Kapitel 2
vSphere-Architektur

Dieses Kapitel beschäftigt sich mit dem strukturellen Aufbau einer virtuellen Infrastruktur. Wir gehen den Fragen nach, welche Elemente dazugehören, wie sie ineinandergreifen und wie sie aufgebaut sind.
Autor dieses Kapitels ist Bertram Wöhrmann, Ligarion.
buch@ligarion.de

Mit der Version vSphere 7 und deren Neuerungen geht VMware ganz konsequent den Weg weiter zum *Software-Defined Datacenter* (SDDC). Die Abstrahierung von Storage wird immer weiter ausgebaut. Im Bereich des Netzwerks hat NSX seinen Platz gefunden (hier werden Switches, Router und Firewalls virtualisiert), und mit *VMware SD-WAN by VeloCloud* (Virtualisierung von WAN-Anbindungen) wird der Produkt-Stack noch ausgebaut. VMware entwickelt den Stack immer weiter und versucht so, das SDDC zu komplettieren.

Das ist aber nur ein Teil des Software-Stacks für das SDDC. Für einen effektiven Betrieb ist es möglich bzw. notwendig, weitere Softwarekomponenten zu nutzen.

Viele Themen reißen wir in diesem Kapitel nur kurz an. Wir denken, dass es sinnvoller ist, die detaillierten Erklärungen direkt in demjenigen Abschnitt auszuführen, in dem wir auch die passende Komponente beschreiben.

2.1 Infrastrukturbestandteile eines Software-Defined Datacenter (SDDC)

Die Infrastruktur eines Software-Defined Datacenter bietet nicht nur Komponenten zum Virtualisieren von Betriebssystemen (vSphere-Server). Hinzu kommen Komponenten für das Management der Infrastruktur, und da bildet der *vCenter Server* mit dem *Lifecycle Manager* nur den bekannten Anfang. Des Weiteren werden Komponenten für die Virtualisierung des Netzwerks (NSX) benötigt, genauso wie Komponenten für die Virtualisierung des Storages (vSAN).

Zum gesamten VMware-Design eines SDDC gehören noch Komponenten zur Automatisierung, nämlich *vRealize Automation* und der *Orchestrator*. Bei der Fehleranalyse werden Sie von *vRealize Operations* und *vRealize Log Insight* unterstützt. Als letztes Glied in der Kette wird *vRealize Business for Cloud* zur Nutzungsmessung und Kostenanalyse genutzt.

Wenn Sie es sich leicht machen wollen, arbeiten Sie mit dem Stack *VMware Cloud Foundation*. Hierbei handelt es sich um die Zusammenfassung aller Komponenten des SDDC in einem Software-Stack. Mehr dazu können Sie in Kapitel 22 lesen.

2.2 vSphere-Host

Der physische Server, der seine Ressourcen – wie CPU, Hauptspeicher (RAM), Netzwerkkarten und Festplattenspeicher – über eine Virtualisierungsschicht (Hypervisor) den virtuellen Maschinen zur Verfügung stellt, ist der *vSphere-Host* (siehe Abbildung 2.1).

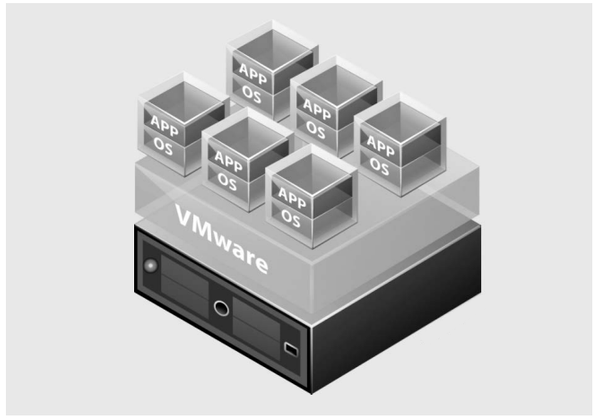


Abbildung 2.1 vSphere-Host-Struktur

2.2.1 Hardware

Ursprünglich kamen als Prozessorbasis für den Einsatz von VMware vSphere nur 64-Bit-x86-Prozessoren zum Einsatz. Auf anderen CPUs war das System nicht lauffähig, da der VMkernel einen 64-Bit-Kernel besitzt. Mit vSphere 7 hat sich das geändert. Eine Unterstützung von ARM-Prozessoren ist jetzt inkludiert. Das gilt auch für ARM-basierte Erweiterungskarten.

Für die Installation benötigen Sie mindestens eine CPU mit zwei Cores. Der minimale Arbeitsspeicherbedarf hat sich auf 4 GB erhöht, wobei VMware angibt, dass 8 GB Memory benötigt werden, um alle Funktionen nutzen zu können. Des Weiteren ist ein unterstützter Storage-Controller erforderlich. Möglich sind SCSI, SAS, SATA und Fibre-Channel. Abschließend wird noch mindestens eine Netzwerkkarte benötigt, damit Sie auf das System zugreifen können. Im Normalfall werden aber wohl mehrere Netzwerkports zum Einsatz kommen.

Intel VT-x und AMD-V/RVI

Alle Prozessoren, für die VMware Support anbietet, müssen eine Erweiterung zur Unterstützung von Virtualisierungstechnologien aufweisen. Durch diese Technologien wird im Wesentlichen der *Virtual Machine Monitor* (VMM) in seiner Arbeit unterstützt. Dadurch reduziert sich der Overhead. Auch der Prozess der Migration einer aktiven virtuellen Maschine zwischen verschiedenen Prozessorgenerationen wird erleichtert.

Die unterstützten CPUs von Intel, AMD und ARM bringen eine solche Technologie mit.

2.2.2 Hardware Compatibility List (HCL)

Wie andere Betriebssystemhersteller bzw. Hersteller von Hypervisoren pflegt auch die Firma VMware eine *Hardware Compatibility List* (HCL). Vergewissern Sie sich, dass die Komponenten, die Sie einsetzen wollen, in dieser Liste aufgeführt sind. Sie müssen zwar keine Bedenken haben, dass ein nicht gelistetes System nicht funktionieren wird, aber Sie haben nur Support für Ihre Virtualisierungslandschaft, wenn Sie sich aus der Liste der unterstützten Hardware bedienen.

Die HCL finden Sie unter *https://www.vmware.com/resources/compatibility/search.php*.

2.3 Architektur eines vSphere-Hosts

Die Architektur eines vSphere-Hosts definiert sich mithilfe verschiedenen Kernkomponenten (siehe Abbildung 2.2). Auf diese wollen wir im Folgenden eingehen.

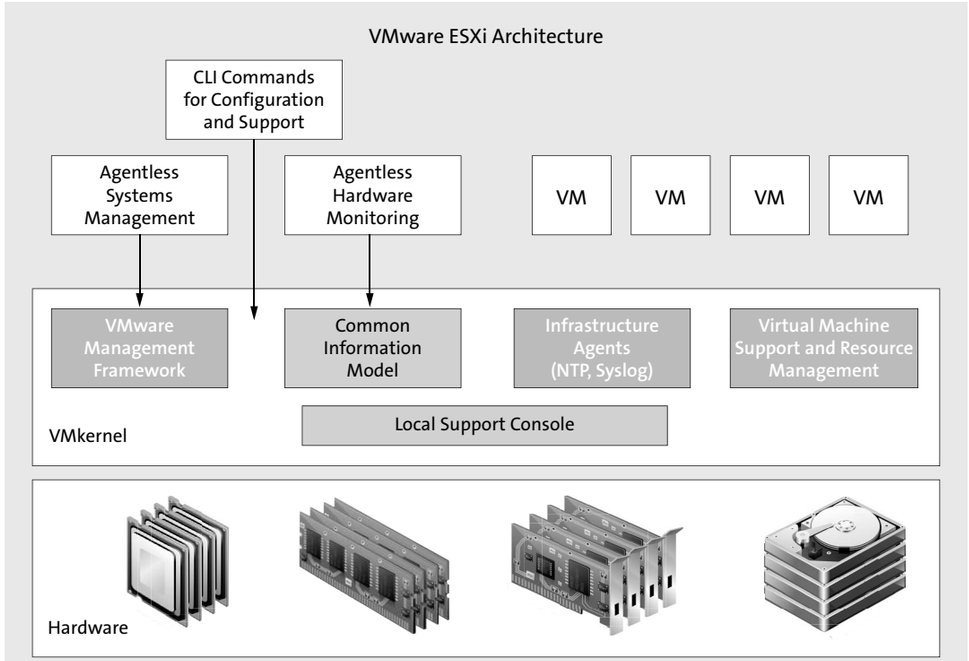


Abbildung 2.2 Struktur von VMware vSphere ESXi

VMkernel

Der VMkernel ist eine sehr schlanke Implementierung des Hypervisors. Er kontrolliert und verwaltet die meisten Ressourcen eines vSphere-ESXi-Servers. Die Regelung des Zugriffs auf

die Ressourcen CPU, Memory und Disk wird mithilfe eines Schedulers erreicht. Der Kernel hat neben einem TCP/IP-Stack zur Netzwerkkommunikation auch einen Storage-Stack für die Kommunikation mit Speichermedien. Der VMkernel ist eine Eigenentwicklung von VMware und nicht, wie viele meinen, ein Linux-Derivat.

Reliable Memory

Reliable Memory dient der Absicherung des Hypervisors zur Laufzeit. Um diese Funktion genau zu verstehen, sollten Sie wissen, dass der Hypervisor von VMware nach dem Booten für seine Funktion keine Festplatte mehr benötigt, weil der gesamte Hypervisor in den Arbeitsspeicher geladen wird. Aus diesem Grund ist es wichtig, dass der Bereich im Arbeitsspeicher, in dem die Software abgelegt wird, keine »Probleme« bereitet. Mit der Funktion *Reliable Memory* hat VMware eine Engine implementiert, die den Arbeitsspeicher scannt, um mögliche problematische Bereiche zu erkennen. Stellt sie Probleme fest, wird der Hypervisor dort nicht abgelegt. Die »nicht mehr optimalen« Speicherzellen werden vom Hypervisor gemieden, und er wird während der Laufzeit in anderen Bereichen abgelegt.

VMware Management Framework

Sie können das System ohne zusätzlich zu installierende Agents verwalten. Ob Sie direkt auf den Host zugreifen oder den Host über einen vCenter Server managen, ist Ihnen dabei vollkommen freigestellt.

Common Information Model (CIM)

Mit dem *Common Information Model* gibt es eine offene Schnittstelle zum Management von Hardwareressourcen. Damit Ihre zum Einsatz kommende Hardware komplett unterstützt wird, müssen die passenden Treiber in dem ESXi-Image enthalten sein. Das Standard-Image von VMware bietet lediglich eine allgemeine Unterstützung. Arbeitet Ihr Hardwareanbieter nicht mit dieser freien Implementierung, müssen Sie bei ihm nach einem herstellerspezifischen Image fragen.

Infrastructure Agents

Die implementierten Infrastrukturagenten sind für das Syslogging, das SNMP-Handling und die Zeitsynchronisation zuständig. Zusätzlich werden hier die lokalen User verwaltet.

Resource Management

Der *Resource Manager* partitioniert die Hardware, um den virtuellen Maschinen mithilfe eines Share-Mechanismus die Ressourcen zur Verfügung zu stellen. Dabei werden die Einstellungen zur Reservierung und zur Limitierung der Ressourcen CPU und Memory beachtet sowie die Shares aller *Core Four* (CPU, Memory, Network und Disk) berücksichtigt. Der Resource Manager wird als Teilprozess des VMkernels gestartet.

Virtual Machine Support

Der *Virtual Machine Support* ist für die Virtualisierung der CPU zuständig. Er gibt die CPU-Befehle der virtuellen Maschine an die physische Hardware weiter. Außerdem kümmert er sich um die Verwaltung der virtuellen Maschine nach deren Start.

Hardware Interface Layer

Der *Hardware Interface Layer* setzt die Hardwareanfragen der VM in die physische Adressierung um und ermöglicht so eine Adressierung der Ressourcen. Außerdem koordiniert er die Bereitstellung des VMFS (*Virtual Machine File System*) und der spezifischen Gerätetreiber. Er dient als Bindeglied zwischen dem VMkernel und der eigentlichen Serverhardware.

2.4 Grundlagen der CPU-Virtualisierung

Eine Emulation bildet Prozessoranfragen des Gasts über *Software* ab. Der Gast hat in diesem Fall keinen direkten Zugriff auf die CPU. Ein Virtualisierer leitet die Prozessoranfragen des Gasts direkt an die *Hardware* weiter.

VMware vSphere ist ein Virtualisierer. Unter vSphere wird die CPU einer virtuellen Maschine direkt vom Hostsystem abgeleitet und auch für bestimmte Arten von CPU-Instruktionen teilweise physisch verwendet. Aus diesem Grund sieht eine VM dieselbe CPU, wie sie im Host vorhanden ist (siehe Abbildung 2.3).

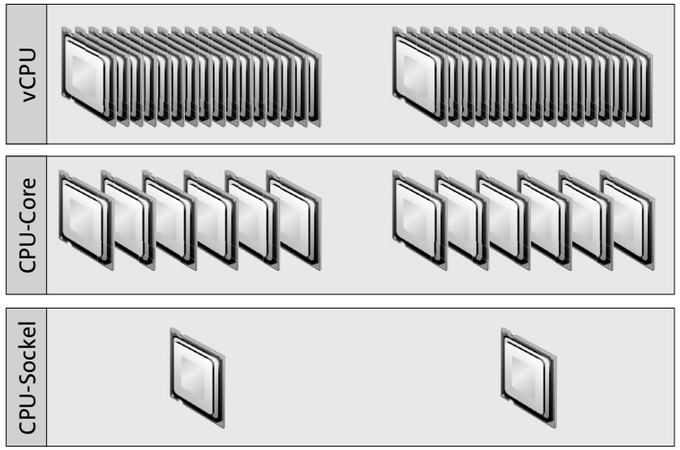


Abbildung 2.3 Zusammenhang zwischen physischen, logischen und virtuellen CPUs

Die virtuelle CPU einer VM kann CPU-Instruktionen in zwei verschiedenen Modi abarbeiten: im *Direct Execution Mode* und im *Virtualization Mode*. In den meisten Fällen werden die CPU-Instruktionen im Direct Execution Mode ausgeführt, der nahe an der Geschwindigkeit

der realen CPU liegt. Sollte der Befehl nicht in diesem Modus ausführbar sein, wird der Virtualization Mode verwendet. Eine virtualisierte CPU bedient sich so oft wie möglich der realen physischen CPU-Ressource, und die Virtualisierungsschicht greift nur bei der Ausführung von bestimmten CPU-Instruktionen ein.

Durch diese Umsetzung entsteht der oft erwähnte Virtualisierungs-Overhead, den wir näher in Abschnitt 2.5.2, »Memory-Overhead«, im Zusammenhang mit dem Arbeitsspeicher beschreiben.

Dazu sei als Hintergrund erwähnt, dass eine CPU grundsätzlich vier Privilegierungsstufen hat, sogenannte *Ringe* oder auch *Domains* (siehe Abbildung 2.4). Ring 0 hat die höchste Priorität. Hier liegt der Kernel Mode im x86 Umfeld wird er auch als *Supervisor Mode* bezeichnet, der manipulativ auf Hauptspeicher und Interrupts zugreifen darf. Auf dieser Stufe läuft normalerweise der Kernel des Betriebssystems, im Fall von VMware vSphere also der Hypervisor-VMkernel. In den Ringen 1 bis 3 liegt der User-Mode, wobei normalerweise lediglich Ring 3 genutzt wird. Es gibt nur wenige Applikationen, die direkt auf Ring 1 oder Ring 2 zugreifen.

