte auflisten, dann fügt man auch hier zusätzlich den Parameter „-Properties *“ hinzu.

Computerkonto anlegen

Ein gängiges Anliegen besteht darin, Computerkonten im AD schon anzulegen, bevor die entsprechenden Rechner der Domäne beitreten. Auf diese Weise können sie schon vorab der richtigen OU zugeordnet werden und landen nicht im Container „Computer“.

Diesen Zweck erfüllt das Cmdlet „New-ADComputer“, dem man über die Parameter „-Name“ und „-Path“ den Namen und den Ort im AD übergibt. Wie in den obigen Beispielen ist auch hier die Angabe des Pfades in Form eines Distinguished Name erforderlich. ■

PC-WELT
ist eine Publikation des weltgrößten Computerzeitschriften-Verlags IDG und erscheint in vielen Ländern:

IMPRESSUM

Verlag

IDG Tech Media GmbH
Lyonel-Feininger-Straße 26
80807 München
Telefon: 089/36086-0
Telefax: 089/36086-118
E-Mail: *redaktion@pcwelt.de*
Internet: *www.pcwelt.de*

Chefredakteur
Sebastian Hirsch
(v.i.S.d.P. – Anschrift siehe Verlag)

Gesamtanzeigenleitung
Stefan Wattendorff
E-Mail: swattendorff@idgtech.de

Inhaber- und Beteiligungsverhältnisse
Alleiniger Gesellschafter der IDG Tech Media GmbH ist die IDG Communications Media AG, München, eine 100%ige Tochter der International Data Group, Inc., Boston, USA. Aufsichtsratsmitglieder der IDG Communications Media AG sind: Patrick J. McGovern (Vorsitzender), Edward Bloom, Toby Hurlstone.

WEITERE INFORMATIONEN

Redaktion

Lyonel-Feininger-Str. 26, 80807 München
E-Mail: *redaktion@pcwelt.de*

Chefredakteur: Sebastian Hirsch
(verantwortlich für den redaktionellen Inhalt)
Stellvertretender Chefredakteur:
Christian Löbering (cl)
Chef vom Dienst: Andrea Kirchmeier (ak)
Hardware & Testcenter: Thomas Rau (Leitung/tr), Sandra Ohse (so), Verena Ottmann (vo), Michael Schmelzle (ms), Dennis Steimels (ds), Friedrich Stiemer (fs), Ines Walke-Chomjakov (iwc)
Software & Praxis: Christian Löbering (stellvertretender Chefredakteur/cl), Arne Arnold (afa), Daniel Behrens (dab), Birgit Götz (bg), Peter Stelzel-Morawietz (psm)
Website-Management:
Hans-Christian Dirscherl (hc), Panagiotis Kolokythas (pk), Benjamin Schischka (bs)
Redaktionsassistenz: Manuela Kubon

Freier Mitarbeiter Redaktion:
Wolfgang Sommergut
Titelgestaltung:
Schulz-Hamparian, Editorial Design / Thomas Lutz
Freier Mitarbeiter Layout/Grafik:
Alexander Dankesreiter
Freie Mitarbeiterin Schlussredaktion:
Andrea Röder
Freier Mitarbeiter Video: Christian Seliger

Freier Mitarbeiter Digitale Medien:
Ralf Buchner

PC-WELT bei Facebook: www.facebook.com/pcwelt (Sebastian Hirsch v.i.S.d.P., Benjamin Schischka (bs))
PC-WELT bei Twitter: http://twitter.com/pcwelt (Sebastian Hirsch v.i.S.d.P., Panagiotis Kolokythas (pk))
PC-WELT in den Appstores: www.pcwelt.de/magazinapp
News-App der PC-WELT (kostenlos): www.pcwelt.de/iphoneapp, www.pcwelt.de/pcwapp
Einsendungen: Für unverlangt eingesandte Beiträge sowie Hard- und Software übernehmen wir keine Haftung. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, Beiträge auf anderen Medien herauszugeben, etwa auf CD-ROM und im Online-Verfahren.

Bildnachweis: sofern nicht anders angegeben: Anbieter

Anzeigen

Anzeigenabteilung
Tel. 089/36086-210, Fax 089/36086-263,
E-Mail: *media@pcwelt.de*
Gesamtanzeigenleitung:
Stefan Wattendorff (-212)

Chefredakteur Customer Solutions:
Andreas Perband (-818)

Objektleitung Tech Media Sales:
Christine Nestler (-293)
Senior Key Account Manager:
Thomas Ströhlein (-188)
Account Manager:
Moritz Kaiser (-854)
Junior Account Manager:
Claudia Jeck (-770)
Manager Sales Operations Group:
Marius Wolf (-410)
Handelsvertreter: Hartmut Wendt (-168)

Manager Ad-Management Print:
Thomas Weber (-728)

Digitale Anzeigenannahme – Datentransfer:
Zentrale E-Mail-Adresse: *AnzeigendispoPrint@pcwelt.de*. FTP: *www.idgverlag.de/dispocenter*
Digitale Anzeigenannahme – Ansprechpartner:
Andreas Frenzel (-239), E-Mail: *afrenzel@idg.de*
Walter Kainz (-258), E-Mail: *wkainz@idg.de*

Anzeigenpreise:
Es gilt die Anzeigenpreisliste 31 (1.1.2014).

