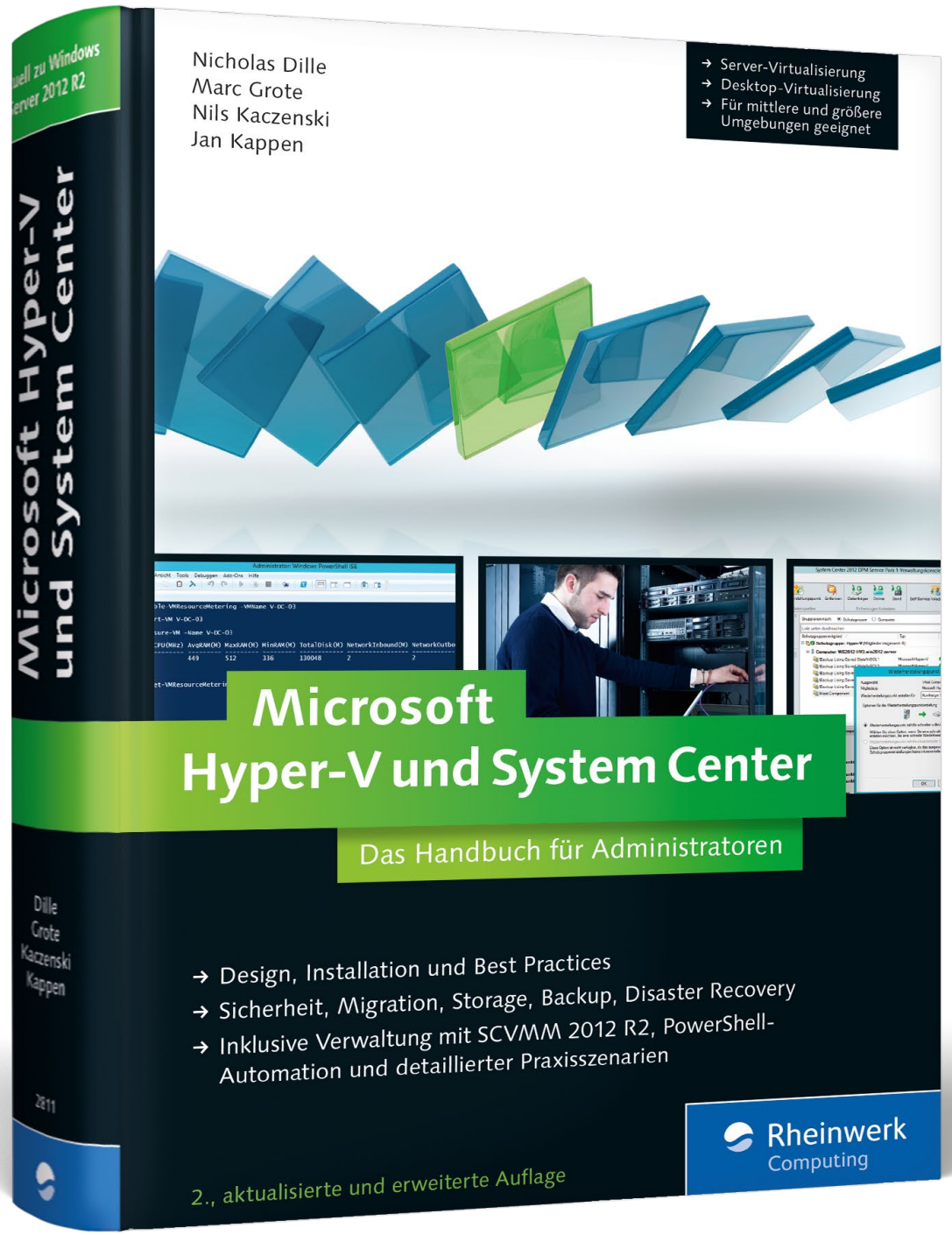


Leseprobe

Umfangreiches Praxiswissen, direkt von bekannten Hyper-V-Experten: Genau das ist es doch, wonach immer alle suchen! Diese Leseprobe bietet Ihnen einen ersten Überblick zu Hyper-V, und Sie erfahren mehr über die Themen Verfügbarkeit, Failover-Clustering und Speicher-Cluster mit Windows Server 2012.

Leseprobe weiterempfehlen

Nicholas Dille, Marc Grote, Nils Kaczenski, Jan Kappen

Microsoft Hyper-V und System Center

967 Seiten, gebunden, 2. Auflage 2014
69,90 Euro, ISBN 978-3-8362-2811-4

www.rheinwerk-verlag.de/3570

Kapitel 2

Hyper-V im Überblick

Studien schätzen, dass mittlerweile mehr als die Hälfte der Windows Server-Systeme nicht mehr auf Hardware, sondern in virtuellen Computern läuft. Ein Grund mehr, sich mit Virtualisierung auseinanderzusetzen. Und wenn schon, denn schon: Dann richtig und zwar mit »Windows Server 2012 Hyper-V«, dem neuen Star am Virtualisierungshimmel. Dieses Kapitel beschäftigt sich mit der grundlegenden Funktionsweise von Hyper-V. Ein Wissen, das Ihnen nicht nur hilft, Hyper-V zu verstehen, sondern auch bessere Virtualisierungslösungen zu bauen.

Carsten Rachfahl, MVP Virtual Machine

Hyper-V lässt sich zwar Windows-typisch recht leicht bedienen und verwalten, doch unter der Haube ist es natürlich ein sehr komplexes Produkt. Es ist hilfreich, die Grundlagen, einige Hintergründe und die Architektur des Hypervisors zu kennen, um besser verstehen zu können, was im Einzelfall geschieht. Besonders beim Entwurf einer Virtualisierungsinfrastruktur und bei der Problemanalyse sind solche Kenntnisse nützlich.

Der Begriff *Hypervisor*, der vielleicht nicht jedem Leser geläufig ist, bezeichnet die Software-Komponente, die auf einem physischen Server läuft und die virtuellen Maschinen steuert, die auf derselben Server-Hardware in Betrieb sind. Es ist Aufgabe des Hypervisors, die Ressourcen der Hardware bedarfsgerecht an die virtuellen Maschinen (VM) zu verteilen. Zu diesen Ressourcen zählen vor allem die Rechenleistung der CPUs, der Arbeitsspeicher, die Speichersysteme (oft pauschalisierend als »Festplatten« bezeichnet, obwohl das in größeren Umgebungen zu ungenau ist) und der Zugriff auf das Netzwerk. Vereinfacht gesagt, sorgt der Hypervisor über eine Zeitplanung dafür, dass er alle VMs abwechselnd versorgt – das *Zeitscheibenprinzip*, das in der IT oft zur Anwendung kommt, ist auch hier relevant. Manchmal wird der Hypervisor auch als *Virtual Machine Monitor* bezeichnet, was dieselbe Kontrollfunktion ausdrückt.

Es gibt eine Reihe von Begriffen und Konzepten, mit denen Server-Virtualisierung beschrieben wird. Im Folgenden beschränken wir uns auf einen Ausschnitt, der aus unserer Sicht für das Verständnis von Hyper-V wichtig ist.

Wichtige Begriffe für Hyper-V

An dieser Stelle geben wir Ihnen einen kurzen Überblick über wichtige Begriffe in Hyper-V, die Sie einordnen können sollten. Sie werden feststellen, dass diese Begriffe im Web, in Artikeln oder Vorträgen nicht immer ganz korrekt verwendet werden. Zu vielen der Begriffe finden Sie im Verlauf dieses Kapitels und auch im ganzen Buch weitere Erläuterungen. Die Reihenfolge der Ausdrücke ist nicht alphabetisch, sondern an inhaltlichen Zusammenhängen orientiert.

- **Host, Host-Server**: Als »Host« oder »Host-Server« bezeichnet man in der Virtualisierung meist den physischen Server, auf dem die Virtualisierungs-Software und eine oder mehrere virtuelle Maschinen laufen. Manchmal wird als »Host« auch die Virtualisierungs-Software selbst, also der Hypervisor, bezeichnet, aber das ist eigentlich nicht richtig.
- **Hypervisor**: die Software-Komponente, die für den Betrieb von virtuellen Maschinen auf einem Host-Server zuständig ist.
- **Hyper-V-Server**: Der Begriff wird uneinheitlich verwendet. Oft ist damit ein Host-Server gemeint, der mit Hyper-V läuft. Selten bezeichnet der Ausdruck eine virtuelle Maschine innerhalb von Hyper-V. Vor allem aber gibt es ein eigenes Produkt namens »Hyper-V Server 2012«, die kostenlose Fassung von Microsofts Virtualisierungs-Software.
- **Parent Partition**: In Hyper-V ist die »Parent Partition« die erste Instanz des Server-Betriebssystems, in der die Steuerung der gesamten Virtualisierung stattfindet.
- **Root Partition**: ein weiterer Ausdruck für die Parent Partition, der aber weniger gebräuchlich ist.
- **Management OS**: ein anderer Ausdruck für die Parent Partition. Manche Autoren trennen auch zwischen der »Parent Partition« als virtueller Instanz und dem »Management OS« als dem Betriebssystem, das in der Parent Partition läuft. In diesem Buch verwenden wir aber beide Begriffe synonym.
- **Host-Betriebssystem**: ein anderer Ausdruck für das Management OS, manchmal auch bezogen auf andere Virtualisierungsprodukte oder als allgemeiner Begriff verwendet.
- **Child Partition**: ein anderer Ausdruck für eine virtuelle Maschine, die als eigene Instanz separat zur Parent Partition auf Hyper-V läuft.
- **Virtuelle Maschine** oder **virtueller Computer**: eine virtuelle Instanz eines Computers, die innerhalb eines Hypervisors läuft.
- **Gast**: Eine virtuelle Maschine wird manchmal als »Gast« oder »Guest« bezeichnet (denn der englische Ausdruck »Host« bedeutet »Gastgeber«).

- **Integrationsdienste**: die Treiber, Dienste und Anpassungen, die innerhalb einer virtuellen Maschine in Hyper-V laufen und für eine optimale Zusammenarbeit des VM-Betriebssystems mit dem Hypervisor sorgen. Manchmal auch als *Integrationskomponenten* bezeichnet, weil Microsoft auf Englisch etwas uneinheitlich mal *Integration Components* und mal *Integration Services* verwendet.
- **Virtueller Server**: Dieser Ausdruck wird leider sehr uneinheitlich verwendet. Manche meinen damit den Host-Server, andere meinen eine virtuelle Maschine. Diesen Begriff sollten Sie vermeiden.
- **VOSE**: ein Ausdruck aus den Microsoft-Lizenzbestimmungen. Inhaltlich bezeichnet *VOSE* eine virtuelle Maschine (*Virtual Operating System Environment*).
- **POSE**: Das Gegenstück aus den Microsoft-Lizenzbestimmungen bezeichnet das Betriebssystem, das direkt auf einem physischen Server installiert ist (*Physical Operating System Environment*).

2.1 Die Architektur

Genau wie die anderen wichtigen Produkte am Markt für Server-Virtualisierung gehört auch Hyper-V der Kategorie der »Typ-1«-Hypervisoren an. Diese Klassifikation finden Sie in den folgenden Abschnitten erläutert. Ebenso stellen wir Ihnen einige weitere Beschreibungskategorien vor, durch die sich Hyper-V teilweise von seinen Mitbewerberprodukten unterscheidet.

2.1.1 Hypervisor Typ 1

Hypervisoren vom *Typ 1* sind eine Software, die direkt auf Basis der Server-Hardware läuft. Sie bauen nicht auf einem allgemeinen Betriebssystem auf, sondern sind als relativ »schmale« Software-Schicht implementiert, die sich auf das Wesentliche konzentriert (siehe auch Abbildung 2.1). Dadurch, dass die gesamte Hardware so der Kontrolle des Hypervisors unterliegt, ist gewissermaßen der gesamte Server für die Virtualisierung reserviert und muss sich um keine anderen Aufgaben kümmern. Auf diese Weise können Typ-1-Hypervisoren sehr effizient die Leistung der Hardware an die virtuellen Maschinen weitergeben.

Beispiele für diese Kategorie sind neben Hyper-V die Produkte VMware vSphere Hypervisor (früher als ESX Server bzw. ESXi bekannt), Citrix XenServer und sein Open-Source-Verwandter Xen sowie zahlreiche andere Vertreter.

Ein anderer Begriff für diese Kategorie ist *Bare-Metal-Hypervisor*, weil die Kontrollinstanz direkt auf der Hardware, also dem »nackten Blech«, installiert ist. Manchmal findet man auch den Ausdruck *nativer Hypervisor*.

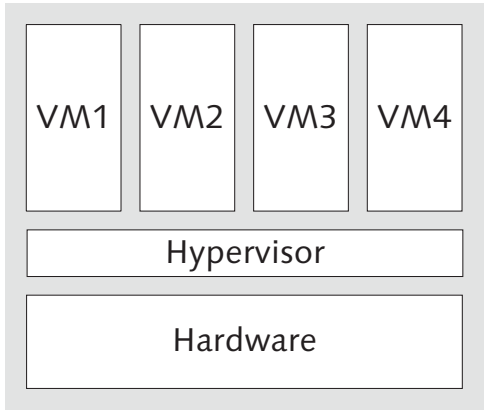


Abbildung 2.1 Architektur eines Hypervisors vom Typ 1: Der Hypervisor ersetzt das Betriebssystem auf der Hardware und kontrolliert alle Vorgänge von Grund auf.

2.1.2 Hypervisor Typ 2

Die *Typ-2*-Hypervisoren sind keine eigenständigen Produkte in dem Sinn, dass man sie direkt auf einem Server installiert. Sie benötigen ein separates Betriebssystem als »Unterlage« und setzen als Applikation oder als Dienst darauf auf. Aus diesem Grund bezeichnet man sie auch als *Hosted Hypervisors*.

Da in diesem Fall das unterliegende Betriebssystem auch andere Zwecke erfüllen kann, ist die Gesamtumgebung weniger stark für den Betrieb der Server-Virtualisierung optimiert. In manchen Situationen ist das durchaus erwünscht, aber es hat den Nachteil, dass die Typ-2-Virtualisierung weniger effizient ist und daher die dort betriebenen virtuellen Maschinen weniger performant sind.

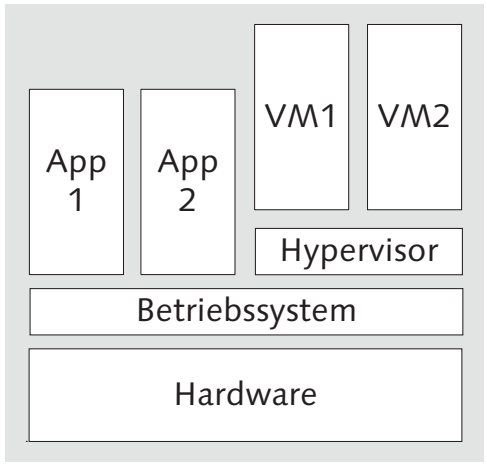


Abbildung 2.2 Architektur eines Hypervisors vom Typ 2: Auf der Hardware läuft ein Allzweck-Betriebssystem, der Hypervisor ist eine von mehreren Anwendungen.

In der Server-Virtualisierung spielen Typ-2-Hypervisoren seit einigen Jahren praktisch keine Rolle mehr. Bekannte Vertreter aus diesem Bereich waren VMware Server (vorher als *GSX Server* vermarktet) und Microsoft Virtual Server.

Recht weit verbreitet sind diese Hypervisoren aber immer noch bei der clientseitigen Virtualisierung, beispielsweise in der Software-Entwicklung oder für Demonstrationszwecke. In solchen Fällen läuft die Virtualisierungs-Software auf einem »allgemeinen« PC parallel zu Standardapplikationen wie etwa Microsoft Office, und der Anwender nutzt virtuelle Maschinen auf seinem Computer eher sporadisch, etwa um Vorgänge auszuprobieren. Wichtige Produkte für diesen Einsatzzweck sind VMware Workstation, Oracle VirtualBox und einige andere. Das Produkt Virtual PC von Microsoft gilt hier als technisch überholt.

In einem Spezialfall hat diese Form der Virtualisierung aber eine etwas größere Verbreitung, nämlich für den Betrieb älterer Software, die mit einem modernen Betriebssystem inkompatibel ist. Ein Beispiel dafür ist der sogenannte »XP Mode« von Windows 7 (siehe Abbildung 2.3), in dem im Hintergrund (auf Basis von Virtual PC) eine VM mit Windows XP werkelt. Windows 8 bietet diese Funktion nicht mehr, bei Bedarf kann man sie über Zusatzprodukte nachbilden. Die integrierte Virtualisierungslösung Hyper-V bietet zwar eine Lösung zur Virtualisierung von weiteren Betriebssystemen, bringt aber keinen »XP Mode« mit.

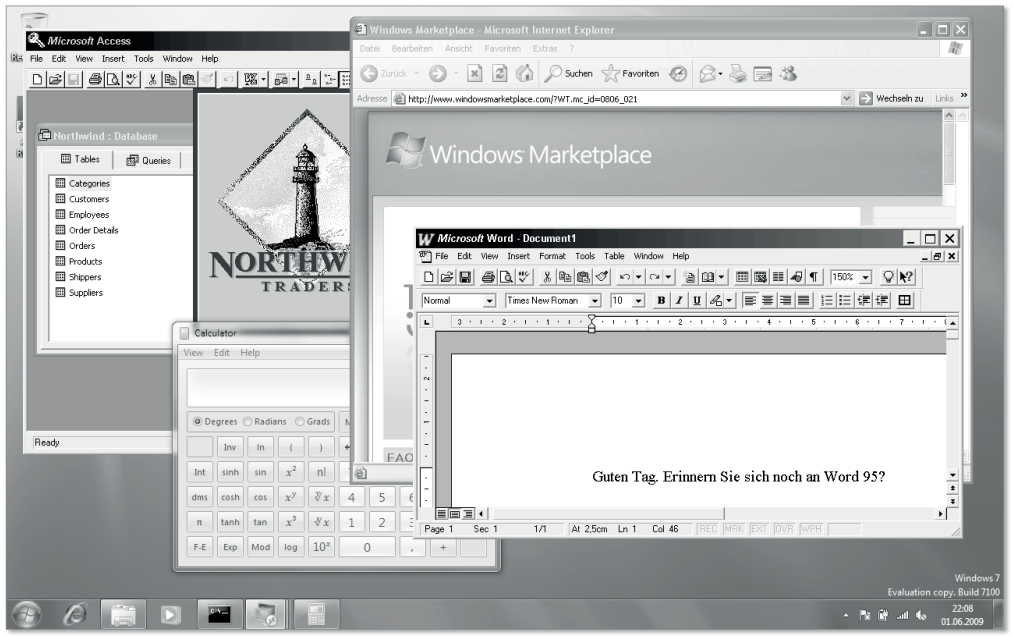


Abbildung 2.3 Der »XP Mode« in Windows 7 beruht auf einem Typ-2-Hypervisor. Er stellt eine VM mit Windows XP bereit, in der ältere Anwendungen als Fenster laufen können. In Windows 8 gibt es den »XP Mode« nicht mehr.

Innerhalb der Typ-1-Hypervisoren hilft noch ein zweiter Ansatz, um die Produkte grundlegend voneinander zu unterscheiden. Hier gibt es vor allem eine technische Trennung zwischen dem langjährigen Marktführer VMware und den beiden anderen wichtigen Produkten Hyper-V und XenServer.

2.1.3 Monolithischer Hypervisor

VMwares vSphere betrachtet man oft als einen *monolithischen Hypervisor*, weil er gewissermaßen »aus einem Block« besteht. Das bedeutet vereinfacht, dass alle hardwarespezifischen Treiber direkt innerhalb der Hypervisor-Schicht implementiert sein müssen, damit der Hypervisor mit einer bestimmten Hardware-Ausstattung zusammenarbeitet.

Ein Vorteil dieser Konstruktion besteht darin, dass der Hypervisor in seinem Kommunikationsaufbau relativ einfach sein kann, weil er alle Treiber und Komponenten direkt kontrolliert und keine aufwendige Infrastruktur zur Steuerung benötigt.

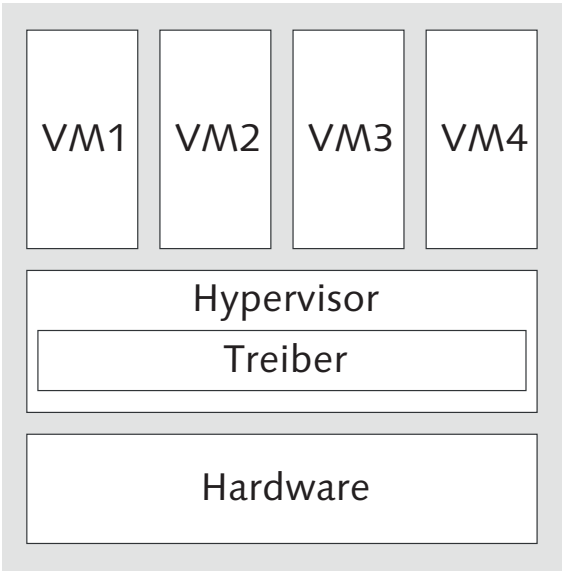


Abbildung 2.4 Im monolithischen Hypervisor sind alle Treiber und Komponenten in den Hypervisor integriert, er bildet also einen zusammenhängenden Block.

Der wesentliche Nachteil besteht darin, dass alle Treiber ausdrücklich für den Hypervisor entwickelt und mit diesem getestet werden müssen. Das hält die Auswahl an Komponenten gering, die direkt mit dem Hypervisor zusammenarbeiten können, weil der Entwicklungsaufwand diese teuer macht. Bei einer neuen Generation an Hardware kann es vorkommen, dass diese erst durch ein Update des Hypervisors genutzt werden kann. Zudem muss der Hersteller der Virtualisierungs-Software aus

eigenem Interesse eine intensive Qualitätsprüfung externer Treiber vornehmen, weil Fehler in dieser Sorte von Software schnell die ganze Infrastruktur in Mitleidenschaft ziehen. Das wäre nicht nur schlecht für die Betreiber, sondern wirft auch ein schlechtes Licht auf den Virtualisierungsanbieter, auch wenn er selbst vielleicht gar nicht die Verantwortung für die fehlerhafte Komponente trägt. In der Praxis ist dies der Hauptgrund für das restriktive Hardware-Zertifizierungsprogramm von VMware.

2.1.4 Microkernel-Hypervisor

Im Gegensatz dazu verstehen sich einige andere Produkte als *Microkernel-Hypervisor*, weil sie die Software-Schicht des eigentlichen Hypervisors bewusst »schmal« halten und die Spezifika der Hardware außerhalb des eigenen Kernels behandeln. Solche Virtualisierer benötigen parallel zum eigentlichen Hypervisor eine separate Instanz, die die Hardware-Treiber enthält und über diese eine Abstraktionsebene in Form einer standardisierten Kommunikationsschnittstelle legt. Der Hypervisor und die virtuellen Maschinen sprechen damit die Treiber (und die Hardware) nicht direkt an, sondern nur über die Schnittstelle.

Vertreter dieser Gattung sind Citrix XenServer und Microsoft Hyper-V. In XenServer heißt die steuernde Instanz *Dom0*, bei Hyper-V bezeichnet man sie als *Parent Partition* oder *Management OS*. Beide sind für den Betrieb der Virtualisierungsplattform unverzichtbar.

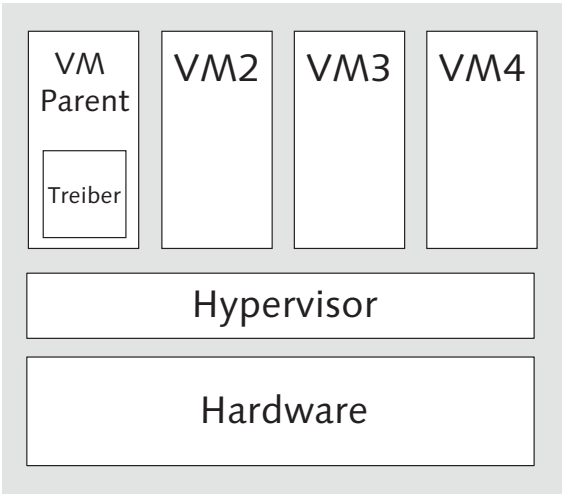


Abbildung 2.5 Der Microkernel-Hypervisor setzt den Hypervisor als sehr »schmale« Komponente um, die keine Treiber und Ergänzungen enthält. Alle hardwarespezifischen Elemente sind Teil einer speziellen virtuellen Maschine.

Der Vorteil, den besonders Hyper-V aus dieser getrennten Konstruktion zieht, liegt in einer hohen Kompatibilität mit Treibern und Komponenten. Da die Parent Partition ein Windows-Betriebssystem ist, können die Hardware-Hersteller auf eine vertraute Umgebung bei der Entwicklung von Treibern zurückgreifen und benötigen keine separaten Prozesse, um für Hyper-V zu entwickeln. Das sorgt für eine sehr breite Basis an einsetzbarer Hardware für die Server-Virtualisierung.

Zusätzlich bietet diese Trennung eine ergänzende Schutzebene. Die Treiber bei den Microkernel-Hypervisoren müssen eine sehr hohe Qualität aufweisen, um das System stabil zu halten. Da aber Windows (bzw. im Fall von XenServer Linux) bereits über sehr ausgereifte Techniken für Fehlerbehandlung, Prozessisolation etc. verfügen, müssen die Entwickler des Hypervisors nicht selbst für den Schutz vor Fehlern oder Angriffen sorgen. Darüber hinaus sorgt ein Zertifizierungsprogramm dafür, dass die zur Verfügung gestellten Treiber ausgiebig getestet werden.

2.2 Paravirtualisierung und Emulation

Eine weitere Unterscheidung von Virtualisierungstechniken bezieht sich auf die Integration von Hardware und Betriebssystemen der virtuellen Maschinen. Die Frage ist dabei, welche Hardware dem Betriebssystem innerhalb der virtuellen Maschine präsentiert wird, wie der Hypervisor damit umgeht und welche Performance dies am Ende der virtuellen Maschine ermöglicht. Hier gibt es eine große Bandbreite an Techniken, die die Virtualisierungshersteller zunehmend parallel einsetzen.

Ein großer Nutzen der Virtualisierung besteht in einer Abstraktion der Hardware: Da die virtuelle Maschine unter Kontrolle eines Hypervisors läuft, das heißt mit der tatsächlichen Hardware keinen direkten Kontakt hat, kann man die Details der Gerätschaften vor ihr verbergen. Dadurch benötigt die VM selbst keine speziellen Treiber – das erhöht die Kompatibilität und sorgt dafür, dass man eine VM auch von einem physischen Server auf einen anderen übertragen kann und sie dort trotzdem ohne Anpassung läuft –, sie »sieht« ja weiterhin nicht die echte, sondern die abstrahierte Hardware.

Wenn man allerdings in jedem Fall einen bestimmten Satz an »klassischer« Hardware emuliert, um ihn den virtuellen Maschinen zu präsentieren, beschneidet man die Leistungsfähigkeit der VMs. Zum einen ist es sehr aufwendig, Geräte zu emulieren, denn der Hypervisor muss dann zwischen den Befehlen übersetzen, die die VM absetzt, und denen, die die echte Hardware wirklich versteht. Zum anderen ist es auf diese Weise nicht möglich, neue Funktionen oder Leistungsmerkmale zur Verfügung zu stellen.

Aus diesem Grund nutzen heutige Virtualisierer das Prinzip der Emulation nur möglichst selten. Oft greifen sie auf das Prinzip der »Paravirtualisierung« zurück: Zwischen der realen Hardware des Host-Servers und der virtuellen Hardware der VM gibt es eine weitere Schicht, die zwischen beiden vermittelt. Damit dies möglichst effizient geschieht, muss das Betriebssystem innerhalb der VM von dieser Schicht wissen, man muss es daher anpassen. Bei den meisten kommerziellen Produkten geschieht dies, indem man einen Satz spezieller Treiber innerhalb der VM installiert.

Tatsächlich vermeiden die meisten Hersteller den Ausdruck »Paravirtualisierung«, denn klassisch versteht man darunter eher eine Anpassung der Betriebssysteme auf der Code-Ebene. Da kommerzielle Betriebssystem-Hersteller eine derartige Anpassung aber kaum erlauben würden, soll die genutzte Technik auch gar nicht erst so klingen, als täten sie dies.

Während XenServer und Hyper-V von Anfang an primär auf das Prinzip der Paravirtualisierung setzten, hat VMware lange Zeit nur den Emulationsweg beschritten und Paravirtualisierung erst recht spät eingeführt (mit Version ESX 3.5 Update 1). Man erkennt den Ansatz der Paravirtualisierung oft einfach daran, dass für den leistungsfähigen und effizienten Betrieb einer VM spezielle Treiber nötig sind, die keine herkömmliche Hardware ansprechen. Bei aktuellen VMware-Systemen sind das beispielsweise die *VMNet-Netzwerkkarten* sowie die VMI-Schnittstelle, in Hyper-V die *Integration Services* und in XenServer die *Enlightenments*.

Keines der genannten Produkte setzt aber ausschließlich auf einen technischen Weg, sondern alle Hersteller setzen Techniken verschiedener Art und Herkunft (Emulation, Paravirtualisierung, Hardware-Virtualisierung) nebeneinander ein, um für verschiedene Situationen passende Lösungen bieten zu können.

2.3 Hardware-Virtualisierung

In ernst zu nehmender Größenordnung hielt die Server-Virtualisierung Einzug in die Welt der Client-Server-Umgebungen, als VMware sein Produkt ESX Server am Markt etablierte. Dessen Version 2, eingeführt im Sommer 2003, verfügte bereits über einige Merkmale, die heutige virtuelle Infrastrukturen auszeichnen: Mechanismen für Clustering und Hochverfügbarkeit, SAN-Integration und vor allem eine Live-Migration-Technik namens vMotion, mit der man laufende virtuelle Maschinen von einem physischen Host-Server auf einen anderen verschieben konnte, ohne sie anzuhalten oder die Benutzerverbindungen zu unterbrechen.

In der gesamten Frühzeit der Server-Virtualisierung (bezogen auf die Client-Server-Welt mit Intel-basierten Rechnern) beruhte die Technik nur auf Software. Zwar gab es in anderen Rechnerarchitekturen, beispielsweise der IBM-Großrechner-Welt, teils schon jahrzehntelang Hardware, die sich unterhalb der Software-Ebene in mehrere

logische Systeme (dort meist *Partitionen* genannt) aufteilen ließ. Doch es dauerte bis zum Jahreswechsel 2005/2006, als Intel und sein Mitbewerber AMD die ersten Prozessoren auf den Markt brachten, die auf der Hardware-Ebene Unterstützung für Virtualisierung enthielten.

Durch diese erweiterten Prozessorfunktionen, am Markt bekannt als *Intel-VT* und *AMD-V*, lassen sich Hypervisoren wesentlich effizienter und sicherer betreiben als auf Basis der vorherigen CPUs. Durch einen neuartigen Aufbau sind die Prozessoren in der Lage, Befehle aus den virtuellen Maschinen auch dann direkt umzusetzen, wenn sie den *Protected Mode* der CPU voraussetzen. Dadurch ist es für den Hypervisor unnötig, diese Befehle abzufangen und zur Ausführung zu übersetzen (manchmal als *Maskieren* bezeichnet). Dies entlastet die CPU, weil sie für denselben Vorgang weniger Arbeit aufwenden muss.

Hyper-V setzt diese Prozessorfunktionen zwingend voraus, denn die Software ist von vornherein für diese CPU-Integration entwickelt worden. Andere Virtualisierungsprodukte profitieren ebenfalls von den Funktionen, können in anderen Betriebsmodi aber auch mit einfachen Prozessoren arbeiten. Zwar mag dies wie ein konzeptioneller Nachteil von Hyper-V erscheinen, doch sind alle Server, die in der Praxis für Virtualisierung infrage kommen, ohnehin seit vielen Jahren mit den nötigen Funktionen ausgestattet.

Sowohl AMD-V als auch Intel-VT bedienen sich eines speziellen architektonischen Kniffs, um die Kontrolle der CPU über die Virtualisierung zu ermöglichen. Schon im Grundprinzip der x86-Prozessorarchitektur gibt es in der CPU mehrere sogenannte »Ringe«, über die ein Betriebssystem Berechtigungen umsetzen kann. Jeder Ring stellt eine Berechtigungsstufe dar, in der bestimmte CPU-Befehle möglich sind. Ein Betriebssystem kann diese Ringe nutzen, um Prozesse voneinander zu trennen und vorzugeben, welche Aktivitäten ein Prozess ausführen kann und welche nicht.

Die x86-Architektur kennt die Ringe 0, 1, 2 und 3, doch alle relevanten Betriebssysteme nutzen nur den Ring 0 (sogenannter »Kernel Mode«) und den Ring 3 (sogenannter »User Mode«). Prozesse des User Modes dürfen keine Funktionen des Rings 0 nutzen.

Die Virtualisierungsprozessoren haben nun einen neuen Ring –1 eingeführt, der sozusagen »unterhalb« des Rings 0 liegt. Auf diesem Ring –1 arbeitet der Hypervisor und behält so die Kontrolle über alle höheren Ringe. Durch diesen Trick können die virtuellen Betriebssysteme ohne weitere Anpassung den Ring 0 für Kernel-Operationen nutzen. Der Hypervisor ist in der Lage, von seinem hoch privilegierten Ring –1 aus mehrere Betriebssystem-Kernel im Ring 0 zu verwalten.

Mehr zu dem Konzept der CPU-Ringe lesen Sie in einem knappen, aber guten Wikipedia-Artikel unter *http://de.wikipedia.org/wiki/Ring_(CPU)* (Kurzlink: *http://qccq.de/s/h201*).

Mit Windows Server 2012 unterstützt Hyper-V optional eine weitere Technik der Hardware-Virtualisierung, nämlich *Single-Root I/O Virtualization* (SR-IOV), eine Funktion neuartiger Netzwerkkarten. Diese Technik ähnelt weit mehr dem Vorbild der partitionierbaren Hardware aus der Großrechnerwelt als die CPU-Virtualisierungsfunktionen, denn sie bildet tatsächlich auf der Hardware-Ebene mehrere logische Geräte, die sich aus Sicht der darüber laufenden Software wie mehrere getrennte Einheiten darstellen. Der technische Nutzen besteht in einer weit effizienteren Abwicklung des Netzwerkverkehrs.

2.4 Der VMBus und die Integration Services

Wie in Abschnitt 2.2, »Paravirtualisierung und Emulation«, dargestellt, ist für die Technik der Paravirtualisierung eine Kommunikationsschicht nötig, über die das Betriebssystem einer virtuellen Maschine auf die Hardware zugreifen kann. Im Fall von Hyper-V nennt man diese Komponente *VMBus*.

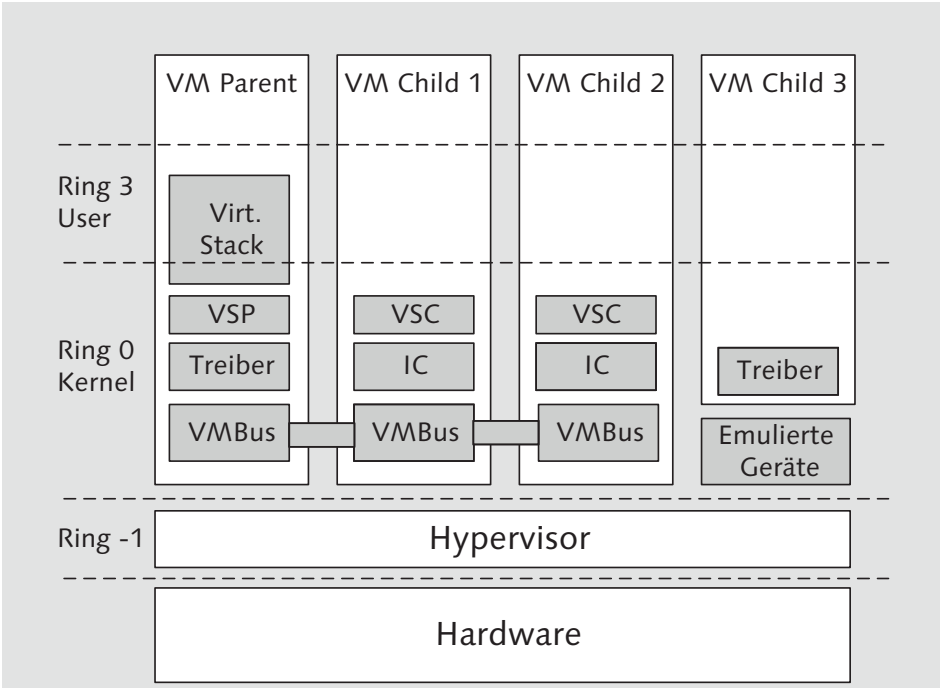


Abbildung 2.6 Das Hyper-V-Architekturschema. Für Hyper-V optimierte VM-Betriebssysteme nutzen den VMBus und die Integrationsdienste (Integration Components, IC) zur Kommunikation.

Vereinfacht können Sie sich diese vorstellen wie einen virtualisierten Hardware-Bus, wie ihn etwa der PCI-Bus darstellt. Das virtuelle Betriebssystem kann über seinen Treiber-Stack seine Zugriffe auf die Hardware auf diesen Bus legen und erhält von dort die jeweiligen Daten bzw. Funktionen zurück. Den tatsächlichen Aufbau des VMBus kontrolliert die Parent Partition, denn nur dort sind die hardwarespezifischen Treiber für die tatsächlich vorhandenen Geräte installiert. Abbildung 2.6 stellt diesen Aufbau dar.

Um auf den VMBus zugreifen zu können, bedarf es aber einiger Anpassungen im Gast-Betriebssystem. Dazu dienen die *Integrationsdienste* (Integration Services, manchmal auch Integration Components), die Sie sich wie einen Satz von Treibern und Werkzeugen vorstellen können, die im Betriebssystem der virtuellen Maschine laufen. In XenServer sind diese Dienste als *Enlightenments* bekannt, bei VMware als *VMware Tools*. In Abbildung 2.6 verfügen die »VM Child 1« und »VM Child 2« über diese Dienste.

Neben dem reinen Hardware-Zugriff steuern diese Dienste auch noch einige weitere Funktionen der Virtualisierung. Dazu zählen einfachere Vorgänge wie der Zeitabgleich der virtuellen Maschine mit dem Host-Server oder auch komplexere wie der »Heartbeat« zur Überwachung der VM oder die Kommunikation mit dem Host-Server über die Verwendung des Arbeitsspeichers im Fall von *Dynamic Memory*. Details zu den Integrationsdiensten lesen Sie in Abschnitt 5.2.10, »Integrationsdienste«.

Sofern die virtuellen Maschinen auf Ihrem Host-Server dasselbe Windows-Betriebssystem ausführen wie der Host selbst, enthalten sie bereits die passenden Integrationsdienste. Ältere Windows-Versionen innerhalb einer VM sollten Sie auf den jeweils neuesten Stand der Integrationsdienste bringen, um Stabilität, Leistung und Funktionsumfang zu gewährleisten. Für einzelne virtuelle Maschinen können Sie die Installation über die Remote-Verbindungskonsole des Hyper-V-Managers über den Menüpunkt Aktion • Installationsdatenträger für Integrationsdienste einlegen vornehmen (siehe auch Abbildung 2.7). Müssen Sie eine größere Anzahl von virtuellen Maschinen versorgen, ist die Automatisierung per PowerShell, dem Virtual Machine Manager oder einem anderen Werkzeug sinnvoll. Auch hierzu finden Sie mehr in Kapitel 5, »Virtuelle Maschinen«.

Die Integrationsdienste gibt es auch für andere Betriebssysteme, vor allem für Linux. Einige Distributionen haben eine Version der Komponenten bereits in ihrem Lieferumfang, für andere können Sie diese selbst einbinden. Da die Entwicklung schnell voranschreitet, sollten Sie bei der Installation und später regelmäßig prüfen, welche Version für welche Distribution verfügbar und unterstützt ist.

Abbildung 2.7 Die Integrationsdienste lassen sich über die Verbindungskonsole im Hyper-V-Manager installieren oder aktualisieren.

Sofern in einer VM unter Hyper-V ein Betriebssystem läuft, in dem die Integrationsdienste nicht vorhanden sind, stellt Hyper-V emulierte Geräte zur Verfügung. Das Prinzip finden Sie in Abbildung 2.6 in der »VM Child 3« dargestellt. Diese emulierten Geräte sind weit weniger leistungsfähig als ihre »paravirtuellen« Pendants. Besonders beim Netzwerkverkehr lässt sich dies oft beobachten: Ein virtueller Server, der unter Hyper-V mit einer »älteren Netzwerkkarte« (»Legacy Network Adapter«) ausgestattet ist – so lautet hier die Bezeichnung für eine emulierte, nicht paravirtualisierte Karte –, zeigt oft Ping-Rundlaufzeiten im Bereich von Sekunden statt der üblichen Millisekunden (in einem Fall haben wir mehr als 30 Sekunden beobachten können). Installiert man die Integrationsdienste und stattet die VM mit einer synthetischen Netzwerkkarte aus, ändert sich die Netzwerkperformance üblicherweise schlagartig auf die erwarteten Werte.

2.5 Die Parent Partition

Die *Parent Partition* spielt in der Virtualisierung mit Hyper-V eine besondere Rolle. Manchmal bezeichnet man diese Instanz auch vereinfachend als »den Host«, wobei das nicht ganz richtig ist – der »Host« wäre eher der ganze Hardware-Server mitsamt dem Hypervisor und der Parent Partition. Auch der Ausdruck *Management-Betriebssystem* oder kurz *Management OS* ist verbreitet, aber auch dies trifft die Funktion der Parent Partition nicht ganz. Trotzdem verwenden wir diesen Ausdruck an einigen Stellen in diesem Buch, da dies der von Microsoft genutzte Name ist.

Wie in Abschnitt 2.1.4, »Microkernel-Hypervisor«, erwähnt, dient diese spezielle Instanz dazu, den Hardware-Zugriff aller virtuellen Maschinen zu steuern und die

Gerätetreiber für die tatsächliche Hardware bereitzuhalten. Der Ausdruck *Partition* für diese Instanz ist dabei in der Server-Virtualisierung eher unüblich und leitet sich aus der traditionellen Virtualisierungswelt der Großrechner her.

Streng genommen, kann man die Parent Partition auch als erste virtuelle Maschine des Hyper-V-Hosts bezeichnen. Diese »Eltern-VM« kommt dabei auf eine spezielle Weise zustande, von der Sie sich nicht auf eine falsche Fährte führen lassen sollten. Um die Vorgänge zu erläutern, schauen wir uns den Installationsprozess eines Hyper-V-Hosts genauer an.

Zunächst installieren Sie Windows Server 2012 »ganz normal« auf dem Server. Während der Installation stellen Sie die nötigen Treiber zur Verfügung, spielen die aktuellen Updates ein und führen die Grundkonfiguration durch. Erst wenn Sie dies abgeschlossen haben, richten Sie die Server-Rolle »Hyper-V« über den Server-Manager ein. Das erfordert wenige Angaben und zwei Neustarts, und danach sieht Ihr Server aus wie vorher – ein ganz normaler Windows Server.

Tatsächlich ist nun aber Gravierendes geschehen: Der Hypervisor ist gewissermaßen nachträglich unter das bereits laufende Windows geschoben worden und hat die Kontrolle über das gesamte System übernommen. Dadurch ist der eben erst auf der Hardware installierte Windows Server zur ersten virtuellen Maschine geworden, die »nur noch« der Steuerung des Hypervisors dient und ihm einige wichtige Funktionen bereitstellt.

Lasst die Eltern in Ruhe!

Die Sonderfunktionen der Parent Partition sind der Grund, warum Sie innerhalb der Parent Partition auf keinen Fall weitere Dienste einrichten sollten. In der Projektpraxis diskutieren wir immer wieder mit Kunden, die »den Host« noch besser ausnutzen möchten und daher direkt in der Parent Partition zusätzlich Dienste wie Active Directory, Dateidienste oder gar Applikationen wie SQL Server installieren möchten. Das ist aber überhaupt keine gute Idee.

Halten Sie sich vor Augen: Die Parent Partition ist an jedem Ein- und Ausgabevorgang beteiligt, zu dem irgendeine virtuelle Maschine auf die Hardware zugreifen muss. Denn nur in der Parent Partition laufen die dazu nötigen Treiber. Das bedeutet aber, dass »der Parent« auch die nötigen Ressourcen braucht, um seine wichtige Aufgabe zu erfüllen.

Jeder Dienst, den die Parent Partition daneben noch ausführt, belegt dieselben Ressourcen und schränkt damit alle laufenden VMs ein. Würden Sie einen Dateiserver, einen SQL Server oder eine andere Applikation direkt innerhalb des »Parents« laufen lassen, kann dieser durchaus unter Last stehen, und dann hat die Parent Partition einfach keine Ressourcen mehr für ihre eigentliche Funktion frei, nämlich die Unterstützung der virtuellen Maschinen.

Die Empfehlung lautet daher: Installieren Sie alle produktiven Funktionen nur innerhalb von virtuellen Maschinen, denn dafür sind diese da. Richten Sie keine produktiven Dienste in der Parent Partition ein, sondern beschränken Sie diese auf das, was für die Virtualisierung wirklich nötig ist. Dies kommt Ihnen auch bei der Sicherung und Wiederherstellung des Hosts zugute.

In der Parent Partition legen Sie einige zentrale Konfigurationsparameter für Hyper-V fest, die wir in Kapitel 3, »Den Host-Server einrichten«, genauer vorstellen. Ebenso finden Sie hier die Einstellungen für »den Host« selbst, also etwa das Teaming für die physischen Netzwerkkarten oder die Anbindung des Festplattenspeichers, der die virtuellen Festplatten für die VMs bereitstellt.

Ein Umstand führt allerdings immer wieder zu Missverständnissen: Die meisten Betriebssystem-Einstellungen der Parent Partition beziehen sich nur auf diese eine »virtuelle Maschine« und haben mit den anderen VMs, die der Server hostet, nichts zu tun. Legen Sie etwa in der Parent Partition eine IP-Adresse für eine Netzwerkverbindung fest, gilt diese ausschließlich für die Netzwerkkommunikation der Parent Partition – die IP-Konfigurationen der VMs auf demselben Host sind davon völlig getrennt, auch wenn sie durch die Virtualisierung vielleicht über dieselbe physische Karte laufen.

2.6 Der Virtualisierungs-Stack

Innerhalb der Parent Partition läuft der sogenannte *Virtualization Stack*. Das ist ein Satz von Komponenten, Diensten und Treibern, die die virtuelle Infrastruktur auf dem Host-Server bereitstellen und steuern. Erst durch diesen Aufbau wird die Parent Partition zur Management-Instanz, denn hier finden sich die nötigen Schnittstellen und Funktionen, um virtuelle Maschinen zu erzeugen, zu konfigurieren und zu betreiben.

Sie haben bereits gelesen, dass die Parent Partition alle Hardware-Zugriffe der virtuellen Maschinen kontrolliert. Das gilt mit zwei Ausnahmen: Die Zuweisung von CPU-Ressourcen – also »Rechenzeit« – und Arbeitsspeicher ist Kernaufgabe des Hypervisors. Das bedeutet, dass auch der Parent Partition ihre CPU-Leistung und ihr Arbeitsspeicher vom Hypervisor zugewiesen wird und sie nicht selbst darüber bestimmt. Dies ist ein wichtiger Faktor, den Sie beim Sizing der Umgebung beachten sollten – mehr darüber lesen Sie in Abschnitt 3.1.5, »Die Host-Reserven«.

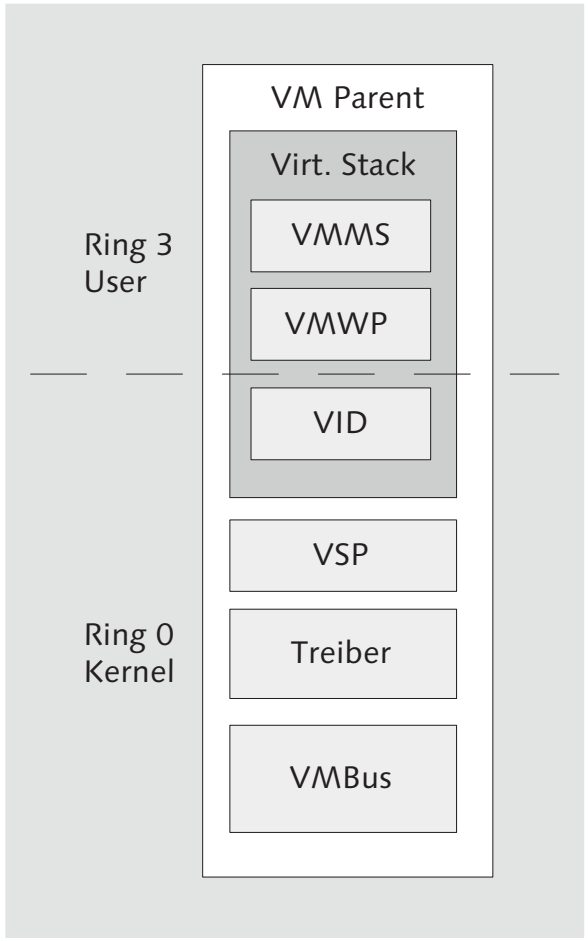


Abbildung 2.8 Der Virtualization Stack stellt innerhalb der Parent Partition einige wichtige Funktionen für den Betrieb virtueller Maschinen bereit.

2.6.1 Virtual Machine Management Service

Der *Virtual Machine Management Service* (VMMS) ist verantwortlich für den Zustand jeder einzelnen virtuellen Maschine auf dem betreffenden Host-Server. Dabei gibt er einige Aufgaben an den *Virtual Machine Worker Process* (VMWP) ab, den Sie im folgenden Abschnitt kennenlernen.

Folgende Zustände einer VM kontrolliert der *VMMS*:

- Starten
- Wird ausgeführt (Aktiv)
- Aus (Nicht aktiv)
- Snapshot wird erstellt

- Snapshot wird angewendet
- Snapshot löschen
- Zusammenführung wird ausgeführt (Snapshot zusammenführen)

Die Aktionen Anhalten, Pausieren und Abschalten hingegen steuert der jeweilige *VMWP*.

Der VMMS bietet Automatisierungsschnittstellen für *WMI*, die *PowerShell* oder COM-Programme wie *VBScript*. Außerdem lässt er sich natürlich über die grafische Oberfläche der Parent Partition ansprechen. Ebenso bietet er die Grundlage für die Verwaltung mit übergeordneter Software wie etwa dem *System Center Virtual Machine Manager*.

2.6.2 Virtual Machine Worker Process

Sobald der *Virtual Machine Management Service* eine konkrete virtuelle Maschine startet, erzeugt er für diese einen separaten Prozess, den man als *Virtual Machine Worker Process* (VMWP) bezeichnet. Dieser Prozess läuft im Kontext des eingebauten Systemkontos *Netzwerkdienst*, das heißt mit reduzierten Berechtigungen. Dadurch, dass jede VM einen separaten *VMWP* hat, ist eine hohe Isolation der virtuellen Maschinen gewährleistet.

Neben den Basisoperationen für den Betrieb der virtuellen Maschine stellt der *VMWP* auch das virtuelle Motherboard bereit, in dem Funktionen wie das BIOS, der Zugriff auf den Arbeitsspeicher und einige andere systemnahe Elemente implementiert sind, die nicht über den *Virtual Machine Bus* laufen.

Eine VM gewaltsam beenden

Sehr selten kann es vorkommen, dass eine virtuelle Maschine unter Hyper-V nicht mehr auf Steuerungsanforderungen reagiert. Als Administrator haben Sie in einer solchen Situation keine Möglichkeit mehr, auf das Gast-Betriebssystem zuzugreifen. Ebenso gelingt es Ihnen dann nicht, die VM über die Steuerungsfunktionen der Parent Partition zu beeinflussen, um sie etwa zu beenden.

In solchen Situationen ist manchmal das »gewaltsame« Beenden der letzte Ausweg. Dazu erzwingen Sie das Abschalten des zugehörigen VM Worker-Prozesses. Vorsicht aber: Das Verfahren ist nicht offiziell unterstützt.

So können Sie vorgehen:

1. Identifizieren Sie den *GUID* (Globally Unique Identifier) der virtuellen Maschine, indem Sie im Dateisystem der Parent Partition den Ordner öffnen, in dem die Konfiguration der VM gespeichert ist. Notieren Sie sich den (etwas kryptischen) Namen der *XML*-Datei – die ersten fünf bis zehn Zeichen reichen normalerweise aus.

2. Rufen Sie in der Parent Partition den Task-Manager auf, und öffnen Sie dort die Registerkarte Prozesse.
3. Klicken Sie mit der rechten Maustaste in die Überschriftenzeile, und aktivieren Sie das Häkchen neben Befehlszeile.
4. Nun sehen Sie zu jedem Prozess die genaue Befehlszeile, mit der er gestartet wurde. Sortieren Sie die Ansicht nach Name, und scrollen Sie zu den Einträgen namens *vmwp.exe*.
5. Identifizieren Sie den zugehörigen VMWP-Prozess über den GUID, der in der Befehlszeile steht – er muss dem *XML*-Dateinamen entsprechen, den Sie im ersten Schritt notiert haben.
6. Diesen Prozess können Sie per Rechtsklick beenden. Vorsicht: Die virtuelle Maschine wird hart abgeschaltet, als wäre bei einem echten Server der Strom ausgefallen!
7. Sollte Ihr Host-Server Teil eines Failover-Clusters sein, wird dieser die virtuelle Maschine sofort neu starten. Meist sollte sie dann aber auch wieder ordnungsgemäß arbeiten.

2.6.3 Virtual Devices

Die *virtuellen Geräte* oder *Virtual Devices* (VDev) stellen den virtuellen Gast-Systemen den Zugriff auf »Hardware« bereit, die aber in Form von Software-Modulen implementiert ist. Die VDevs befinden sich je nach ihrem Typ an verschiedenen Stellen im Virtualisierungs-Stack.

Hyper-V unterscheidet folgende Gerätetypen:

- **Core VDevs** stehen allen virtuellen Maschinen zur Verfügung, weil die Systemarchitekturen, die sich mit Hyper-V virtualisieren lassen, diese voraussetzen. Hierbei gibt es zwei Untertypen:
  - **Emulierte Geräte**: Dieser Typ bildet das Verhalten eines konkreten Gerätemodells nach, sodass vorhandene Treiber in einem Gast-Betriebssystem ordnungsgemäß arbeiten. Es ist dabei nicht nötig, dass das zugehörige Gerät auch tatsächlich im Host-Server vorhanden ist. Die meisten Core VDevs gehören diesem Typ an, dazu zählen unter anderem das *BIOS*, der *ISA*- und der *PCI-Bus*, die Tastaturschnittstelle und viele andere. Auch die *ältere Netzwerkkarte* (Legacy Network Adapter), die Sie optional in eine virtuelle Maschine einbinden können, gehört dazu.
  - **Synthetische Geräte**: Dieser Typ stellt kein konkretes Gerät bereit, sondern eher eine Geräteklasse. Tatsächlich handelt es sich hier um *paravirtualisierte* Geräte (siehe dazu Abschnitt 2.2, »Paravirtualisierung und Emulation«), das

heißt einen Durchgriff auf die echte Hardware im Host-Server. Da diese Technik den *Virtual Machine Bus* (VMBus) nutzt, steht sie nur Gast-Betriebssystemen zur Verfügung, in denen die Integrationsdienste installiert sind (siehe dazu Abschnitt 2.4, »Der VMBus und die Integration Services«). Typischerweise ist die Performance synthetischer Geräte höher als die von emulierten Geräten.

- **Plug-in VDevs**: Diese VDevs bilden ebenfalls keine konkreten Geräte nach und sind größtenteils nicht einmal »Geräte« im vertrauten Sinn. Sie bilden eine Schnittstelle für verschiedene Virtualisierungsdienste und ermöglichen die Kommunikation über den VMBus.

2.6.4 Virtualization Service Providers und Virtualization Service Clients

Die *Virtualization Service Providers* (VSP) und die *Virtualization Service Clients* (VSC) gehören zusammen und bilden gewissermaßen die Endpunkte im Virtual Machine Bus (VMBus). Ein VSP ist eine Server-Schnittstelle in der Parent Partition, die bestimmte Gerätefunktionen zur Verfügung stellt. Ein VSC läuft in dem Gast-Betriebssystem einer VM und kann über den VMBus auf einen VSP zugreifen.

Hinter *VSPs* und *VSCs* verbergen sich die paravirtualisierten Geräte, die Sie auch schon als *synthetische* Geräte kennengelernt haben. Da der Zugriff auf solche virtuellen Hardware-Komponenten meist wesentlich schneller vonstattengeht als die Nutzung eines emulierten Geräts, stellt der Aufbau aus VSP, VMBus und VSC das zentrale Leistungselement eines Hyper-V-Systems dar.

2.7 Child Partitions

Als *Child Partitions* bezeichnet man in Hyper-V die virtuellen Maschinen. Sie stehen im Gegensatz zur Parent Partition, die eine privilegierte Stellung im System innehat und als einzige die Konfiguration des Host-Servers sowie den Zugriff auf die Hardware steuert (siehe Abschnitt 2.5, »Die Parent Partition«). Da die Child Partitions keine Verwaltungsaufgabe für das Virtualisierungssystem übernehmen, sind sie für die produktiven Zwecke eines Unternehmens gedacht.

Die Child Partitions lassen sich in zwei Klassen unterscheiden, je nachdem, ob sie für Hyper-V angepasst sind oder nicht.

2.7.1 An Hyper-V angepasste Gast-Systeme

Wenn in einem Betriebssystem, das in einer virtuellen Maschine unter Hyper-V läuft, die Integrationsdienste (Integration Services) installiert sind (siehe Abschnitt 2.4, »Der VMBus und die Integration Services«), ist es an die Besonderheiten von

Hyper-V angepasst. Man spricht hier auch von *Hyper-V-Aware*, denn das VM-Betriebssystem »weiß« gewissermaßen, dass es innerhalb von Hyper-V läuft. Die Integration Services stellen die nötigen Funktionen, Anpassungen und Treiber bereit, damit die virtuelle Maschine optimal mit Hyper-V zusammenarbeitet. Vor allem sind dies die Komponenten, die Sie in Abschnitt 2.6, »Der Virtualisierungs-Stack«, kennengelernt haben.

Für Windows-Betriebssysteme ab Windows Server 2003 SP2 bzw. ab Windows XP SP3 sind die Integrationsdienste in Hyper-V enthalten. Sie können diese über die Hyper-V-Verwaltungswerkzeuge in einer VM installieren (siehe dazu Abschnitt 5.2.10, »Integrationsdienste«). Seit Windows Server 2008 und Windows Vista ist die jeweils aktuelle Fassung der Integrationsdienste sogar schon im Betriebssystem enthalten. Wenn Sie in einer VM dasselbe Betriebssystem ausführen wie auf dem Host-Server (etwa Windows Server 2012), sind die Integrationsdienste auf dem aktuellen Stand und müssen nicht nachträglich installiert werden. Führt der Host-Server hingegen eine neuere Windows-Version aus als die VM, sollten Sie deren Integrationsdienste aktualisieren. Wie das funktioniert, beschreiben wir ebenfalls in Kapitel 5, »Virtuelle Maschinen«.

Integrationsdienste für einige Nicht-Windows-Systeme finden Sie nur im Einzelfall. Microsoft selbst entwickelt aktiv die betreffenden Komponenten für Linux, sodass die Integration Services in vielen Linux-Distributionen bereits enthalten sind. Die jeweils aktuelle Fassung finden Sie über den Download-Bereich der Microsoft-Webseite.

2.7.2 Nicht an Hyper-V angepasste Gast-Systeme

Die Anpassung des Gast-Betriebssystems an Hyper-V ist keine zwingende Voraussetzung. Technisch können Sie problemlos etwa Windows 2000 oder gar Windows NT 4.0 in einer virtuellen Maschine unter Hyper-V betreiben. Für diese und andere Betriebssysteme gibt es keine Integrationsdienste, sodass dort nur *emulierte* Geräte bereitstehen (siehe dazu Abschnitt 2.6.3, »Virtual Devices«). Diese Geräte sind teilweise weit weniger leistungsfähig als die *synthetischen* Geräte, wie sie die Integrationsdienste zur Verfügung stellen. Dadurch müssen Sie beim Betrieb derartiger virtueller Maschinen oft deutliche Einschränkungen in der Leistungsfähigkeit hinnehmen.

2.7.3 Neuerungen unter Windows Server 2012 R2

Seit Hyper-V unter Windows Server 2012 R2 gibt es zwei Generationen von VMs. Die bisher einfach als »virtueller Computer« bekannte VM ist nun eine VM der Generation 1, hinzugekommen ist die VM der Generation 2. Diese Art von virtuellem

Computer kommt komplett ohne Emulation aus und ist ausschließlich unter Windows Server 2012 R2 nutzbar. Statt eines BIOS wird eine UEFI Firmware genutzt, dies ermöglicht unter anderem die Nutzung von Secure Boot, dem Booten von Festplatte und DVD-Laufwerk über den SCSI-Controller und die Nutzung eines PXE-Boots über die Netzwerkkarte. Die Anzahl der »Hardware«-Komponenten einer VM der Generation 2 ist deutlich geringer als die der Hardware einer VM der Generation 1. Es fehlen z. B. der IDE-Controller sowie die ältere Netzwerkkarte.

2.8 Best Practices Analyzer

Seit Windows Server 2008 R2 enthalten die Windows Server-Betriebssysteme eine Funktion namens *Best Practices Analyzer* oder kurz *BPA*. Dabei handelt es sich um eine ganze Infrastruktur, die Administratoren dabei unterstützen soll, die Konfiguration ihres Servers nach Empfehlungen von Microsoft einzurichten.

Den Kern des BPA-Systems bildet das Produktwissen aus dem technischen Support des Herstellers. Dort haben sich in teilweise jahrelanger Support-Praxis Empfehlungen angesammelt, die insbesondere für größere und anspruchsvolle sowie eigene Implementierungen der Microsoft-Produkte gelten. Viele dieser Hinweise lassen sich durchaus als Regeln formulieren und automatisiert auf eine real vorhandene Infrastruktur anwenden. Genau dies tun die Best Practices Analyzers: Sie sammeln Informationen über die Konfiguration einer bestimmten Server-Applikation und ihrer Umgebung und überprüfen diese anhand vorab festgelegter Regeln.

Den ersten BPA gab es bereits vor etwa zehn Jahren für Microsofts Exchange Server. Zunächst war das Analysewerkzeug als separates, kostenloses Produkt erhältlich. Die Entwicklung war in enger Zusammenarbeit zwischen Microsofts technischem Support, der Entwickler-Produktgruppe und der Microsoft-nahen Community vollzogen worden. Da der Exchange-BPA schnell sehr erfolgreich war und dazu beitrug, die technische Qualität von Kundenumgebungen zu verbessern – was natürlich auch den Support-Aufwand für Microsoft verringerte –, entwickelte man in Redmond weitere BPA-Fassungen für andere Produkte. Seit Windows Server 2008 R2 ist die gesamte Struktur nun auf einheitlicher Basis zum Teil des Betriebssystems geworden. In unregelmäßigen Abständen aktualisiert Microsoft das Regelwerk für bestimmte BPA-Funktionen, es lohnt sich also, auch nach den optionalen Windows Updates Ausschau zu halten.

Natürlich enthält Windows Server 2012 auch einen Best Practices Analyzer für Hyper-V (ebenso wie für zahlreiche weitere Dienste wie DNS, Active Directory etc.). Sie finden den BPA im *Server-Manager* auf der Rollen-Seite für Hyper-V (siehe Abbildung 2.9). Sofern Ihnen dort unter der Überschrift Best Practices Analyzer keine Ergebnisdaten angezeigt werden, ist die Funktion noch nie gelaufen. In diesem Fall

klicken Sie auf die Schaltfläche AUFGABEN und führen über BPA-ÜBERPRÜFUNG STARTEN den Analyzer aus. Nach einiger Zeit wird Ihnen das Ergebnis direkt im Server-Manager angezeigt.

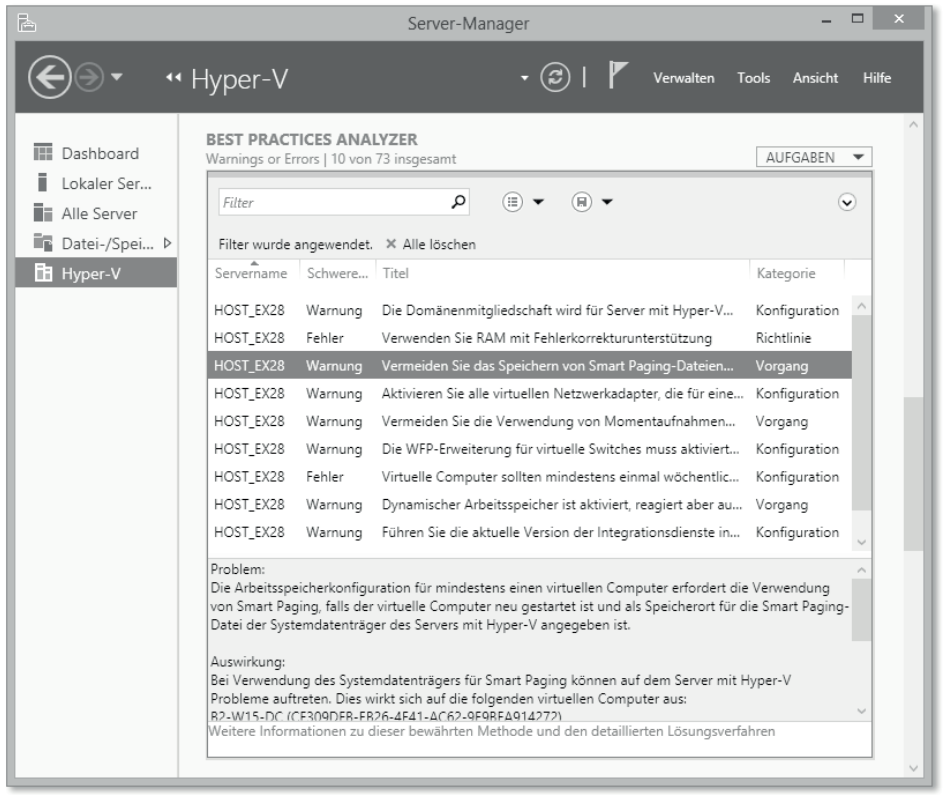


Abbildung 2.9 Der Best Practices Analyzer für Hyper-V findet sich im Server-Manager.

Der BPA teilt seine Ergebnisse in verschiedene Kategorien ein und bietet Filteroptionen für die Anzeige. Auf diese Weise können Sie sich etwa auf »Fehler« und »Warnungen« konzentrieren. Halten Sie sich dabei vor Augen, dass ein »Fehler« im BPA nicht unbedingt auf einen echten technischen Fehler im Sinn etwa des Ereignisprotokolls hinweist. Gemeint ist hier eher, dass eine bestimmte Konfiguration nicht den Regeln entspricht, die Microsoft für eine Hyper-V-Umgebung vorschlägt.

Es besteht kein Zwang, jede dieser Regeln genau umzusetzen. Microsoft wird Sie bei technischen Problemen grundsätzlich auch unterstützen, wenn es BPA-Fehler gibt, es kann allerdings sein, dass man Sie im Rahmen eines technischen Support-Calls im Einzelfall zur Korrektur auffordert.

Auf jeden Fall aber bilden die BPA-Regeln eine sehr gute Orientierung für den Aufbau und die Detailkonfiguration eines Hyper-V-Systems, zumal die Ergebnisse meist gut

erläutert sind. Es empfiehlt sich durchaus, die BPA-Analyse regelmäßig auszuführen, besonders nach Änderungen der Konfiguration oder Updates des Regelwerks durch Microsoft.

Regelmäßige Überprüfungen können Sie beispielsweise mit der PowerShell automatisieren. Dazu dienen Ihnen die *Commandlets* des Moduls `BestPractices` (siehe Abbildung 2.10).