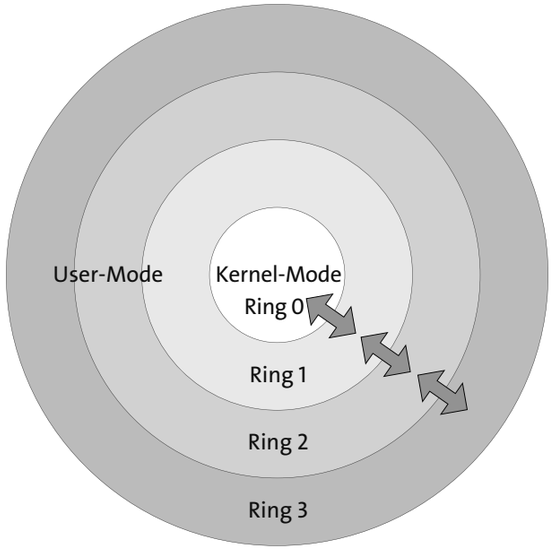


Abbildung 2.4 Ringstruktur der CPU

Bei einer virtuellen Maschine verhält sich das etwas anders: Die eigentlich an Ring 0 gestellten Anfragen des Betriebssystems werden an Ring 3 umgeleitet. Damit die Daten in Ring 1 bis 3 verarbeitet werden können, wird der physische Speicher in virtuelle Speicherseiten aufgeteilt. Der Memory-Controller (*Memory Management Unit*, MMU) übernimmt an dieser Stelle die Umsetzung von physischen Speicherinhalten in virtuelle. Damit der Programmcode auch richtig ausgeführt werden kann, enthält jede Speicherseite die Information dazu, auf welchem Ring der Code ausgeführt werden muss. Um zu verhindern, dass ein solch

komplexes System beeinflusst wird – z. B. durch Schadcode –, wurde das sogenannte *NX-Flag* kreiert (*No Execution Flag*). Diese Information hilft dem System, Daten von Programmcode zu unterscheiden. Der Mechanismus verhindert, dass Programmcode im Bereich der Daten ausgeführt werden kann.

Applikationen verwenden in der Regel den unprivilegierten Ring einer CPU, daher laufen diese Befehle im Direct Execution Mode. Wird hingegen eine Instruktion vom Betriebssystem ausgeführt, geschieht dies in der Regel modifizierend auf dem privilegierten Ring der CPU. Diese Anfragen werden von der Virtualisierungsschicht, dem VMM (*Virtual Machine Monitor*), abgefangen.

Dieser Managementaufwand wird als der *Virtualisierungs-Overhead* bezeichnet. Er hängt von der Arbeitslast der virtuellen CPU und der Menge der Aufrufe an den privilegierten Ring ab. Die Auswirkungen zeigen sich in verlängerten Laufzeiten der einzelnen Befehle und in einer erhöhten CPU-Last.

Die reale CPU wird an das Betriebssystem der VM durchgereicht. Aus diesem Grund sind dem Betriebssystem auch die Besonderheiten der eingesetzten CPU bekannt. Verschiedene Betriebssysteme nutzen diese CPU-spezifischen Befehle. Es kann auch sein, dass der Gast während der Installation auf diese Besonderheiten hin optimiert wurde. Das Verschieben einer solchen speziellen VM auf andere vSphere-Server mit unterschiedlichen CPUs – insbesondere beim Wechsel zwischen Intel- und AMD-Prozessoren – beeinträchtigt unter Umständen die Funktionalität des Betriebssystems bzw. der Applikation.

2.4.1 CPU-Affinität

Die *CPU-Affinität* (engl. *CPU Affinity*) bezeichnet eine Konfigurationsoption der virtuellen Maschine, und zwar die direkte Zuweisung einer physischen CPU bzw. eines Kerns. Diese Technik sollten Sie nur in Ausnahmefällen (z. B. zum Troubleshooting) verwenden, weil sie etliche Auswirkungen auf andere Bereiche der virtuellen Infrastruktur hat. Zum einen wird dadurch die CPU-Lastverteilung des ESXi-Servers außer Kraft gesetzt, zum anderen kollidiert diese CPU-Zuordnung mit eventuell vorgenommenen Einstellungen von CPU-Shares und CPU-Reservierung. Durch das Umgehen der CPU-Lastverteilung kann der Hypervisor den Forderungen seitens der VM eventuell nicht mehr nachkommen. Die mögliche Virtualisierungsquote und die Flexibilität reduzieren sich. Die Nutzung von vMotion ist durch die CPU-Affinität eingeschränkt, und *Distributed Resource Scheduling* verhindert diese sogar.

2.4.2 Hyperthreading

Der vSphere-Server unterstützt die Hyperthreading-Technologie von Intel. Diese bietet bei Nutzung von Ein-Sockel-Prozessoren ein auf Hardwareebene realisiertes Multithreading zur Verbesserung der CPU-Performance. Dabei kann ein physischer Core – im Intel-Wortgebrauch wird er als *Hyperthread* bezeichnet – gleichzeitig zwei Threads ausführen. Er verhält

sich mit aktiviertem Hyperthreading ähnlich wie zwei logische Cores. Sofern ein Betriebssystem und die darauf laufenden Applikationen mehrere CPUs nutzen können, sind hierdurch Geschwindigkeitsvorteile möglich. Dabei reicht die Performance nicht an eine Verdopplung heran, wie sie durch eine Dual-Core-VM erreicht würde. Ungeeignete Applikationen werden durch die Hyperthreading-Technologie unter Umständen auch verlangsamt, wenn sie zu viele der gemeinsam genutzten Ressourcen eines Cores verwenden.

Auf der Hardwareebene muss das Hyperthreading im BIOS aktiviert sein. Im Host ist Hyperthreading per Default aktiv; bei Bedarf deaktivieren Sie es über den Webclient im Tab CONFIGURE eines vSphere-Hosts unter SETTINGS • HARDWARE • OVERVIEW • PROCESSORS • EDIT HYPERTHREADING (siehe Abbildung 2.5).

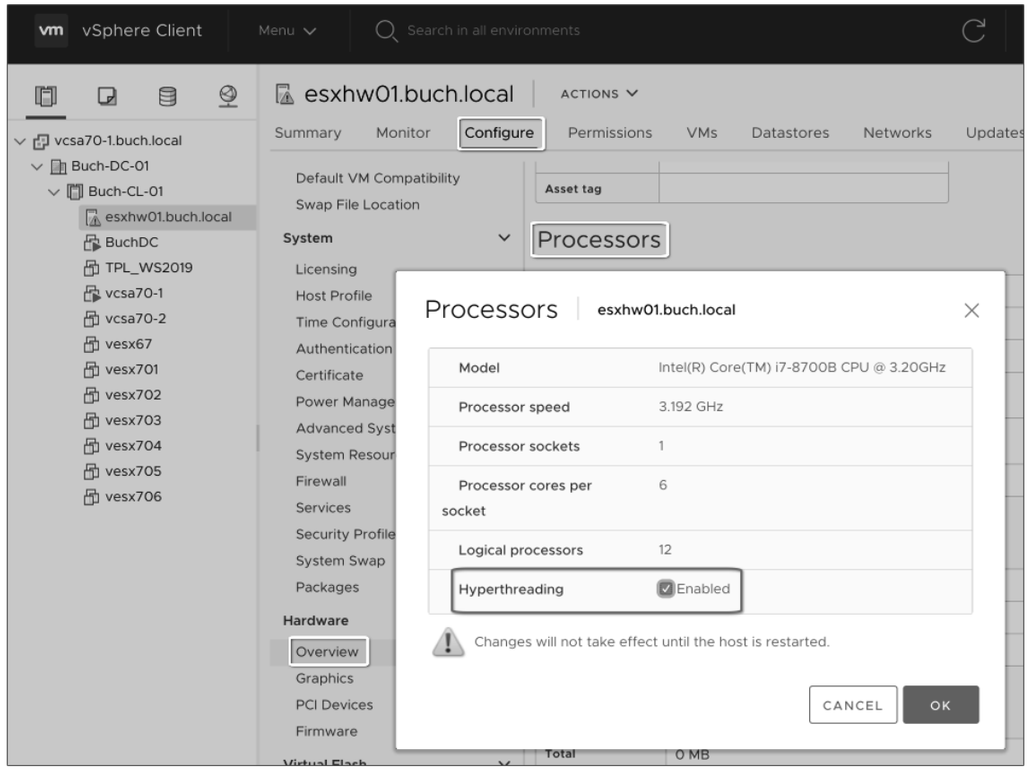


Abbildung 2.5 Aktivierung des Hyperthreadings auf dem vSphere-Host

Der vSphere-Server teilt die Last zwischen den Cores auf, um eine ausgewogene Auslastung zu erreichen. Wenn für eine logische CPU keine Last gefordert wird, wird sie in einen speziellen *Halt State* geschaltet. Dabei kann eine andere VM auf dem Core von den zusätzlichen freien Ressourcen dieser CPU profitieren.

2.4.3 Virtual SMP (vSMP)

Auch in virtuellen Umgebungen ist es möglich, virtuelle Maschinen mit mehr als einer vCPU zu erstellen. Die aktuelle Version von VMware vSphere unterstützt bis zu 256 virtuelle CPUs pro VM. VMware nennt diese Funktion *Virtual SMP* (*Symmetric Multi Processing*) oder auch vSMP. Dabei gilt es einiges zu beachten: Grundsätzlich – und das unterscheidet eine virtuelle Maschine nicht von einem physischen Server – ist nicht jede Applikation multiprozessorfähig. Bevor Sie eine vSMP-Maschine erzeugen, sollten Sie das abklären und dabei nicht nur das Betriebssystem (achten Sie auf die HAL (*Hardware Abstraction Layer*) bzw. den Kernel), sondern auch die Anwendung beachten.

Schauen wir noch einmal zurück auf den Beginn von Abschnitt 2.4, »Grundlagen der CPU-Virtualisierung«, wo wir den logischen Aufbau einer CPU erklärt haben. Da es allen CPUs einer VM möglich sein muss, auf identische Speicheradressen zuzugreifen – auch beim Cache –, wird sofort klar, dass eine virtuelle Maschine mit mehreren CPUs dann am leistungsfähigsten arbeiten kann, wenn alle virtuellen Prozessoren auf einer logischen oder physischen CPU liegen. Befinden sich die Prozessoren auf unterschiedlichen Sockeln, können die virtuellen CPUs nicht in optimaler Geschwindigkeit miteinander kommunizieren. Die Ursache dafür ist, dass der Informationsaustausch der CPUs untereinander über den Frontside-Bus erfolgen muss. Ein ähnliches Verhalten zeigt sich bei der Überschreitung der NUMA-Grenzen. Die Geschwindigkeitseinbußen sind dabei aber nicht so groß wie im vorhergehenden Fall.

Auch beim Betriebssystem müssen Sie auf einiges achten. Denken Sie bitte daran, dass Sie bei mehreren CPUs in einer VM einen Multiprozessor-Kernel installieren müssen. Einen Weg zurück – zumindest bei Windows-VMs – unterstützt Microsoft nicht. Manche Betriebssysteme haben Einschränkungen bei der Anzahl der CPUs, nicht aber bei der Anzahl der Cores!

Sehen wir uns nun an, wie VMware mit dem Thema vSMP und der Tatsache umgeht, dass freie Ressourcen anderen VMs zur Verfügung gestellt werden. Während eine CPU im physischen Umfeld exklusiv einem Betriebssystem zur Verfügung steht, teilen sich die virtuellen Maschinen die CPU-Zyklen. Zur optimalen Abarbeitung der Prozesse werden diese in einem SMP- bzw. vSMP-System parallelisiert. Steht eine Instanz, die gerade einen Teilprozess abarbeitet, nicht zur Verfügung, müssen alle anderen Teilprozesse so lange warten, bis auch dieser Prozess parallel zu den anderen abgearbeitet wurde. Diese Art der parallelen Abarbeitung wird auch *Co-Scheduling* genannt und dient grundsätzlich dazu, die Performance eines Systems zu erhöhen.

Es könnte vorkommen, dass ein Watchdog-Timer auf einen Schwesterprozess warten muss. Reagiert dieser Prozess aber nicht in einem passenden Zeitfenster, stirbt er. Zur Messung dieser Varianzen wird der sogenannte *Skew* herangezogen. Dieser Wert repräsentiert den zeitlichen Unterschied zwischen den Prozessteilen. Überschreitet der Skew einen definierten Schwellenwert, wird die CPU der VM mit angehalten (*co-stopped*). Sie wird erst wieder mitgenutzt (*co-started*), wenn genügend Ressourcen für die Abarbeitung auf der physischen

CPU vorhanden sind. Der Co-Stop verhindert, dass sich der Skew-Wert erhöht; dieser kann nur sinken.

Mit dem *Relaxed Co-Scheduling* gibt es eine Funktion, die dafür sorgt, dass angehaltene vCPUs keine Skew-Wert-Erhöhung mehr erfahren. Somit wird ein zu häufiges Co-Scheduling verhindert (siehe Abbildung 2.6).

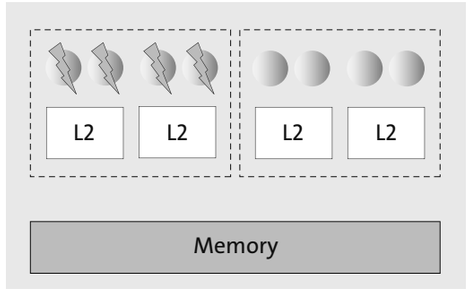


Abbildung 2.6 SMP-Handling alt

Der Skew-Wert hat aber noch eine weitere Funktion: Der VMkernel nutzt diesen Wert, um die Arbeitslast auf die physischen CPUs zu verteilen. Eine geskewte CPU hat Rechenzeit übrig, die andere VMs nutzen können.

Die deutliche Minderung des Co-Stoppings erlaubt nun auch die Nutzung aller Prozessorkerne (siehe Abbildung 2.7).

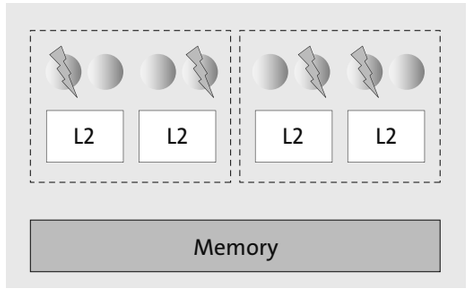


Abbildung 2.7 SMP-Handling aktuell

CPU-Anfragen der VMs müssen nicht unnötig warten, weil nicht genügend Kerne einer physischen CPU verfügbar sind. Somit hat der aktuelle CPU-Scheduler wesentlich mehr Möglichkeiten, CPU-Anfragen zu verteilen.

Seit vSphere 5.x hat sich eine weitere Änderung an dieser Stelle ergeben, die die Performance noch einmal erheblich steigert: VMware hat die *NUMA*-Architektur (*Non-Uniform Memory Access*) in die VM eingeführt (siehe Abbildung 2.8). Die Voraussetzung ist die virtuelle Hard-

ware Version 8. Die Funktion wird bei VMs mit mehr als acht virtuellen CPUs automatisch aktiviert. Unterstützt wird sie sowohl von Intel- als auch von AMD-CPUs.

Lassen Sie uns zuerst darauf eingehen, was NUMA genau ist. NUMA ist interessant für Multiprozessorsysteme. Hier hat jede CPU ihren lokalen Arbeitsspeicher, den sie aber auch anderen CPUs zur Verfügung stellen kann. Auf physischer Ebene erkennen Sie das daran, dass jede CPU ihre eigenen Speicherbänke besitzt. Im Sinne einer guten Performance sollten diese Bänke auch symmetrisch mit Memory bestückt werden. Eine solche Kombination aus CPU plus zugehörigem Speicher nennt man *NUMA-Knoten* (*Node*). Es ist wichtig zu beachten, dass es mittlerweile CPUs gibt, die mehr als einen NUMA-Knoten pro CPU haben.

In Abbildung 2.8 sehen Sie eine CPU mit zwei NUMA-Knoten, die wie empfohlen symmetrisch mit Arbeitsspeicher ausgestattet sind (in diesem Fall 16 GB).