Bankverbindungen: Deutsche Bank AG, Konto 666 22 66, BLZ 700 700 10; Postbank München, Konto 220 977-800, BLZ 700 100 80
Anschrift für Anzeigen: siehe Verlag
Erfüllungsort, Gerichtsstand: München

IGS Anzeigenverkaufsleitung für ausländische Publikationen:
Tina Ölschläger (-116)

Verlagsrepräsentanten für Anzeigen
Europa: Shane Hannam, 29/31 Kingston Road, GB-Staines, Middlesex TW 18 4LH, Tel.: 0044-1-784210210. USA East: Michael Mullaney, 3 Speen Street, Framingham, MA 01701, Tel.: 001-2037 522044. Taiwan: Cian Chu, 5F, 58 Minchuan E Road, Sec. 3, Taipei 104 Taiwan, R.O.C., Tel.: 00886-225036226. Japan: Tomoko Fujikawa, 3-4-5 Hongo Bunkyo-Ku, Tokyo 113-0033, Japan, Tel.: 0081-358004851.

Vertrieb

Leitung Marketing & Vertrieb: Matthias Weber (-154) **Auflagenkoordination:** Michael Lesar (-656)
Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstr. 1, 85716 Unterschleißheim,
Tel. 089/31906-0, Fax 089/31906-113
E-Mail: *info@mzv.de*, Internet: *www.mzv.de*

Produktion: Jutta Eckebrecht (Leitung), Michael Lesar (-656)
Druck: Mayr Miesbach GmbH, Am Windfeld 15, 83714 Miesbach, Tel. 08025/294-267

Verlag

IDG Tech Media GmbH
Lyonel-Feininger-Str. 26, 80807 München
Tel. 089/36086-0, Fax 089/36086-118,
E-Mail: *redaktion@pcwelt.de*, Internet: *www.pcwelt.de*

Geschäftsführer: York von Heimburg
Verlagsleitung: Jonas Triebel

Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Tech Media GmbH ist die **IDG Communications Media AG**, München, die 100%ige Tochter der International Data Group Inc., Boston, USA, ist.

Vorstand:
York von Heimburg, Keith Arnot, David Hill
Aufsichtsratsvorsitzender:
Patrick J. McGovern

ISSN 2193-9225

PC-WELT-LESER-SERVICE

Haben Sie PC-Probleme?
Besuchen Sie einfach unser Forum im Internet unter *www.pcwelt.de/forum,* und schildern Sie dort Ihr Anliegen. Häufig kennen andere PC-WELT-Leser die Lösung für Ihr Problem!

Kontakt zur Redaktion
Wir haben E-Mail-Adressen für Sie eingerichtet, falls Sie uns etwas mitteilen wollen. Allgemeine Leserbriefe und Anregungen zum Heft: *leserbrief@pcwelt.de*, zu pcwelt.de: *online@pcwelt.de*

PC-WELT-Kundenservice: Fragen zu Bestellungen (Abonnement, Einzelhefte), zum bestehenden Abonnement / Premium-Abonnement, Umtausch defekter Datenträger, Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH,
PC-WELT-Kundenservice
Postfach 810580
70522 Stuttgart

Tel: 0711/7252-277
(Mo bis Fr, 8 bis 18 Uhr),
Fax: 0711/7252-377,
Österreich: 01/2195560,
Schweiz: 071/31406-15,
E-Mail: *shop@pcwelt.de*,
Internet: *www.pcwelt.de/shop*

PC-WELT XXL

So nutzen Sie Ubuntu, Mint & Co.

Das komplette Handbuch für Einsteiger & Profis

Jetzt am Kiosk oder online bestellen!

12,90 €

Leseproben, Infos und Bestellmöglichkeit unter:

www.pcwelt.de/linux-xxl

Telefon: 0711/7252277 E-Mail: shop@pcwelt.de

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

PC-WELT MAGAZIN-APP

Eine digitale Ausgabe PC-WELT GRATIS für alle!

Als Print-Abonnent erhalten Sie Ihre Ausgabe in der App **IMMER GRATIS** inklusive DVD-Inhalten zum Download.

Mehr Infos und Download-Links unter:

www.pcwelt.de/magazinapp

„PC-WELT“ ist erhältlich auf:

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg. Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John, Kundenservice Tel.: 0711/7252277, E-Mail: shop@pcwelt.de