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> Get-Command -Module BestPractices

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Get-BpaModel                                       BestPractices
Cmdlet          Get-BpaResult                                      BestPractices
Cmdlet          Invoke-BpaModel                                    BestPractices
Cmdlet          Set-BpaResult                                      BestPractices


PS C:\Windows\System32\WindowsPowerShell\v1.0>
```

Abbildung 2.10 Die PowerShell-Cmdlets für den BPA gehören dem Modul »BestPractices« an.

Mit folgendem Kommando führen Sie auf dem lokalen Server einen BPA-Scan der Hyper-V-Rolle aus:

```
Invoke-BpaModel Microsoft/Windows/Hyper-V
```

Windows speichert dieses Ergebnis, und im Server-Manager können Sie es im Bereich BEST PRACTICES ANALYZER über den Befehl AUFGABEN • AKTUALISIEREN anzeigen. Direkt in der PowerShell geben Sie die Ergebnisse mit diesem Kommando aus:

```
Get-BpaResult Microsoft/Windows/Hyper-V
```

2.9 Vergleich mit Hyper-V 2.0

Gegenüber dem Windows Server 2008 R2 und den darin enthaltenen Funktionen wurde Hyper-V unter Windows Server 2012 stark erweitert. Neben den reinen Zahlen und Fakten gibt es auch einige Funktionen, die verbessert oder erweitert wurden, ohne dass sich diese Verbesserungen in Zahlen ausdrücken lassen. Dieser Abschnitt zeigt die Unterschiede zwischen den beiden Versionen auf und beschreibt die Änderungen sowie Erweiterungen der einzelnen Features.

2.9.1 Zahlen, Daten, Fakten

Da unterschiedliche Lösungen gern über die maximalen Werte verglichen werden, finden Sie hier in Tabelle 2.1 eine Auflistung der Betriebsgrenzen von Hyper-V unter Windows Server 2008 R2 sowie Windows Server 2012 und Windows Server 2012 R2.

Beide Versionen haben die gleichen Werte, daher werden sie in einer Spalte zusammengefasst.

Wie Sie in Tabelle 2.1 erkennen können, ist keiner der Werte gleich geblieben. Die kleinste Steigerung hat die Anzahl der aktiven VMs mit dem Faktor 2,66 erhalten (384 zu 1.024), die größte mit einer Steigerung um 16 haben das RAM sowie die CPUs einer VM erhalten (64 zu 1.024 bzw. 4 zu 64).

Funktion	Windows Server 2008 R2	Windows Server 2012 (R2)
Anzahl logischer Prozessoren im Host	64	320
Physikalischer Arbeitsspeicher	1 TB	4 TB
Virtuelle Prozessoren	512	2.048
CPUs pro virtuelle Maschine	4	64
RAM pro virtuelle Maschine	64 GB	1 TB
Aktive virtuelle Systeme	384	1.024
Maximale Cluster-Knoten	16	64
Virtuelle Systeme pro Cluster	1000	8000

Tabelle 2.1 Maximalwerte der jeweiligen Funktionen unter Windows Server 2008 R2 und Windows Server 2012 sowie Windows Server 2012 R2

Neben diesen Werten gibt es auch eine Liste von Funktionen, die sich nicht in reinen Zahlen ausdrücken lassen (siehe Tabelle 2.2 und Tabelle 2.3).

Netzwerkfunktion	Windows Server 2008 R2	Windows Server 2012 (R2)
Zusammenfassen von Interfaces (Teaming)	ja, aber Unterstützung durch Kartenhersteller notwendig	ja
Spoofing von MAC-Adressen	ja, mit Service Pack 1	ja
Schutz vor ARP-Spoofing	ja, mit Service Pack 1	ja
SR-IOV-Unterstützung	nein	ja

Tabelle 2.2 Vergleich der Netzwerkfunktionen zwischen Windows Server 2008 R2 und Windows Server 2012 sowie Windows Server 2012 R2

Netzwerkfunktion	Windows Server 2008 R2	Windows Server 2012 (R2)
Quality of Service (QoS)	nein	ja
Bandbreiten-Management	nein	ja
Port-Spiegelung	nein	ja
IPSec-Taskabladung	nein	ja
NIC-Teamvorgang	nein	ja

Tabelle 2.2 Vergleich der Netzwerkfunktionen zwischen Windows Server 2008 R2 und Windows Server 2012 sowie Windows Server 2012 R2 (Forts.)

Speicherfunktion	Windows Server 2008 R2	Windows Server 2012 (R2)
Storage-Live-Migration	nein	ja
Ablage von VMs auf einem Fileserver	nein	ja, realisiert durch SMB 3.0
Fibre Channel in einer VM	nein	ja
Größe der virtuellen Festplatten	VHD bis zu 2 TB	VHD bis zu 2 TB, VHDX bis zu 64 TB
Native 4K-Unterstützung	nein	ja
Snapshot-Zusammenführung im Betrieb	nein, nur bei ausgeschalteter VM	ja
Zuweisung einer neuen Parent Disk (Live New Parent)	nein	ja
Offloaded data transfers (ODX)	nein	ja

Tabelle 2.3 Vergleich der Speicherfunktionen zwischen Windows Server 2008 R2 und Windows Server 2012 sowie Windows Server 2012 R2

2.9.2 Die großen und kleinen Erweiterungen

Im Bereich des Netzwerks hat der Windows Server 2012 eine der größten Erweiterungen erfahren. Unter Windows Server 2008 R2 ist die Möglichkeit, Netzwerke voneinander zu isolieren, die über dieselbe physikalische Infrastruktur betrieben werden, begrenzt auf die Funktion *Virtual Local Area Networks* (*VLAN*). Mit Windows Server

2012 steht Ihnen eine vollständig isolierte Netzwerkschicht zur Verfügung, die für einen sicheren und komplett voneinander getrennten Netzwerkverkehr genutzt werden kann. Ermöglicht wird dies durch den *Hyper-V Extensible Switch*, einen virtuellen *Layer-2*-Switch. Diese Schicht kann durch Erweiterungen angepasst und erweitert werden, hierbei gibt es keine Herstellerbegrenzungen, das heißt, die Erweiterungen müssen nicht von Microsoft veröffentlicht oder geprüft werden. Jeder Hersteller kann eine entsprechende Erweiterung entwickeln und anbieten. Ein Beispiel für solch eine Erweiterung ist ein Virenscanner, der sämtlichen Netzwerkverkehr aus und in die VM scannt und Schadcodes automatisch erkennt und blockiert. Dies erspart unter Umständen den Einsatz von Virenscannern in jeder *VM*, was sich in Bezug auf die Performance positiv auswirkt. Jeder Hyper-V-Switch kann seine eigene Konfiguration haben, das heißt, Erweiterungen sind pro Switch aktiv, nicht pro Host. Dies ermöglicht den Einsatz mehrerer *Hyper-V-Switches* mit unterschiedlichen Erweiterungen und Konfigurationen. Pro Hyper-V-Switch können mehrere Erweiterungen aktiviert werden.

Erweiterungen sind zum Beispiel in der Lage, das Verhalten der VMs (in Bezug auf den Netzwerkverkehr) zu lernen, um so das virtuelle Netzwerk optimal anpassen zu können. Sie wären in der Lage, verdächtiges Verhalten zu erkennen und entsprechend ihrer Konfiguration zu reagieren, zum Beispiel werden bei dauerhaft stark erhöhtem Traffic innerhalb einer VM automatisch eine Bandbreiten-Regulierung und ein Virenscanner aktiv, die den Traffic untersuchen.

Die Virtualisierung des Netzwerks ermöglicht den Betrieb mehrerer *VMs* in einem Subnetz über Hosts hinweg, selbst mit einem privaten Netzwerk. Die Nutzung von VLANs ist nicht mehr zwingend notwendig. Dies erleichtert das Management und erhöht die Anzahl der möglichen Gast-Netzwerke auf über 4.096 (pro Netzwerk können maximal 4.096 VLANs vergeben werden, dies ist technisch die Grenze).

Mithilfe von *Private Virtual Local Area Network* (PVLAN) können Sie kontrollieren, welche VMs miteinander kommunizieren dürfen. Diese Funktion ermöglicht einen Betrieb von VMs mit denselben privaten IP-Bereichen. Dies macht eine Nutzung für Hoster sehr interessant, da die Systeme des Kunden den gewünschten privaten IP-Bereich haben können, unabhängig davon, ob dieser auf benachbarten Systemen ebenfalls genutzt wird.

Es gibt insgesamt zwei Techniken, mit denen eine Virtualisierung des Netzwerks erreicht wird: *IP Address Rewrite* und *Generic Routing Encapsulation* (NVGRE). Mehr zum Thema Netzwerkvirtualisierung durch Adressvirtualisierung und eine ausführliche Erklärung beider Techniken finden Sie in Abschnitt 3.3.10, »Hyper-V-Netzwerkvirtualisierung«.

Unter *Windows Server 2012 R2* wurde die Anzahl der nutzbaren Techniken auf *NVGRE* reduziert, *IP Address Rewrite* ist nicht mehr enthalten.

Die Funktion *DHCP-Wächter* sorgt dafür, dass unerwünschte (virtuelle) DHCP-Server keine Störung im Netzwerk erzeugen. *Router-Wächter* funktioniert ähnlich, hierbei werden Router-Ankündigungen und Umleitungen von anderen, virtuellen Systemen blockiert.

Auf einige dieser Funktionen wird in den späteren Kapiteln noch näher eingegangen, daher wird an dieser Stelle auf eine ausführliche Erklärung verzichtet.

2.10 Virtuelle Gäste

Damit Sie Ihre virtuellen Betriebssysteme zuverlässig betreiben können, sind gewisse Regeln einzuhalten. Wir zeigen Ihnen, wie Sie mit unterstützten Betriebssystemen und Konfigurationen einen stabilen Betrieb erreichen.

2.10.1 Funktionierende und unterstützte VM-Betriebssysteme

Unter Hyper-V können sehr viele Betriebssysteme betrieben werden, aber nur einige von ihnen werden seitens Microsoft unterstützt. Dies liegt unter anderem daran, dass die Systeme ab einem gewissen Alter nicht mehr unterstützt werden und keinen Support mehr erfahren. Eine aktuell gepflegte und zuverlässige Quelle sind die Seiten von Microsoft: *http://technet.microsoft.com/library/hh831531.aspx* (Kurzlink: *http://qccq.de/s/h501*).

Zu den offiziell unterstützten Systemen gehören:

Unterstützte Gast-Betriebssysteme (Server)

- Windows Server 2012
- Windows Server 2008 R2 mit Service Pack 1
- Windows Server 2008 R2
- Windows Server 2008 mit Service Pack 2
- Windows Home Server 2011
- Windows Small Business Server 2011 (Essentials)
- Windows Small Business Server 2011 (Standard)
- Windows Server 2003 R2 mit Service Pack 2
- Windows Server 2003 mit Service Pack 2
- CentOS 6.0–6.3
- CentOS 5.7 sowie 5.8
- Red Hat Enterprise Linux 6.0–6.3
- Red Hat Enterprise Linux 5.7 sowie 5.8

- SUSE Linux Enterprise Server 11 SP2
- Open SUSE 12.1
- Ubuntu 12.04

Unterstützte Gast-Betriebssysteme (Client)

- Windows 8
- Windows 7 mit Service Pack 1
- Windows 7
- Windows Vista mit Service Pack 2
- Windows XP mit Service Pack 3
- Windows XP x64 mit Service Pack 2
- CentOS 6.0–6.3
- CentOS 5.7 sowie 5.8
- Red Hat Enterprise Linux 6.0–6.3
- Red Hat Enterprise Linux 5.7 sowie 5.8
- SUSE Linux Enterprise Server 11 SP2
- Open SUSE 12.1
- Ubuntu 12.04

Neben diesen offiziell unterstützten Systemen gibt es noch einige andere Betriebssysteme, die als VM problemlos betrieben werden können, auch wenn Sie im Problemfall nicht auf den Support von Microsoft zurückgreifen können. Hierzu zählen unter anderem die zuvor genannten Betriebssysteme ohne den entsprechenden Service-Pack-Level, Betriebssysteme von Microsoft, die keinen offiziellen Support mehr erfahren (Windows 2000 Server, Windows 98 etc.), sowie Linux-Distributionen wie *Debian*.

Je nach Betriebssystem gibt es hinsichtlich der Konfiguration und des Betriebs des virtuellen Computers gewisse Bedingungen. Zur Unterstützung und Nutzung von synthetischer Hardware werden Treiber benötigt, die entweder im Betriebssystem direkt enthalten sind oder alternativ nachträglich installiert werden können. Sind diese Treiber nicht verfügbar oder lassen sich nicht installieren, muss die VM mit emulierter Hardware arbeiten (zum Beispiel mit der *älteren Netzwerkkarte*). Dies ist mittlerweile bei allen Microsoft-Betriebssystemen ab Windows 2000 und älter der Fall, wobei sich ein *Windows 2000* oder die jeweilige Server-Variante auch mit den *Integrationskomponenten* von Windows Server 2008 R2 (SP1) oder Windows Server 2008 betreiben lässt.

Wenn Sie ein Unix-Betriebssystem einsetzen, können Sie auf die *Integrationsdienste* für Linux zurückgreifen oder sich alternativ einen Kernel kompilieren, der die entsprechenden Treiber beinhaltet. Ob die Treiber vorhanden sind oder die Möglichkeit einer Kernel-Kompilierung in Ihrem speziellen Fall möglich ist, müssen Sie selbst herausfinden, da die Anzahl an Distributionen und Versionen nahezu unüberschaubar ist.

2.10.2 Technische Limits

Bei dem Betrieb von virtuellen Betriebssystemen gibt es einige Einschränkungen, auf die in diesem Abschnitt eingegangen wird. Die meisten dieser Einschränkungen sind für viele Szenarien nicht relevant, in der einen oder anderen Situation kann es allerdings trotzdem vorkommen, dass Sie an diese Grenzen stoßen.

Die CPU

Sie können in einer VM maximal 64 vCPUs verwenden, sofern das Betriebssystem dies unterstützt. Diese Begrenzung wird in den meisten Anwendungsfällen niemals erreicht, allerdings gibt es noch eine weitere Begrenzung bzw. Abhängigkeit: Die Anzahl der vCPUs kann die Anzahl der logischen Prozessoren nicht übersteigen. Dies bedeutet, dass Sie bei einem Server mit zwei Quad-Core-CPUs ohne Hyper-Threading nur maximal acht vCPUs pro VM zuweisen können, eine höhere Anzahl lässt der Wizard nicht zu. Bedenken Sie dies, wenn Sie eine bestimmte Anzahl an vCPUs innerhalb Ihrer VM benötigen.

Der Arbeitsspeicher

Sie können einer VM maximal 1 TB an Arbeitsspeicher zuweisen. Diese Zahl ist aktuell nahezu unerreichbar hoch, allein die Kosten für diese Anzahl an RAM sind enorm. Ein weiterer Punkt, der neben der maximalen Größe bedacht werden muss, ist die Zuweisung von dynamischem Arbeitsspeicher. Behalten Sie hier immer im Hinterkopf, dass Sie **keine** (!) Überprovisionierung technisch nutzen können.

Natürlich können Sie für jede VM einen Maximalwert von 1 TB eintragen, technisch nutzt Ihre VM allerdings immer nur das, was auch zur Verfügung steht. Dies ist zwar eine Einschränkung, wir sehen diese allerdings sehr positiv. Sollte es bei einer Überprovisionierung einmal dazu kommen, dass RAM-Inhalte auf die Festplatte ausgelagert werden müssten, wäre das in etwa so, als wenn Sie in einem Formel-1-Wagen bei 300 km/h schlagartig auf die Bremse treten und maximal 2 km/h fahren. Hyper-V hat solch eine Technik nicht implementiert, in unseren Augen eine kluge Entscheidung.

Die Netzwerkkarten

Sie haben bei der Anzahl der physischen Netzwerkkarten in Ihrem Host keine direkte Begrenzung, allerdings werden Sie ab einer gewissen Anzahl an Karten keinen Platz mehr in Ihrem Server haben, um weitere Karten einbauen zu können.

Aufseiten der VM sieht das Ganze schon »ein wenig« begrenzter aus, Sie können eine VM mit maximal zwölf Karten ausstatten. Die Anzahl von synthetischen und emulierten Karten ist hierbei nicht gleichgültig – Sie können maximal acht synthetische und vier emulierte Karten pro VM zuweisen. Aufseiten des Hosts können Sie eine unendliche Anzahl an virtuellen Switchen erstellen, die Anzahl externer Switches ist hierbei auf die Anzahl an Karten bzw. Ports (eine Karte kann natürlich mehrere Ports besitzen) begrenzt. Interne oder private Netzwerke können in einer unendlichen Anzahl erstellt werden.

Fibre Channel

Sie können mit Hyper-V unter Windows Server 2012 erstmals innerhalb einer VM einen *Fibre-Channel-Host-Bus-Adapter* (FC-HBA) verwenden. Bedingung für die Nutzung ist hierbei die Funktion *N_Port ID Virtualization* (NPIV), die es erlaubt, dass jede VM eigene *Worldwide Names* (WWN) erhält, da nur so eine Kommunikation mehrerer VMs über einen Adapter möglich ist. Diese Funktion muss nicht nur vom *FC-HBA* unterstützt werden, sondern von allen Geräten, die in die Fibre-Channel-Kommunikation involviert sind.

Lokale Schnittstellen

Bei der Nutzung der lokalen Schnittstellen hat sich gegenüber den vorherigen Versionen nichts geändert. Es ist weiterhin nicht möglich, lokal angeschlossene USB-Geräte oder Geräte am COM- sowie Parallel-Port zu nutzen. Wir hören oft Beschwerden über diese »Einschränkung«, die Begründung von Microsoft erscheint allerdings schlüssig und sinnvoll: Lokale Geräte stören oder verhindern den Umzug einer VM auf einen anderen Host, somit wird keine Technik implementiert, die die Nutzung von lokalen Komponenten wie USB-Sticks oder -Festplatten ermöglicht, die wiederum einen Transfer der VM verhindert.

2.10.3 Alte Betriebssysteme betreiben

Möchten Sie ein oder mehrere Betriebssysteme virtualisieren, die bereits eine geraume Zeit auf dem Markt sind und schon vor der Virtualisierungstechnik erschienen sind, kann es zu Problemen mit der simulierten Hardware kommen. Dies liegt daran, dass die Betriebssysteme zu einer Zeit entwickelt wurden, in der ein Prozessor auch wirklich nur *ein* Prozessor war und sich die Größen von Arbeitsspeicher in MB oder sogar KB beschreiben ließen. Solche Systeme kommen nicht mit den aktuellen Mehrkern-CPUs zurecht und verweigern auch als *VM* den Betrieb. Hier konnte unter Windows Server 2008 oder Windows Server 2008 R2 eventuell nachgeholfen werden, indem in den Eigenschaften einer VM unter Prozessor die Option Prozessorfunktionen einschränken aktiviert wurde. Diese Option gibt es unter *Windows Server 2012* nicht mehr, zumindest nicht im GUI. Falls Sie die *vCPU* für den Betrieb einer VM

einschränken müssen, kann dies nur noch über die *PowerShell* durchgeführt werden. Der Befehl dazu lautet:

```
Get-VM VM_Name | Get-VMProcessor | Set-VMProcessor ⮐
-CompatibilityForOlderOperatingSystemsEnabled $true
```

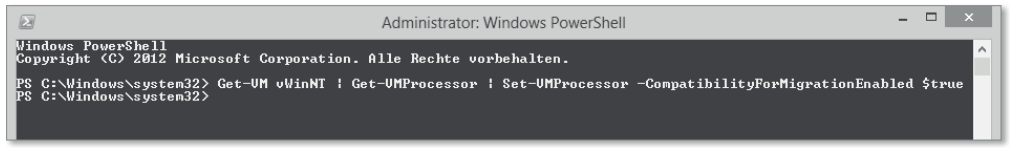


Abbildung 2.11 Nutzung der PowerShell zur Aktivierung der eingeschränkten Prozessorfunktionen

Um diese Änderung wieder rückgängig zu machen, muss folgender Befehl ausgeführt werden:

```
Get-VM VM_Name | Set-VMProcessor ⮐
-CompatibilityForOlderOperatingSystemsEnabled $false
```

2.11 Mit der PowerShell administrieren

Vor dem Release von Windows Server 2012 war eine Administration von Hyper-V über die PowerShell nur durch die Installation einer *PowerShell Management Library for Hyper-V* möglich, die über *http://pshyperv.codeplex.com* heruntergeladen und installiert werden muss. Mit dieser Bibliothek stehen Ihnen knapp 80 Befehle (*Commandlets* genannt, im weiteren Verlauf teilweise mit *Cmdlets* abgekürzt) zur Verfügung, mit denen Sie Hyper-V unter Windows Server 2008 R2 oder Ihren Hyper-V Server 2008 R2 administrieren können. Neben Befehlen zur Erstellung, Verwaltung und Änderung von VMs stehen Ihnen auch noch weitere Möglichkeiten zur Verfügung, zum Beispiel die Arbeit mit VHD-Dateien.

Die wohl bekannteste Anwendung findet diese Bibliothek bei der Nutzung eines automatischen Export-Skripts, das vom deutschen MVP Carsten Rachfahl geschrieben wurde und unter *http://www.hyper-v-server.de/tools/hyper-v-sicherung-mittels-powershell-script* (Kurzlink: *http://qccq.de/s/h202*) zur Verfügung steht. Mithilfe dieses Skripts können Sie per geplanten Task eine oder mehrere VMs herunterfahren, diese in ein lokales oder ein Netzwerkverzeichnis exportieren und danach wieder starten.

Achtung: Da es sich hierbei allerdings nicht um eine offizielle Entwicklung von Microsoft handelt, bietet Microsoft bei Fehlern oder Problemen keinen Support.

Ab Windows Server 2012 ist die Administration von Hyper-V per PowerShell fester Bestandteil des Betriebssystems und direkt bei der Grundinstallation mit dabei.

Ihnen stehen mehr als 160 Commandlets zur Verfügung, um die Administration zu automatisieren und zu vereinfachen. Im weiteren Verlauf dieses Abschnitts zeigen wir Ihnen einige dieser Commandlets, eine komplette Liste aller Befehle zur Administration von *Hyper-V* inklusive einer ausführlichen Beschreibung erhalten Sie unter *http://technet.microsoft.com/en-us/library/hh848559.aspx* (Kurzlink: *http://qccq.de/s/h203*).

Jan Kappen hat das erwähnte Export-Skript für die Nutzung unter Windows Server 2012 angepasst, diese Version steht unter *http://www.hyper-v-server.de/management/hyper-v-sicherung-mittels-powershell-skript-fr-windows-server-2012* (Kurzlink: *http://qccq.de/s/h204*) zum Download zur Verfügung.

2.11.1 Der Einstieg

Wenn Sie bisher noch keinen Kontakt mit der PowerShell hatten, sollten Sie sich das Thema einmal unvoreingenommen anschauen. Dieser Abschnitt bietet Ihnen genau solch eine Möglichkeit, da wir bei den Grundlagen beginnen und später mit einigen Beispielen praktische Anwendungsmöglichkeiten aufzeigen, die Ihnen das Leben als Administrator etwas einfacher machen können. Kleiner Tipp: Die Administration eines oder mehrerer Hyper-V-Hosts kann größtenteils per PowerShell erledigt werden, dies erspart Ihnen eine Menge Zeit gegenüber der Administration per GUI bei häufig wiederkehrenden Aufgaben.

Die PowerShell aufrufen

Sie können eine PowerShell öffnen, indem Sie im Start-Menü beginnen, das Wort »powershell« zu tippen. Nach einigen Buchstaben sehen Sie links im Menü, dass Sie die Wahl zwischen mehreren Programmen haben (siehe Abbildung 2.14). Sie können die PowerShell auch über den Server-Manager über das Menü TOOLS • WINDOWS POWERSHELL oder über AUSFÜHREN • POWERSHELL.EXE aufrufen.

Korrekter Aufruf der PowerShell

Achten Sie darauf, dass Sie die PowerShell mit administrativen Rechten aufrufen, da sonst die Ausführung von Befehlen teilweise nicht funktioniert und Sie mitunter sehr »interessante« Fehlermeldungen erhalten, die nicht unbedingt auf fehlende Rechte zurückzuführen sind. Bei der Nutzung einer administrativen PowerShell sollten Sie stets vorsichtig agieren und wissen, was Sie tun, da Sie mit den falschen Befehlen eine Menge Schaden anrichten können.

Neben der nativen 64-Bit-Version steht Ihnen auch noch eine 32-Bit-Version zur Verfügung. Die 32-Bit-Variante findet nur selten Anwendung, nutzen Sie grundsätzlich erst einmal die 64-Bit-Variante.

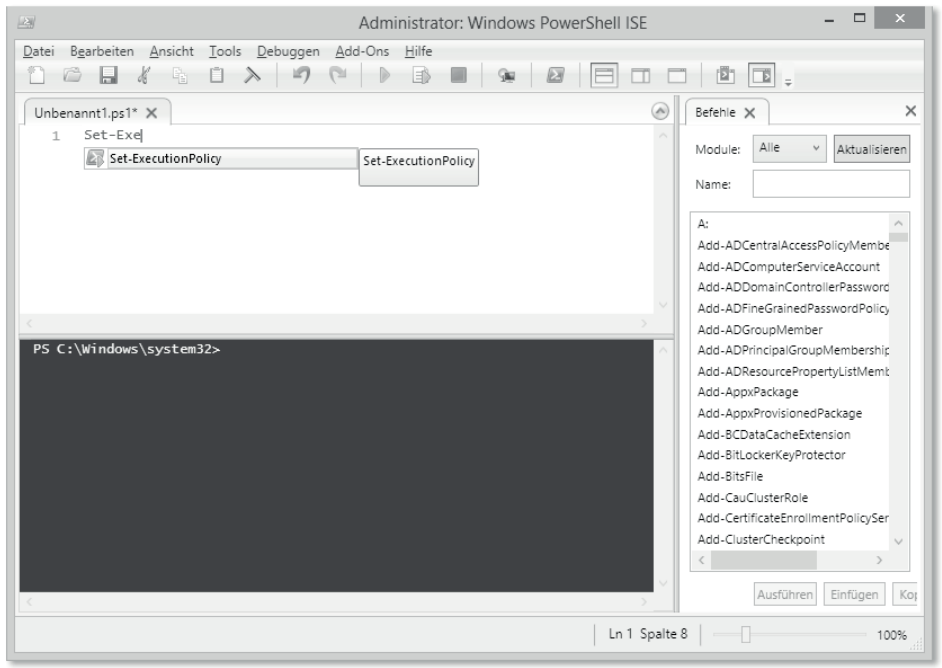


Abbildung 2.12 Autovervollständigung mittels »Intellisense« im »PowerShell ISE«

Neben der PowerShell-Konsole können Sie unter Windows Server 2012 erstmals das *PowerShell ISE* (siehe Abbildung 2.12) verwenden. *ISE* steht für *Integrated Scripting Environment* und stellt Ihnen eine grafische Oberfläche zur Erstellung, Bearbeitung oder einfach nur zur Sichtung eines PowerShell-Skripts zur Verfügung. Die Erstellung oder Modifikation eines Skripts gestaltet sich im ISE sehr einfach, da das Programm die Syntax farblich kennzeichnet. Mittels *Intellisense* werden Ihre Eingaben automatisch vervollständigt, zudem haben Sie über ein Menü eine Übersicht über die bei Ihrem Befehl vorhandenen Parameter und Möglichkeiten (siehe Abbildung 2.12). Wenn Sie mit der Maus über den Befehl fahren, können Sie im eingeblendeten Menü die möglichen Parameter einsehen (siehe Abbildung 2.13).

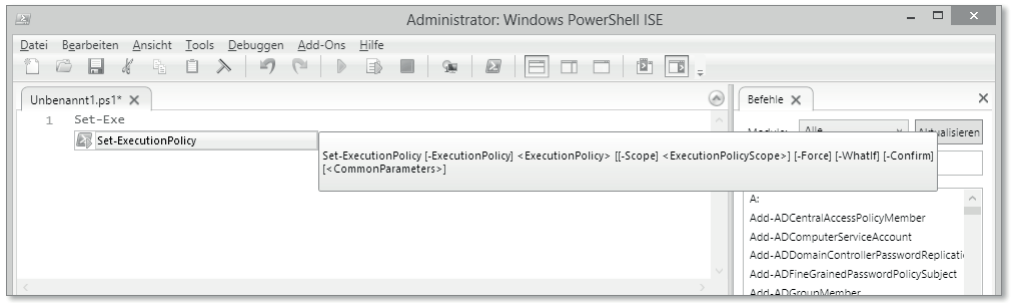


Abbildung 2.13 Eingeblendete Parameter eines Befehls im PowerShell ISE

Nach dem Aufruf einer PowerShell wie in Abbildung 2.14 erwartet Sie ein weißer blinkender Cursor in einer blauen Box, der auf Ihre Befehle wartet (Abbildung 2.15).

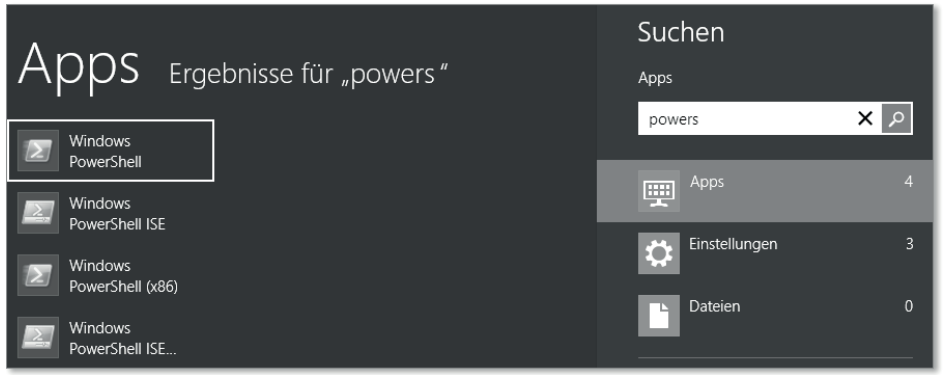


Abbildung 2.14 Der Aufruf einer PowerShell über das Startmenü

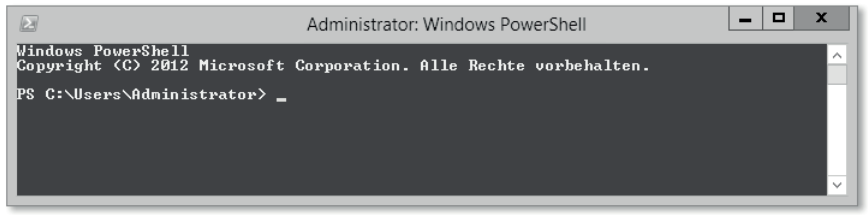


Abbildung 2.15 Eine Windows PowerShell direkt nach dem Aufruf

Die Hilfe nutzen

Innerhalb der PowerShell steht für jeden Befehl eine kurze Hilfe zur Verfügung, die Ihnen den Namen, die Syntax und mögliche Aliasse anzeigt. Diese Hilfe können Sie einsehen, wenn Sie hinter das entsprechende Commandlet den Parameter `-?` setzen (siehe Abbildung 2.16) oder alternativ den Befehl `Get-Help <cmdlet-Name>` nutzen.

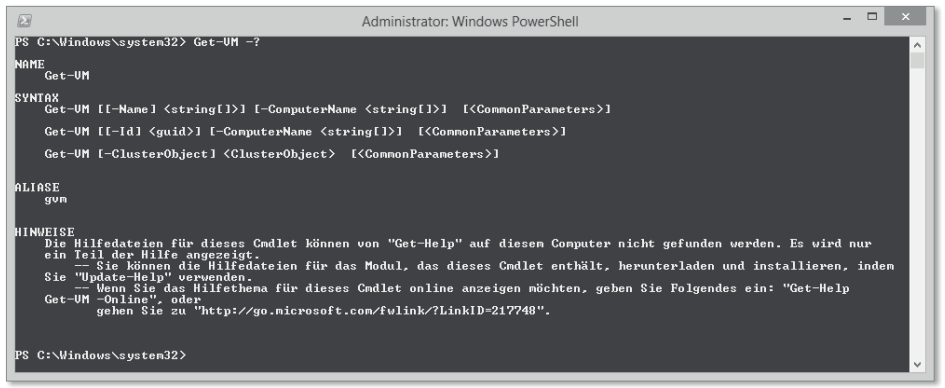


Abbildung 2.16 Aufruf der integrierten Hilfe zu einem PowerShell-Befehl

Neben diesen Informationen erhalten Sie als weitere Ausgabe den Hinweis, dass die Hilfe-Dateien für dieses Cmdlet nicht auf Ihrem Computer gefunden wurden. Dies hat den Grund, dass die Hilfe-Dateien stetig erweitert und angepasst werden, außerdem wird auf jedem Server Speicherplatz gespart, wenn diese Dateien standardmäßig nicht installiert sind und nur bei Bedarf installiert werden. Die Hilfe liefert Ihnen neben der Information der fehlenden Hilfe-Dateien auch direkt den Befehl mit, mit dem Sie die aktuellen Dateien von Microsoft herunterladen können. Hierzu geben Sie in der PowerShell den Befehl

```
Update-Help
```

ein. Nach dem Aufruf wird online eine Verbindung zu den Servern von Microsoft aufgebaut und die Dateien werden heruntergeladen, falls der Server mit dem Internet verbunden ist und die Verbindung nicht per Firewall oder sonstigen Kontrollmechanismen gesperrt ist. Da dies zum einen für Hyper-V-Hosts nicht empfohlen und zum anderen in vielen Umgebungen nicht möglich ist, scheitert der Aufruf von `Update-Help` mit einer Fehlermeldung.

In diesem Fall können Sie sich helfen, indem Sie die aktualisierten Hilfe-Dateien auf einen Server oder PC mit *PowerShell 3.0* und aktiver Internetverbindung herunterladen und danach auf Ihrem Hyper-V-Host einspielen. Speichern Sie die Dateien mit dem auch in Abbildung 2.17 gezeigten Befehl

```
Save-Help -DestinationPath C:\temp
```

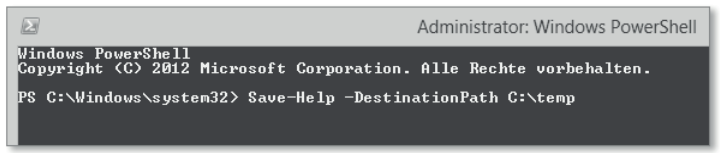


Abbildung 2.17 Befehl zur Speicherung der Hilfe-Dateien

Sie können diese Dateien nun per Wechseldatenträger oder Netzwerk auf einen gemeinsam genutzten Speicherplatz oder direkt auf Ihren Server übertragen und die Hilfe-Dateien mit dem Befehl

```
Update-Help -SourcePath C:\temp
```

importieren.

Tipp

Wenn Sie den Befehl zum Update der Hilfe-Dateien oder zur lokalen Speicherung an diesem Tag bereits ausgeführt haben, erfolgt keine erneute Prüfung. Dies können Sie umgehen, indem Sie den Parameter `-Force` an den Aufruf anhängen.

Cmdlets zur Administration von Hyper-V nutzen

Um alle zur Verfügung stehenden *Commandlets* für Hyper-V anzeigen zu lassen, führen Sie den folgenden Befehl aus:

```
Get-Command -Module Hyper-V
```

Diese Ausgabe ermöglicht es Ihnen, alle zur Verfügung stehenden Commandlets zu studieren und das für Ihren Fall benötigte auszuwählen. Wenn Sie sich zum Beispiel eine Liste aller auf Ihrem Host befindlichen VMs anzeigen lassen möchten, realisieren Sie dies am einfachsten mit dem Befehl:

```
Get-VM
```

Die Auflistung zeigt Ihnen den Namen, den aktuellen Betriebsstatus, die Auslastung der CPU, die Zuweisung des Arbeitsspeichers, die Laufzeit und den Status Ihrer VMs an. Wenn Sie nun eine VM starten möchten, erreichen Sie dies am einfachsten über den Befehl:

```
Start-VM -Name VM1
```

Sie können mehrere Befehle miteinander verbinden, dies wird über die PowerShell-Pipeline ermöglicht. Mehrere Befehle werden nacheinander abgearbeitet, wobei das Ergebnis oder die Ausgabe des ersten Befehls im zweiten Befehl verarbeitet wird. Ein Beispiel hierfür wäre die Auflistung aller VMs, allerdings mit einer Filterung auf den Namen, da der Rest aktuell uninteressant ist:

```
Get-VM | Select-Object -Property Name
```

Wie Sie in Abbildung 2.18 erkennen können, wird nun nur der Name der VMs ausgegeben, keine weiteren Details.

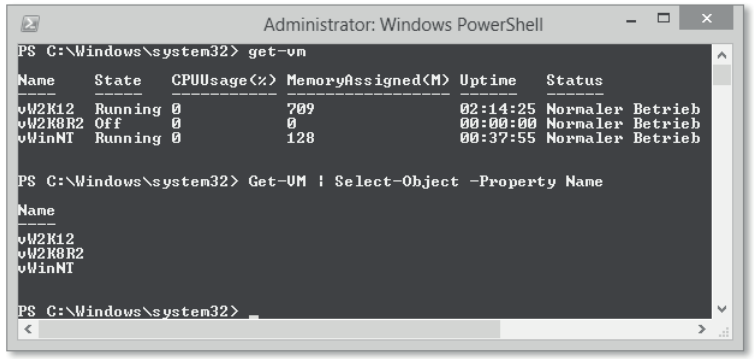


Abbildung 2.18 Ausgabe einer Liste aller VMs, gefiltert auf den Namen der VMs

Dies sind nur einige Beispiele für Befehle, die zur Administration genutzt werden können. Die Nutzung von PowerShell bringt Ihnen nach einer kurzen Zeit der Eingewöhnung einen erheblichen zeitlichen Vorteil, gerade wenn Sie gewisse Aufgaben in regelmäßigen Abständen durchführen müssen. Um die Nutzung der PowerShell für Sie im Verlauf dieses Buches ein wenig einfacher zu gestalten, listen wir bei vielen Themen die betreffenden PowerShell-Cmdlets auf. Da dieses Buch aber nicht primär von PowerShell handelt, gehen wir nicht sehr in die Tiefe, sondern zeigen Ihnen nur den Weg dorthin. Im nächsten Abschnitt zeigen wir Ihnen einige Beispiel-Skripte, die verdeutlichen, welche Möglichkeiten Sie mit der Nutzung von PowerShell haben.

2.11.2 Beispiel-Skripte

Um Ihnen die Möglichkeiten einer Administration per PowerShell zu zeigen, haben wir Ihnen an dieser Stelle zwei Beispiel-Skripte aufgeführt.

In Listing 2.1 und Listing 2.2 sehen Sie die betreffenden Skripte und können anhand der Kommentare die Funktion der Codezeilen genau nachvollziehen.

Skript für Anmerkungen zu einer VM

Das folgende Skript liest die MAC- und IP-Adressen aller VMs auf einem Host aus und schreibt diese in die Anmerkungen der jeweiligen VMs. Bestehende Informationen werden nicht überschrieben oder gelöscht, ein erneutes Ausführen des Skripts aktualisiert die Informationen, ohne zusätzliche Informationen zu löschen oder zu überschreiben.

```
#
# Dieses Skript erweitert die Bemerkungen einer VM um
# die Angaben von IP- und MAC-Adressen:
#
# 000000000000 (a.b.c.d e::f) 000000000001 (...)
### existing notes
#
# Existierende Bemerkungen werden beibehalten.
#

Get-VM | foreach {
    $oMachine = $_

    # Extrahiere existierende Bemerkungen
    [string]$sUserNotes = $oMachine.Notes
    # Entferne früher vorangestellte Daten (delimiter ###)
    [int]$iIndex = $sUserNotes.IndexOf(" ###")
    if ($iIndex -gt 0) {
        # enthält jetzt nur die Bemerkungen des Eigentümers
        $sUserNotes = $sUserNotes.Substring($iIndex + 5)
```

```
    }

    # Variable wird zusätzliche Bemerkungen pro VM enthalten
    [string]$sNotes = ""

    # alle Netzwerkkarten durchgehen
    $oMachine.NetworkAdapters | foreach {
        $oAdapter = $_

        # fügt MAC- und IP-Adressen hinzu
        $sNotes += "$($oAdapter.MacAddress) (" ➲
        $sNotes += $oAdapter.IPAddresses ➲
        $sNotes += ") "
    }

    # fügt Trennzeichen und existierende Bemerkungen hinzu
    $sNotes += "### $sUserNotes"

    # aktualisiert VM mit neuen Bemerkungen
    Set-VM -Name $oMachine.Name -Notes $sNotes
}
```

Listing 2.1 Skript zur automatischen Erweiterung der VM-Bemerkungen

Skript für ein NIC-Team mit virtuellen Netzwerkkarten

Der Auszug aus dem folgenden Skript wurde uns freundlicherweise vom deutschen MVP Carsten Rachfahl zur Verfügung gestellt. Das gesamte Skript fasst die beiden Ports einer 10-GBit/s-Dual-Port-Karte zu einem Team zusammen, danach erstellt es die zur Einrichtung eines *Failover-Clusters* benötigten Netzwerkkarten und versieht sie mit den entsprechenden Bindungen. Auf Wunsch kann mit diesem Skript das Team auch wieder komplett entfernt werden. Der Grund für die Erstellung dieses Skripts war die Installation bei einem Kunden, der diese Art von Netzwerkkonfiguration gern nutzen und bei der Anschaffung von weiteren Cluster-Knoten eine einfache Möglichkeit haben wollte, diese neue Hardware komplett identisch mit den bestehenden Knoten zu konfigurieren. Wir beschränken uns hier auf einen Teilbereich, bei dem die Karten zu einem Team zusammengefasst und basierend auf diesem Team weitere virtuelle Karten erstellt werden.

```
# Erstellung eines Teams mit allen Karten
   New-NetLBFOTeam -Name "TEAM" -TeamNICName "TEAM" ➲
   -TeamMembers Ethernet* -TeamingMode LACP ➲
   -LoadBalancingAlgorithm HyperVPort -Confirm:$false
# Erstellung einer virtuellen Switch, basierend auf dem
  vorher erstellten Team-Interface
      New-VMSwitch "ConvergedSwitch" -MinimumBandwidthMode weight ➲
      -NetAdapterName "TEAM" -AllowManagementOS 0 -Confirm:$false

# Konfiguration der Bandbreiten-Reservierung
      Set-VMSwitch "ConvergedSwitch" ➲
      -DefaultFlowMinimumBandwidthWeight 10

# Erstellung von virtuellen Netzwerkkarten (vNics)
      # vNic Management
          Add-VMNetworkAdapter -ManagementOS -Name "Management" ➲
          -SwitchName "ConvergedSwitch"
      # vNic CSV
          Add-VMNetworkAdapter -ManagementOS -Name "CSV" ➲
          -SwitchName "ConvergedSwitch"

# Konfiguration der Bandbreiten-Reservierung
      # vNic Management
          Set-VMNetworkAdapter -ManagementOS -Name "Management" ➲
          -MinimumBandwidthWeight 20 -verbose
      # vNic CSV
          Set-VMNetworkAdapter -ManagementOS -Name "CSV" ➲
          -MinimumBandwidthWeight 25 -verbose
```

Listing 2.2 Erstellung eines Netzwerkkarten-Teams und zwei vNics

Diese beiden Skripte geben nur im Ansatz wieder, welche Möglichkeiten Sie mit der Nutzung von PowerShell-Skripten haben. Da nahezu alle Produkte von Microsoft eine Administration per PowerShell erlauben oder teilweise sogar voraussetzen, sollten Sie diese Möglichkeiten nutzen, auch wenn Ihnen eine Administration per GUI einfacher und leichter erscheint. Eine Übersicht über alle verfügbaren Befehle für nahezu alle Rollen und Features finden Sie auf der folgenden Technet-Seite: *http://technet.microsoft.com/de-de/library/hh801904.aspx* (Kurzlink: *http://qccq.de/s/h205*).

Weitere interessante Informationen erhalten Sie im *Windows PowerShell Blog*, geführt von der Microsoft-Produktgruppe für die PowerShell: *http://blogs.msdn.com/b/powershell* (Kurzlink: *http://qccq.de/s/h206*).

2.12 Microsoft Hyper-V Server 2012

Der *Hyper-V Server 2012* ist die dritte Version, die Microsoft kostenfrei zur Verfügung stellt. Das System ist eine im Umfang reduzierte Version von Windows Server 2012, bei der nach der Installation direkt die Hyper-V-Rolle aktiv ist und auf dem keine

weiteren Rollen oder Features installiert werden können, alle benötigten Features sind bereits aktiviert. Der Hyper-V Server 2012 ist, genau wie die Core-Variante von Windows Server 2012, nur bedingt lokal administrierbar. In den Möglichkeiten der Virtualisierung steht der Hyper-V Server 2012 seinem »großen Bruder«, der als Rolle unter *Windows Server 2012 Standard* oder *Datacenter* verfügbar ist, in nichts nach. Alle Funktionen und Möglichkeiten, die Sie mit Hyper-V als Rolle in den kostenpflichtigen Versionen haben, haben Sie auch im Hyper-V Server 2012.

Was Sie beachten müssen: Sie erwerben mit diesem Produkt keine Lizenzen oder Lizenzrechte. Alle Betriebssysteme, die nicht kostenfrei erworben werden können und die auf einem Hyper-V-Server betrieben werden, müssen laut ihren Bedingungen lizenziert werden.

2.12.1 Installieren und einrichten

Die Installation von Hyper-V Server 2012 gestaltet sich recht einfach. Die Software kann frei verfügbar von Microsoft heruntergeladen werden und ist ca. 1,7 GB groß. Nachdem die ISO-Datei auf einen Datenträger gebrannt und in das System eingelegt wurde, beginnt das bekannte Windows-Setup. Während dieses Setups wird die Sprache der Tastatur abgefragt, zudem können Sie eine Partitionierung der Festplatten vornehmen. Bei der Einrichtung und dem Betrieb eines Hyper-V-Servers gelten die gleichen Bedingungen und Empfehlungen wie bei der Nutzung von Windows Server 2012 Standard oder Datacenter. Diese können Sie in Kapitel 3, »Den Host-Server einrichten«, nachlesen.

Nach der erfolgreichen Installation und der Vergabe des lokalen Administrator-Kennworts erwartet Sie das von den vorherigen Versionen bekannte Bild (siehe dazu Abbildung 2.19).

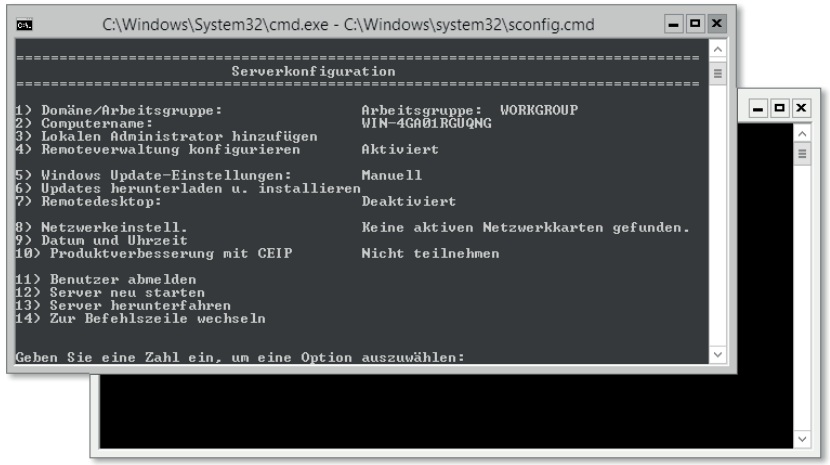


Abbildung 2.19 Der Hyper-V-Server nach dem ersten Start

Das System wird primär über die *Server-Konfiguration* verwaltet. Die Aufgaben, die mit diesem Tool übernommen werden können, sind folgende:

- Wechsel zwischen Domäne und Arbeitsgruppe
- Ändern des Computernamens
- Management der lokalen Administratoren
- Konfiguration des Remote-Managements
- Konfiguration des Windows Update-Verhaltens
- Konfiguration von Remote Desktop
- Konfiguration des Netzwerks
- Konfiguration von Datum und Uhrzeit
- Teilnahme am Programm zur Verbesserung der Software
- Abmelden des aktuellen Benutzers
- Neustart des Servers
- Herunterfahren des Servers
- Schließen des Fensters und Wechsel zur Befehlszeile

Kleiner Tipp: Falls Sie die *Server-Konfiguration* versehentlich schließen, können Sie diese durch den folgenden Aufruf wieder öffnen:

```
C:\Windows\System32\sconfig.cmd
```

Neben der Möglichkeit, das System lokal über die Konsole zu verwalten, steht Ihnen auch eine Verwaltung per PowerShell oder per *MMC* zur Verfügung. Hierzu muss die Remote-Verwaltung aktiviert sein, was standardmäßig der Fall ist. Falls sie ausgeschaltet werden soll, können Sie dies über den Punkt REMOTEVERWALTUNG KONFIGURIEREN vornehmen. Sobald mehrere Hosts gemeinsam verwaltet werden sollen, kommen in der Regel Management-Lösungen zum Einsatz, die solch einen Betrieb deutlich vereinfachen. Ein Beispiel wäre der *System Center Virtual Machine Manager*.

Die Hyper-V-Rolle muss bei einem Hyper-V Server 2012 nicht manuell aktiviert werden, da das System nach der Installation direkt im *Management OS*-Betrieb läuft, das heißt, die Virtualisierung ist bereits aktiv und kann genutzt werden. Eine Verwaltung der VMs und eine Konfiguration des Systems per GUI sind lokal nicht möglich, da kein Hyper-V-Manager vorhanden ist. Hierzu muss entweder ein Windows Server 2012 mit den *Hyper-V-Verwaltungstools* oder ein Client-Betriebssystem mit den *Remoteserver-Verwaltungstools*, kurz *RSAT*, genutzt werden. In Abbildung 2.20 sehen Sie ein Windows 8 mit Hyper-V-Manger, der mit einem Hyper-V Server 2012 verbunden ist.

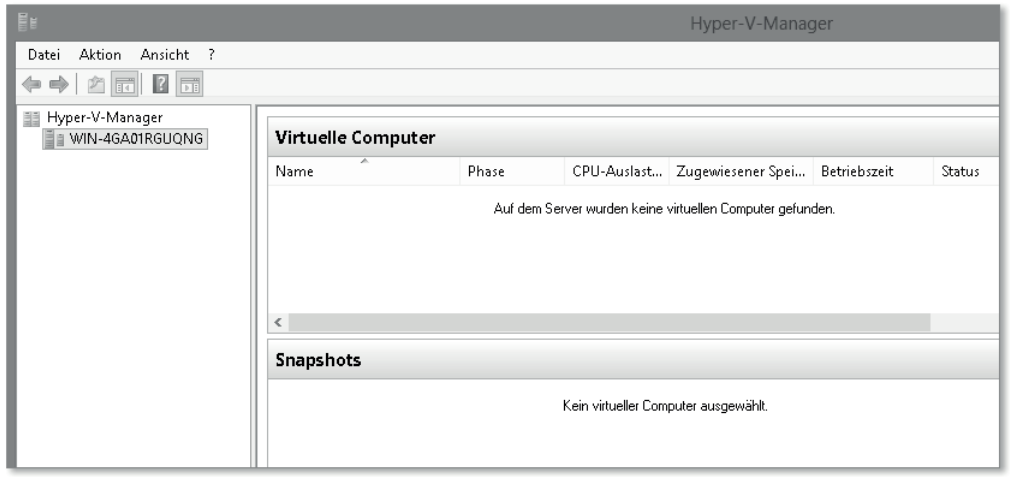


Abbildung 2.20 Verbindung zu einem Hyper-V Server 2012 mit dem Hyper-V-Manager auf Windows 8

2.12.2 Auf einem USB-Stick installieren

Sie können einen Hyper-V Server 2012 (neben weiteren Betriebssystemen wie Windows 8, Windows Server 2012 etc. – beachten Sie in diesem Fall allerdings die Unterstützung seitens Microsoft) auf einem USB-Stick installieren und diesen als Boot-Medium nutzen. Da in vielen Server-Modellen zum Beispiel USB- oder Speicherkarten-Schnittstellen verbaut sind, lassen sich diese als Datenträger des Host-Betriebssystems nutzen. Diese Vorgehensweise hat unter anderem den Vorteil, dass Sie alle zur Verfügung stehenden Slots mit Festplatten füllen und diese ausschließlich als Datenträger der VM-Daten nutzen. Ob Sie einen USB-Stick oder eine Speicherkarte nutzen, hängt zum einen von Ihnen als Entscheider, zum anderen von den technischen Möglichkeiten der Hardware ab. Achten Sie generell auf die Lese- und Schreibgeschwindigkeiten des Speichermediums, hier gibt es gravierende Unterschiede. Falls möglich, nutzen Sie USB 3.0-Sticks oder Speicherkarten der neuesten Generation. Achten Sie zusätzlich auf Kennzahlen der Hersteller und Aussagen von Käufern im Internet, die bereits Erfahrungen gesammelt haben.

Bevor Sie mit der Installation beginnen, benötigen Sie den Datenträger von Hyper-V Server 2012. Schieben Sie den Stick in einen freien Anschluss, und öffnen Sie eine administrative Eingabeaufforderung. Öffnen Sie das Programm `diskpart` für den Start des Programms zur Partitionierung. Lassen Sie sich mit dem Befehl `list disk` die verfügbaren Datenträger anzeigen, wählen Sie danach Ihren Datenträger mit dem Befehl `select disk 2` aus (die Zahl `2` muss ersetzt werden mit der Nummer des Datenträgers). Führen Sie als Nächstes den Befehl `clean` aus, um den Datenträger zu löschen. Mit dem Befehl `create partition primary` erstellen Sie eine Partition auf dem

Datenträger, mit `select partition 1` setzen Sie den Fokus auf die soeben erstellte Partition. Der Befehl `active` markiert die erstellte Partition als aktiv. Sie können die Partition mit einem Dateisystem (in unserem Fall NTFS) mit dem Befehl `format fs=ntfs quick` formatieren. Nach der Formatierung benötigen Sie noch einen Laufwerksbuchstaben für die Partition, diesen weisen Sie mit `assign letter=s` zu. Welchen Buchstaben Sie verwenden ist gleich, er darf nur nicht anderweitig belegt sein. Einen Screenshot der Formatierung und Partitionierung sehen Sie in Abbildung 2.21.

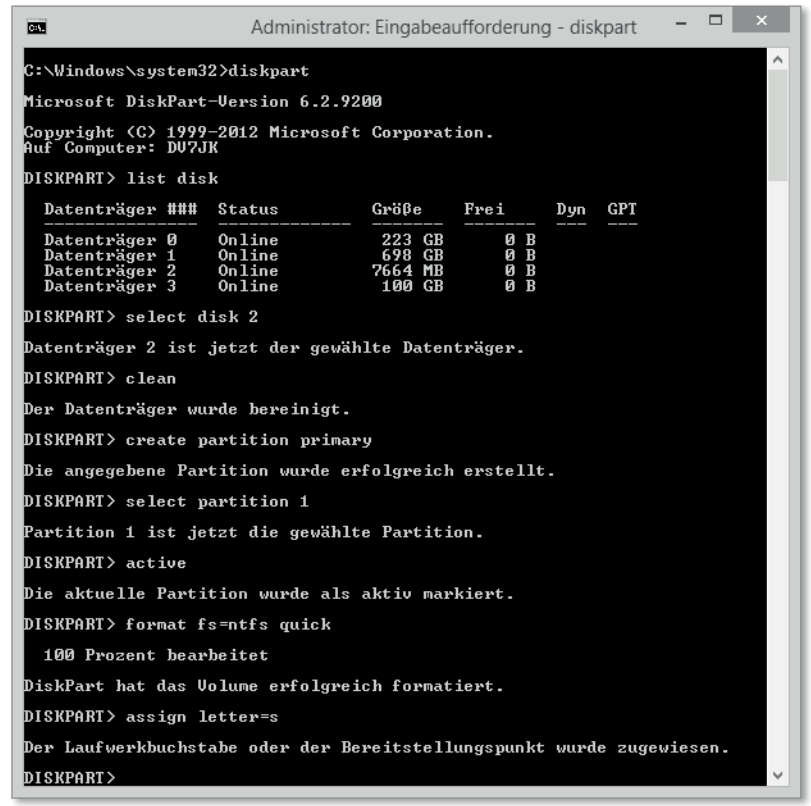


Abbildung 2.21 Partitionierung und Formatierung eines USB-Sticks mit »Diskpart« zur Nutzung als Boot-Medium

Beenden Sie `diskpart` mit dem Befehl `exit`, schließen Sie das Fenster aber noch nicht.

Laden Sie den *Hyper-V Server 2012* herunter, und mounten oder entpacken Sie die .iso-Datei. Schauen Sie sich den Ordner *boot* an, hier befindet sich eine Datei mit dem Namen *bootsect.exe*. Wechseln Sie zurück in die noch geöffnete *Eingabeaufforderung*, und führen Sie den Befehl `G:\boot\bootsect.exe/nt60 S:` wie in Abbildung 2.22 aus. Laufwerk `G:` in diesem Beispiel ist die gemountete .iso-Datei, Laufwerk `S:` ist Ihr USB-Stick.

Kopieren Sie nun den kompletten Inhalt der .iso-Datei auf Ihren USB-Stick. Nachdem der Kopiervorgang abgeschlossen ist, können Sie den USB-Stick entfernen, an dem gewünschten Server oder PC anschließen und von ihm booten. Es startet ein Setup, nach der Durchführung kann der USB-Stick dauerhaft als Boot-Datenträger verwendet werden.

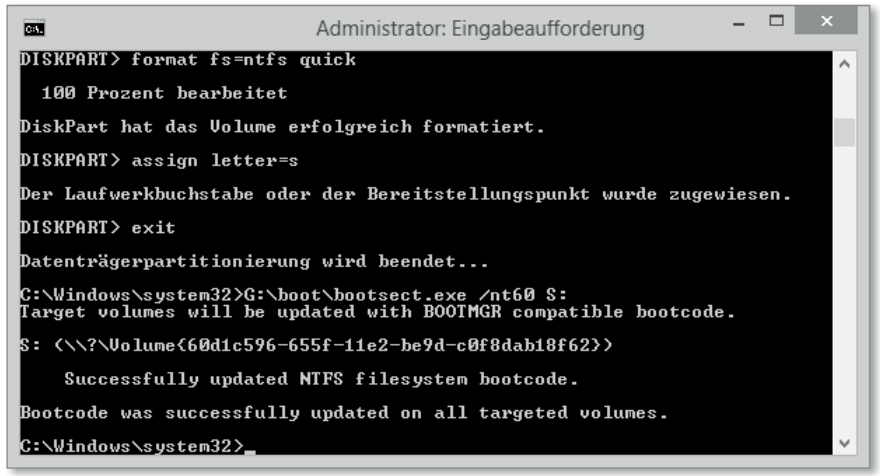


Abbildung 2.22 Der USB-Stick wird mithilfe des Programms »bootsect.exe« angepasst.

2.12.3 Hyper-V Server 2012 ohne Domäne verwalten

Bei der Nutzung eines *Hyper-V-Servers* müssen Sie sich im Klaren darüber sein, dass Sie ohne Dritthersteller-Programme keine Möglichkeit einer lokalen Administration der VMs haben. Eine weitere Einschränkung ist, dass Sie das System nicht als Mitglied eines Failover-Clusters verwenden können, da hier eine Domänenmitgliedschaft zwingend erforderlich ist.

Zur Administration muss ein Windows 8-Client oder ein anderer Server genutzt werden, auf dem ein Hyper-V-Manager vorhanden ist. Da sich die Systeme teilweise nicht in derselben Domäne oder überhaupt nicht in einer Domäne befinden, ist die Herstellung einer Verbindung zu diesen Systemen nicht einfach. Man kann diese trotzdem herstellen, wenn man die richtigen Kniffe kennt. Diese möchten wir Ihnen nun vorstellen.

Einstellungen überprüfen

Wenn Sie sich auf dem Hyper-V-Server in der Server-Konfiguration befinden, können Sie mit Option 4) Remoteverwaltung konfigurieren einstellen, ob eine Verwaltung von extern möglich ist. Standardmäßig ist dies in der aktuellen Version der Fall.

Falls die Remote-Verwaltung deaktiviert ist, können Sie diese mit Auswahl der Option 4) und einer Bestätigung mit Option 1) wieder aktivieren (siehe Abbildung 2.23).

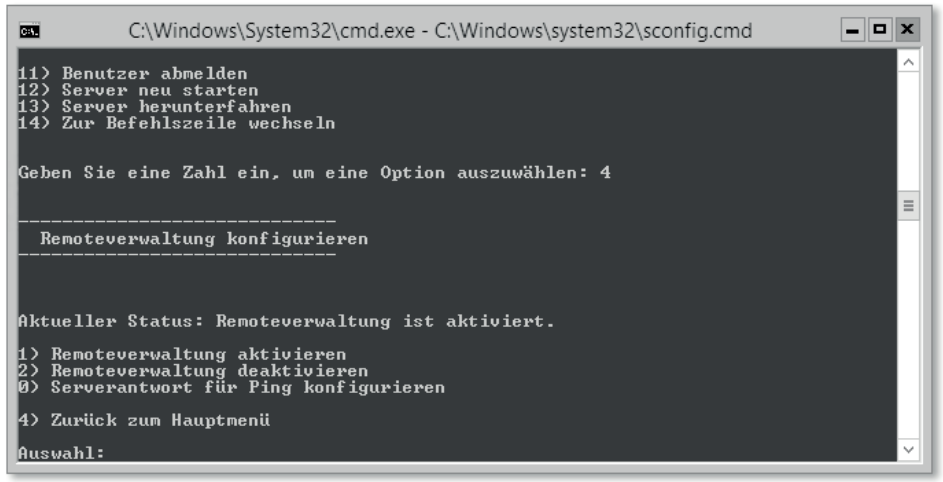


Abbildung 2.23 Option zur Aktivierung oder Deaktivierung der Remote-Verwaltung eines Hyper-V Servers 2012

Freigabe konfigurieren

Wenn Sie nun eine Verbindung zu Ihrem Hyper-V Server 2012 aufbauen, wird dieser Versuch durch eine Fehlermeldung beendet. Sie müssen weitere Schritte unternehmen, um erfolgreich eine Verbindung aufbauen zu können.

- Öffnen Sie auf Ihrem Client eine administrative PowerShell, und geben Sie den folgenden Befehl ein:

  ```
  Set-Item WSMan:\localhost\Client\TrustedHosts -Value ↵
  Name_Ihres_Hyper-V-Server –Concatenate
  ```

- Navigieren Sie auf Ihrem Client in der Systemsteuerung zu System und Sicherheit • Verwaltung • Komponentendienste, klicken Sie unter Computer rechts auf Arbeitsplatz, und wählen Sie die Option Eigenschaften. Auf dem Karteireiter COM-Sicherheit klicken Sie unter Zugriffsberechtigungen auf Limits bearbeiten... und geben der Gruppe ANONYMOUS-ANMELDUNG das Recht Remotezugriff.

Sie können nun eine Verbindung zu Ihrem Hyper-V-Server aufbauen und remote eine Administration durchführen (siehe Abbildung 2.24). Die Firewall muss sowohl auf dem Client als auch auf dem Server nicht angepasst werden, die entsprechenden Freigaben sind standardmäßig aktiviert.

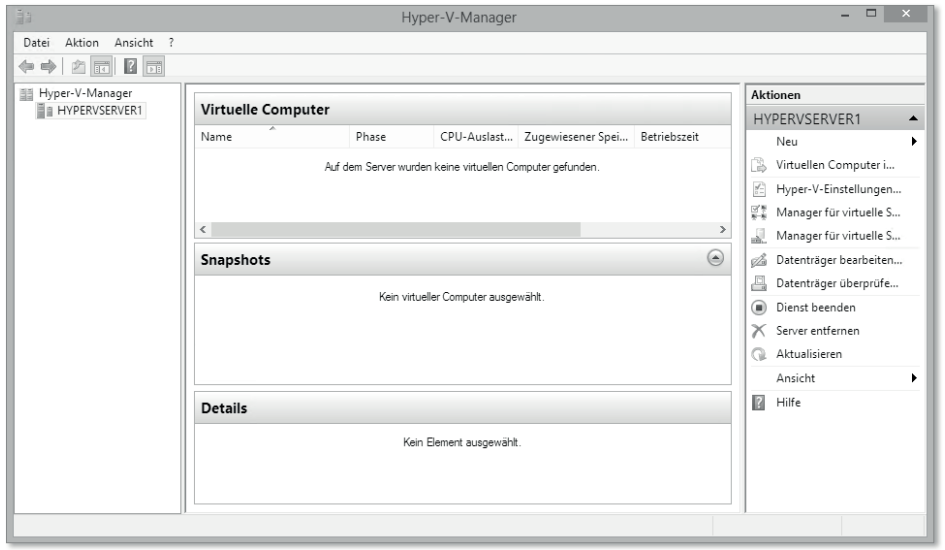


Abbildung 2.24 Administration eines Hyper-V Servers 2012 mit dem Hyper-V-Manager auf einem Windows 8-Client

Das Ding mit der Namensauflösung

Achten Sie bei der Nutzung dieser Art von Administration darauf, dass Sie immer mit den Namen der jeweiligen Systeme arbeiten. Registrieren Sie die Namen sowie IP-Adressen, wenn möglich, auf einem DNS-Server in Ihrer Umgebung, um eine »einfache« Art der Auflösung zu erhalten. Falls dies nicht möglich ist, können Sie die Daten in die Hosts-Datei unter *C:\Windows\system32\drivers\etc* eintragen, um eine Auflösung auch ohne DNS zu ermöglichen. Achten Sie bei dieser Variante allerdings darauf, dass Sie die Daten ändern, wenn Sie die IP-Adressen oder Namen der Systeme ändern.

2.12.4 Dritthersteller-Tools zur Verwaltung nutzen

Neben der Administration über ein anderes System gibt es auch die Möglichkeit, auf dem Hyper-V-Server selbst ein Programm zur Administration zu installieren. Der wohl bekannteste Vertreter dieser Art ist das Programm *5nine Manager for Hyper-V* und wird von der Firma 5nine vertrieben. Es gibt sowohl eine kostenfreie als auch eine kostenpflichtige Variante. In der kostenfreien Variante können Sie Ihre VMs anpassen und »von außen« administrieren, eine Verbindung mit der Konsole und eine lokale Administration des Systems ist nur in der kostenpflichtigen Variante möglich.

Nachdem Sie das Paket heruntergeladen und entpackt haben, müssen Sie die Datei *core-preinstall.bat* ausführen. Diese installiert bei Bedarf alle benötigten Features. Führen Sie danach die Datei *59Manager.exe* aus, um die Installation zu starten. Nach dem erfolgreichen Setup können Sie das Programm starten, indem Sie im Hauptverzeichnis (standardmäßig wird das Programm nach *C:\Program Files\5nine\59Manager for Hyper-V* installiert) die Datei *5nine.Manager.exe* starten. Im daraufhin sich öffnenden Programm können Sie Ihre VMs einsehen und grundlegende Aufgaben erledigen. Abbildung 2.25 zeigt einen Screenshot des Programms direkt nach dem Aufruf.

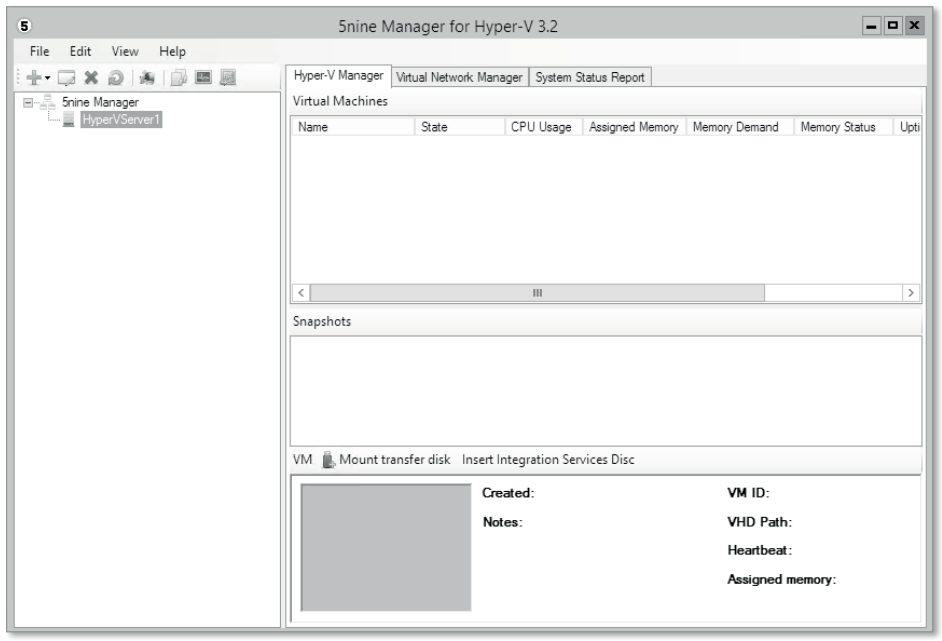


Abbildung 2.25 »5nine Manager for Hyper-V« auf einem Hyper-V Server 2012

Das Programm kann nicht nur auf einem Hyper-V-Server oder der Core-Variante eines Windows Servers ausgeführt werden. Wenn Sie Gefallen an dem Programm finden, können Sie die Administration auch komplett auf dieses Programm verlagern.

2.12.5 Hyper-V Server 2012 R2

Mit dem Release von Windows Server 2012 R2 ist natürlich auch wieder eine neue Version des Hyper-V-Servers erschienen. Die mittlerweile vierte Version kann wie gewohnt von Microsoft kostenlos heruntergeladen und eingesetzt werden. Nach der Installation steht Ihnen wie gewohnt kein Desktop zur Verfügung, dafür beinhaltet der Hyper-V-Server alle technischen Funktionen und Eigenschaften, die im Windows Server 2012 R2 Standard oder Datacenter enthalten sind (abgesehen von der automa-

tischen Aktivierung der Gastbetriebssysteme, diese Funktion ist nur im Windows Server 2012 R2 Datacenter enthalten). Sie können die kostenfreie Version z. B. verwenden, um Ihre Replikation um einen weiteren Standort zu erweitern.

2.13 Hyper-V auf dem Client

Unter Windows 8 in den Versionen *Pro* und *Enterprise* ist Hyper-V erstmalig auch in einem Client-Betriebssystem von *Microsoft* enthalten. Somit ist es möglich, auf dem eigenen PC oder Notebook virtuelle Systeme mithilfe der Hyper-V-Technologie zu betreiben.

2.13.1 Anforderungen und Einschränkungen

Die Funktion der Virtualisierung mit Hyper-V unter Windows 8 ist nur in den Versionen Pro und Enterprise möglich. Eine weitere Einschränkung besteht darin, dass der Prozessor die Funktion *Second Level Address Translation* (SLAT) beherrschen muss, da sonst eine Installation der Funktion nicht möglich ist.

Im Funktionsumfang wurde Hyper-V ebenfalls leicht beschränkt. Mit einem *Hypervisor* auf Client-Basis ist keine komplette Live-Migration einer VM möglich, lediglich eine Verschiebung der Dateien einer VM (Storage-Migration) ist erlaubt.

Dies sind die einzigen beiden Einschränkungen, alle anderen Funktionen, die man mit Windows Server 2012 nutzen kann, sind auch im Client vorhanden.

2.13.2 Installieren und Nutzen

Die Installation von Hyper-V erfolgt über Systemsteuerung • Programme • Programme und Features • Windows-Features aktivieren oder deaktivieren. In dem Fenster mit den verfügbaren Features können Sie unter Hyper-V das Feature *Hyper-V-Plattform* installieren. Falls diese Option ausgegraut ist, können Sie mit dem Mauszeiger über das Feature fahren und sehen eine kurze Information mit dem Grund, warum die Hyper-V-Plattform nicht installiert werden kann. In den meisten Fällen wird dies daran liegen, dass die CPU nicht den Anforderungen entspricht. Die Fehlermeldung lautet in diesem Fall: *Hyper-V kann nicht installiert werden. Der Prozessor hat keine SLAT-Fähigkeiten (Second Level Address Translation)*.

Ein System lässt sich sehr einfach auf Funktionalität mit Hyper-V hin testen. Hierzu müssen Sie in einer Eingabeaufforderung den Befehl `systeminfo` eingeben. Nach einem kurzen Moment werden Ihnen einige Informationen zu Ihrem System angezeigt, unter anderem, ob Ihr System den Anforderungen entspricht. Insgesamt werden im Bereich Anforderungen für Hyper-V vier Eigenschaften abgefragt:

- Erweiterungen für den VM-Überwachungsmodus
- Virtualisierung in Firmware aktiviert
- Adressübersetzung der zweiten Ebene
- Datenausführungsverhinderung verfügbar

Steht hinter allen vier Eigenschaften ein Ja, können Sie Hyper-V auf Ihrem Gerät nutzen. Ist mindestens eine der Optionen mit einem Nein versehen, lässt sich Hyper-V nicht nutzen.

Neben der Hyper-V-Plattform können Sie die *Hyper-V-Verwaltungstools* installieren. Bei der Aktivierung von Hyper-V-Plattform werden Sie gefragt, ob diese Tools automatisch mit installiert werden sollen, sie können aber auch separat installiert werden, zum Beispiel, wenn Sie über Ihren Client einen oder mehrere Hosts mit Hyper-V administrieren möchten. Die Gruppe Hyper-V-Verwaltungstools enthält die Hyper-V-GUI-Verwaltungstools und das Hyper-V-Modul für Windows PowerShell (siehe Abbildung 2.26).

Wenn Sie die Hyper-V-Plattform zur Installation ausgewählt und bestätigt haben, fordert Sie das System zu einem Neustart auf. Nachdem Ihr System mehrfach neugestartet ist, kann Hyper-V genutzt werden. Im Startmenü befinden sich zwei neue Symbole: Hyper-V-Manager und Hyper-V-Verbindung mit virtuellem Computer.

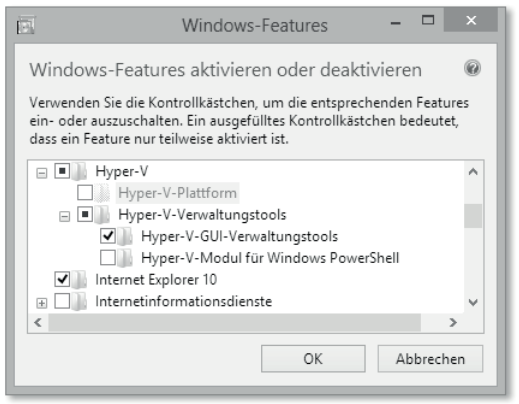


Abbildung 2.26 Windows-Features aktivieren oder deaktivieren, in der Abbildung die »Hyper-V-Plattform« und die »Hyper-V-Verwaltungstools«

Nach dem ersten Aufruf des Hyper-V-Managers wird versucht, eine Verbindung mit dem Hyper-V-Dienst herzustellen, dies ist allerdings nur dann erfolgreich, wenn Sie als Administrator an dem System angemeldet sind. Bei der Verwendung eines Benutzerkontos ohne Administrationsrechte erhalten Sie die folgende Meldung:

Sie besitzen nicht die erforderliche Berechtigung für diese Aufgabe. Wenden Sie sich an den Administrator der Autorisierungsrichtlinie für den Computer »localhost«.

Dieses Problem können Sie umgehen, indem Sie sich entweder als Administrator an Ihrem System anmelden, den Hyper-V-Manager als Administrator starten oder in der Verwaltung Ihres Systems das betreffende Benutzerkonto in die lokale Gruppe HYPER-V-ADMINISTRATOREN aufnehmen (siehe Abbildung 2.27). Mitglieder dieser Gruppe erhalten uneingeschränkten Zugriff auf alle Funktionen von Hyper-V, ohne direkt Administrator des gesamten Betriebssystems zu werden.

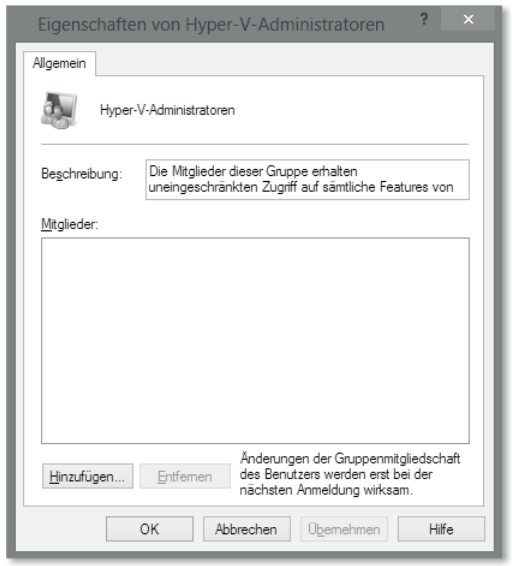


Abbildung 2.27 Eigenschaften der lokalen Gruppe »Hyper-V-Administratoren« auf Windows 8 Enterprise

2.13.3 Windows Server 2012 remote verwalten

Mit Windows 8 und den installierten *Hyper-V-GUI-Verwaltungstools* ist es möglich, einen oder mehrere Windows Server 2012-Hosts mit aktivierter Hyper-V-Rolle zu administrieren. Bisher war hierfür die Installation der *Remoteserver-Verwaltungstools* (RSAT) notwendig, unter Windows 8 ist die Installation nur noch erforderlich, wenn Rollen oder Features administriert werden sollen, die nicht in Windows 8 enthalten sind. Da dies bei Hyper-V nicht der Fall ist, muss in der Systemsteuerung lediglich das Feature HYPER-V-GUI-VERWALTUNGSTOOLS aktiviert werden.

Der Zugriff auf einen Host per Hyper-V-Manager ist standardmäßig nur Domänen-Administratoren erlaubt, allerdings gibt es auf den Server 2012-Systemen ebenfalls eine Gruppe *Hyper-V-Administratoren*. Hier können Sie bei Bedarf Benutzer

eintragen, die keine domänenweiten Administratoren sind, aber trotzdem das Hyper-V-Management übernehmen sollen.

Die Verwaltung von *Hyper-V*-Hosts mit den Betriebssystem-Versionen Windows Server 2008 und Windows Server 2008 R2 ist nicht möglich, bei einem Zugriff auf solch ein System erhalten Sie diese Fehlermeldung:

Mit dieser Version von Hyper-V-Manager können keine Server mit Hyper-V unter Windows Server 2008 oder Windows Server 2008 R2 verwaltet werden.

Interessanterweise können Sie von einem Windows Server 2008 R2 über den Hyper-V-Manager einen Windows Server 2012 administrieren. Hierbei werden allerdings alle Funktionen ausgeblendet, die dem Windows Server 2008 R2 noch nicht bekannt sind. Diese Art der Administration ist nicht unterstützt, daher empfiehlt sich dies nicht.

2.14 Zusammenfassung

Dieses Kapitel hat Ihnen einen Einblick in die Struktur von Virtualisierungslösungen gegeben. Dieses Wissen ist wichtig, um verstehen zu können, in welchem komplexen Zusammenhang viele der alltäglichen Aufgaben stehen. Der Vergleich zwischen Hyper-V in den früheren Versionen und unter Windows Server 2012 zeigt, in welchem Umfang Microsoft die eigene Lösung erweitert und verbessert hat. Neben einem kurzen Einblick in die Administration per PowerShell kennen Sie nun ebenfalls die Möglichkeiten, einen Hyper-V-Server zu betreiben und Hyper-V unter Windows 8 einzusetzen.

Kapitel 4

Host-Farmen und Verfügbarkeit

Windows Server 2012 Hyper-V releases us from the traditional boundary of storage, host, and cluster, enabling our workloads to move where we want them, when we want them, without affecting our service level agreements to our customers. It has also made disaster recovery possible for all by building in Hyper-V Replica.

Aidan Finn, MVP Virtual Machine

Die Idee der Hochverfügbarkeit für IT-Systeme ist nicht neu. Bereits seit vielen Jahren stehen zahlreiche Lösungsansätze für die Erhöhung der Ausfallsicherheit und der Leistungssteigerung von IT-Systemen zur Verfügung. Es haben sich zahlreiche Lösungen am Markt etabliert. Angefangen bei der Redundanz auf Server-Ebene mithilfe von zwei Netzteilen und ausfallredundanten Festplattensystemen über Server, die sich über Netzwerkverbindungen oder spezielle Speichernetze replizieren und synchron halten, bis hin zu redundanten Rechenzentren, die sich an verschiedenen Orten der Erde befinden. Dieses Kapitel konzentriert sich auf das Thema Host-Farmen mit dem Ziel, zuverlässige Umgebungen für virtuelle Maschinen unter Hyper-V zur Verfügung zu stellen.

4.1 Warum ist Verfügbarkeit ein Thema?

Keine Frage, sicher fallen Ihnen noch viele weitere Beispiele ein, die die Abhängigkeit moderner Geschäftsprozesse von der IT belegen. Das gilt schon lange nicht mehr nur für »technische« Unternehmen, sondern für alle Wirtschaftsbereiche. Der Grad der Rechnerunterstützung mag unterschiedlich sein, doch nirgends geht es mehr ganz ohne.

Durch Virtualisierung hoffen viele Verantwortliche, die Abhängigkeit zu verringern, denn schließlich läuft ein virtueller Server unabhängig von der konkreten Hardware, in der es viele Teile gibt, die ausfallen können. Tatsächlich aber führt die Virtualisierung von Servern zunächst zu einer höheren Ausfallwahrscheinlichkeit. Wenn in einer herkömmlichen Umgebung ein einzelner Server ausfällt, ist dessen Funktion nicht mehr nutzbar, die anderen Rechner arbeiten aber weiter. Sobald Server-Virtualisierung hinzukommt, hat der Ausfall einer einzelnen Server-Hardware ganz andere

Folgen, denn das betrifft nicht mehr nur einen Server, sondern fünf, zehn oder noch mehr, die virtuell auf dieser Hardware laufen.

Steht ein einzelnes System nicht zur Verfügung, kann dies gravierende Folgen haben, die dem Unternehmen mehr schaden als zuvor. Die Abhilfe dafür ist Redundanz: Nicht ein einzelnes System ist zuständig für eine bestimmte Aufgabe, sondern mehrere, die füreinander einspringen können. Wer sich mit dem strategischen Einsatz von Virtualisierung in seinem Unternehmen beschäftigt, wird daher fast zwangsläufig schnell zu anspruchsvollen Aufbauten gelangen, die mit Server-Farmen, Clustering oder Netzwerkspeicher arbeiten. Noch vor wenigen Jahren wäre das im Mittelstand kein Thema gewesen, heute ist es fast üblich.

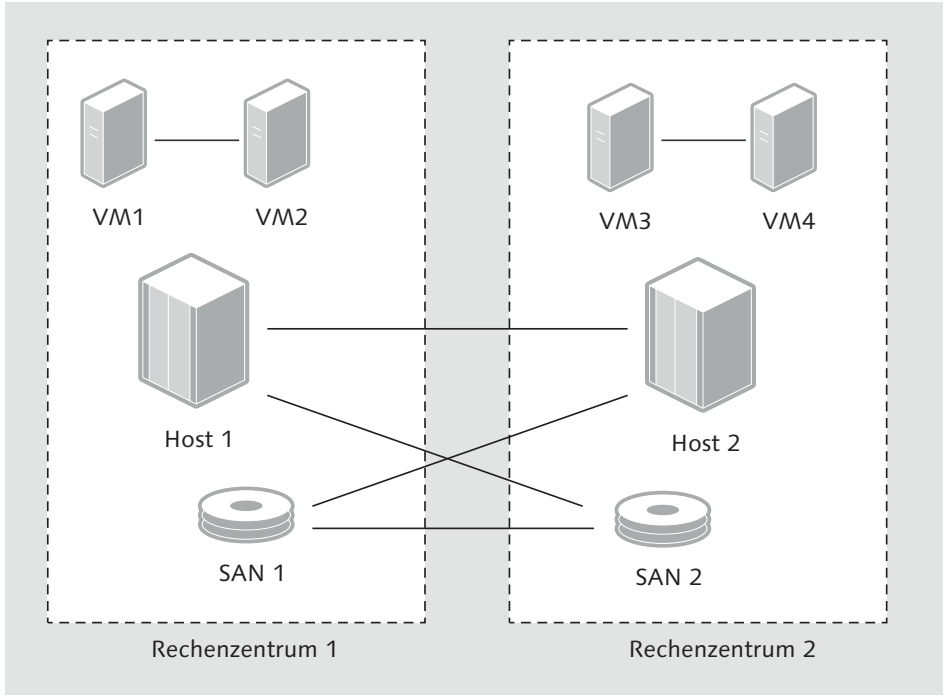


Abbildung 4.1 Clustering auf mehreren Ebenen: Bei sehr hohen Anforderungen an den ausfallsicheren Betrieb lassen sich viele Redundanzen einrichten.

4.1.1 Was ist überhaupt Verfügbarkeit?

Der etwas sperrige Begriff der »Verfügbarkeit« hat in der IT eine spezielle Bedeutung. Kurz gefasst, bezeichnet man damit die Möglichkeit, auf einen Dienst oder Datenbestand zuzugreifen. Die Betonung liegt dabei auf »einen« Dienst oder Datenbestand: Die Anforderung nach Verfügbarkeit bezeichnet nicht das gesamte Netzwerk und steht auch nicht allgemein im Raum, sondern es geht um ganz bestimmte Komponenten. Bei der Contoso AG beispielsweise ist der Speicherbereich, auf dem die

IT-Abteilung ISO-Dateien zur Software-Installation ablegt, sicher weniger kritisch als die Datenbank des ERP-Systems.

Welche IT-Komponente wichtig ist und für welche Teile des Netzwerks weniger hohe Anforderungen gelten, leitet sich aus den Geschäftsprozessen ab. Die Frage ist: Auf welche Elemente ist das Unternehmen so angewiesen, dass ein längerer Ausfall der Nutzung spürbare Schäden hervorrufen würde?

Diese Frage ist gar nicht einfach zu beantworten. In vielen IT-Abteilungen wird die Entscheidung daher eher nach der Frage getroffen: Wann beginnt es im Helpdesk ungemütlich zu werden, weil das Telefon so oft klingelt? Zwischen beiden Fragen mag zwar durchaus ein Zusammenhang bestehen, doch ist nur die erste Formulierung wirklich geeignet, Gegenmaßnahmen zu definieren und Budgets zu verhandeln.

Verfügbarkeiten gibt man oft in Prozentwerten an. Dabei stellt man die Zeit, in der der Zugriff auf einen bestimmten Dienst besteht, ins Verhältnis zur gesamten Zeit. War also innerhalb von zehn Stunden die Datenbank für zehn Stunden nutzbar, lag die Verfügbarkeit bei 100 Prozent. Wäre sie eine Stunde offline gewesen, hätte die Verfügbarkeit 90 Prozent betragen.

Besonders im Marketing für hochpreisige IT-Komponenten begegnen Ihnen solche Prozentwerte sehr oft. In Tabelle 4.1 sehen Sie, was typische Werbeversprechen tatsächlich bedeuten würden. Als Königsklasse gilt dabei »Five-Nine«, das heißt 99,999 Prozent Verfügbarkeit – auf ein Jahr bezogen nur wenig mehr als fünf Minuten Ausfallzeit.

Prozentwert	Ausfallzeit pro Jahr
99 %	3,65 Tage
99,9 %	über 8 Stunden
99,99 %	eine knappe Stunde
99,999 %	5 Minuten

Tabelle 4.1 Prozentangaben für Verfügbarkeit und was sie auf ein Jahr bezogen bedeuten

Solche Zahlenspiele nützen Ihnen aber in der Praxis herzlich wenig. Die meisten Unternehmen etwa beeinträchtigt es überhaupt nicht, wenn ein Server die ganze Nacht ausfällt, auch wenn die rechnerische Verfügbarkeit dadurch ganz schlecht aussieht. Wichtig ist, dass die IT-Administration die Systeme am nächsten Morgen schnell wieder bereitstellen kann. Die meisten Unternehmen wären mit ihrer eigenen Organisation auch gar nicht in der Lage, die vier oder fünf »Neunen« zu erreichen, selbst wenn alle Lieferanten das zusagen: Ganz banal wäre es beispielsweise

notwendig, dass jemand mitten in der Nacht das per Eildienst gelieferte Ersatzteil entgegennehmen oder den Technikern des Service-Partners den kontrollierten Zugang zum Server-Raum ermöglichen kann.

Nehmen Sie die mathematischen Angebereien der kommerziellen Anbieter daher als das, was sie sind, nämlich reine Werbeaussagen. Im echten Leben können Sie mit einem hoch motorisierten Sportwagen auch nur selten 250 Stundenkilometer schnell fahren, der Normalverkehr spielt sich zwischen 30 und 120 Stundenkilometern ab, und selbst davon ist der größte Teil der langsame Stadtverkehr. In diesen Standardsituationen muss das System sich bewähren. Und genauso ist es auch für den Aufbau Ihrer IT wichtig, dass er zu Ihrem Unternehmen und seinen Geschäftszielen passt.

4.1.2 Wie abhängig sind wir wirklich?

Es ist also offenbar wichtig, über die konkreten Anforderungen des eigenen Unternehmens nachzudenken. Die Aufgabe ist nicht einfach, und deshalb ist sie auch so unbeliebt. Denn sie erfordert, nimmt man sie ernst, dass man mit verschiedenen Kollegen und Hierarchieebenen spricht, von denen nur wenige einen IT-technischen Hintergrund haben. Aus Sicht der Geschäftsprozesse ist die IT ein Werkzeug oder eine Infrastruktur, die bestimmte technische Grundlagen für die »eigentlichen« Aktivitäten des Unternehmens bereitstellt. Selbstverständlich sehen wir in der IT das etwas anders – dürfen wir auch, aber das steht in diesem Moment nicht im Mittelpunkt.

Um Anforderungen herauszuarbeiten, auf deren Grundlage Sie ein Verfügbarkeits-Design für Ihre IT aufbauen können, müssen verschiedene Stellen des Unternehmens eine durchaus komplexe Frage beantworten, die wir bereits kurz erwähnt haben: Wie lange kann ein bestimmter IT-Dienst oder -Datenbestand als Ausnahme ausfallen, ohne dass es für das Unternehmen kritisch wird? Dabei bedeutet »kritisch« nicht, dass es unbequem wird, sondern es bezieht sich tatsächlich auf messbare Schäden für das Unternehmen. Je nach Geschäftsbetrieb kann es sich dabei um den Verderb frischer Ware handeln, um entgangene Aufträge oder um Image-Schäden.

Halten Sie sich dabei vor Augen, dass es »die eine« Verfügbarkeit nicht gibt. Diese Fragen sind für jedes Unternehmen und in der Regel sogar für jeden einzelnen Geschäftsprozess unterschiedlich zu beantworten. Manche Firmen haben mehrere Prozesse, die spätestens nach einigen Stunden wieder funktionsfähig sein müssen, bei anderen gibt es nur eine zentrale Komponente, die aber erst nach mehreren Tagen Ausfall wirklich kritisch wird, weil es solange noch Möglichkeiten gibt, um einen Schaden herum zu improvisieren. Dass dies dann zu Aufwand und Nacharbeiten führt, ist zunächst nicht relevant, solange sie geleistet werden können.

In der Klärung dieser Fragen hat es sich bewährt, zunächst mit den Fachabteilungen zu diskutieren, welche IT-Komponenten, -Dienste und -Datenbestände sie überhaupt benötigen. Mit der dabei entstandenen Liste können Sie theoretisch durchspielen, was geschehen würde, wenn das jeweilige Element nicht zur Verfügung stünde. Konzentrieren Sie sich dabei stets auf die Frage: Wann entsteht ein ernsthafter Schaden für das Unternehmen?

Auf diese Weise kann eine Matrix für die Anforderungen entstehen, die Sie meist in verschiedene Verfügbarkeitsklassen gliedern können. Es mag beispielsweise Komponenten geben, die nach spätestens einem halben Arbeitstag wieder laufen müssen, andere müssen am nächsten Tag wieder erreichbar sein, und auf wieder andere Elemente kann die Firma zur Not auch mehrere Tage verzichten. Eine so strukturierte Matrix könnte so aussehen wie das Beispiel in Tabelle 4.2. Dabei handelt es sich ausdrücklich nur um ein Beispiel – die jeweiligen Verfügbarkeitsklassen und die Zuordnung werden bei Ihnen sicher anders aussehen.

Dienst	Klasse 1: 4 Stunden	Klasse 2: 8 Stunden	Klasse 3: 3 Tage
ERP-System	✓		
E-Mail		✓	
Data Warehouse			✓
Dateiserver	✓		

Tabelle 4.2 Matrix für Verfügbarkeitsklassen (nur ein Beispiel – sowohl die Klassen als auch die Zuordnung können in Ihrem Fall anders sein)

4.1.3 Was ist eigentlich ein Ausfall?

Allzu oft sind wir als IT-Experten verleitet, einen Ausfall als ein plötzliches, unerwartetes Ereignis anzusehen, das die Qualität eines Unfalls hat. Da ist der Verschleiß von Festplatten, der zur ungünstigsten Zeit einen Headcrash oder das Versagen des Motors nach sich zieht, oder ein elektrischer Fehler in einem komplexen Bauteil wie einem RAM-Modul oder einem Controller, der den Server als Ganzen außer Funktion setzt. Genau auf diese Vorfälle setzt auch nahezu das gesamte Herstellermarketing. Die Antwort auf solche Befürchtungen besteht dann meist in Hardware-Redundanz – man setzt also zwei oder mehr Elemente ein, um den Ausfall eines einzelnen Elements überstehen zu können.

Es gibt aber noch eine zweite Kategorie von Ausfällen, die einem erst bei einem sorgfältigeren Blick bewusst wird: Nahezu jeder Wartungsvorgang setzt ein System außer Betrieb. Dabei ist es zunächst sekundär, ob es sich um die Erweiterung der Hardware

handelt, um den Austausch eines defekten Bauteils (das aufgrund von Redundanzen selbst keinen Ausfall verursacht hat) oder um Software-Updates. Solche Vorgänge haben den unbestreitbaren Vorteil, dass sie nicht plötzlich und überraschend auftreten, sondern sich in der Regel planen lassen. Man spricht hier auch von »geplanten Ausfällen« oder, bezogen auf die Prozesse, von »geplanter Downtime« im Gegensatz zur »ungeplanten Downtime«, die durch die beschriebenen Unfälle auftritt.

In der Praxis spielt bei Systementwürfen allzu oft nur die »ungeplante Downtime« eine Rolle. So gibt es viele Hersteller von anspruchsvollen (und teuren) Geräten, die im Kleingedruckten darauf hinweisen, dass die angegebenen Verfügbarkeitswerte (mit vier oder gar fünf »Neunen«, versteht sich) sich nur auf ungeplante Ausfälle beziehen, dass diese Werte aber gleichzeitig nur erreichbar sind, wenn man das System regelmäßig wartet – was wiederum Downtime bedeutet, die aber nicht gewertet wird.

Seien Sie in diesem Zusammenhang auch aufmerksam, wenn Sie für Ihre Infrastruktur externe Dienste mit zugesagten Verfügbarkeiten nutzen. Nicht selten verbergen deren Anbieter in ihren Bedingungen überraschende Klauseln, die vielleicht Ihren Zielen widersprechen. So gibt es beispielsweise Cloud-Anbieter, die alle Ausfälle unterhalb von fünf Minuten pro Stunde gar nicht erst zählen.

Für Ihr System-Design kann diese Unterscheidung Folgen haben – das muss aber nicht notwendig so sein, zumindest nicht für jede Komponente. So ist es durchaus möglich, beispielsweise ein virtuelles Exchange-System so auszulegen, dass es nicht nur bei ungeplanter Downtime durch Hardware-Ausfälle weiterläuft (dazu eignet sich etwa ein Failover-Cluster für Hyper-V), sondern dass auch geplante Downtime durch Updates für die Anwender keinen Nutzungsausfall bedeutet. Wie Sie vielleicht wissen, dauern gerade Exchange-Updates oft sehr lange. Wenn Sie für Exchange auf der Dienstebene einen Failover-Cluster einrichten, können Sie jeden Teil des Clusters unabhängig vom anderen aktualisieren, und der Dienst als solcher läuft weiter.

In vielen Unternehmen allerdings ist es gar kein ernsthaftes Problem, wenn alle paar Wochen nach Ankündigung ein Dienst wegen Wartung nicht zur Verfügung steht. Ein Failover-Cluster ist dann vielleicht gar nicht nötig, um ungeplante Downtime zu überbrücken. Hier kann ein Unternehmen durchaus Geld sparen, wenn es seine Anforderungen realistisch einschätzt.

Es gibt noch eine weitere Dimension von IT-Ausfällen, die Sie betrachten sollten. Die Zeit *nach* einem Ausfall haben viele Verantwortliche nämlich nicht im Blick, dabei kann sie noch einmal erhebliche Aufwände nach sich ziehen. So ist das Umschalten von einem System auf ein Notfallsystem die eine Sache, die vielleicht entscheidend zum Weiterlaufen der Geschäftsprozesse beiträgt. Irgendwann ist dann aber das »Hauptsystem« repariert, und der Betrieb muss zurückgeschaltet werden. Manchmal stellt sich dies als unerwartet komplexer Vorgang dar, der seinerseits (geplante) Downtime erfordert.

4.1.4 Wenn Redundanz zum Problem wird

In der IT haben wir uns daran gewöhnt, das Prinzip der Redundanz zu nutzen, wenn wir Ausfällen vorbeugen möchten. Wir verstehen darunter, dass wir wichtige Komponenten oder Daten nicht nur einmal vorhalten, sondern zwei- oder mehrfach, damit bei einem Ausfall nicht gleich alles verloren ist. So hilfreich dieser Grundsatz ist, so schnell kann er selbst zum Problem werden.

Es ist dabei aufschlussreich, dass der lateinische Ursprung des Begriffs Redundanz für »Überfluss« steht – es ist also zu viel da. Tatsächlich kann das Streben nach Ausfallsicherheit in der IT paradoxerweise dafür sorgen, dass Ausfälle nicht seltener, sondern wahrscheinlicher werden.

Ein Blick in die Mathematik kann dies illustrieren. Ein Wert, der die Zuverlässigkeit technischer Geräte angeben soll, heißt »Mean Time Between Failures (MTBF)« und gibt an, wie groß statistisch der zeitliche Abstand zwischen zwei wesentlichen Störungen ist (siehe Abbildung 4.2).

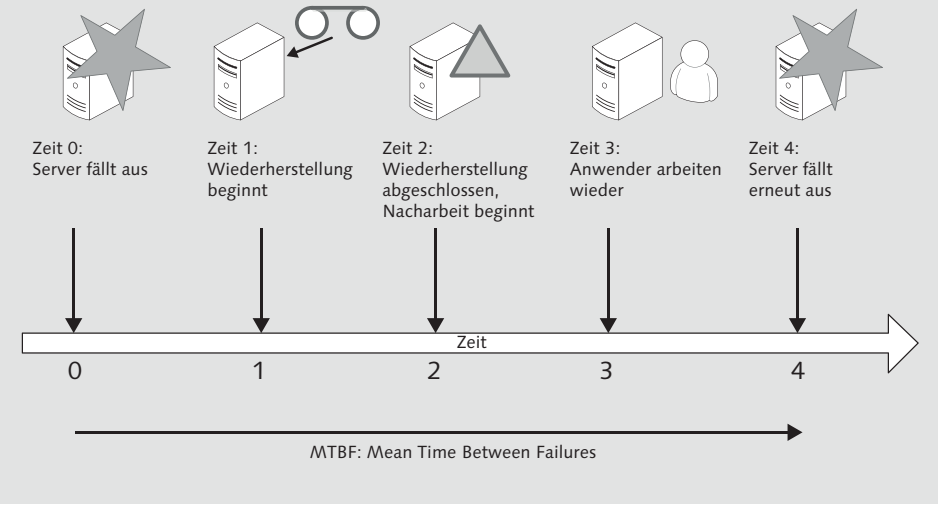


Abbildung 4.2 Die »Mean Time Between Failures« (MTBF) gibt als statistischer Wert den zeitlichen Abstand zwischen zwei Ausfällen an.

Hat man eine Komponente mit einer sehr hohen MTBF von 20 Jahren, mag man sich in der IT auf der sicheren Seite sehen. Bei der zweiten gleichartigen Komponente muss man aber innerhalb derselben Zeit schon mit zwei Ausfällen rechnen – und bei zehn Geräten tritt rechnerisch alle zwei Jahre eine Störung auf. Da einerseits IT-Equipment aus vielen komplexen und teils stark beanspruchten Bauteilen besteht und andererseits die meisten MTBF-Werte viel niedriger sind, besteht in realen

Umgebungen mit hoher Redundanz ein beträchtliches Gesamtrisiko, dass es zu einem kritischen Ausfall kommt (siehe Abbildung 4.3).

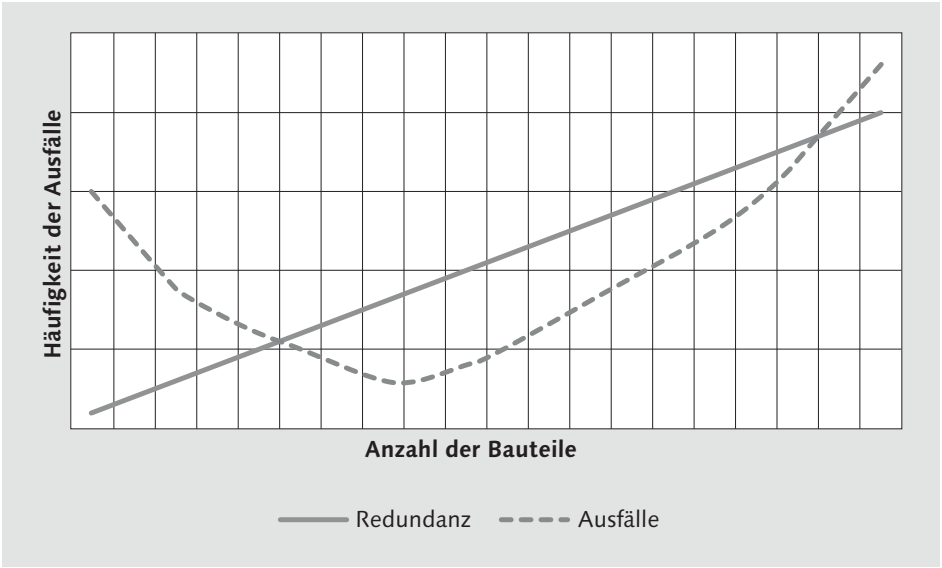


Abbildung 4.3 Nutzen und Last der Redundanz: Gegen den Ausfall eines Bauteils kann man sich schützen, indem man zwei Bauteile vorsieht. Ab einer gewissen Größe wird die Redundanz aber selbst zum Problem: Je mehr Bauteile beteiligt sind, desto wahrscheinlicher wird ein Ausfall.

Doch auch ein allgemeiner Blick auf ein IT-Netzwerk stützt diese Ansicht. In den letzten Jahren haben auch in mittelständischen und kleineren Unternehmen immer mehr aufwendige Techniken Einzug in die IT gehalten. Nicht zuletzt hat gerade die Virtualisierung für eine erneute Zunahme der Komplexität gesorgt, weil neben anspruchsvollen Servern und Netzwerkkonstrukten auch Speichernetzwerke mit ihren Spezialprotokollen und Techniken wie Zoning, MPIO oder LUN-Reservierungen dazugehören.

Das schon kurz erwähnte »verschachtelte Clustering«, bei dem nicht nur Host-Cluster betrieben werden, sondern innerhalb der VM-Farm auch noch Gast-Cluster für Ausfallsicherheit sorgen, erhöht die Unübersichtlichkeit noch einmal deutlich. Nicht ohne Grund schränken viele Hersteller für solche rekursiven Aufbauten den Support ein. Auch die Verantwortlichen in den Anwenderunternehmen stehen allzu oft ratlos da, wenn es in solchen Umgebungen tatsächlich zu einem Ausfall kommt.

Betrachten Sie vor diesem Hintergrund die Idee der »Vollredundanz«, an der viele Kunden sich orientieren, kommen Sie vielleicht zu differenzierteren Urteilen darüber. Mit diesem Begriff bezeichnen wir hier das Konzept, das gesamte Server-Netzwerk (oder dessen wichtige Teile) vollständig auf zwei getrennte Rechenzentren

aufzuteilen (siehe auch Abbildung 4.1). Im oft zitierten »Fall des Falles« möchte das Unternehmen dann in der Lage sein, von einem Rechenzentrum auf das andere umzuschalten, um nahtlos weiterzuarbeiten.

So bestechend diese Idee ist, geht sie doch von einigen Voraussetzungen aus, die in der Praxis leider nicht immer gegeben sind. Üblicherweise setzt die Planung solcher Spiegel- oder Notfall-Rechenzentren auf der Vorstellung auf, dass das gesamte »Haupt-Rechenzentrum« ausfällt und ein sofortiger und eindeutiger Schwenk »auf die andere Seite« stattfindet. Natürlich kann dies gelingen. Leidvolle Projekterfahrung zeigt aber, dass dies so nicht immer funktioniert. Dabei spielt gar nicht immer technisches oder menschliches Versagen eine Rolle, sondern das Hindernis kann auch darin bestehen, dass es gar keinen Komplettausfall gibt und daher die angemessene Reaktion nicht so einfach festzulegen ist. Der Vorgang könnte also beispielweise so aussehen:

- Nach einem Ausfall einer oder mehrerer Komponenten zeigen sich bei den Anwendern erste Störungen. Applikationen arbeiten nicht wie gewohnt, der Zugriff auf Dateien bricht ab.
- Der Helpdesk registriert die Situation anhand der vermehrt aufgegebenen Support-Tickets und versucht, die Lage einzuschätzen. Da übliche First- und Second-Level-Maßnahmen nicht sofort Abhilfe schaffen, wird nach einem definierten Zeitraum der Third Level hinzugezogen.
- Das Fehlerbild zeigt sich nicht eindeutig. Einzelne Dienste funktionieren, andere nicht. Es gibt Einschränkungen, deren Ursache nicht eindeutig zu klären ist. Die Frage, ob ein Failover auf das Notfall-Rechenzentrum die Lage entspannt, steht im Raum. Da dies jedoch Folgen hat – nicht jeder Dienst steht dann in einer Qualität zur Verfügung, die das normale Tagesgeschäft ermöglicht, und einzelne Datenverluste können beim Umschalten nicht ausgeschlossen werden –, zieht sich die Entscheidung darüber längere Zeit hin.
- Nachdem der Umschaltvorgang von entscheidungsbefugten Mitarbeitern beschlossen ist, müssen die IT-Administratoren die nötigen Schritte identifizieren, um die nötige Handlungssicherheit zu erreichen. Erst danach erfolgt die Umschaltung, die ihrerseits einigen Aufwand erzeugt.
- Da das Notfall-Rechenzentrum nicht alle Dienste vorhält, schafft das IT-Team für einige Funktionen Workarounds. Einige andere Applikationen stehen nicht zur Verfügung.
- Nach der Behebung der Fehler ist die geordnete Rückschaltung auf das Hauptsystem einzuleiten. Hierbei gilt es zu prüfen, ob die Datenbestände des Notfall-Rechenzentrums in das Hauptsystem übernommen werden können oder ob Integrationsaufwände anstehen, die vielleicht nur mit punktuellen Datenverlusten umzusetzen sind. Da die verschiedenen Applikationen unterschiedliche Speichermechanismen verwenden, erfolgt diese Prüfung separat für mehrere Dienste.

4.1.5 Grenzen des Clusterings

Cluster und Host-Farmen sind trotz ihrer hohen Komplexität gut geeignet, um eine Reihe von denkbaren Ausfällen zu überbrücken. In vielen Fällen können die Anwender weiterarbeiten, und das Unternehmen hat in seinen Geschäftsprozessen keine Einschränkungen hinzunehmen. Gleichwohl gibt es auch viele Situationen, in denen ein Cluster nicht helfen kann. Hier sind andere Mechanismen gefordert, um die Auswirkungen gering zu halten.

Einige Beispiele sollen dies näher darstellen. Denken Sie etwa an Fehler in einer Anwendung: Es gibt gar kein Hardware-Problem, sondern die Applikation oder das Betriebssystem der geclusterten Server arbeitet nicht richtig. Ein solches Problem wird wahrscheinlich alle Systeme betreffen, die an einem Cluster beteiligt sind. Auch einen Ausfall vorgelagerter Dienste kann ein Cluster nicht ausgleichen: Wenn im Unternehmen DNS ausfällt, kann der Exchange Server noch so zuverlässig arbeiten – niemand kann darauf zugreifen.

Zu den tückischsten Schäden gehören logische Fehler im Datenbestand. Stellen Sie sich etwa vor, dass ein bislang unentdeckter Bug in einer SQL-Abfrage Ihrer Warenwirtschaft dafür sorgt, dass nach einem harmlosen Knopfdruck alle Kunden dieselbe Kundennummer haben. Das macht sicher den Nummernkreis sehr übersichtlich, aber alle weiteren kaufmännischen Prozesse dürften fehlschlagen. Die Ausfallsicherheit auf der Hardware-Ebene bringt Ihnen in dieser Situation leider gar nichts. Im Gegenteil, wahrscheinlich haben die dort implementierten Spiegelmechanismen dafür gesorgt, dass das logische Problem auf alle beteiligten Systeme übergegriffen hat.

Es müssen aber gar nicht solche Verkettungen unglücklicher (und zugegebenermaßen durchaus unwahrscheinlicher) Umstände sein. Das einfache Löschen oder Ändern von Daten reicht schon aus. Hat ein Anwender bewusst oder versehentlich wichtige Datenbestände manipuliert, ist auch das ein Fall, in dem Hardware-Redundanz nicht hilft. Hier kommt es auf ein Wiederherstellungskonzept an, mit dem auch solche Schäden heilbar sind und das selbst möglichst geringe Folgeschäden verursacht (etwa wenn durch den notwendigen Restore-Vorgang alle anderen Prozesse auf veraltete Daten zurückgeworfen sind).

4.1.6 Das Konzept entscheidet

Wie Sie den vorangegangenen Abschnitten entnehmen können, sind Clustering und technische Redundanz kein Allheilmittel, sondern nur Bausteine in einem Gesamtplan, der eine angemessene Verfügbarkeit von Diensten und Datenbeständen sicherstellen soll. Wie dieser Gesamtplan aussieht, ist immer eine individuelle Frage, die jedes Unternehmen selbst beantworten muss. Selbstredend wird ein einmal entwor-

fener Plan dabei auch nicht für alle Zeiten gelten, sondern er muss sich veränderten Bedingungen anpassen.

Am Anfang eines Verfügbarkeitskonzepts steht immer die Festlegung, welche Anforderungen denn für die einzelnen Applikationen und Daten gelten. Dies zu erarbeiten und festzulegen, ist keine Aufgabe der IT-Abteilung, sondern der Fachabteilungen: Schließlich sind es die Fachkollegen, die ihre Geschäftsprozesse mit der adäquaten IT-Unterstützung erledigen müssen. Das IT-Team kann dabei unterstützen, die Details zu erarbeiten, aber ersetzen kann es die nötige Festlegung in der Fachabteilung nicht. Das Gesamtgerüst der Anforderungen für das Unternehmen festzulegen, ist wiederum eine originäre Aufgabe der Geschäftsführung, denn sie ist als Organisationseinheit (und je nach Unternehmensform auch persönlich) für die Vorsorge verantwortlich, die den Bestand des Unternehmens sichert.

In Abschnitt 4.1.2, »Wie abhängig sind wir wirklich?«, haben wir Ihnen beispielhaft ein einfaches Werkzeug aufgezeigt, das die nötige Diskussion unterstützen kann. Machen Sie sich aber darauf gefasst, dass Sie weitere Hilfsmittel und vor allem viel Zeit benötigen, um die Anforderungen realistisch und verbindlich zu erarbeiten.

Es zeigt sich immer wieder, dass dieser wichtige erste Schritt, sich über Anforderungen und Ziele zu verständigen, in echten Kundenprojekten übergangen oder nur stiefmütterlich behandelt wird. Schon in Kapitel 1, »Einleitung«, haben wir daher darauf hingewiesen, wie elementar unserer Ansicht nach diese Definition ist: Ein Projekt ohne Ziel kann nur scheitern.

Beim Aufbau einer zuverlässigen Virtualisierungsumgebung gibt es zwei Zeitpunkte, an denen Mängel der Zieldefinition sehr deutlich werden. Der erste ist der Moment, in dem Sie als Planer der Umgebung den Kostenplan zusammengestellt haben und bei der Geschäftsleitung das Budget beantragen müssen. Kommt es hier zu hochgezogenen Augenbrauen oder entsetzten Aufschreien, weil die Leitung die Kosten für völlig unangemessen hält, dann waren vielleicht die Anforderungen falsch definiert. Genau wie bei einer Versicherungspolice steigt der Preis für IT-Zuverlässigkeit mit dem Grad der Absicherung. Einen geringeren Preis erzielt man oft nur noch durch ein Absenken des Schutzniveaus. Oft stellt man erst in dieser Phase fest, dass eine geringere Absicherung auch ausreicht – oder anders gesagt: dass man im ersten Schritt die Anforderungen zu hoch angesetzt hat.

Der zweite Zeitpunkt, an dem viele Verantwortliche feststellen, dass die ursprünglichen Ziele falsch oder nicht gut genug definiert waren, tritt kurz nach einem Ausfall ein. Wenn die Vorgesetzten der Meinung sind, dass dieser Schaden nicht hätte eintreten dürfen, kann es durchaus sein, dass sie zu Projektbeginn die Anforderungen falsch definiert und dadurch das Budget nicht ausreichend dimensioniert haben.

Auf der technisch-organisatorischen Ebene ist es wichtig, dass Sie Verfügbarkeit nicht als isoliertes Phänomen betrachten. Nicht ein einzelnes System muss die Hochver-

fügbarkeit herstellen, sondern die ganze Umgebung muss dazu in der Lage sein. Das bedeutet nicht nur, dass Sie neben den redundanten Servern und dem ausfallsicheren Speichersystem auch daran denken, die Switches abzusichern, über die die Anwender die Dienste nutzen. Es beinhaltet durchaus auch das Know-how, das Sie in Ihrem Team benötigen, um die Infrastruktur zu betreiben und auf Fehler zu reagieren.

Notfallvorsorge ermöglicht strukturierte Improvisation

Damit Sie im Fall des Falles nicht konzeptlos dastehen, empfiehlt sich eine Notfallvorsorge. In der Praxis hat es sich dabei bewährt, nicht jede Detailkomponente einzeln durchzuplanen, sondern die Informationen zusammenzustellen, die Sie im Fehlerfall benötigen, um handlungsfähig zu bleiben.

Wie Sie in diesem Abschnitt unseres Buches festgestellt haben, lehrt uns unsere Erfahrung, dass sich Störungen und Ausfälle meist anders darstellen, als man vorher gedacht hat. Meist werden Sie also ohnehin an vielen Stellen von einem Notfallkonzept abweichen müssen, weil die Situation es einfach erfordert.

Sie sollten daher natürlich planen und vor allem dokumentieren. Bauen Sie Ihre Planung und Dokumentation dabei aber so auf, dass Sie auf deren Grundlage gut improvisieren und flexibel handeln können. Sie erleichtern sich dies, wenn Sie da, wo es möglich ist, Funktionen statt Konfigurationen beschreiben. Nur an Stellen, an denen bestimmte Konfigurationsdetails relevant sind, hinterlegen Sie diese.

4.2 Failover-Clustering

In diesem Teil des Kapitels widmen wir uns der Installation und Konfiguration eines Failover-Clusters mit Windows Server 2012. Diese Technik dient auch als Basis der Hochverfügbarkeit für Hyper-V. Zunächst stellen wir Ihnen vor, wie das Failover-Clustering in Windows Server 2012 allgemein arbeitet, denn das Prinzip lässt sich auf sehr unterschiedliche Dienste anwenden. So könnte es in einer Hyper-V-Umgebung durchaus einen Host-Cluster für die Virtualisierung, einen separaten Speicher-Cluster und einen virtualisierten Cluster für Exchange Server oder SQL Server geben.

4.2.1 Überblick

Bei einem Failover-Cluster handelt es sich in der Microsoft-Terminologie um eine Gruppe aus unabhängigen Computern, die miteinander interagieren, um die Verfügbarkeit und Skalierbarkeit von Cluster-Rollen (Anwendungen auf dem Cluster) zu erhöhen. Jeder Cluster-Server wird als *Cluster-Knoten* bezeichnet und ist über das Netzwerk mit den jeweils anderen Cluster-Knoten verbunden. Die Windows-Funktion Failover-Cluster ist für die Kommunikation und Koordinierung der Cluster-Knoten

zuständig. Wenn auf einem oder mehreren der Cluster-Knoten ein Fehler auftritt, werden die Aufgaben des ausgefallenen Cluster-Knotens sofort von anderen Cluster-Knoten übernommen. Diesen Vorgang nennt man *Failover*. Das Wiederaufnehmen der Funktion durch den zuvor ausgefallenen Cluster-Knoten bezeichnet man als *Failback*.

Zusätzlich werden die Cluster-Rollen aktiv überwacht, um sicherzustellen, dass diese ordnungsgemäß funktionieren. Wenn Windows einen Fehler feststellt, startet es die Cluster-Rollen neu oder verschiebt sie auf einen anderen Cluster-Knoten. Die Failover-Cluster-Funktion sorgt dafür, dass die Unterbrechungen auf Anwenderseite nur minimal sind, allerdings ist die konkrete Ausfallzeit von dem Failover der Ressourcen und der Zeit für die Wiederaufnahme der Funktionen der Anwendungen abhängig.

Die Failover-Cluster-Funktion in Windows Server 2012 wird als Feature über den Server-Manager oder mithilfe der PowerShell installiert und mit dem Snap-in Failover-Cluster-Manager und den PowerShell-Cmdlets für Failover-Clustering verwaltet. Dateifreigaben in einem Dateiserver-Cluster können außerdem mithilfe der Tools in den Datei- und Speicherdiensten verwaltet werden.

4.2.2 Terminologie

Windows-Failover-Cluster verwenden eine eigene Terminologie zur Beschreibung der einzelnen Funktionen eines Clusters. Das Verständnis für die wichtigsten Cluster-Begriffe ist entscheidend für eine effiziente Cluster-Administration, sodass die folgende Tabelle 4.3 die wichtigsten Begriffe erklärt.

Cluster-Begriff	Beschreibung
Quorum	die Datenbank eines Failover-Clusters und zuständig als Voter für Cluster mit gleicher Anzahl an Cluster-Knoten
Cluster-Knoten	ein Mitglied (Server) eines Failover-Clusters
Failover	Übernahme der Funktionen eines ausgefallenen Cluster-Knotens durch einen anderen Cluster-Knoten
Failback	Übertragen der Cluster-Ressourcen auf den ursprünglichen Cluster-Knoten
Cluster Shared Volume (CSV)	eine neue Speichertechnik seit Windows Server 2008 R2, mit der mehrere Cluster-Knoten gleichzeitig auf gemeinsam genutzten Festplattenspeicher zugreifen können
Cluster-IP-Adresse	die IP-Adresse für den virtuellen Cluster-Namen (CNO – Cluster Name Object)

Tabelle 4.3 Wichtige Begriffe für das Failover-Clustering in Windows

Cluster-Begriff	Beschreibung
Cluster Name Object (CNO)	der NetBIOS-/DNS-Name der virtuellen Cluster-Ressource
Heartbeat	die Kommunikationsverbindung zwischen Cluster-Knoten zur Ermittlung des Zustands der Cluster-Knoten
Cluster-Rolle	die Anwendung, die in einem Cluster hochverfügbar gemacht werden soll
Cluster-Datenträger	der Datenträger zur Speicherung der Daten einer Cluster-Rolle
Cluster-Netzwerke	die Netzwerkkarten und Netzwerke, die von einem Cluster verwendet werden
Cluster-Validierung	die Vorgehensweise zur Ermittlung, ob die verwendete Hard- und Software clusterfähig ist
WSFC	Windows Server Failover-Clustering
Ressourcengruppe	Eine Sammlung von Cluster-Ressourcen, die als einzelnes Cluster-Objekt verwaltet werden. In der Regel enthält eine Ressourcengruppe alle Cluster-Ressourcen, die zum Ausführen einer bestimmten Anwendung oder eines Dienstes erforderlich sind.
Ressourcenabhängigkeit	Eine Ressource, von der eine andere Ressource abhängt. Wenn Ressource X von Ressource Y abhängt, dann ist Y eine Abhängigkeit von X.
Netzwerknamenressource	Ein logischer Server-Name, der als Cluster-Ressource verwaltet wird. Eine Netzwerknamenressource muss mit einer IP-Adressressource verwendet werden.
Bevorzugter Besitzer	Ein Cluster-Knoten, auf dem eine Ressourcengruppe bevorzugt ausgeführt wird. Jede Ressourcengruppe ist einer Liste von bevorzugten Besitzern zugeordnet. Während eines automatischen Failovers wird die Ressourcengruppe in den nächsten bevorzugten Knoten in der Liste der bevorzugten Besitzer verschoben.
Möglicher Besitzer	Ein sekundärer Cluster-Knoten, auf dem eine Cluster-Ressource ausgeführt werden kann. Jede Ressourcengruppe ist einer Liste von möglichen Besitzern zugeordnet. Ein Failover für Ressourcengruppen kann nur zu Knoten erfolgen, die als mögliche Besitzer aufgeführt sind. Auf nicht als möglichen Besitzer aufgeführten Cluster-Knoten kann kein Failover von Cluster-Ressourcen durchgeführt werden.

Tabelle 4.3 Wichtige Begriffe für das Failover-Clustering in Windows (Forts.)

Diese Tabelle hat Ihnen nur eine Auflistung der wichtigsten Begriffe aus dem Bereich des Windows-Failover-Clusterings gegeben. Im Lauf der Arbeit mit einem Failover-Cluster werden Sie weiteren Abkürzungen und Begriffen begegnen. Möchten Sie eine Erklärung für weitere Begriffe erhalten, können Sie die Windows-Hilfefunktion für den Failover-Cluster verwenden, die eine gute Erklärung vieler Fachbegriffe bietet.

4.2.3 Cluster-Arten

Die Cluster-Funktion kann generell in verschiedene Cluster-Konzepte unterteilt werden. Die gebräuchlichsten Cluster-Konzepte sind:

- Compute-Cluster
- Standby-Cluster (Aktiv/Passiv)
- Aktiv-/Aktiv-Cluster
- Multi-Site-Cluster

Bei einem *Compute-Cluster* handelt es sich um einen Cluster-Verbund mit dem Ziel, die Rechenkapazität zu erhöhen, indem die Rechenkapazitäten der einzelnen Cluster-Knoten über spezielle Hard- und Software zusammengefasst werden. Microsoft hat einige Jahre lang mit der *High Performance Computing Edition* (HPC) einen Compute-Cluster zur Verfügung gestellt, sich aus diesem Geschäftsfeld aber zurückgezogen.

Bei einem *Standby-Cluster* handelt es sich (zumindest in der Vergangenheit) um die wohl häufigste Form des Clusterings im Windows-Umfeld. Ein Cluster bestehend aus zwei Cluster-Knoten bietet eine Hochverfügbarkeit, indem ein Cluster-Knoten die aktiven Aufgaben übernimmt und somit als *aktiver Cluster-Knoten* bezeichnet wird. Ein weiterer Cluster-Knoten dient als *passiver Cluster-Knoten* und übernimmt im Fall eines Ausfalls des aktiven Cluster-Knotens alle Aufgaben. Hierzu startet er die ausgefallene Applikation stets neu, sodass für die Anwender eine kurze Unterbrechung auftritt.

Im Gegensatz zum Aktiv-/Passiv-Cluster übernehmen in einem *Aktiv-/Aktiv-Cluster* beide Cluster-Knoten aktiv Aufgaben, führen in der Regel also eine bestimmte Applikation parallel aus. Fällt einer der Cluster-Knoten aus, muss der verbleibende Cluster-Knoten in der Lage sein, die Aufgaben des anderen Cluster-Knotens zusätzlich zu übernehmen.

Bei einem *Multi-Site-Cluster* handelt es sich eigentlich nicht um eine spezielle Form eines Clusters. Ein Multi-Site-Cluster kann als Aktiv-/Aktiv- oder als Aktiv-/Passiv-Cluster betrieben werden. Die Unterscheidung zu einem »herkömmlichen« Cluster ist bei einem Multi-Site-Cluster nur die räumliche Trennung der Cluster-Knoten. Während bei einem traditionellen Cluster die Cluster-Knoten räumlich relativ eng beieinanderstehen (bedingt durch den gemeinsamen Zugriff auf Cluster-Datenträger

durch SCSI/SAS oder Fibre Channel), können Cluster-Knoten in einem Multi-Site-Cluster über Kontinente hinweg verteilt sein.

Ein Beispiel für eine Form eines Multi-Site-Clusters ist *Microsoft Exchange Server 2007*, der es erstmals mit der Funktion der *Cluster Continuous Replication* (CCR) ermöglichte, dass Cluster-Knoten ohne gemeinsamen Speicher in Form eines SANs auskamen. Hierzu speichert Exchange seine Datenbanken lokal auf den Exchange Servern und repliziert sie über das Netzwerk. Mit Exchange Server 2010 und 2013 wurde das Multi-Site-Cluster-Konzept mit der Funktion der Datenbanken für die Hochverfügbarkeit (DAG – Database Availability Group) ausgebaut.

4.2.4 Historie des Windows-Clusterings

Microsoft hat bereits sehr früh begonnen, eine Hochverfügbarkeitslösung auf Windows Server-Basis anzubieten. Begonnen hat das Cluster-Engagement von Microsoft mit *Windows NT 4.0 Server* im März 1996 in der Enterprise Edition unter dem Codenamen *Wolfpack*. Unterstützt wurden maximal zwei Cluster-Knoten in einem Cluster.

In *Windows 2000 Server* wurde die maximale Anzahl der unterstützten Cluster-Knoten versionsspezifisch geändert: *Windows 2000 Advanced Server* unterstützte eine maximale Anzahl von zwei Cluster-Knoten, die *Windows 2000 Datacenter Edition* vier Cluster-Knoten. Mit *Windows Server 2003* betrug die maximale Anzahl unterstützter Cluster-Knoten sowohl in der Enterprise als auch in der Datacenter Edition acht Cluster-Knoten.

Neben zahlreichen technischen Änderungen der Cluster-Funktionen in *Windows Server 2008* wurde die maximale Anzahl unterstützter Cluster-Knoten auf 16 erhöht, was sich auch in *Windows Server 2008 R2* nicht geändert hat. Die grafische Oberfläche zur Cluster-Verwaltung wurde erheblich vereinfacht und eine neue Form der Cluster-Validierung eingeführt, die es auch ermöglicht, Hardware einzusetzen, die nicht in der Hardware-Kompatibilitätsliste (HCL – Hardware Compatibility List) von Microsoft aufgeführt ist.

Mit dem Erscheinungsdatum von *Windows Server 2012* hat Microsoft neben der Einführung von zahlreichen technischen Neuerungen und Verbesserungen die maximale Anzahl der Cluster-Knoten auf 64 erhöht und ermöglicht nun auch die Nutzung der Failover-Cluster-Funktionen in der Standard- und Datacenter-Version von Windows Server 2012. Die Fassung Windows Server 2012 R2 erweitert die Techniken für Skalierbarkeit und Fehlertoleranz des Systems.

4.2.5 Neuerungen im Failover-Cluster

In diesem Abschnitt stellen wir Ihnen die neuen Funktionen und Techniken vor, die Windows Server 2012 eingeführt hat. Sie gelten auch für Windows Server 2012 R2,

ebenso wie das gesamte Fundament des Clusterings. Den Erweiterungen von Windows Server 2012 R2 widmen wir einen eigenen Abschnitt 4.2.21, »Neu in Windows Server 2012 R2«.

Failover-Cluster in Windows Server 2012 stellen eine hochverfügbare und skalierbare Infrastruktur für viele Anwendungen wie Exchange Server, Hyper-V, SQL Server und Dateiserver, aber auch für Anwendungen wie DHCP und iSCSI-Target-Server zur Verfügung. Die Server-Anwendungen können auf physischen Servern, aber auch auf virtuellen Maschinen laufen. Nach eingehender Validierung und Prüfung der Vorgaben der jeweiligen Anwendungshersteller sind sogar Hybrid-Cluster möglich, bei denen ein Knoten physisch arbeitet und ein anderer virtuell. Failover-Cluster stellen seit Windows Server 2008 R2 auch eine neue Funktion mit dem Namen *Cluster Shared Volume* (CSV) zur Verfügung, die den Cluster-Knoten einen konsistenten, verteilten Namensraum für die Datenablage zur Verfügung stellt.

Windows Server 2012 unterstützt jetzt sowohl in der Standard Edition als auch in der Datacenter Edition eine maximale Anzahl von 64 Cluster-Knoten und eine maximale Anzahl von 8.000 aktiven virtuellen Maschinen pro Cluster. Die maximale Anzahl von virtuellen Maschinen pro Cluster-Knoten beträgt 1.024 (zum Vergleich lag die Anzahl in Windows Server 2008 R2 bei 384).

Die Verwaltung eines Failover-Clusters erfolgt mithilfe der *Failover-Cluster-Verwaltungskonsole* oder – neu in Windows Server 2012 – mithilfe des *Server-Managers*. Eine Verwaltung des Clusters mithilfe der PowerShell ist ebenfalls möglich.

Das mit Windows Server 2008 R2 eingeführte Cluster Shared Volume (CSV) wurde vollständig überarbeitet. Es bietet jetzt neben Geschwindigkeitsverbesserungen und verbesserter Wiederherstellbarkeit die Möglichkeit, auch anderen Anwendungen wie SQL Server und den Dateidiensten die CSV-Technik in Form des Dateiservers für das horizontale Skalieren (SOFS) zur Verfügung zu stellen. Zusätzlich kann jeder verfügbare Cluster-Datenträger mithilfe der Failover-Cluster-Verwaltungskonsole zu einem CSV-Datenträger konvertiert und ebenso leicht wieder in einen verfügbaren Cluster-Datenträger zurückkonvertiert werden.

Da sich die maximale Anzahl an Cluster-Knoten in Windows Server 2012 auf bis zu 64 Cluster-Knoten erhöht hat, steigt der Aufwand für die Installation von Updates in einem Cluster, da Updates in der Regel eine Einschränkung der Verfügbarkeit von Anwendungen auf den Servern bedingen und oft sogar einen Neustart erfordern. Um Cluster-Administratoren die Installation von Updates zu erleichtern, stellt die Failover-Cluster-Funktion von Windows Server 2012 einen Assistenten zur automatischen Installation von Windows Updates in einer Cluster-Umgebung zur Verfügung. Die als *Cluster Aware Updating* (CAU, clusterfähiges Aktualisieren) bezeichnete Funktion erlaubt eine annähernd vollautomatische Aktualisierung eines Windows-Clusters.

Wenn Sie als Administrator die Dienste einer virtuellen Maschine nicht mit dedizierten Überwachungslösungen wie *System Center 2012 Operations Manager* oder Lösungen von anderen Anbietern überwachen können oder möchten, stellen die Failover-Cluster-Dienste in Windows Server 2012 eine neue Möglichkeit zur Überwachung von Diensten innerhalb der virtuellen Maschine zur Verfügung. Diese erfolgt mithilfe der Failover-Cluster-Verwaltungskonsole.

Seit Windows Server 2008 prüft ein Cluster-Validierungsprozess die Cluster-Hardware auf Cluster-Tauglichkeit hin anhand von Microsofts Vorgaben. Die Cluster-Validierungsgeschwindigkeit in Windows Server 2012 wurde im Vergleich zu Windows Server 2008 R2 für die Überprüfung der Hyper-V- und CSV-Funktionen noch einmal verbessert.

Eine Abhängigkeit der Cluster-Server-Funktion von einer Active-Directory-Domänenumgebung für das Failover-Cluster-Dienstkonto wurde mit Windows Server 2012 reduziert. Das Windows-Dienstkonto für den Failover-Cluster kann jetzt auch ohne Kontakt zu einem Active-Directory-Domänencontroller den Cluster-Dienst starten. An der Notwendigkeit, dass alle Cluster-Knoten in einem Failover-Cluster Mitglied einer Active-Directory-Domäne sein müssen, hat sich jedoch nichts geändert.

Im Bereich der Cluster-Quorum-Konfiguration hat es in Windows Server 2012 eine sinnvolle Erweiterung gegeben. Der Cluster-Dienst unterstützt jetzt die Funktion des dynamischen Quorums, indem sichergestellt wird, dass ein Cluster bei einer sich ändernden Anzahl an Cluster-Knoten, zum Beispiel durch Ausfall eines Cluster-Knotens, weiterhin funktionsfähig bleibt und für eine Entscheidungsmehrheit (Vote Majority) sorgt.

Failover-Cluster unter Windows Server 2008 R2 können recht einfach zu Windows Server 2012 migriert werden. Dabei unterstützt ein eigener Assistent zur Übertragung von Applikationen und Rollen in einem Cluster. Die Cluster-Migration von Windows Server 2012 zu Windows Server 2012 R2 ist in vielen Fällen sogar noch einfacher geworden – im Fall von Hyper-V etwa entfallen Wartezeiten für die Anwender in einer solchen Situation vollständig.

Eine weitere sinnvolle Erweiterung der Failover-Cluster-Funktionen in Windows Server 2012 ist die Integration des Windows-Aufgabenplaners in die Cluster-Funktion. Sie müssen in Windows Server 2012 also nicht mehr die gleichen Aufgaben auf jedem Cluster-Knoten manuell anlegen oder durch Ex- und Import der Aufgaben dafür sorgen, dass alle Cluster-Knoten einen konsistenten Aufgabenplaner haben.

Abgerundet werden diese zahlreichen neuen Funktionen durch eine Vielzahl von neuen PowerShell-Cmdlets, mit deren Hilfe Sie zahlreiche Aspekte der Cluster-Administration und -Verwaltung skripten können. Auf einige werden wir im Verlauf dieses Kapitels hinweisen.

Der Server-Manager und die Failover-Cluster-Verwaltungskonsole in Windows Server 2012 erleichtern insbesondere die Administration von Clustern mit einer großen Anzahl von Cluster-Knoten. Der Server-Manager ist in der Lage, alle Cluster-Knoten in einem Failover-Cluster zu ermitteln und zentral zu verwalten. Sie können mit einer einzelnen Instanz des Server-Managers alle Cluster-Knoten remote verwalten, Windows-Rollen und -Funktionen installieren und die Failover-Cluster-Verwaltungskonsole starten. Mithilfe von Suchfiltern und benutzerdefinierten Ansichten können Sie zum Beispiel eine große Anzahl von virtuellen Maschinen oder andere Cluster-Rollen einfacher verwalten. Durch eine Mehrfachauswahl von virtuellen Maschinen können Sie gemeinsame Aktionen wie das Herunterfahren und Starten von virtuellen Maschinen oder eine Live-Migration von mehreren virtuellen Maschinen gleichzeitig starten.

Windows Server 2012 erlaubt mehrere gleichzeitige Live-Migrationen

Eine der eindrucksvollsten Neuerungen bei der Live-Migration ist die Möglichkeit, mehrere Live-Migrationen gleichzeitig zu starten. Sie können in der Hyper-V-Verwaltungskonsole die Anzahl gleichzeitiger Live-Migrationen festlegen. Wenn Sie mehr Maschinen zur Live-Migration auswählen, als festgelegt wurde, werden die weiteren anstehenden Live-Migrationen in eine Warteschlange gestellt und sequenziell abgearbeitet.

Hyper-V VM Replica (VM-Replikation) ist eine weitere Neuerung in Windows Server 2012. Hyper-V Replica erlaubt es Ihnen, eine virtuelle Maschine mithilfe einer asynchronen Replikation auf einen anderen Hyper-V-Server zu übertragen. Die Replikation funktioniert zu anderen Hyper-V-Servern, die Mitglied derselben Active-Directory-Domäne sind, zu Hosts in einem Failover-Cluster oder zu Hyper-V-Servern, die sich in einer anderen Domäne oder sogar in einer Arbeitsgruppe befinden.

Somit ermöglicht Hyper-V Replica Disaster-Recovery-Szenarien, in denen virtuelle Maschinen in ein Backup-Rechenzentrum oder zu einem Hoster repliziert werden. Im Katastrophenfall können dann die replizierten VMs im Backup-Rechenzentrum gestartet werden. Wenn virtuelle Maschinen in einem Windows-Failover-Cluster ausgeführt werden und für die Funktion der Hyper-V Replica eingerichtet werden sollen, stellen die Cluster-Funktionen in Windows Server 2012 eine Cluster-Rolle mit dem Namen Hyper-V-Replikatbroker zur Verfügung, der unter anderen die Aufgaben der Koordination der Hyper-V Replica-Funktionen im Failover-Cluster übernimmt. Ausführliche Informationen zu Hyper-V Replica finden Sie in Abschnitt 4.7, »VM-Replikation«.

Um Administratoren eine bessere Steuerungsmöglichkeit zu geben, auf welche Cluster-Knoten virtuelle Maschinen in einem Failover-Cluster verschoben werden, erlaubt es Windows Server 2012, festzulegen, in welcher Reihenfolge virtuelle

Maschinen nach einem Failover auf einem anderen Hyper-V-Host gestartet werden und auf welchem Host-Server dies geschehen soll, um eine bessere Lastverteilung zu ermöglichen. Folgende Prioritätseinstellungen stehen zur Verfügung:

- HOCH
- MITTEL (STANDARD)
- GERING
- KEIN AUTOSTART

Ist KEIN AUTOSTART konfiguriert, startet die virtuelle Maschine nach einem Failover nicht automatisch. Der Windows-Cluster-Dienst stellt virtuelle Maschinen mit geringer Priorität *offline*, wenn höher priorisierte virtuelle Maschinen aufgrund von Ressourcenknappheit nicht starten könnten.

System Center 2012 Virtual Machine Manager erlaubt eine granulare Steuerung der Lastverteilung

Für eine granulare Steuerung des Failovers von virtuellen Maschinen bietet sich der System Center 2012 Virtual Machine Manager an, der die Funktion der *Dynamic Optimization* (DO) bietet. Sie kann anhand vieler weiterer Kriterien die Lastverteilung von virtuellen Maschinen in einem Failover-Cluster steuern.

Für Wartungsarbeiten können Administratoren einen Cluster-Knoten mit Windows Server 2012 einfacher in den *Wartungsmodus* versetzen (siehe Abbildung 4.4). Der Failover-Cluster verschiebt automatisch alle Cluster-Rollen basierend auf den Prioritätseinstellungen zu anderen Cluster-Knoten und versetzt den Cluster-Knoten dann in den Wartungsmodus. Ist der Wartungsmodus beendet, werden die zuvor verschobenen Cluster-Rollen automatisch wieder auf den ursprünglichen Cluster-Knoten verschoben.

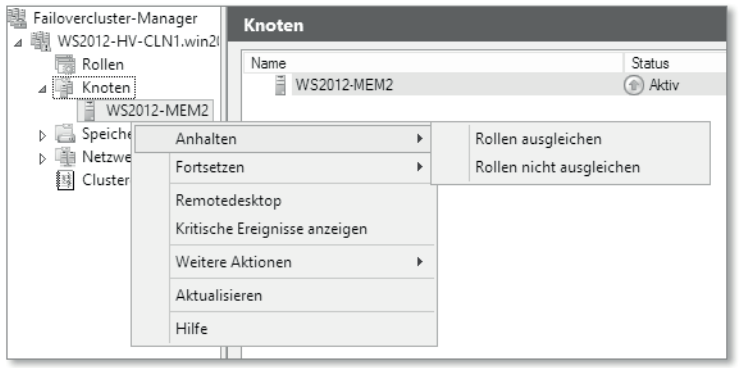


Abbildung 4.4 Cluster-Wartungsmodus

Zu den Neuerungen des Cluster Shared Volumes (CSV) in Windows Server 2012 gehören, ursprünglich eingeführt mit Windows Server 2008 R2:

- Unterstützung für das *horizontale Skalieren*. Mithilfe von CSV können jetzt auch Dateiserver mit Windows Server 2012 im Cluster betrieben werden.
- Mithilfe des Protokolls *Server Message Block 3.0* (SMB) können virtuelle Maschinen auf einer SMB-Freigabe gespeichert werden.
- Unterstützung für Bitlocker-Laufwerksverschlüsselung
- Unterstützung für *Volume Shadow Copy Service Backup Requestor* (VSS) zur anwendungs- und crashkonsistenten Sicherung mithilfe von VSS-Snapshots
- direkter Input-/Output-Zugriff
- Integration mit der SMB-Multichannel- und SMB-Direct-Funktion des SMB 3.0-Protokolls in Verbindung mit der Funktion *Remote Direct Memory Access* (RDMA) von Netzwerkkarten
- Der CSV-Datenträgerzugriff kann auf bestimmte Cluster-Knoten beschränkt werden.
- Unterstützung für Storage Spaces. Storage Spaces von Windows Server 2012 können in CSV integriert werden.
- Automatische Dateisystemreparaturen eines CSV-Volumes können im laufenden Betrieb durch das NTFS-Dateisystem ohne Ausfallzeit durchgeführt werden.

Da ein Failover-Cluster für diverse Konfigurationsoptionen Zugriff auf ein Active Directory benötigt, wurden in Windows Server 2012 folgende Änderungen in der Integration mit den Active-Directory-Diensten durchgeführt:

- Der Speicherort für Cluster-Computerobjekte kann jetzt frei gewählt werden; diese werden nicht mehr automatisch im Containercomputer erstellt, wie das bis Windows Server 2008 R2 der Fall war. Sie können den Speicherort des Cluster-Objekts mithilfe der Windows PowerShell oder bei der Erstellung des Clusters in der Failover-Cluster-Verwaltungskonsole durch Angabe des *Distinguished Names* (DN) festlegen.
- Failover-Cluster können jetzt in ein delegiertes Active-Directory-Administrationsmodell integriert werden.
- *Virtuelle Computerobjekte* (VCO: Virtual Computer Objects), erstellt von dem Failover-Cluster, können jetzt automatisch wiederhergestellt werden, sollten diese durch Active-Directory-Administratoren versehentlich gelöscht werden.
- Ein Failover-Cluster kann jetzt *Read Only Domain Controller* (RODC) zur Authentifizierung verwenden.
- Der Cluster-Dienst kann auch ohne Kontakt zu einem Active-Directory-Domänencontroller gestartet werden.

Keine Group Managed Service Accounts für das Failover-Clustering

Windows-Failover-Clustering kann keinen Gebrauch von der neuen Funktion der Group Managed Service Accounts in Windows Server 2012 machen.

Wie bereits erwähnt, bieten die Failover-Cluster-Dienste zahlreiche Neuerungen im Bereich der Cluster-Quorum-Konfiguration. Zu den wesentlichen Neuerungen gehören:

- erweiterter Assistent zur Konfiguration der Cluster-Quorum-Einstellungen
- Administratoren können jetzt den Cluster-Knoten bestimmen, der für die Quorum-Ermittlung zuständig ist.
- Die Failover-Cluster-Dienste können jetzt das Quorum in einem Cluster dynamisch bestimmen und bei Ausfall von Cluster-Knoten das Quorum automatisch anpassen.

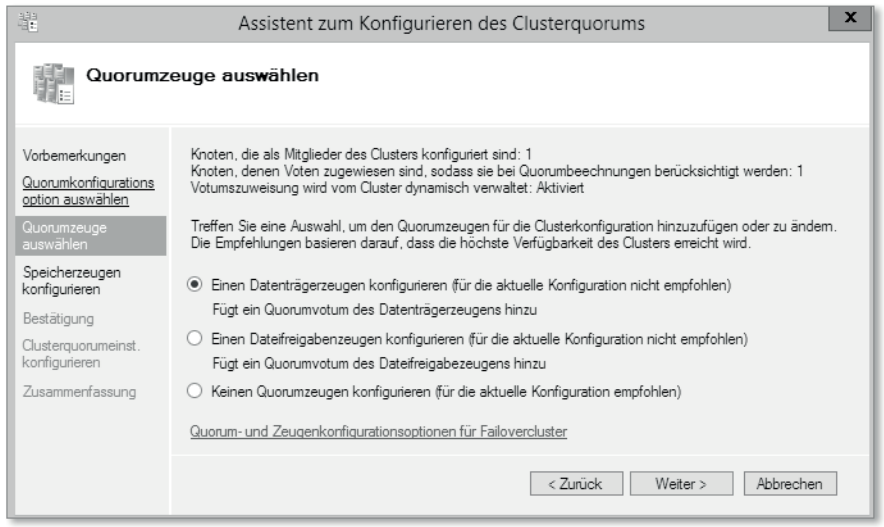


Abbildung 4.5 Quorum-Konfiguration für den Cluster

Um die Migration eines Failover-Clusters mit Windows Server 2008, Windows Server 2008 R2 oder Windows Server 2012 zu erleichtern, stellt Windows Server 2012 einen Cluster-Migrationsassistenten zur Verfügung, der die Konfigurationseinstellungen von Cluster-Rollen, Cluster-Diensten und -Anwendungen migriert. Die Funktionen umfassen:

- Exportieren und Importieren von virtuellen Maschinen
- Migration von Cluster-Datenträgern zu CSV-Datenträgern
- Zuordnen von Cluster-Datenträgern und virtuellen Netzwerken
- Verwendung von existierenden Cluster-Datenträgern

Wie in Abschnitt 4.2.6, »Hardware für einen Cluster«, gezeigt wird, können jetzt mit dem Aufgabenplaner erstellte Aufgaben in den Cluster-Dienst integriert werden, damit diese auf allen Cluster-Knoten zur Verfügung stehen. Zu den Möglichkeiten der Aufgabenplaner-Integration gehören:

- Aufgabenerstellung auf allen Cluster-Knoten
- Aufgabenerstellung auf ausgewählten Cluster-Knoten
- Ausführung von Aufgaben auf nur einem zufällig gewählten Cluster-Knoten
- Ausführung von Aufgaben nur auf einem Cluster-Knoten, der aktuell Besitzer der Cluster-Ressource ist

Die Erstellung und Verwaltung von Aufgaben mit dem Aufgabenplaner kann mithilfe der folgenden PowerShell-Cmdlets durchgeführt werden:

- `Register-ClusteredScheduledTask`
- `Set-ClusteredScheduledTask`
- `Get-ClusteredScheduledTask`
- `Unregister-ClusteredScheduledTask`

Konsequenterweise erweitert Microsoft mit Windows Server 2012 auch die Unterstützung der Failover-Cluster-Verwaltung mithilfe der PowerShell. Hierdurch stehen zahlreiche PowerShell-Cmdlets zur Verfügung. Dazu gehören:

- Verwaltung von Checkpoints für die Cluster-Registrierung
- Erstellung von Dateiservern für das horizontale Skalieren
- Überwachung von Anwendungen und Diensten in virtuellen Maschinen
- Update der Einstellungen eines *Distributed Network Names* (DNN)
- Erstellen und Verwalten von Aufgaben mit dem Aufgabenplaner im Cluster

Kommandozeilenprogramm »Cluster.exe« wird nicht mehr unterstützt

Das Kommandozeilenprogramm *Cluster.exe*, das bis Windows Server 2008 R2 für die Verwaltung eines Clusters verwendet wurde, steht in Windows Server 2012 nicht mehr zur Verfügung und wurde komplett durch die PowerShell ersetzt.

Eine Übersicht über die PowerShell-Befehle zur Verwaltung der Windows-Failover-Cluster-Funktion finden Sie auf der Webseite *http://technet.microsoft.com/en-us/library/hh847239.aspx* (Kurzlink: *http://qccq.de/s/h401*).

Mit dem folgenden PowerShell-Befehl wird ein neuer Windows-Failover-Cluster mit zwei Cluster-Knoten erstellt:

```
New-Cluster -Name Contoso-CLU01 -Node CLU-ND01,CLU-ND02 ⮐
-StaticAddress 192.168.34.222
```

4.2.6 Hardware für einen Cluster

Die beiden IT-Mitarbeiter der Firma A. Datum GmbH planen den Einsatz eines Failover-Clusters mit Hyper-V, bestehend aus zwei Cluster-Knoten mit Anbindung an einen iSCSI-Storage zur Speicherung der virtuellen Maschinen von Hyper-V. Da der Cluster nur etwa zehn virtuelle Maschinen betreiben soll, sind die Anforderungen an die Hardware und das Speichersubsystem überschaubar.

Die IT-Administratoren entscheiden sich für eine Hardware-Kombination, die die Anforderungen an eine Cluster-Lösung unterstützt, damit im produktiven Betrieb keine Probleme mit Inkompatibilitäten zwischen Hard- und Software entstehen. Als Speichersubsystem-Lösung wählt die A. Datum GmbH ein iSCSI-Speichersystem mit einer Netzwerkanbindung von 1 GBit/s. Das Gerät bietet zwei redundante Storage-Controller und die Möglichkeit, mehrere Netzwerk-Ports zusammenzufassen, um die Kapazität zu erhöhen und für eine Ausfallsicherheit der Netzwerkverbindungen zu sorgen.

Die Auswahl der Hardware-Lösung erfolgte unter diesen Anforderungen von Microsoft an eine zertifizierte Cluster-Lösung:

- Die Hardware-Komponenten der Failover-Cluster-Lösung müssen die Windows-Logo-Anforderungen *Zertifiziert für Windows Server 2012* erfüllen.
- Für eine Cluster-Lösung für Hyper-V muss gemeinsam genutzter Speicher (SAN) zur Verfügung stehen und auf allen Cluster-Knoten verfügbar sein.
- Speicher-Controller können Komponenten für Serial Attached SCSI (SAS), Fibre Channel, Fibre Channel over Ethernet (FCoE) oder iSCSI sein.
- Die vollständige Cluster-Konfiguration (Server, Netzwerk, Software und Speicher) muss alle Tests im Cluster-Validierungsassistenten bestehen.

Bei der Auswahl der Hardware und Software für die Cluster-Lösung haben sich die beiden IT-Mitarbeiter auch Gedanken über die notwendige Netzwerk-Bandbreite, benötigten Arbeitsspeicher auf den Cluster-Knoten und benötigten Speicherplatz im SAN gemacht. Dabei müssen unter anderen folgende Aspekte berücksichtigt werden:

- Wie viele virtuelle Maschinen sollen auf einem Hyper-V-Host betrieben werden?
- Wie hoch sind die Arbeitsspeicheranforderungen pro virtuelle Maschine?
- Wie viel Festplattenplatz wird von einer virtuellen Maschine benötigt?
- Wie viele virtuelle und logische CPUs werden pro virtuelle Maschine benötigt?
- Wie hoch sind die I/O-Anforderungen (IOPS) für das Festplattensubsystem?
- Wie viel Netzwerk-Bandbreite wird pro virtuelle Maschine benötigt?
- Soll ein Hyper-V-Host in der Lage sein, bei Ausfall eines Cluster-Knotens alle virtuellen Maschinen auszuführen?

Bei der Kalkulation der Anforderungen an eine Hyper-V-Cluster-Lösung ist das Hyper-V-Kalkulator-Tool von Aidan Finn sehr hilfreich. Beachten Sie jedoch hierbei, dass es sich nicht um die offizielle Aussage von Microsoft handelt und die Zahlen in jeder Umgebung variieren können. Das Tool kann von folgender Webseite heruntergeladen werden:

https://skydrive.live.com/?cid=847C7D34B429AD95&id=847C7D34B429AD95%21312
(Kurzlink: *http://qccq.de/s/h402*)

4.2.7 Cluster-Validierung

Bis einschließlich Windows Server 2003 musste die Hardware für einen Windows-Failover-Cluster vollständig von Microsoft zertifiziert sein, was die Auswahl auf wenige Hersteller beschränkte, die spezielle Cluster-Versionen ihrer Hardware anboten. Damals galt auch die Empfehlung, dass alle Cluster-Knoten in der Hardware-Ausstattung nahezu identisch konfiguriert sind.

Seit Windows Server 2008 qualifiziert der Cluster-Validierungsassistent Failover-Cluster auf eine andere Weise. Mit dem Cluster-Validierungsassistenten müssen Sie die Server, die als Knoten in einem Cluster verwendet werden sollen, einer Reihe von detaillierten Tests unterziehen. Bei der Cluster-Validierung werden die zugrunde liegende Hardware der Server, Speichersubsysteme, Netzwerkkarten und Software auf die Lauffähigkeit in einem Failover-Cluster hin getestet. Die erfolgreiche Cluster-Validierung ist deshalb notwendig, weil der Microsoft-Support (Customer Support Services, CSS) im Fall einer Support-Anfrage durch den Kunden die Vorlage des Cluster-Validierungsberichts verlangt, bevor er die Unterstützung aufnimmt. Um eine unterstützte Cluster-Lösung zu gewährleisten, sind folgende Hardware- und Software-Anforderungen zu erfüllen:

- Alle Hardware- und Software-Komponenten müssen die Anforderungen erfüllen, die für die Vergabe des Logos *Zertifiziert für Windows Server 2012* gelten.
- Die vollständig konfigurierte Lösung (Server, Netzwerk und Speicher) muss sämtliche Tests des Cluster-Validierungsassistenten bestehen.

Ziel der Cluster-Validierung ist es, Hardware- oder Konfigurationsprobleme vor der Cluster-Installation zu erkennen. Sie können mithilfe der Cluster-Validierung sicherstellen, dass Ihr System alle Anforderungen an eine unterstützte Cluster-Konfiguration unterstützt. Des Weiteren kann die Cluster-Validierung auch als Diagnose-Tool auf konfigurierten Failover-Clustern ausgeführt werden, um bei Hardware- oder Software-Änderungen am Cluster zu prüfen, ob die Konfiguration weiterhin unterstützt wird.

Wenn die Cluster-Validierung auf einem bereits konfigurierten Failover-Cluster ausgeführt wird, verwendet der Test der Datenträgerressourcen nur solche Datenträger,

die administrativ in der Failover-Cluster-Verwaltungskonsole in den Offline-Modus versetzt wurden oder keiner Cluster-Rolle zugeordnet sind. Damit verhindert der Cluster-Validierungsdienst, dass der Zugriff auf Anwendungen und Speichersysteme unterbrochen wird. Für einen erforderlichen Test der Cluster-Datenträger ist es möglich, dem Cluster einen zusätzlichen Datenträger zu präsentieren, der auf allen Cluster-Knoten bereitgestellt wird, aber nicht den produktiven Cluster-Rollen zugewiesen ist. Somit kann der Cluster-Validierungsassistent die korrekte Funktionsweise der Speichersubsysteme testen, ohne für eine Unterbrechung der produktiven Cluster-Ressourcen zu sorgen.

Wenn der Failover-Cluster alle Validierungstests bestanden hat und Sie keine Änderungen an der Cluster-Konfiguration (Hardware- und Software-Änderungen) vornehmen, gilt die Cluster-Konfiguration als validiert. Sobald eine Änderung an der Cluster-Konfiguration vorgenommen worden ist, muss der Cluster erneut mit dem Cluster-Validierungsassistenten geprüft werden und alle Tests bestehen.

Zur Validierung einer anstehenden Cluster-Installation bietet es sich an, die zu verwendende Hard- und Software vor der Cluster-Validierung bereits so weit konfiguriert zu haben, wie der Endzustand des Clusters sein soll. Nachdem Sie die Hard- und Software des Clusters vorkonfiguriert haben, müssen Sie noch mithilfe des Server-Managers das Failover-Cluster-Feature installieren. Anschließend können Sie von einem beliebigen zukünftigen Cluster-Knoten die Failover-Cluster-Verwaltungskonsole starten und den Konfigurationsüberprüfungs-Assistenten ausführen (siehe Abbildung 4.6).

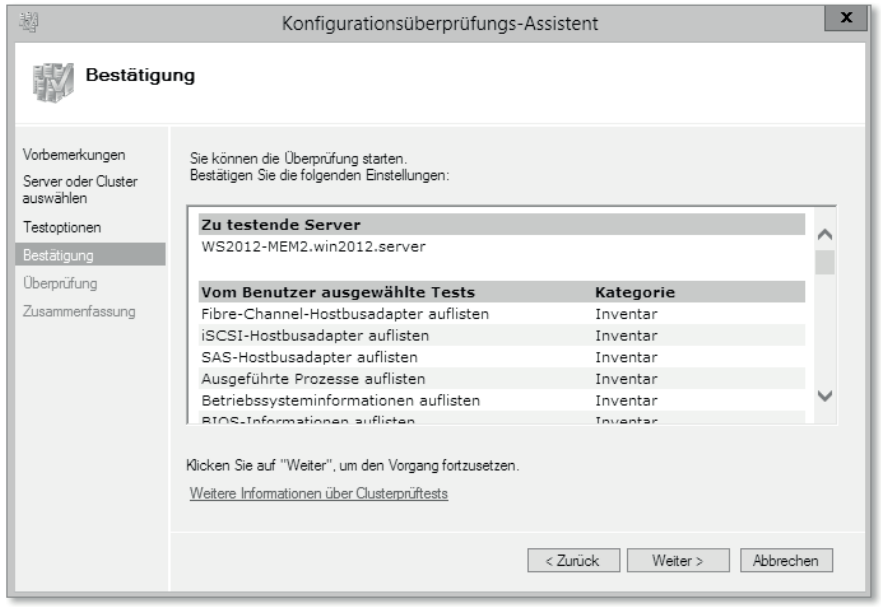


Abbildung 4.6 Cluster-Validierungsprozess

Wählen Sie die Server aus, die in den Cluster aufgenommen werden sollen, und starten Sie den Cluster-Validierungsassistenten, wozu Sie alle verfügbaren Tests auswählen. Sind noch nicht alle erforderlichen Komponenten für den zukünftigen Failover-Cluster auf allen Cluster-Knoten konfiguriert, können Sie auch nur einzelne Validierungstests durchführen, um Teilsysteme auf Cluster-Tauglichkeit hin zu prüfen. Der abschließende Test vor der endgültigen Cluster-Installation muss jedoch mit allen Testverfahren durchgeführt werden, und alle Tests müssen erfolgreich sein.

Nach Abschluss der Tests erscheint eine Zusammenfassungsseite, der Sie die Ergebnisse der einzelnen Tests entnehmen können. Für jeden Bereich der Cluster-Validierung werden detaillierte Ergebnisse angezeigt, die für eine etwaige Validierung nicht erfolgreicher Tests behilflich sind, wie in Abbildung 4.7 zu sehen ist.

Abbildung 4.7 Ergebnis des Failover-Cluster-Prüfberichts

Die Validierungsergebnisse werden mithilfe unterschiedlicher Symbole farblich gekennzeichnet. Validierungsergebnisse können drei Farbzustände annehmen: Grün, Gelb und Rot.

Validierungsergebnisse mit einem grünen Symbol haben den Test erfolgreich bestanden, Symbole mit einem gelben Symbol signalisieren einen Warnzustand und sagen aus, dass einige Prüfpunkte den Test nicht vollständig bestanden haben. Prüf-

ergebnisse mit dem gelben Warnsymbol besagen, dass der Cluster *eventuell* für das Clustering geeignet ist. Im Fall der Eröffnung eines Support-Calls bei Microsoft kann es sein, dass Sie aufgefordert werden, den Cluster-Validierungsbericht für die beanstandeten Punkte neu zu erzeugen, wenn diese im Zusammenhang mit gemeldeten Problemen stehen könnten.

Das rote Symbol im Cluster-Validierungsbericht besagt, dass der Test nicht erfolgreich war und eine unterstützte Cluster-Installation mit dieser Konfiguration nicht möglich ist. Ein weiteres Symbol im Prüfbericht gibt Auskunft darüber, ob der Validierungstest abgebrochen wurde, wenn der Test zum Beispiel von einem anderen Test abhängig war, der nicht erfolgreich durchgeführt werden konnte.

Bei »Rot« kein Support – mit wenigen Ausnahmen

Konnte eine Cluster-Validierung nicht erfolgreich abgeschlossen werden, wird die Konfiguration in der Regel nicht von Microsoft unterstützt. Bei wenigen Ausnahmen gibt es aber doch eine Unterstützung für die Cluster-Konfiguration seitens Microsoft, wenn zum Beispiel ein Multi-Site- oder geografisch verteilter Cluster erstellt werden soll, der keinen gemeinsamen freigegebenen Speicher verwendet. In diesem Szenario generiert der Cluster erwartungsgemäß eine Fehlermeldung. Der Cluster kann jedoch trotzdem erfolgreich in Betrieb genommen werden.

4.2.8 Best Practices für Cluster

Auch wenn die Voraussetzungen für eine von Microsoft unterstützte Failover-Cluster-Konfiguration seit Windows Server 2008 nicht mehr so strikt sind wie in früheren Windows-Versionen, empfiehlt es sich, alle Cluster-Knoten mit möglichst identischer Hardware und Anwendungskonfiguration einzurichten, um mögliche Probleme im laufenden Betrieb zu minimieren. Die verwendete Hardware muss das Zertifikat *Zertifiziert für Windows Server 2012* besitzen. Im Besonderen sollte für die folgenden Hardware-Komponenten auf eine zertifizierte Lösung geachtet werden:

- Prozessortechniken
- Netzwerkadapter
- Host-Bus-Adapter (HBA)
- Direct Attached Storage (DAS)
- Storage Area Network (SAN)

Nicht nur die Hardware sollte den Voraussetzungen für eine zertifizierte Cluster-Lösung gerecht werden, sondern auch die Software und die eingesetzten Dienste gilt es, sorgfältig einzurichten. Zu üblichen Best-Practice-Empfehlungen gehören:

- identische Windows Server-Konfiguration
- identischer Update-Stand für das Betriebssystem und die Applikationen
- einheitliche Konfiguration der Netzwerkadapter auf allen Cluster-Knoten
- funktionsfähige DNS-Namensauflösung
- Mitgliedschaft aller Cluster-Knoten in derselben Active-Directory-Domäne
- Der Benutzer zur Erstellung und Verwaltung des Failover-Clusters muss lokale Administrator-Berechtigungen auf allen Cluster-Knoten besitzen und das Recht haben, Computerobjekte im Active Directory zu erstellen und alle Objekte zu lesen.

Obwohl ein Failover-Cluster schon im Gesamtaufbau für ein hohes Maß an Ausfallsicherheit sorgt, sollten verschiedene Cluster-Komponenten ebenfalls redundant und ausfallsicher ausgelegt sein. Dazu gehören:

- Anbindung der Cluster-Knoten an eine unterbrechungsfreie Stromversorgung (USV), die idealerweise ihrerseits redundant ausgelegt ist
- Verwendung von redundanten Netzteilen in allen Cluster-Knoten
- redundante Anbindung aller Host-Bus-Adapter (HBA) an das SAN bzw. den SAN-Switch
- Verwendung von Netzwerkkarten-Teaming (bzw. entsprechenden Redundanztechniken wie MPIO für Speichernetze) für die Netzwerkanbindungen

Zu den allgemeinen Empfehlungen für die Betriebssystem-Konfiguration der Cluster-Knoten gehören:

- Die Windows-Funktion zur Erstellung eines Kernel-Speicherabbilds im Fall eines Betriebssystem-Fehlers sollte aktiviert werden.
- Service Packs und Updates sollten auf allen Cluster-Knoten identisch eingespielt werden.
- Die Gerätetreiber sollten auf allen Cluster-Knoten identisch und aktuell sein. Das betrifft auch die Firmware der verwendeten Hardware.
- Alle Cluster-Knoten sollten identische Windows Server-Rollen und -Funktionen installiert haben.
- Alle Windows-Dienste in einem Failover-Cluster sollten identisch sein und dieselbe Startart und Konfiguration besitzen.

Nach der Installation des Failover-Clusters und der Übergabe an den Produktionsbetrieb sollte eine Performance-Baseline mithilfe der Leistungsüberwachung von Windows Server 2012 erstellt werden, um bei Leistungsproblemen verlässliche Informationen zu haben, welche Komponente für den Leistungseinbruch verantwortlich ist.

Die Contoso AG setzt als Virenscanner auf den Cluster-Knoten *System Center 2012 Endpoint Protection Client* und hat sichergestellt, dass für die Cluster-Konfiguration die entsprechenden Ausnahmen für einen Antivirenscan durchgeführt worden sind. Für eine korrekte Konfiguration einer Antiviren-Software auf einem Cluster-Knoten empfiehlt sich der folgende Artikel: *http://support.microsoft.com/kb/250355/en-us* (Kurzlink: *http://qccq.de/s/h403*).

Ein weiterer wichtiger Aspekt für einen ordnungsgemäßen Cluster-Betrieb ist die Überwachung der Cluster-Knoten, der Dienste und auch der Cluster-Rollen. Aus unserer Erfahrung können wir sagen, dass einige Firmen Cluster einsetzen, aber die Cluster-Knoten nicht überwachen. Dies führt zum Beispiel bei Zwei-Knoten-Clustern bisweilen dazu, dass der Ausfall eines Cluster-Knotens nicht auffällt und sich die Administratoren Wochen später wundern, dass der Cluster nicht mehr funktioniert, weil auch der zweite Cluster-Knoten ausgefallen ist.

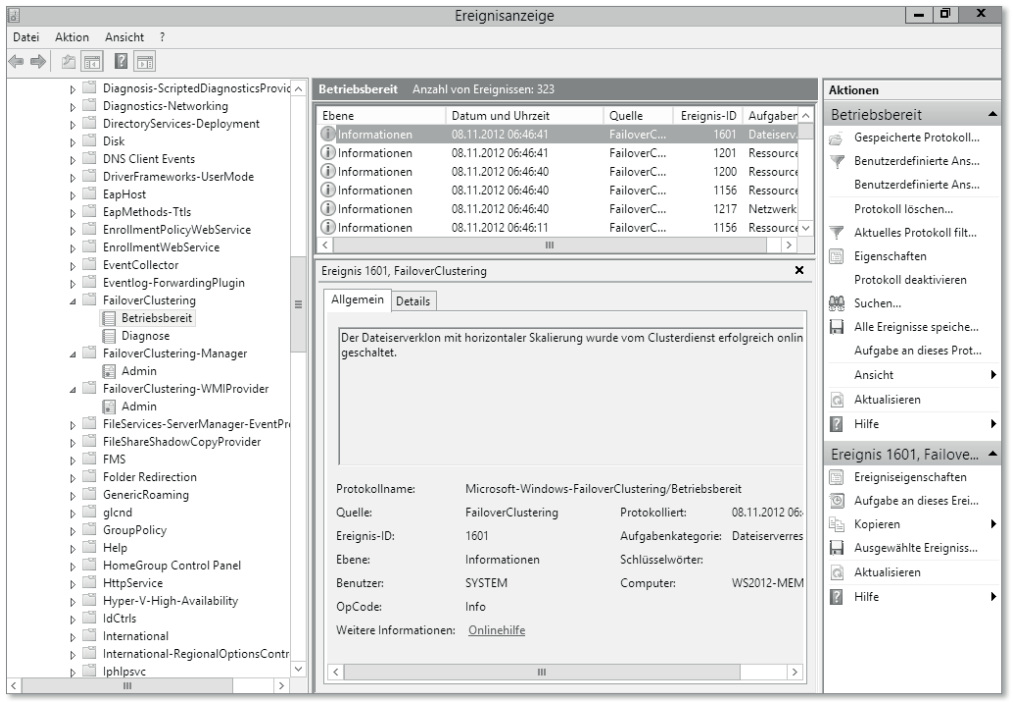


Abbildung 4.8 Die Windows-Ereignisanzeige erlaubt die Erstellung von Aufgaben an Ereignis-IDs.

Die Überwachung eines Cluster-Knotens kann mithilfe von Windows-Bordmitteln mit der Ereignisanzeige und eines Abonnements realisiert werden, indem Sie das jeweilige Ereignis auswählen und im Bereich AKTIONEN diesem Ereignis eine Aufgabe hinzufügen, wie in Abbildung 4.8 zu sehen ist.

Es können aber auch andere Überwachungsprogramme wie *WhatsUp* von Ipswitch oder *System Center 2012 Operations Manager* (OpsMgr) verwendet werden, der eine sehr enge Integration der Überwachung eines Failover-Clusters mithilfe von SCOM-Management-Packs ermöglicht. Eine detaillierte Übersicht über weitere Empfehlungen für den ordnungsgemäßen Betrieb eines Windows-Failover-Clusters liefert der folgende Artikel: *http://blogs.technet.com/b/aevalshah/archive/2012/05/15/windows-server-2008-r2-failover-clustering-best-practice-guide.aspx* (Kurzlink: *http://qccq.de/s/h404*).

4.2.9 Cluster-Quorum

Unter einem Quorum versteht man in der Failover-Cluster-Terminologie eine Komponente des Clusters, die bei einem Teilausfall die Datenintegrität wahren soll. Bei Ausfall der Netzwerkverbindung zwischen den Cluster-Knoten (des sogenannten *Cluster Interconnects* oder *Cluster-Heartbeats*) besteht das Risiko, dass sich der Cluster in zwei Teile aufspaltet. Dies ist auch als *Split-Brain-Problem* bekannt.

Split Brain

Ein »Split Brain« ist ein Risiko jedes Cluster-Systems. Er kann auftreten, wenn die Teile eines Clusters jeweils für sich genommen noch funktionieren, aber keine Kommunikation mehr miteinander aufbauen können. Hierbei könnte es geschehen, dass jeder Teil des Clusters die jeweilige Applikation und ihre Daten separat online hält und Änderungen daran akzeptiert. Hierbei könnten Anwender auf dem einen Cluster-Knoten die Daten anders bearbeiten als die Anwender auf dem anderen Knoten – die Datenbestände driften schnell auseinander und sind später nicht mehr zu integrieren. Bildlich bezeichnet man dies als »Split Brain«, weil gewissermaßen die eine Hälfte des »Hirns« nicht mehr weiß, was die andere tut.

Das Cluster-Quorum in einem Failover-Cluster befindet sich klassisch auf einem Datenträger, der über ein SAN angebunden ist. Man bezeichnet dies auch als *Zeugendatenträger*. Eine andere Form des Cluster-Quorums ist die Knotenmehrheit, bei der jeder Cluster-Knoten eine Stimme (Vote) erhält. Im Lauf der Weiterentwicklung der Cluster-Funktionen in verschiedenen Windows-Versionen kamen weitere Abwandlungen des Quorums in Form des Dateifreigabemehrheits-Quorums hinzu. Wenn Netzwerkprobleme zwischen den Cluster-Knoten auftreten, kann dies dazu führen, dass die Cluster-Knoten überhaupt nicht mehr miteinander kommunizieren. Hierbei muss jeder Cluster-Knoten feststellen können, ob er der »überlebende« Teil des Clusters ist, also aktiv bleiben darf, oder ob er selbst isoliert ist und der nicht mehr erreichbare Teil des Clusters die Applikation weiterbetreibt. Windows-Cluster regeln dies über das Prinzip der Mehrheit (»Quorum« kann »Mehrheit« bedeuten): Es darf

derjenige Teil des Clusters aktiv bleiben, der die Mehrheit der verbleibenden »Stimmen« versammelt. Jeder Server verfügt dabei über eine Stimme.

Um das Split-Brain-Problem bei einer geraden Anzahl von Cluster-Knoten (zwei, vier, sechs Server etc.) zu vermeiden, muss in der Cluster-Software für jede Cluster-Gruppe ein Abstimmungsalgorithmus verwendet werden, um zu bestimmen, ob diese Cluster-Gruppe zu einer bestimmten Zeit ein Quorum aufweist. Da ein angegebener Failover-Cluster eine bestimmte Anzahl von Knoten und eine bestimmte Quorum-Konfiguration aufweist, steht für den Cluster fest, aus wie vielen *Stimmen* (Voter) eine Mehrheit besteht. Liegt die erreichte Anzahl unterhalb der Mehrheit, wird der Cluster nicht mehr ausgeführt. Die Knoten fragen weiterhin das Vorhandensein weiterer Knoten ab, falls ein anderer Cluster-Knoten erneut im Netzwerk auftritt. Die Cluster-Knoten können jedoch erst wieder als Cluster verwendet werden, wenn das Quorum wieder zur Verfügung steht.

Stellen Sie sich beispielsweise die Situation vor, wenn in einem Failover-Cluster mit fünf Knoten die Knoten 1, 2 und 3 miteinander kommunizieren können, jedoch nicht mit den Knoten 4 und 5. Die Knoten 1, 2 und 3 bilden eine Mehrheit und werden weiterhin als Cluster ausgeführt. Die Knoten 4 und 5 stellen eine Minderheit dar und werden daher nicht mehr als Cluster ausgeführt. Wenn für Knoten 3 die Kommunikation mit anderen Cluster-Knoten verloren geht, werden keine Cluster-Knoten mehr im Cluster ausgeführt. Alle funktionierenden Knoten fragen jedoch weiterhin die Kommunikation ab, sodass der Cluster neu gebildet und ausgeführt werden kann, wenn das Netzwerk wieder bereitsteht.

Im Lauf der Weiterentwicklung der Windows Server-Versionen wurden weitere Quorum-Konfigurationen eingeführt. Ein Beispiel ist Exchange Server 2007 mit der Funktion *Cluster Continuous Replication* (CCR). Diese führte mithilfe des Failover-Clusters eine neue Quorum-Option ein, bei der das Quorum auf einer Dateifreigabe (Zeugenfreigabe) auf einem beliebigen Windows Server-System liegt. Somit stellt die Zeugenfreigabe genau wie der Zeugendatenträger neben dem *Cluster Interconnect* (Cluster-Heartbeat) einen *Single Point of Failure* (SPOF) dar.

Als »SPOF« bezeichnet man in der Cluster-Terminologie eine Komponente in einem Cluster, die bei Ausfall die komplette Funktion des Clusters unterbrechen kann. Lösungen zur Vermeidung eines SPOFs sind bei dem Zeugendatenträger zum Beispiel SAN-Spiegelung oder bei einer Zeugenfreigabe ein hochverfügbarer Dateiserver.

Verwenden Sie die empfohlene Quorum-Konfiguration

Verwenden Sie für die meisten Situationen die Quorum-Konfiguration, die von der Failover-Cluster-Software als für den Cluster geeignet identifiziert wird.

Windows Server 2012 legt das Quorum selbstständig fest. Um eine sinnvolle Stimmenzahl zu erreichen, die das Split-Brain-Problem vermeidet, passt Windows die Quorum-Einstellungen sogar dynamisch an, wenn Sie den Cluster verändern. Im Failover-Cluster-Manager können Sie die Quorum-Einstellungen bei Bedarf selbst anpassen. Führen Sie dazu einen Rechtsklick auf den Clusternamen aus, und wählen Sie aus dem Kontextmenü Weitere Aktionen • Clusterquorumeinstellungen konfigurieren. Der folgende Assistent (siehe Abbildung 4.9) erlaubt Ihnen eine angepasste Auswahl aus den Elementen, die wir im Folgenden beschreiben.

Knotenmehrheit

Die Knotenmehrheit kann den Ausfall der Hälfte der Knoten (aufgerundet) abzüglich eines Knotens tolerieren. Beispielsweise kann ein Cluster mit sieben Knoten drei Knotenausfälle tolerieren. Dieses Quorum wird für Cluster mit einer ungeraden Anzahl von Knoten empfohlen.

Knoten- und Datenträgermehrheit

Die Knoten- und Datenträgermehrheit kann den Ausfall der Hälfte der Knoten (aufgerundet) tolerieren, wenn der Zeugendatenträger online geschaltet bleibt. Beispielsweise kann ein Cluster mit zwei Knoten, in dem der Zeugendatenträger online geschaltet ist, einen Knotenausfall tolerieren. Der Datenträger bildet genau wie die Server-Knoten eine Stimme – fällt also der Datenträger aus, darf gleichzeitig die Hälfte der Server-Knoten abzüglich eines Knotens ausfallen. Daher muss immer mehr als die Hälfte der Stimmen online bleiben.

Dieses Quorum wird für Cluster mit einer geraden Anzahl von Knoten empfohlen.

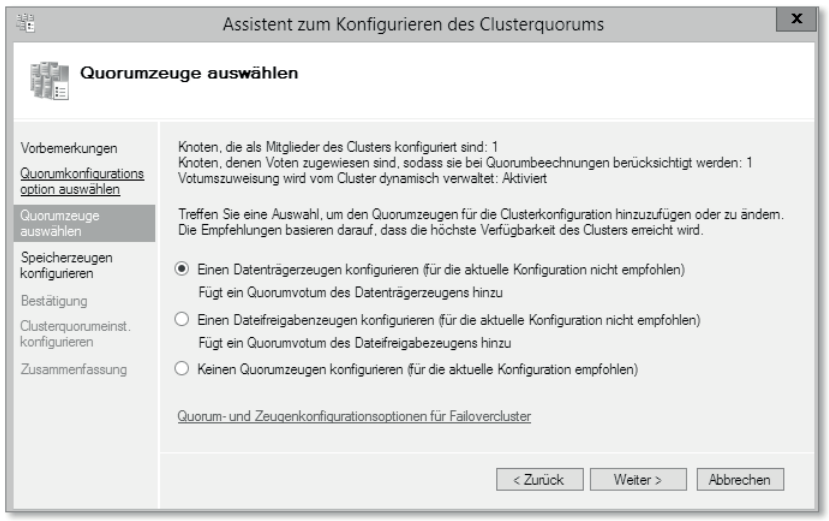


Abbildung 4.9 Quorum-Konfiguration

Knoten- und Dateifreigabemehrheit

Die *Knoten- und Dateifreigabemehrheit* funktioniert ähnlich wie die *Knoten- und Datenträgermehrheit*, doch anstelle eines Zeugendatenträgers wird für diesen Cluster eine Dateifreigabe als »Zeuge« verwendet. Wenn Sie die Knoten- und Dateifreigabemehrheit verwenden, muss mindestens einer der verfügbaren Cluster-Knoten eine aktuelle Kopie der Cluster-Konfiguration enthalten, damit Sie den Cluster starten können. Anderenfalls müssen Sie das Starten des Clusters über einen bestimmten Knoten erzwingen.

Dieses Quorum wird für Cluster mit besonderen Konfigurationen verwendet. Ein Beispiel für die Verwendung dieses Quorum-Typs ist *Exchange Server 2013* mit der Funktion der *Database Availability Group* (DAG) oder ein Multi-Site-Cluster, der aufgrund der Entfernungen zwischen den Cluster-Knoten ohne einen gemeinsam genutzten Datenträgerzeugen auskommen muss.

Keine Mehrheit: Nur Datenträger

Bei Verwendung dieses Quorum-Typs kann der Cluster einen Ausfall aller Cluster-Knoten bis auf einen tolerieren – aber nur, wenn der Datenträger online geschaltet ist. Diese Konfiguration wird jedoch nicht empfohlen, da der Datenträger einen SPOF darstellt. Sie entspricht dem früheren Modell bis Windows Server 2003.

Das Quorum verändern

Neu in Windows Server 2012 ist die Möglichkeit, im laufenden Betrieb Änderungen an der Quorum-Konfiguration vorzunehmen. Sie können zum Beispiel ohne Ausfall der Cluster-Funktion den Zeugendatenträger verschieben oder die Quorum-Konfiguration verändern und die Art des Quorums wechseln. Eine Änderung des Cluster-Quorums ist auch mithilfe der PowerShell möglich. Der folgende Befehl setzt das Cluster-Quorum auf die *Knoten- und Datenträgermehrheit:*

```
Set-ClusterQuorum -NodeAndDiskMajority "Quorum-Disk"
```

4.2.10 Cluster-Speicher

Ein wichtiger Bestandteil jedes Failover-Clusters sind die Datenträger und Speichersubsysteme, die von dem Cluster zur Speicherung der Cluster-Konfiguration und des Betriebssystems verwendet werden, sowie die Datenträger, die als Cluster-Ressource zur Speicherung der Daten dienen.

Als Speicher für das lokale Betriebssystem und die Auslagerungsdatei bietet sich eine RAID-1-Konfiguration auf Datenträger per SAS oder SATA an. Es besteht auch die Möglichkeit, Festplatten über das SAN anzubinden und die Cluster-Knoten dann über das SAN zu booten (Diskless Server). Als Festplattenkapazität müssen Sie den

benötigten Festplattenplatz für Windows Server 2012, die Größe der Auslagerungsdatei und den benötigten Festplattenplatz für lokal zu installierende Anwendungen, Dienstprogramme und Agenten (zum Beispiel Backup-Programme) berücksichtigen.

Als Festplattenspeicher für das Quorum muss eine gemeinsam genutzte Festplatte (LUN, Logical Unit Number) aus dem SAN zur Verfügung gestellt werden. Cluster können an das SAN über SAS, iSCSI, Fibre Channel oder Infiniband und weitere Techniken angebunden werden. Die Größe des Datenträgers für das Quorum (Datenträgerzeuge) sollte eine Kapazität von 512 MB bis 1 GB haben. In der Regel ist der tatsächliche Speicherbedarf für das Quorum jedoch wesentlich geringer.

Den Bedarf an zusätzlichen Datenträgern aus dem SAN bestimmen die Anwendungen, die als Cluster-Rolle in dem Failover-Cluster installiert werden sollen. Im Fall eines Failover-Clusters mit der Hyper-V-Funktion müssen die zusätzlichen Datenträger über das SAN bereitgestellt und mithilfe des Failover-Cluster-Managers in ein *Cluster Shared Volume* (CSV) konvertiert werden. Das CSV verwendet als unterliegendes Dateisystem NTFS und erweitert dessen Funktionen um den gleichzeitigen Zugriff von mehreren Cluster-Knoten, weshalb es als *CSVFS* (Cluster Shared Volume File System) bezeichnet wird.

Eine neue Speichertechnik, bereitgestellt von Windows Server 2012 und Windows 8, sind die Storage Spaces. Storage Spaces in Windows Server 2012 stellen eine Form der Speichervirtualisierung zur Verfügung. Mehrere Datenträger unterschiedlichen Typs können zu einem Storage Pool zusammengeschlossen werden. Aus diesem Storage Pool können dann neue Datenträger erstellt werden, die unterschiedliche Redundanzoptionen in Form von RAID-ähnlichen Techniken besitzen können. Mehr zu Storage Spaces lesen Sie in Kapitel 3, »Den Host-Server einrichten«.

Bei der Dimensionierung des Speichersystems sollten Sie neben einer redundanten Anbindung der Cluster-Knoten an das SAN auch noch die I/O-Anforderungen berücksichtigen. Je nach Art der Anwendung in einem Cluster erzeugen die Anwendungen und Zugriffe unterschiedliche Lasten, die das Speichersubsystem abdecken muss. Das ist besonders wichtig, wenn das SAN auch noch zur Speicherung von anderen Anwendungen und Daten verwendet wird oder weitere Cluster-Server andere Dienste bereitstellen. Die I/O-Anforderungen zu ermitteln, kann sehr anspruchsvoll sein, da oft keine genauen Werte bekannt sind. Wenn Ihnen die I/O-Anforderungen aber bekannt sind, können Sie die *IOPS* (I/O Operations per Second) Ihres Datenträger-Subsystems ermitteln, das heißt die Leistungsfähigkeit gemessen in Zugriffsvorgängen. Hieraus können Sie eine Gleichung aufstellen, ob die erwartete Auslastung von dem Speichersubsystem abgedeckt werden kann. Um die I/O-Anforderungen für einen Cluster mit Hyper-V zu ermitteln, stellt Microsoft das *MAP-Toolkit* (Microsoft Assessment and Planning Toolkit) zur kostenlosen Nutzung zum Download auf der Webseite *http://technet.microsoft.com/en-us/solutionaccelerators/dd537570.aspx* (Kurzlink: *http://qccq.de/s/h405*) zur Verfügung.

4.2.11 Einen Cluster einrichten

Der erste Schritt zur Installation eines Failover-Clusters nach Einrichtung der Hardware ist die Konfiguration des Betriebssystems von Windows Server 2012. Sie sollten immer eine aktive Patch-Strategie betreiben und die notwendigen Windows Updates vor der Failover-Cluster-Installation installieren.

Je nach Gruppenrichtlinien-Strategie in Ihrem Active Directory kann es nützlich sein, alle Cluster-Knoten und die virtuellen Cluster-Namensobjekte in einer eigenen Organisationseinheit (OU) zu platzieren und sicherzustellen, dass eventuelle Gruppenrichtlinien, die die Cluster-Funktion stören könnten (zum Beispiel Gruppenrichtlinien zur Steuerung der Windows-Firewall oder Software-Verteilungsrichtlinien), keine Auswirkung auf diese Organisationseinheit haben. Voraussetzung für die Erstellung von Cluster-Namensobjekten in selbst gewählten Organisationseinheiten im Active Directory ist, dass das Cluster-Computerobjekt das Recht hat, neue Computerobjekte im Active Directory zu erstellen. Dieses Recht müssen Sie mit den entsprechenden Active-Directory-Verwaltungsprogrammen erteilen.

Möchten Sie einen Virenscanner auf dem Cluster-Knoten installieren, sollten Sie die empfohlenen Ausnahmen für das Scannen von Dateien, Verzeichnissen, Prozessen und Dateiendungen beachten, wie in folgendem Knowledge-Base-Artikel beschrieben: *http://support.microsoft.com/kb/250355/en-us* (Kurzlink: *http://qccq.de/s/h403*).

In einem Failover-Cluster ist in der Regel eine Vielzahl von Netzwerkkarten verbaut. Wenn Sie Hyper-V in einem Failover-Cluster betreiben, steigt die Anzahl der notwendigen Netzwerkkarten noch einmal, es sei denn, es werden neue Funktionen wie Converged Fabrics verwendet. Aus diesem Grund ist es wichtig, bereits im Vorfeld vor der Cluster-Installation für eine korrekte Namensgebung der Netzwerkkarten und eine passende IP-Adresskonfiguration zu sorgen.

Da für die korrekte Funktion eines Failover-Clusters minimal zwei Netzwerkkarten benötigt werden, eine Netzwerkkarte für den Zugriff auf das LAN und eine Netzwerkkarte für die Cluster-Kommunikation (Heartbeat, Cluster Interconnect), zeigt Abbildung 4.10 ein Beispiel für eine sinnvolle Namensgebung.

Für einen Failover-Cluster mit weiteren Netzwerkkarten für das Hyper-V-Management, einer Netzwerkkarte für die Live-Migration und der Anbindung von virtuellen Maschinen sind weitere Konfigurationseinstellungen erforderlich. Details dazu finden Sie in Abschnitt 3.3, »Das Netzwerk«.

Nachdem die Administratoren der Contoso AG und der A. Datum GmbH alle notwendigen Vorbereitungen der Windows-Konfiguration getroffen haben, kann jetzt mit der eigentlichen Cluster-Installation begonnen werden. Zuerst muss mithilfe des Server-Managers auf allen Cluster-Knoten die Funktion FAILOVER-CLUSTERING installiert werden.

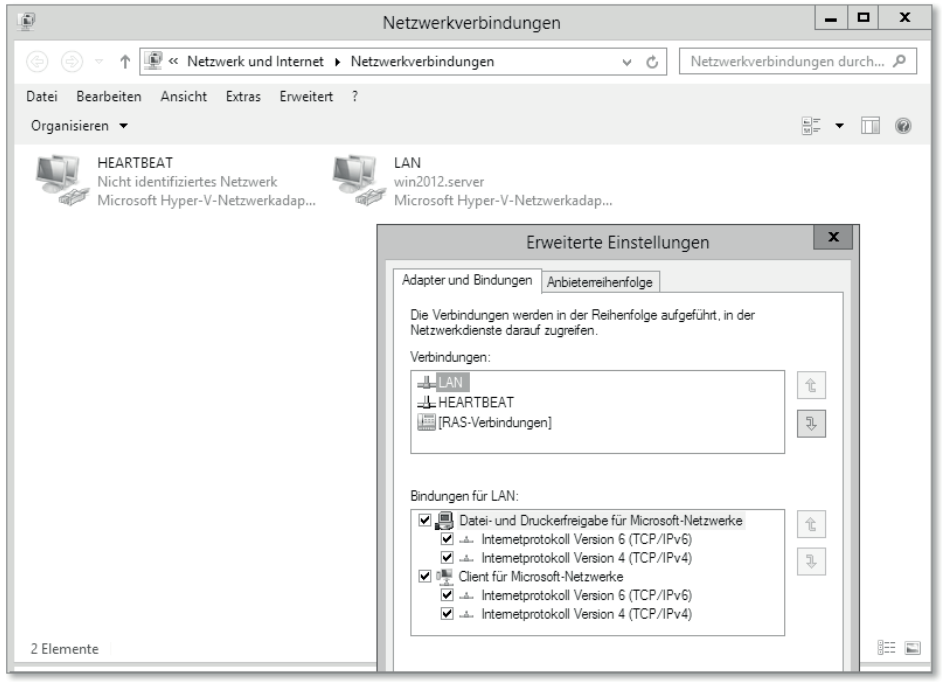


Abbildung 4.10 Netzwerkkarten-Benennung und -Bindungsreihenfolge

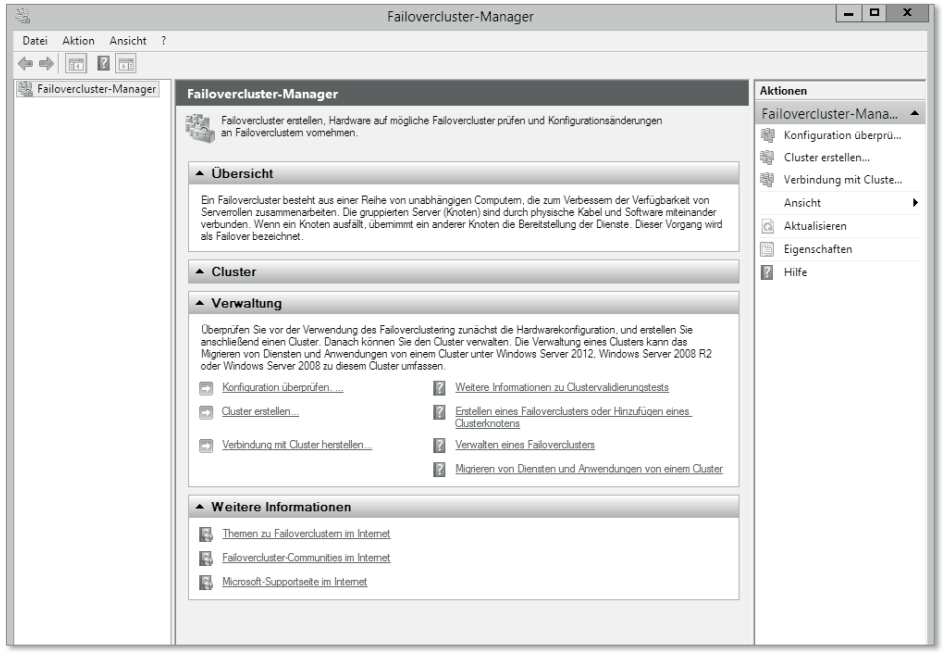


Abbildung 4.11 Failover-Cluster-Manager – Verwaltungskonsole

Die Cluster-Installation kann stellvertretend für alle Cluster-Knoten auf einem einzigen Server erfolgen. Starten Sie den Failover-Cluster-Manager, und beginnen Sie mit dem Cluster-Validierungsprozess, indem Sie mit der rechten Maustaste auf den Knoten FAILOVER-CLUSTER-MANAGER klicken und im Kontextmenü KONFIGURATION ÜBERPRÜFEN auswählen (Abbildung 4.11). Geben Sie die DNS-Namen aller Server an, die Bestandteil des Clusters werden sollen, und führen Sie alle Tests durch.

Im Anschluss an die Cluster-Validierung können Sie sich den Failover-Cluster-Prüfbericht anzeigen lassen und eventuell gefundene Probleme beheben. Erst wenn alle Tests erfolgreich waren, sollten Sie mit der Cluster-Installation fortfahren (siehe Abbildung 4.12).

Abbildung 4.12 Erfolgreiche Cluster-Validierung

Wenn Sie die Cluster-Installation nicht direkt aus der Ereignisanzeige des Failover-Cluster-Prüfberichts starten, können Sie die Cluster-Installation durch einen Klick im Kontextmenü des Knotens FAILOVER-CLUSTER-MANAGER aufrufen. Da Sie den Test bereits erfolgreich durchgeführt haben, können Sie die Installation des Clusters unter Ignorierung der Meldung starten. Geben Sie den Cluster-Namen und eine IP-Adresse an (Abbildung 4.13), unter denen der Cluster aus dem LAN bzw. aus dem Management-Netzwerk erreichbar sein soll. Hierbei handelt es sich um einen zusätz-

lichen Computernamen, der dem gesamten Cluster zugeordnet wird, sowie um eine feste oder per DHCP vergebene IP-Adresse, die entweder dem LAN oder dem Management-Netzwerk entstammt. Beginnen Sie anschließend die Cluster-Installation. Diese erfordert in der Regel keinen Neustart des Servers.

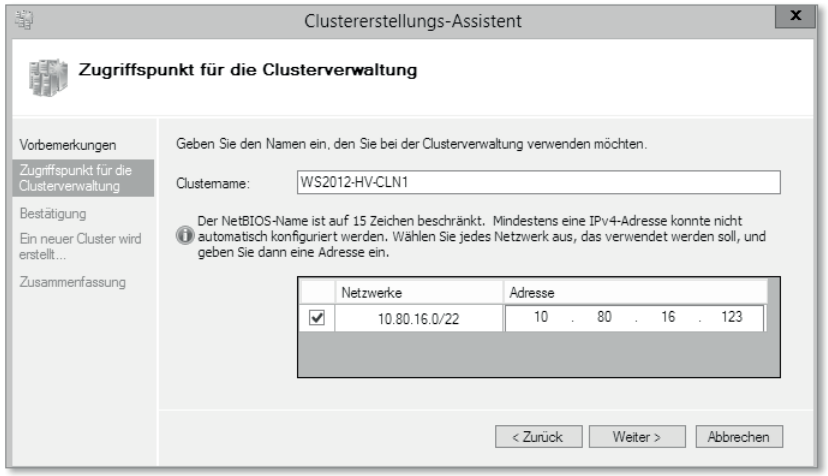


Abbildung 4.13 Zugriffspunkt des Clusters konfigurieren

Nach erfolgreicher Cluster-Installation prüfen Sie als Erstes die Cluster-Ereignisse (Abbildung 4.14) in der Failover-Cluster-Verwaltungskonsole und beheben eventuelle Probleme.

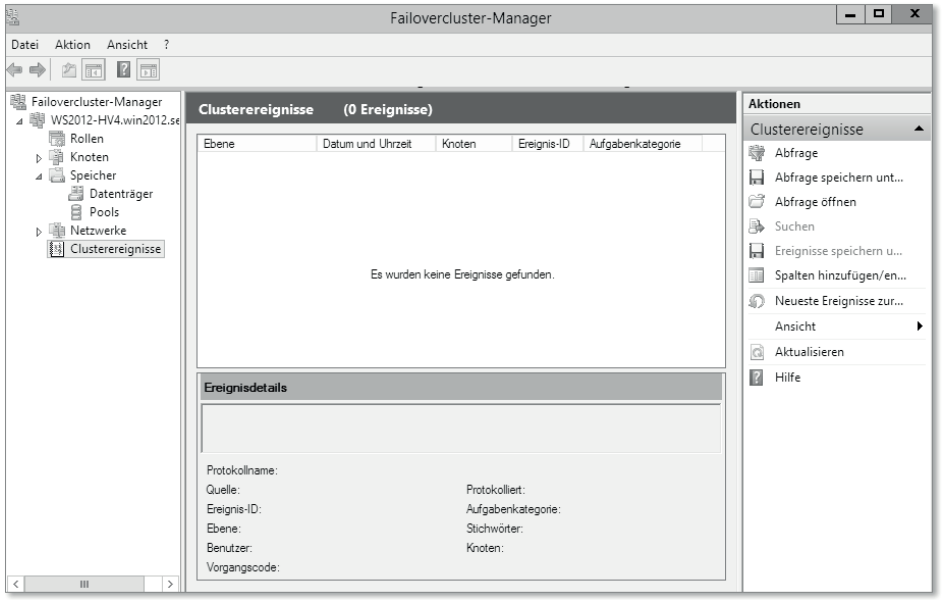


Abbildung 4.14 Überprüfung der Cluster-Ereignisse

Anschließend navigieren Sie zum Knoten SPEICHER • DATENTRÄGER und prüfen, ob die Cluster-Installation die korrekte LUN als Zeugendatenträger (Quorum) konfiguriert hat, und benennen den Datenträger entsprechend seiner Funktion um, wie in Abbildung 4.15 zu sehen ist. Sollte nicht der gewünschte Datenträger als Quorum eingebunden worden sein, korrigieren Sie dies. Bei der Identifizierung kann es sehr hilfreich sein, sich an der konfigurierten Größe zu orientieren (wie erwähnt, sollte der Quorum-Datenträger mit einem Volumen von 512 MB bis 1 GB eingerichtet sein).

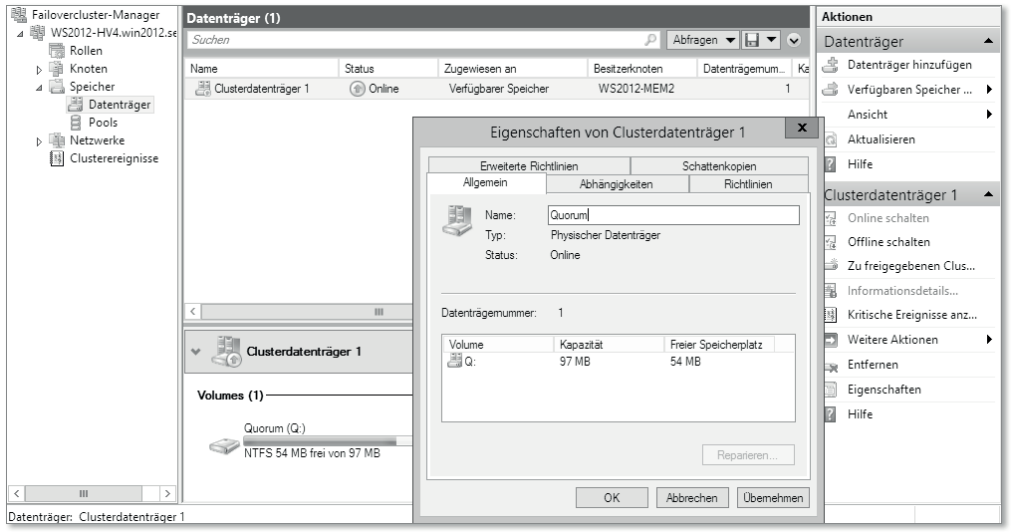


Abbildung 4.15 Prüfung und Benennung der richtigen Datenträger

Nun sollten Sie die erkannten Netzwerke nach ihrer Funktion in der Failover-Cluster-Verwaltungskonsole umbenennen. Es empfiehlt sich hier, den Namen der Netzwerke an diejenigen in der Windows-Konfiguration anzupassen (Abbildung 4.16).

In den Eigenschaften der Netzwerke sollten Sie auch den Verwendungszweck der Netzwerkkarten festlegen. Für die Netzwerkkarte des Cluster-Interconnects (Heartbeat) müssen Sie den Radiobutton NETZWERKKOMMUNIKATION FÜR CLUSTER IN DIESEM NETZWERK ZULASSEN aktivieren und sicherstellen, dass das Kontrollkästchen CLIENTS DAS HERSTELLEN EINER VERBINDUNG ÜBER DIESES NETZWERK GESTATTEN deaktiviert ist. Eine dedizierte Netzwerkkarte für den Cluster-Heartbeat ist nicht zwingend notwendig, da auch die Netzwerkkarte für die Live-Migration diese Funktion übernehmen kann. Bei der Netzwerkkarte für die LAN-Verbindung stellen Sie sicher, dass den Clients eine Verbindung über das Netzwerk gestattet ist.

Sofern Ihr Cluster per iSCSI mit einem SAN verbunden ist, schalten Sie für das iSCSI-Netzwerk sowohl die Cluster-Kommunikation als auch die Client-Verbindungen ab. Bei allen weiteren Netzwerken, die eventuell in Ihrem Cluster vorhanden sind, sollten Sie dies je nach dem Zweck dieser Netzwerke entscheiden. Allgemein kann es

nützlich sein, die Cluster-Kommunikation auf mehr als einem Netzwerk zu erlauben, denn dies kann dazu beitragen, den Kommunikationsausfall zu vermeiden und eine Split-Brain-Situation zu verhindern.

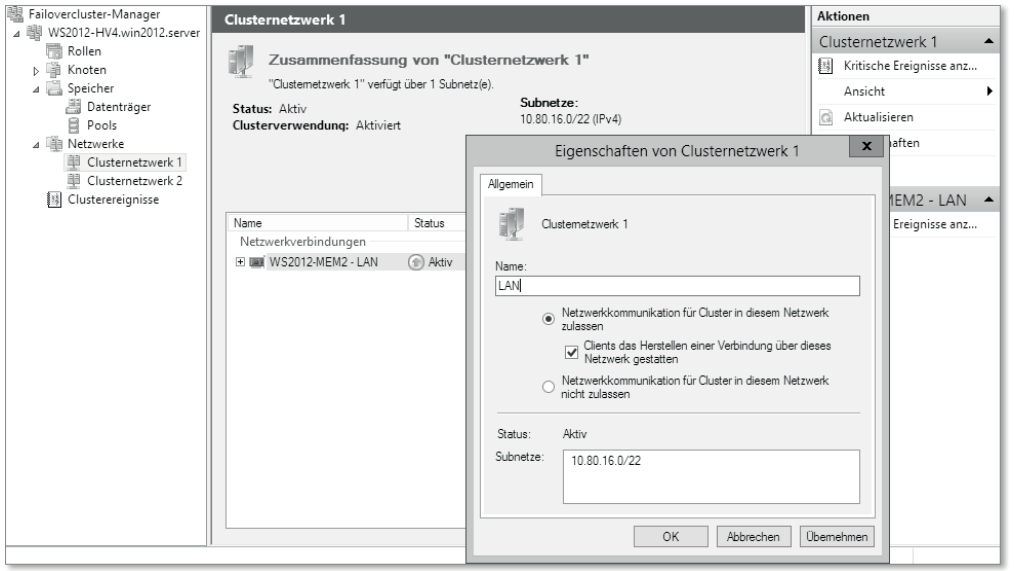


Abbildung 4.16 Benennung der Netzwerkkarten im Failover-Cluster

Sollte der Windows-Failover-Cluster mit der Cluster-Rolle *Hyper-V*, *Dateiserver für das horizontale Skalieren* oder *SQL Server 2012* installiert werden, müssen Sie im Kontextmenü des Knotens NETZWERKE noch die verwendeten Netzwerkkarten für die Live-Migration konfigurieren (siehe Abbildung 4.17).

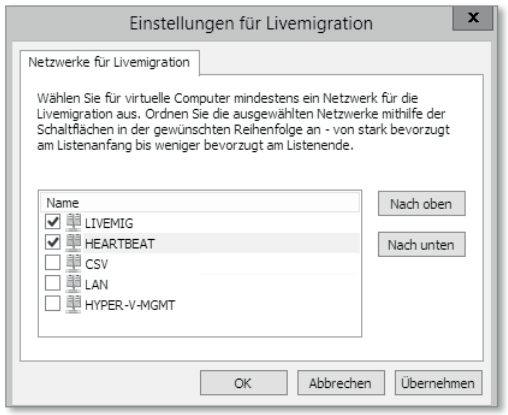


Abbildung 4.17 Auswahl der Netzwerke für die Live-Migration

Die grundlegende Cluster-Installation und -Konfiguration ist somit erfolgreich abgeschlossen, und Sie können mit der Installation der ersten Cluster-Rolle beginnen und sich anschließend in die Administration eines Windows-Failover-Clusters einarbeiten.

4.2.12 Gast-Cluster

Seit Windows Server 2008 R2 gehören auch »Gast-Cluster« zu den offiziell unterstützten Szenarien. Dabei handelt es sich um Failover-Cluster, deren Knoten virtuelle Maschinen sind. Aufgrund der flexiblen Support-Richtlinie, die Microsoft seinerzeit definiert hat, sind sogar »Hybrid-Cluster« zulässig, die teilweise aus physischen Servern und teilweise aus virtuellen Maschinen bestehen. Wichtig für die Supportaussage durch den Hersteller ist stets, dass der Bericht zur Cluster-Validierung (siehe Abschnitt 4.2.7, »Cluster-Validierung«) ein positives Ergebnis bestätigt.

Der besondere Vorteil eines Gast-Clusters für eine Virtualisierungsumgebung besteht in einer hohen Flexibilität auch im Normalbetrieb. Schon durch den Aufbau des Host-Clusters können Sie einige regelmäßige Wartungsarbeiten im laufenden Tagesbetrieb durchführen, ohne die Anwender einzuschränken. Dazu zählen Updates und andere Arbeiten an den Host-Servern, die etwa einen Neustart der Hosts erfordern. In einem Cluster fällt es leicht, die virtuellen Maschinen oder andere Cluster-Rollen vor den Arbeiten auf einen anderen Knoten zu verschieben, sodass es keine Unterbrechung der jeweiligen Applikation gibt.

Stehen hingegen Updates oder Wartungsvorgänge innerhalb einer virtuellen Maschine an, so kann ein Host-Cluster den Ausfall nicht überbrücken: Die virtuelle Maschine muss kurz außer Betrieb gehen. Hier kann der Gast-Cluster einen Ausweg bilden, indem er zusätzlich eine Redundanz auf der Ebene der Applikation bildet. Haben Sie etwa auf zwei VMs einen Exchange- oder einen SQL-Server-Cluster implementiert, so können Sie die betreffende Applikation auf die jeweils andere VM übertragen und so immer eine der beiden VMs in Ruhe bearbeiten. Da die Anwender keine Unterbrechung erfahren, kann dies im normalen Tagesbetrieb geschehen.

Die meisten Applikationen benötigen in einem Cluster den Zugriff auf ein gemeinsames Speichersystem. Auch diesen Zugriff können Sie in einem Gast-Cluster bereitstellen. Dazu haben Sie in Windows Server 2012 und in Windows Server 2012 R2 folgende Möglichkeiten, die virtuellen Cluster-Knoten an ein zentrales Speichersystem anzubinden:

- Anbindung per iSCSI direkt aus der virtuellen Maschine an Speicherbereiche im SAN (Logical Unit Number, LUN). Hierzu benötigen Sie eine normale Ethernet-Verbindung im Host-Server, die auf das iSCSI-SAN zugreifen kann, und eine entsprechende virtuelle Netzwerkkarte in der VM.

- Anbindung per Virtual Fibre Channel (vFC) aus der virtuellen Maschine an eine LUN im FC-SAN. Dies erfordert einen aktuellen Fibre-Channel-HBA (Host-Bus-Adapter) im Host-Server, eine kompatible Fibre-Channel-Infrastruktur sowie einen virtuellen Fibre-Channel-HBA in der VM.
- Anbindung per Fibre Channel over Ethernet (FCoE) – dies entspricht im Wesentlichen der Technik von Fibre Channel, nutzt aber eine spezielle Hardware im Host-Server.

Mehr zu dieser Art, virtuelle Maschinen an ein SAN anzubinden, finden Sie in Abschnitt 5.2.8, »LUNs in einer VM«.

In Windows Server 2012 R2 kommt eine weitere, insgesamt deutlich einfachere Technik hinzu, virtuelle Maschinen für einen Gast-Cluster mit einem gemeinsamen Speicherbereich zu versorgen. Es handelt sich dabei um *Shared Virtual Disks* oder kurz *Shared VHDX*. Dies beschreibt die neue Technik, eine vorhandene virtuelle Festplatte in Form einer VHDX-Datei gleichzeitig an mehrere virtuelle Maschinen als Daten-Festplatte anzubinden. Die VHDX-Datei übernimmt dann die Funktion einer LUN aus dem SAN. Die aufwendige Anbindung der VMs an das SAN per iSCSI oder vFC entfällt dadurch.

Diese neue Technik hat einige Voraussetzungen und Besonderheiten, die wir ihnen in Abschnitt 5.2.7, »Festplatten«, genauer vorstellen.

Abgesehen von der Speicher-Anbindung gelten für einen Gast-Cluster dieselben Anforderungen wie für einen herkömmlichen Failover-Cluster aus physischen Servern. Sie können die Angaben aus diesem Kapitel also direkt auf den virtuellen Cluster übertragen.

4.2.13 Cluster-Rollen

Das Failover-Clustering in Windows Server 2012 stellt eine Reihe von Cluster-Rollen zur Verfügung, die Sie mithilfe der Failover-Cluster-Funktion hochverfügbar machen können. Solche Cluster-Rollen werden im Fehlerfall eines Cluster-Knotens auf einen anderen Cluster-Knoten verschoben. Dieser Prozess wird als *Failover* bezeichnet. Ist der ursprüngliche Besitzer der Cluster-Rollen wieder verfügbar, können die Ressourcen automatisch oder manuell auf den Cluster-Knoten verschoben werden. Dieser Prozess wird als *Failback* bezeichnet.

Das Failover-Clustering in Windows Server 2012 stellt eine Reihe von vordefinierten Cluster-Rollen (Abbildung 4.18) zur Verfügung. Dazu gehören unter anderen:

- Allgemeine Anwendung
- Allgemeiner Dienst
- Allgemeines Skript

- Anderer Server
- Dateiserver
- DFS-Namespaceserver
- DHCP-Server
- Hyper-V-Replikatbroker
- Virtueller Computer

Cluster-Rolle »Drucker«-Server wurde aus dem Failover-Cluster entfernt

Die Cluster-Rolle *Drucker-Server* steht seit Windows Server 2012 nicht mehr zur Verfügung, da Microsoft empfiehlt, die Hochverfügbarkeit eines Drucker-Servers durch Verwendung einer virtuellen Maschine in einem Failover-Cluster mit Hyper-V einzurichten. Dies vermeidet eine Reihe von Problemen, die bei dem früheren Konstrukt insbesondere durch Druckertreiber verursacht wurden.

Die generischen Cluster-Rollen Allgemeine Anwendung, Allgemeiner Dienst und Allgemeines Skript können zur Einrichtung entsprechender Dienste und Anwendungen verwendet werden, die keine native Cluster-Funktion bieten. Microsoft empfiehlt jedoch, bei der Verwendung von Failover-Clustern nur Cluster-Rollen einzurichten, für die der Hersteller eine zugehörige Cluster-DLL bereitstellt, weil sich diese Cluster-Rollen enger in das Clustering integrieren und erweiterte Funktionen wie Überwachung und erweiterte Steuerungsmöglichkeiten zur Verfügung stehen. Manche Hersteller von Speichersystemen nutzen die generischen Cluster-Rollen, um zum Beispiel Failover-Funktionen in Form von Skripten zur Verfügung zu stellen.

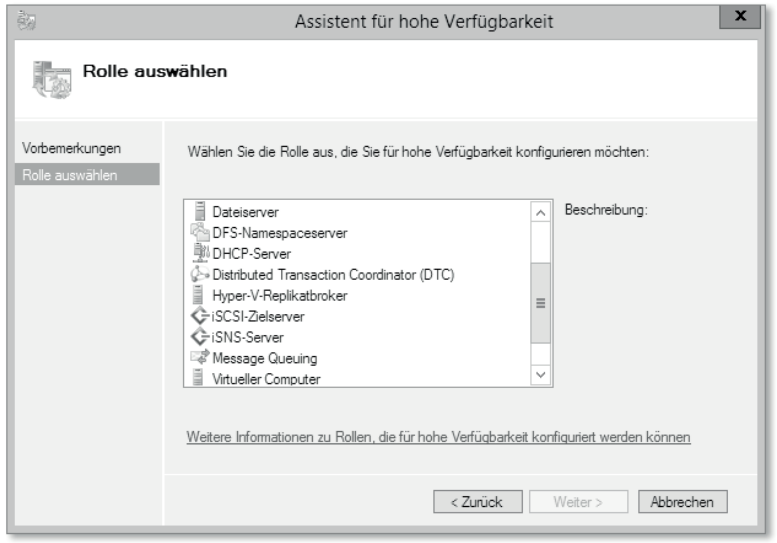


Abbildung 4.18 Verfügbare Cluster-Rollen

Eine Cluster-Rolle besteht aus verschiedenen Elementen. Am Beispiel der Cluster-Rolle *Dateiserver* werden folgende Elemente verwendet:

- Rollentyp
- Dateiservertyp
- Clientzugriffspunkt
- Gemeinsamer Festplattenspeicher

Bei dem Rollentyp handelt es sich um die Cluster-Rolle, die installiert werden soll. Im Fall der Cluster-Rolle *Dateiserver* ist der Dateiserver-Typ Dateiserver mit horizontaler Skalierung für Anwendungsdaten. Bei dem Clientzugriffspunkt handelt es sich um den NetBIOS-Namen der Cluster-Rolle. Der NetBIOS-Name der Cluster-Rolle wird dann von Clients verwendet, die auf die Cluster-Ressource zugreifen möchten.

Der Failover-Cluster erstellt für den Clientzugriffspunkt ein virtuelles Computerobjekt im Active Directory und einen entsprechenden DNS-Host-Eintrag in der *Forward Lookup Zone* der internen Active-Directory-Domäne. Für die Cluster-Rolle Dateiserver mit der Funktion der horizontalen Skalierung ist ein gemeinsamer Speicher notwendig, der im Cluster als Cluster Shared Volume (CSV) zur Verfügung steht. Wenn Sie als Option für den Rollentyp Dateiserver Dateiserver zur allgemeinen Verwendung auswählen, ist ein CSV nicht notwendig. Die Cluster-Rolle verwendet dann gemeinsamen Speicher, der nach dem *Shared-Nothing*-Prinzip zur Verfügung gestellt wird. Der Failover-Cluster sorgt dann dafür, dass immer nur ein Cluster-Knoten Zugriff auf den gemeinsamen Speicher hat.

Weitere Cluster-Elemente für andere Cluster-Rollen erforderlich

Andere Rollentypen benötigen je nach Funktion andere und weitere Elemente wie Cluster-IP-Adressen.

Die Firma Contoso AG entscheidet sich zur Einrichtung eines Failover-Clusters mit der Cluster-Rolle Dateiserver und dem Dateiserver-Typ Dateiserver mit horizontaler Skalierung für Anwendungsdaten. Dieser soll bei Contoso nur als Datenablage für die Test- und Laborumgebung dienen, die aber ebenfalls mit hohen Verfügbarkeitsanforderungen arbeitet. Tatsächlich wäre die Funktion des Dateiserver-Clusters auch für Produktionszwecke geeignet, doch hierfür steht bei Contoso bereits ein SAN-System bereit.

Cluster-Rollen können auch mithilfe der PowerShell erstellt und konfiguriert werden. Der folgende Befehl erstellt eine neue Cluster-Rolle vom Typ *Dateiserver* mit dem Namen Contoso-FS1:

```
Add-ClusterFileServerRole -Storage "FS-DISK007" -Name ⮌
contoso-FS1
```

Nachdem die Administratoren der Contoso AG einen Zwei-Knoten-Cluster eingerichtet und alle notwendigen Voraussetzungen geschaffen haben, können sie mit der Einrichtung der Cluster-Rolle Dateiserver beginnen. Die Contoso-Administratoren haben für den Cluster eine LUN eines älteren SAN-Systems zur Speicherung der Daten angebunden. Als Nächstes muss die LUN als Cluster Shared Volume bereitgestellt werden. Die Einrichtung des CSVs erfolgt in der Failover-Verwaltungskonsole im Knoten SPEICHER unter DATENTRÄGER. Dort wird der verfügbare Speicher ausgewählt und im Bereich AKTIONEN ZU FREIGEGEBENEN CLUSTERVOLUMES HINZUFÜGEN ausgewählt (Abbildung 4.19).

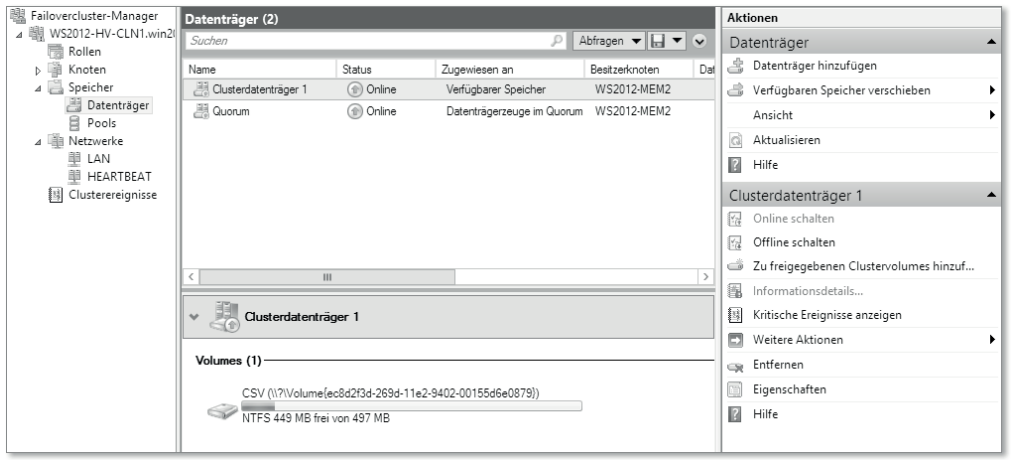


Abbildung 4.19 Hinzufügen des Datenträgers zum CSV

Als Nächstes folgt die Einrichtung der Cluster-Rolle, indem Sie im Kontextmenü des Knotens ROLLEN auf ROLLE KONFIGURIEREN klicken und im ASSISTENT FÜR HOHE VERFÜGBARKEIT die Rolle DATEISERVER und als Dateiserver-Typ DATEISERVER MIT HORIZONTALER SKALIERUNG FÜR ANWENDUNGSDATEN auswählen (Abbildung 4.20).

Der Name für den CLIENTZUGRIFFSPUNKT lautet FILESRV01. Der Name des Client-Zugriffspunkts ist gleichzeitig der Name für ein neues virtuelles Computerobjekt im Active Directory und für den DNS-Host-Eintrag. Schließen Sie den Assistenten für die hohe Verfügbarkeit ab, und prüfen Sie anschließend, ob alle notwendigen Einstellungen erfolgt sind und Sie den verteilten Netzwerknamen des Client-Zugriffspunkts per DNS-Namensauflösung von einem Client erreichen können.

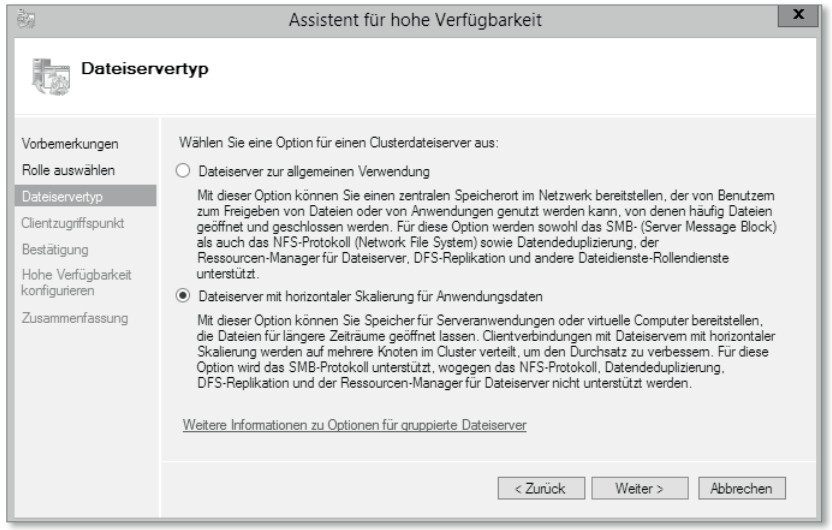


Abbildung 4.20 Auswahl des Dateiserver-Typs

Sollte die Auswahl des Netzwerks für die Live-Migration noch nicht im Vorfeld erfolgt sein, können Sie jetzt in der Failover-Cluster-Verwaltungskonsole den Knoten NETZWERKE auswählen und im Kontextmenü den Menüpunkt EINSTELLUNGEN FÜR LIVE-MIGRATION anklicken und das Netzwerk für die Live-Migration auswählen (Abbildung 4.21).

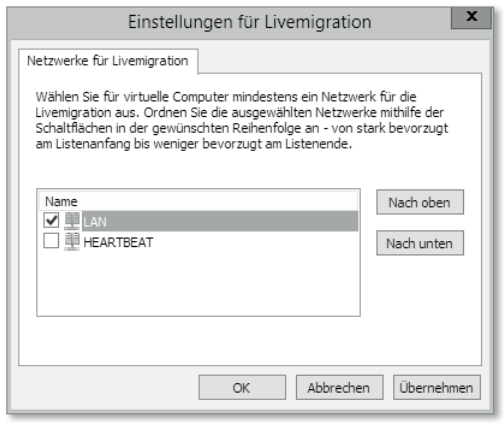


Abbildung 4.21 Auswahl des Netzwerk-LANs für die Live-Migration

Als nächsten Schritt können Sie nun neue SMB-Freigaben für die Cluster-Rolle erstellen. Navigieren Sie dafür zu der erstellten Cluster-Rolle *Dateiserver*, und wählen Sie im Bereich AKTIONEN die Aktion DATEIFREIGABE HINZUFÜGEN aus, wie in Abbildung 4.22 zu sehen ist.

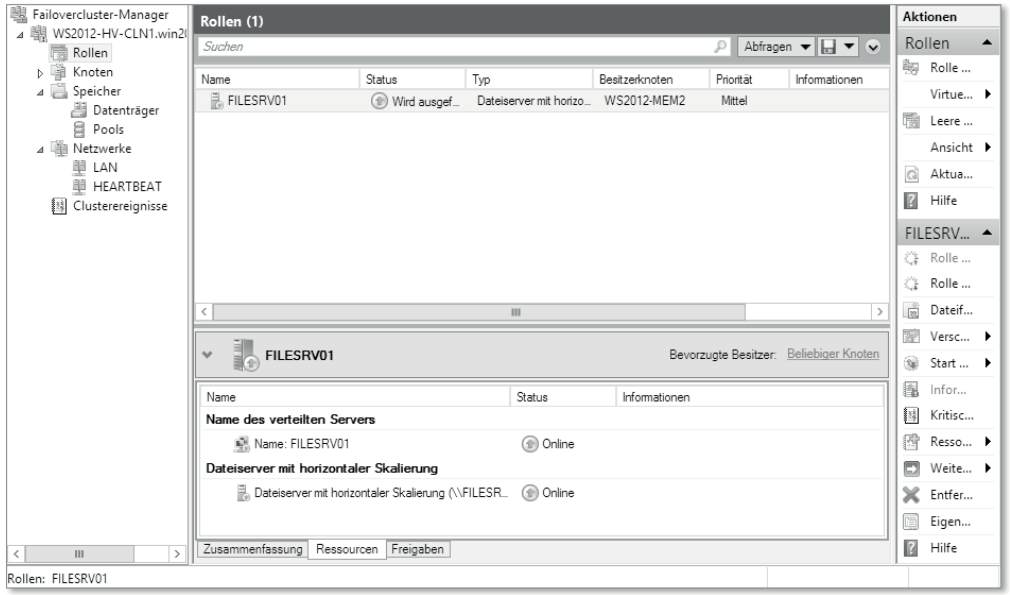


Abbildung 4.22 Hinzufügen einer Dateifreigabe zum CSV

Als Profil wählen Sie wie in Abbildung 4.23 SMB-Freigabe Anwendungen, als Freigabeort das CSV oder einen benutzerdefinierten Pfad aus und vergeben Sie einen entsprechenden Freigabenamen.

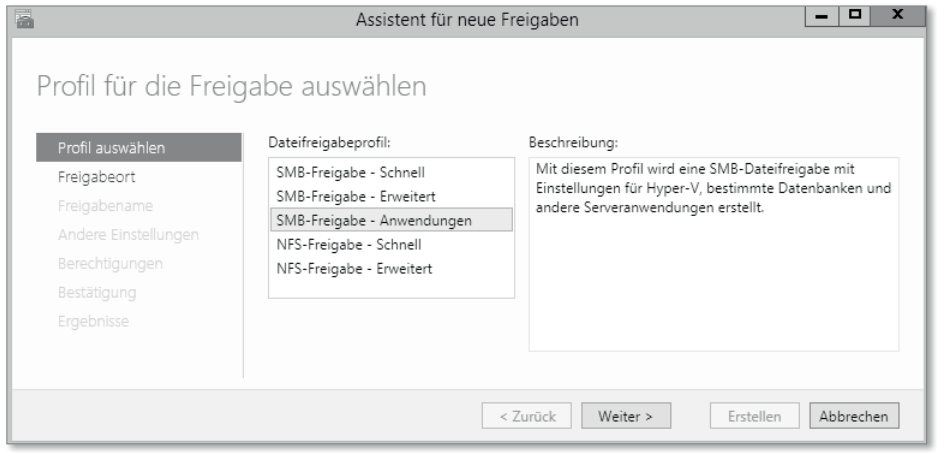


Abbildung 4.23 Auswahl des Freigabeprofils

Auf der Seite Andere Einstellungen des Assistent für neue Freigaben haben Sie unter anderen die Möglichkeit, den Datenzugriff auf die Freigaben zu verschlüsseln. Damit werden sämtliche SMB-Zugriffe von Clients auf den Dateiserver verschlüsselt (Abbildung 4.24).

Anschließend vergeben Sie noch Berechtigungen für den Zugriff auf die SMB-Freigabe und schließen dann den Assistent für neue Freigaben ab. Sie sollten jetzt den Zugriff auf die SMB-Freigabe testen und sich davon überzeugen, dass die Option der fortlaufenden Verfügbarkeit auch ordnungsgemäß funktioniert.

Als Test bietet sich das Programm *FSUTIL.EXE* an, das in der Lage ist, Dateien von beliebiger Größe zu erstellen. Erstellen Sie zum Beispiel eine Datei von 10 GB Größe auf einem Client, und kopieren Sie diese Datei auf die Freigabe des geclusterten Dateiservers. Während des Kopiervorgangs führen Sie dann ein geplantes Failover der Cluster-Rolle auf einen anderen Cluster-Knoten durch, indem Sie in der Failover-Cluster-Verwaltungskonsole in dem Knoten Rollen auf die Dateiserver-Rolle klicken und im Kontextmenü den Menüpunkt Verschieben auswählen, um die Cluster-Rolle auf einen anderen Cluster-Knoten zu verschieben. Die Funktion der fortlaufenden Verfügbarkeit sollte jetzt sicherstellen, dass der Dateikopierprozess nicht unterbrochen wird, wenn SMB 3.0-fähige Clients wie Windows 8 oder Windows Server 2012 auf die Dateifreigabe zugreifen.

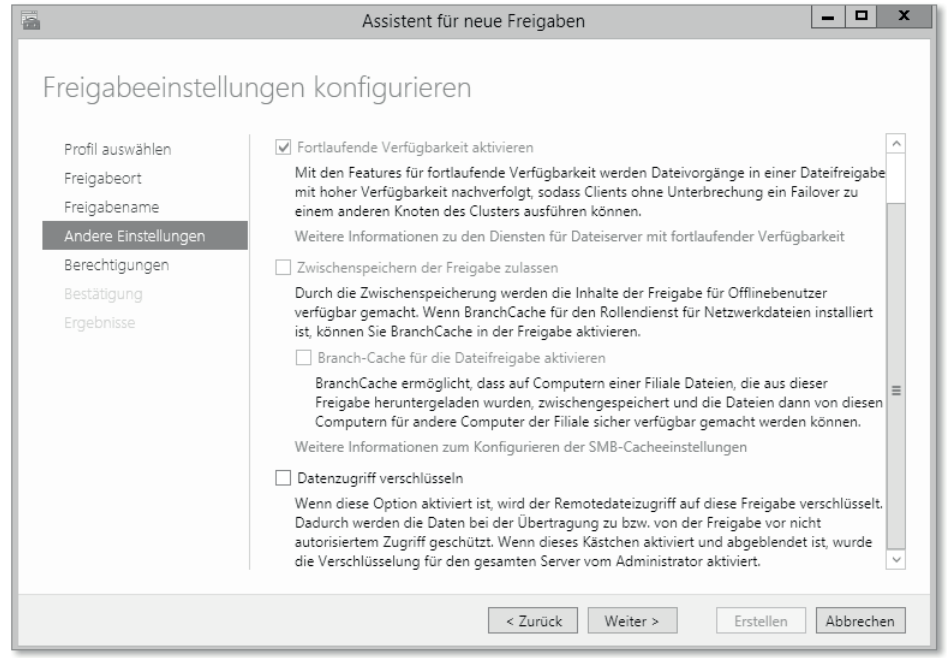


Abbildung 4.24 Erweiterte Freigabeeinstellungen

Nachdem sich die Contoso-Administratoren von der korrekten Funktionsweise des neuen Dateiservers im Failover-Cluster überzeugt haben, können sie mit der Migration der Daten und Freigaben von dem alten Dateiserver beginnen.

4.2.14 Failover-Cluster verwalten

Nach der erfolgten Cluster-Installation und der Konfiguration der ersten Cluster-Rollen ist es nun für den täglichen Betrieb notwendig, dass sich die Administratoren der Contoso AG und der A. Datum GmbH mit den Verwaltungsfunktionen der Failover-Cluster-Verwaltungskonsole vertraut machen, um tägliche Routine- und Überwachungsaufgaben durchführen zu können. Zu den selten notwendigen Tätigkeiten gehört die Festlegung der Berechtigungen zur Verwaltung des Failover-Clusters. Eine Failover-Cluster-Installation legt eine Reihe von Standardberechtigungen fest, wie in Abbildung 4.25 zu sehen ist.

Die Gruppe der lokalen Administratoren hat Vollzugriff auf die gesamte Cluster-Konfiguration. Somit haben auch alle Mitglieder der Gruppe der Domänen-Administratoren Vollzugriff auf die Cluster-Verwaltung, da bei Beitritt des Cluster-Knotens zur Domäne die Gruppe der Domänen-Administratoren der lokalen Gruppe der Administratoren hinzugefügt wird. In speziellen Szenarien kann es nötig sein, anderen Benutzerkonten zusätzliche Berechtigungen zur Cluster-Verwaltung zu erteilen. Bei der Contoso AG erteilen die Administratoren für einen externen Sicherheitsrevisor die Leseberechtigung, damit der Revisor sich einen Überblick über die Cluster-Konfiguration verschaffen kann.

Abbildung 4.25 Cluster-Verwaltungsberechtigungen

Zu den täglichen Aufgaben der Cluster-Administration sollte auch die Auswertung von Cluster-Ereignissen gehören. Die Failover-Cluster-Verwaltungskonsole (Abbildung 4.26) stellt eine aggregierte Sicht der Cluster-Ereignisse zur Verfügung. In der Failover-Cluster-Verwaltungskonsole werden die Ereignisse der letzten 24 Stunden aller Cluster-Knoten angezeigt.

Abbildung 4.26 Anzeige clusterweiter Ereigniseinträge

Für eine detaillierte Auswertung der Cluster-Ereignisse können Sie aber auch die Ereignisanzeige verwenden (siehe Abbildung 4.27). Sie finden die Cluster-Ereignisse, indem Sie in der Ereignisanzeige auf den Knoten Anwendungs- und Dienstprotokolle klicken, Microsoft • Windows auswählen und sich dann zum Beispiel die Ereignisse der Kategorie Failover-Clustering in der Kategorie Betriebsbereit anzeigen lassen.

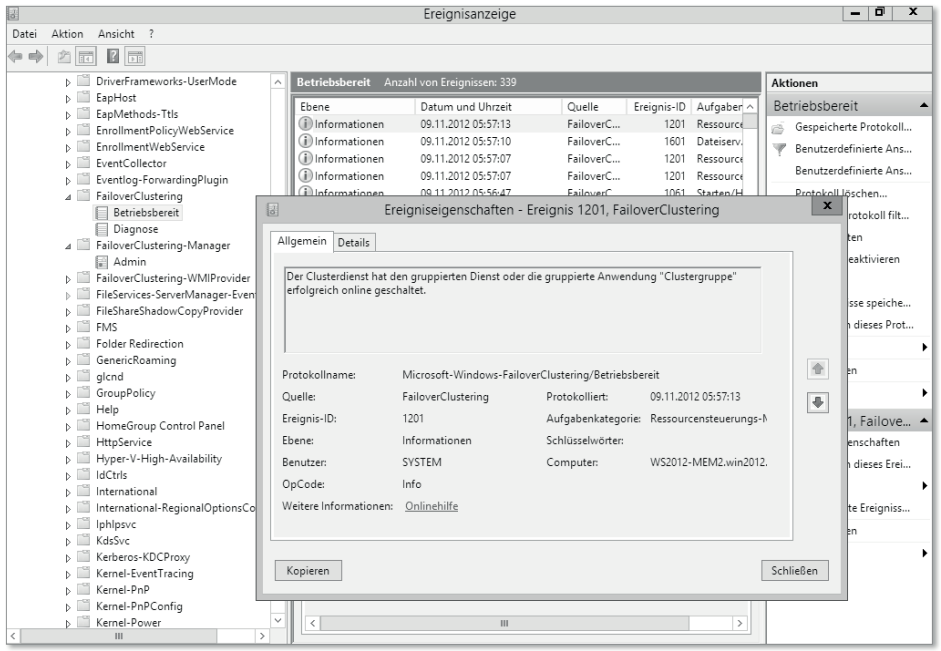


Abbildung 4.27 Detaillierte Anzeige aller clusterrelevanten Informationen

Seit Windows Server 2012 haben Sie nun die Möglichkeit, alle Cluster-Ereignisse sämtlicher Cluster-Knoten der letzten 24 Stunden in der Failover-Cluster-Verwaltungskonsole zurückzusetzen (Abbildung 4.28). Klicken Sie dazu im Kontextmenü des Failover-Cluster-Objekts auf NEUESTE EREIGNISSE ZURÜCKSETZEN.

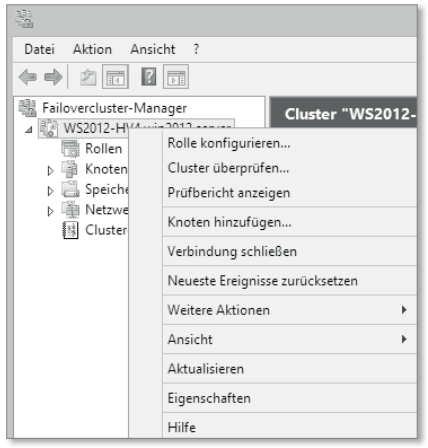


Abbildung 4.28 Cluster-Ereignisse auf allen Cluster-Knoten zurücksetzen

Für ein fundiertes Verständnis der Funktionsweise eines Failover-Clusters ist es wichtig zu verstehen, wie die einzelnen Cluster-Rollen und deren Cluster-Ressourcen in Abhängigkeit zueinander stehen. Eine Cluster-Rolle besteht aus verschiedenen Cluster-Ressourcen, wie zum Beispiel einem Netzwerknamen, IP-Adresse, Festplattenressource etc. Im Fall eines Failovers der Cluster-Rolle oder -Ressource bestimmen die Abhängigkeiten, welche Ressourcen in welcher Reihenfolge verschoben werden müssen. Abbildung 4.29 zeigt die Abhängigkeit einer Netzwerknamenressource von einer Cluster-IP-Adresse.

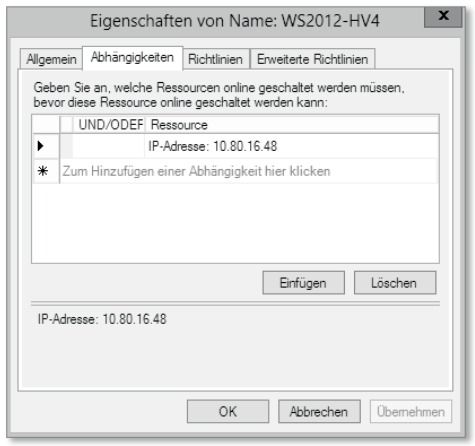


Abbildung 4.29 Cluster-Abhängigkeiten einer Cluster-Ressource

Im Fall eines automatischen oder manuellen Failovers der Cluster-Rolle würden die Cluster-Ressourcen gemäß ihrer Abhängigkeit gestoppt und ein Failover auf einen anderen Cluster-Knoten durchgeführt werden. Dort starten die Komponenten wieder in der Reihenfolge der Abhängigkeiten. Für das Beispiel der Netzwerknamenressource und der Cluster-IP-Adresse würde der Netzwerkname als Erstes offline geschaltet werden und anschließend die Cluster-IP-Adresse. Bei einem Failover auf einen anderen Cluster-Knoten würden die Cluster-Ressourcen in umgekehrter Reihenfolge wieder gestartet werden.

Die Ermittlung der Abhängigkeiten in einem Failover-Cluster mit vielen Cluster-Rollen und -Ressourcen kann sehr aufwendig sein. Aus diesem Grund können Sie sich in der Failover-Cluster-Verwaltungskonsole einen Abhängigkeitsbericht der Ressourcen anzeigen lassen (siehe Abbildung 4.30). Um sich zum Beispiel den Abhängigkeitsbericht des eingerichteten Dateiservers für das horizontale Skalieren anzeigen zu lassen, klicken Sie im Kontextmenü der Dateiserver-Rolle auf WEITERE AKTIONEN • ABHÄNGIGKEITSBERICHT ANZEIGEN.

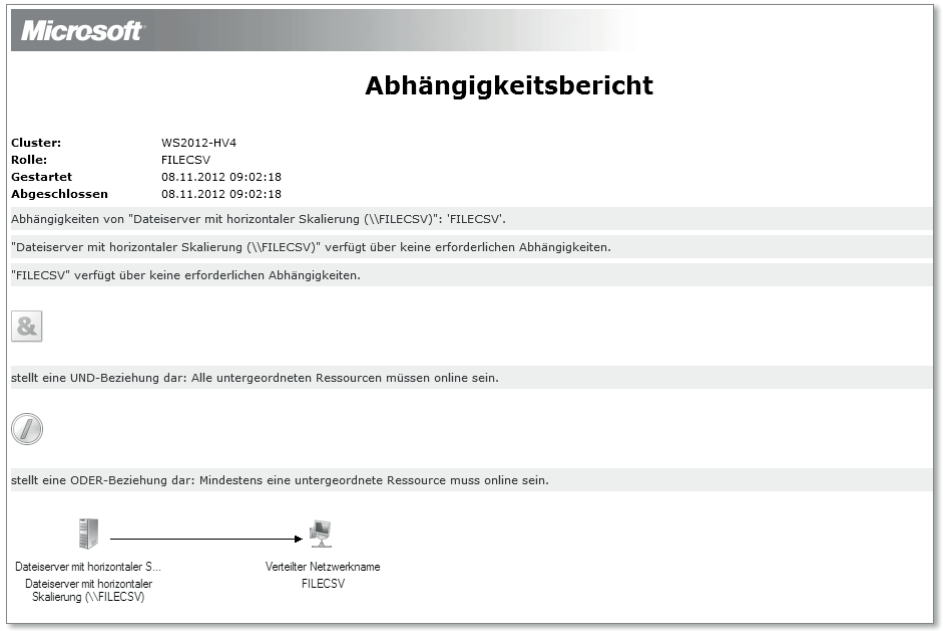


Abbildung 4.30 Cluster-Abhängigkeitsbericht

Für geplante Wartungsarbeiten können Sie ein geplantes Failover von Cluster-Rollen auf einen anderen Cluster-Knoten durchführen, indem Sie in der Failover-Cluster-Verwaltungskonsole im Kontextmenü der Cluster-Rolle VERSCHIEBEN • KNOTEN AUSWÄHLEN anklicken und dann den Ziel-Cluster-Knoten auswählen. Wenn Sie die Option BESTMÖGLICHER KNOTEN verwenden, entscheidet der Cluster-Dienst

anhand der Platzierungseinstellungen, der Besitzer-Vorgaben und anderer Kriterien, auf welchen Cluster-Knoten ein Failover durchgeführt werden soll. Die Cluster-Rolle und alle zugehörigen Ressourcen werden jetzt auf den anderen Cluster-Knoten verschoben. Nach Abschluss der Wartungsarbeiten können Sie die Cluster-Rolle wieder auf den ursprünglichen Cluster-Knoten zurückverschieben. Es besteht die Möglichkeit, einen automatischen Failback der Cluster-Rollen einzurichten (Abbildung 4.31), dieser ist jedoch standardmäßig deaktiviert, und Sie sollten Cluster-Rollen auch nur nach ausgiebigen Tests für einen automatischen Failback konfigurieren.

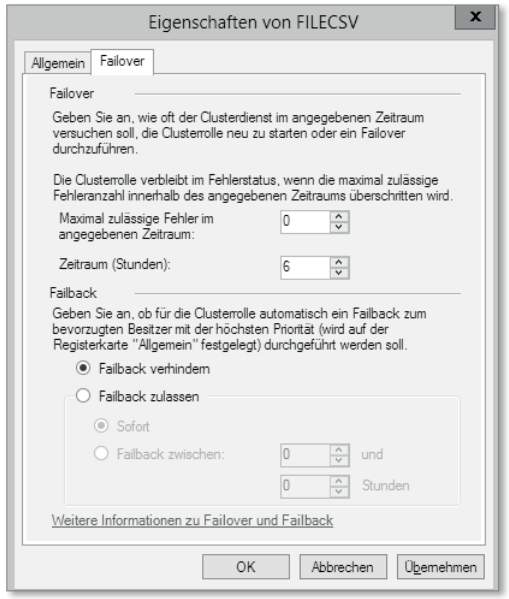


Abbildung 4.31 Failback-Konfiguration

Der Grund ist hier, dass ein automatischer Failback dazu führen könnte, dass Cluster-Rollen in einem »Pingpong-Verfahren« immer zwischen zwei Cluster-Knoten verschoben werden und somit die Verfügbarkeit der Cluster-Rolle wesentlich eingeschränkt ist. Stellen Sie sich dazu folgendes Szenario vor: Der aktuelle Cluster-Knoten als Rolleninhaber hat einen Software-Fehler, der dazu führt, dass der Cluster-Knoten einen Stopp-Fehler (Bluescreen) setzt und automatisch neu startet. Durch den Cluster-Heartbeat erkennt der andere Cluster-Knoten, dass die Kommunikation zu seinem Partner unterbrochen wurde, und führt ein Failover der Cluster-Rollen durch. Der ursprüngliche Cluster-Knoten nimmt nach seinem Neustart seine Funktionen wieder auf, tritt dem Failover-Cluster erneut bei, und der Cluster führt einen Failback der Cluster-Rollen durch. Kurze Zeit später bootet der aktuelle Cluster-Knoten aufgrund des Bluescreens erneut – der eigentliche Fehler ist ja noch gar nicht behoben. Der Failover-/Failback-Prozess wiederholt sich in einer Schleife.

Zu einer ganzheitlichen Verwaltung eines Failover-Clusters gehört neben der täglichen Auswertung von Windows-Ereignissen auch eine regelmäßige Leistungsüberwachung, um bei Leistungsproblemen eine qualifizierte Aussage über mögliche Leistungsengpässe treffen zu können. Aus diesem Grund gehört es zu den Best Practices, nach erfolgter Failover-Cluster-Installation eine *Performance-Baseline* zu erstellen. Die Performance-Baseline kann dann zu Vergleichen herangezogen werden, wenn es im laufenden Betrieb des Clusters zu Leistungsproblemen kommt, indem die Baseline mit den aktuellen Werten der Leistungsmessung verglichen wird. Windows Server 2012 liefert hierfür das Leistungsüberwachungs-Tool, das die Leistung zahlreicher Windows-Komponenten und Anwendungen überwachen kann. Während der Installation der Failover-Cluster-Funktion wird die Leistungsüberwachung um zahlreiche clusterspezifische Leistungsindikatoren erweitert, wie in Abbildung 4.32 zu sehen ist.

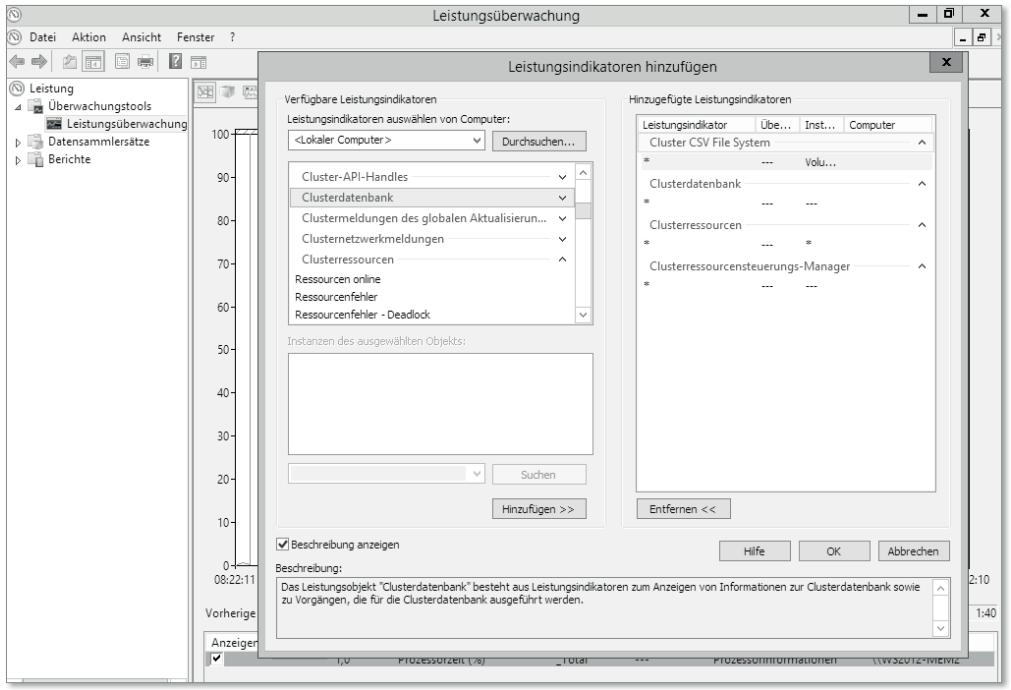


Abbildung 4.32 Failover-Cluster-Überwachung mit der Windows-Leistungsüberwachung

Mithilfe dieser Leistungsindikatoren können Sie sehr detailliert die Leistung der einzelnen Komponenten zur Laufzeit ermitteln, aber auch eine Performance-Baseline für spätere Vergleiche erstellen. Eine Übersicht über empfohlene Leistungsindikatoren, die überwacht werden können, finden Sie auf folgender Webseite: *http://blogs.msdn.com/b/clustering/archive/2009/09/04/9891266.aspx* (Kurzlink: *http://qccq.de/s/h406*).

4.2.15 Clusterfähiges Aktualisieren

Bei der *clusterfähigen Aktualisierung* (CAU: Cluster Aware Updating) handelt es sich um eine Funktion in Windows Server 2012, die Software-Updates auf allen Cluster-Knoten durchführt, ohne eine Unterbrechung der Dienste zu verursachen. Dies setzt Funktionen wie die Live-Migration von virtuellen Maschinen in einem Hyper-V-Cluster oder bei Dateiservern die Funktion des horizontalen Skalierens (Scale-out Fileserver) voraus. Bei allen anderen Cluster-Rollen wird von CAU ein normales Failover der Ressourcen auf einen anderen Cluster-Knoten durchgeführt.

CAU umfasst folgende Funktionen:

- Konfiguration des CAUs mithilfe der Failover-Verwaltungskonsole (Abbildung 4.33) oder mit PowerShell-Cmdlets
- Verwaltung von CAU mit der eigenständigen Anwendung *ClusterUpdateUI.exe* im Verzeichnis *%systemroot%\system32*
- Integration in die vorhandene Windows Update-Infrastruktur (WU)
- Integration in die Windows Server Update Services (WSUS) von Windows Server 2012
- Verwendung der Windows Management Instrumentation (WMI)
- Nutzung des Windows Remote Managements (WinRM)
- Update-Ausführungsprofile, die die Einstellungen für das CAU konfigurieren
- eine erweiterbare Architektur, die zusätzlich zu dem standardmäßigen Windows Update-Plug-in zusätzliche Plug-ins von Drittanbietern unterstützt, um zum Beispiel BIOS- oder Firmware-Aktualisierungen für die Cluster-Hardware in CAU zu unterstützen

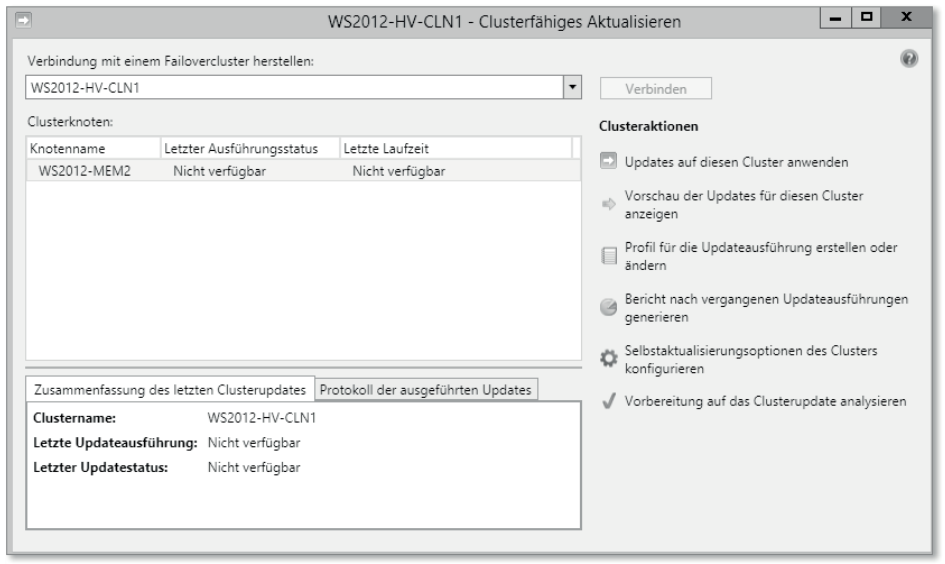


Abbildung 4.33 CAU-Verwaltungskonsole

CAU wurde nur für bestimmte Cluster-Rollen getestet

Für Windows Server 2012 wurden von Microsoft nur die folgenden Cluster-Rollen für CAU getestet und zertifiziert: SMB 3.0, Hyper-V, DFS-Replikation, DFS-Namespaces, iSCSI und NFS.

CAU führt folgende Tätigkeiten durch:

- Aktiviert den Wartungsmodus für den Cluster-Knoten, der von CAU mit Updates versorgt werden soll.
- Verschiebt die Cluster-Rollen zu einem anderen Cluster-Knoten per Live-Migration oder klassischem Failover.
- Installiert die notwendigen Updates.
- Führt einen Neustart des Cluster-Knotens durch, wenn das notwendig ist.
- Entfernt den Cluster-Knoten aus dem Wartungsmodus.
- Verschiebt die Cluster-Rollen wieder zurück auf den Cluster-Knoten.
- Wiederholt die Update-Aufgaben auf einem nächsten Cluster-Knoten.

CAU ermöglicht zwei Arten von Aktualisierungen von Cluster-Knoten:

- Remote-Aktualisierung
- Selbstaktualisierung

Bei der *Remote-Aktualisierung* können Sie von einem Computer mit Windows 8 oder Windows Server 2012 aus eine CAU-Aktualisierungsausführung starten. Sie können eine Aktualisierungsausführung über die Benutzeroberfläche (Teil der *Remote Server Administration Tools*, *RSAT*) oder mithilfe des PowerShell-Cmdlets `Invoke-CauRun` starten. Bei der Remote-Aktualisierung handelt es sich um den Standardaktualisierungsmodus für CAU. Mit der Aufgabenplanung von Windows Server 2012 oder Windows 8 können Sie das PowerShell-Cmdlet `Invoke-CauRun` per Zeitplan auf einem Remote-Computer ausführen, bei dem es sich nicht um einen der Cluster-Knoten handelt.

Einschränkungen bei der Remote-Aktualisierung

Bei der Verwendung der Remote-Aktualisierung stehen nicht alle CAU-Funktionen zur Verfügung. Details über die Einschränkungen im Remote-Aktualisierungsmodus liefert die Cluster-Online-Hilfe.

Mithilfe der *Selbstaktualisierung* kann der Failover-Cluster basierend auf einem Update-Ausführungsprofil selbstständig eine Aktualisierung des Clusters durchführen. Damit der Selbstaktualisierungsmodus genutzt werden kann, müssen Sie dem

Cluster die CAU-Cluster-Rolle hinzufügen. Diese steht dann wie jede andere Cluster-Rolle im gesamten Cluster zur Verfügung und kann über die gewohnten Cluster-Failover-Mechanismen auf unterschiedlichen Cluster-Knoten ausgeführt werden.

CAU verwendet Cluster-APIs (Application Programming Interface), um das Failover und den Failback von Cluster-Rollen und -Ressourcen effizient zu verwalten. Die Cluster-API-Implementierung wählt die Cluster-Knoten durch interne Metriken und intelligente Platzierungsheuristiken (wie zum Beispiel die Arbeitsauslastung der Cluster-Knoten) aus.

Von CAU wird für die Cluster-Knoten kein Lastenausgleich ausgeführt. CAU versucht aber, zugehörige Cluster-Rollen zusammenhängend auf einen anderen Cluster-Knoten zu verschieben. Sobald die Aktualisierung eines Cluster-Knotens durch CAU beendet wurde, werden die Cluster-Rollen wieder von einem anderen Cluster-Knoten auf den ursprünglichen Inhaber verschoben.

CAU und der SCVMM

Worin unterscheidet sich CAU nun von der Funktion des System Center 2012 Virtual Machine Managers (VMM), die ebenfalls alle Hyper-V-Server zentral mit notwendigen Windows Updates versorgt?

Von System Center 2012 Virtual Machine Manager werden nur Hyper-V-Cluster und alleinstehende Hyper-V-Server aktualisiert, während mit CAU beliebige Typen unterstützter Failover-Cluster, einschließlich der Hyper-V-Cluster, aktualisiert werden können. Wenn Sie also Cluster einsetzen, die nicht ausschließlich Hyper-V als Cluster-Rolle installiert haben, sollten Sie für diese Cluster-Rollen CAU verwenden. Wenn Sie eine Lizenz für System Center besitzen, empfehlen wir die Verwendung von CAU für andere Cluster-Rollen als Hyper-V und den VMM für die Automatisierung von Updates für Hyper-V. Da CAU nur auf Windows Server 2012 unterstützt wird, müssen Sie für Hyper-V-Cluster auf älteren Windows-Betriebssystemen ohnehin den VMM verwenden, wenn Sie nicht den System Center 2012 Configuration Manager einsetzen oder ein manuelles Update der Cluster-Knoten durchführen.

Für die Automatisierung von Updates in einem Failover-Cluster kann, wie bereits erwähnt, die Failover-Cluster-Verwaltungskonsole oder die PowerShell verwendet werden. Beiden Verwaltungsinstrumenten ist gemeinsam, dass die meisten Einstellungen in einer XML-Datei gespeichert werden können, um diese in Update-Ausführungsprofilen zu verwenden. Weitere Informationen zu dieser Funktion finden Sie in dem Artikel *http://technet.microsoft.com/de-DE/library/jj134224* (Kurzlink: *http://qccq.de/s/h407*).

Die Funktionen von CAU werden mithilfe von Plug-ins bereitgestellt und erweitert. Windows Server 2012 wird mit zwei Plug-ins ausgeliefert:

- Microsoft.WindowsUpdatePlugin
- Microsoft.HotfixPlugin

Zusätzliche verfügbare Plug-ins von Drittanbietern müssen separat installiert werden. Wenn Sie den Selbstaktualisierungsmodus von CAU verwenden, muss das Plug-in auf allen Cluster-Knoten installiert werden. Das ist nicht der Fall bei der Remote-Aktualisierung, bei der das Plug-in nur auf dem Remote-Computer installiert werden muss, den Sie für die Ausführung von CAU verwenden. Zur Registrierung von CAU-Plug-ins müssen Sie die PowerShell und das Commandlet `Register-CauPlugin` verwenden. Weitere Informationen zur Installation und Konfiguration von Plug-ins liefert der Artikel *http://technet.microsoft.com/de-de/library/jj134213.aspx* (Kurzlink: *http://qccq.de/s/h408*).

4.2.16 Die Aufgabenplanung einbinden

Mithilfe des Aufgabenplaners von Windows Server 2012 können Administratoren automatisiert Aufgaben ausführen, zum Beispiel für Wartungsaufgaben in einer Cluster-Umgebung oder für regelmäßige Tätigkeiten wie das Ausführen von Wartungsskripten, Backup-Skripten etc. Vor Windows Server 2012 mussten die Aufgaben immer auf jedem Cluster-Knoten manuell angelegt werden. Man konnte dort zwar Aufgaben des Aufgabenplaners exportieren und auf einen anderen Cluster-Knoten importieren, mit einer steigenden Anzahl an Cluster-Knoten ist dieser Aufwand jedoch nicht zu unterschätzen.

Seit Windows Server 2012 kann die PowerShell Aufgaben für den Aufgabenplaner erstellen, die clusterfähig sind und somit auf jedem Cluster-Knoten ausgeführt werden können. Microsoft hat sich für diese Möglichkeit entschieden, da mit Windows Server 2012 bis zu 64 Cluster-Knoten in einem Failover-Cluster laufen können.

In Windows Server 2012 existieren drei Typen von Aufgaben im Aufgabenplaner:

1. **Ausführung auf jedem Cluster-Knoten**
   Die Aufgabe kann auf jedem Cluster-Knoten ausgeführt werden. Die Cluster-Verwaltung stellt jedoch sicher, dass die Aufgabe immer nur auf einem Cluster-Knoten ausgeführt wird.
2. **Ressourcenspezifische Ausführung**
   Die Aufgabe wird nur in einer Instanz für eine spezifische Cluster-Ressource ausgeführt. Die Aufgabe wird auf dem Cluster-Knoten ausgeführt, der aktuell der Besitzer der Ressource ist. Ein Beispiel für eine ressourcenspezifische Ausführung ist die Zuordnung einer Aufgabe zur Defragmentierung einer Festplatte an eine Disk-Ressource.

3. **Ausführung im gesamten Cluster**
   Die Aufgabe wird nur als eine Instanz auf allen Cluster-Knoten des Failover-Clusters ausgeführt. Die Aufgabe wird somit auf allen Cluster-Knoten zeitgleich ausgeführt.

Die Verwaltung der Aufgaben in einem Cluster kann ausschließlich mithilfe der PowerShell erfolgen. Mit der PowerShell erstellte Aufgaben treten zwar im grafischen Verwaltungs-Tool des Aufgabenplaners auf, können dort aber lediglich eingesehen werden.

Die am häufigsten verwendeten PowerShell-Befehle sind:

- `Get-ClusteredScheduledTask`
  Erstellt eine Abfrage aller clusterrelevanten geplanten Aufgaben.
- `Register-ClusteredScheduledTask`
  Erstellt eine Aufgabe in einem Failover-Cluster.
- `Set-ClusteredScheduledTask`
  Modifiziert eine bereits erstellte Aufgabe im Cluster.
- `Unregister-ClusteredScheduledTask`
  Entfernt die geplante Aufgabe aus dem Cluster.

Das folgende Beispiel zeigt die Erstellung einer Aufgabe im Cluster zur Defragmentierung der LUN für das Hyper-V Cluster Shared Volume (CSV) mithilfe der PowerShell:

```
Register-ClusteredScheduledTask -Cluster Contoso-CL1 ↩
-TaskName DefragCLUDisk -TaskType ResourceSpecific ↩
-Resource Hyper-V-CSV -Action $action -Trigger $trigger
```

Das nächste Beispiel zeigt die Erstellung einer Aufgabe für ein automatisches Backup einer Ressource, aktiv ausgeführt auf einem Cluster-Knoten:

```
Register-ClusteredScheduledTask -Cluster Contoso-CL1 ↩
-TaskName BackupCSV-Disk -TaskType AnyNode -Action ↩
$action -Trigger $trigger
```

Das letzte Beispiel zeigt die Ausführung einer Aufgabe im Cluster zur automatischen Anmeldung eines Dienstkontos auf allen Cluster-Knoten:

```
Register-ClusteredScheduledTask -Cluster Contoso-CL1 ↩
-TaskName AutoLogin -TaskType ClusterWide -Action ↩
$action -Trigger $trigger
```

4.2.17 Node Vote Weights

In Windows Server 2012 lässt sich in der Failover-Cluster-Verwaltungskonsole festlegen, welche Cluster-Knoten als *Voter* (Zeuge) in einem Failover-Cluster fungieren

können. Standardmäßig ist jeder Cluster-Knoten ein Voter im Cluster und wird von dem Cluster zur Berechnung der Quorum-Mehrheit verwendet. Auch wenn ein Cluster-Knoten nicht mehr als Voter fungiert, arbeitet der Cluster weiterhin, Cluster-Datenbank-Updates werden weiterhin durchgeführt und der Cluster-Knoten kann Cluster-Anwendungen hosten. Ein Grund für die Änderung der Cluster-Voter sind Multi-Site-Cluster mit Windows Server 2012. Mit der neuen Funktion können Sie Cluster-Knoten im Backup-Rechenzentrum aus der Berechnung der Quorum-Mehrheit entfernen. Diese Einstellung ist nützlich, wenn Sie das Failover von Cluster-Rollen und -Ressourcen in das Backup-Rechenzentrum manuell initialisieren möchten.

Das *Cluster Node Weight* kann mithilfe der PowerShell ermittelt und geändert werden. Der Befehl

```
Get-Clusternode |fl -property Nodename, State, NodeWeight
```

zeigt das Cluster Node Weight an. Der Wert 0 zeigt an, dass der Cluster-Knoten kein Node Weight hat, der Wert 1 (Standard) besagt, dass der Cluster-Knoten ein Voter im Cluster ist.

4.2.18 Node Drain

Windows Server 2012 vereinfacht es, einen Cluster-Knoten in den Wartungsmodus zu versetzen, um zum Beispiel Software- oder Hardware-Wartung durchzuführen. Auf einem Cluster in Windows Server 2008 R2 mussten Sie einen Cluster-Knoten zu Wartungszwecken manuell in den Wartungsmodus versetzen und anschließend die aktiven Cluster-Rollen und -Ressourcen auf einen anderen Cluster-Knoten verschieben.

Mit Windows Server 2012 können Sie jetzt den Cluster-Knoten anhalten, den Sie zu Wartungszwecken aus dem Cluster nehmen möchten, und die Rollen ausgleichen. Mit dieser Funktion werden alle aktiven Cluster-Rollen und -Ressourcen auf einen anderen Cluster-Knoten basierend auf den Cluster-Platzierungseinstellungen verschoben, und der Cluster-Knoten wird anschließend in den Wartungsmodus versetzt. Sie können jetzt Wartungsarbeiten an dem Cluster-Knoten durchführen und nach erfolgter Wartung den Cluster-Knoten wieder zum Cluster hinzufügen, indem Sie in der Failover-Cluster-Verwaltungskonsole auf den Knoten klicken und im Kontextmenü Fortsetzen und Failback für Rollen ausführen auswählen (siehe Abbildung 4.34).

Cluster-Wartungsmodus wird auch von CAU verwendet

Die neue Funktion des Wartungsmodus wird auch von der neuen Funktion des clusterfähigen Aktualisierens verwendet.

Der Wartungsmodus kann auch mithilfe der PowerShell konfiguriert werden. Der folgende Befehl verschiebt alle aktiven Ressourcen von Cluster-Knoten CLU-CLN01 auf CLU-CLN02:

```
Suspend-ClusterNode -Name CLU-CLN01 -Target CLU-CLN02 –Drain
```

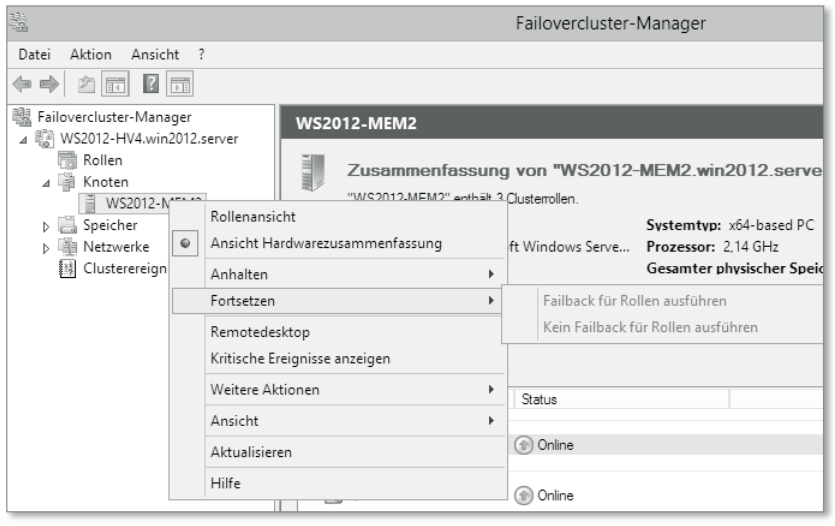


Abbildung 4.34 Node Drain

Der Wartungsmodus schlägt fehl, wenn eine Live-Migration einer virtuellen Maschine im Vorfeld gescheitert ist oder eine Cluster-Rolle nicht verschoben werden konnte, weil dieser Cluster-Knoten der letzte mögliche Eigentümer der Cluster-Ressource ist.

Da das Verschieben von Cluster-Ressourcen und -Rollen ein sehr zeitaufwendiger Prozess sein kann, lässt sich der Wartungsmodus abbrechen. Dazu wählen Sie in der Failover-Cluster-Verwaltungskonsole auf der Ebene des Cluster-Knotens FORTSETZEN. Die bereits verschobenen Cluster-Ressourcen werden dann wieder auf den ursprünglichen Cluster-Knoten verschoben.

Wenn in dem Failover-Cluster als Cluster-Rolle Hyper-V ausgeführt wird, verwendet der Cluster-Wartungsmodus die Live-Migration, um virtuelle Maschinen unterbrechungsfrei auf einen anderen Cluster-Knoten zu verschieben. Da das Verschieben von vielen virtuellen Maschinen per Live-Migration ein sehr zeitaufwendiger Prozess sein kann, können Administratoren statt der Live-Migration eine Quick-Migration nutzen, die zu einer kurzen Ausfallzeit der Dienste in der virtuellen Maschine führt.

4.2.19 Virtual Machine Monitoring

Die Failover-Cluster-Funktion in Windows Server 2012 bietet eine neue Funktion zur Überwachung der Dienste von virtuellen Maschinen (VM) in einer Hyper-V-Cluster-Umgebung. Diese arbeitet mit den Wiederherstellungsoptionen von Diensten des Betriebssystems der virtuellen Maschine zusammen.

Bei Auftreten eines ersten und zweiten Dienstfehlers versucht Windows, den Dienst in der virtuellen Maschine neu zu starten. Sollte der Dienst nach dem zweiten Versuch nicht starten, stellt der Dienst-Manager der virtuellen Maschine weitere Wiederherstellungsaktionen ein und übergibt die weitere Fehlerbehebung an den Cluster-Dienst von Windows Server 2012. Der Cluster-Dienst überwacht die Dienste in periodischen Abständen; kann ein Dienst nicht wiederhergestellt werden, setzt der Cluster den Status der virtuellen Maschine auf *Unhealthy* und löst weitere Aktionen aus:

- Die Ereignisanzeige der virtuellen Maschine protokolliert die Ereignis-ID 1250, sodass andere Programme wie der System Center 2012 Operations Manager reagieren können.
- Der Status der virtuellen Maschine wechselt zu APPLICATION IN VM CRITICAL.
- Die virtuelle Maschine wird auf demselben Cluster-Knoten neu gestartet. Läuft der Dienst in der virtuellen Maschine nach dem Neustart immer noch nicht, wird die VM auf einem anderen Cluster-Knoten erneut gestartet.

Damit der Cluster-Dienst die virtuelle Maschine überwachen kann, sind folgende Voraussetzungen zu schaffen:

- Das Hyper-V-Betriebssystem muss Windows Server 2012 oder Microsoft Hyper-V Server 2012 sein.
- Die virtuelle Maschine muss als Betriebssystem Windows Server 2012 ausführen, und für den *VM-Heartbeat* müssen die Hyper-V-Integrationskomponenten in aktueller Fassung installiert und aktiviert sein.
- Das Betriebssystem in der virtuellen Maschine muss Mitglied derselben Domäne wie der Hyper-V-Host oder einer vertrauenswürdigen Domäne sein.
- Der Administrator des Hyper-V-Clusters benötigt lokale administrative Berechtigungen in der virtuellen Maschine.
- Die Firewall der virtuellen Maschine muss eine Ausnahme für die Überwachung der virtuellen Maschine konfiguriert haben.

Die Überwachung der Dienste einer virtuellen Maschine kann mithilfe der Failover-Cluster-Verwaltungskonsole oder mit der PowerShell (Abbildung 4.35) eingerichtet werden.

Zur Einrichtung der Überwachung mit der Failover-Cluster-Verwaltungskonsole navigieren Sie zu der virtuellen Maschine, wählen im Kontextmenü Weitere Aktionen aus und klicken dann auf Überwachung konfigurieren.

Um mithilfe der PowerShell beispielweise den Druck-Spooler-Dienst einer virtuellen Maschine zu überwachen, können Sie folgenden Befehl verwenden:

```
Add-ClusterVMMonitoredItem -VirtualMachine Contoso-SRV1 ↵
-Service spooler
```

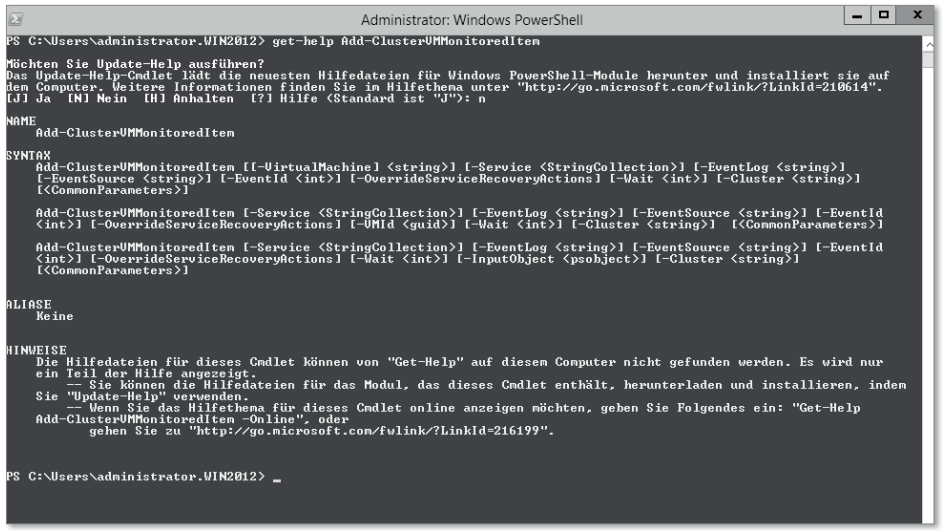


Abbildung 4.35 PowerShell-Cmdlet zur Einrichtung des VM-Monitorings

4.2.20 Cluster per PowerShell verwalten

Da das Cluster-Kommandozeilenprogramm *Cluster.exe* in Windows Server 2012 nicht mehr zur Verfügung steht, wurde die PowerShell um die Möglichkeit erweitert, die Cluster-Verwaltung mithilfe von PowerShell-Cmdlets durchzuführen.

Für jeden PowerShell-Befehl können Sie sich eine detaillierte Hilfe anzeigen lassen. Mit den Befehlen

```
Get-Help <cmdlet name> -Detailed
Get-Help <cmdlet name> -Examples
Get-Help <cmdlet name> -Full
```

erhalten Sie eine Übersicht über die Commandlets und deren Funktion sowie mögliche Parameter.

Mit dem Befehl `Get-Cluster` erhalten Sie eine Übersicht über den konfigurierten Cluster. Möchten Sie sich alle Cluster-Ressourcen anzeigen lassen, verwenden Sie den

Befehl `Get-ClusterResource`. Das Hinzufügen von Ressourcen zum Cluster erfolgt mit dem Befehl `Add-ClusterServerRole` oder `Add-ClusterResource`. Mit dem Befehl `Move-ClusterGroup` können Sie Ressourcengruppen oder Cluster-Rollen auf einen anderen Cluster-Knoten verschieben.

Mit den Commandlets, die mit Remove beginnen, können Sie Cluster-Ressourcen, Cluster-Knoten oder Datenträgerressourcen entfernen. Das Commandlet `Remove-ClusterGroup` entfernt zum Beispiel eine Cluster-Gruppe aus dem Failover-Cluster.

Mit den Set-Cmdlets können Sie Cluster-Parameter setzen und verändern. Das Commandlet `Set-ClusterLog` ermöglicht zum Beispiel die Festlegung der maximalen Größe des Cluster-Logs sowie der Detailtiefe der zu überwachenden Einträge.

Weitere Informationen zur Verwaltung des Windows-Failover-Clusters mithilfe der PowerShell finden Sie auf der Webseite *http://technet.microsoft.com/en-us/library/hh847239.aspx* (Kurzlink: *http://qccq.de/s/h401*).

4.2.21 Neu in Windows Server 2012 R2

In Windows Server 2012 R2 hat Microsoft die grundlegende Funktion des Failover-Clusters nicht verändert. Was Sie in den vorangegangenen Abschnitten darüber gelesen haben, trifft also zum größten Teil auch weiter zu. Verbesserungen bringt die R2-Version vor allem im Hinblick auf die Skalierbarkeit und die Stabilität mit. Viele der neuen Funktionen arbeiten gewissermaßen »unsichtbar« im Hintergrund, ohne dass Sie sie konfigurieren müssen.

Eine systematische Übersicht der neuen Funktionen und ihrer Details finden Sie bei Microsoft unter der Adresse:

http://technet.microsoft.com/en-us/library/dn265972.aspx (Kurzlink: *http://qccq.de/s/h409*)

Das Cluster-Dashboard

Eine kleine, aber nützliche Änderung hat der Failover-Cluster-Manager erfahren. Er bietet nun eine schnelle Statusansicht für alle verbundenen Cluster. Viele Kunden verwalten mehrere Windows-Cluster parallel, und mit Windows Server 2012 R2 wird dies noch zunehmen. So könnte es mehrere separate Hyper-V-Cluster geben, die an einen (oder mehrere) Dateiserver-Cluster vom Typ Scale-Out Fileserver angebunden sind. Auf Ebene der virtuellen Maschinen sind mittlerweile sogenannte »Gast-Cluster« sehr verbreitet (siehe dazu den Abschnitt 4.2.12, »Gast-Cluster«).

Haben Sie also mehrere Failover-Cluster, so können Sie diese nun auf Ihrer Administrator-Workstation bequem parallel mit einer einzigen Konsole des Failover-Cluster-Managers verwalten. Das Dashboard zeigt Ihnen auf einen Blick den jeweiligen Cluster-Aufbau und den Zustand der Systeme (vgl. Abbildung 4.36).

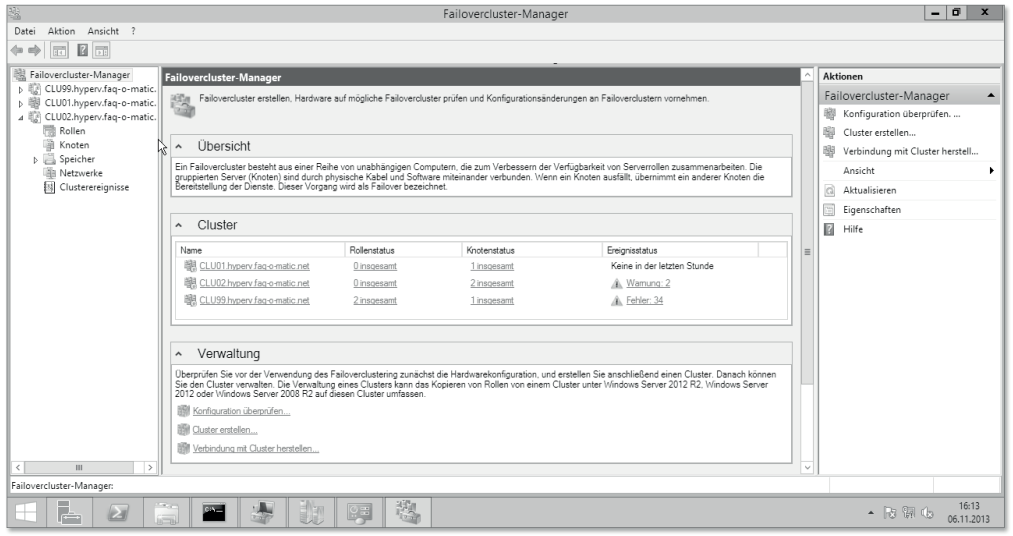


Abbildung 4.36 Der Hyper-V-Manager in Windows Server 2012 R2 gibt eine schnelle Übersicht über den Zustand mehrerer parallel arbeitender Cluster.

Auch die Quorum-Stimmenzahl können Sie auf einen Blick kontrollieren. Klicken Sie dazu auf den Zweig KNOTEN. Der Failover-Cluster-Manager listet im Detailbereich die grundsätzliche Zahl der Stimmen *(Vote)* und die tatsächliche aktuelle Stimmenverteilung der einzelnen Cluster-Knoten auf (siehe Abbildung 4.37).

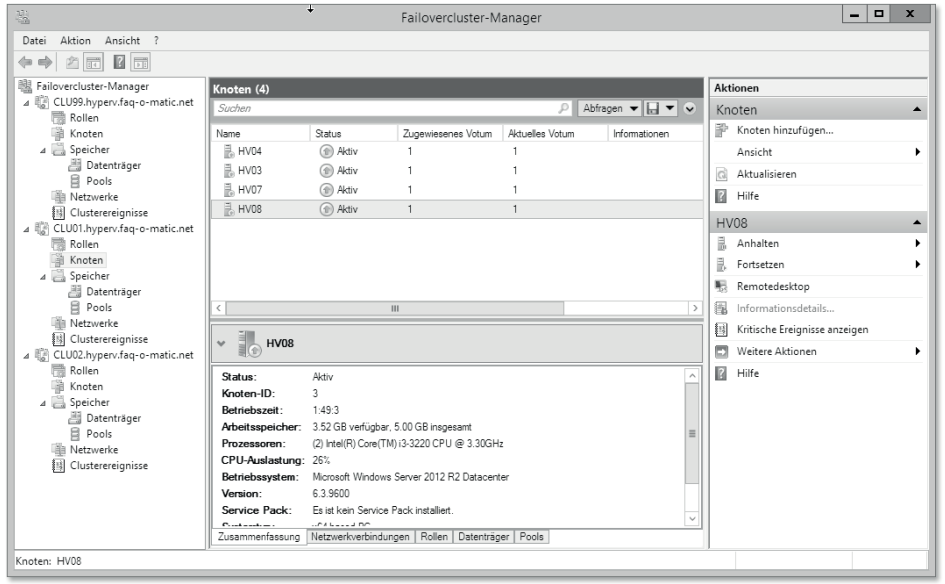


Abbildung 4.37 In der Übersicht der Cluster-Knoten lässt sich die Stimmenzahl für das Quorum ablesen.

Virtual Machine Drain

Wenn Sie einen Hyper-V-Cluster-Knoten herunterfahren, so wird dieser automatisch alle seine laufenden VMs auf andere Knoten im selben Cluster per Live-Migration verschieben. Dies erleichtert den Vorgang für Sie als Administrator und sorgt gleichzeitig für eine höhere Betriebssicherheit.

Schon vorher konnten Sie natürlich die VMs eines Host-Servers auf andere Hosts im Cluster migrieren, sie mussten dies aber manuell tun. In Windows Server 2012 hat der Failover-Cluster dies durch *Node Drain* (siehe Abschnitt 4.2.18, »Node Drain«) erleichtert, doch auch diese Funktion mussten Sie ausdrücklich aufrufen.

Fuhren Sie bisher einen Host-Server herunter, ohne die VMs zu verschieben, so hat Hyper-V diese per Schnellmigration *(Quick Migration)* übertragen, also in den gespeicherten Zustand versetzt und auf einem anderen Host fortgesetzt. Dies führte zu einer kurzen Unterbrechung der VM (und bei bestimmten Applikationen konnte es sogar zu Problemen führen). Die neue Automatik *Virtual Machine Drain* sorgt beim Herunterfahren von selbst für die Live-Migration und vermeidet so unerwünschte Ausfallzeiten für die virtuellen Maschinen.

Mithilfe der PowerShell können Sie diese Funktion ein- oder ausschalten, indem Sie die Eigenschaft *DrainOnShutdown* des Clusters auf 0 (aus) oder 1 (ein, dies ist der Standardwert) setzen. Folgendes Kommando zeigt den aktuellen Zustand:

```
(Get-Cluster).DrainOnShutdown
```

Optimierte Cluster-Überwachung

Da es in Hyper-V-Clustern Situationen geben kann, in denen die Netzwerklatenz für die Cluster-Kommunikation höher ist als normal, ohne dass dies einen Fehler darstellt, hat Microsoft für dieses Szenario die clusterinternen Überwachungseinstellungen geändert. Während allgemein der Cluster-Dienst nach dem Ausbleiben der Heartbeatsignale eines Cluster-Knotens für fünf Sekunden ein Failover einleitet, liegt die Grenze nur für Hyper-V-Cluster-Knoten nun bei zehn Sekunden im selben Subnet und bei 20 Sekunden für Knoten in anderen IP-Subnets.

Im Normalfall senden alle Cluster-Knoten, auch die mit der Hyper-V-Rolle, jede Sekunde ein Heartbeatsignal an ihre Partner. Sie können davon ausgehen, dass dies im Regelfall auch eingehalten wird. Aufgrund der Besonderheiten im Hyper-V-Netzwerkstack haben einige Kunden aber festgestellt, dass das kurze Timeout-Intervall von fünf Sekunden manchmal zu unnötigen Failover-Vorgängen führt.

Tatsächlich können Sie den Wert sogar selbst konfigurieren. Microsoft rät allerdings davon ab, weil hierdurch leicht Folgefehler entstehen können, die schwierig aufzudecken sind. Sollten Sie Bedarf zur Eigenkonfiguration haben, so setzen Sie über die PowerShell mit dem Commandlet `Set-ClusterParameter` die Parameter `SameSubnetThreshold` bzw. `CrossSubnetThreshold` auf den gewünschten Wert in Sekunden.

Dynamisches Quorum-Modell

Im Abschnitt 4.2.9 »Cluster-Quorum« haben wir Ihnen die Quorum-Einstellungen für den Cluster vorgestellt. In Windows Server 2012 schlägt Windows selbst das am besten geeignete Quorum-Modell vor, und Sie können es im laufenden Betrieb verändern. Die R2-Version geht noch weiter und setzt das passende Modell automatisch anhand der verfügbaren Informationen über den Cluster. Auch nach Veränderungen im Cluster-Aufbau brauchen Sie also normalerweise nichts selbst an der Konfiguration des Quorums zu ändern, weil Windows selbst dafür sorgt.

Technisch verbirgt sich dahinter ein recht einfacher Mechanismus, der immer dann aktiv werden kann, wenn neben den eigentlichen Cluster-Knoten auch ein Zeuge im Cluster vorhanden ist, also eine Quorum-Disk oder ein zusätzlicher Server (zu den Möglichkeiten siehe den Abschnitt 4.2.9 »Cluster-Quorum«). Der Cluster untersucht laufend die Anzahl der Stimmen, die die Cluster-Knoten gemeinsam haben. Sollte diese gerade sein, so erhält auch der Zeuge eine Stimme, um zu einer ungeraden Gesamtsumme zu kommen. Ist die Zahl der aktiven Cluster-Knoten ungerade, so setzt Windows den Stimmenwert des Zeugen auf 0 (null).

Den aktuellen Wert können Sie über die PowerShell überprüfen:

```
(Get-Cluster).WitnessDynamicWeight
```

Entscheidung bei 50-Prozent-Ausfällen

Auch mit dem dynamischen Quorum-Modell kann es Situationen geben, in denen beide Seiten eines Clusters keine Mehrheit im Gesamtsystem haben, wenn es zu einem Netzwerkausfall zwischen den Standorten kommt. In einer solchen Situation war es bis einschließlich Windows Server 2012 so, dass beide Seiten zur Sicherheit ihre Dienste einstellen, um das »Split-Brain-Szenario« zu vermeiden. Windows Server 2012 R2 kann dies durch einen zusätzlichen Mechanismus namens *Tie Breaker* verhindern.

Dies erläutert sich gut mit einem Beispiel. Nehmen wir an, Sie hätten einen Cluster mit sechs Knoten und einem Dateiserver-Zeugen aufgebaut. Jeweils drei Knoten laufen an Standort A und an Standort B. Im Normalbetrieb hat der Cluster sieben Stimmen, es kann also nicht zu *Split Brain* kommen. Nun fällt der Zeugenserver aus, der Rest der Cluster-Knoten läuft aber weiter. Windows Server 2012 R2 wird nun automatisch einem der Cluster-Knoten seine Stimme entziehen, um auf eine ungerade Stimmenanzahl zu kommen. Dadurch haben die Knoten an einem Standort zwei Stimmen, die am anderen Standort drei Stimmen.

Sollte es nun zu einer Unterbrechung der WAN-Leitung zwischen beiden Standorten kommen, so werden sich die Cluster-Dienste an dem Standort mit den zwei Stimmen selbsttätig beenden. Der »Rest-Cluster« am anderen Standort läuft weiter.

Die Auswahl des Knotens, der seine Stimme verliert (und damit die Entscheidung, an welchem Standort der Cluster sich beendet), trifft Windows nach dem Zufallsprinzip. Mithilfe der PowerShell können Sie die neue Cluster-Eigenschaft *LowerQuorumPriorityNodeID* konfigurieren, um für diesen Fall vorzugeben, welcher Cluster-Knoten seine Stimme verlieren soll. Dazu bestimmen Sie zunächst mit dem Kommando `Get-ClusterNode | ft` die Node-IDs aller Knoten. Danach legen Sie für einen der Knoten mit folgendem Kommando fest, dass er bei einem 50-Prozent-Ausfall seine Stimme abgeben muss. Hierbei steht *9* im Beispiel für die Node-ID des betreffenden Servers.

```
(Get-Cluster).LowerQuorumPriorityNodeID = 9
```

Automatische Quorum-Erkennung nach Ausfällen

In seltenen Ausnahmefällen kann es notwendig sein, dass Sie in einem Cluster das Quorum erzwingen. Hierbei starten Sie auf einem Teil der Cluster-Knoten die Cluster-Dienste neu und teilen ihnen dabei mit, dass sie unabhängig von der vorgegebenen Grundkonfiguration das Quorum (und damit die gesamte Funktion des Clusters) übernehmen sollen. Bislang war es nach einer solchen »Notoperation« erforderlich, dass Sie den anderen Cluster-Knoten auf ähnlichem Weg manuell mitteilen, dass sie auf keinen Fall das Quorum übernehmen dürfen. In Windows Server 2012 R2 ist dieser letzte Schritt für die anderen Cluster-Knoten nicht mehr erforderlich, weil die Cluster-Dienste den Zustand selbst erkennen können.

Stellen Sie sich zur Illustration einen geografisch verteilten Cluster mit drei Knoten an Standort A und zwei Knoten an Standort B vor. Die WAN-Verbindung zwischen beiden Standorten fällt aus. Da an Standort A drei der fünf Knoten laufen, verfügt Standort A über das Quorum und arbeitet weiter, während sich die Cluster-Knoten an Standort B automatisch herunterfahren. Dies ist das normale und erwünschte Verhalten, um das »Split-Brain-Problem« zu vermeiden.

Nun stellen Sie in unserem Beispiel fest, dass die Cluster-Knoten an Standort A keine Netzwerkverbindung nach außen haben, die an Standort B hingegen schon. Sie starten also die Knoten an Standort B neu und setzen für den Dienststart auf der Kommandozeile oder in der Konsole DIENSTE den Schalter `/fq` (für *Force Quorum*). Dadurch übernehmen die Cluster-Knoten das Quorum und betreiben die geclusterten Dienste.

Sobald nun die Verbindung zwischen Standort A und Standort B wieder besteht, müssen Sie nichts weiter unternehmen, wenn alle Cluster-Knoten unter Windows Server 2012 R2 laufen. Diese erkennen die Situation und stellen den korrekten Aufbau von selbst wieder her.

Cluster ohne Active-Directory-Namensobjekte

In einigen seltenen Fällen stellt es für Administratoren eine Hürde dar, dass die Cluster-Knoten in einem Windows-Failover-Cluster eine tiefe Integration in Active Directory benötigen. Nicht nur müssen die Server Mitglieder der Domäne sein und damit zumindest bei der Einrichtung direkten Kontakt zu den Domänencontrollern haben. Zusätzlich war es bislang auch erforderlich, bei der Definition eines Clusters in Active Directory zu schreiben, denn das sogenannte »*Cluster-Naming Object*« *(CNO)* musste als Computerkonto in der Domäne erzeugt werden.

Da es sich hierbei streng genommen nur um den eigentlichen Namen des Clusters handelt, der nur für die Administration verwendet wird, besteht eigentlich keine Notwendigkeit, ein »vollwertiges« Computerobjekt zu erzeugen. Daher ist es in Windows Server 2012 R2 nun möglich, den Namen nur in DNS zu hinterlegen. Das erleichtert in einigen Umgebungen das Vorgehen, weil keine Abstimmung mehr mit der Active-Directory-Administration notwendig ist.

Es gibt allerdings auch Einschränkungen in dieser Konfiguration:

- Die Authentisierung des Namensobjekts erfolgt per NTLM, wenn es nicht in Active Directory hinterlegt ist. In Umgebungen, die nur auf Kerberos setzen, ist dieser Weg damit nicht gangbar.
- Für einige Cluster-Szenarien ist diese Konfiguration nicht unterstützt. Dazu zählen:
  - Alle Clusterapplikationen, die **Microsoft Message Queuing** als Rolle im Cluster voraussetzen, genießen keinen Support.
  - **Dateiserver-Cluster** werden unterstützt, trotzdem rät Microsoft von dieser Konfiguration ab, weil die vollständige Kerberos-Authentisierung für das eingesetzte SMB-Protokoll *(Server Message Block)* dringend empfohlen wird.
  - Auch für **Hyper-V-Cluster** gibt es Support in dieser Konfiguration, jedoch benötigt die Live-Migration im Cluster die Kerberos-Authentisierung. Daher ist die Live-Migration hierbei nicht möglich.
  - **SQL Server** genießt in diesem Aufbau volle Unterstützung, jedoch rät Microsoft hierbei, für die darauf basierenden Applikationen die SQL-Server-Authentisierung anstelle der Windows-Authentisierung zu verwenden.
- Bitlocker und das *Cluster-Aware Updating (CAU)* sind nicht unterstützt.
- Einige administrative Funktionen sind eingeschränkt, etwa das Kopieren von Cluster-Rollen oder die Verwaltung eines *Scale-Out Fileservers (SOFS)* über den Server-Manager.

Um einen Cluster in dieser Konfigurationsvariante aufzusetzen, nehmen Sie alle künftigen Cluster-Knoten in dieselbe AD-Domäne auf und installieren Sie das Feature Failover-Cluster-Unterstützung. Führen Sie die Cluster-Validierung aus und sorgen Sie dafür, dass dort keine »roten« Elemente angezeigt werden.

Erzeugen Sie den Cluster dann nicht über die grafische Oberfläche des Failover-Cluster-Managers, sondern mit der PowerShell. Dazu nutzen Sie ein Kommando ähnlich dem folgenden Beispiel:

```
New-Cluster CLU01 -Node SRV01,SRV02 -StaticAddress 192.168.1.16 ([UP)]
-NoStorage -AdministrativeAccessPoint Dns
```

Verteilung von CSV-Aktivitäten

Durch den *Scale-Out Fileserver (SOFS),* der mit Windows Server 2012 eingeführt wurde, sind die *Cluster-Shared Volumes (CSV)* zu einer bevorzugten Speichertechnik in Windows-Clustern geworden. Hyper-V-Cluster nutzen diese Funktion schon länger, denn hierfür war sie ursprünglich entstanden.

Durch CSV ist es möglich, dass mehrere Cluster-Server gleichzeitig auf eine Speichereinheit *(Logical Unit Number, LUN)* zugreifen, ohne dass es zu Schreibkonflikten kommt. Die Verwaltung dieser Zugriffe kann in manchen Situationen eine hohe Last erzeugen, weil für jede CSV-Einheit ein bestimmter Cluster-Knoten die Koordination ausführt. Diesen Knoten nennt man den *CSV Coordinator* oder auch *CSV Owner*.

In Windows Server 2012 R2 sorgt der Cluster selbstständig für eine Verteilung der CSV-Owner-Rollen, sobald es mehr als ein CSV im Cluster gibt. Das sorgt für eine Lastverteilung, sodass Engpässe nicht mehr oder zumindest weit seltener auftreten als bisher.

Ergänzend setzt Windows Server 2012 R2 für die CSV-Technik nun eine separate Instanz des Server-Dienstes ein, der seit jeher das Netzwerkprotokoll SMB (Server Message Block) bedient. Dies sorgt zusätzlich dafür, Verzögerungen durch starken Netzwerkverkehr zu vermeiden.

Damit Sie sich nun nicht sorgen müssen: Die Lastspitzen, die wir hier beschreiben, sind ohnehin sehr selten; in den meisten Clustern wird man sie praktisch nie bemerken.

CSV-Cache

Bereits in Windows Server 2012 gab es im Cluster eine Cache-Funktion für *Cluster-Shared Volumes (CSV).* Diese war dort standardmäßig abgeschaltet, weil sie physischen Speicher der beteiligten Server exklusiv belegt. Ein solcher Eingriff sollte nur durch ausdrückliche Konfiguration erfolgen.

Der CSV-Cache kann Lesevorgänge für Daten beschleunigen, die auf einem CSV gespeichert sind, indem er einen Teil der Daten parallel im Arbeitsspeicher vorhält. Fordert ein Prozess dieselben Daten erneut an, so kann Windows dies aus dem RAM bedienen, statt einen erneuten Plattenzugriff auszuführen.

Mittlerweile hat Microsofts Support so viel Erfahrung mit CSV-Konstrukten gesammelt, dass er den CSV-Cache ausdrücklich empfiehlt. In erster Linie gilt dies natürlich für *Scale-Out Fileserver,* in denen intensive Lesevorgänge erfolgen und in denen der physische Arbeitsspeicher für die Dateidienste bereitsteht. Doch auch für Hyper-V-Cluster empfiehlt Microsoft, den Cache zu verwenden, auch wenn dadurch weniger physisches RAM für die virtuellen Maschinen bereitsteht.

Das Maximum an reservierbarem Speicher für den CSV-Cache liegt nun bei 80 Prozent der verfügbaren Ressourcen. Für Hyper-V wäre das natürlich nicht geeignet. Nehmen Sie hier den Cache in Ihre Planung für die Ressourcen Ihrer Cluster-Knoten mit auf.

Die Konfiguration des CSV-Cache erfolgt über die Cluster-Eigenschaften `EnableBlockCache` (ist standardmäßig mit dem Wert 1 belegt und damit eingeschaltet) und `BlockCacheSize` (steht standardmäßig auf 0 – hier geben Sie die Anzahl Megabytes vor, die der Cache auf jedem beteiligten Server-Knoten umfassen soll). Um etwa einen Wert von 512 MB zu setzen, nutzen Sie folgendes PowerShell-Kommando:

```
(Get-Cluster).BlockCacheSize = 512
```

VM-Netzwerkverbindungen überwachen

Es kann in einem Cluster vorkommen, dass auf einem der beteiligten Knoten einzelne Netzwerkverbindungen ausfallen. Solange der Cluster-Knoten insgesamt noch kommunikations- und arbeitsfähig bleibt, führt dieser teilweise Ausfall nicht zu einem Failover. In einer Hyper-V-Umgebung kann dies unerwünschte Auswirkungen haben.

Stellen sie sich eine virtuelle Maschine vor, die in Ihrem Netzwerk wichtige Dienste anbietet. Sie läuft auf einem Cluster-Knoten, der eine größere Zahl von Netzwerkverbindungen bereitstellt und einige davon über virtuelle Switches in Hyper-V den VMs zugänglich macht. Nun fällt diejenige Netzwerkverbindung aus, die die oben genannte VM benötigt; die anderen Verbindungen arbeiten weiter. Aus Sicht des Clusters ist dies kein Grund, ein Failover auszuführen, weil die Clusterfunktion als solche noch gegeben ist. Die betreffende VM ist aber nicht erreichbar. Würde die VM auf einem anderen Cluster-Knoten laufen, bei dem die Netzwerkverbindung noch funktioniert, wäre die VM weiter nutzbar.

In Windows Server 2012 R2 können Sie einzelne Netzwerkverbindungen virtueller Maschinen als *Geschütztes Netzwerk* definieren (siehe Abbildung 4.38). Sollte eine solche Verbindung ausfallen, so versucht Windows, die VM per Live-Migration auf einen anderen Cluster-Knoten zu verschieben, auf dem diese Verbindung noch arbeitet.

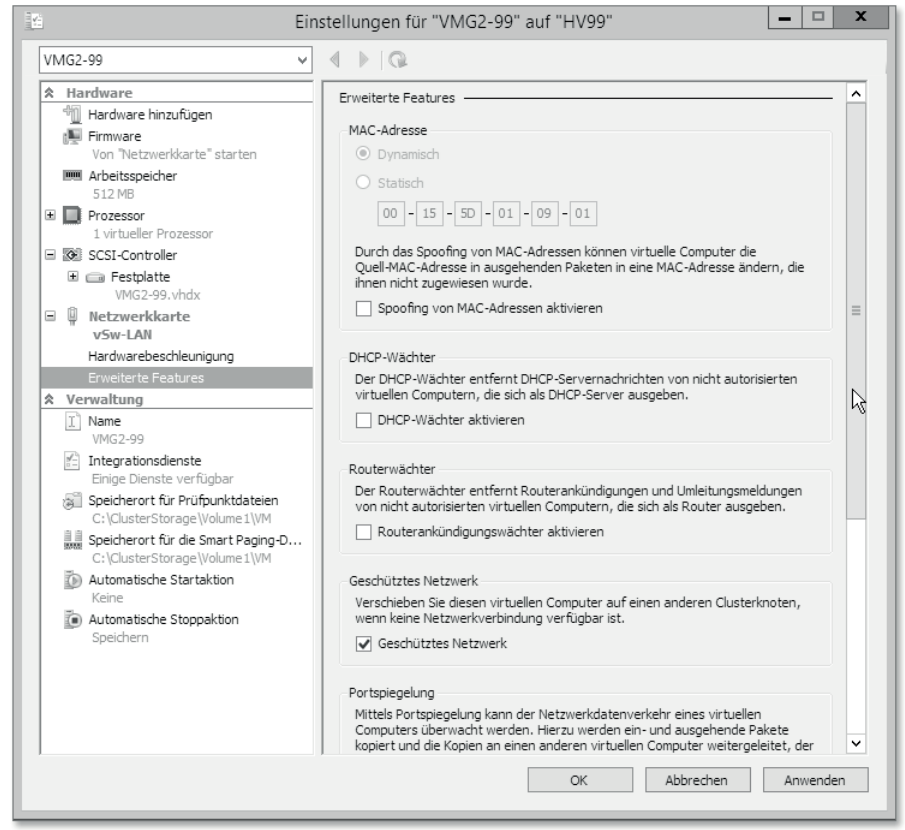


Abbildung 4.38 Definieren Sie eine VM-Netzwerkverbindung als »Geschütztes Netzwerk«, so versucht Hyper-V die betreffende VM auf einen anderen Host zu verschieben, falls die Verbindung des Netzwerks abreißt.

Shared VHDX

Eine wichtige neue Funktion für »Gast-Cluster«, deren Cluster-Knoten aus virtuellen Maschinen bestehen, besteht in Shared Virtual Disks, in der deutschen Übersetzung etwas holprig freigegebene virtuelle Festplatten. Es handelt sich dabei um virtuelle Festplatten in Gestalt von VHDX-Dateien, die gleichzeitig an mehrere virtuelle Maschinen angebunden sind, um als Cluster-Datenträger zu dienen.

Auf diese Weise können Sie Gast-Cluster wesentlich einfacher einrichten als bisher, weil die umständliche Integration der virtuellen Cluster-Server in das SAN entfällt. Details zur Einbindung von VHDX-Dateien als Shared Virtual Disks finden Sie in Abschnitt 5.2.7 »Festplatten«.

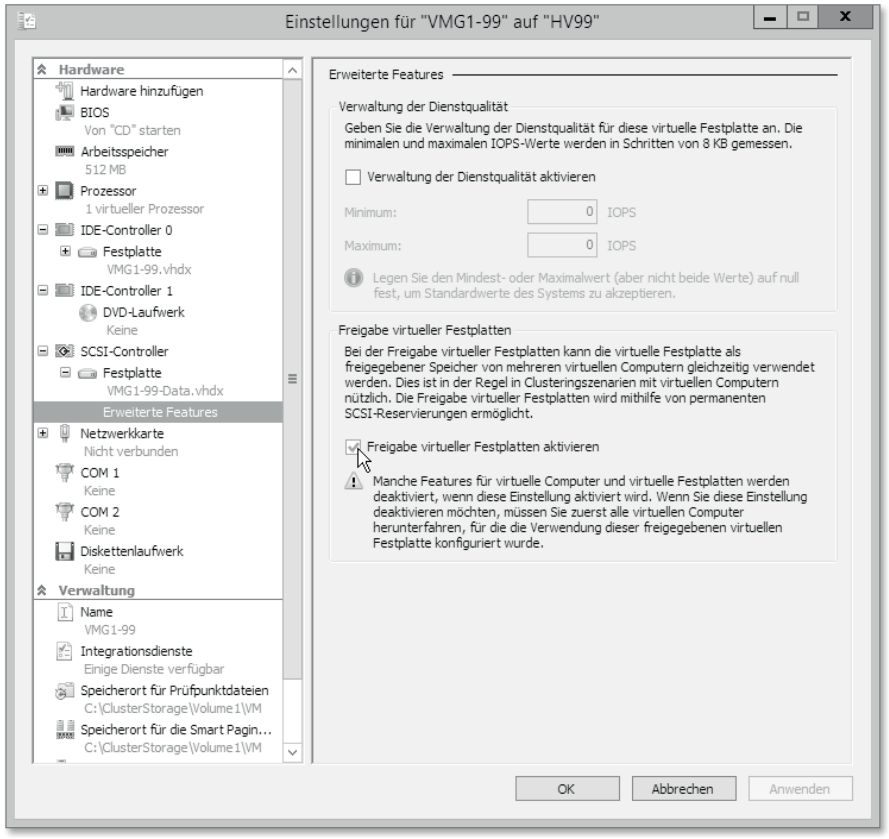


Abbildung 4.39 Über »Freigabe virtueller Festplatten aktivieren« können Sie eine VHDX-Datei, die auf einem Dateiserver-Cluster liegt, an mehrere virtuelle Maschinen gleichzeitig anbinden. Dies erleichtert es, VM-Cluster einzurichten.

4.3 Speicher-Cluster mit Windows Server 2012

Mit Windows Server 2012 hat Microsoft besonders die Speicherfunktionen seines Server-Betriebssystems ausgebaut. Dadurch ist es nun möglich, auch anspruchsvolle Storage-Anforderungen vollständig mit Windows Servern zu erfüllen. Einige Beobachter sehen hier eine Antwort von Microsoft auf Entwicklungen am Server-Markt: Jahrelang haben die Anbieter von spezialisierten Speichergeräten immer mehr »klassische« Funktionen von Windows Servern in ihre Systeme integriert. Nun deckt umgekehrt Microsoft mit seinem Windows Server viele Funktionen leistungsfähiger Speichersysteme ab.

Zu diesem Kontext gehört die Möglichkeit, ausfallsichere Speichersysteme mit Standard-Hardware und einem Standard-Betriebssystem aufzubauen. Durch die neuen *Storage Spaces*, die weiterentwickelten iSCSI-Speicher-Server (der Fachausdruck ist

iSCSI-Target) und die Dienste für Failover-Cluster sind alle Komponenten bereits in der Grundversion von Windows Server 2012 enthalten, die für einen leistungsfähigen Speicher-Server nötig sind. Neben diesen Funktionen haben die Entwickler in Redmond auch die herkömmlichen Dateidienste neu entwickelt und als Speicherrückgrat für die Server im Rechenzentrum positioniert. Zwei der neuen Techniken lassen sich verbinden, um mit einfacher Hardware eine blockbasierte Speichertechnik aufzubauen, die neben hoher Ausfallsicherheit auch ein großes Maß an Flexibilität bietet. Mit den Storage Spaces, die erstmals in Windows Server 2012 enthalten sind, können Sie herkömmliche RAID-Systeme ersetzen und die Handhabungs- und Kostenvorteile einfacher Festplatten ausnutzen. Die Speicher-Volumes, die Sie in diesen Storage Spaces ablegen, können dann als Basis für iSCSI-Speicherbereiche dienen, die über das Netzwerk als dedizierte Festplatten für Server-Systeme (sogenannte LUNs, Logical Unit Numbers) bereitgestellt werden.

Im Folgenden stellen wir Ihnen überblicksweise vor, wie Sie Storage Spaces und das iSCSI-Target in einem Failover-Cluster bereitstellen. Berücksichtigen Sie bei einer produktiven Umsetzung, dass für den Aufbau eines adäquaten Speichersystems in einem Server-Netzwerk umfassende Planung notwendig ist. Zudem soll unsere Darstellung nicht den Eindruck vermitteln, als seien dedizierte Speichersysteme ohne Weiteres durch einfache Windows Server zu ersetzen. Gerade in größeren, anspruchsvollen Umgebungen können kommerzielle Storage-Einheiten eine Reihe von Vorteilen bieten.

4.3.1 Storage Spaces im Cluster

Die grundsätzliche Einrichtung von Storage Spaces und die Logik hinter der Technik stellen wir in Abschnitt 3.4.4, »Storage Spaces verwenden«, genauer vor. Details finden Sie an der angegebenen Stelle.

Storage Spaces eignen sich auch, um den Datenspeicher für einen Failover-Cluster einzurichten. Dazu müssen Sie allerdings eine Reihe von Einschränkungen beachten:

- Für Storage Spaces im Cluster dürfen Sie nur JBOD-Geräte (*Just a Bunch of Disks* – dies bezeichnet einen Festplattenstapel, der die Festplatten einzeln ansprechbar macht, ohne weitere Logik wie RAID vorzuhalten) mit *Shared-SAS*-Anbindung verwenden. Die Ansprache über andere Bus-Techniken wie Fibre Channel oder iSCSI wird nicht unterstützt.
- Alle Cluster-Knoten, die die Storage Spaces verwenden sollen, müssen über das Shared-SAS-Bus-System eine Verbindung zu dem JBOD-Speichergerät haben.
- Mindestens drei physische Festplatten sind für einen Cluster-Pool notwendig.
- Alle Platten müssen in der Cluster-Validierung positiv bewertet werden.
- Soll der Speicher-Pool als Grundlage eines CSV-Systems (Cluster Shared Volume) dienen, müssen seine Volumes mit NTFS formatiert sein.

- Die Storage Spaces müssen vom Typ *Einfach* oder *Spiegel* sein, der Typ *Parität* wird im Cluster nicht unterstützt.
- Die Bereitstellungsmethode muss *Fest* lauten, es darf sich also nicht um *Thin Provisioning* handeln.

Darüber hinaus sollten Sie in einer Produktionsumgebung einen Speicher-Server immer völlig dediziert betreiben. Sie sollten also keine weiteren Funktionen oder Dienste dort einrichten oder betreiben. Zudem empfiehlt es sich, auch die I/O-Last auf dem jeweiligen Server zu begrenzen und nicht zu viele externe Server zur Nutzung eines einzelnen Speicher-Servers zu konfigurieren.

Um Storage Spaces auf einem Failover-Cluster zu nutzen, richten Sie den Cluster zunächst mit einer Grundkonfiguration ein. Sofern das Festplattensystem die aufgezählten Voraussetzungen erfüllt, spielt es keine Rolle, ob Sie den Speicher-Pool bereits vor der Installation des Features *Failover-Clustering* definiert haben oder ob Sie dies nachträglich tun. Verbinden Sie sich über das Verwaltungsprogramm Failover-Cluster-Manager mit Ihrem Cluster, und klicken Sie im Verwaltungsbaum mit der rechten Maustaste auf Speicher • Pools. Falls Sie noch keinen Speicher-Pool erzeugt haben, wählen Sie Neuer Speicherpool, anderenfalls lautet die Auswahl Speicherpool hinzufügen (siehe Abbildung 4.40).

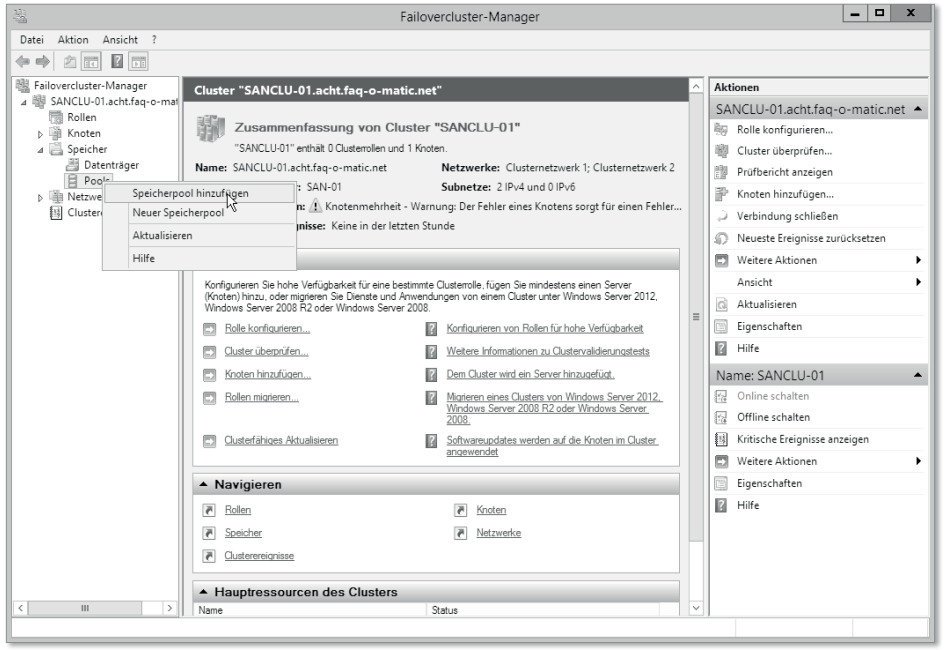


Abbildung 4.40 Einen vorhandenen Speicher-Pool können Sie im Failover-Cluster-Manager in den Cluster aufnehmen. Im selben Menü haben Sie die Möglichkeit, einen neuen Speicher-Pool zu erzeugen.

Zum Erzeugen eines neuen Speicher-Pools wenden Sie exakt die Schrittfolge an, die wir in Abschnitt 3.4.4, »Storage Spaces verwenden«, beschrieben haben. Existiert bereits ein Pool, wählen Sie diesen aus dem erscheinenden Dialogfeld aus.

Storage Space als Spiegel erzeugt »Redirected I/O«

Wenn Sie ein Cluster Shared Volume (CSV) auf einem Storage Space vom Typ »Spiegel« einrichten, muss der Cluster auf alle beteiligten physischen Laufwerke parallel die Daten schreiben.

Damit dies gelingt, schaltet der Cluster das CSV in den Modus »Redirected I/O«, also führt nur der Coordinator Node sämtliche Schreibzugriffe des Clusters durch. Im Effekt ist der Speicherzugriff langsamer als bei einem CSV-System, das auf dedizierten Datenträgern beruht. Ob dies für Sie eine relevante Einschränkung bedeutet, sollten Sie selbst festlegen.

Nach Abschluss der Zuweisung sehen Sie unter Pools den ausgewählten Speicher-Pool, und unter Datenträger finden Sie die ausgewählten Volumes. Diese Datenträger können Sie nun für weitere Cluster-Ressourcen nutzen, etwa als iSCSI-Target.

4.3.2 iSCSI-Target als Cluster-Rolle

Sofern Ihr Cluster über Datenträger verfügt, die als Cluster-Ressourcen nutzbar sind, können Sie diese für ein iSCSI-Target verwenden. Dabei kann es sich um Storage Spaces im Cluster handeln, wie wir sie in Abschnitt 4.3.1 beschrieben haben. Sie können aber natürlich auch herkömmliche Laufwerke nutzen, die von allen Cluster-Knoten erreichbar sind.

Um die Funktion des iSCSI-Targets im Cluster einzurichten, führen Sie zunächst die Grundinstallation des Failover-Clusters aus, sofern dies noch nicht geschehen ist. Im Failover-Cluster-Manager klicken Sie dazu mit der rechten Maustaste auf Rolle und wählen im Kontextmenü Neue Rolle. In dem Assistenten, der sich öffnet, wählen Sie dann die Rolle iSCSI-Zielserver aus (siehe Abbildung 4.41). Im darauffolgenden Schritt Clientzugriffspunkt legen Sie die IP-Adresse und den Namen fest, mit dem Clients (das sind in diesem Fall nicht Anwender, sondern Server) eine Verbindung mit dem iSCSI-Target herstellen sollen. Danach wählen Sie die verfügbaren Datenträger für den iSCSI-Speicherbereich aus und folgen dem Assistenten bis zum Ende.

Nun besteht Ihr Target aus einem Namen, einer IP-Adresse und einem Datenträger. Es fehlen allerdings noch die eigentlichen Speichereinheiten, die das Target für die anzubindenden Server bereithalten soll, das heißt die *LUNs* (Logical Unit Numbers). Die eigentliche Konfiguration des iSCSI-Targets nehmen Sie nicht im Failover-Cluster-Manager vor, sondern im Server-Manager. Die nötigen Schritte sind die gleichen

wie bei einem Einzel-Server, Sie können sich daher an das Verfahren halten, das wir in Abschnitt 3.4.5, »iSCSI-Target mit Windows Server 2012«, beschrieben haben.

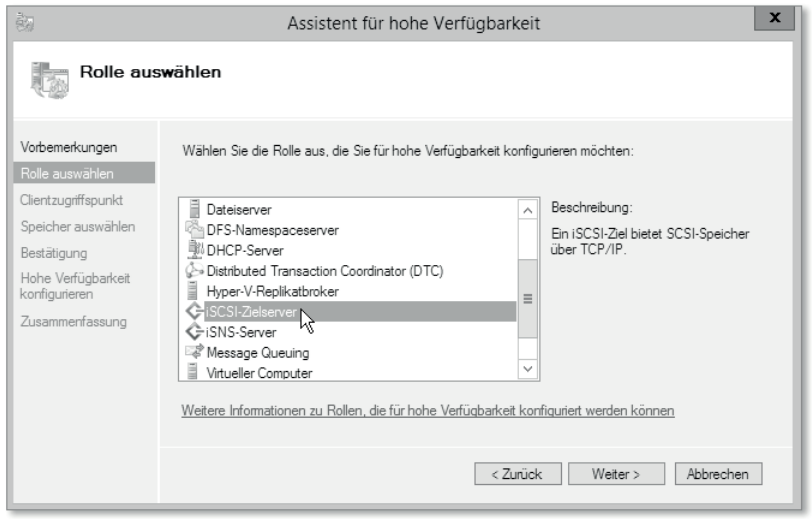


Abbildung 4.41 Im Failover-Cluster-Manager weisen Sie die Rolle »iSCSI-Zielserver« zu, um ein iSCSI-Target als Cluster zu erzeugen.

4.4 NAS statt SAN

Der Aufbau und Betrieb eines *Storage Area Networks* (SAN) erfordert zusätzliches Fachwissen und bedeutet Aufwand. Manche Unternehmen scheuen davor zurück, in beides zu investieren, und setzen lieber auf den bekannten *Network Attached Storage* (NAS). Mehr zu diesen Begriffen finden Sie in Abschnitt 3.4.1, »Crashkurs Storage: DAS, NAS, SAN oder was?«.

Hyper-V in einer Testumgebung

Sollten Sie Hyper-V in einer Testumgebung installieren und aufgrund von Ressourcenengpässen die Netzwerkfreigabe auf demselben Server einrichten wollen, wird die Verwendung der Netzwerkfreigabe fehlschlagen.

Das liegt daran, dass beim Zugriff auf die Netzwerkfreigabe desselben Servers keine Übersetzung des Systemkontos zum Computerkonto stattfindet. Dadurch lassen sich keine NTFS-Berechtigungen für den Zugriff von Hyper-V auf demselben Server definieren. Infolgedessen erhält der Hyper-V-Host keinen Zugriff auf die Netzwerkfreigabe.

Allerdings unterstützt erst Windows Server 2012 Hyper-V das Speichern von virtuellen Maschinen auf Netzwerkfreigaben offiziell. Die Authentifizierung an der Netz-

werkfreigabe erfolgt nach der Vorgabe von Microsoft mithilfe des Credential Security Support Providers (CredSSP), was Konfigurationsaufwand bei der Berechtigung der Netzwerkfreigabe zur Folge hat. Kommt allerdings die eingeschränkte Kerberos-Delegation (Kerberos Constrained Delegation, KCD) zum Einsatz, müssen die Computerkonten der Hyper-V-Hosts angepasst werden.

4.4.1 Authentifizierung mit »CredSSP«

Der Einsatz von CredSSP ist die Vorauswahl nach der Installation von Windows Servern und erfordert die explizite Pflege der NTFS-Berechtigungen der Netzwerkfreigabe, damit virtuelle Maschinen dort abgelegt und verwendet werden können.

Wenn ein Hyper-V-Host auf die Netzwerkfreigabe zugreift, sind zwei NTFS-Berechtigungen notwendig: Vollzugriff für das Computerkonto des Hyper-V-Hosts und Vollzugriff für den Hyper-V-Administrator.

Die erste NTFS-Berechtigung ist notwendig, weil der initiale Zugriff auf die Freigabe mithilfe des lokalen Systemkontos des Hyper-V-Hosts erfolgt. Dies wird zum Computerkonto übersetzt und benötigt daher die Zugriffsrechte. Anschließend wird der Kontext zum Hyper-V-Administrator gewechselt, sodass auch diese NTFS-Berechtigung unabdingbar ist.

Die Berechtigungen der Freigabe müssen entsprechend konfiguriert werden, damit sowohl das Computerkonto jedes Hyper-V-Hosts als auch das Benutzerkonto jedes Hyper-V-Administrators zugreifen kann. Das kann einigen Aufwand erzeugen, da zusätzliche Hyper-V-Hosts nachträglich berechtigt werden müssen.

Die Anpassungen der NTFS-Berechtigungen können auch direkt mit PowerShell durchgeführt werden, anstatt den manuellen Weg über den Windows Explorer zu wählen. Listing 4.1 zeigt dies:

```
$$acl = Get-Acl c:\VmStore
$acl.SetAccessRuleProtection($True, $False)
$rule = New-Object System.Security.AccessControl.FileSystemAccess-Rule ⮐
("hv01$","FullControl" , "ContainerInherit, ObjectInherit", "None", "Allow")
$acl.AddAccessRule($rule)
$rule = New-Object System.Security.AccessControl. ⮐
FileSystemAccessRule("CONTOSO\Administrator", ⮐
"FullControl", "ContainerInherit, ObjectInherit", ⮐
"None", "Allow")
$acl.AddAccessRule($rule)
Set-Acl c:\VmStore $acl
```

Listing 4.1 Die notwendigen NTFS-Rechte können mithilfe von PowerShell eingerichtet werden.

4.4.2 Authentifizierung mit Kerberos

Anstatt das Computerkonto jedes Hyper-V-Hosts einzeln zu berechtigen, kann der Einsatz von *eingeschränkter Kerberos-Delegation* (Kerberos Constrained Delegation) den administrativen Aufwand verringern. Dabei wird das Computerkonto jedes Hyper-V-Hosts um eine Delegation ergänzt, die den Fileserver dem Hyper-V-Host vertrauen lassen.

Sie müssen für das Computerkonto jedes Hyper-V-Hosts eine Delegation hinzufügen. Das Hinzufügen erfordert zuerst das Computerkonto des Fileservers und dann die Auswahl des Dienstes CIFS. Anschließend erscheint die Delegation in der Liste des Hyper-V-Hosts (siehe Abbildung 4.42).

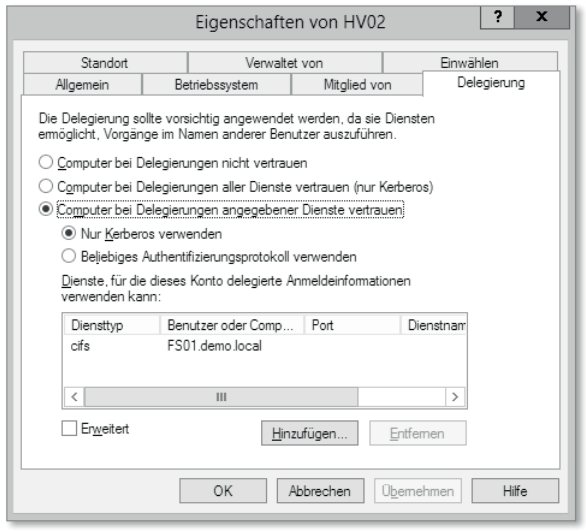


Abbildung 4.42 Die Delegation mithilfe von Kerberos wird im Computerobjekt im Active Directory vorgenommen.

Nach der Einrichtung der Delegation im Computerkonto jedes Hyper-V-Hosts müssen lediglich die Hyper-V-Administratoren Vollzugriff auf die Netzwerkfreigabe erhalten. Dazu können die PowerShell-Befehle in Listing 4.1 verwendet werden.

Sollen die Delegationen mittels PowerShell konfiguriert werden, ist das Commandlet `Set-KCD` von Microsoft-Mitarbeiter Matthijs ten Seldam notwendig (*http://blogs.technet.com/b/matthts/archive/2012/10/05/set-kcd-configuring-kerberos-constrained-delegation-kcd.aspx*, Kurzlink: *http://qccq.de/s/h410*). Damit reduziert sich die Einrichtung der Delegation auf einen Befehl pro Hyper-V-Host (siehe Listing 4.2).

```
Set-KCD -TrustedComputer hv01 -TrustingComputer fs01
-ServiceType CIFS -Add
```

Listing 4.2 Verwaltung der Delegation mithilfe von PowerShell

Windows Server 2012 Scale-Out Fileserver (SOFS)

Wird die Netzwerkfreigabe in einem Cluster als Scale-Out Fileserver (SOFS) bereitgestellt, erfolgt die Delegation mit dem Computernamen des SOFS statt der einzelnen Cluster-Knoten.

In diesem Abschnitt haben wir Ihnen das notwendige Wissen vermittelt, um erfolgreich eine hochverfügbare Hyper-V-Infrastruktur mithilfe des Windows Server 2012-Failover-Clusterings einzurichten. Funktionen wie die Live-Migration, Quick-Migration oder das Failover des Windows-Clusterings erlauben es, auch große Host-Farmen mit Windows Server 2012 zu betreiben und Hunderte von virtuellen Maschinen mit Hyper-V performant und ausfallsicher zu verwalten. In diesem Abschnitt haben Sie auch einen Überblick über die Einrichtung diverser Speichersysteme wie iSCSI, Storage Spaces und Fibre Channel erhalten und sind nun in der Lage, mithilfe der Hyper-V Replica-Funktion virtuelle Maschinen für ein Wiederherstellungsszenario auf anderen Hyper-V-Servern zu betreiben.

4.4.3 Scale-Out Fileserver

Ein *Scale-Out Fileserver* (SOFS) ist ein eigener Failover-Cluster, welcher ausschließlich zur Bereitstellung der Dateiserver-Rolle verwendet wird. Dies ermöglicht den Betrieb einer oder mehrerer hochverfügbarer Freigaben, die sogar den kompletten Ausfall eines Knotens ohne Datenverlust oder Downtime überstehen.

Der Aufbau eines Scale-Out Fileservers ist kein einfaches Unterfangen, allerdings werden Sie mit einem günstigen und hochperformanten System belohnt. Microsoft hat mit Windows Server 2012 R2 das erste Mal die Empfehlung herausgegeben, diese Form von Storage als primäre Wahl zu sehen. In diesem Kapitel sprechen wir grundsätzlich nur von dem Failover-Cluster für die Bereithaltung Ihrer Dateiserver-Rolle, nicht über ein Failover-Cluster zur Bereitstellung Ihrer VMs.

Der Scale-Out Fileserver an sich ist technisch gesehen eine Rolle, die in dem bereits angesprochenen Failover-Cluster betrieben wird, ähnlich der vielleicht schon bekannten Dateiserver-Rolle im Failover-Cluster. Die Rolle ist mit einem eigenen Objekt im Active Directory vertreten und unter einem eigenen Namen erreichbar. Da für die Ausführung der Rolle eine spezielle Hardware (und Software in Form von Windows Server 2012 oder Windows Server 2012 R2) benötigt wird, sprechen wir in den folgenden Abschnitten immer vom Gesamt-Konstrukt Scale-Out Fileserver. Anhand der Beschreibungen, Screenshots oder Fotos wird jeweils deutlich, welcher Teil gemeint ist.

Woraus besteht ein Scale-Out Fileserver?

Die einfachste Form eines Scale-Out Fileserver besteht aus zwei Server-Systemen sowie einem gemeinsam nutzbaren Speicherplatz, meist in Form eines JBOD-Shelfs (»Just a Bunch of Disks«). Die in dem JBOD verbauten Festplatten und/oder SSDs werden per SAS von den beiden Systemen angesprochen, in beiden steckt jeweils ein oder mehrere SAS-HBAs. Mehrere Wege zum JBOD (z. B. über mehrere Controller und/oder mehrere Kabel) führen zu einem höheren Durchsatz zwischen JBOD und Server. Falls mehrere Wege existieren müssen Sie, ähnlich wie bei mehreren iSCSI-Verbindungen, das Feature *Multipfad-E/A (MPIO)* verwenden. Neben einem höheren Durchsatz sinkt durch mehrere Karten die Wahrscheinlichkeit eines Ausfalls, ähnlich einem Netzwerk-Team. Solch ein Aufbau kann wie in Abbildung 4.43 aussehen:

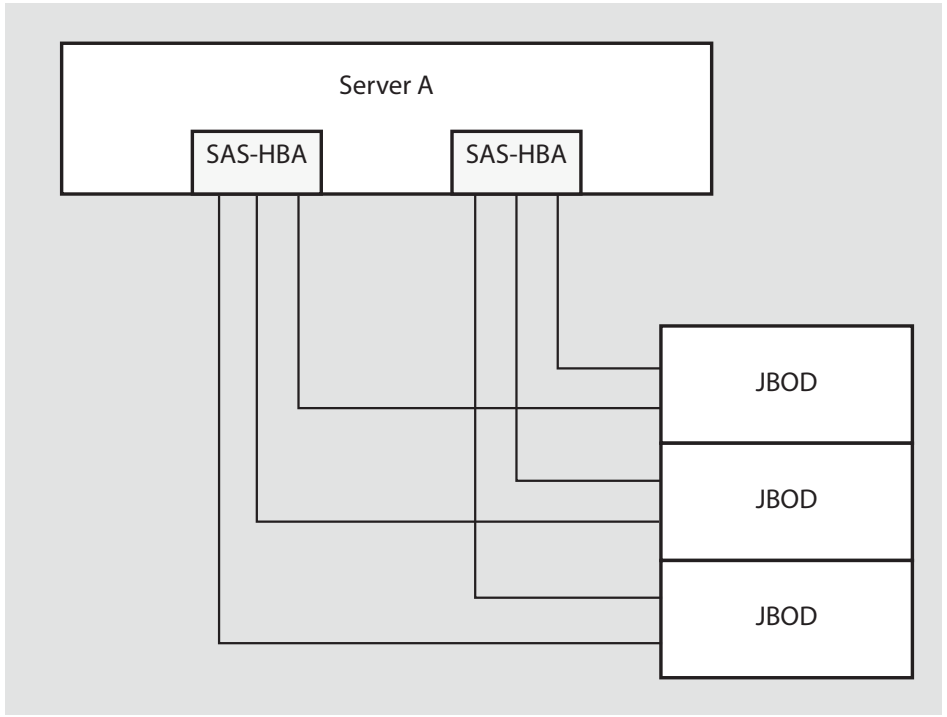


Abbildung 4.43 Anbindung eines Servers an drei JBODs mit zwei HBAs über insgesamt sechs Pfade

Die Dateiserver-Rolle im Failover-Cluster stellt unter einem Namen ein oder mehrere Freigaben zur Verfügung, in die die Daten Ihrer VMs gespeichert werden. Falls Sie nun daran denken, Ihren Clients einen hochverfügbaren Fileserver mit Hilfe der SOFS-Rolle bereitzustellen, so müssen wir Sie leider enttäuschen. Ein Scale-Out Fileserver dient ausschließlich zur Bereitstellung von Speicherplatz für Anwendungen, z. B. Hyper-V. Natürlich können Sie eine VM auf diesem Share speichern, in der die Daten Ihrer Clients liegen.

Lokaler Speicher

Die gemeinsame Nutzung von lokalen Festplatten in einem oder mehreren Servern ist nicht möglich, es wird zwingend gemeinsam verwendeter Speicher benötigt. Lokale Festplatten oder SSDs werden lediglich für das lokale Betriebssystem benötigt.

Für mehr Speicherplatz, eine höhere Bandbreite und mehr HDDs/SSDs in Ihrem SOFS können Sie entweder mehr als ein JBOD anschließen oder die Art des Speichers ändern.

Wenn Sie mehrere JBODs nutzen möchten, brauchen Sie natürlich von jedem JBOD mindestens eine SAS-Verbindung zu jedem Ihrer Failover-Cluster-Knoten. Bei drei JBODs und zwei Servern sind dies insgesamt sechs Kabel, bei der Nutzung von Multichannel direkt zwölf. Wenn Sie nun mehr als zwei Server nutzen möchten, steigt die Anzahl der Verbindungen sehr schnell an, teilweise beschränken die SAS-Anschlüsse an Ihren JBODs hier die Möglichkeiten. Der Aufbau eines SOFS mit zwei Cluster-Knoten und drei JBODs ist in der Praxis sehr beliebt. Hier werden pro Server zwei SAS-Kabel zu jedem JBOD geführt (jeweils von einer Karte), dies erhöht die Bandbreite und die Ausfallsicherheit.

Wenn Sie einen sehr großen Bedarf an Speicherplatz und Performance haben, lässt sich dies ab einer gewissen Zahl nicht mehr mit »einfachen« JBODs erreichen, in diesem Fall werden als Speicher ein oder mehrere SAN-Systeme genutzt, die Anbindung an die SOFS-Knoten erfolgt hier per Fibre Channel oder iSCSI, je nach Art des SANs. Dies wäre auch eine Möglichkeit, wie Sie Ihre vorhandene Infrastruktur weiterhin betreiben und trotzdem die Vorteile von SMB nutzen können.

Dinge, die Sie vor der Einrichtung wissen sollten

Die Planung eines SOFS ist beinahe der wichtigste Teil der kompletten Implementierung, da es hier nahezu unendlich viele Möglichkeiten gibt. Damit Sie keine unangenehmen Überraschungen während der Installation oder nachher im Test/Betrieb erleben, versuchen wir hier möglichst viele Informationen und Erfahrungen aufzuführen, die wir bisher mit dem Thema Scale-Out Fileserver erlebt haben.

Wichtig: Zertifizierte Hardware

Achten Sie beim Aufbau eines Scale-Out Fileservers unbedingt auf eine Zertifizierung aller Komponenten durch Microsoft. Auf *http://www.windowsservercatalog.com* finden Sie alle für Windows Server 2012 und Windows Server 2012 R2 zertifizierten Hardware-Komponenten. Da es sich hier um einen der wichtigsten Grundsteine für einen fehlerfreien Betrieb Ihrer IT handelt, sollten Sie an dieser Stelle sehr sorgfältig prüfen, welche Komponenten unterstützt werden und wie der Stand der Treiber der jeweiligen Geräte ist.

Die Art und die Anzahl der JBODs

Wenn Sie den Einsatz von mehr als einem JBOD planen, müssen Sie darauf achten, dass die Geräte Ihrer Wahl die Funktion *SCSI Enclosure Services (SES-3)* in der Version 3 besitzen. Nur mit dieser Eigenschaft melden die Geräte, an welchem Platz sich eine bestimmte Festplatte befindet.

Kapazität	Bus	U/Min	Modell	Zuordnung	Chassis	Medientyp
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CEA000 : Slot 7	HDD
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CE0000 : Slot 8	HDD
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CE9000 : Slot 8	HDD
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CEA000 : Slot 8	HDD
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CE9000 : Slot 9	HDD
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CEA000 : Slot 9	HDD
932 GB	SAS		ST91000640SS	Automatisch	SES Enclosure 500093D001CE0000 : Slot 9	HDD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE9000 : Slot 21	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CEA000 : Slot 21	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE0000 : Slot 21	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE9000 : Slot 22	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CEA000 : Slot 22	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE0000 : Slot 22	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE0000 : Slot 23	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CEA000 : Slot 23	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE9000 : Slot 23	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE0000 : Slot 24	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CE9000 : Slot 24	SSD
186 GB	SAS		S842E200M2	Automatisch	SES Enclosure 500093D001CEA000 : Slot 24	SSD

Abbildung 4.44 Ein Teil der eingesteckten HDDs und SSDs in insgesamt drei JBODs. Der Server kann den Standort der Datenträger sehen.

Sie kennen diese Funktion wahrscheinlich von Ihrem RAID-Controller, hier kann der Controller meist auch erkennen, welche Festplatte an welchem Port hängt (und

deren LED dann z. B. im Fehlerfall zum Leuchten bringen). Falls die Gehäuse diese Funktion nicht haben, kann das Betriebssystem bei der Einrichtung der Spiegelung die Blöcke nicht bewusst in einem anderen JBOD als dem eigenen speichern. Dies kann zur Folge haben, dass bei dem Ausfall eines JBODs sowohl die Festplatte mit dem gewissen Block als auch die Festplatte mit dem gespiegelten Block ein paar Festplatten weiter offline geht. Für Sie bedeutet dies eine Unterbrechung bzw. einen Ausfall des Storage bzw. der Freigabe. Wenn der Failover-Cluster weiß, welche Festplatte sich wo befindet, kann er bewusst die Blöcke einer Festplatte im ersten JBOD auf die in einem anderen Gehäuse speichern. In diesem Fall stehen die Daten bei einem Ausfall eines der JBODs weiter zur Verfügung.

An diese im letzten Satz angesprochene Fähigkeit ist eine andere Bedingung geknüpft: Der Einsatz von mindestens drei JBODs. Wenn Sie zwei JBODs einsetzen und ein komplettes Gehäuse geht offline, fährt das andere ebenfalls herunter. Dies geschieht durch eine fehlende Mehrheit an JBODs, keines der beiden JBODs hat eine Mehrheit an Datenträgern. Sobald ein drittes JBOD mit mindestens einer Festplatte vorhanden ist, kommt es beim Ausfall eines kompletten Chassis nicht zu einem Ausfall der CSV-Datenträger.

Die hier beschriebene Funktion der Spiegelung von Blöcken in unterschiedlichen JBODs nennt man *Enclosure Awareness*. Bei dieser Art der Speicherung könnte ein komplettes JBOD ausfallen oder offline gehen, ohne dass der Betrieb dadurch unterbrochen wird.

2-Wege- vs. 3-Wege-Spiegelung

Grundsätzlich können Sie die Daten auf Ihren Festplatten entweder einmal oder zweimal spiegeln, dies legen Sie während der Erstellung der virtuellen Datenträger unter Resilienzeinstellungen konfigurieren fest (siehe Abbildung 4.45). Bei der einfachen Spiegelung wird von jedem Block eine Kopie auf einer zweiten Festplatte gespeichert, die beim Ausfall der primären Festplatte zur Verfügung steht. Sie können allerdings auch eine 3-Wege-Spiegelung aufbauen. Bei dieser Betriebsart werden alle Blöcke insgesamt drei Mal gespeichert. Dies erhöht den Schutz vor einem Ausfall, senkt bei der gleichen Anzahl an Festplatten gegenüber der 2-Wege-Spiegelung allerdings die verfügbare Nettokapazität bzw. bedingt mehr Festplatten, um auf die gleiche Größe an Speicherplatz zu gelangen.

Resilienzeinstellungen und die Enclosure Awareness

Die Enclosure Awareness greift sowohl bei einem Zwei-Wege- als auch bei einem Drei-Wege-Spiegel.

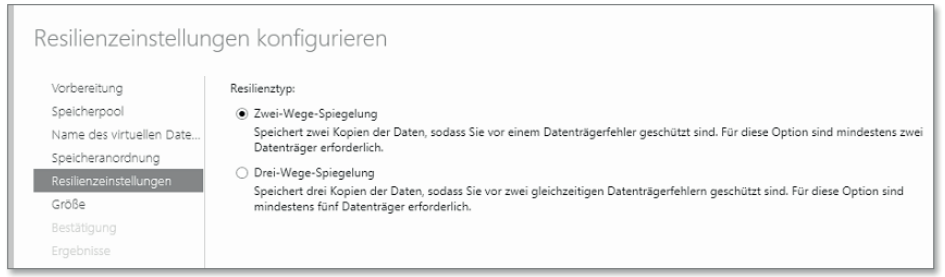


Abbildung 4.45 Konfiguration der Resilienz bei der Erstellung eines virtuellen Datenträgers

Die Anzahl an Festplatten

Wenn Sie nach der Einrichtung der virtuellen Datenträger in den Failover-Cluster-Manager schauen, werden Sie sehen, dass unter *Resilienz* ein paar Informationen zu Ihrem Datenträger stehen: die Art der Spiegelung, die Anzahl der Spalten und die Größe des Interleaves. Wir möchten an dieser Stelle kurz erläutern was es mit diesen Eigenschaften auf sich hat und wie diese im Zusammenhang stehen.

Die Art der Spiegelung

Dieser Wert ist am einfachsten zu erklären. Hierbei handelt es sich um die Art der Sicherheit für die Daten auf Ihrem virtuellen Datenträger. In den meisten Fällen steht diese Einstellung auf *mirror*, d. h. alle Blöcke werden auf zwei (2-Wege-Spiegelung) oder drei Festplatten (3-Wege-Spiegelung) gespiegelt.

Spalten

Die Zahl der Spalten (im englischen *columns* genannt) zeigt Ihnen, auf wie vielen Festplatten gleichzeitig Datenblöcke gespeichert werden können. Die maximale Anzahl liegt bei acht. Ohne manuelles Eingreifen wird dieser Wert automatisch konfiguriert, Sie können ihn aber auch manuell per PowerShell beeinflussen.

Wenn Sie zwei physische Datenträger zu einem Pool zusammenfassen und einen gespiegelten virtuellen Datenträger erzeugen, haben Sie eine Spaltenanzahl von 1, da die Daten nur auf einem Datenträger gespeichert werden können (und parallel dazu natürlich auf dem zweiten, dies erhöht allerdings nicht den Durchsatz). Erhöhen Sie die Anzahl der physischen Datenträger auf vier, erhöht sich die Anzahl der Spalten auf zwei. In Bezug auf die Performance bedeutet dies, dass diese sich ggf. verdoppeln kann, da insgesamt zwei Datenträger zur Speicherung der Daten zur Verfügung stehen. Kann ein physischer Datenträger maximal 100 MB/s schreiben, können zwei Datenträger insgesamt 200 MB/s schreiben. Das bedeutet, dass Sie für die größtmögliche Performance eine Spalten-Anzahl von acht und mindestens 16 physische Datenträger benötigen.

Interleave

Die Interleave-Größe (im englischen *stripes* genannt) sagt aus, in welche Größe eine Datei, die gespeichert werden soll, aufgeteilt wird. Wenn Sie eine 2 MB große Datei auf einem virtuellen Datenträger speichern, der eine Spaltenanzahl von zwei hat, werden pro Festplatte eine gewisse Anzahl an Interleaves gespeichert. Bei einer Interleave-Größe von 256 KB (dies ist der Standard-Wert) werden von jedem Datenträger vier Interleaves gespeichert (2 MB werden in acht Interleaves von jeweils 256 KB aufgeteilt, jeder physische Datenträger speichert jeweils die Hälfte).

Tiering

Seit *Windows Server 2012 R2* können Sie zwei unterschiedliche Arten an Datenträgern in einem Pool verwenden, um Ihre Daten zu speichern: Festplatten (HDDs) oder Flashmedien (SSDs). Festplatten oder SSDs konnten schon unter *Windows Server 2012* eingesetzt werden, allerdings nicht gemeinsam in einem Pool. Ob es sich bei den Festplatten um SAS- (10k bzw. 15k rpm) oder Nearline-SAS (7.2k rpm) handelt, ist hierbei egal, allerdings sollten in einem Volume grundsätzlich nur gleiche Arten von Festplatten betrieben werden (plus ggf. SSDs). Denken Sie hier an gewöhnliche RAID-Controller, hier lassen sich auch keine SAS-Festplatten mit Nearline-SAS bzw. SATA-Festplatten in einem Verbund betreiben.

Diese als *Speicherebenen* oder auch *Tiering* bekannte Funktionalität bietet einige Möglichkeiten, um die Transferraten Ihrer Daten zu beschleunigen. Vorteile eines Scale-Out Fileserver mit Tiering sind unter anderem eine erhöhte Zugriffsrate von oft angefragten Blöcken oder die Nutzung von einem Teil der SSD-Kapazität als Schreib-Cache. Die Funktion des Schreib-Caches wird weiter hinten in diesem Abschnitt beschrieben, auf die Beschleunigung beim Zugriff auf häufig benötigte Blöcke werden wir jetzt eingehen.

In einem Volume, welches basierend auf HDDs und SSDs aufgebaut wird, können Sie die Größe beider Bereiche bei der Einrichtung wählen. Der SSD-Bereich wird primär für »heiße Blöcke« verwendet, d. h. für Daten die häufig und wiederholt angefragt werden. Der Speicherbereich auf den HDDs wird verwendet, um »kalte Daten« abzuspeichern. Dies kann z. B. ein Großteil Ihrer Daten auf Ihrem virtuellen Dateiserver sein. Diese Daten müssen dauerhaft zur Verfügung stehen, allerdings wird nur ein Bruchteil dieser Daten während der täglichen Arbeit von Ihnen oder Ihren Kollegen benutzt.

Blöcke, keine Dateien!

Machen Sie sich von Anfang an bewusst, dass es sich bei den Daten im »heißen« oder im »kalten« Bereich nicht um komplette Dateien, sondern um Blöcke mit der Größe von 1 MB handelt. Sie können manuell ausgewählte Dateien dauerhaft im SSD-Bereich Ihres Volumes speichern, dies ist aber kein Standard-Verhalten.

Im Scale-Out Fileserver gibt es einen geplanten Task, der in der Standard-Einstellung einmal täglich um 01:00 Uhr morgens überprüft, ob eine Umsortierung von Blöcken notwendig ist (Abbildung 4.46). Dieser Prozess sorgt dafür, dass die als »heiß« markierten Blöcke in den SSD-Bereich verschoben werden (sofern Sie nicht schon hier liegen) und die »kalten« Blöcke auf den Festplatten lagern und ggf. hierhin verschoben werden. Sie können die Ausführung dieser geplanten Aufgabe manuell anpassen und z. B. nur am Wochenende laufen lassen, da die Ausführung unter der Woche durch eine Produktion nicht gewünscht ist. Während der Zeit steht Ihr Scale-Out Fileserver natürlich weiterhin zur Verfügung, allerdings kann es zu Performance-Einbußen kommen, da die Blöcke von den HDDs auf die SSDs oder anders herum verschoben werden.

Sie können den geplanten Task natürlich auch mehrfach am Tag oder auch manuell ausführen, bedenken Sie allerdings immer die zusätzliche Belastung Ihrer Datenträger.

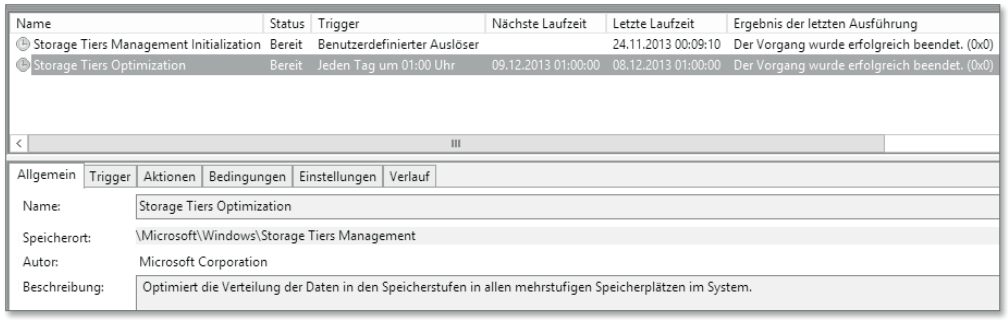


Abbildung 4.46 Geplanter Task zur Verteilung der Daten in einem Storage Pool mit Tiering

Die Installation eines Scale-Out Fileservers

In diesem Abschnitt möchten wir auf die Installation eines Scale-Out Fileservers eingehen. Die hier beschriebene Vorgehensweise hat so wirklich in der Realität stattgefunden, daher können wir Ihnen einige Screenshots der Installation zeigen.

Die verwendete Hardware

Als Server kommen zwei Systeme mit einer Bauhöhe von zwei Höheneinheiten (HE) zum Einsatz. Beide Server haben jeweils zwei SAS-Controller mit vier externen physischen Anschlüssen sowie einen internen Controller, der für die Installation des Betriebssystems verantwortlich ist. Für die Bereitstellung des Storage im Netzwerk steht eine Dual-Port 10 GbE-Karte zur Verfügung. In Summe sind dies vier PCIe-Karten. Neben der 10 GbE-Karte sind vier 1GbE-Ports vorhanden.

Die Server sind mit zwei CPUs ausgestattet und besitzen jeweils 192 GB RAM. Das Betriebssystem wird auf zwei 10k SAS-Festplatten installiert, die zu einem RAID1 konfiguriert sind.

Es kommen drei JBODs zum Einsatz, die mit jeweils neun 10k SAS-Festplatten und vier SSDs bestückt sind. Jeweils eine der neun SAS-Festplatten pro JBOD wird als Hot-Spare-Festplatte zugeordnet (Abbildung 4.47). Dies reduziert die Gefahr eines Datenverlusts bei einem Ausfall von mehr als einer Festplatte im Pool.

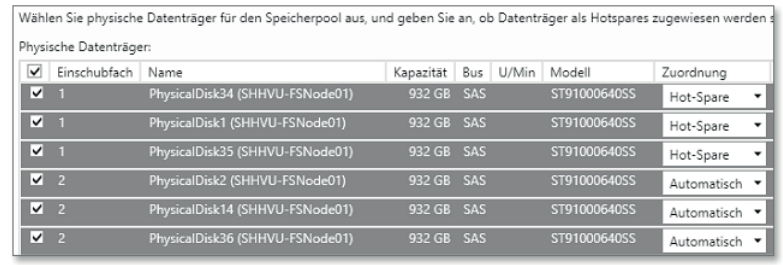


Abbildung 4.47 Konfiguration der jeweils ersten Festplatte in jedem JBOD als Hot-Spare-Festplatte

Die Vorbereitung der Cluster-Knoten

Bevor Sie mit der Einrichtung des Failover-Clusters beginnen können, müssen Sie einige Bedingungen erfüllen. Installieren Sie nach der Grundinstallation des Betriebssystems alle aktuell vorhandenen Windows Updates. Vergeben Sie eine feste IP-Adresse auf einem der 1GbE-Ports oder erstellen Sie ein Team, um die Verfügbarkeit und den Durchsatz zu erhöhen. Fügen Sie die Systeme danach Active Directory hinzu und installieren Sie die folgenden Rollen und Features:

- Dateiserver
- Dateiserver-VSS-Agent-Dienst
- Failover-Clustering
- Multipfad-E/A (falls benötigt)

Aktivieren Sie nach der Installation unter Eigenschaften von MPIO im Reiter Multipfade suchen die Option Unterstützung für SAS-Geräte hinzufügen. Nach einem Neustart sehen Sie unter Geräte mit MPIO einen weiteren Eintrag mit dem Namen *MSFT2011SASBusType_0xA* (Abbildung 4.48).

Zu diesem Zeitpunkt müssen Sie auf jedem der beiden Knoten alle Festplatten und SSDs sehen, die in Ihren JBODs eingesteckt sind.

Richten Sie das Storage-Netzwerk auf Ihren Cluster-Knoten ein. Die beiden Ports der 10GbE-Karte werden mit einer festen IP-Adresse in jeweils einem eigenen Subnetz konfiguriert. Dies ist notwendig, da SMB Multichannel bei aktiviertem Failover-Cluster-Feature nur greift, wenn die Karten in unterschiedlichen Subnetzen konfiguriert sind.

Abbildung 4.48 Weiterer Eintrag unter »Geräte mit MPIO« nach Aktivierung von Multichannel für SAS-Geräte

Unterschiedliche Netze, gleiche Endadresse

Sie vereinfachen sich die Konfiguration und später die Administration, wenn Sie jedem Server in jedem Subnetz die gleiche Adresse geben. Dies erleichtert die Einrichtung und das Zurechtfinden auf Ihren Systemen, in den Switchen und weiteren Geräten. Der erste Host hat z. B. immer die Endadresse .101, der zweite .102 usw.

Die Installation des Failover-Clusters

Öffnen Sie den Failover-Cluster-Manager auf einem der beiden Knoten und führen Sie den Menüpunkt Konfiguration überprüfen... aus. Fügen Sie beide Systeme hinzu und lassen Sie mit allen Tests die Systeme überprüfen. Im Bereich des Storage gibt es einige Warnungen, diese können aber nach Prüfung meist ignoriert werden, da sich einige z. B. auf iSCSI-Anbindungen beziehen. Beginnen Sie nun die Erstellung des Failover-Clusters. Vergeben Sie einen aussagekräftigen Namen und eine IP-Adresse. Achten Sie unbedingt darauf, dass Sie *nicht* den gesamten verfügbaren Speicher automatisch hinzufügen lassen. Dies muss nach der Erstellung manuell gemacht werden.

Nach der Erstellung bekommen Sie eine Warnung, dass kein geeigneter Datenträger für den Quorumzeugen vorhanden ist (Abbildung 4.49). Um dieses Thema kümmern wir uns später.

Benennen Sie die Netzwerke um, um ihnen einen sprechenden Namen zu geben. Dies erleichtert Ihnen die Arbeit mit den Netzwerken im späteren Verlauf.

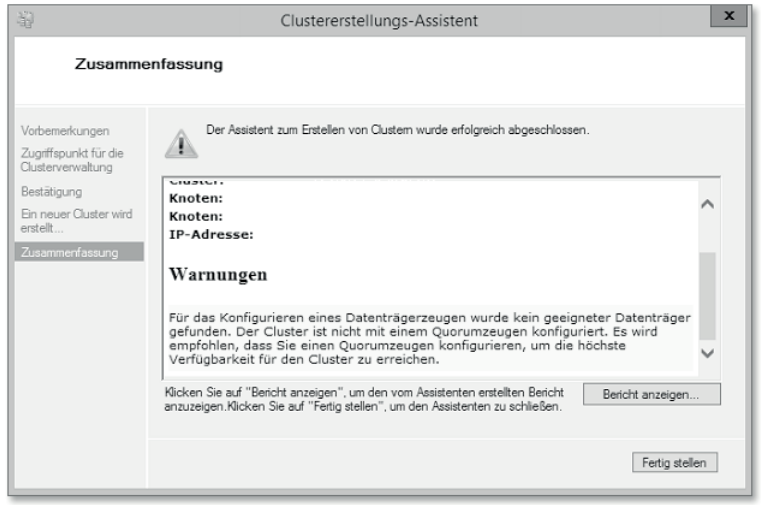


Abbildung 4.49 Warnung direkt nach Erstellung des Failover-Clusters. Es steht aktuell kein geeigneter Datenträger für den Quorumzeugen zur Verfügung.

Die Erstellung eines Storage Pools und Einrichtung von virtuellen Datenträgern

Wechseln Sie im Failover-Cluster-Manager unter Speicher auf Pools. Über die Option Neuer Speicherpool können Sie einen neuen Pool anlegen. Nach den Vorbemerkungen werden Sie nach dem Namen des Pools, einer Beschreibung und der Gruppenzuordnung für den Pool gefragt. Einen Schritt weiter unter Physische Datenträger müssen Sie die Datenträger auswählen, die Mitglied in dem Pool werden sollen. Unter Zuordnung können Sie bei Bedarf ausgewählte Festplatten als Hot-Spare-Festplatten konfigurieren.

Abbildung 4.50 Erstellung eines neuen Speicherpools mit insgesamt 27 HDDs und 12 SSDs

Nach einer Zusammenfassung kann die Erstellung des Pools beginnen, dies dauert meist weniger als eine Minute. Nach der Erstellung können Sie die Eigenschaften des Speicherpools per Powershell auslesen, dies geht mit dem Befehl

```
Get-StoragePool | fl *
```

Sie bekommen eine Auflistung aller Attribute und Einstellungen des Pools (Abbildung 4.51). Relevant ist in unserem Fall der Wert *EnclosureAwareDefault*, dieser steht nach der Erstellung auf FALSE. Dies bedeutet, dass alle auf diesem Pool erzeugten virtuellen Datenträger nicht Enclosure Aware sind. An dieser Stelle kann dieser Wert auf TRUE geändert werden. Dies bewirkt, dass automatisch alle erzeugten Datenträger so erzeugt werden, dass die Daten immer über mindestens ein weiteres Enclosure gespiegelt werden und nicht im gleichen JBOD.

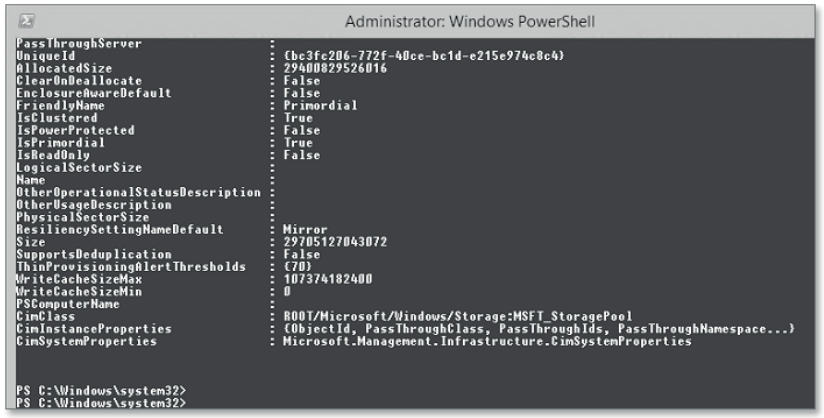


Abbildung 4.51 Eigenschaften eines Speicherpools

Dies lässt sich mit dem Befehl

```
Set-StoragePool -FriendlyName "<Name des Pools>" -EnclosureAwareDefault $true
```

realisieren. Nun können die Datenträger per GUI erzeugt werden und sind trotzdem Enclosure Aware.

Falls es nach der Anpassung des Storage Pools zu einer Reduzierung des nutzbaren SSD-Speicherplatzes bei der Erstellung eines virtuellen Datenträgers kommt, kann dies umgangen werden, indem der Wert *EnclosureAwareDefault* auf FALSE stehen bleibt und stattdessen die virtuellen Datenträger per PowerShell angelegt werden.

```
$SSD = Get-StorageTier -FriendlyName Microsoft_SSD_Template

$HDD = Get-StorageTier -FriendlyName Microsoft_HDD_Template

Get-StoragePool <Pool-Name> | New-VirtualDisk -FriendlyName "<Disk-Name>" ⮒
-ResiliencySettingName "Mirror" -StorageTiers $SSD, $HDD -StorageTierSizes ⮒
<Größe SSD-Speicher>, <Größe HDD-Speicher> -IsEnclosureAware $true
```


Bei der Erstellung des Datenträgers müssen Sie die jeweiligen Größen von SSD- und HDD-Speicherplatz angeben. Einsehen können Sie die Werte in den Eigenschaften des virtuellen Datenträgers (Abbildung 4.52).

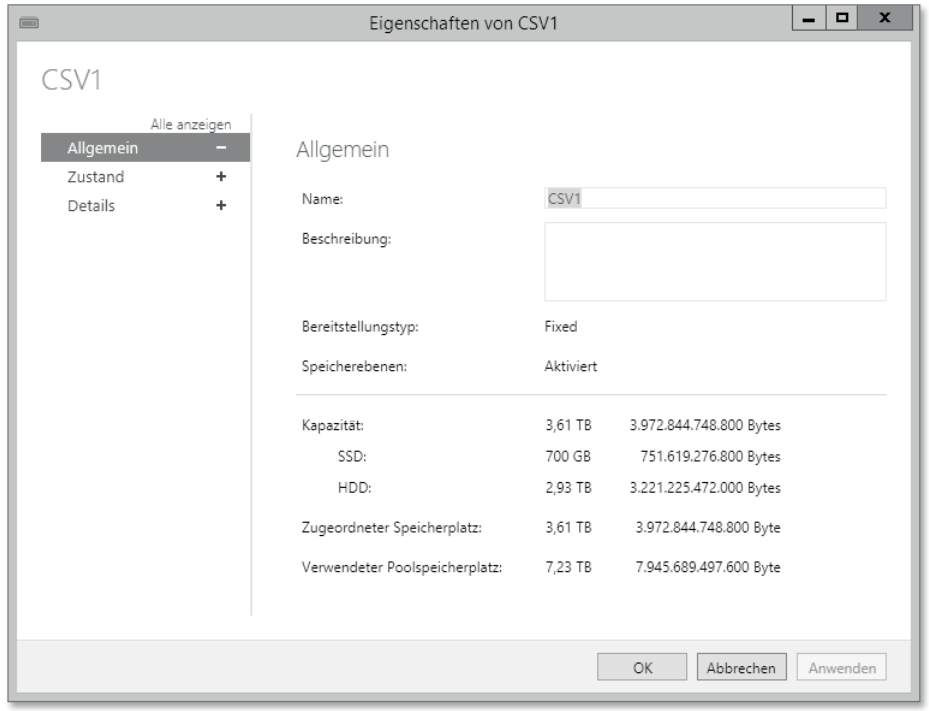


Abbildung 4.52 Eigenschaften eines virtuellen Datenträgers mit Ansicht der Kapazitätsaufteilung

Bei der Anzahl der virtuellen Datenträger kommt es auf die Anzahl der Failover-Cluster-Knoten an. Sie sollten mindestens so viele Datenträger erstellen wie Server vorhanden sind plus einen weiteren Datenträger mit einer Größe von ein paar Gigabyte, der als Quorum-Datenträger verwendet wird. Dies liegt daran, dass unter *Windows Server 2012 R2* die Datenträger in einem *Failover-Cluster* automatisch ausgeglichen werden. Bei zwei Knoten und zwei freigegebenen Clustervolumes ist jeder Knoten Besitzer eines Datenträgers. Somit werden über beide Server Daten angefragt und verarbeitet.

Wenn es sich bei Ihrem Failover-Cluster zur Bereitstellung der Hyper-V VMs ebenfalls um Windows Server 2012 R2 handelt, wird hier pro Share eine neue Verbindung aufgebaut, nicht pro Zugriff auf den Scale-Out Fileserver. Dies bewirkt, dass der gleichzeitige Zugriff auf mehrere Freigaben (da mehrere VMs auf dem Host auf unterschiedlichen Freigaben gespeichert sind) mit mehreren Sitzungen realisiert wird. Ein *Windows Server 2012* verhält sich hier anders, es wird nur eine Sitzung auf-

gebaut, egal wie viele Freigaben angesprochen werden. Dies bewirkt umgeleiteten Traffic zwischen den SOFS-Knoten. Achten Sie aus diesem Grund besonders darauf, sowohl Ihren *Scale-Out Fileserver* als auch Ihren *Hyper-V Failover-Cluster* mit *Windows Server 2012 R2* zu betreiben. Abbildung 4.53 zeigt den Zugriff auf zwei Freigaben, die jeweils über einen der beiden Dateiserver-Knoten bereitgestellt werden.

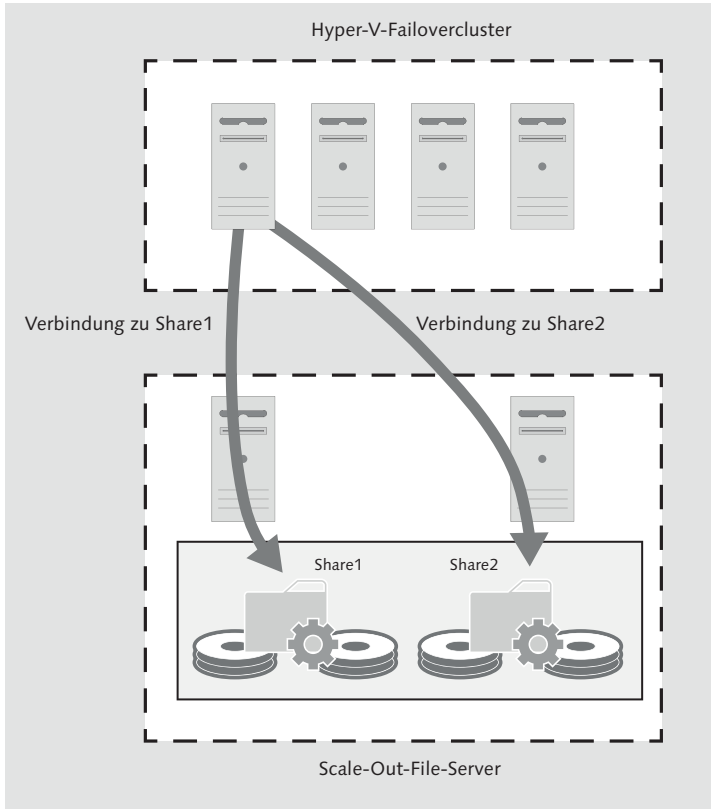


Abbildung 4.53 Verbindung zu zwei Freigaben. Alle Server werden mit Windows Server 2012 R2 betrieben.

Falls sowohl *Scale-Out Fileserver* als auch das *Hyper-V Failover-Cluster* oder eines der beiden Systeme mit *Windows Server 2012* betrieben werden, sieht der Aufbau der Verbindungen anders aus, in diesem Fall herrscht zwischen den Dateiserver-Knoten umgeleiteter Traffic (Abbildung 4.54).

Zurück in der Konfiguration fügen Sie nach der Formatierung (Tipp: In den Wartungsmodus schalten) der virtuellen Datenträger diese zu den *freigegebenen Clustervolumes* hinzu und konfigurieren den kleinen Datenträger als Datenträgerzeuge.

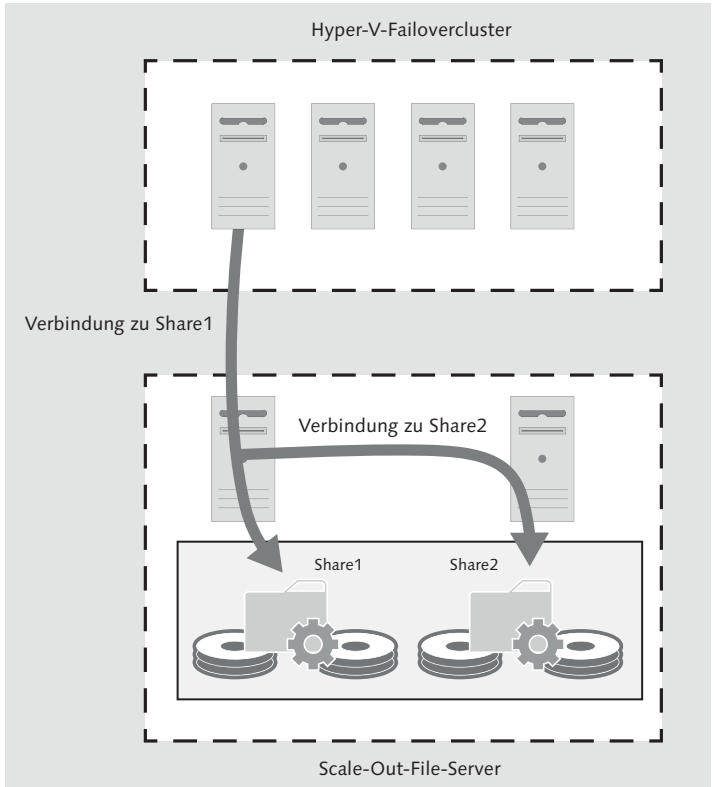


Abbildung 4.54 Keine direkte Verbindung zum zweiten Dateiserver-Knoten. Die Daten werden zwischen den beiden Knoten übertragen (Redirected I/O).

Die Installation und Bereitstellung der Dateiserver-Rolle

Erstellen Sie im *Failover-Cluster-Manager* eine neue Rolle und wählen Sie im Assistenten Dateiserver aus. Unter Dateiservertyp wählen Sie die Option Dateiserver mit horizontaler Skalierung für Anwendungsdaten (Abbildung 4.55).

Vergeben Sie danach einen Namen für den Zugriff auf die Dateiserver-Rolle. Nach der Erstellung wird die Rolle angelegt und gestartet. Zu diesem Zeitpunkt können Sie bereits auf den UNC-Pfad mit dem von Ihnen definierten Namen zugreifen, sehen dort allerdings noch keine Freigaben. Diese müssen Sie erst über die Dateiserver-Rolle im *Failover-Cluster-Manager* anlegen. Wählen Sie hierzu im Kontextmenü die Option Dateifreigabe hinzufügen. Es öffnet sich ein Assistent, der Sie durch die Erstellung der Freigabe führt. Wählen Sie unter Profil auswählen das Dateifreigabeprofil SMB-Freigabe – Anwendungen. Als Freigabeort wählen Sie das erste der vorhandenen *CSVFS*-Volumes aus (Abbildung 4.56). Wählen Sie nun einen Namen für die Freigabe. Eine Angleichung der Namen von Freigabe und CSV-Datenträger ist ratsam und vereinfacht die Administration.

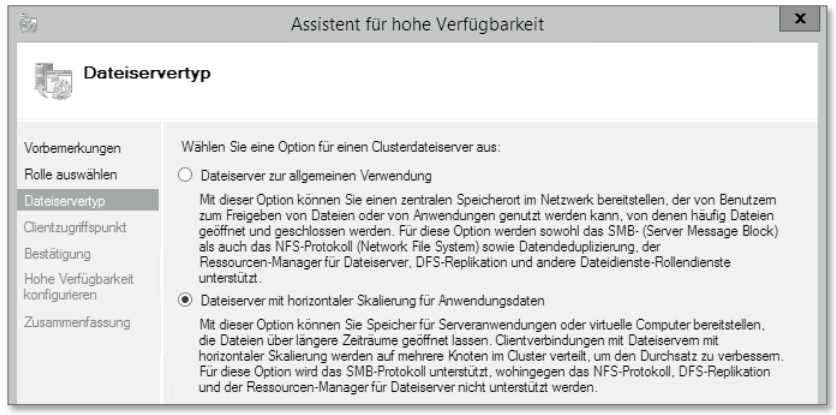


Abbildung 4.55 Wahl des Dateiservertyps im Assistenten zur Erstellung der Dateiserver-Rolle

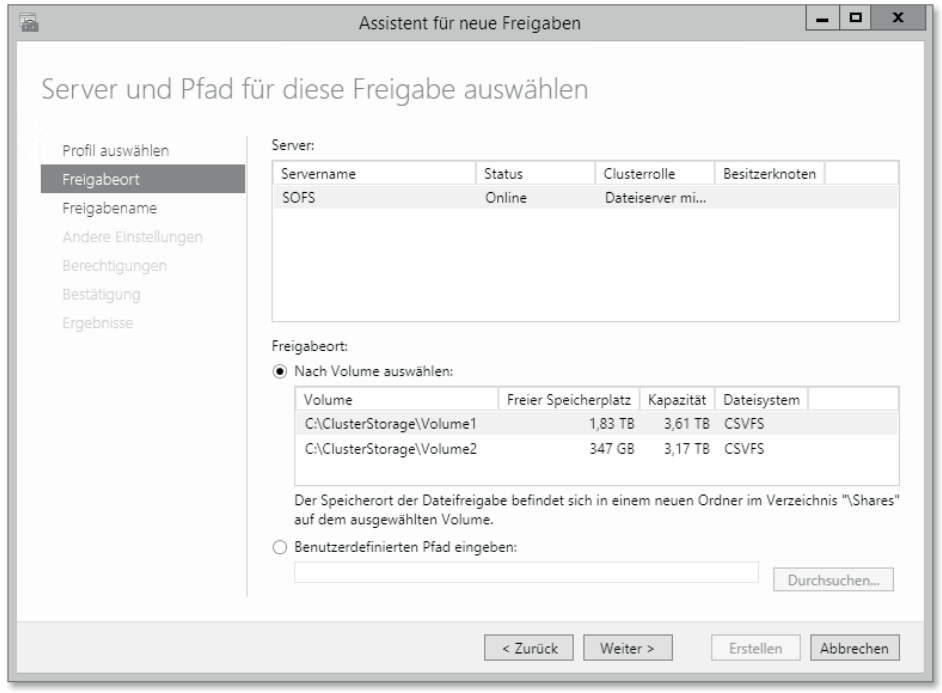


Abbildung 4.56 Auswahl des Freigabeorts während der Erstellung einer Freigabe im Scale-Out Fileserver

Die Berechtigungen der Freigabe müssen angepasst werden. Entfernen Sie hierzu die Vererbung und löschen Sie als erstes den Zugriff für Benutzer. Nehmen Sie nun die Computerkonten der Hyper-V-Hosts auf, die Zugriff auf diese Freigabe erhalten sollen. Bei einer größeren Anzahl an Hosts können Sie diese über eine Gruppe hinzufügen. Vergeben Sie einen Vollzugriff für diese Systeme. Wenn Sie einen oder mehrere *Failover-Cluster* zur Bereitstellung von VMs per Hyper-V haben, müssen Sie die Objekte ebenfalls aufnehmen und mit den passenden Rechten (Vollzugriff) konfigurieren. Die Aufnahme aller oder ausgewählter Administratoren vollendet die Konfiguration. Nach einer Bestätigung wird die Freigabe erstellt, nach einem Aufruf des UNC-Pfades sehen Sie die gerade erstellte Freigabe. Wiederholen Sie dieses Vorgehen für alle Freigaben bzw. CSV-Datenträger.

Read- und Write-Cache

Da es sich bei einem Scale-Out Fileserver um einen CSV-Datenträger handelt, können Sie den *CSV Block-Cache* nutzen, um den wiederholten Lese-Zugriff auf gleiche Blöcke zu beschleunigen. Hierbei wird ein Teil des verfügbaren Arbeitsspeichers als Lese-Cache genutzt. Standardmäßig steht die Menge des genutzten Speichers auf 0 MB, Sie können den Wert per *PowerShell* auslesen:

```
Get-Cluster | ft Name, BlockCacheSize
```

Unter Windows Server 2012 R2 wurden in Bezug auf den CSV Block-Cache ein paar Dinge angepasst. Die Funktion ist nun direkt bei der Installation eingeschaltet, die Menge an genutztem Arbeitsspeicher liegt wie erwähnt bei null. Sie können den Wert anpassen und aktuell bis zu 80 % an Arbeitsspeicher für die Caching-Funktion nutzen. Unter Windows Server 2012 war die Block-Cache-Funktion per Standard ausgeschaltet und musste manuell eingeschaltet werden. Nach dem Einschalten mussten die CSV-Datenträger einmal offline und erneut online geschaltet werden, damit die Funktion nutzbar wurde. Dies war meist nicht zeitnah möglich, da die CSV-Datenträger bereits produktiv genutzt wurden. Weiterhin war es nur möglich, maximal 20 % des vorhandenen RAMs zu nutzen. Eine Anpassung der Cache-Größe unter Windows Server 2012 R2 können Sie mit dem folgenden Befehl vornehmen:

```
(Get-Cluster).BlockCacheSize = 2048
```

Unter Windows Server 2012 wird ein weiterer Befehl benötigt:

```
Get-Cluster).SharedVolumeBlockCacheSizeInMB = 2048
```

```
Get-ClusterSharedVolume "CSV-Name" | Set-ClusterParameter CsvEnableBlockCache 1
```

Wenn Sie in Ihrem Scale-Out Fileserver einen Pool aus HDDs und SSDs verwenden, wird ein Teil der SSD-Kapazität als Write-Back-Cache genutzt. Diese Caching-Funktion werden Sie von RAID-Controllern kennen, hier wird mit einem Speicher (meistens zwischen 256 MB und 2 GB) und einer Batterie die Schreib-Performance teilweise enorm gesteigert. Bei der Nutzung der Storage Spaces wird per Standard 1 GB an SSD-Speicherplatz genutzt. Microsoft empfiehlt, diesen Wert nicht zu verändern, da der Betrieb mit dem Standard-Wert optimal ist.

4.5 Host-Cluster mit Hyper-V

Das Failover-Clustering dient natürlich auch zur Implementierung einer hochverfügbaren Hyper-V-Umgebung. Dabei sollten Sie sich an die empfohlene Installationsreihenfolge halten:

1. Grundinstallation von Windows Server 2012 auf den physischen Servern, Einrichtung aller Updates und Treiber
2. Vorkonfiguration der lokalen Ressourcen: Anbinden des Datenspeichers, Benennen der Netzwerkkarten, Einrichten der Netzwerkkarten-Teams
3. Installation der Server-Rolle *Hyper-V*
4. Konfiguration der virtuellen Switches
5. Installation des Server-Features *Failover-Cluster-Unterstützung*

Beachten Sie dabei, dass Sie zunächst Hyper-V einrichten und konfigurieren und erst danach den Cluster bilden. Diese Reihenfolge ist vielen Administratoren nicht bewusst. Die nötigen Schritte und Planungsgrundlagen für die Rolle Hyper-V sind dabei die gleichen wie bei einem einzelnen Host-Server, Sie können sich deshalb an den ausführlichen Darstellungen in Kapitel 3, »Den Host-Server einrichten«, orientieren. Beachten Sie dabei vor allem die Informationen zur Auswahl und Konfiguration der Netzwerkverbindungen sowie zur Anbindung des Datenspeichers aus dem SAN.

Stellen Sie sicher, dass Sie alle Netzwerkeinstellungen auf beiden Cluster-Knoten analog einrichten und die Netzwerke auf allen Cluster-Knoten denselben VLANs zugeordnet sind. Die identische Konfiguration der Netzwerkkarten und Netzwerkkarten-Einstellungen ist sehr wichtig, da die Funktionen der Live-Migration und Quick-Migration voraussetzen, dass eine virtuelle Maschine auf jedem Cluster-Knoten identische Netzwerkeinstellungen wiederfindet, um eine kontinuierliche Netzwerkkommunikation sicherzustellen. Dazu ist eine zwingende Voraussetzung, dass die virtuellen Hyper-V-Switches (vSwitch) auf allen Cluster-Knoten exakt die gleichen Namen tragen, einschließlich der Groß- und Kleinschreibung.

Nachdem die Netzwerkkarten entsprechend konfiguriert worden sind, kann die Installation der Hyper-V-Rolle auf allen zukünftigen Cluster-Knoten durchgeführt werden. Während der Hyper-V-Installation fordert der Installationsassistent Sie auf, die Netzwerkkarte für das Hyper-V-Management anzugeben. Diese Netzwerkkarte wird dann für den Zugriff auf das Host-System von Clients aus dem LAN oder aus dem Management-Netzwerk verwendet. Wählen Sie hierzu die zuvor für das Management festgelegte Netzwerkkarte aus.

Nachdem Sie die grundlegende Hyper-V-Konfiguration durchgeführt haben, sollten Sie den *Hyper-V Best Practices Analyzer* von Windows Server 2012 starten, um zu

überprüfen, ob die Konfiguration den Empfehlungen von Microsoft entspricht. Den Best Practice Analyzer finden Sie im Server-Manager in der Hyper-V-Rolle.

Für die Speicheranbindung müssen Sie sicherstellen, dass die jeweiligen Speicher-LUNs (Logical Unit Number) für das Cluster-Quorum und das zukünftige Cluster Shared Volume (CSV) auf allen Cluster-Knoten zur Verfügung gestellt werden. Da in diesem Moment der Cluster-Dienst noch nicht läuft, um gleichzeitige Zugriffe zu koordinieren, gehen Sie folgendermaßen vor:

1. Legen Sie, sofern noch nicht geschehen, auf dem Speichersystem die LUNs an – mindestens zwei Stück: eine kleine mit 500 MB bis 1 GB für das Quorum, eine große als Datenspeicher. Tragen Sie, sofern in Ihrem SAN-System vorgesehen, alle Cluster-Server als zugriffsberechtigte *Initiators* ein.
2. Stellen Sie auf dem ersten Cluster-Knoten eine Verbindung zu den LUNs her. Initialisieren und formatieren Sie die LUNs, und vergeben Sie sinnvolle Laufwerkbuchstaben.
3. Stellen Sie nun die Verbindung von dem oder den weiteren Cluster-Knoten her. Achtung: Schalten Sie die Datenträger auf diesen weiteren Servern *nicht* online! Da in diesem Moment keine Koordination der Zugriffe stattfindet, darf zunächst nur der erste Server die LUNs online halten.

Nach Anbindung des SAN-Speichers können Sie mit der Installation und Konfiguration des Failover-Clusters beginnen, wie in Abschnitt 4.2.11, »Einen Cluster einrichten«, beschrieben wurde. Prüfen Sie nach der Erstellung des Clusters, ob der Cluster-Installationsassistent korrekt die LUN für das Cluster-Quorum erkannt hat. Sollte das nicht der Fall sein, können Sie in der Failover-Cluster-Verwaltungskonsole im Kontextmenü des Cluster-Objekts die Quorum-Einstellungen ändern. Weitere Informationen zu den möglichen Quorum-Optionen finden Sie in Abschnitt 4.2.10, »Cluster-Speicher«.

Als Nächstes sollten Sie ein *Cluster-Shared Volume* (CSV, in der deutschen Oberfläche Freigegebenes Clustervolume; siehe Abbildung 4.57) zum Cluster hinzufügen, das zur Speicherung der virtuellen Maschinen verwendet wird und die Funktion der Live-Migration ermöglicht. Starten Sie dazu den Failover-Cluster-Manager, navigieren Sie zum Knoten Speicher • Datenträger, markieren Sie den Datenträger für das zukünftige Cluster Shared Volume, und klicken Sie im Bereich Aktionen auf Zu freigegebenem Cluster-Volume hinzufügen. Der Datenträger wird dann anschließend als freigegebenes Cluster-Volume gelistet. Prüfen Sie anschließend, ob Sie von allen Cluster-Knoten auf das CSV zugreifen können.

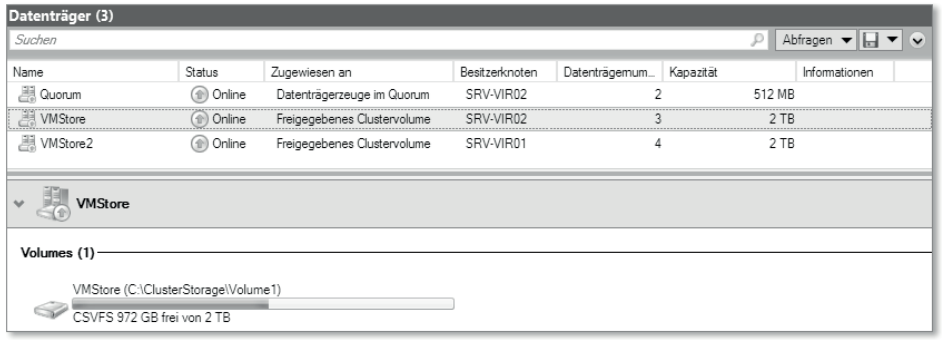


Abbildung 4.57 Datenträger für Hyper-V im Cluster sollten als »Freigegebenes Cluster-Volume« eingerichtet sein.

Es ist zu empfehlen, nach der Erstellung des CSVs dessen Namen zu ändern, um eine bessere Übersicht über den Verwendungszweck der CSVs zu erhalten. Der Standardname für das erste CSV lautet *Volume1*. Weitere CSVs werden entsprechend *Volume2* oder *Volume3* genannt. Das CSV können Sie im Windows Explorer umbenennen. Navigieren Sie in das Verzeichnis *C:\ClusterStorage*, und benennen Sie dort die Cluster Shared Volumes um. Die Umbenennung sollte vor der ersten Installation von virtuellen Maschinen im Cluster erfolgen, da sich sonst der Speicherort der virtuellen Maschinen ändert und Sie die Konfiguration der virtuellen Maschinen nachträglich ändern müssen.

Nachdem Sie das Cluster Shared Volume zum Cluster hinzugefügt haben, können Sie im Hyper-V-Manager den Speicherort für virtuelle Festplatten und virtuelle Maschinen auf das CSV-Volume setzen. Klicken Sie dazu im Kontextmenü des Hyper-V-Servers auf Hyper-V-Einstellungen. Legen Sie dort den Speicherort auf das CSV. Wenn Sie den System Center 2012 Virtual Machine Manager verwenden, können Sie in der SCVMM-Verwaltungskonsole im Knoten Fabric in den Eigenschaften der Hyper-V-Server den Speicherort für virtuelle Maschinen auf das CSV setzen.

Nun können Sie mit der Erstellung einer neuen virtuellen Maschine im Cluster beginnen. Klicken Sie dazu in der Failover-Cluster-Verwaltungskonsole auf den Knoten Rollen, und wählen Sie im Kontextmenü Virtueller Computer • Neuer virtueller Computer aus. Legen Sie den Cluster-Knoten zur Speicherung der virtuellen Maschinen fest, und folgen Sie den Anweisungen des Assistent für neue virtuelle Computer. Als Speicherort für den neuen virtuellen Computer wählen Sie das Cluster Shared Volume aus (Abbildung 4.58).

Schließen Sie den Assistenten unter Angabe der notwendigen Parameter wie Arbeitsspeicher, virtueller Netzwerkkarte, Angabe der virtuellen Festplatte und der Installationsoptionen des Betriebssystems der virtuellen Maschine ab.

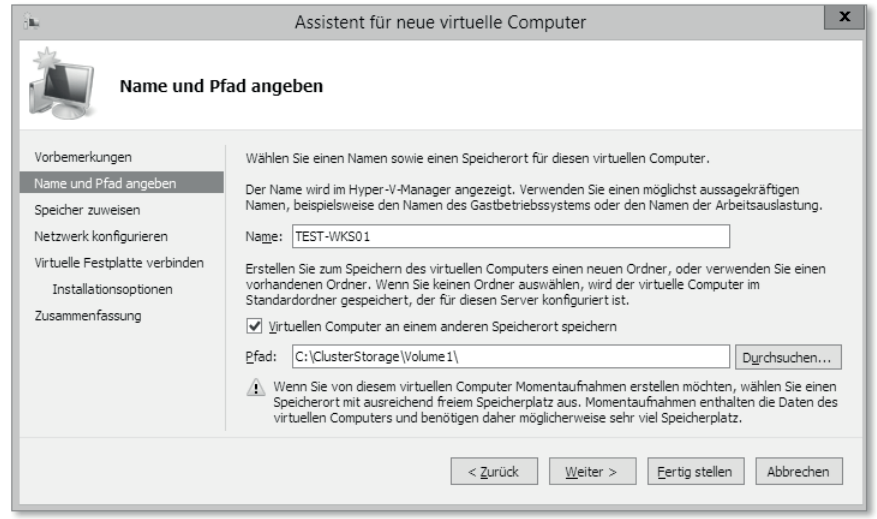


Abbildung 4.58 Neue VMs im Cluster speichern Sie im Verzeichnis C:\ClusterStorage – dies ist das Cluster-Shared Volume.

Externe Datenträger müssen im Cluster erreichbar sein

Wenn Sie der virtuellen Maschine einen Datenträger (etwa eine ISO-Datei) für die Installation des Betriebssystems oder zur Installation von Anwendungen zur Verfügung stellen, müssen Sie sicherstellen, dass alle Cluster-Knoten Zugriff auf den Datenträger haben, damit die Funktion der Live-Migration einwandfrei durchgeführt werden kann. Eine Option wäre es, auf allen Cluster-Knoten ein identisches Verzeichnis zur Speicherung der Datenträger (ISO-Dateien) anzulegen und die ISO-Ablage auf allen Cluster-Knoten identisch zu halten. Diese Option erfordert jedoch sehr viel Speicherplatz und den Aufwand, alle Speicherorte synchron zu halten.

Da die Contoso AG System Center 2012 Virtual Machine Manager einsetzt, nutzen die Administratoren dort die Option zur gemeinsamen Verwendung von ISO-Images aus einer SCVMM-Bibliothek. Somit werden die ISO-Images während des Installationsprozesses nicht auf das Cluster Shared Volume kopiert, sondern der Zugriff auf das ISO-Image wird über das Netzwerk erteilt. Informationen zur Verwendung dieser Option bietet Kapitel 6, »System Center Virtual Machine Manager«.

Die virtuelle Maschine wird jetzt mit der Option zur Hochverfügbarkeit konfiguriert. Nachdem der Assistent zur Erstellung der virtuellen Maschine beendet ist, können Sie mit der Installation des Betriebssystems in der virtuellen Maschine beginnen und die Funktionen der Quick-Migration oder Live-Migration testen.

Immer die »höchste« Konsole nutzen

Die Konfiguration und Verwaltung einer virtuellen Maschine in einem Hyper-V-Cluster sollten Sie ausschließlich in der Failover-Cluster-Verwaltungskonsole durchführen. Bei Einsatz des System Center Virtual Machine Managers 2012 hingegen sollten Sie die SCVMM-Verwaltungskonsole nutzen.

Sowohl der Cluster als auch SCVMM speichern die Konfigurationsinformationen an speziellen Stellen und geben sie dann an Hyper-V weiter. Bearbeiten Sie hingegen die VM-Konfiguration über den Hyper-V-Manager, kann es sein, dass der Cluster bzw. der SCVMM diese Änderungen selbst nicht »kennt« und dann nach Aktualisierungen, nach Failover- oder Migrationsvorgängen die Änderung nicht mehr wirksam ist.

Nur wenn gewünschte Änderungen über die VMM- bzw. Failover-Cluster-Konsolen nicht zugänglich sind, sollten Sie den Hyper-V-Manager dafür nutzen.

Nachdem die Contoso-Administratoren in unserem Fallbeispiel festgestellt haben, dass der Failover-Cluster mit der Hyper-V-Rolle einwandfrei seine Dienste leistet, entscheiden sie sich für die Übernahme einiger virtueller Maschinen von testweise eingerichteten Hyper-V-Servern in den Failover-Cluster. Als Erstes kopieren sie die abgeschaltete virtuelle Maschine mit der virtuellen Festplatte und der Konfigurationsdatei auf das Cluster Shared Volume in ein eigenes Verzeichnis. Anschließend importieren sie die virtuelle Maschine über den Hyper-V-Manager, indem sie im Kontextmenü des Hyper-V-Servers auf Virtuellen Computer importieren klicken und den Ordner mit dem Speicherort der zu importierenden virtuellen Maschine angeben (siehe Abbildung 4.59).

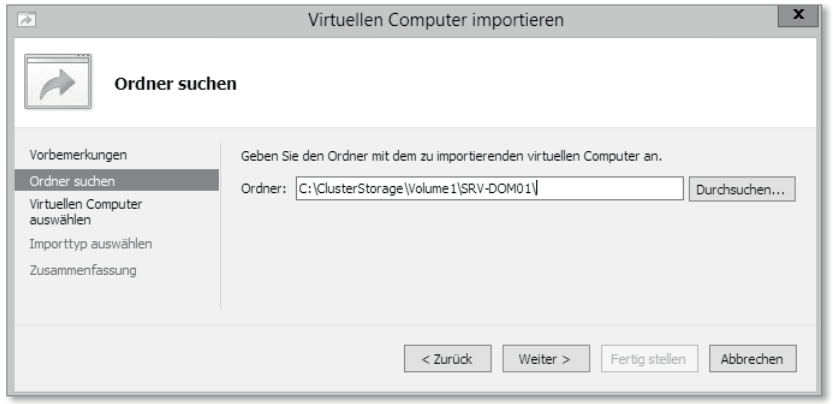


Abbildung 4.59 Über die Importfunktion lässt sich eine bestehende VM nachträglich in einen Cluster bringen.

Im Importassistenten ordnen die Administratoren der virtuellen Netzwerkkarte einen vSwitch des Hyper-V-Clusters zu, wählen den Importtyp aus und starten anschließend den Import der virtuellen Maschine. Nach einem Test können Sie die virtuelle Maschine für die Hochverfügbarkeit in der Failover-Cluster-Verwaltungskonsole konfigurieren. Dazu klicken Sie im Failover-Cluster-Manager im Kontextmenü des Cluster-Objekts auf Rolle konfigurieren • Rolle auswählen • Virtuellen Computer auswählen, wie in Abbildung 4.60 zu sehen ist.

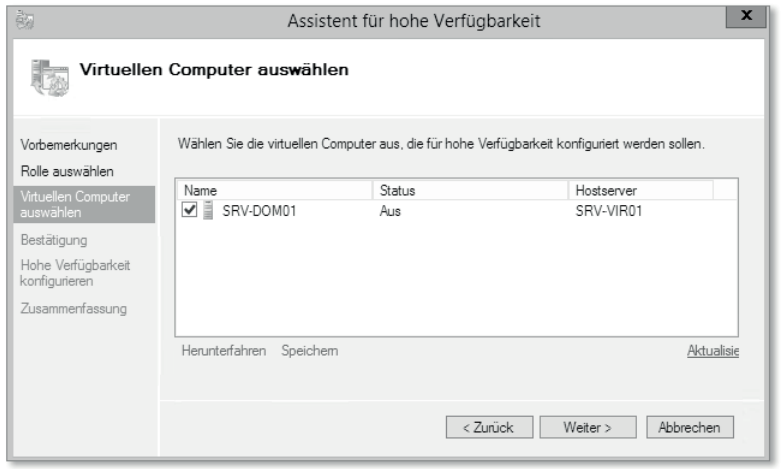


Abbildung 4.60 Eine VM, die bereits auf einem der Host-Server im Cluster läuft, lässt sich nachträglich in eine Cluster-VM umwandeln.

Da die Contoso AG System Center 2012 Virtual Machine Manager zur Verwaltung der Hyper-V-Umgebung einsetzt, erstellen die Administratoren in der SCVMM-Verwaltungskonsole eine neue Host-Gruppe und installieren den SCVMM-Agenten auf den Hyper-V-Servern. Dann ordnen sie den Hyper-V-Cluster der neuen Host-Gruppe zu. Weitere Informationen zum Einsatz des SCVMM 2012 bietet Ihnen Kapitel 6, »System Center Virtual Machine Manager«.

4.6 Live-Migration

Durch die Konsolidierung von Diensten als virtuelle Maschinen auf leistungsstarker Hardware wird die Menge an Systemen im Rechenzentrum deutlich reduziert. Dadurch entsteht allerdings eine starke Abhängigkeit von der verbleibenden Hardware. Insbesondere stellen sich neue Herausforderungen bei Wartungen, beim Patch-Management oder in Wiederanlaufszenarien. Gleichzeitig steigen die Anforderungen an die Verfügbarkeit.

Das Dilemma lässt sich mithilfe der *Live-Migration* elegant lösen, da virtuelle Maschinen im laufenden Betrieb von einem Hyper-V-Host auf einen anderen verschoben werden können, ohne Ausfallzeit hinnehmen zu müssen. Das funktioniert sowohl in einem Failover-Cluster als auch mit separat betriebenen Hyper-V-Hosts.

4.6.1 Funktionsweise

Eine virtuelle Maschine besteht aus der Konfiguration, virtuellen Festplatten, Arbeitsspeicher und Netzwerkkarten. Verschieben Sie eine virtuelle Maschine auf einen anderen Hyper-V-Host, müssen all diese Komponenten auf dem Ziel-Host erreichbar sein bzw. in Betrieb genommen werden. Sind einzelne Elemente der virtuellen Maschine auf dem Ziel-Host nicht verfügbar bzw. erreichbar, muss die Live-Migration mit einer *Speichermigration* (siehe Abschnitt 4.6.6, »Speicher-Live-Migration«) kombiniert werden, was von Microsoft glücklicherweise im selben Assistenten umgesetzt wurde.

Zu Beginn der Live-Migration wird eine Netzwerkverbindung zum Ziel-Host aufgebaut. Darüber wird zuerst die Konfiguration übertragen, damit der Ziel-Host die virtuelle Maschine anlegen und Arbeitsspeicher reservieren kann.

Der Arbeitsspeicher unterliegt ständigen Veränderungen durch das Gast-Betriebssystem, sodass die Übergabe an den Ziel-Host eine zeitkritische Angelegenheit darstellt. Der Inhalt des Arbeitsspeichers der virtuellen Maschine wird einmalig vollständig an den Ziel-Host übertragen. Da nach Abschluss der Übertragung bereits wieder Veränderungen am Arbeitsspeicher stattgefunden haben, findet anschließend eine differenzielle Übertragung dieser Veränderungen zum Ziel-Host statt.

Sind all diese Vorbereitungen abgeschlossen, stoppt der Hyper-V-Host die Ausführung der virtuellen Maschine, und der Ziel-Host übernimmt die Ausführung an genau diesem Punkt. Außerdem gibt der Quell-Host die virtuellen Festplatten, Snapshots und andere Elemente im Storage frei, sodass der Ziel-Host exklusiven Zugriff erhält.

Zum Zeitpunkt der Übergabe an den Ziel-Host kommt es zu einer kurzen Unterbrechung der Erreichbarkeit, da die Netzwerk-Switches über den Wechsel informiert werden müssen. In der Regel geht lediglich ein ICMP-Ping-Paket verloren, bis der Ziel-Host die Ausführung übernommen hat. Das beeinträchtigt die Ausführung der virtuellen Maschine und der betriebenen Dienste nicht, da Kommunikationsprotokolle den Verlust einzelner Datenpakete durch eine erneute Übertragung problemlos kompensieren können.

4.6.2 Einsatzszenarien

Aufgrund der zuvor beschriebenen Funktionsweise der Live-Migration eignet sie sich im Allgemeinen zur Umverteilung virtueller Maschinen, mit dem Ziel, Arbeiten an einem Hyper-V-Host vorzunehmen, die den Betrieb der virtuellen Maschinen gefährden könnten. Folglich wird durch die Live-Migration die Flexibilität erhöht. Es handelt sich insbesondere nicht um ein Werkzeug zur Erhöhung der Ausfallsicherheit. Dafür sei auf die VM-Replikation in Abschnitt 4.7 verwiesen.

Der Einsatz der Live-Migration ist ein hilfreiches Werkzeug in den folgenden Szenarien:

Sollten Sie Wartungsarbeiten an der Hardware des Hyper-V-Hosts durchführen müssen, hilft die Live-Migration, den unterbrechungsfreien Betrieb der virtuellen Maschinen zu gewährleisten. Es kann sich dabei zum Beispiel um Aktualisierungen von Firmware oder das Einspielen von Windows Updates für den Hyper-V-Host handeln. Zu Beginn der Wartung verschieben Sie alle Gast-Systeme auf einen anderen Hyper-V-Host, und nach Abschluss der Arbeiten führen Sie einen Lastenausgleich durch.

Eine besondere Variante dieses Einsatzszenarios stellt das Cluster Aware Updating (CAU) dar, das in Abschnitt 4.2.15, »Clusterfähiges Aktualisieren«, vorgestellt wurde. Dabei werden Aktualisierungen automatisch auf allen Hyper-V-Hosts installiert, ohne dass ein manueller Eingriff notwendig wird. Die virtuellen Maschinen werden dabei automatisch mithilfe der Live-Migration verschoben, damit die Installation von Updates ohne Beeinträchtigung der virtuellen Maschinen stattfinden kann.

Die Leistungsfähigkeit der virtualisierten Dienste hängt stark von den Leistungsreserven des Hyper-V-Hosts ab. Daher ist eine gleichmäßige Verteilung der Last der virtuellen Maschinen auf alle verfügbaren Hyper-V-Hosts von Vorteil. Dabei hilft die Live-Migration, da eine Umverteilung der virtuellen Maschinen im laufenden Betrieb ermöglicht wird.

4.6.3 Voraussetzungen

Da Hyper-V die Fähigkeiten eines Prozessors ausreizt, um die optimale Performance zu erreichen, ist die Live-Migration nur zwischen Hosts desselben CPU-Herstellers und mit derselben Version möglich. Werden allerdings unterschiedliche Prozessoren in den Hyper-V-Hosts eingesetzt, muss die Kompatibilität des Prozessors der virtuellen Maschine aktiviert werden (siehe Abbildung 4.61).

Diese Einschränkung gilt auch für den Einsatz von RemoteFX. Die Live-Migration ist nur zwischen Hosts möglich, auf denen derselbe Hersteller und dieselbe Version der Grafikkartenkerne eingesetzt werden.

Des Weiteren muss die Netzwerkkonfiguration der virtuellen Maschine auf den neuen Hyper-V-Host übertragbar sein. Das heißt, dass der virtuelle Switch auf beiden

Hosts denselben Namen haben muss. Ebenso müssen die Hosts an dieselben Subnetze angeschlossen sein.

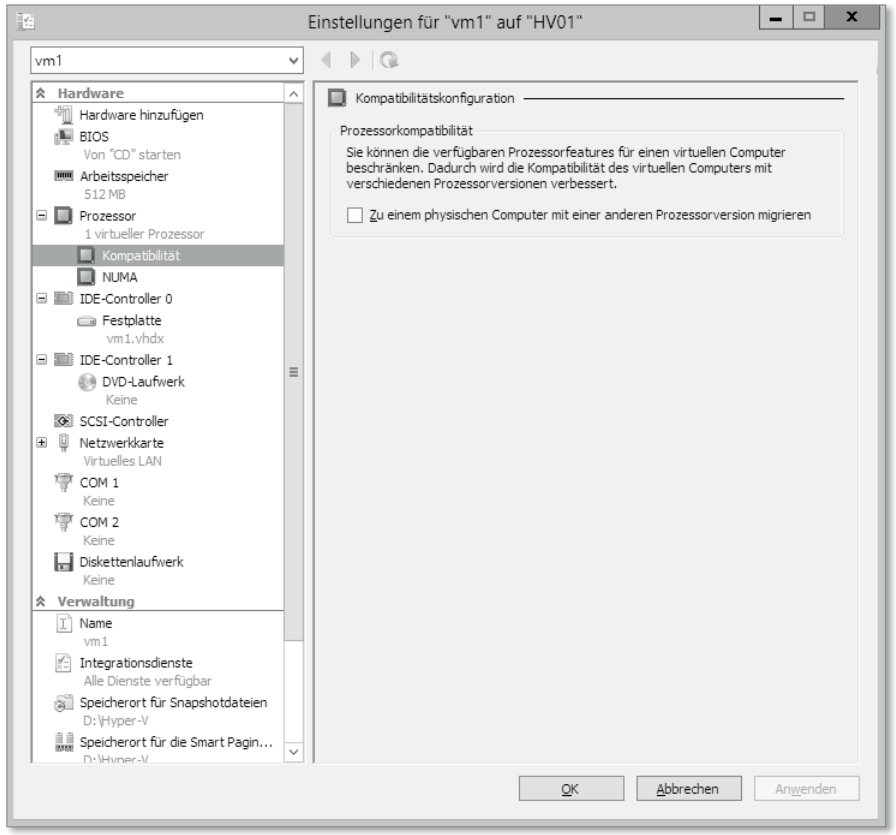


Abbildung 4.61 Nur mit aktivierter Prozessorkompatibilität können Sie Live-Migrationen auf einen Hyper-V-Host durchführen, dessen Prozessor einen anderen Typ desselben Herstellers hat.

Wird eine virtuelle Maschine mit direktem Zugriff auf die lokale Festplatte (Passthrough Storage) betrieben, ist eine Live-Migration nicht möglich, wenn eine Shared Nothing Live-Migration (SNLM) verwendet wird, da sich dieser Zugriff nicht virtualisieren lässt und bei der Live-Migration verloren ginge. Innerhalb einer Failover-Cluster-Umgebung ist es jedoch möglich, eine lokale Festplatte als Passthrough Storage zu betreiben.

Microsoft empfiehlt den Einsatz eines separaten Netzwerkadapters zur Isolation des Datenverkehrs durch die Live-Migration. Lässt sich das nicht realisieren, wird der Einsatz des Bandbreiten-Managements oder die Verwendung von Converged Fabrics empfohlen (siehe Abschnitt 4.6.7), um anderen Datenverkehr auf demselben Netzwerkadapter nicht zu beeinträchtigen.

4.6.4 Konfiguration

Die Einstellungen zur Anpassung des Verhaltens der Live-Migration befinden sich in den Hyper-V-Einstellungen des Hosts. Diese können über das Kontextmenü eines Hyper-V-Hosts oder über die Aktionen auf der rechten Seite des Hyper-V-Managers aufgerufen werden. Unterhalb des Eintrags LIVEMIGRATIONEN werden die Einstellungen angezeigt (siehe Abbildung 4.62).

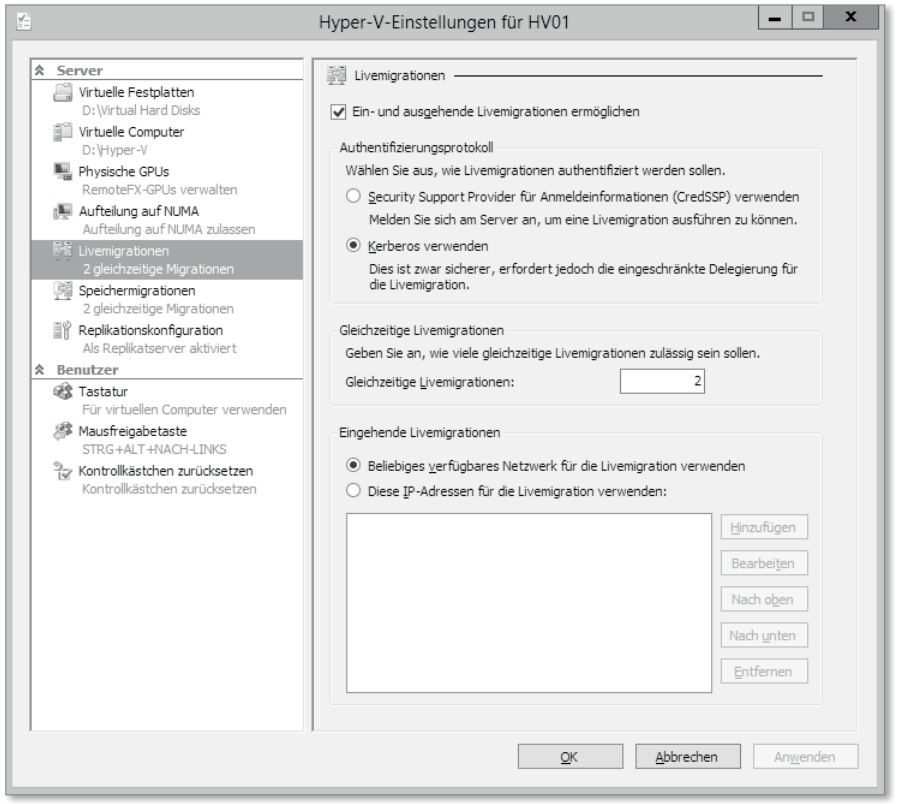


Abbildung 4.62 Die Konfiguration der Live-Migration befindet sich in den Einstellungen des Hyper-V-Hosts.

Live-Migrationen lassen sich für jeden Hyper-V-Host separat aktivieren oder deaktivieren (EIN- UND AUSGEHENDE LIVEMIGRATIONEN ERMÖGLICHEN). Dabei kann nicht nach eingehenden und ausgehenden Live-Migrationen unterschieden werden, da es als dauerhafte Einstellung keinen Sinn ergibt, nur eine Richtung für Live-Migrationen zu definieren. Mehr Flexibilität bei der Verteilung virtueller Maschinen kann mithilfe des Failover-Clusterings erreicht werden (siehe Abschnitt 4.2). Die PowerShell bietet die Commandlets `Enable-VMMigration` und `Disable-VMMigration` zur Steuerung dieser Eigenschaft.

Die Auswahl des Authentifizierungsprotokolls hat direkten Einfluss darauf, wie Sie Live-Migrationen zwischen den Hyper-V-Hosts durchführen können. Die Standardeinstellung (Credential Security Support Provider, CredSSP) ermöglicht Ihnen, Live-Migrationen nur dann zu starten, wenn Sie am Quell-Host angemeldet sind. Selbst wenn Sie passende Anmeldedaten für einen anderen Hyper-V-Host verwendet haben, schlägt eine Live-Migration mit einem anderen Hyper-V-Host fehl. Ihnen wird die folgende Fehlermeldung angezeigt:

Fehler beim Laden des virtuellen Computers.
Fehler beim Abrufen der Datenträgerinformationen
Das Konto »...« verfügt nicht über die erforderlichen Berechtigungen zum Öffnen der Anlage.

Die Verwendung von Kerberos zur Authentifizierung ist daher sinnvoll, wenn Sie mehrere Hyper-V-Hosts betreiben. Bevor Sie die Authentifizierung auf Kerberos umstellen, müssen Sie allerdings die eingeschränkte Delegation (Constrained Delegation) konfigurieren (siehe Kasten »Eingeschränkte (Constrained) Kerberos-Delegation«).

Eingeschränkte (Constrained) Kerberos-Delegation

Der Einsatz der eingeschränkten Kerberos-Delegation vereinfacht das Leben, wenn mehrere Hyper-V-Hosts zum Einsatz kommen oder die Administration mithilfe der Werkzeuge zur Remote-Administration auf einer Arbeitsstation ausgeführt wird.

Die Konfiguration erfolgt mithilfe des Verwaltungswerkzeugs Active-Directory-Benutzer und Computer. Führen Sie die folgenden Schritte für das Computerkonto jedes Hyper-V-Hosts aus:

- Wechseln Sie auf die Registerkarte Delegierung.
- Fügen Sie alle anderen Hyper-V-Hosts für den Dienst *Microsoft Virtual System Migration Service* (MVSMS) hinzu.
- Fügen Sie alle CIFS-Hosts für den Dienst CIFS hinzu (im Fall eines Scale-Out Fileservers ist nur das Konto des virtuellen Fileservers notwendig).
- Neustart des Hyper-V-Hosts

Damit auch die Speicher-Live-Migration mithilfe von Netzwerkfreigaben möglich ist (siehe Abschnitt 4.6.6), fügen Sie zusätzlich alle anderen Hyper-V-Hosts für den Dienst CIFS hinzu. In Abschnitt 4.4.2, »Authentifizierung mit Kerberos«, wird die Einrichtung der Delegation für den Dienst CIFS ausführlich beschrieben und lässt sich einfach auf den Dienst Hyper-V übertragen.

Mit der Einstellung für Gleichzeitige Livemigrationen wird konfiguriert, an wie vielen Live-Migrationen dieser Hyper-V-Host gleichzeitig teilnehmen darf (in der PowerShell konfigurierbar mit `Set-VMHost`). Ein- und ausgehende Live-Migrationen werden separat gezählt. Die Festlegung dieses Schwellenwertes hat direkten Einfluss

auf die Dauer von Live-Migrationen und die Leistung der virtuellen Maschinen auf diesem Hyper-V-Host. Während Live-Migrationen ablaufen, werden zusätzliche Kapazitäten des Netzwerks und der Speicheranbindung benötigt. Das kann zu einem Flaschenhals führen.

Mithilfe der letzten Option lassen sich IP-Adressen oder IP-Adressbereiche definieren, von denen Live-Migrationen eingehen dürfen (Eingehende Livemigrationen • Diese IP-Adressen für die Livemigration verwenden). Die Anpassung der Liste ermöglicht die Separation unterschiedlicher Hyper-V-Farmen beispielsweise aufgrund unterschiedlicher Verantwortung im Betrieb. Die Liste wird automatisch gepflegt, wenn Failover-Clustering zum Einsatz kommt (siehe Abschnitt 4.2). In der PowerShell nutzen Sie die Commandlets `Add-VMMigrationNetwork`, `Get-VMMigrationNetwork`, `Set-VMMigrationNetwork` und `Remove-VMMigrationNetwork`.

Die Live-Migration ist nur dann möglich, wenn in der Windows-Firewall die Regel namens Hyper-V (MIG-TCP eingehend) aktiviert ist.

4.6.5 Verwendung

Das Verschieben einer virtuellen Maschine auf einen anderen Hyper-V-Host initiieren Sie entweder über das Kontextmenü der virtuellen Maschine oder über die Aktionen für die ausgewählte virtuelle Maschine durch Auswahl des Befehls Verschieben (siehe Abbildung 4.63). Die PowerShell erledigt dies mit dem Kommando `Move-VM`.

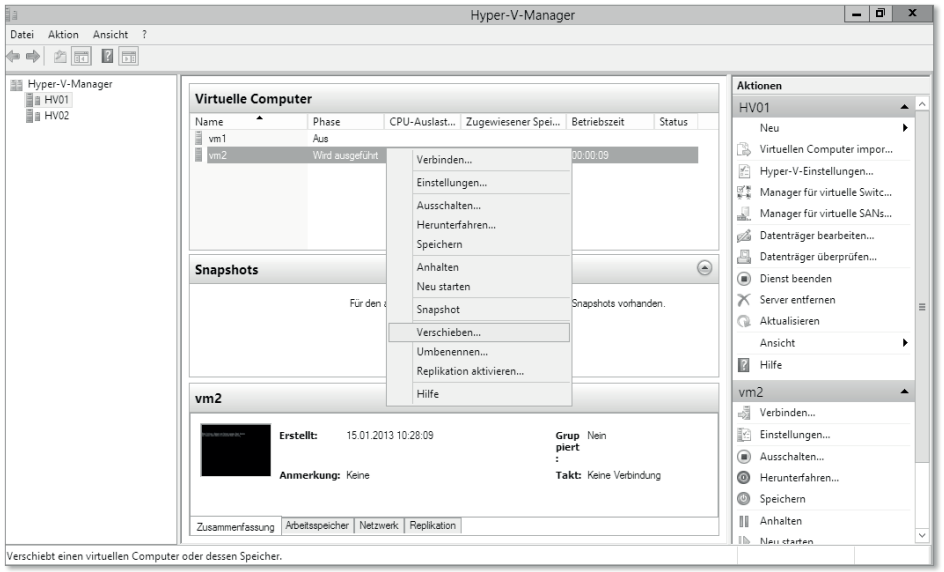


Abbildung 4.63 Die Live-Migration einer virtuellen Maschine wird entweder über das Kontextmenü oder die Aktionen in Hyper-V-Manager aufgerufen.

Das Verschieben einer virtuellen Maschine wird durch einen Assistenten vorbereitet. Nach dem Überspringen der Vorbemerkungen muss der Verschiebungstyp ausgewählt werden (siehe Abbildung 4.63). Eine Live-Migration wird durch den Punkt Virtuellen Computer verschieben ausgelöst.

Im nächsten Schritt wählen Sie den Ziel-Host für die Live-Migration aus (siehe Abbildung 4.64). Entweder geben Sie den Ziel-Host manuell ein oder klicken auf die Schaltfläche Durchsuchen, um einen Hyper-V-Host zu suchen.

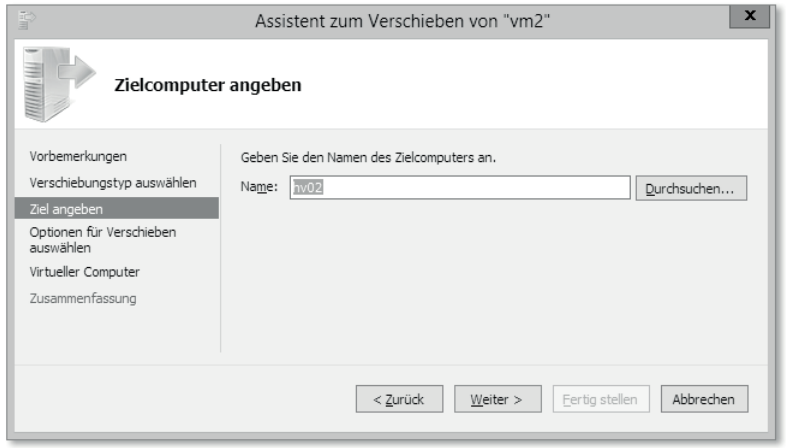


Abbildung 4.64 Der Zielcomputer ist ein Hyper-V-Host, der die Ausführung der virtuellen Maschine übernehmen soll.

Sollte der Ziel-Host nicht für Live-Migrationen konfiguriert sein, wird der Assistent Ihnen die folgende Fehlermeldung präsentieren:

> *Der Zielcomputer »hv02« ist nicht zum Senden oder Empfangen der Livemigrationen konfiguriert. Ändern Sie zum Beheben dieses Problems die Hyper-V-Einstellungen auf dem Zielcomputer.*

Falls Live-Migrationen im Ziel-Host aktiviert sind, die IP-Adresse des Quell-Hosts allerdings ausgeschlossen wurde, wird der Assistent Ihnen die folgende Fehlermeldung präsentieren:

> *Der Zielcomputer »hv02« ist nicht zum Empfangen von Livemigrationen konfiguriert. Ändern Sie zum Aktivieren von Migrationen auf dem Zielcomputer die Hyper-V-Netzwerkeinstellungen für eingehende Livemigrationen.*

Im nächsten Schritt werden die Optionen für das Verschieben der virtuellen Maschine festgelegt (siehe Abbildung 4.65).

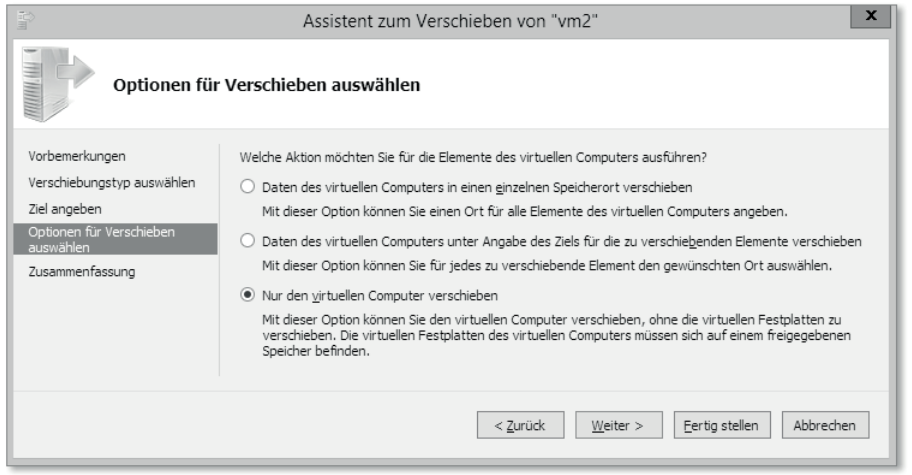


Abbildung 4.65 Wenn Sie gemeinsam genutzten Speicher für die beteiligten Hyper-V-Hosts verwenden, verschieben Sie nur den virtuellen Computer.

Die drei verfügbaren Varianten ermöglichen das Verschieben unterschiedlicher Teile der virtuellen Maschine:

1. Daten des virtuellen Computers in einen einzelnen Speicherort verschieben
   Die Ausführung der virtuellen Maschine wird auf dem Ziel-Host fortgesetzt. Gleichzeitig werden die Konfiguration und alle virtuellen Festplatten an einen neuen Speicherort verschoben.

   Diese Option sollten Sie einsetzen, wenn der Speicherort der virtuellen Maschine nicht auf gemeinsam genutztem Speicher liegt (*Shared Nothing Live-Migration*). Dabei werden alle Elemente an einem Speicherort abgelegt.
2. Daten des virtuellen Computers unter Angabe des Ziels für die zu verschiebenden Elemente verschieben
   Für den Fall, dass Sie die Konfiguration, die virtuellen Festplatten und die Snapshots getrennt speichern, erlaubt Ihnen diese Option, sehr detailliert separate Speicherorte für alle Elemente zu definieren.
3. Nur den virtuellen Computer verschieben
   Es wird lediglich die Ausführung der virtuellen Maschine auf einem anderen Hyper-V-Host fortgesetzt. Sowohl die Konfiguration als auch die Festplatten verbleiben am aktuellen Speicherort. Es wird vorausgesetzt, dass der Ziel-Host ebenfalls auf den Speicherort der virtuellen Maschine zugreifen kann.

   Setzen Sie bereits gemeinsam genutzten Speicher für die virtuellen Maschinen ein, können Sie mit dieser Option die Live-Migration beschleunigen, da die Konfiguration und die Festplatten am bisherigen Speicherort verbleiben.

Auch in kleinen Umgebungen empfiehlt sich die Verwendung von gemeinsam genutztem Speicher, sodass die Live-Migration nur die dynamischen Teile der virtuellen Maschine zum Ziel-Host übertragen muss.

Zum Abschluss des Assistenten werden noch einmal die von Ihnen gewählten Einstellungen angezeigt (siehe Abbildung 4.66). Die Beschreibung unterscheidet sich abhängig vom Verschiebetyp.

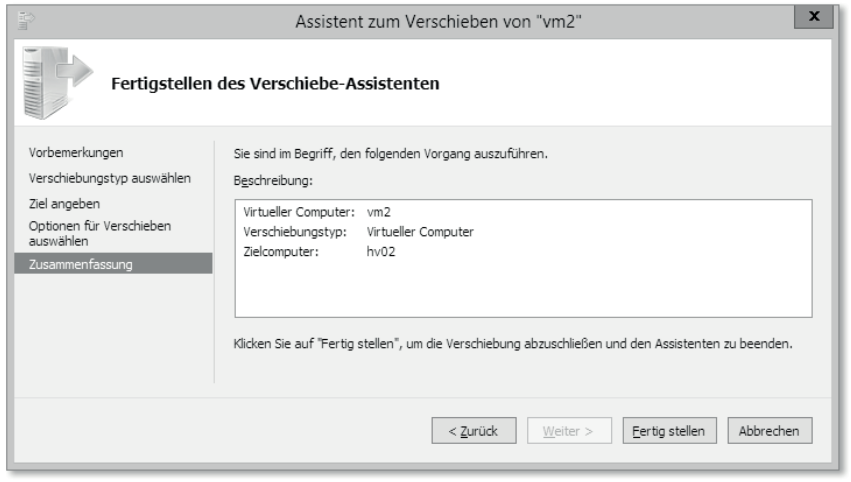


Abbildung 4.66 Die Zusammenfassung bietet Ihnen einen Überblick, bevor die Live-Migration durchgeführt wird.

4.6.6 Speicher-Live-Migration

Eine besondere Variante der Live-Migration kommt zum Einsatz, wenn Quell- und Ziel-Host keinen gemeinsamen Speicher teilen, um die virtuellen Festplatten und Snapshots zu speichern. Dann müssen zusätzlich die virtuellen Festplatten kopiert und abgeglichen werden, damit der Ziel-Host nach der Übergabe darauf zugreifen kann.

Während der Abgleich des Arbeitsspeichers stattfindet, werden alle Änderungen an den virtuellen Festplatten gleichzeitig in den bestehenden und den neuen Speicherort geschrieben. Zum Zeitpunkt der Übergabe erhält der Ziel-Host exklusiven Zugriff auf den neuen Speicherort, sodass auch die virtuellen Festplatten vollständig unter seiner Kontrolle stehen. Es ist ebenso möglich, lediglich den Speicherort einer virtuellen Maschine zu ändern, ohne die Ausführung auf einen anderen Hyper-V-Host zu verlegen.

Die Live-Migration kann während des gesamten Prozesses abgebrochen werden, bevor die Kontrolle an den Ziel-Host übergeben wurde.

Diese Art der Live-Migration wird auch *Shared Nothing Live-Migration* genannt, weil Quell- und Ziel-Host nicht einmal gemeinsamen Speicher benötigen.

Die Speicher-Live-Migration wird durch denselben Assistenten wie die bekannte Live-Migration initiiert (siehe Abbildung 4.67). Nach den Vorbemerkungen des Assistenten wird die Speicher-Live-Migration durch die Auswahl von SPEICHER DES VIRTUELLEN COMPUTERS VERSCHIEBEN ausgelöst (in der PowerShell: `Move-VM`).

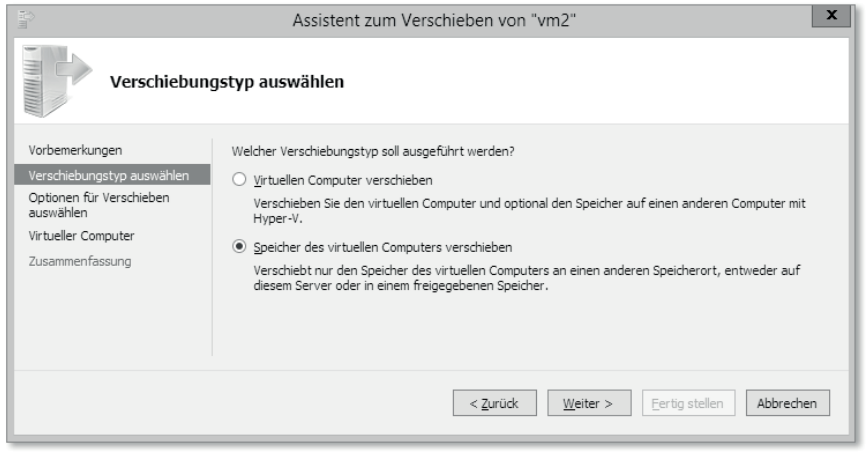


Abbildung 4.67 Das Verschieben des Speichers einer virtuellen Maschine wird mit demselben Assistenten gestartet, der auch für die Live-Migration zuständig ist.

Die Speicher-Live-Migration führt zu derselben Auswahl für das Verschieben des Speichers wie in Abbildung 4.68 der Live-Migration.

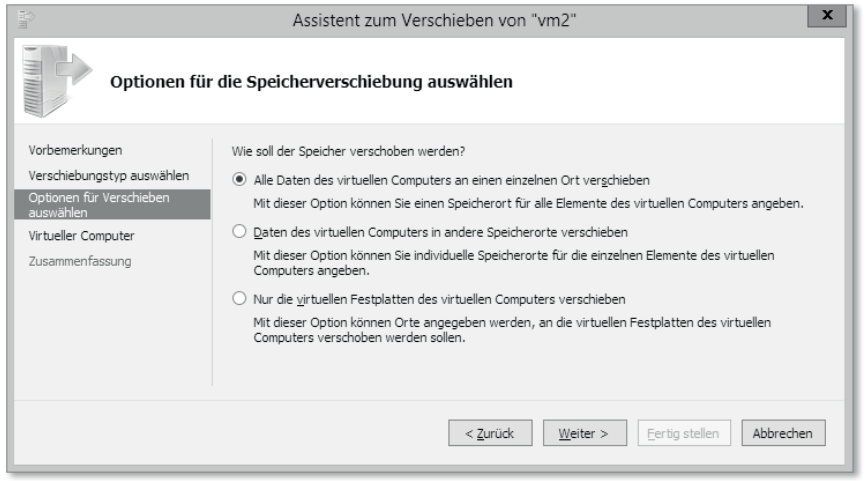


Abbildung 4.68 In den meisten Fällen sind die Daten einer virtuellen Maschine an einem einzelnen Ort abgelegt.

Die Auswahl zum Verschieben der Daten an einen einzelnen Speicherort führt zur Eingabe des Ordners, in dem die virtuelle Maschine gespeichert werden soll (siehe

Abbildung 4.69). Im Gegensatz zum Hinzufügen einer neuen virtuellen Maschine erstellt Hyper-V dabei allerdings keinen Unterordner mit dem Namen der virtuellen Maschine. Bei Bedarf sollten Sie daher den Namen der virtuellen Maschine eigenhändig anhängen.

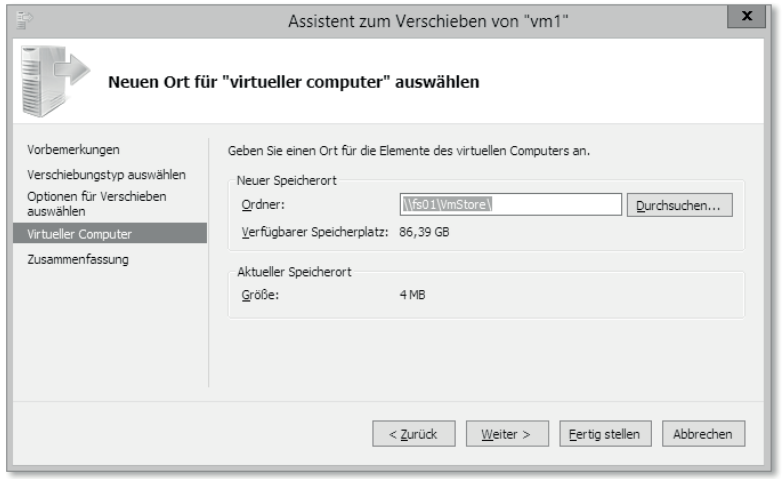


Abbildung 4.69 Der Zielordner für die Speichermigration darf seit Windows Server 2012 auch eine Dateifreigabe sein.

Mit dem Bestätigen der Zusammenfassung führt Hyper-V die Speicher-Live-Migration mit den konfigurierten Parametern aus (siehe Abbildung 4.70).

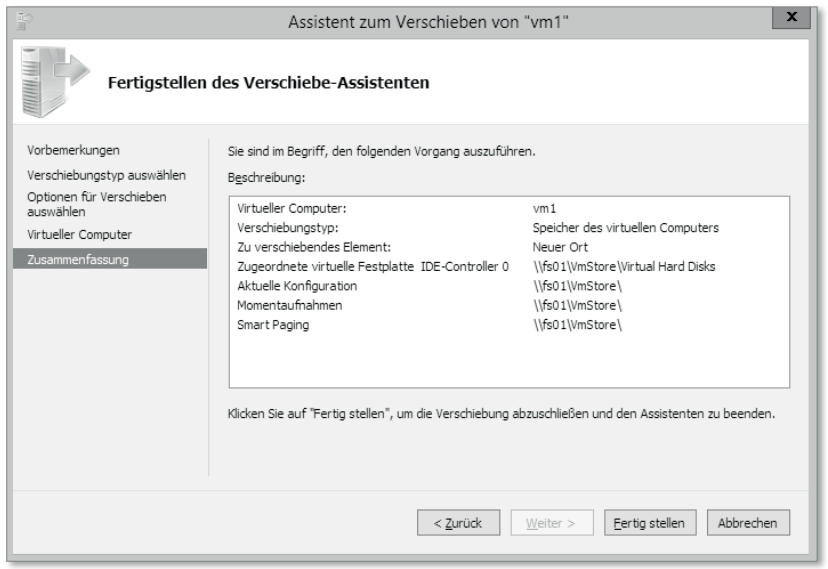


Abbildung 4.70 Die Zusammenfassung für die Speicher-Live-Migration zeigt Ihnen die gewählten Parameter, bevor der Prozess startet.

4.6.7 Bandbreiten-Management

Die Live-Migration verursacht eine hohe Netzwerkbelastung, die gleichzeitige Kommunikation auf derselben Netzwerkverbindung stark behindern kann. Daher soll das Bandbreiten-Management (Quality of Service, QoS) dann zum Einsatz kommen, wenn der Datenverkehr durch die Live-Migration nicht in einem separaten Netzwerk isoliert werden kann.

Microsoft empfiehlt für die Live-Migration wenigstens eine dedizierte Netzwerkschnittstelle mit 1 GBit/s – besser aber 10 GBits/s. Sollte dies nicht möglich sein, kann der Datenverkehr mit dem Cluster-Heartbeat kombiniert werden, sodass von 2 × 1 GBit/s 40 Prozent bzw. von 2 × 10 GBits/s 50 Prozent für die Live-Migration genutzt werden können. Für detaillierte Informationen über die Geschwindigkeit einer Live-Migration in Abhängigkeit von der verwendeten Netzwerk-Bandbreite und des Arbeitsspeichers der virtuellen Maschinen liefert die folgende Webseite: *http://technet.microsoft.com/de-de/library/ff428137(v=ws.10).aspx* (Kurzlink: *http://qccq.de/s/h411*).

Die Konfiguration des Bandbreiten-Managements ist in allen Editionen von Windows Server 2012 enthalten. Es ist dafür gedacht, den Netzwerkverkehr des Host-Systems zu kontrollieren und zu beeinflussen und sollte daher nicht innerhalb einer virtuellen Maschine zum Einsatz kommen. Damit das Bandbreiten-Management zusätzlich von der Netzwerk-Hardware im Rechenzentrum umgesetzt wird, muss die eingesetzte Hardware dem Standard »Data Center Bridge« (DCB) folgen.

In Hyper-V müssen die folgenden vier Typen von Daten unterschieden werden:

1. Kommunikation mit Dateifreigaben (SMB)
2. Live-Migrationen zwischen Hyper-V-Hosts
3. Kommunikation zwischen Cluster-Knoten (Heartbeat)
4. Verwaltung des Hyper-V-Hosts

Das Konzept des Bandbreiten-Managements beruht darauf, jeder Klasse von Daten eine minimale Bandbreite zuzuweisen, sodass selbst bei hoher Netzwerkauslastung ein minimaler Anspruch an den Durchsatz im Netzwerk gestellt werden kann. Dieser Anspruch wird mithilfe eines Gewichts bestimmt, das prozentual zu verstehen ist. Zusätzlich wird eine Priorität vergeben, die im DSCP-Feld (Differentiated Services Code Point) des IPv4- bzw. IPv6-Headers vermerkt wird. So lässt sich die Priorisierung auch außerhalb der Hyper-V-Hosts durchsetzen.

```
New-NetQosPolicy "Live Migration" -LiveMigration ⮐
-MinBandwidthWeight 30 -Priority 5
New-NetQosPolicy "SMB" -SMB -MinBandwidthWeight 50 –Priority 3
```