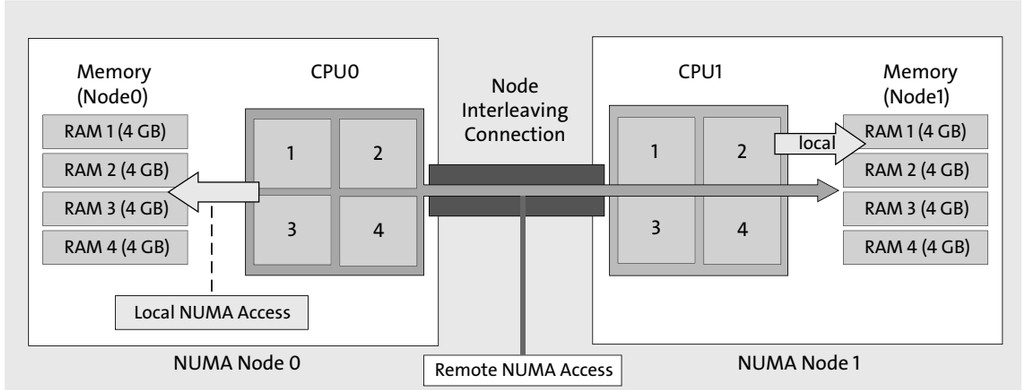


Abbildung 2.8 Die NUMA-Architektur

So wird gewährleistet, dass überwiegend auf schnellen lokalen Speicher zugegriffen werden kann. Das macht sich bei der Gesamtperformance positiv bemerkbar, denn mehrere Prozessoren können nicht konkurrierend auf Speicherbereiche zugreifen. Mit der extremen Steigerung der Cores pro Prozessor ist das ein immer größer werdendes Problem. Gerade bei hochlastigen Anwendungen könnten sich die CPUs bzw. Cores untereinander ausbremsen.

Benötigt ein Kern nun mehr Arbeitsspeicher, als die eigene CPU direkt adressieren kann, kann er diesen anfordern. Über einen Remote-NUMA-Zugriff kann der Speicher einer anderen CPU angefordert und für die eigenen Belange verwendet werden. Dass dieser Zugriff langsamer ist als das Nutzen des eigenen Speichers, müssen wir wohl nicht extra erwähnen.

Welche Vorteile oder Nachteile hat das für eine virtuelle Maschine? Lassen Sie uns tiefer einsteigen und die möglichen Szenarien betrachten. Eine NUMA-VM bekommt einen sogenannten *Home-Node*. Das bedeutet, sie bekommt damit einen Prozessor und Speicher zugewiesen. Braucht eine VM Speicher, wird er optimalerweise vom Home-Node zugewiesen. Dadurch

sind schnelle Zugriffszeiten garantiert. Ist der Workload in einem Home-Node zu hoch, kann bzw. wird die VM auf einen anderen Home-Node verschoben. Gewährleistet werden kann das aber nur, wenn die ESXi-Optimierung aktiv ist. Ist sie das nicht, tritt nicht selten ein Fall wie der in Abbildung 2.9 dargestellte auf.

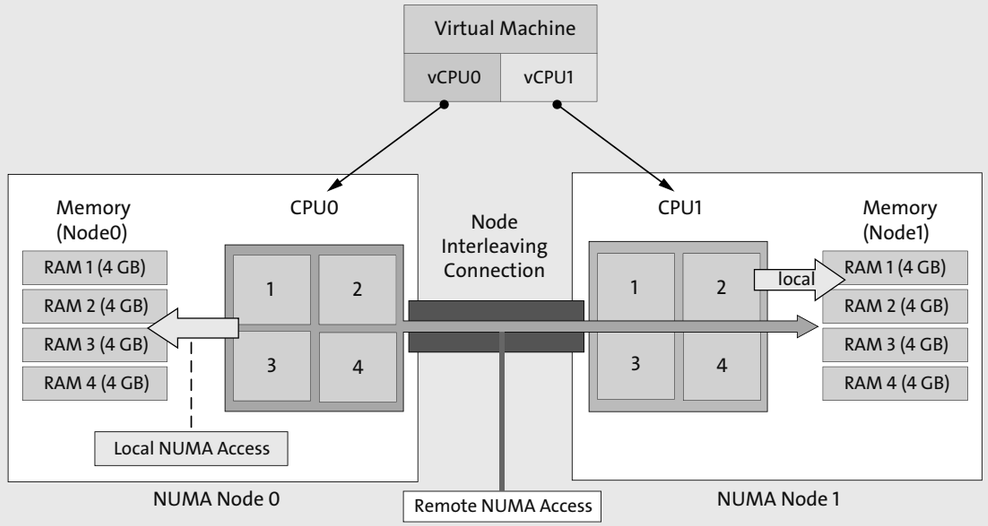


Abbildung 2.9 Verteilung der vCPUs bei deaktivierter ESXi-Optimierung

Aufgrund der inaktiven Optimierung kann es bei Mehrprozessor-VMs passieren, dass sich die vCPUs auf mehrere Prozessoren verteilen, was zur Folge hat, dass die virtuelle Maschine nicht optimal arbeiten kann. In der Grundkonfiguration aktiviert sich NUMA automatisch in der virtuellen Maschine ab der virtuellen Hardwareversion 8. Dennoch sollte immer mit der aktuellsten Version der virtuellen Hardware gearbeitet werden. Da stellt sich sofort die Frage, wie Sie die ESXi-Optimierung aktivieren können (siehe Abbildung 2.10). Lassen Sie uns an dieser Stelle das Pferd von hinten aufzäumen, denn es ist einfacher, die Konfigurationen aufzulisten, die eine NUMA-Optimierung verhindern. In den folgenden Situationen können Sie NUMA also nicht nutzen:

- NUMA ist in der BIOS-Konfiguration des Servers deaktiviert.
- CPU-Affinitätsregeln binden die virtuelle Maschine an Cores, die auf unterschiedlichen NUMA-Knoten liegen.
- Die VM nutzt mehr Arbeitsspeicher, als ein NUMA-Knoten direkt adressieren kann.
- In der VM werden mehr CPU-Kerne genutzt, als ein NUMA-Knoten bereitstellen kann.
- Es sind weniger als vier Cores insgesamt oder zwei Cores pro NUMA-Knoten nutzbar.

Bei den zuletzt genannten Werten handelt es sich um die Standardeinstellungen des ESXi-Hosts. Diese können Sie in den ADVANCED SETTINGS an Ihre Bedürfnisse anpassen. Die Werte `Numa.RebalanceCoresTotal` und `Numa.RebalanceCoresNode` sind für diese Einstellungen verantwortlich.

Es handelt sich also um eine Funktion, die speziell auf die Performanceoptimierung von Mehrprozessor-VMs abzielt.

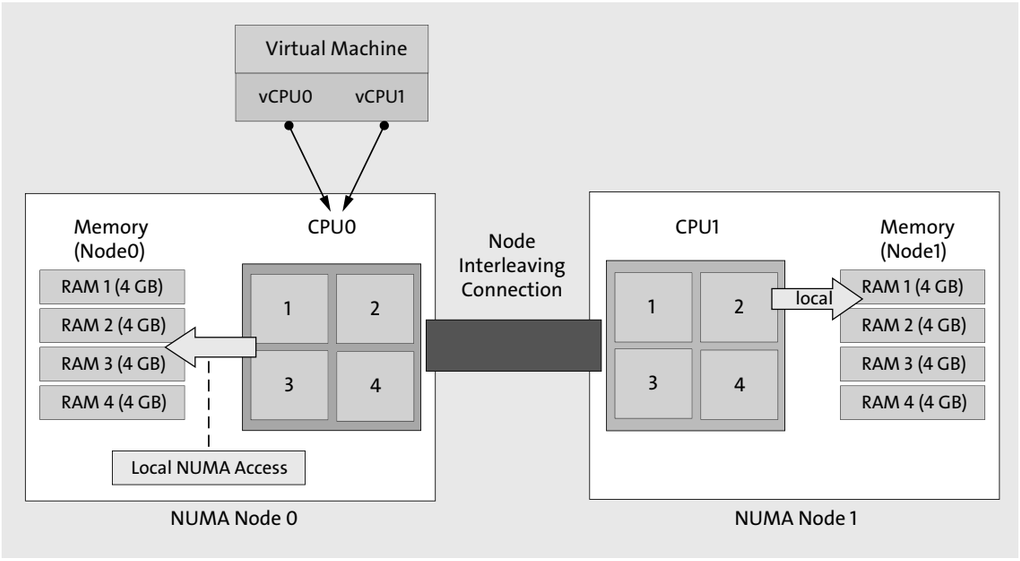


Abbildung 2.10 Aktivierte ESXi-Optimierung: Die VM liegt auf einem NUMA-Knoten.

Zwar gilt auch weiterhin unter vSphere vSMP, dass weniger mehr ist, allerdings ist es wesentlich entspannter geworden, Mehrprozessor-VMs zu verwenden. Die Hauptkriterien sollten immer noch die Anforderungen der Anwendung und des Systems sein und nicht der Gedanke, dass mehr CPUs auch automatisch mehr Leistung bedeuten.

Bedenken Sie aber bitte auch hier, dass es zwar möglich ist, VMs anzulegen, deren Anzahl von vCPUs der Anzahl der gesamten Cores der unterliegenden Hardware entspricht, aber in diesem Fall ist es nicht unwahrscheinlich, dass viele Remote-NUMA-Zugriffe stattfinden. Das bedeutet, dass die Prozessoren untereinander auf ihre Speicherbereiche zugreifen.

Für eine optimale Performance sollte somit eine virtuelle Maschine maximal so viele vCPUs besitzen, wie physische Cores auf einer CPU vorhanden sind. Diese Performanceeinschränkung greift auch, wenn Sie einer VM mehr Arbeitsspeicher zuweisen, als ein NUMA-Knoten – sprich eine physische CPU – direkt adressieren kann, ohne remote auf den Bereich einer anderen CPU zugreifen zu müssen.

2.4.4 Best Practices

Nachfolgend finden Sie einige Empfehlungen zum Umgang mit CPU-Reservierung, -Limits und -Shares:

- Erfahrungsgemäß werden Prozessoren nicht zurückgerüstet, auch wenn sie eigentlich nicht benötigt werden. Bei Mehrprozessor-VMs fangen Sie einfach mit einer Zweiprozessormaschine an. Weitere Prozessoren lassen sich immer noch später hinzukonfigurieren. Vergeben Sie niemals mehr Prozessoren, als sich Cores auf der CPU befinden.
- Einer virtuellen Maschine sollten Sie zu Beginn grundsätzlich niedrige CPU-Ressourcen zuweisen, um im laufenden Betrieb die Ressourcenauslastung anhand der vCenter-Performancemessung zu analysieren.
- Es ist besser, mit CPU-Shares anstelle von CPU-Reservierungen zu arbeiten, wenn Rechenleistung priorisiert werden soll.
- Beim Einsatz von CPU-Reservierungen sollten Sie das aktuelle Minimum definieren, das eine VM benötigt, nicht aber die gewünschte absolute Menge an CPU in MHz. Wenn eine VM mehr Ressourcen benötigt, weist der vSphere-Server diese – je nach definierten Shares – bis zu einem eventuell definierten CPU-Limit dynamisch zu. Des Weiteren ist zu beachten, dass der Einsatz von CPU-Reservierungen die auf einem Host zur Verfügung stehenden CPU-Ressourcen limitieren kann und dadurch weniger VMs gestartet werden können. Zu hohe Reservierungen behindern möglicherweise auch Funktionen wie DRS oder HA. Das Verschieben von virtuellen Maschinen kann durch die Ressourcenauslastung der vSphere verhindert werden.

2.5 Grundlagen der Memory-Virtualisierung

Der physische Speicher eines Hosts wird in zwei Segmente unterteilt: *System* und *Virtual Machines*. Der Speicherbereich für das System wird vom VMkernel und von den Gerätetreibern verwendet und ist nicht konfigurierbar. Er wird mit einer Größe von mindestens 50 MB beim Starten des vSphere-Hosts angelegt und variiert je nach Anzahl und Art der verwendeten PCI-Geräte und deren Treibern. Der Speicherbereich für virtuelle Maschinen ist der Rest des physischen Speichers und wird komplett für die VMs genutzt.

Zur Verdeutlichung erklären wir zunächst die generelle Nutzung von Speicher innerhalb eines Betriebssystems. Speicher wird in einem Betriebssystem über virtuelle Speicheradressen erreicht, die auf physische Adressen verweisen (siehe Abbildung 2.11). Es ist nicht erlaubt, dass eine virtuelle Maschine auf den physischen Speicher eines vSphere-Hosts direkt zugreift. Um den virtuellen Maschinen Speicher zur Verfügung zu stellen, bietet vSphere eine weitere, virtuelle Schicht. Diese gaukelt der VM die physischen Speicheradressen vor.

Im VMware-Jargon heißt der physische Speicher im Host *Machine Memory Pages*, und die der VM virtualisiert vorgegaukelten physischen Speicherseiten werden *Physical Memory*

Pages genannt. Die Physical Memory Pages für eine VM sind – so wie es ein Betriebssystem erwartet – durchgängig mit Nullen gefüllt. Sie sind durch die Virtualisierungsschicht aus verschiedenen Bereichen zusammengefasst, aber nicht zusammenhängend. Diese Bereiche sind z. B. normale physische Speicherbereiche (*Machine Memory Pages*) von vSphere Shared Pages oder auch Swapped Pages. Das virtuelle Speichermanagement erfolgt durch den Host über den VMkernel, und zwar unabhängig von dem Betriebssystem, das in der VM läuft. Der VMkernel greift von der VM alle Befehle ab, die auf den Speicherbereich schreibend zugreifen möchten, und leitet sie auf die der VM vorgegaukelten Physical Memory Pages um.

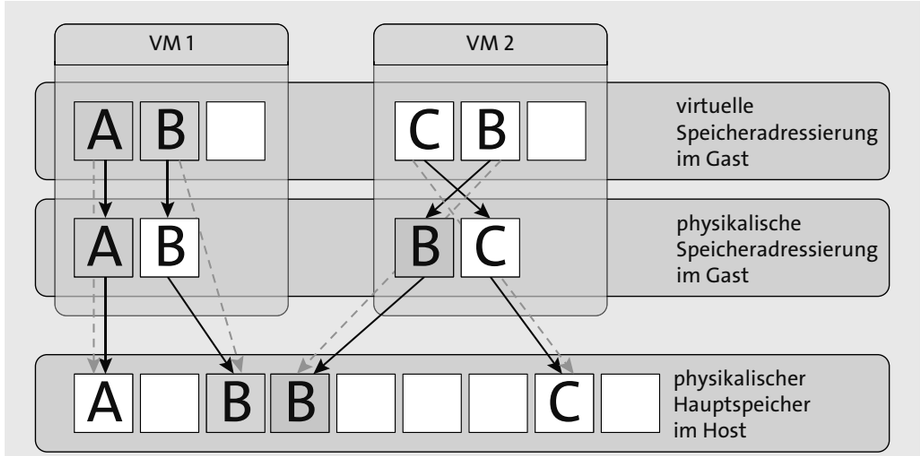


Abbildung 2.11 Speicheradressierung zwischen VM und Host

Der Speicher wird normalerweise in 4-KB-Blöcke eingeteilt. Es werden aber auch Memory-Blöcke von 2 MB unterstützt. Diese Funktion können Sie nur pro VM konfigurieren. Dazu aktivieren Sie in der Konfigurationsdatei die Funktion `Mem.AllocGuestLargePage=1`. Dies ist empfehlenswert, wenn die VM große Speicherseiten benötigt, wie z. B. ein Datenbankserver.

2.5.1 Virtual Machine Memory

Der Speicherbereich, der für die VMs zur Verfügung steht, wird *Virtual Machine Memory* genannt und bietet allen VMs die Speicherressourcen des vSphere-Servers abzüglich eines Virtualisierungs-Overheads. Dem Betriebssystem wird vorgegaukelt, dass der Speicher, der in der Konfiguration festgelegt wurde, auch vorhanden ist. Der physisch zugewiesene Speicher kann aber variieren – bis zum konfigurierten Maximum. Auch hier setzen Sie über die Einstellung der Shares-Werte eine Priorität gegenüber den anderen VMs, die auf demselben Host arbeiten. Eine Reservierung weist den Speicher der virtuellen Maschine fest zu.

2.5.2 Memory-Overhead

Der Memory-Overhead hängt von der Anzahl der CPUs und natürlich von dem Speicher ab, der der VM zugewiesen ist. Dieser Memory-Overhead stellt einen Speicherbereich zur Verfügung, um VM-Frame-Buffer sowie verschiedene Virtualisierungsdatenstrukturen abzulegen. Die Nutznießer dieses Speichers sind der vmx-Prozess (*Virtual Machine Executable*), der VMM (*Virtual Machine Monitor*), Speicher für die Verwaltung von Geräten und Speicher für das Management und die benötigten Agenten.

2.5.3 Memory-Overcommitment

vSphere bietet die Möglichkeit, mehr RAM an virtuelle Maschinen zu vergeben, als physisch im Host selbst vorhanden ist. Dieses Feature nennt sich *Memory-Overcommitment* und setzt sich aus mehreren verschiedenen Techniken zusammen: aus der *Memory-Compression*, dem *Page-Sharing*, dem *Memory-Ballooning* und dem *Memory-Swapping*. Mit all diesen Techniken versucht man, ungenutzte Speicherbereiche von einer VM auf andere Maschinen zu verteilen, die aktuell mehr Speicher benötigen. Die Priorisierung erfolgt auch in diesem Fall über die eingestellten Share-Werte.

2.5.4 Memory-Compression

Ist das Memory-Overcommitment aktiviert, wird damit auch die Memory-Compression eingeschaltet. Die Speicherseiten werden automatisch komprimiert und im Arbeitsspeicher vorgehalten. Die Performance ist dabei nur geringfügig eingeschränkt, denn der Zugriff auf den Arbeitsspeicher ist allemal schneller, als wenn das System auf geswappte Daten zugreifen muss. Zwei Einstellungen beeinflussen dabei das Verhalten der Funktion. In den ADVANCED SETTINGS lässt sich die Funktion ganz deaktivieren, indem Sie den Parameter `Mem.MemZipEnable` auf 0 setzen. Der Parameter `Mem.MemZipMaxPct` gibt prozentual an, wie viel Speicher der VM maximal als Kompressionscache genutzt werden soll. Der Standardwert dieses Parameters liegt bei 10 %.

2.5.5 Content-based Page-Sharing

Die Page-Sharing-Technik wird beim Betrieb von mehreren VMs auf einem Host verwendet. Es wird versucht, identische Memory-Pages der VMs zusammenzufassen. Die dabei beobachtete Speicherblockgröße ist so klein, dass es vollkommen unerheblich ist, ob auf den virtuellen Servern identische Software installiert ist oder nicht.

Trotzdem gelingt dies umso besser, je homogener die verschiedenen Gastbetriebssysteme sind, also wenn mehr identische Serverapplikationen auf ihnen laufen. Ein gutes Beispiel ist eine Serverfarm mit identischen Webservern, die aber alle unterschiedlichen Webcontent hosten. Es ist zu erwarten, dass diese Systeme eine große Anzahl von identischen Speicherblöcken haben, die von der VMM zusammengefasst werden können. So werden redundante Speicherinhalte eliminiert. Will nun eine der virtuellen Maschinen einen solchen Speicherbereich beschreiben, wird für diesen Server eine Kopie des Speicherblocks exklusiv angelegt, sodass er ihn frei nutzen kann. Bei dieser Technik sind bis zu 30 % Speicherersparnis erreichbar. Bei weniger homogenen Memory-Inhalten reduziert sich die Ersparnis auf ca. 5 %.

2.5.6 Memory-Ballooning

Das in Abschnitt 2.5.3 beschriebene Memory-Overcommitment kann nur dann einwandfrei funktionieren, wenn dem Host ein Mechanismus zur Verfügung steht, der das Management des Arbeitsspeichers im virtuellen System übernimmt – und das natürlich im laufenden Betrieb. Dafür ist das sogenannte *Memory-Ballooning* zuständig (siehe Abbildung 2.12).

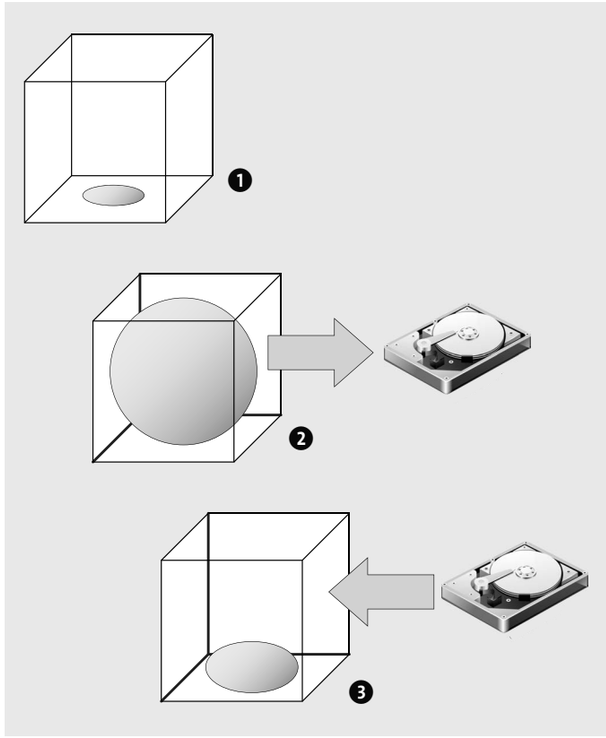


Abbildung 2.12 Darstellung des Memory-Balloonings

Der Memory-Balloon-Treiber (*vmmemctl*) kommt ins Spiel, wenn der Speicher eines Hosts zu knapp wird oder wenn eine VM an ihre Speichergrenzen stößt. Braucht der Host Speicher, hat das Ballooning immer Vorrang vor dem Swappen.

Wird Speicher benötigt, gibt der *Virtual Machine Monitor* (VMM) dem Ballooning-Treiber das Kommando zur Anforderung von Speicher vom Betriebssystem (siehe Abbildung 2.12, ❶). Ist genug Speicher vorhanden, gibt die VM demjenigen Treiber Speicher, der in der Free-List steht. Ist kein freier Speicher vorhanden, wird es dem Gastbetriebssystem überlassen, welcher Speicher freigegeben werden kann.

Der vSphere-Kernel gibt im Hintergrund die vom Ballooning-Treiber markierten Speicherseiten frei, bis genug Speicher für den Host akquiriert worden ist ❷. Anschließend beginnt der Ballooning-Treiber, den reservierten Speicher wieder freizugeben ❸.

Das Verhalten des Memory-Ballonings können Sie pro vSphere-Server durch den Parameter `mem.CtlMaxPercent` festlegen. Dieser Wert bestimmt die maximale Speichermenge in Prozent, die durch diese Technik von einer virtuellen Maschine abgezogen werden kann.

2.5.7 Memory-Swapping

Das *Memory-Swapping* dient ebenso wie das Ballooning dazu, der VM mehr Arbeitsspeicher zuzuweisen. Diese Technik ist für den Host die letzte, aber auch langsamste Möglichkeit, Speicher für andere virtuelle Maschinen zur Verfügung zu stellen. Beim Start einer VM wird automatisch eine solche Swap-Datei angelegt.

Das Swapping tritt zu dem Zeitpunkt in Aktion, zu dem der Hypervisor nicht die Möglichkeit hat, über den Ballooning-Treiber festzustellen, welche Speicherseiten zurückgegeben werden können. Die Ursache dafür kann auch sein, dass keine VMware Tools installiert sind oder kein Ballooning-Treiber vorhanden ist. Bootet die VM (zu diesem Zeitpunkt sind noch keine VMware Tools aktiv), ist der Treiber auch nicht produktiv. Des Weiteren kommt diese Technik zum Zuge, wenn das Memory-Ballooning zu langsam ist, um den Speicherbedarf einer VM zu decken. Das Swapping ist generell langsamer als das Ballooning. Es wird eine Swap-Datei pro VM auf dem Volume abgelegt, und zwar im Verzeichnis der virtuellen Maschine. Das Swapping garantiert einer VM eine verfügbare Speichermenge, die mindestens ausreicht, damit die VM starten kann.

Dieser Speicherbereich, die Swap-Datei, ist der der VM jetzt neu zugewiesene Speicher und wird beim Einschalten einer VM angelegt. Die Größe variiert je nach VM und ist die Differenz zwischen dem Reservierungswert und dem zugewiesenen Speicher einer VM.

Eine Besonderheit bei der Verwendung von Memory-Swapping sollten Sie beachten: Fällt der ESXi-Server aus, werden diese Swap-Dateien nicht mehr automatisch gelöscht. Sie müssen sie dann manuell löschen, wozu das Stoppen und Starten einer VM notwendig wird.

Ein weiteres Feature von VMware vSphere gibt es noch: Es nennt sich *Swap to Host Cache*. Was soll damit erreicht werden? Voraussetzung für die Nutzung der Funktion ist das Vorhandensein einer lokalen SSD-Platte im vSphere-Host. Sie können diese Platte als lokale Swap-Disk für die virtuellen Maschinen einrichten. Der Vorteil liegt auf der Hand: Wenn schon geswappt werden muss, dann geschieht das auf einer sehr schnellen lokalen Disk.

2.5.8 Best Practices

Im Folgenden finden Sie einige Empfehlungen zum Umgang mit Memory-Reservation, Memory-Limits und Memory-Shares:

- Grundsätzlich sollten Sie den Einsatz von Memory-Overcommitment vermeiden. Es bewirkt auf jeden Fall eine Verlangsamung. Sollte die Überbelegung des Speichers unvermeidbar sein, achten Sie darauf, dass nicht das Memory-Swapping genutzt wird, denn es reduziert die Performance einer VM deutlich.
- Sie sollten Memory-Shares gegenüber Memory-Reservierungen den Vorzug geben. Das gilt auch hier nur für die Priorisierung.
- Beim Einsatz von Memory-Reservierungen sollten Sie ein Minimum an RAM definieren, den eine VM benötigt. Falls eine VM mehr Ressourcen braucht, werden diese vom Host, je nach Shares, bis zum eventuell definierten Memory-Limit dynamisch zugewiesen. Beachten Sie außerdem, dass der Einsatz von Memory-Reservierungen die auf einem vSphere-Server zur Verfügung stehenden Speicherressourcen limitiert. Somit können weniger VMs gestartet werden – selbst dann, wenn andere VMs den reservierten Speicherbereich nicht nutzen. Auch kann das *Distributed Resource Scheduling* (DRS) in seiner Funktion behindert werden, da hier die Ressourcenauslastung des Hosts ein Verschieben von virtuellen Maschinen verhindert. Sie können diese Einschränkung aber umgehen, indem Sie die Slot-Size in der Cluster-Konfiguration von Hand ändern.
- Ein Delegieren des Ressourcenmanagements erreichen Sie idealerweise durch die Einführung von Ressourcenpools. Dabei geben Sie die Grenzen des Ressourcenpools an (also die Reservierung und das Limit), um die darin laufenden virtuellen Maschinen von den weiteren Ressourcen eines Hosts zu isolieren.

2.6 Grundlagen der Hardwarevirtualisierung

Wie wir bis jetzt gezeigt haben, wird bei der klassischen Virtualisierung dem Gast eine virtuelle Hardware zur Verfügung gestellt. Das sehen Sie sehr schön, wenn Sie eine virtuelle Maschine booten: Sofort ist der vom Computer bekannte BIOS-Schirm sichtbar. Gehen Sie in die Tiefen des BIOS, stellt sich die virtuelle Maschine wie ein ganz normaler Computer dar. Alle Elemente eines Computers werden in der VM emuliert, seien es der Festplattencontroller, die Netzwerkkarte oder andere Hardwareelemente. Wie schon beschrieben, handelt es sich um einen »normalen« PC, nur eben virtuell. Der Vorteil besteht darin, dass Sie ein Betriebssystem – die passenden Treiber vorausgesetzt – einfach in die virtuelle Hülle bringen können. Anschließend installieren Sie die Applikation, und fertig ist der virtuelle Server.

Es gibt aber noch andere Varianten von virtuellen Maschinen: die sogenannten *paravirtualisierten VMs*.

Abbildung 2.13 stellt den Unterschied zwischen beiden Varianten dar. Sie veranschaulicht, dass bei der paravirtualisierten Maschine der Layer der virtuellen Hardware fehlt. Dafür existiert eine definierte Schnittstelle. Sie steuert die Ressourcen und den direkten gemeinsamen Zugriff auf die physische Hardware. Ein solcher Mechanismus kann aber nur funktionieren, wenn dem Betriebssystem der Hypervisor »bekannt« ist. Als Ergebnis erhöht sich die Performance der virtuellen Maschine, denn es fehlt die Schicht der virtuellen Hardware. Die direkte Kommunikation zwischen dem Gastsystem und dem Hypervisor wird als *Paravirtualisierung* bezeichnet.

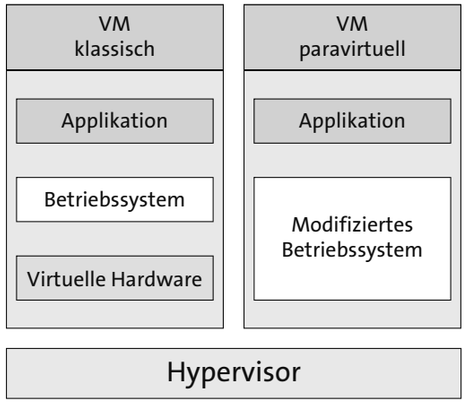


Abbildung 2.13 Unterschied zwischen klassischer und paravirtualisierter VM

Nicht alle Betriebssysteme unterstützen die Paravirtualisierung. Das rührt daher, dass starke Eingriffe in den Kernel erforderlich sind.

Im Gegensatz zu dem Ansatz, dass der Layer der virtuellen Hardware vollständig entfällt (bei komplett unterstütztem Betriebssystem), gibt es Teilansätze, auf die wir kurz eingehen wollen. Lassen Sie uns zuvor etwas ausholen: Warum geht VMware diesen Weg, und welche Vorteile bringen die Technologien?

Der Layer der Hardwarevirtualisierung ist eine Softwarekomponente, die die Hülle für die VM simuliert. Das bedeutet aber im Gegenzug, dass alle Aktionen, die über diese Schicht laufen, Last in diesem Layer erzeugen, bevor die Daten an die eigentliche Hardwarekomponente gelangen (wie z. B. die Netzwerkkarte). Das erzeugt Rechenzeit auf der CPU und bremst die Performance. Der Ansatz, dem nun gefolgt wird, besteht darin, Teilkomponenten zu paravirtualisieren. Der Vorteil dabei ist, dass nicht der gesamte Kernel angepasst werden muss, sondern dass es reicht, passende »Hardwaretreiber« für das Gastbetriebssystem zur Verfügung zu stellen.

Es gibt bereits entsprechende Ansätze bei dem paravirtualisierten SCSI-Adapter (PVSCSI). Auf die Funktionen des Adapters gehen wir an entsprechender Stelle in Kapitel 20, »Virtuelle Maschinen«, ein.

2.7 Management einer virtuellen vSphere-Infrastruktur

Für das Management von virtuellen Infrastrukturen wird ein passendes System benötigt. Wenn Sie noch die alten vSphere-Versionen kennen, erwarten Sie an dieser Stelle den *Platform Services Controller* (PSC) und den *vCenter Server*. Das ist inzwischen nicht mehr richtig, stattdessen sagen wir: Back to the Roots. Wie schon in den Anfängen des vCenter Servers gibt es nur noch eine Komponente. Der PSC als einzelne Komponente ist tot, er ist wieder komplett in das vCenter eingeflossen.

Damit aber nicht genug: Aus Redundanzgründen für mehrere Standorte oder aufgrund der Größe können auch weiterhin mehrere Systeme nebeneinander installiert werden. Sie können als Einzelsystem zum Einsatz kommen oder werden über eine gemeinsame Domain miteinander verbunden. Die Ausfallsicherheit mit *vCenter High Availability* (vCenter HA) führt dazu, dass keine zusätzlichen Komponenten wie z. B. Loadbalancer benötigt werden, um die Ausfallsicherheit eines vCenter Servers zu gewährleisten.