```
New-NetQosPolicy "Cluster" -IPDstPort 3343 -MinBandwidthWeight 10 ↩
-Priority 6
New-NetQosPolicy "Management" -Default -MinBandwidthWeight 10
```

Listing 4.3 Einrichtung der Gewichtung und Priorität für die vier Klassen von Netzwerkdaten

Die Identifizierung der vier Klassen von Netzwerkverkehr geschieht anhand der eingebauten Parameter für SMB-Datenverkehr (`-SMB`) und Live-Migrationen (`-LiveMigration`). Der Cluster-Heartbeat wird über den Ziel-Port 3343 erkannt (`-IPDstPort`).

Der restliche Datenverkehr wird als administrative Kommunikation kategorisiert (`-Default`; siehe auch Listing 4.3).

4.6.8 Live-Migration im Failover-Cluster

Die Live-Migration funktioniert auch im Failover-Cluster wie gewohnt unabhängig davon, ob als gemeinsamer Speicher ein SAN oder NAS zum Einsatz kommt. Dies ist die Grundlage für das clusterfähige Aktualisieren, das in Abschnitt 4.2.15 beschrieben wurde.

Sie können die Live-Migration auch zwischen zwei Failover-Clustern ohne gemeinsamen Speicher durchführen. Dann sollten Sie aber vorher die Hochverfügbarkeit der virtuellen Maschine deaktivieren, da sonst ein Failover innerhalb des Clusters automatisch geschieht.

Innerhalb eines Failover-Clusters können Sie außerdem beliebig viele gleichzeitige Live-Migrationen starten. Trotzdem werden nie mehr Live-Migrationen gleichzeitig ausgeführt, als Sie konfiguriert haben (siehe Abschnitt 4.6.4, »Konfiguration«). Stattdessen werden die überzähligen Live-Migrationen in eine Warteschlange gestellt und nacheinander abgearbeitet.

4.6.9 Neuerungen in Windows Server 2012 R2

Mit der Aktualisierung auf R2 von Windows Server 2012 stehen drei Optionen für die Konfiguration ausgehender Live-Migrationen zur Verfügung, die einen deutlichen Einfluss auf die Geschwindigkeit der Live-Migration haben (siehe LEISTUNGSOPTIONEN in Abbildung 4.71).

Bisher führte Windows Server 2012 »R1« die Live-Migration in dem Modus durch, der nun mit TCP/IP bezeichnet wird. Es handelt sich dabei um eine proprietäre Datenverbindung zwischen dem Quell- und Ziel-Host.

In Windows Server 2012 R2 wird standardmäßig dieselbe Datenverbindung genutzt. Zusätzlich wird aber eine Komprimierung der Daten durchgeführt, sodass die Live-

Migration schnell durchgeführt und dadurch schneller beendet wird. Dieser Modus nennt sich KOMPRIMIERUNG und ist die Voreinstellung in Windows Server 2012 R2.

Mit der Auswahl der SMB-basierten Live-Migrationen werden die Daten mittels SMB 3.0 zwischen Quell- und Ziel-Host ausgetauscht. Dadurch können SMB Multichannel und SMB Direct für die Live-Migration genutzt werden.

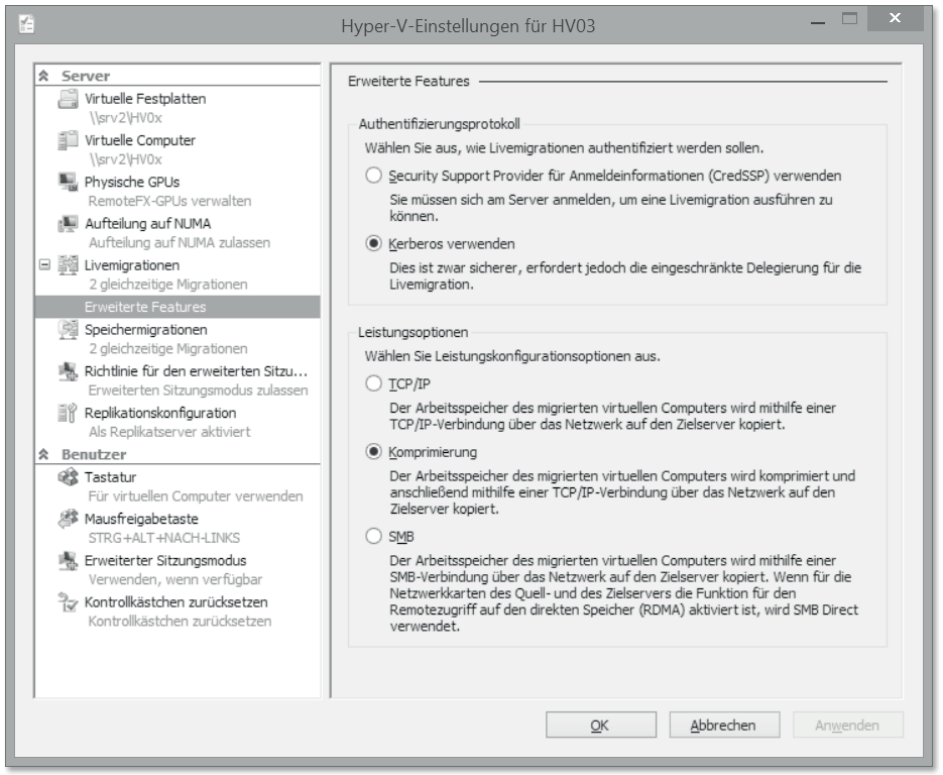


Abbildung 4.71 Die Leistungsoptionen bestimmen den Betriebsmodus für ausgehende Live-Migrationen.

Microsoft empfiehlt, die komprimierte Live-Migration zu nutzen, wenn der Hyper-V-Host mit einem oder mehreren 1GbE-Verbindungen angebunden ist. Da dies heutzutage den Standard darstellen sollte, wurde die Komprimierung vorausgewählt. Die Nutzung der SMB-basierten Live-Migration sollte demnach in schnellen Netzwerken mit 10GbE-Anbindungen genutzt werden.

Windows Server 2012 R2 ermöglicht die Live-Migration virtueller Maschinen von einem Hyper-V-Host mit Windows Server 2012 und erlaubt dadurch die schrittweise Migration einer Hyper-V-Umgebung auf die neue Betriebssystem-Version. Bitte beachten Sie, dass eine Live-Migration zurück von Windows Server 2012 R2 nicht unterstützt wird.

4.7 VM-Replikation

Die Replikation sorgt dafür, dass virtuelle Maschinen zwar nur in einem Rechenzentrum ausgeführt werden, das zweite Rechenzentrum aber eine stets aktuelle Kopie – das Replikat – vorhält (siehe Abbildung 4.72). Fällt das erste Rechenzentrum aus, kann die virtuelle Maschine in dem anderen Rechenzentrum hochgefahren werden.

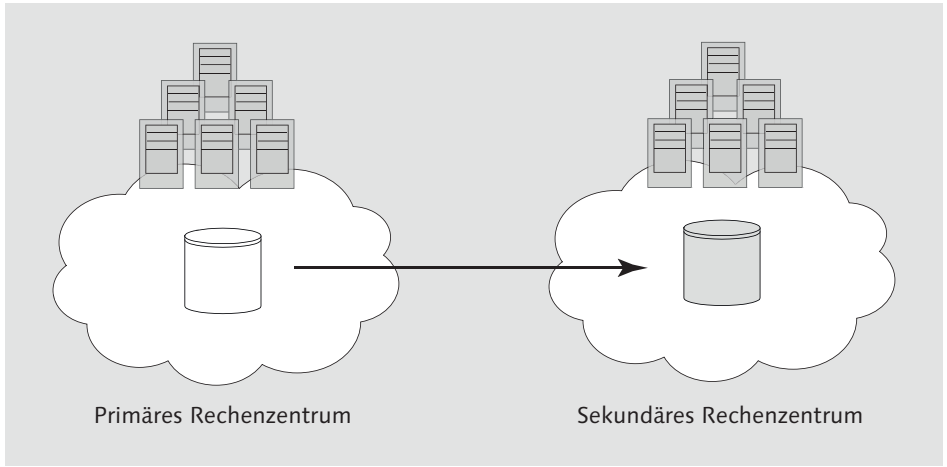


Abbildung 4.72 Die VM-Replikation überträgt virtuelle Maschinen zwischen Rechenzentren.

Die VM-Replikation ist insbesondere dann sinnvoll, wenn die Rechenzentren nicht über gemeinsamen Speicher, sondern lediglich über eine WAN-Verbindung verfügen. Der Einsatz ist auch in Netzwerken mit geringer Bandbreite und hoher Latenz möglich.

Beachten Sie, dass die VM-Replikation keinen Ersatz für den Failover-Cluster darstellt. Replizierte, virtuelle Maschinen werden weder automatisch in Betrieb genommen, noch wird ein automatischer Failback vorgenommen. Die VM-Replikation erfordert daher den manuellen Eingriff, nachdem ein Ausfall festgestellt wurde bzw. der Ausfall behoben wurde.

4.7.1 Funktionsweise

Die VM-Replikation stellt keine vollautomatische Lösung für Ausfälle ganzer Rechenzentren dar. Es gibt weder einen Heartbeat für die Replikation, um einen Ausfall zu bemerken, noch eine dritte Instanz (Witness) neben Quell- und Ziel-Host, um das aktive Rechenzentrum automatisch zu wählen. Die VM-Replikation dient daher zur Sicherung von virtuellen Maschinen in einem zweiten Rechenzentrum und erfordert eine Überwachung und Alarmierung sowie Ihren manuellen Eingriff, sollte ein Rechenzentrum ausfallen.

Bevor die Replikation aufgenommen werden kann, müssen der primäre Hyper-V-Host und der Replikat-Server eine Kopie der virtuellen Maschine austauschen, um anschließend die Veränderungen übertragen zu können. Ist dies erfolgt, sichert Hyper-V alle Schreibzugriffe im Hyper-V Replica Log (HRL) auf dem primären Hyper-V-Host. Im Abstand von fünf Minuten wird das HRL zum Replikat-Server übertragen. Dort wird das HRL rückwärts angewendet, sodass nur die letzte Änderung eines Datenblocks an den virtuellen Festplatten am Ziel angewendet wird. Dieser Mechanismus hat eine asynchrone Replikation zur Folge, die mit hohen Latenzen umgehen kann.

Sollte die Replikation nicht wie geplant alle fünf Minuten stattfinden können, werden auf dem primären Hyper-V-Host Ereignisse generiert. Hyper-V versucht dann, in regelmäßigen Zeitabständen das HRL zu replizieren. Sollte die Größe des HRLs die Hälfte der virtuellen Festplatte betragen, wird die Replikation angehalten. Die Replikation wird nicht automatisch wieder aufgenommen, sondern erfordert den manuellen Eingriff eines Administrators.

Zusätzlich bietet die VM-Replikation die Möglichkeit, Wiederherstellungspunkte zu definieren, um die Konsistenz von Anwendungen innerhalb der virtuellen Maschine zu verbessern (siehe Abschnitt 4.7.9, »Wiederherstellungspunkte«).

Obwohl die VM-Replikation für WAN-Verbindungen entworfen wurde, empfiehlt es sich, die Anzahl gleichzeitiger Replikationen zu beschränken. Beispielsweise ermöglicht eine WAN-Verbindung mit einer Bandbreite von 1,5 Mbps, 100 ms Latenz und ein Prozent Paketverlust bis zu drei gleichzeitige Replikationen. Steht eine Bandbreite von 300 Mbps bei 10 ms Latenz und derselben Paketverlustrate zur Verfügung, können auch zehn gleichzeitige Replikationen durchgeführt werden.

VM-Replikation im Hyper-V-Poster

Microsoft hat eine grafische Übersicht der gesamten Hyper-V-Rolle erstellt und diese in Form eines Posters veröffentlicht. Darin wird der VM-Replikation ein ganzer Abschnitt gewidmet, der die zentralen Fakten übersichtlich darstellt. Zusätzlich beschreibt ein begleitendes Dokument die VM-Replikation im Detail.

Quelle: Windows Server 2012 Hyper-V Component Architecture Poster and Companion References; *https://www.microsoft.com/en-us/download/details.aspx?id=29189* (Kurzlink: *http://qccq.de/s/h412*)

4.7.2 Die Hosts konfigurieren

Ähnlich wie bei der Live-Migration muss ein Hyper-V-Host für das Empfangen der VM-Replikation konfiguriert werden (siehe Abbildung 4.73). In der PowerShell nutzen Sie dafür die Commandlets `Get-VMReplicationServer` und `Set-VMReplicationServer`.

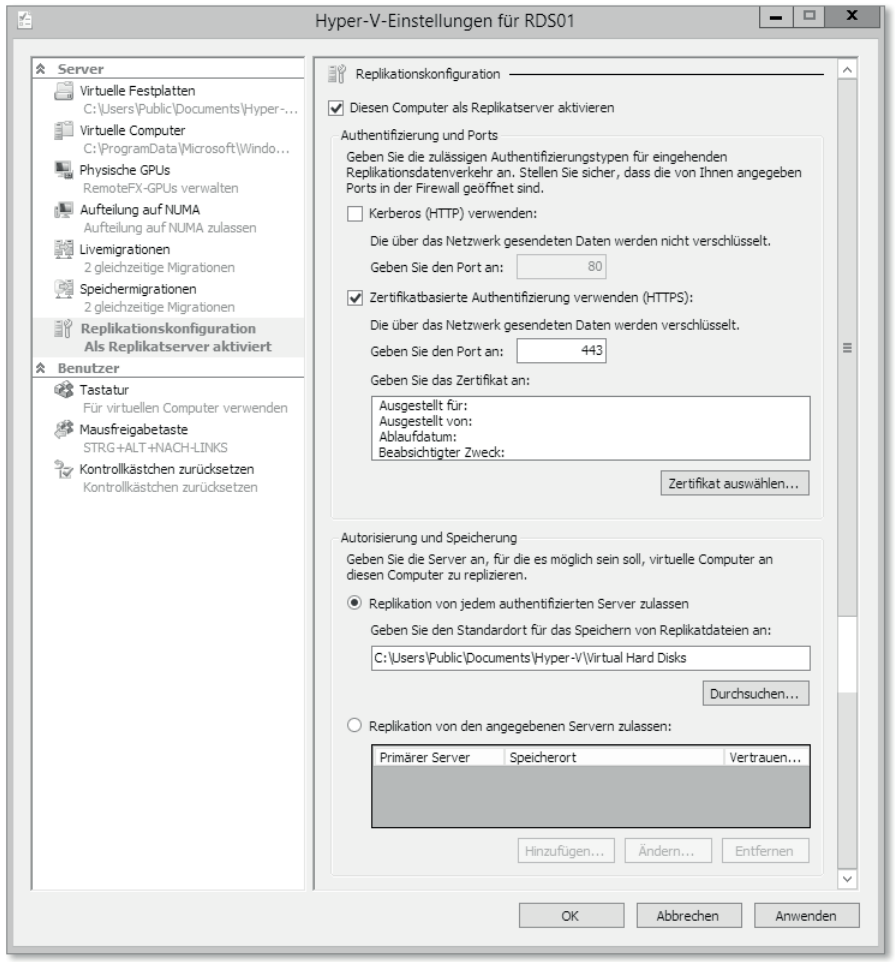


Abbildung 4.73 Die Konfiguration für die VM-Replikation befindet sich in den Einstellungen des Hyper-V-Hosts.

Die Wahl der Authentifizierung (HTTP oder HTTPS) legt auch gleichzeitig die verwendeten Netzwerk-Ports fest (80 oder 443). Die Verwendung von HTTP ist innerhalb eines AD-Waldes ausreichend – allerdings erfolgt die Replikation unverschlüsselt. Der Einsatz von HTTPS bietet zwar höhere Sicherheit, erfordert aber zusätzlich ein Zertifikat, das auf den Host-Namen des Hyper-V-Hosts ausgestellt sein muss, und alle an der Replikation beteiligten Server müssen der ausstellenden Zertifizierungsstelle vertrauen.

Ist die VM-Replikation aktiviert, können Sie detailliert steuern, für welche Hyper-V-Hosts dieser Server als Replikat-Server zur Verfügung steht. Es ist keine Einschränkung vorausgewählt. In diesem Fall werden die Replikatdateien an genau einem Ort gespeichert, den Sie selbst anpassen können, falls Sie die Daten auf einem separaten

Volumen speichern möchten. Alternativ steht Ihnen die Möglichkeit zur Verfügung, eine Liste von Hyper-V-Hosts zu pflegen, die mit diesem Server eine Replikationsbeziehung aufbauen dürfen. Dabei können Sie für jeden Hyper-V-Host einen separaten Speicherort definieren, um die Replikatdateien voneinander zu trennen. Die PowerShell hält hierfür die Befehle `Get-VMReplicationAuthorizationEntry`, `New-VMReplicationAuthorizationEntry`, `Set-VMReplicationAuthorizationEntry` und `Remove-VMReplicationAuthorizationEntry` bereit.

Abhängig von der gewählten Authentifizierungsmethode ist es notwendig, eine Regel in der Windows-Firewall zu aktivieren. Für HTTP lautet diese Hyper-V Replikat – HTTP-Listener (TCP eingehend), und für HTTPS ist es Hyper-V Replikat – HTTPS-Listener (TCP eingehend).

4.7.3 VM-Replikation aktivieren

Die Replikation einer virtuellen Maschine wird über die Aktionen oder das Kontextmenü gestartet (Abbildung 4.74). Es folgt ein Assistent zur Einrichtung der Replikation. In der PowerShell nutzen Sie `Get-VMReplication` und `Enable-VMReplication`.

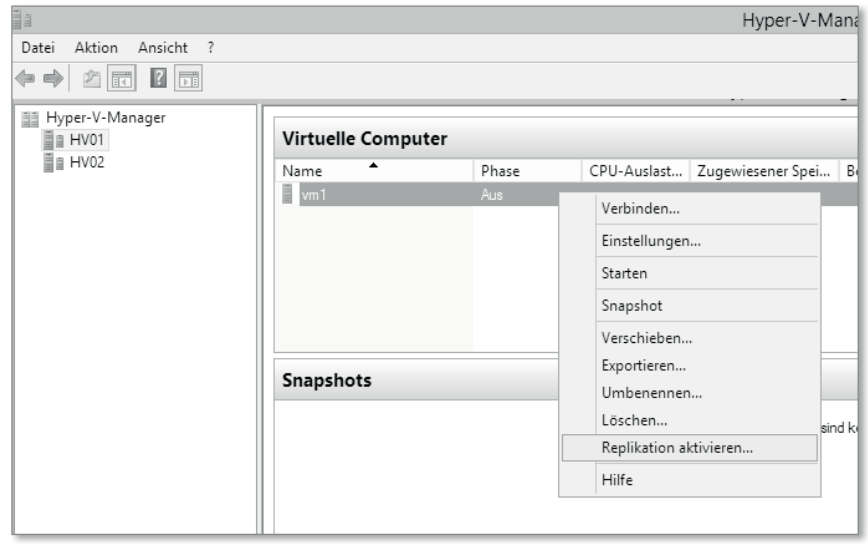


Abbildung 4.74 Aktivieren Sie die Replikation für eine virtuelle Maschine über das Kontextmenü oder die Aktionen im Hyper-V-Manager.

Direkt nach den Vorbemerkungen fordert der Assistent Sie auf, den Replikat-Server anzugeben, auf den die virtuelle Maschine repliziert werden soll (siehe Abbildung 4.75).

Anschließend sind die Verbindungsparameter für den Replikat-Server erforderlich. Dabei können Sie den Authentifizierungstyp – HTTP oder HTTPS – wählen und die Kompression abschalten (siehe Abbildung 4.76).

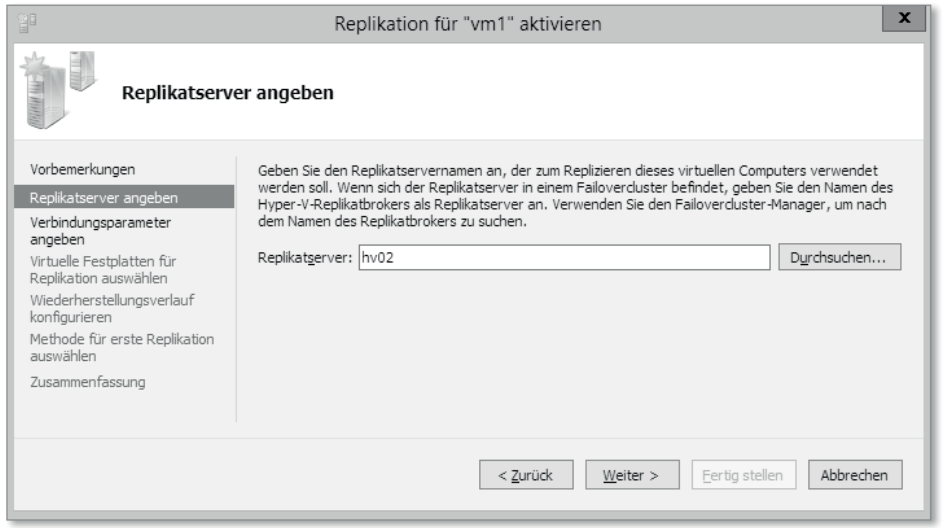


Abbildung 4.75 Der Replikat-Server ist das Ziel der Replikation für die virtuelle Maschine.

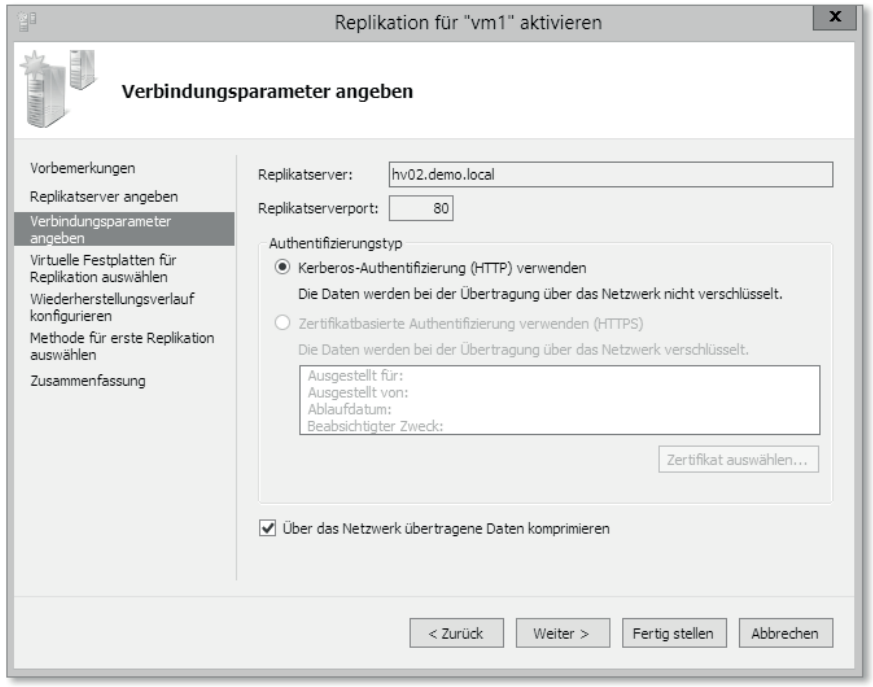


Abbildung 4.76 Die Authentifizierung kann entweder mit Kerberos oder mit Zertifikaten durchgeführt werden.

Beachten Sie, dass die Kompression in der Vorauswahl aktiviert ist und dies den Prozessor des Hyper-V-Hosts belastet. Abhängig von der Auslastung des Hyper-V-Hosts

ist es ratsam, die Auswirkungen der Kompression zu evaluieren, um die Beeinträchtigung der laufenden virtuellen Maschinen auszuschließen.

Im nächsten Schritt bietet der Assistent Ihnen an, bestimmte virtuelle Festplatten von der Replikation auszuschließen (siehe Abbildung 4.77). Das kann die Replikation beschleunigen, wenn virtuelle Festplatten lediglich temporäre Daten beinhalten, die bei der Inbetriebnahme im sekundären Rechenzentrum nicht relevant sind, zum Beispiel dedizierte Festplatten für die Auslagerungsdatei oder temporäre Daten für die Anwendung in der virtuellen Maschine.

Dabei ist allerdings zu beachten, dass die Inbetriebnahme nur dann erfolgen kann, wenn Sie diese virtuellen Festplatten im sekundären Rechenzentrum generieren und an die virtuelle Maschine anschließen, bevor Sie diese hochfahren.

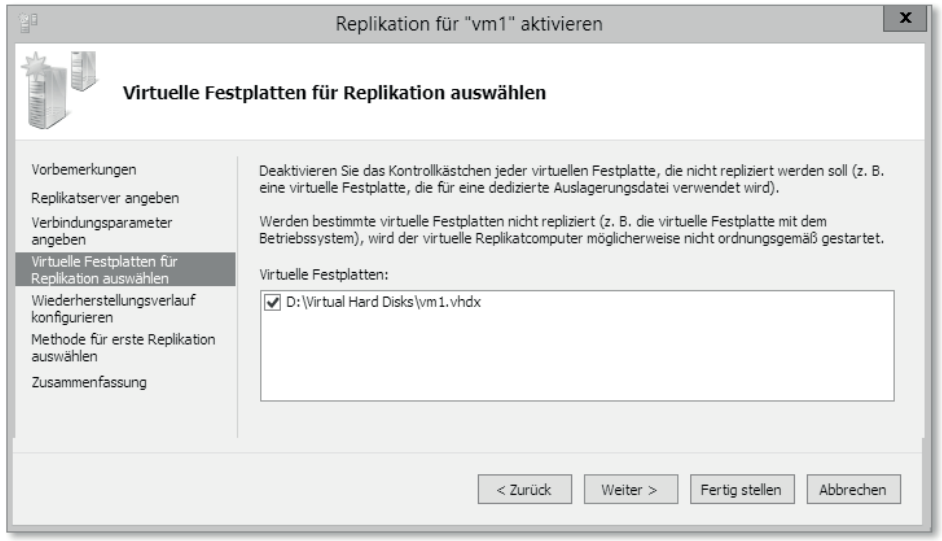


Abbildung 4.77 Nur die hier ausgewählten Festplatten werden repliziert. Diese Auswahl können Sie nachträglich nicht mehr ändern.

Im Anschluss ermöglicht der Assistent die Konfiguration von Wiederherstellungspunkten für die Replikation. In der Regel ist das aber nicht notwendig, da die Vorgabe ausreicht (siehe Abbildung 4.78). Eine Abweichung von dieser Konfiguration ist für Anwendungen mit besonderen Konsistenzanforderungen erforderlich. Mehr dazu lesen Sie in Abschnitt 4.7.9, »Wiederherstellungspunkte«.

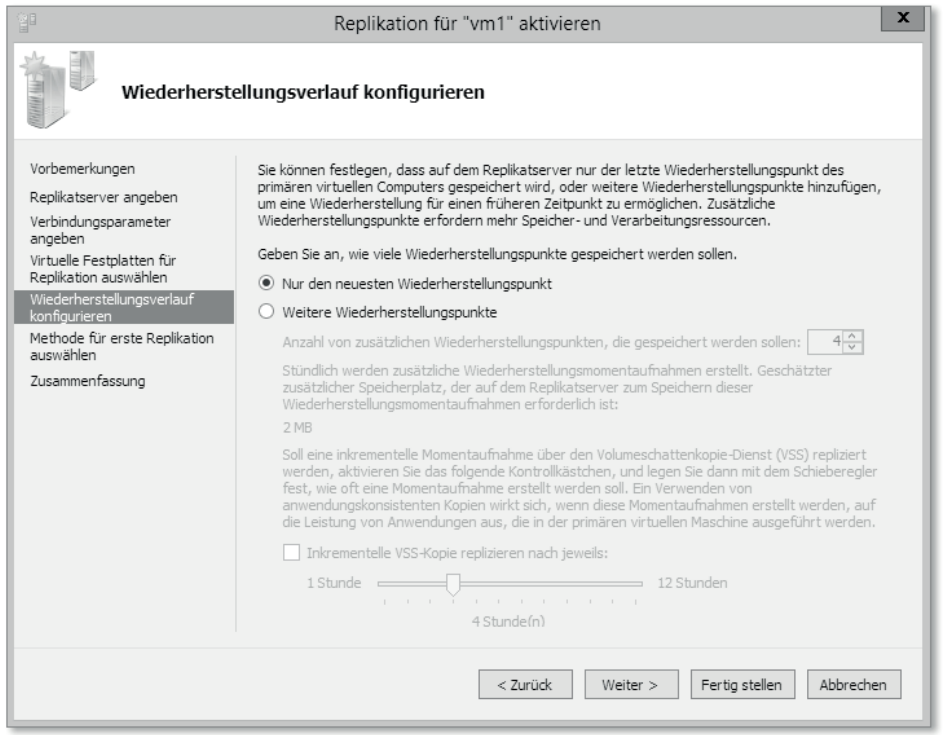


Abbildung 4.78 Oft reicht ein einzelner Wiederherstellungspunkt aus – wenn nicht, helfen die zusätzlichen Einstellungen.

Bevor die Replikation aufgenommen werden kann, müssen Sie die betroffene virtuelle Maschine einmalig auf den Replikat-Server übertragen. Dafür sieht der Assistent drei Varianten vor (siehe Abbildung 4.79):

1. Sollten Sie die Erstkopie im Netzwerk senden wollen, müssen Sie mit einer deutlichen Belastung des Netzwerks rechnen. Es empfiehlt sich, die Erstkopie außerhalb der Kernarbeitszeiten auszuführen.
2. Ist es Ihnen nicht möglich, die Erstkopie über das Netzwerk zu senden, wählen Sie Erstkopie mithilfe eines externen Mediums senden. Nach der Angabe eines Speicherorts wird dort ein Export der virtuellen Maschine erzeugt, den Sie auf einem beliebigen Weg zum Replikat-Server befördern müssen.
3. Die dritte Option Vorhandenen virtuellen Computer auf dem Replikatserver als Anfangskopie verwenden bietet Ihnen die Möglichkeit, eine vorhandene virtuelle Maschine als Erstkopie zu verwenden. Beachten Sie aber, dass es sich um die Wiederherstellung einer existierenden Sicherung der betroffenen virtuellen Maschine handeln muss.

Zusätzlich können Sie entscheiden, die Erstkopie sofort zu erstellen oder zu einem späteren Zeitpunkt damit zu beginnen. In der PowerShell verwenden Sie die Kommandos `Import-VMInitialReplication`, `Start-VMInitialReplication` und `Stop-VMInitialReplication`.

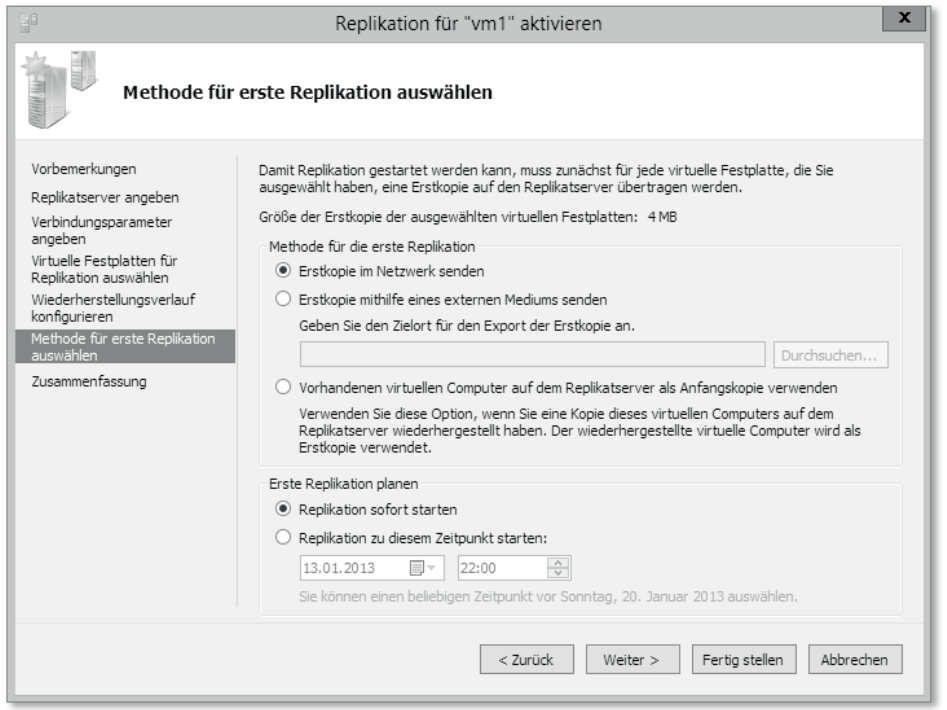


Abbildung 4.79 Die Wahl der Methode für die Übertragung der Erstkopie kann durch den hohen Datenverkehr eine Beeinträchtigung des produktiven Netzwerks zur Folge haben.

Zuletzt zeigt der Assistent Ihnen eine Zusammenfassung der gewählten Parameter wie in Abbildung 4.80. Nach einem Klick auf Fertig stellen wird die VM-Replikation eingerichtet.

Nach dem Aktivieren der Replikation für eine virtuelle Maschine verändern sich die Aktionen bzw. das Kontextmenü, sodass ein Untermenü zur Verwaltung der Replikation angezeigt wird (siehe Abbildung 4.81). Sie können nun die virtuelle Maschine auf dem Hyper-V-Host im sekundären Rechenzentrum in Betrieb nehmen (Geplantes Failover, siehe dazu auch Abschnitt 4.7.7), die Replikation anhalten, den Replikationsstatus anzeigen (siehe Abbildung 4.82) oder die Replikation entfernen. Die PowerShell hält die Commandlets `Suspend-VMReplication` und `Resume-VMReplication` sowie `Remove-VMReplication` bereit.

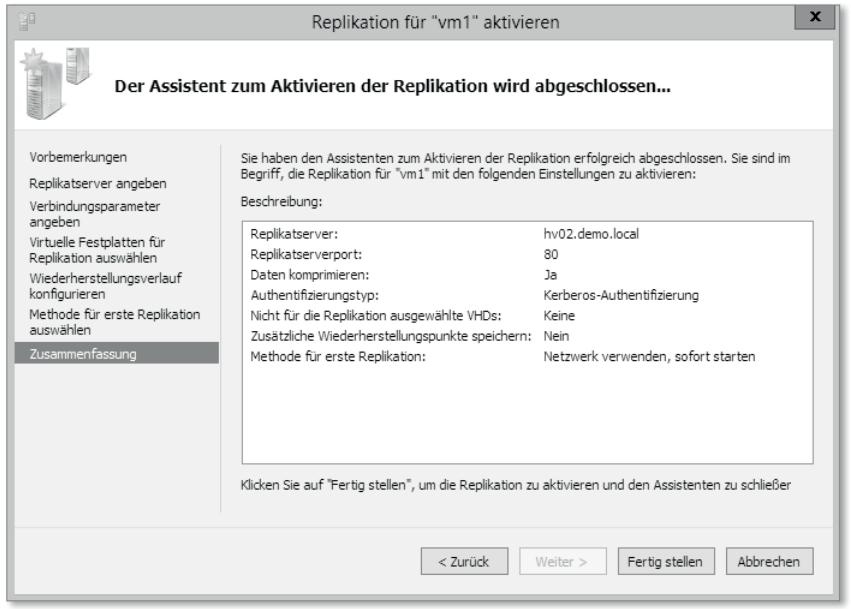


Abbildung 4.80 Vor dem Beginn der VM-Replikation erhalten Sie eine Zusammenfassung der gewählten Einstellungen.

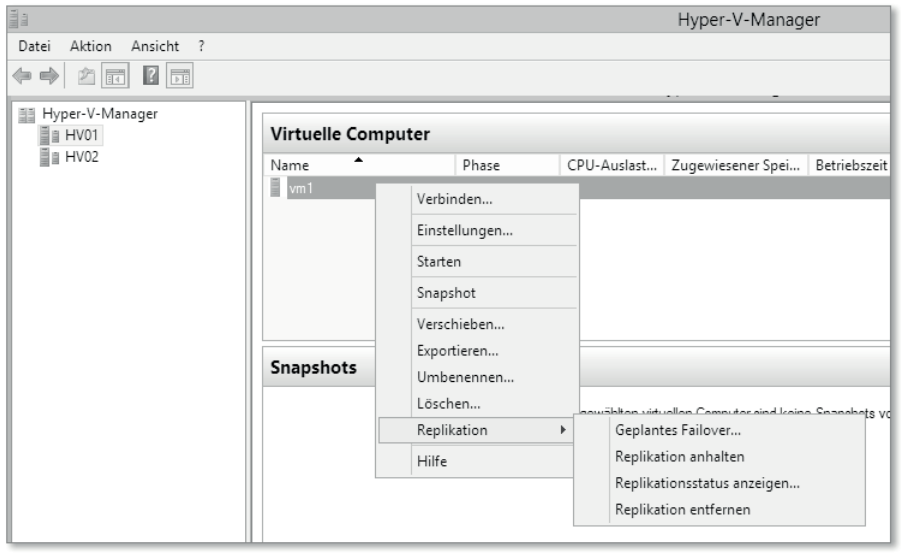


Abbildung 4.81 Sie verwalten die VM-Replikation über das Kontextmenü oder die Aktionen im Hyper-V-Manager.

Außerdem zeigt die Registerkarte REPLIKATION alle Informationen über die konfigurierte VM-Replikation (siehe Abbildung 4.82).

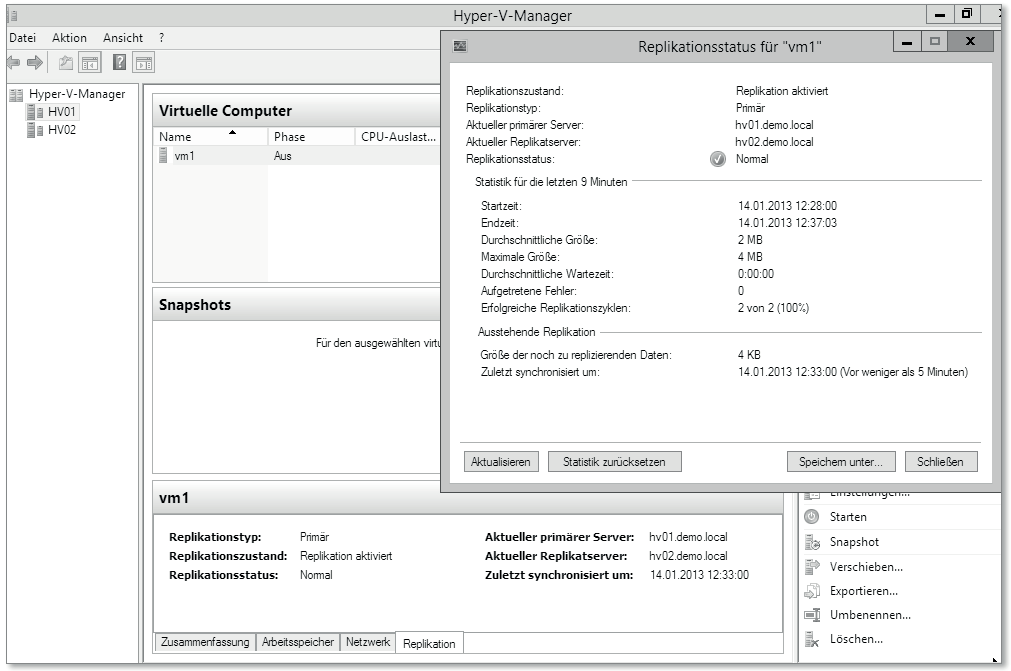


Abbildung 4.82 Der Replikationsstatus für eine virtuelle Maschine bietet einen detaillierten Überblick über die Replikation.

4.7.4 VMs konfigurieren

Mit dem Aktivieren der VM-Replikation erhält die virtuelle Maschine zusätzliche Einstellungen, um die Besonderheiten der Replikation und das Failover in das sekundäre Rechenzentrum widerzuspiegeln.

Jede Netzwerkkarte wird um einen Eintrag FAILOVER-TCP/IP erweitert (siehe Abbildung 4.83). Dieser dient dazu, eine alternative Netzwerkkonfiguration für IPv4 und IPv6 zu definieren, die im sekundären Rechenzentrum verwendet wird, sobald die virtuelle Maschine dort hochgefahren wird. Dadurch kann die VM-Replikation auch dann eingesetzt werden, wenn das Netzwerksegment der virtuellen Maschine im primären Rechenzentrum nicht im sekundären Rechenzentrum verfügbar ist.

In der PowerShell nutzen Sie die Kommandos `Get-VMNetworkAdapterFailoverConfiguration` und `Set-VMNetworkAdapterFailoverConfiguration`.

Kommen dynamische IP-Adressen zum Einsatz, können Sie diese Einstellungen ignorieren, da sie nur für die Anpassung statischer IP-Adressen verwendet werden.

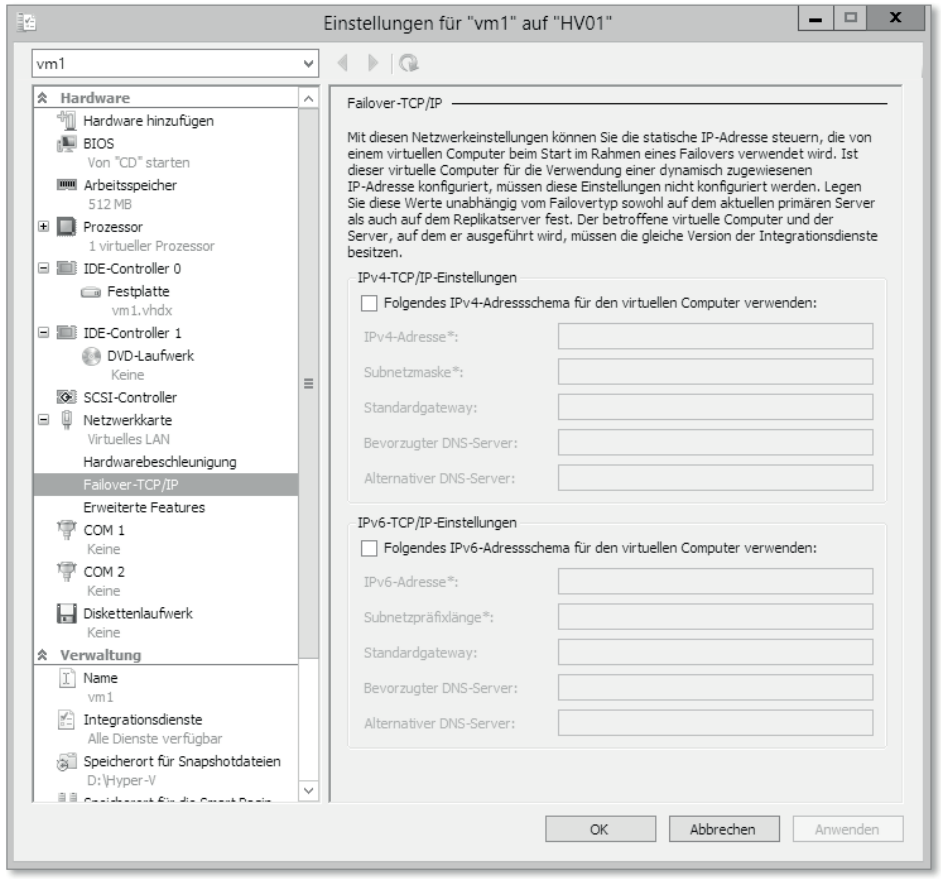


Abbildung 4.83 Die Konfiguration von TCP/IP-Einstellungen für den Failover-Fall stellt sicher, dass die virtuelle Maschine im Zielnetz mit der Außenwelt kommunizieren kann.

Unterhalb des Punktes REPLIKATION können Sie fast alle Einstellungen der VM-Replikation ändern, falls sich an der Konfiguration der Umgebung etwas verändern sollte. So können Sie

- Authentifizierung und Kompression verändern (siehe Abbildung 4.84) sowie
- die Wiederherstellungspunkte neu definieren (siehe Abbildung 4.85 und Abschnitt 4.7.9).
- In der PowerShell nutzen Sie dafür `Get-VMReplication` und `Set-VMReplication`.

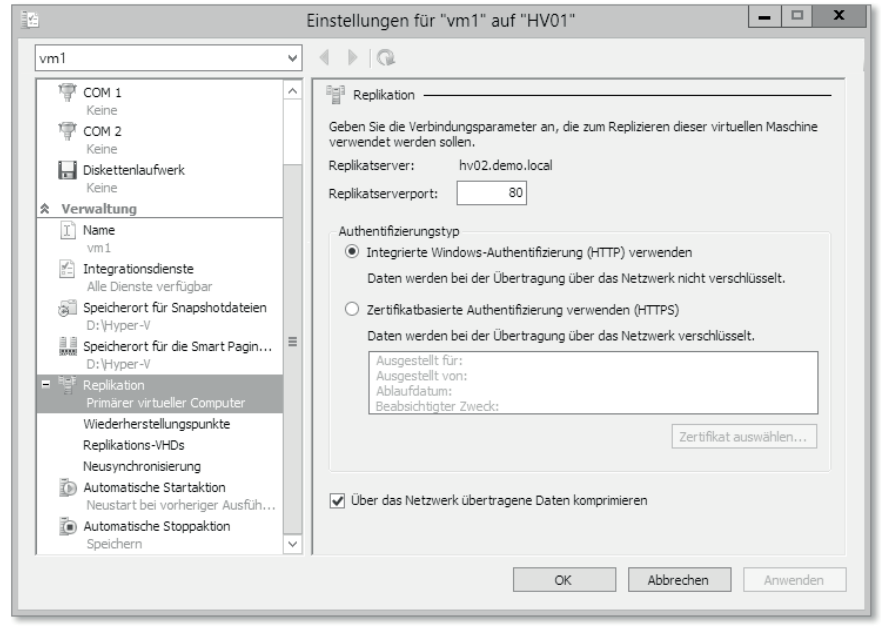


Abbildung 4.84 Die Verwendung der Kerberos-Authentifizierung ist innerhalb einer Domäne ohne zusätzlichen Aufwand möglich.

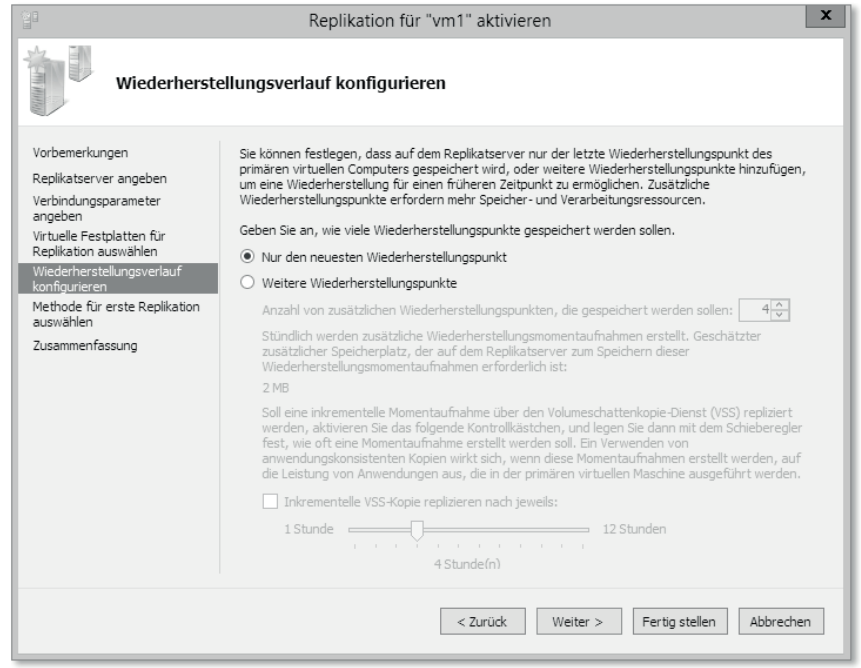


Abbildung 4.85 Sollten Sie feststellen, dass ein Wiederherstellungspunkt für die VM-Replikation nicht ausreicht, können Sie die Konfiguration nachträglich anpassen.

Eine Anpassung der replizierten virtuellen Festplatten ist im Nachhinein leider nicht möglich (siehe Replikations-VHDs in Abbildung 4.86). Es wird lediglich angezeigt, welche virtuellen Festplatten repliziert werden und welche nicht.

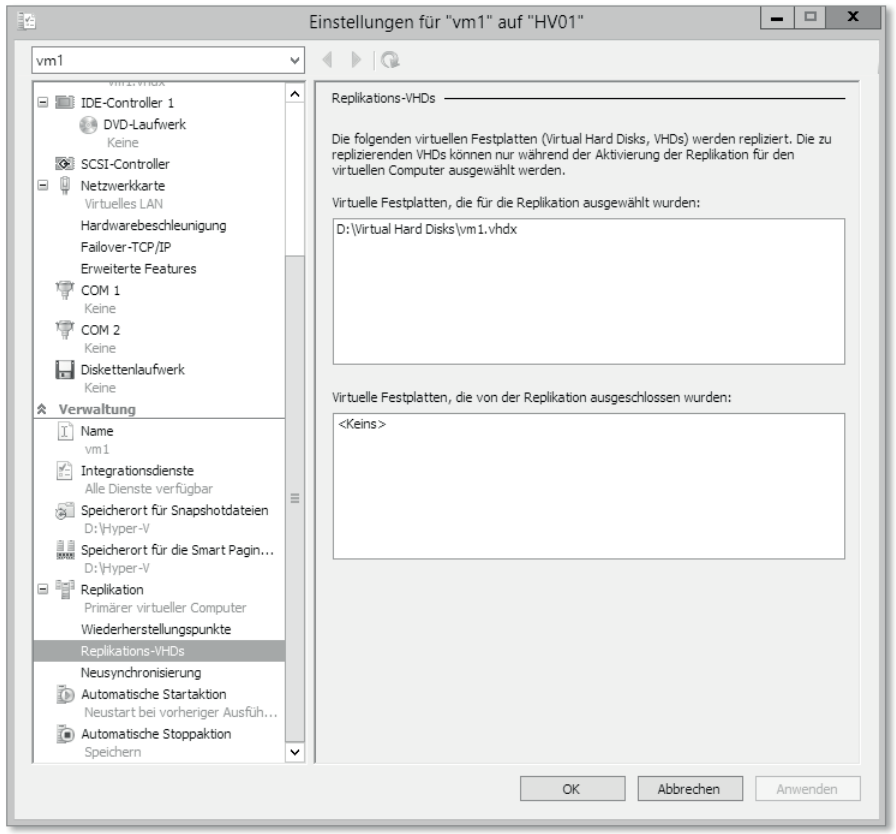


Abbildung 4.86 Die replizierten VHDs einer virtuellen Maschine werden angezeigt, können aber nicht mehr verändert werden, ohne die Replikation zu beenden und neu einzurichten.

Sollte für die virtuelle Maschine eine erneute Synchronisation notwendig werden, können Sie diese unterhalb von Neusynchronisierung konfigurieren (siehe Abbildung 4.87).

Beachten Sie dabei die Belastung der Prozessoren des Hyper-V-Hosts für die Kompression sowie die Belastung des Netzwerks für die Übertragung zum Replikat-Server.

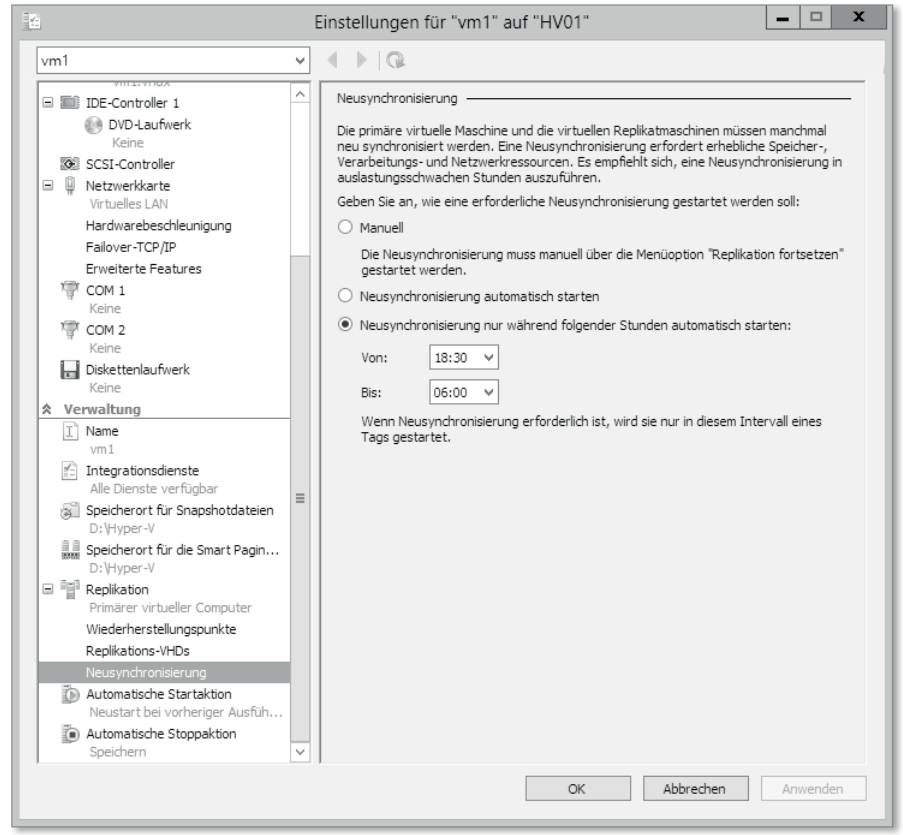


Abbildung 4.87 Sollte eine Neukonfiguration notwendig sein, wird diese anhand der hier konfigurierten Einstellungen durchgeführt.

4.7.5 Das Replikat

Das Replikat erscheint im sekundären Rechenzentrum als heruntergefahrene virtuelle Maschine mit demselben Namen wie das Original. Auf der Registerkarte Replikation (siehe Abbildung 4.88) informiert Hyper-V Sie unter anderem darüber, dass es sich um das Replikat handelt, und von welchem Hyper-V-Host die Replikation durchgeführt wird.

Den Versuch, das Replikat zu starten, anstatt ein Failover durchzuführen, quittiert Hyper-V mit der folgenden Fehlermeldung und schützt Sie damit vor dem versehentlichen Hochfahren des Replikats:

> *Fehler beim Versuch, die ausgewählten virtuellen Computer zu starten.*
> *Fehler beim Starten von »vm1«.*
> *Der Start des virtuellen Computers wurde verhindert, da eine Replikation ausgeführt wird.*

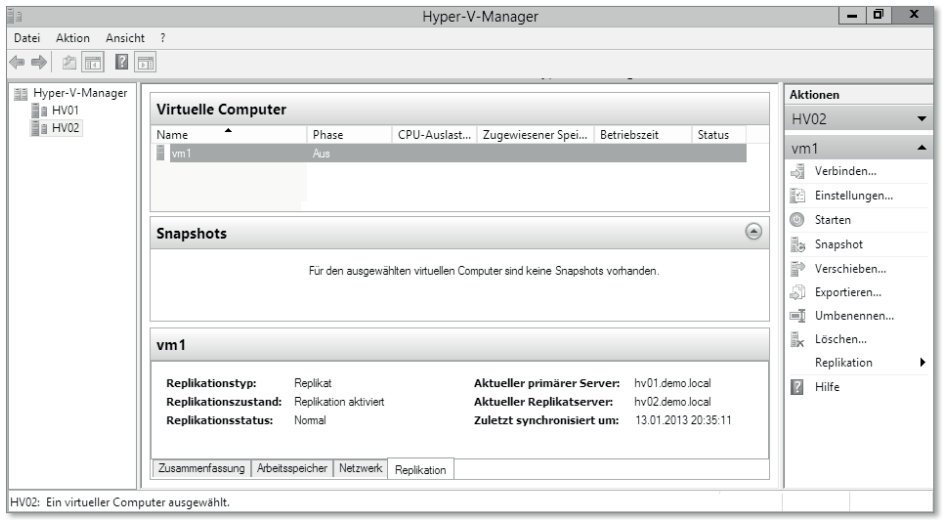


Abbildung 4.88 Der Replikat-Server zeigt an, dass es sich bei der virtuellen Maschine um ein Replikat handelt.

Den Replikationsstatus erreichen Sie über das Kontextmenü der virtuellen Maschine oder die Aufgaben auf der rechten Seite des Hyper-V-Managers unter dem Eintrag Replikation. So erhalten Sie einen detaillierten Überblick über die konfigurierte Replikation (siehe Abbildung 4.89). Dies können Sie über die PowerShell auch mit `Measure-VMReplication`, `Reset-VMReplicationStatistics` und `Test-VMReplication-Connection` erreichen.

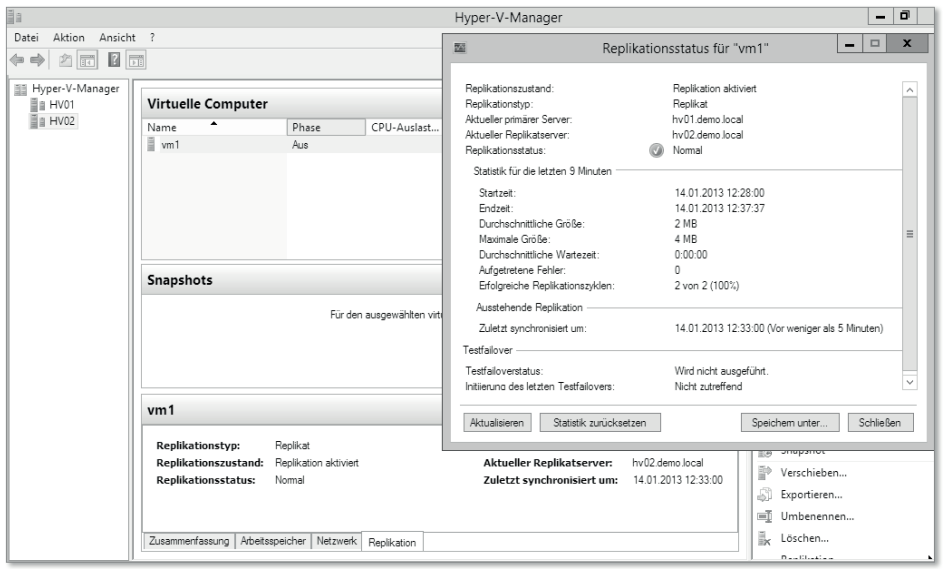


Abbildung 4.89 Auch der Replikat-Server zeigt den detaillierten Replikationsstatus an.

4.7.6 Replizierte VMs testen

Mit der Verwendung einer Notfalllösung geht die Verantwortung einher, die Funktionsfähigkeit regelmäßig zu überprüfen. Dazu bietet die VM-Replikation die Möglichkeit des Testfailovers an (siehe Abbildung 4.90). Als Erstes muss dafür der gewünschte Wiederherstellungspunkt ausgewählt werden (siehe Abbildung 4.91). Mit der PowerShell erreichen Sie dies über Start-`VMFailover` und `Stop-VMFailover`.

Mehr über Wiederherstellungspunkte finden Sie in Abschnitt 4.7.9.

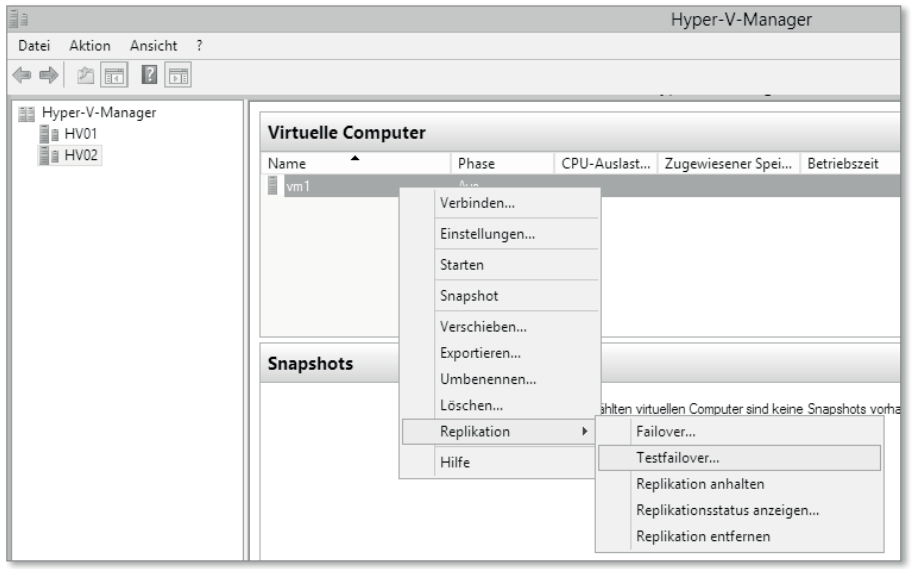


Abbildung 4.90 Der Testfailover wird über das Kontextmenü oder die Aktionen im Hyper-V-Manager ausgelöst.

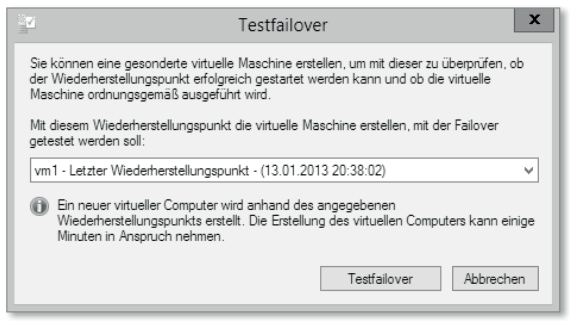


Abbildung 4.91 Der Testfailover wird anhand eines bestimmten Wiederherstellungspunktes durchgeführt.

Auf der Basis dieses Wiederherstellungspunktes wird eine neue virtuelle Maschine erstellt (siehe Abbildung 4.92), die als Testreplikat markiert wird und den Namen der

ursprünglichen virtuellen Maschine mit angehängtem »Test« trägt. Diese Maschine ist identisch mit dem Replikat konfiguriert, wurde aber vom Netzwerk getrennt, indem für alle Netzwerkkarten der virtuelle Switch auf NICHT VERBUNDEN gestellt wurde (siehe Abbildung 4.93).

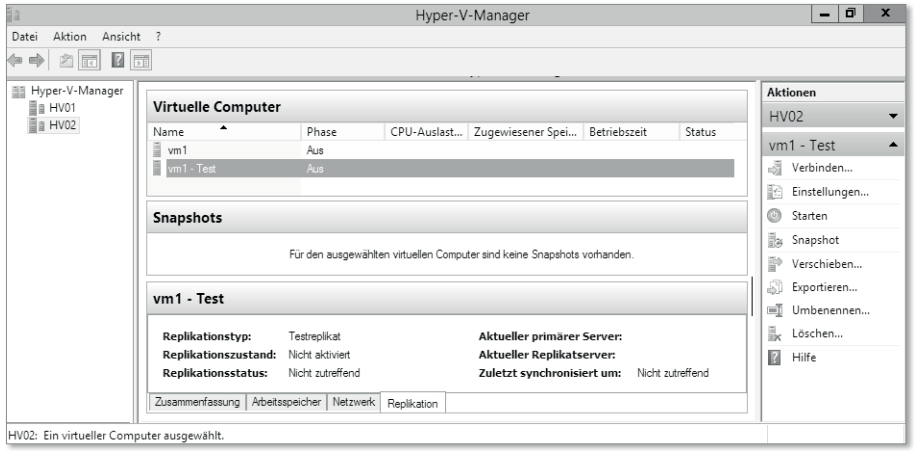


Abbildung 4.92 Auf dem Replikat-Server wird eine neue virtuelle Maschine für den Failovertest angelegt.

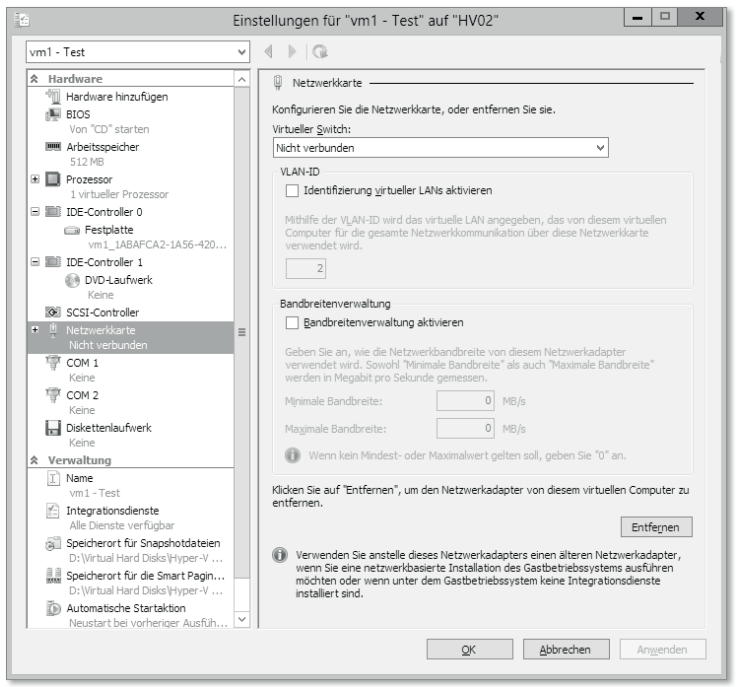


Abbildung 4.93 Die Netzwerkverbindungen der virtuellen Maschine für den Failovertest werden beim Anlegen getrennt, um den Betrieb der primären Kopie nicht zu gefährden.

Mithilfe dieses Testreplikats kann ein rudimentärer Funktionstest der virtuellen Maschine vorgenommen werden, ohne dass die Ausführung der primären virtuellen Maschine unterbrochen oder beeinträchtigt wird.

Sollte der Funktionstest die Verbindung zu Backend-Systemen erfordern, ist größte Vorsicht geboten, da eine aktive Netzwerkverbindung zum Produktionsnetzwerk den Betrieb der primären virtuellen Maschine beeinträchtigen kann. Dies kann durch doppelte Computernamen, identische Netzwerkkonfiguration, doppelte Security Identifier (SID) oder anwendungsbezogene Konflikte verursacht werden.

4.7.7 Geplantes Failover

Im Rahmen von regelmäßigen Notfalltests sollten Sie das Failover der replizierten virtuellen Maschinen überprüfen. Dazu bietet Hyper-V die Möglichkeit, ein GEPLANTES FAILOVER über die Aktionen einer virtuellen Maschine durchzuführen (siehe Abbildung 4.94).

Bevor Sie ein geplantes Failover vornehmen dürfen, müssen Sie die betroffene virtuelle Maschine herunterfahren. Anderenfalls bricht der Vorgang mit einer Fehlermeldung ab, ohne dass eine Veränderung an der bestehenden Konfiguration vorgenommen wurde. Die Notwendigkeit, die virtuelle Maschine auf dem primären Hyper-V-Host herunterzufahren, hat zur Folge, dass sich eine kurze Ausfallzeit ergibt.

Das geplante Failover wird durch einen Dialog begleitet, der Sie über die notwendigen Teilschritte und deren Status informiert (siehe Abbildung 4.96). Vor dem Auslösen des Failovers haben Sie die Wahl, ob die virtuelle Maschine anschließend sofort gestartet werden soll. Abhängig von der Auswahl, quittiert Hyper-V den erfolgreichen Vorgang entweder mit der Information, dass die virtuelle Maschine gestartet wurde oder dass die primäre Kopie nun auf dem Ziel-Host gestartet werden kann.

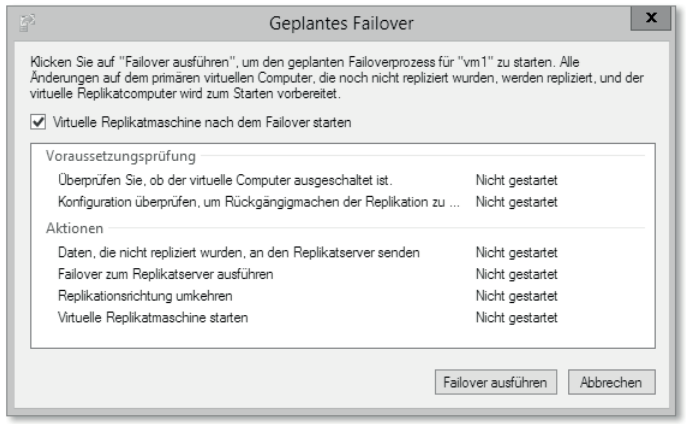


Abbildung 4.94 Der Fortschritt des geplanten Failovers wird detailliert angezeigt.

Mit dem Auslösen des geplanten Failovers führt Hyper-V einen letzten Abgleich der virtuellen Maschine mit dem Replikat durch und übergibt dann die Ausführung an den Replikat-Server. Gleichzeitig wird die Replikation umgekehrt, sodass die virtuelle Maschine wieder durch die VM-Replikation abgesichert ist.

4.7.8 Das Replikat in Betrieb nehmen

Schlägt die Replikation fehl, meldet der primäre Hyper-V-Host dies mit zwei Einträgen in der Ereignisanzeige. Diese Ereignisse werden unterhalb von Anwendungs- und Dienstprotokolle • Microsoft • Windows • Hyper-V-VMMS • Admin angezeigt. Es handelt sich dabei um die Ereignis-IDs 29292 und 32315 mit der Quelle Hyper-V-VMMS.

Der Fehler mit der Ereignis-ID 29292 informiert Sie darüber, dass die Replikation nicht möglich gewesen ist, und nennt dabei die betroffene virtuelle Maschine, den beteiligten Hyper-V-Host und den Port für die Replikation:

> *Die Änderungen für den virtuellen Computer »vm1« konnten nicht repliziert werden, da der Replikatserver »hv02.demo.local« an Port »80« nicht erreichbar ist. Das Zeitlimit für den Vorgang wurde erreicht (0x00002EE2). (ID des virtuellen Computers: F2216DE3-7560-4469-91E8-9D4F54D8B251)*

Gleichzeitig wird eine Warnung mit der Ereignis-ID 32314 generiert, die Sie über das weitere Vorgehen des Hyper-V-Hosts in Kenntnis setzt:

> *Fehler beim Replizieren der Änderungen für den virtuellen Computer »vm1« mit der ID »F2216DE3-7560-4469-91E8-9D4F54D8B251«. Die Replikation wird nach 1 Minute wiederholt.*

Die Replikation wird dreimal nach einer Minute und einmal nach zwei Minuten wiederholt, sodass in den ersten fünf Minuten nach der fehlerhaften Replikation insgesamt vier erneute Versuche unternommen werden. Anschließend erfolgt ein Versuch der erneuten Replikation nach weiteren fünf Minuten, dann 20 Minuten und anschließend nur noch alle 30 Minuten.

In der Regel ist es ausreichend, den Fehler in der Kommunikation zwischen Hyper-V-Host und dem Replikat-Server zu beheben und dann die Replikation fortzusetzen (siehe Abbildung 4.95).

Unter Umständen kann es notwendig sein, dass eine erneute Synchronisation durchgeführt wird. Die darf nach der Vorgabe von Microsoft aber nur zwischen 18:30 und 06:00 Uhr durchgeführt werden.

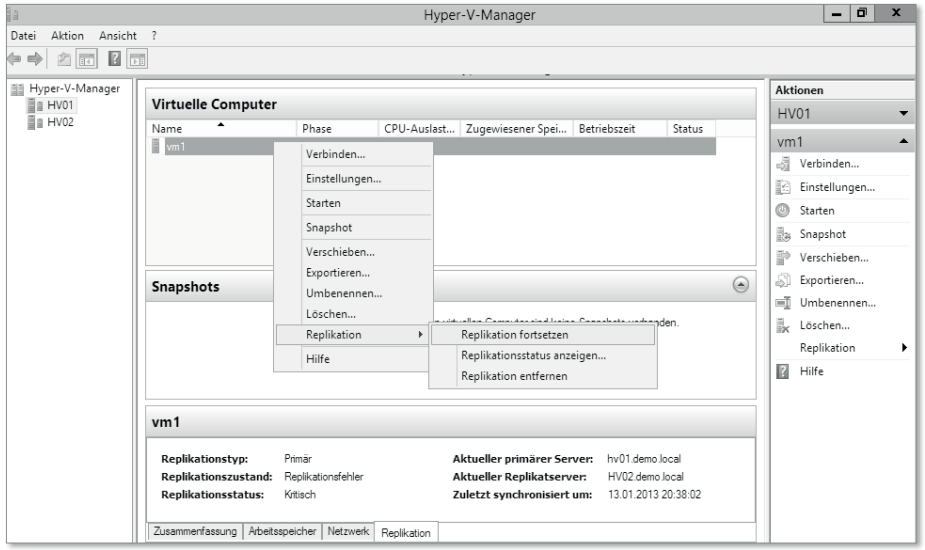


Abbildung 4.95 Fortsetzen der Replikation

Beide an der Replikation beteiligten Hyper-V-Hosts melden die verpassten Replikationszyklen im Replikationsstatus (siehe Abbildung 4.96). In beiden Fällen wechselt der Status nicht automatisch wieder in den Zustand Normal, sondern verbleibt auf Warnung. Die Ursache dafür liegt in der Statistik des Replikationsstatus, die erfolgreiche und fehlerhafte Replikationen zählt. Erst mit dem Zurücksetzen des Status mithilfe der Schaltfläche Statistik zurücksetzen (siehe Abbildung 4.96) erhalten Sie den fehlerfreien Status.

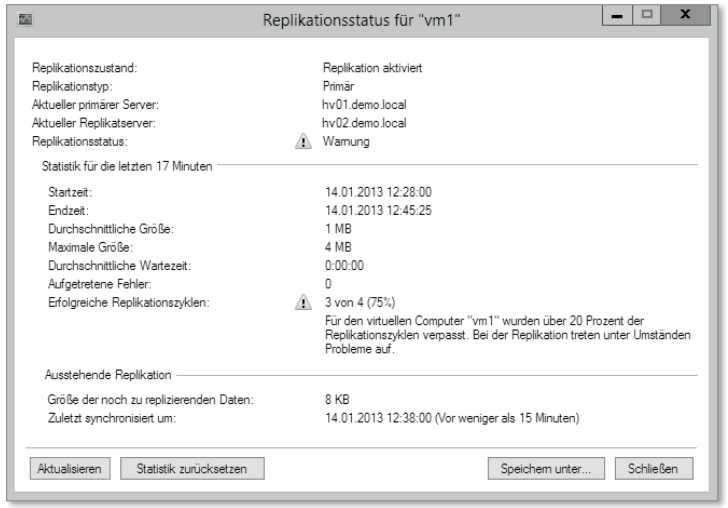


Abbildung 4.96 Werden Replikationszyklen aufgelassen, melden sowohl der primäre Server als auch der Replikat-Server Warnungen im Replikationsstatus.

Die Inbetriebnahme des Replikats erreichen Sie entweder über das Kontextmenü der virtuellen Maschine oder in den Aktionen des Hyper-V-Managers. Jeweils steht unterhalb des Eintrags Replikation der Befehl Failover zur Verfügung. Der Ablauf des Failovers ist ähnlich wie beim geplanten Failover (siehe Abschnitt 4.7.7). Sie werden ebenfalls aufgefordert, einen der vorhandenen Wiederherstellungspunkte zu wählen. Im Rahmen des Failovers werden alle anderen Wiederherstellungspunkte entfernt. Im Gegensatz zum geplanten Failover wird die Replikationsbeziehung nicht umgekehrt.

4.7.9 Wiederherstellungspunkte

Der Assistent für die VM-Replikation sieht vor, dass nur ein Wiederherstellungspunkt zum Replikat-Server übertragen und dort vorgehalten wird. Das bedeutet, dass immer nur der Stand vorhanden ist, der im fünfminütigen Intervall übertragen wird.

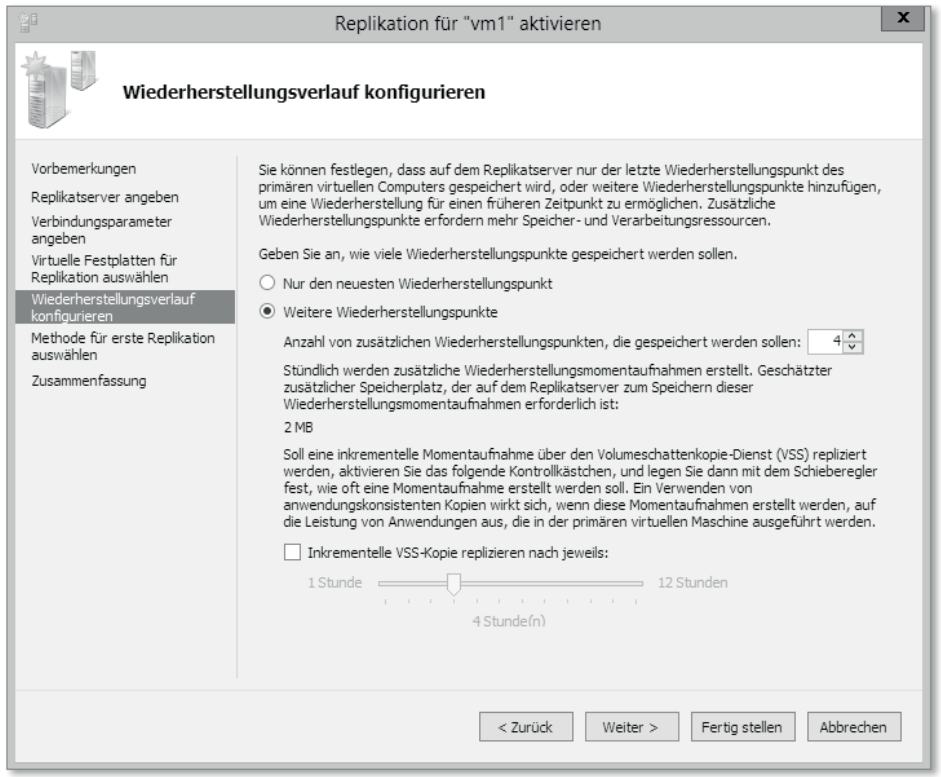


Abbildung 4.97 Mithilfe mehrerer Wiederherstellungspunkte können Sie zu unterschiedlichen Zuständen zurückkehren.

Abhängig von dem Dienst, den Sie in der betroffenen virtuellen Maschine betreiben, kann es sinnvoll sein, mehr Wiederherstellungspunkte zu konfigurieren. In Abbildung 4.97 sehen Sie die Konfiguration von vier Wiederherstellungspunkten, die im Abstand von einer Stunde gespeichert werden. Sie haben dadurch stets die Möglichkeit, zu einem von vier älteren Zuständen zurückzukehren.

Schalten Sie die inkrementelle VSS-Kopie ein, damit zusätzlich zu den konfigurierten Wiederherstellungspunkten eine Momentaufnahme mithilfe der Schattenkopien erzeugt und zum Replikat-Server übertragen wird.

4.7.10 Neuerungen in Windows Server 2012 R2

Mit Windows Server 2012 R2 werden mehrere Verbesserungen für die VM-Replikation eingeführt, wodurch dieses Feature noch mehr Szenarien abdecken kann.

Während Windows Server 2012 ein fest eingestelltes Replikationsintervall von fünf Minuten mitbrachte, lässt sich das Intervall nun in drei Schritten konfigurieren (siehe Abbildung 4.98). Mit 30 Sekunden wird eine höhere Frequenz erreicht, wodurch die Aktualität des Replikats steigt. Es wird allerdings auch eine höhere Netzwerkbelastung verursacht. Stellt die Bandbreite im Netzwerk die größere Herausforderung dar, lässt sich das Intervall auf 15 Minuten verlängern.

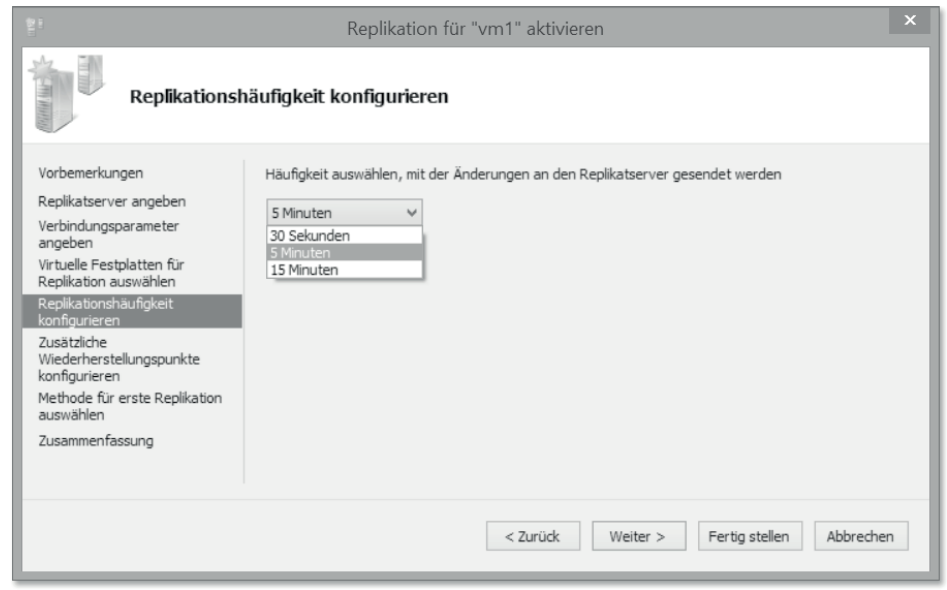


Abbildung 4.98 Das Replikationsintervall lässt sich nun auf 30 Sekunden, fünf Minuten und 15 Minuten konfigurieren.

In Windows Server 2012 R2 wird die maximale Anzahl von Wiederherstellungspunkten auf 24 erhöht (siehe Abbildung 4.99).

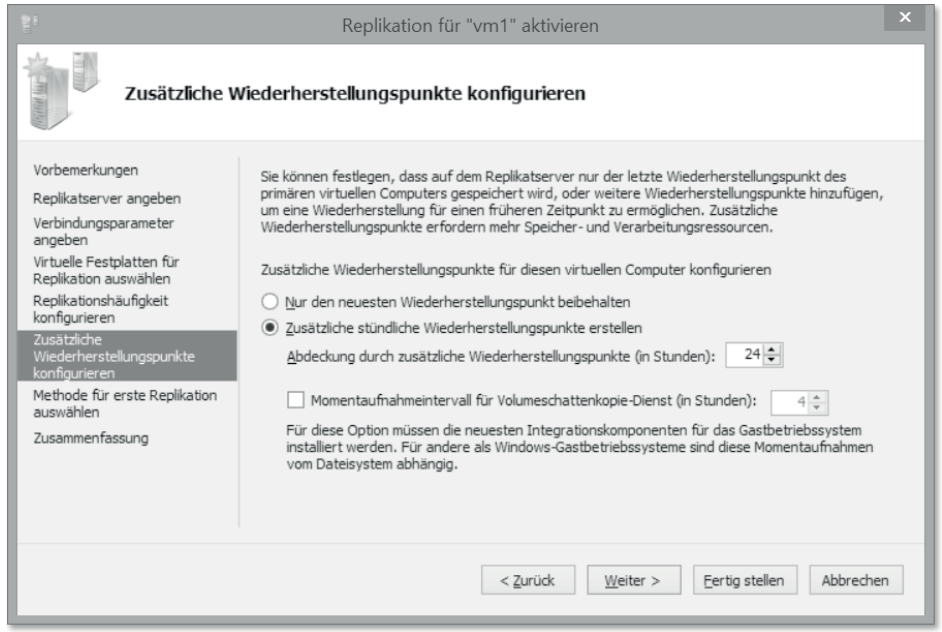


Abbildung 4.99 Die maximale Anzahl von Wiederherstellungspunkten beträgt nun 24.

Zusätzlich führt Windows Server 2012 R2 nun eine zweistufige Replikation ein, sodass ein Replikat auf einen dritten Server repliziert werden kann (siehe Abbildung 4.100). Es ist vorstellbar, dass eine virtuelle Maschine mit diesem Mechanismus zuerst in einen separaten Brandabschnitt in demselben Rechenzentrum übertragen wird und von dort weiter in ein zweites Rechenzentrum repliziert wird. Beachten Sie, dass eine virtuelle Maschine nicht gleichzeitig auf zwei Replikat-Server übertragen werden kann!

Hyper-V Recovery Manager

Microsoft hat zwischenzeitlich auch den Hyper-V Recovery Manager (HRM) als Dienst in Windows Azure eingeführt. Dabei handelt es sich um die Möglichkeit, die VM-Replikation zwischen den eigenen Rechenzentren zu orchestrieren und zu überwachen. Die Replikation virtueller Maschinen von und nach Windows Azure ist dabei explizit ausgeschlossen.

Lesen Sie mehr darüber in der offiziellen Ankündigung (*http://blogs.technet.com/b/scvmm/archive/2013/10/21/announcing-paid-preview-of-windows-azure-hyper-v-recovery-manager.aspx*, Kurzlink: *http://qccq.de/s/h413*) und bei dem Virtual-Machine-MVP Benedict Berger (*http://blog.benedict-berger.de/2013/12/07/hyper-v-recovery-manager*, Kurzlink: *http://qccq.de/s/h414*).

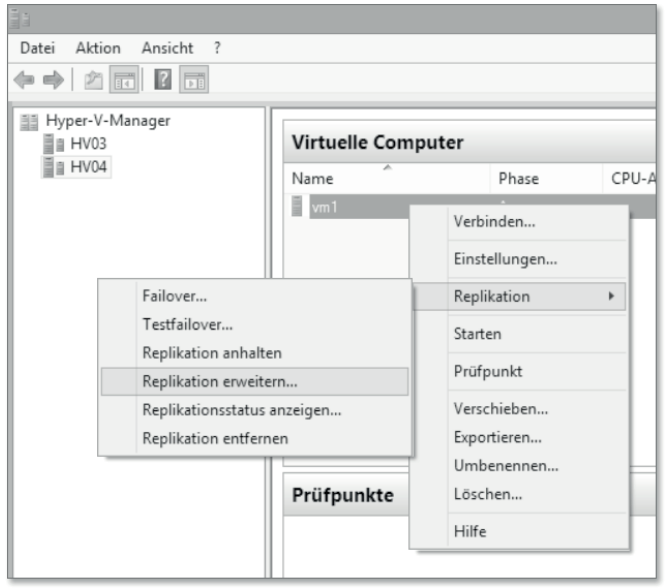


Abbildung 4.100 Die VM-Replikation erlaubt nun die Übertragung eines Replikats auf einen dritten Hyper-V-Host.

Neben diesen wichtigen Verbesserungen der VM-Replikation wurden auch kleine Veränderungen vorgenommen. Die Belastung der Hyper-V-Hosts wurde verringert, da anstatt von Prüfpunkten nun Undo-Logs eingesetzt werden. Die VM-Replikation lässt sich nun auch für Linux-VMs einsetzen. Außerdem funktioniert die Größenveränderung von VHDX-Dateien im laufenden Betrieb (Online VHDX Resize).

4.8 Zusammenfassung

Dieses Kapitel hat Ihnen viele wichtige Informationen für die Einrichtung von hochverfügbaren Hyper-V-Umgebungen mithilfe der Failover-Cluster-Funktionen in Windows Server 2012 vermittelt. Es ist zudem im Detail auf die Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung eingegangen und hat aufgezeigt, wie Sie mit der Funktion Hyper-V Replica für eine Ausfallsicherheit von virtuellen Maschinen ohne eine Cluster-Umgebung sorgen können. Nach intensivem Studium dieses Kapitels sollten Sie jetzt erfolgreich eine eigene Hochverfügbarkeitslösung in Ihrem Unternehmen implementieren können.

Inhalt

3 Den Host-Server einrichten 111

5 Virtuelle Maschinen 431

9 Remotedesktopdienste 871

10 Finale und Ausblick 931

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

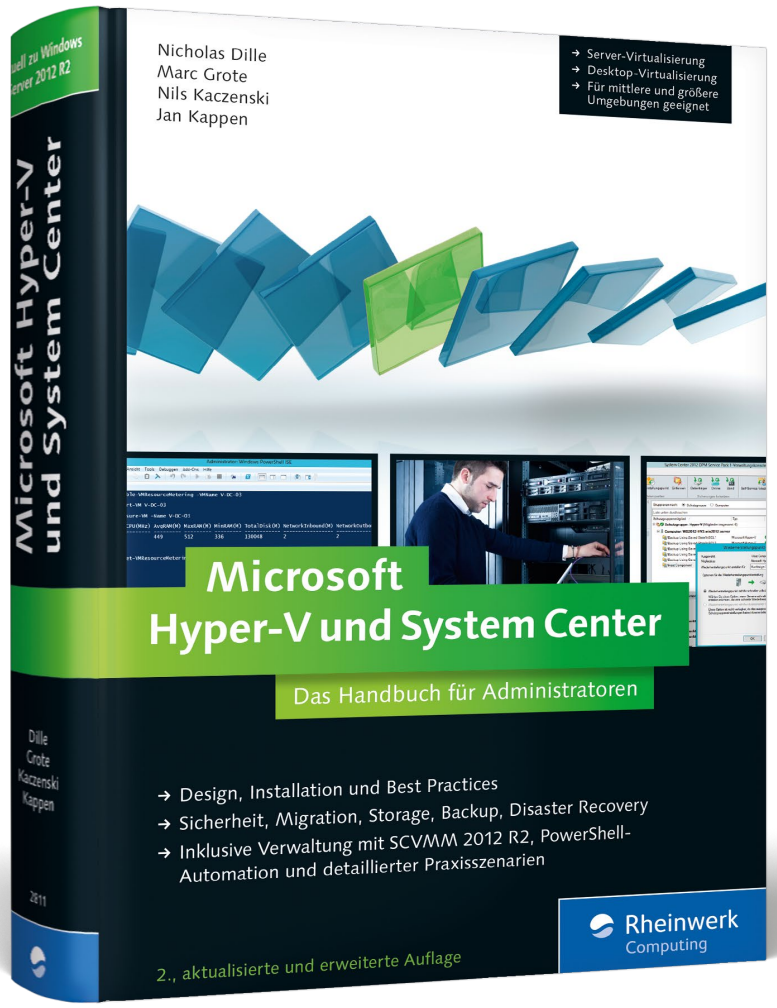
U

V

W

X

Z



Nicholas Dille, Marc Grote, Nils Kaczenski, Jan Kappen

Microsoft Hyper-V und System Center

967 Seiten, gebunden, 2. Auflage 2014
69,90 Euro, ISBN 978-3-8362-2811-4

www.rheinwerk-verlag.de/3570

Nicholas Dille beschäftigt sich seit 10 Jahren mit Zentralisierung, Server-Based Computing und Thin Clients und arbeitet seit über 8 Jahren als IT-Architekt für die sepago GmbH. In Großprojekten konnte er viele weltweit vertretene Konzerne in der Weiterentwicklung der IT-Strategie beraten und technische Konzepte für die Umsetzung verfassen. Seit 2010 ist er MVP.

Marc Grote ist seit 24 Jahren im professionellen IT-Bereich als selbstständiger Consultant und Trainer mit den Schwerpunkten Forefront TMG und UAG, Windows Server mit Schwerpunkt Sicherheit, PKI und Hochverfügbarkeit sowie System Center und Exchange Server tätig. Des Weiteren ist er Fachautor für Windows- und Forefront-Themen und Sprecher auf Konferenzen und Community-Veranstaltungen. Seit 2003 ist er MVP.

Nils Kaczenski ist seit Mitte der 1990er-Jahre als Consultant für Windows-Netzwerke tätig und berät Firmen und Administratoren in technischen und strategischen Fragen. Er wird von Microsoft seit 2003 regelmäßig als Most Valuable Professional (MVP) in der Sparte Directory Services ausgezeichnet.

Jan Kappen arbeitet bei der Rachfahl IT-Solutions und ist dort als Fachexperte für Hyper-V, Windows Server sowie Microsoft Exchange zuständig. Jan betreibt mit Carsten Rachfahl den Blog Hyper-V-Server.de, einen der größten Blogs im deutschsprachigen Raum, der sich exklusiv mit der Virtualisierungslösung aus dem Hause Microsoft beschäftigt.