Wichtig

Mit vSphere-Version 7.0 gibt es keine Möglichkeit mehr, PSC und vCenter zu trennen. Beide Komponenten sind integraler Bestandteil der Appliance. Den PSC gibt es nicht mehr.

Eine Migration von abgekündigten Strukturen in die neue Appliance wird in Abschnitt 5.7 beschrieben.

Eine Windows-Version des vCenters gibt es ebenfalls nicht mehr.

Mögliche und auch nicht unterstützte Topologien sollen im Folgenden näher betrachtet werden.

2.7.1 vCenter-Server-Topologien

Durch die Verschmelzung von PSC und vCenter Server haben sich die Topologien stark vereinfacht. VMware bietet bei der Migration zu der neuen Topologie entsprechende Unterstützung, damit nicht ein völliger Neuaufbau notwendig ist.

Achtung

VMware schränkt, auch mit vSphere 7.0, die unterstützten Topologien weiter ein. Es ist zwar technisch möglich, auch andere Topologien zu installieren, aber für solche Umgebungen gibt es keinen Support!

Bevor wir Ihnen eine Liste der unterstützten Topologien zeigen, müssen Sie noch wissen, dass VMware eine wichtige Änderung bei der Verknüpfung von vCenter Servern vorgenommen hat. Es gibt nur noch eine Möglichkeit der Verlinkung, und zwar den *Enhanced Linked Mode*, den *Embedded Link Mode* gibt es nicht mehr. Für den Anwender, der schon länger mit VMware vSphere arbeitet, ist das etwas verwirrend. War der Enhanced Linked Mode früher

den Windows-vCenter-Servern vorbehalten und der Embedded Linked Mode den Appliances, wurde der Name Embedded Linked Mode aufgegeben, und die Vernetzung von vCenter-Appliances heißt jetzt Enhanced Linked Mode. Diese Namenswechsel sind etwas verwirrend, denn es ist notwendig zu wissen, was für eine Version die im Einsatz befindliche Infrastruktur hat, um zu verstehen, was gemeint ist, wenn vom Enhanced Linked Mode die Rede ist.

Achtung

Der Embedded Linked Mode heißt jetzt Enhanced Linked Mode!

Einen Begriff gilt es im Vorfeld noch näher zu definieren. Eine *SSO-Domain* (*Single-Sign-On-Domain*) ist der Name, den der VMware-Directory-Dienst für die Anmeldung benutzt. Die *Single-Sign-On-Site* gibt es nicht mehr, hier hat ebenfalls eine Vereinfachung der Struktur stattgefunden. Auch ein Wechsel des vCenter Servers in eine andere SSO-Domain ist mittlerweile möglich.

Achtung

Für den Domainnamen sollten ausschließlich Namen genutzt werden, die im Netzwerk noch nicht verwendet werden!

2.7.2 Abgekündigte vCenter-Topologien

Viele altbekannte Topologien wurden abgekündigt, weil ein singulär installierter *Platform Services Controller* (PSC) nicht mehr unterstützt wird.

Folgende Topologien werden nicht mehr unterstützt.

- PSC und vCenter getrennt (siehe Abbildung 2.14)
  - nur eine Single-Sign-On-Domain
  - PSC und vCenter Server getrennt

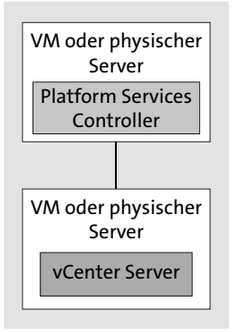


Abbildung 2.14 Externer PSC und vCenter Server

- Mehrere vCenter Server mit externem PSC (siehe Abbildung 2.15)
  - nur eine Single-Sign-On-Domain
  - PSC und vCenter Server getrennt

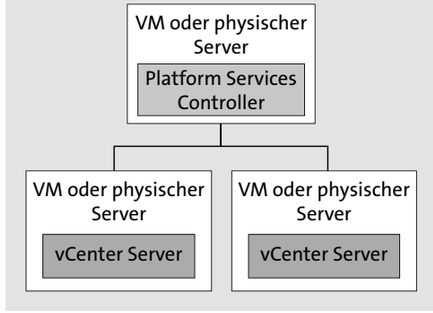


Abbildung 2.15 PSC mit zwei vCenter Servern ohne Loadbalancer

- vCenter embedded mit PSC und zwei vCenter Servern (siehe Abbildung 2.16)
  - nur eine Single-Sign-On-Domain
  - PSC und vCenter embedded und vCenter Server z. T. getrennt

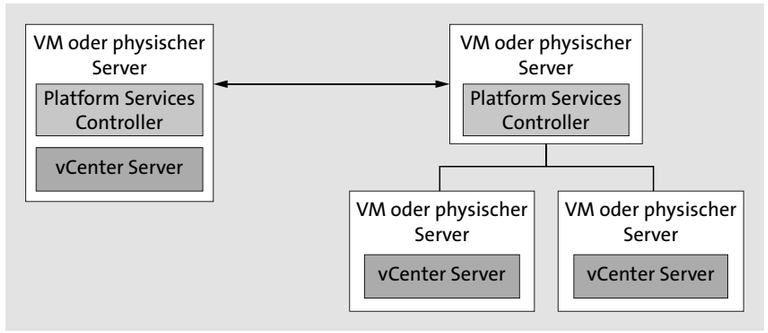


Abbildung 2.16 Embedded VCSA mit Single PSC

- vCenter Server mit zwei PSCs (siehe Abbildung 2.17)
  - nur eine Single-Sign-On-Domain
  - ein oder mehrere vCenter Server möglich
  - zwei externe PSCs (Ihr Betriebssystem muss identisch sein)
  - es können vCenter Server auf Basis von Windows und auf Basis von Appliances kombiniert werden

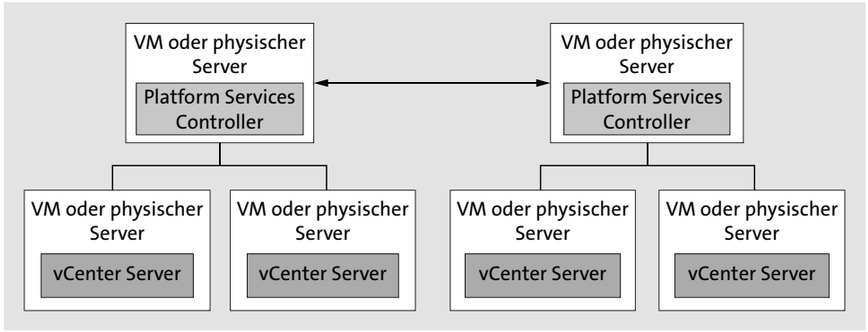


Abbildung 2.17 Zwei PSCs mit mehreren vCenter Servern ohne Loadbalancer

- vCenter Server in zwei Sites mit PSC
  - nur eine Sign-On-Domain (siehe Abbildung 2.18)
  - zwei Sign-On-Sites
  - mindestens ein PSC pro Site
  - mindestens ein vCenter pro Site

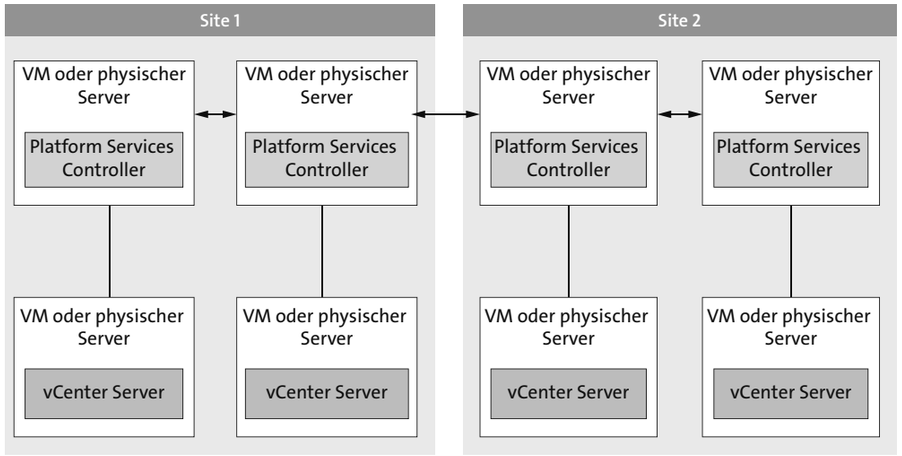


Abbildung 2.18 Zwei Sites, eine Single-Sign-On-Domain

- vCenter Server mit zwei PSCs und Loadbalancing
  - nur eine Sign-On-Domain
  - ein oder mehrere vCenter Server möglich

  - zwei externe PSCs
  - Loadbalancer (siehe Abbildung 2.19)

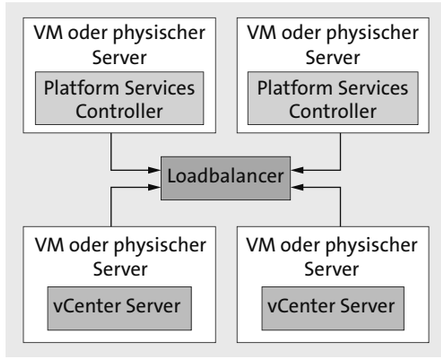


Abbildung 2.19 PSCs mit Loadbalancer

- vCenter Server mit PSCs und Loadbalancing in zwei Sites
  - nur eine Sign-On-Domain
  - zwei Sign-On-Sites (siehe Abbildung 2.20)
  - mindestens ein PSC pro Site
  - mindestens ein vCenter pro Site
  - Loadbalancer

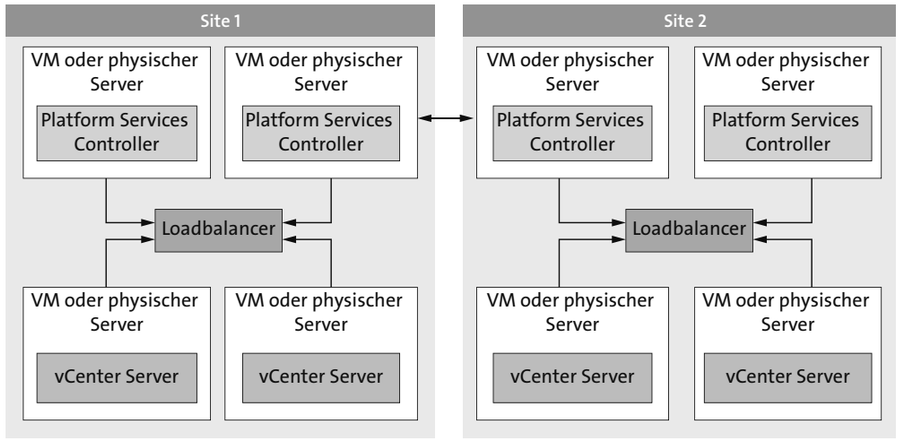


Abbildung 2.20 Zwei Sites mit Loadbalancer

2.7.3 Der Weg zur unterstützten Topologie

Die einzige unterstützte Variante ist die vCenter Server Appliance mit allen integrierten Systemen. Grundsätzlich ist die Vorgehensweise der Migration davon abhängig, welche Topologie derzeit zum Einsatz kommt. Die gute Nachricht ist, dass VMware die passenden Tools hat, um den Weg zur neuen Topologie zu gehen, und es wird mittlerweile auch unterstützt, dass ein vCenter Server Mitglied einer anderen Single-Sign-On-Domain wird, ohne ein Neuinstallation vornehmen zu müssen.

Unerheblich ist, welches Betriebssystem unter der zu aktualisierenden Kombination aus PSC und vCenter Server liegt.

Grundsätzlich muss erst die Topologie angepasst werden, und im Nachgang kann die Migration auf eine neue vCenter-Server-Version erfolgen. Ausnahme ist hier eine einfache Infrastruktur mit einer All-in-One-Appliance bzw. einem PSC mit einem vCenter. Hier kann eine Migration zur Version 7.0 direkt erfolgen.

Achtung

Das Konvertierungstool funktioniert erst ab vCenter-Server-Version 6.7 Update 1.

Mit dem Konvertierungstool bzw. über den vSphere-Webclient wird auf dem vCenter Server ein PSC mit Verbindung zum alten PSC installiert. Anschließend kann der alte PSC dekomissioniert werden. Die Version hat sich nach diesem Prozess nicht geändert. Ein Upgrade kann jetzt im Nachgang erfolgen.

2.7.4 Enhanced Linked Mode

Der jetzige Enhanced Linked Mode erlaubt die Verbindung zwischen verschiedenen vCenter-Server-Systemen (siehe Abbildung 2.21). Damit einhergehend werden Rollen, Rechten, Lizenzen, Policies und Tags repliziert. Eine Anmeldung an einem vCenter Server listet automatisch alle verbundenen Systeme mit auf:

- Nur eine Single-Sign-On-Domain.
- Maximal 15 vCenter Server können in einer Enhanced-Linked-Mode-Gruppe Mitglied werden.

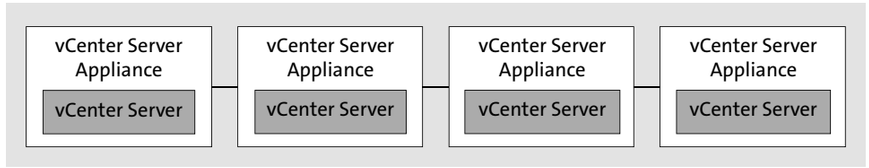


Abbildung 2.21 Enhanced Linked Mode

Kommen mehrere vCenter Server zum Einsatz, sollte darauf geachtet werden, dass sich die SSO-Controller sauber abgleichen. Mehr dazu finden Sie in Abschnitt 6.9.

2.7.5 vCenter Server

Der vCenter Server ist Dreh- und Angelpunkt der VMware-Infrastruktur. Mit dem Managementsystem verwalten Sie das komplette VMware-Datacenter von der Konfiguration der ESXi-Server über das Erstellen von virtuellen Maschinen bis zum Einrichten der VMware-Features HA (*High Availability*) und DRS (*Distributed Ressource Scheduling*) sowie vieler andere Funktionen. Des Weiteren bietet das vCenter eine Zugriffskontrolle auf Basis von Benutzern und Gruppen. Performancedaten der vSphere-Server sowie der virtuellen Maschinen werden ebenfalls gesammelt und in der Datenbank abgelegt.

Der vCenter Server ist nicht zwingend notwendig zum Betreiben von vSphere-Hosts, damit diese die Dienste bereitstellen können, um virtuelle Maschinen zu erstellen. Sie können jeden Host einzeln und unabhängig voneinander verwalten. Viele Dienste aber, wie z. B. DRS, setzen zwingend einen vCenter Server voraus.

Die Software bietet eine zentralisierte Verwaltung aller im VMware-Datacenter zusammengefassten Ressourcen, deren virtueller Maschinen sowie der Benutzer.

Des Weiteren bietet der Managementserver eine Schnittstelle für Plug-ins zur Erweiterung der Funktionalität. Dazu zählen z. B.:

- vSphere Replication
- weitere Tools von VMware
- Tools von Drittanbietern oder auch Freewaretools

Integrierte Dienste

Über die Integration einer SSO-Lösung (*Single Sign On*) wird dem Anwender geholfen, die Anzahl der Anmeldungen im System zu reduzieren. Alle VMware-eigenen Dienste werden anmeldetechnisch unter dem Mantel des SSO-Diensts zusammengefasst. Mit einer Anmeldung findet sich der Administrator im gesamten VMware-Framework wieder und kann so die komplette Umgebung administrieren. Dieser Dienst kann nicht umgangen und muss mitinstalliert werden. Durch eine Verknüpfung des VMware-eigenen SSO mit einem Windows Active Directory kann auch dieses System als Authentifizierungsquelle genutzt werden.

Der SSO-Dienst (siehe Abbildung 2.22) nutzt seine lokale Datenbank oder verifiziert die User über einen eingebundenen Verzeichnisdienst. Ist die Anmeldung erfolgreich, kann der Anwender in seinem HTML5-Client alle VMware-Komponenten sehen und nutzen, ohne sich erneut anmelden zu müssen. Voraussetzung dafür ist natürlich, dass er dafür freigeschaltet ist.

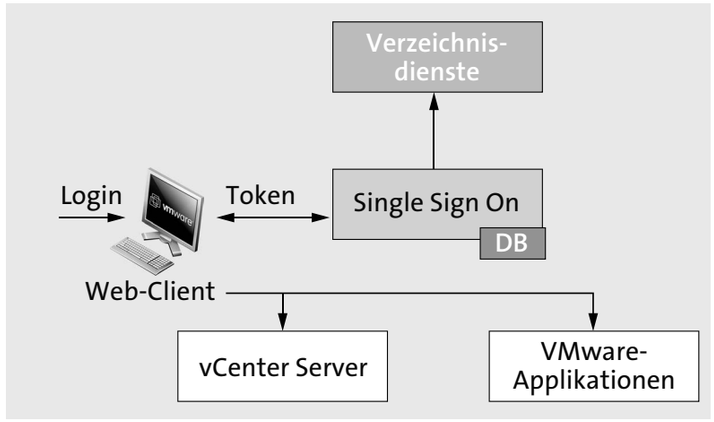


Abbildung 2.22 Aufbau einer SSO-Struktur

Mit dem SSO können sich zentral gepflegte Anwender an allen VMware-Komponenten anmelden. Dabei können unterschiedliche Verzeichnisdienste eingebunden werden:

- Windows Active Directory ab Version 2003
- Active Directory über LDAP
- Open LDAP ab Version 2.4
- die lokale SSO-Datenbank

Die Möglichkeiten der Installation sind dabei vielfältig. Je nach Ausprägung der Landschaften können Sie unterschiedliche Installationsszenarien auswählen.

Editionen

Es gibt drei Versionen des vCenter Servers von VMware:

- *vCenter Server Essentials*
  (maximal drei Hosts, vSphere Essentials bzw. Essentials Plus Version)
- *vCenter Server Foundation*
  (maximal vier Hosts, Standard, Enterprise Plus bzw. VMware vCloud Suite)
- *vCenter Server Standard* (alle vSphere-Versionen)

Wenn Sie ohne Einschränkungen arbeiten wollen, müssen Sie auf die *Standard*-Version des vCenter Servers zurückgreifen. Bei kleineren Umgebungen können Sie die *Foundation*-Version nutzen. Die *Essentials*-Version dient Umgebungen, die noch kleiner sind und nur mit den abgespeckten vSphere-Versionen Essentials bzw. Essentials Plus arbeiten. Ein späteres Upgrade auf die *Standard*-Version ist nur eine Frage des Geldes.

Maximale Ausstattung

Auch das vCenter kann nicht unendlich viele Ressourcen verwalten; es gilt die eine oder andere Einschränkung. Die Angaben in den folgenden Tabellen beziehen sich auf die *Standard*-Version des vCenter Servers.

vCenter Server Appliance	Anzahl
Hosts	2.500
VMs (registriert/eingeschaltet)	45.000/40.000

Tabelle 2.1 Mögliche verwaltbare Infrastruktur für die vCenter Server Appliance

vCenter Server Scalability – Enhanced Linked Mode	Anzahl
Linked vCenter Server	15
Hosts im Linked Mode	15.000
Powered-on VMs	135.000
Registered VMs	150.000

Tabelle 2.2 Mögliche verwaltbare Infrastruktur für das vCenter im Enhanced Linked Mode

Die Zahlen, die VMware hier ansetzt, sind an der einen oder anderen Stelle sicherlich sehr optimistisch gewählt. Sie sollen nur als Richtschnur dienen, damit Sie abschätzen können, wie viele Managementsysteme Sie benötigen.

Zugriff

Damit Sie die virtuelle Infrastruktur auch verwalten können, benötigen Sie ein Werkzeug, um auf die einzelnen Komponenten zuzugreifen. Hier haben Sie nur noch eine Möglichkeit: Der Zugriff auf die Infrastruktur erfolgt mit einem Webbrowser. Mittlerweile sind alle Funktionen im *HTML5-Client* umgesetzt. Der Flash-basierte Client gehört somit zum alten Eisen – endlich.

Lizenzierung

Für die Verwaltung der VMware-Lizenzen in einer vSphere-Infrastruktur wird der im vCenter Server integrierte Lizenzserver eingesetzt. In diese Verwaltungskonsole tragen Sie alle VMware-Lizenzen ein und weisen sie den zugehörigen Hardwarekomponenten zu.

VMware Infrastructure SDK

Es gibt die verschiedensten Möglichkeiten, in der virtuellen Infrastruktur Aufgaben zu automatisieren, auch außerhalb des vCenters und seiner Komponenten. Sie haben als Anwender

verschiedene Optionen zur Verfügung, um eigene Anforderungen abzubilden. Dabei ist es egal, ob Sie mit der PowerShell skripten oder mit C programmieren möchten. Es gibt noch viele weitere Möglichkeiten, das Management der Infrastruktur zu optimieren. VMware stellt eine Auswahl von Softwarepaketen zur Verfügung, damit Anwender das Management an ihre Bedürfnisse anpassen können.

Wenn Sie sich für alle Informationen interessieren, finden Sie auf der eigens dafür eingerichteten Webseite Näheres zu dem gewünschten Thema. Die Webseite erreichen Sie unter *https://www.vmware.com/support/pubs/sdk_pubs.html*. Von dort können Sie auch die Applikationen herunterladen.

Benötigte Netzwerkports – Implementierung

Der Host hat Berührungspunkte mit verschiedenen Komponenten. Hier muss das Netzwerk für unterschiedliche Ports freigeschaltet werden. Sie finden die entsprechenden Ports in Tabelle 2.3.

Port	Protokoll	Kommunikation	Beschreibung
22	TCP	Client → vSphere-Host	SSH-Server
53	UDP	vSphere-Host → DNS-Server	DNS-Abfragen
68	UDP	vSphere-Host → DHCP-Server	DHCP-Abfragen
80	TCP	Client → vSphere-Host	Browser Redirect to HTTPS (443)
88	TCP	vSphere-Host → AD-Server	Kerberos-AD-Authentifizierung
111	TCP/UDP	vSphere-Host → NFS-Server	NFS-Client
123	UDP	vSphere-Host → Time-Server	NTP-Client
162	UDP	vSphere-Host → SNMP-Collector	Senden von SNMP-Traps
389	TCP/UDP	vSphere-Host → LDAP-Server	Kerberos-AD-Authentifizierung
427	UDP	vSphere-Client → vSphere-Host	CIM Service Location Protocol
443	TCP	vSphere-Client → vSphere-Host	Managementverbindung vom Client zum Host
443	TCP	vSphere-Host → vSphere-Host	Provisionierung und Migration von Host zu Host

Tabelle 2.3 Ports für die vSphere-Host-Kommunikation

Port	Protokoll	Kommunikation	Beschreibung
445	UDP	vSphere-Host → MS Directory Service	AD-Authentifizierung
445	TCP	vSphere-Host → MS Directory Service	AD-Authentifizierung
445	TCP	vSphere-Host → SMB-Server	SMB-Verbindungen
514	TCP/UDP	vSphere-Host → Syslog-Server	Anbindung des Syslog-Servers
902	TCP/UDP	vSphere-Host → vCenter	vCenter-Server-Agent-Kommunikation
2049	TCP/UDP	vSphere-Host → NFS-Server	NFS-Datenport
3260	TCP	vSphere-Host → iSCSI-Storage	iSCSI-Datenport
5989	TCP	CIM Server → vSphere-Host	CIM-Transaktionen über HTTP
5989	TCP	vCenter → vSphere-Host	CIM-XML-Transaktionen über HTTPS
5989	TCP	vSphere-Host → vCenter	CIM-XML-Transaktionen über HTTPS
6500	UDP	vSphere-Host → vCenter	Kommunikation zum Syslog-Server
8000	TCP	vSphere-Host (Ziel-VM) → vSphere-Host (Quell-VM)	vMotion-Kommunikation über den VMkernel-Port
8000	TCP	vSphere-Host (Quell-VM) → vSphere-Host (Ziel-VM)	vMotion-Kommunikation über den VMkernel-Port
8100	TCP/UDP	vSphere-Host → vSphere-Host	Datenverkehr zwischen den Hosts für Fault Tolerance
8182	TCP/UDP	vSphere-Host → vSphere-Host	Datenverkehr zwischen den Hosts für vSphere-HA
8200, 8300	TCP/UDP	vSphere-Host → vSphere-Host	Datenverkehr zwischen den Hosts für Fault Tolerance
8301	UDP	vSphere-Host → vSphere-Host	DVS-Portinformationen
8302	UDP	vSphere-Host → vSphere-Host	DVS-Portinformationen

Tabelle 2.3 Ports für die vSphere-Host-Kommunikation (Forts.)

Das vCenter kommuniziert über das Netzwerk mit den Komponenten, die es verwaltet. Die Verbindungen werden über einen Windows-Dienst hergestellt (*vpxd.exe*, gilt nur für die installierbare Version, nicht für die Appliance). In Tabelle 2.4 sehen Sie, welche Ports für die Kommunikation benötigt werden.

Port	Protokoll	Kommunikation	Beschreibung
22	TCP/UDP	SSH-Client → vCenter	nur bei der vCenter Server Appliance relevant
25	TCP	vCenter → SMTP-Server	E-Mail-Benachrichtigungen
53	UDP	vCenter → DNS-Server	DNS-Abfragen
80	HTTP	Client-PC → vCenter	Dieser Port wird für den direkten Webzugriff benötigt. Es erfolgt aber nur eine Umleitung auf Port 443. Es können Konflikte mit einem installierten Microsoft IIS auftreten. (Vorsicht bei der Nutzung des Authentication Proxy!)
88	TCP/UDP	vCenter → AD-Server	Authentifizierung am Active Directory
135	TCP	vCenter → vCenter	vCenter-Linked-Modus
161	UDP	SNMP-Server → vCenter	SNMP-Polling
162	UDP	vCenter → SNMP-Server	Senden von SNMP-Traps
389	TCP/UDP	vCenter → Linked vCenter Server	Dieser Port wird für die Kommunikation mit dem LDAP benötigt.
443	TCP	vSphere-Client → vCenter	Port für die initiale Anmeldung über den vSphere-Webclient
443	TCP	vCenter → vSphere-Hosts	vCenter-Agent, DPM-Kommunikation mit HP ILO
514	UDP	vCenter → Syslog Collector	Syslog-Collector-Port
623	UDP	vCenter → vSphere-Hosts	DPM-Kommunikation via IPMI

Tabelle 2.4 Ports für die vCenter-Server-Kommunikation

Port	Protokoll	Kommunikation	Beschreibung
636	TCP	vCenter → Platform Services Controller	SSL-Verbindung zwischen den Komponenten beim Linked Mode
902	TCP	vCenter → vSphere-Hosts	Kommunikation zwischen vCenter und vSphere-Hosts
902	UDP	vCenter → vSphere-Hosts	Heartbeat-Kommunikation zwischen Hosts und vCenter
902	TCP/UDP	vSphere-Client → vSphere-Hosts	Anzeige der Konsole von VMs
1433	TCP	vCenter → MS SQL	Verbindung zum Datenbankserver MS SQL
1521	TCP	vCenter → Oracle	Verbindung zum Datenbankserver Oracle
2012	TCP	vCenter (Tomcat-Einstellungen) → SSO	Kontroll-Interface für SSO
2014	TCP	vCenter (Tomcat-Einstellungen) → SSO	RPC-Port für VMware Certificate Authority
2020	TCP/UDP	vCenter	Authentication Services Framework
5480	TCP	Client PC → vCenter	Zugriff auf die Webkonfigurationsseite der VCSA
5988	TCP	vSphere-Host → vCenter	CIM-Transaktionen über HTTP
6500	TCP/UDP	vCenter → vSphere-Host	Port für den ESXi Dump Collector
6501	TCP	vCenter → vSphere-Host	Port für den Auto-Deploy-Dienst
6502	TCP	vCenter → vSphere-Client	Port für das Auto-Deploy-Management
7500	UDP	vCenter → vCenter	Java-Port für den vCenter Linked Mode

Tabelle 2.4 Ports für die vCenter-Server-Kommunikation (Forts.)

Port	Protokoll	Kommunikation	Beschreibung
8000	TCP	vCenter → vSphere-Host	vMotion-Anfragen
8005	TCP	vCenter → vCenter	Port für die interne Kommunikation
8006	TCP	vCenter → vCenter	Port für die interne Kommunikation
8009	TCP	vCenter → vCenter	AJP-Port (Apache JServ Protocol); dient der Weiterleitung von Webserveranfragen an einen Applikationsserver
8080	HTTP	Client-PC → vCenter	Webservices über HTTP für die vCenter-Webseite
8083	TCP	vCenter → vCenter	interne Dienstediagnose
8085	TCP	vCenter → vCenter	interne Dienstediagnose/SDK
8086	TCP	vCenter → vCenter	Port für die interne Kommunikation
8087	TCP	vCenter → vCenter	interne Dienstediagnose
8443	HTTPS	Client-PC → vCenter	Webservices über HTTPS für die vCenter-Management-Webseite
8443	TCP	vCenter → vCenter	Port für den Linked Mode
9443	TCP	Client-PC → vCenter	Webclient-Zugriff
10109	TCP	vCenter → vCenter	Service-Management vom vCenter Inventory Service
10111	TCP	vCenter → vCenter	Linked-Mode-Kommunikation des vCenter Inventory Service
10443	TCP	vCenter → vCenter	vCenter Inventory Server Service über HTTPS

Tabelle 2.4 Ports für die vCenter-Server-Kommunikation (Forts.)

Auch das Single Sign On muss mit unterschiedlichen Elementen kommunizieren. Sie finden die Liste in Tabelle 2.5.

Port	Protokoll	Kommunikation	Bemerkungen
2012	TCP	vCenter (Tomcat) → SSO	RPC Control Interface
2014	TCP	vCenter (Tomcat) → SSO	PRC-Port für alle VMware-Certificate-Authority-APIs
7005	TCP	vCenter Server → SSO	–
7009	TCP	vCenter Server → SSO	AJP-Port
7080	TCP	vCenter Server → SSO	HTTP-Zugriff
7444	TCP	vCenter Server → SSO Webclient → SSO	HTTPS-Zugriff SSO-Lookup

Tabelle 2.5 Ports für die SSO-Kommunikation

In Tabelle 2.6 sehen Sie, welche Ports der Update Manager zur Kommunikation nutzt (* betrifft nur die Windows-basierte Version).

Ports	Protokoll	Kommunikation	Beschreibung
80	TCP	Update Manager → Internet	Download von Patches aus dem Internet
80	TCP	vSphere-Host → Update Manager	Kommunikation vom Host zum Update Manager
80	TCP	Update Manager → vCenter*	Kommunikation zwischen Update Manager und vCenter Server
443	TCP	Update Manager → Internet	Download von Patches aus dem Internet
443	TCP	vSphere-Host → Update Manager	Kommunikation vom Host zum Update Manager, Rückweg über 9084
443	TCP	vCenter → Update Manager*	Kommunikation vom vCenter zum Update Manager, Rückweg über 8084
735	TCP	Update Manager → VMs	Update-Manager-Listener-Port für das Patchen von VMs

Tabelle 2.6 Ports für die Update-Manager-Kommunikation

Ports	Protokoll	Kommunikation	Beschreibung
902	TCP	Update Manager → vSphere-Host	Übermittlung von Patches vom Update Manager zum vSphere-Host
1433	TCP	Update Manager → MS SQL*	Verbindung zum Datenbankserver MS SQL
1521	TCP	Update Manager → Oracle*	Verbindung zum Datenbankserver Oracle
8084	TCP	Update Manager → Client-Plug-in	SOAP-Server-Update-Manager
9084	TCP	vSphere-Host → Update Manager	Webserver-Update-Manager auf Updates wartend
9087	TCP	Update Manager → Client-Plug-in	Port für das Hochladen von Host-Update-Files
9000 → 9100	TCP	vSphere-Host → Update Manager	Ports für Hostscanning bzw. Bereich für Portalternativen, wenn 80 und 443 schon anderweitig genutzt werden

Tabelle 2.6 Ports für die Update-Manager-Kommunikation (Forts.)

Beim *vCenter Converter* werden unterschiedliche Ports genutzt. Diese hängen unter Umständen sogar davon ab, welches Betriebssystem importiert werden soll. In Tabelle 2.7 finden Sie die Ports, die für die Übernahme eines Servers benötigt werden.

Ports	Protokoll	Kommunikation	Bemerkungen
22	TCP	vCenter Converter → Source-Maschine	für die Konvertierung von Linux-basierten Systemen
137	UDP	vCenter Converter → Source-Maschine	für die Migration einer aktiven Maschine (wird nicht benötigt, wenn die Quelle kein NetBIOS nutzt)
138	UDP	vCenter Converter → Source-Maschine	
139	TCP	vCenter Converter → Source-Maschine	Kommunikation zwischen zur übernehmenden Maschine und vCenter Converter

Tabelle 2.7 Ports für die vCenter-Converter-Kommunikation

Ports	Protokoll	Kommunikation	Bemerkungen
443	TCP	vCenter Converter Client → vCenter Converter Server	Wird benötigt, wenn der vCenter-Converter-Linux-Client nicht auf dem vCenter-Converter-Server installiert ist.
443	TCP	vCenter Converter → vCenter	Dieser Port wird genutzt, wenn das Ziel ein vCenter ist.
443	TCP	vCenter Converter Client → vCenter	Wird benötigt, wenn der vCenter-Converter-Client nicht auf dem vCenter-Converter-Server installiert ist.
443, 902	TCP	Source-Maschine → vSphere-Host	Datentransport-Port für das Cloning zum vSphere-Host
445	TCP	vCenter Converter → Source-Maschine	Dient der Systemübernahme. Falls die Quelle NetBIOS nutzt, wird dieser Port nicht benötigt.
9089	TCP	vCenter Converter → Source-Maschine	Verteilung des Remote Agents

Tabelle 2.7 Ports für die vCenter-Converter-Kommunikation (Forts.)

Der *vRealize Orchestrator* (vRO) nutzt sehr viele Ports (siehe Tabelle 2.8). Um seine einwandfreie Funktion zu gewährleisten, müssen Sie diese Ports freischalten.

Port	Protokoll	Kommunikation	Bemerkungen
25	TCP	vRO-Server → SMTP-Server	E-Mail-Benachrichtigungen
80	TCP	vRO-Server → vCenter	Informationsaustausch über die virtuelle Infrastruktur
389	TCP/UDP	vRO-Server → LDAP-Server	LDAP-Authentifizierung
443	TCP	vRO-Server → vCenter	Informationsaustausch über die virtuelle Infrastruktur
636	TCP	vRO-Server → LDAP-Server	SSL-LDAP-Kommunikation zur Abfrage von Gruppenmitgliedschaften

Tabelle 2.8 Ports für die Orchestrator-Kommunikation

Port	Protokoll	Kommunikation	Bemerkungen
1433	TCP	vRO-Server → MS SQL	Kommunikation mit MS SQL
1521	TCP	vRO-Server → Oracle	Kommunikation mit Oracle-Datenbanken
3306	TCP	vRO-Server → MySQL	Kommunikation mit MySQL-Datenbanken
5432	TCP	vRO-Server → PostgreSQL	Kommunikation mit PostgreSQL-Datenbanken
8230	TCP	vRO-Client → vRO-Server	Lookup-Port – Kommunikation mit dem Konfigurationsserver
8240	TCP	vRO-Client → vRO-Server	Kommandoport – Kommunikation für Remoteaufrufe
8244	TCP	vRO-Client → vRO-Server	Datenport
8250	TCP	vRO-Client → vRO-Server	Messaging-Port – Weitergabe von Nachrichten im Java-Umfeld
8280	TCP	vRO-Server → vRO-Server	Kommunikation zwischen vRO-Server und Web-Frontend über HTTP
8281	TCP	vRO-Server → vRO-Server	Kommunikation zwischen vRO-Server und Web-Frontend über HTTPS
8281	TCP	vCenter → vRO-Server	Kommunikation zwischen vRO-Server und vCenter-API
8282	TCP	vRO-Client-PC → vRO-Server	HTTP-Server-Port
8283	TCP	vRO-Client-PC → vRO-Server	HTTPS-Server-Port
8286	TCP	vRO-Client-PC → vRO-Server	Java-Nachrichten-Port
8287	TCP	vRO-Client-PC → vRO-Server	SSL-gesicherter Java-Nachrichten-Port

Tabelle 2.8 Ports für die Orchestrator-Kommunikation (Forts.)

Weitere Informationen zu den Ports, die von VMware-Komponenten genutzt werden, finden Sie in einem recht übersichtlichen Dokument, das auf der VMware-Webseite liegt. Schauen Sie dort auf jeden Fall mal rein:

https://kb.vmware.com/s/article/2131180

2.8 Verschlüsselung

Sicherheitsaspekte spielen eine immer größere Rolle. Datentransfers müssen abgesichert werden, Datenbanken und auch komplette virtuelle Maschinen werden aus Sicherheitsgründen verschlüsselt.

Damit VMs sicher verschlüsselt werden können, wird eine zugehörige Infrastruktur benötigt. Mit vSphere 7.0 hat VMware noch einmal nachgerüstet. Der Fokus lag auf einer sicheren Kette zur Bereitstellung von Zertifikaten und der Unterbindung von Möglichkeiten der Manipulation.

Für die Umsetzung hat VMware die *vSphere Trust Authority* (vTA) implementiert. Darüber werden vertrauenswürdige Cluster zur Verfügung gestellt, auf denen dann verschlüsselte VMs laufen können. Die Kommunikation erfolgt über das KMIP-Protokoll (*Key Management Interoperability Protocol*). Das vCenter dient für dieses Thema quasi als Passthrough-Komponente. Dabei ist die vTA ein dedizierter vSphere-Cluster, der nur für die Sicherheit verantwortlich ist und keine Workloads aufnimmt. Aus diesem Grund können diese Systeme auch vSphere-Hosts mit wenigen Ressourcen sein.

Hinweis

Für die einwandfreie Funktion müssen in den Hosts TPM-Chips (*Trusted Platform Module*) verbaut sein. Zusätzlich muss auf dem Server UEFI Secure Boot aktiviert sein.

Die Anzahl der Administratoren auf den vTA sollte auf jeden Fall eingeschränkt werden.

Der vTA fallen dabei unterschiedliche Aufgaben zu – die vTA holt die Schlüssel ab, der KMS-Server liefert sie aus. Damit kann jetzt auch das vCenter verschlüsselt werden.

Die Attestierung von Hosts gehört ebenfalls zu der Aufgabe der vTA. Bekommt ein Host dieses Testat nicht, werden auch keine verschlüsselten Workloads auf ihn verschoben (siehe Abbildung 2.23).

Hinweis

Es muss nicht für jeden Workload-Cluster ein dedizierter vTA-Cluster aufgebaut werden.

Aus Sicherheitsgründen empfiehlt VMware für den vTA-Cluster ein dediziertes vCenter, aus Supportsicht muss das aber nicht sein.

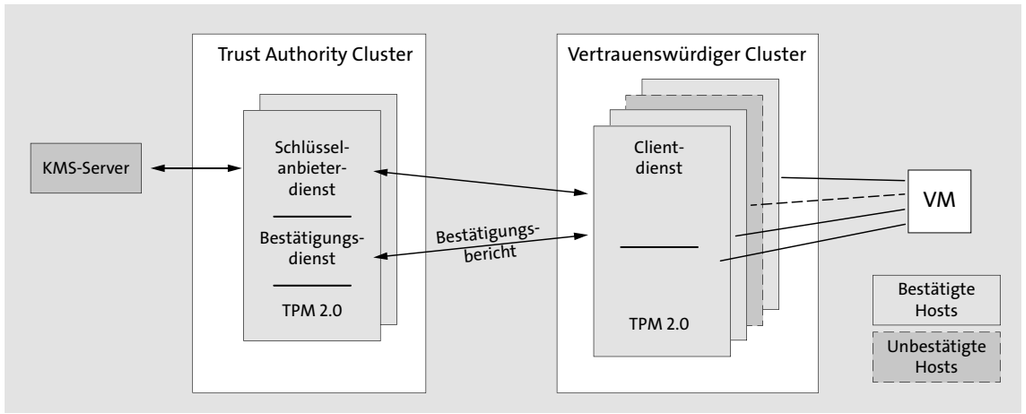


Abbildung 2.23 vSphere Trust Authority Cluster

Die Status- bzw. Konfigurationsdaten werden in Datenbanken auf dem vCenter Server und dem vSphere-Host abgelegt.

Teile der Infrastruktur wurden schon mit vSphere 6.7 eingeführt, aber das System hatte noch ein paar Schwächen. So konnte ein sicherer Workload durch DRS auf einen unsicheren Host verschoben werden. Hinzu kommt die Tatsache, dass der vCenter Server nicht verschlüsselt werden konnte, weil er ja die Schlüssel bereitgestellt hat. Jetzt hält der vTA die Schlüssel, und damit ist auch das vCenter verschlüsselbar.

2.9 Maximale Ausstattung

Auch wenn Sie sich an die *Hardware Compatibility List* (HCL) halten, so müssen Sie doch wissen, welche Ausstattung des Hosts mengenmäßig noch unterstützt wird. Diesen Punkt möchten wir in den folgenden Tabellen näher aufschlüsseln.

In Tabelle 2.9 finden Sie die maximalen Werte für die CPUs; Tabelle 2.10 enthält den maximalen Wert für den Arbeitsspeicher.

CPUs pro Host	Anzahl	Bemerkungen
Logische Prozessoren	768	Die Anzahl berechnet sich wie folgt: Sockel × Cores × Threads
Virtuelle CPUs (vCPUs)	4.096	–
NUMA-Knoten pro Host	16	–

Tabelle 2.9 Maximale CPU-Werte

CPUs pro Host	Anzahl	Bemerkungen
Maximale Anzahl von virtuellen CPUs pro Core	32	Die Anzahl ist abhängig von der Last, die die VMs verursachen. (Gilt ebenfalls für *vSphere 4.0 Update 1*; bei *vSphere 4.0* sind es 20 vCPUs.)
Maximale Anzahl von VMs pro Host	1.024	Die Anzahl ist abhängig von der Last, die die VMs verursachen.

Tabelle 2.9 Maximale CPU-Werte (Forts.)

Memory pro Host	Menge
Arbeitsspeicher	16 TB

Tabelle 2.10 Maximaler Memory-Wert

Angesichts der Menge der Karten geben wir in der Tabelle für die Netzwerkkarten nur die Geschwindigkeit und die Anzahl der möglichen Karten an. In Tabelle 2.11 finden Sie die maximale Anzahl von physischen Netzwerkkarten.

Speed	Anzahl
1 GBit	32
10 GBit	16
20 GBit	16
25 GBit	16
40 GBit	8
50 GBit	8
100 GBit	4
100/10 GBit 1 GBit	16 16

Tabelle 2.11 Maximale Anzahl physischer Netzwerkkarten

Tabelle 2.12 listet dagegen die maximale Anzahl der *virtuellen* Karten bzw. Ports auf.

PCI VMDirectPath	Anzahl
PCI VMDirectPath Devices (pro Host)	8
PCI VMDirectPath Devices (pro VM)	4
vNetzwerk-Standard-Switch	**Anzahl**
Virtuelle Switch-Ports pro vSwitch	4.096
Portgruppen pro vSwitch	512
Portgruppen pro Host	512
vNetzwerk-Distributed-Switch	**Anzahl**
Virtuelle Switch-Ports pro vCenter	60.000
Hosts pro Switch	1.000
VDS pro vCenter	128
vNetzwerk	**Anzahl**
Maximal aktive Ports pro Host	1.016
Virtuelle Switch-Ports gesamt	4.096

Tabelle 2.12 Maximale Anzahl virtueller Karten bzw. Ports

In Tabelle 2.13 finden Sie die maximale Anzahl von parallelen vMotion-Operationen.

Parallele vMotion-Operationen pro Host	Anzahl
1-GBit-Netzwerk	4
10-GBit-Netzwerk	8

Tabelle 2.13 Maximale Anzahl von parallelen vMotion-Operationen

Für den Storage gibt es ebenfalls Einschränkungen. Tabelle 2.14 trennt die verschiedenen Anbindungsmöglichkeiten voneinander und beschreibt außerdem das Filesystem VMFS.

VMFS allgemein	Maximalwert
Volume-Größe	64 TB
vDisks pro Host	2.048

Tabelle 2.14 Maximalwerte im Storage-Umfeld

VMFS allgemein	Maximalwert
Volumes per Hosts	1.024
Hosts pro Volume	64
VMFS-5/6	**Maximalwert**
Files pro Volume	ca. 130.690
Filegröße	62 TB
Blockgröße	1 MB; bei einer Migration von VMFS-3 wird die alte Blockgröße übernommen.
RDM-Größe (virtuelle Kompatibilität)	62 TB
RDM-Größe (physische Kompatibilität)	64 TB
Fibre-Channel	**Maximalwert**
LUNs pro Host	1.024
Anzahl Pfade pro LUN	32
Maximale Anzahl pro Host	1.024
HBAs pro Host	8
Maximale Anzahl von HBA-Ports	16
FCoE	**Maximalwert**
Maximale Anzahl von SW-Adaptern	4
NFS	**Maximalwert**
Maximale Anzahl von NFS-Datastores	256
Hardware-iSCSI-Initiator	**Maximalwert**
LUNs pro Host	1.024
Pfade pro Host	4.096
Pfade pro LUN	8
Software-iSCSI-Initiator	**Maximalwert**
Ziele pro Host	256

Tabelle 2.14 Maximalwerte im Storage-Umfeld (Forts.)

Kapitel 17

Datensicherung von vSphere-Umgebungen

In diesem Kapitel lernen Sie die Möglichkeiten zur Datensicherung und -wiederherstellung von VMware-vSphere-Umgebungen kennen. Für Leser, die Produkte von Drittherstellern einsetzen, bietet das Kapitel eine Einführung in die Datensicherung und -wiederherstellung auf konzeptioneller Ebene. Darüber hinaus wird eines der beliebtesten Backup-Tools, Veeam Backup & Replication, vorgestellt.
Autor dieses Kapitels ist Florian Klotmann, florian@klotmann.net.

17.1 Einführung

Neben der Hochverfügbarkeit und dem Wiederanlauf im Katastrophenfall gehört auch die Datensicherung zur *IT Business Continuity*. Dieses Kapitel widmet sich dem Thema *Datensicherung*, das heißt, wir befassen uns mit dem Sichern der Daten von Applikationen, aber auch mit dem Sichern infrastruktureller Komponenten wie dem Gastbetriebssystem. Darüber hinaus werden Konzepte zum Wiederanlauf aus Sicht der Datensicherung behandelt.

Wir verwenden in diesem Kapitel den *vSphere Web Client* als Grundlage für sämtliche Schritte im vCenter.

Grundsätzliches zu Soft- und Firmwareversionen

Die in diesem Kapitel vorgestellten Produkte beziehen sich auf folgende Release-Stände:

Veeam Backup & Replication 10.0.1.4854 (kompatibel zu vSphere 7)

Neuere Releases können Erweiterungen und Änderungen mit sich bringen, die in diesem Kapitel getroffene Aussagen überholt erscheinen lassen.

Darüber hinaus haben wir die Bebilderung dieses Kapitels »en bloc« durchgeführt. So können Sie in den Abschnitten 14.8 bis 14.10 den Bildern wie in einem Installations- und Konfigurations-Guide folgen.

17.1.1 Allgemeines zur Datensicherung

VMware vSphere bietet verschiedene Optionen für die Datensicherung und -wiederherstellung in virtuellen Umgebungen.

Bevor Sie eine Datensicherung Ihrer virtuellen Umgebung tätigen, sollten Sie Richtlinien definieren. Diese wiederum beruhen auf den *Service Level Objectives* (SLO) Ihres angebotenen Diensts (beispielsweise einer E-Mail-Applikation wie *Microsoft Exchange*). Dabei ist es von Vorteil, mit den Begriffen und Kürzeln aus Tabelle 17.1 vertraut zu sein.

Kürzel	Begriff	Erklärung
RPO	*Recovery Point Objective*	Wiederherstellungspunkt: Wie viel Datenverlust darf der Dienst maximal haben?
RTO	*Recovery Time Objective*	Wiederherstellungszeit: Wie schnell muss der Dienst wieder verfügbar sein?
RT	*Retention Time*	Aufbewahrungszeit: Wie lange muss eine einzelne Datensicherung eines Diensts aufbewahrt werden? Das kann auch rechtliche Aspekte beinhalten, die bedacht werden müssen.
RP	*Retention Points*	Sicherungspunkte: Wie viele einzelne Datensicherungen sollen vorliegen? Bei einer Sicherung alle zwei Tage sowie sieben Retention Points hätte man damit Sicherungen bis zu einem Alter von zwei Wochen.
GFS	*Grandfather-Father-Son*	Soll eine Sicherung in unterschiedliche Aufbewahrungszeiten aufgeteilt werden? Damit können zum Beispiel Wochen- und Monatssicherungen länger als Tagessicherungen vorgehalten werden.
	Datensicherungsgenerationen	Wie viele Kopien eines Dienstes müssen vorgehalten werden?
	Häufigkeit der Datensicherung	Wie oft müssen die Daten des Dienstes gesichert werden?
	Änderungsrate	Wie groß ist die Datenmenge, die sich pro Zyklus ändert? (Hier geht es um die effektiv neu geschriebenen Datenblöcke.)
	Datensicherungsschema	Auf welche Art muss die Datensicherung erfolgen (vollständige, inkrementelle, differenzielle Sicherung)?

Tabelle 17.1 Begriffe der Datensicherung

Die Werte, die Sie aus den Objectives in Tabelle 17.1 ableiten, entscheiden sowohl über die Wahl der *Datensicherungsmethoden* als auch über die zugrunde liegende *infrastrukturelle Architektur*. Je nach den Möglichkeiten der Plattformen, die Sie einsetzen, gibt es herstellerspezifische Unterschiede. Dieses Kapitel konzentriert sich auf die VMware-eigenen Technologien.

17.1.2 Die zwei Typen der Datensicherung

Prinzipiell unterscheidet man zwischen zwei Typen der Datensicherung:

- **Logische Datensicherung** – eine vom Primärspeicher-Volume abhängige Kopie, beispielsweise *VMware Snapshot*
- **Physische Datensicherung** – eine vom Primärspeicher-Volume unabhängige Kopie, beispielsweise *VMware Clone*

Logische Datensicherung

Eine *logische Datensicherung* legt ein Point-in-Time-Abbild (*Snapshot*, *Klon*, *Replikation*) einer virtuellen Maschine, eines VMFS-Datastores, einer LUN oder eines Dateisystems an. Logische Datensicherungen erfolgen sehr schnell und nutzen die Speicherkapazität im *Primärspeichersystem* oder in dessen Replikat. Die Wiederherstellung der Daten aus einer logischen Datensicherung geschieht sehr schnell im Vergleich zu Datensicherungen auf Sekundärspeichersystemen. Das hängt direkt mit den IT-Prozessen (*Standard Operating Procedures*) zur Restaurierung der Daten sowie von der verwendeten Technologie ab. Die logische Datensicherung ermöglicht eine kurze Wiederanlaufzeit eines Dienstes oder – was weitaus üblicher ist – die Wiederherstellung einzelner Dateien. Logische Datensicherung schützt Sie beispielsweise vor korrupten virtuellen Maschinen oder versehentlich gelöschten Dateien innerhalb der VMs.

Physische Datensicherung

Im Gegensatz zur logischen Datensicherung erstellen Sie bei der *physischen Datensicherung* eine vollständige, unabhängige Kopie einer virtuellen Maschine, eines VMFS-Datastores, einer LUN oder eines Dateisystems. Das gibt Ihnen die Möglichkeit, diese Kopie in einem anderen Speichersystem abzulegen, um auch bei beispielsweise einem Hardwaredefekt des Primärspeichers abgesichert zu sein. Dabei kann dies traditionell in einer Bandbibliothek oder einem zusätzlichen Speichersystem erfolgen. Hier gibt es (wie im Verlauf dieses Kapitels beschrieben) via *Veeam Backup & Replication* die verschiedensten Möglichkeiten, um dieses Szenario abzubilden.

Nachteilig wirken sich der Speicherkapazitätsbedarf und die längere Laufzeit der Datensicherung aus. Moderne Datensicherungstechnologien erlauben es, sowohl den Kapazitätsbedarf (Komprimierung oder Deduplizierung der Daten) als auch ihre Laufzeit (quellbasierte Deduplizierung) zu optimieren.

Ein weiteres Einsatzgebiet, das physische Datensicherungen oder eigenständige Zweitkopien erfordert, sind gesetzliche Vorgaben, wie sie beispielsweise das Handelsgesetzbuch in Deutschland oder die Geschäftsbücherverordnung in der Schweiz zur Aufbewahrung digitaler Daten vorschreiben. Damit ist auch immer eine Mindestaufbewahrungsfrist (*Retention Time*) dieser Daten verknüpft.

17.1.3 Stufenweises Datensicherungskonzept

Bei der gleichzeitigen Nutzung von logischer und physischer Datensicherung spricht man von einem *stufenweisen Datensicherungskonzept*.

Es ist daher durchaus eine Best Practice, sowohl die physische wie auch die logische Datensicherung für einen Dienst einzusetzen, um ein SLO (*Service Level Objective*) vollständig abzudecken. Ein SLO kann durchaus auch nach Lösungen zur Disaster-Vorsorge verlangen.

Bei einem Systemausfall (beispielsweise einer VM) oder bei Datenverlust empfiehlt es sich immer – vorausgesetzt, die Datenkonsistenz ist gemäß SLO gegeben –, auf diejenige Sicherungskopie zurückzugreifen, von der aus die Wiederherstellung am schnellsten erfolgt (Beispiel: Snapshot vom Primärspeichersystem).

Tabelle 17.2 fasst die verschiedenen Stufen samt ihrer Vor- und Nachteile zusammen.

Art der Sicherung	Vorteil	Nachteil
Snapshot, Clone (logisch)	schnelle Wiederherstellung	keine Sicherheit vor Primärspeichersystem-, Standort- oder Zweitspeichersystemausfall
Datensicherung auf Zweitspeichersystem (physisch)	schnelle Wiederherstellung	kein Schutz vor Standort- oder Zweitspeichersystemausfall
Replikation (logisch)	schneller Wiederanlauf bei Standort- oder Primärspeichersystemausfall	hohe Kosten für den Zweitstandort
Datensicherung an Zweitstandort (physisch)	Sicherung gegen Standortausfall	langsamere Wiederherstellung, Kosten für den Zweitstandort

Tabelle 17.2 Stufenweises Konzept zur Datensicherung

Typischerweise werden Sie aufgrund der schnellen Wiederherstellungszeit häufiger logische Datensicherungen durchführen als physische. Die logische Datensicherung kann aber die physische Datensicherung keinesfalls ersetzen, weil sie weder Schutz vor einem Systemausfall (logischer oder physischer Natur) noch vor einen Medienbruch (Datenspeicherung auf einem Zweitsystem oder anhand eines anderen Speichermodells) bietet.

Die logische Datensicherung (Snapshot) ist in Kapitel 8 und in Abschnitt 20.19, »Snapshots«, ausführlich beschrieben.

17.2 Grundlagen der Datensicherung

Bei der Datensicherung treffen Sie immer wieder auf die Begriffe, die in Tabelle 17.3 aufgelistet sind.

Begriff	Beschreibung
Sekundärspeichersystem	Dedizierter Speicher als Zielsystem der Datensicherung. Dieses kann auf Festplatten, Bändern, optischen Medien oder auf einer Kombination daraus basieren.
Full Backup	Vollständige Datensicherung eines Systems, einer Datenbank oder einer Applikation.
Active Full	Vollständige Datensicherung, die ausschließlich anhand aller Daten des zu sichernden Objekts erstellt wird.
Synthetic Full	Synthetische, vollständige Datensicherung. Diese wird aus dem letzten *Full Backup* und den inkrementellen oder differenziellen Datensicherungspunkten zusammengestellt.
Incremental Backup	Inkrementelle Datensicherung, ausgehend von dem Datensicherungspunkt, der zuletzt erstellt wurde.
Differential Backup	Differenzielle Datensicherung, ausgehend vom letzten *Full Backup*.
Incremental Forever	Als Erstes wird ein *Active Full*-Backup eines Systems, einer Datenbank oder einer Applikation angelegt, anschließend folgen nur noch inkrementelle Datensicherungen über den gesamten Lebenszyklus.
Image-Level	Es wird die gesamte virtuelle Maschine oder es werden einzelne virtuelle Festplatten gesichert. Die *VMware Tools* werden benötigt, um eine konsistente Sicherung zu gewährleisten. (Dabei werden kurzzeitig Schreibvorgänge auf dem Dateisystem blockiert.)

Tabelle 17.3 Begriffe der Datensicherung

Begriff	Beschreibung
File-Level	Die Datensicherung geschieht auf Dateisystemebene innerhalb eines Gastbetriebssystems und benötigt einen Agenten. Dabei greifen die meisten Sicherungsprogramme auf die *VMware Tools* zurück und/oder ergänzen diese mit eigenen Agenten, wie das zum Beispiel auch hier bei *Veeam Backup & Replication* möglich ist.
Application-Level	Die Datensicherung erfolgt innerhalb des Gastbetriebssystems und sichert wahlweise entweder die gesamte Applikation und Datenbank oder einzelne Instanzen. Dafür wird ein spezieller Agent benötigt.
Changed Block Tracking	Inkrementelle Image-Level-Datensicherung, die auf den Datenblöcken basiert, die während eines Datensicherungsintervalls geändert wurden (siehe auch Abschnitt 17.4.3).
Deduplikation	Bei der Deduplikation von Daten werden Datensätze in kleine Einheiten variabler oder fixer Länge zerlegt, anschließend werden doppelt vorkommende identische Einheiten gelöscht.
Quellbasierte Deduplikation	Die Deduplikation geschieht im Gastbetriebssystem, in der Applikation oder in einem Datensammler (Proxy-System), bevor die Daten über ein Netzwerk zum Sekundärspeichersystem gesendet werden.
Zielbasierte Deduplikation	Die Deduplikation der Daten erfolgt direkt im Sekundärspeichersystem.

Tabelle 17.3 Begriffe der Datensicherung (Forts.)

Wenn es um die Wiederherstellung von Daten geht, ist das Full Backup natürlich die wichtigste Komponente aller Datensicherungspunkte. Dank der inkrementellen und differenziellen Sicherungspunkte sind täglich oder mehrmals am Tag Backups möglich, ohne ein zu großes Zeitfenster dafür einrechnen zu müssen. Außerdem kann dadurch viel Speicherplatz im Sekundärspeichersystem eingespart werden, da nicht in jedem Sicherungspunkt alle Daten des gesicherten Objekts vorhanden sind. Dabei gibt es leider durch die Nutzung der inkrementellen oder differenziellen Sicherungen auch einen Nachteil: Je nach gewünschtem Stand der Daten werden im Fall einer Wiederherstellung nicht nur das Full Backup, sondern auch die inkrementellen oder differenziellen Daten benötigt, die zusätzlich zurückgespielt werden müssen.

Die Methode *Synthetic Full* ist sehr nützlich, da sie es erlaubt, Daten ab dem ersten *Full Backup* nur noch inkrementell zu sichern und so für die Datensicherung eingeplante Zeitfenster trotz Datenwachstums einzuhalten. Die Sicherungsapplikation generiert anhand der

Daten des letzten *Full Backups* (egal ob synthetisch oder nicht) und der darauffolgenden inkrementellen Sicherungen periodisch Vollkopien, die sich entsprechend schnell wiederherstellen lassen.

17.2.1 Deduplikation

Sehr vielversprechend ist die Kombination von *Changed Block Tracking* und quellbasierter Deduplikation.

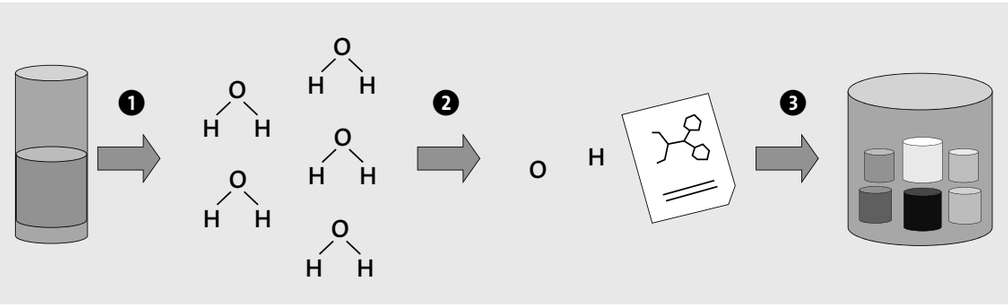


Abbildung 17.1 Schematische Darstellung einer Deduplikation

Abbildung 17.1 zeigt, wie Deduplikation vom Prinzip her funktioniert:

❶ Aufbrechen der Daten in ihre Atome.

❷ Einmaliges Senden und Speichern dieser Atome.

❸ Das führt zu einer massiven Reduktion an gespeicherten Daten.

Dabei hängt die tatsächliche Datenreduktion von der Beschaffenheit der Daten ab. Viele ähnliche oder sogar gleiche Daten reduzieren sich massiv. Hingegen reduzieren sich signifikante Daten, z. B. verschiedene Fotos derselben Landschaft, nur wenig.

Diese Deduplikation kann an der Quelle, also im Gastsystem, auf dem ESXi-Server unter Verwendung des DD-Boost-Protokolls oder am Ziel stattfinden. Im virtuellen Umfeld ist die quellbasierte Deduplikation am effizientesten. Sie profitiert davon, dass nur die eindeutigen Datensegmente sämtlicher auf einem ESXi-Server laufender VMs gesendet werden. Dort wiederum werden lediglich die eindeutigen Datensegmente sämtlicher VMs gespeichert, die in unserem Beispiel durch *Veeam Backup & Replication* geschützt sind.

17.2.2 Medien zur physischen Datensicherung

Datensicherung und Archivierung bilden in der IT-Infrastruktur eine Ausnahme, was die Speichermedien betrifft. Im Primärspeicherbereich werden ausschließlich Festplatten bzw. Flash-Speicher verwendet. Mannigfaltiger präsentiert sich die Situation der verwendeten

Medien im Bereich der Datensicherung. Da finden Sie Bänder, optische Medien, Festplatten und sogar auch Flash-Speicher. Aber am häufigsten treffen Sie wohl immer noch Bandbibliotheken an. Ausschließlich festplattenbasierte Speichersysteme werden jedoch immer populärer.

Bänder sind sehr günstige Medien, was Anschaffung, Betrieb (Strom- und Kühlungskosten) und den Transport (Auslagerung zur Disaster-Vorsorge) betrifft. Ihre Nachteile sind der enorm arbeitsintensive und auch zeitliche Aufwand bei der Administration sowie der Datenwiederherstellung, ihre Unzuverlässigkeit in Sachen Datenkonsistenz sowie eine mangelhafte Validierung der Datenintegrität.

Festplatten sind vergleichsweise teuer in der Anschaffung und im Betrieb, obwohl Technologien wie Deduplikation dem entgegenwirken. Sie eignen sich nicht zum Transport und erfordern zur Disaster-Vorsorge entweder den Betrieb eines zweiten Rechenzentrums, die Erstellung von Bandkopien zur Auslagerung oder eine Cloud-basierte Lösung. Ihre Vorteile liegen in der schnellen Wiederherstellung, der kontinuierlichen Überprüfung der Integrität und in der Möglichkeit, Daten durch deren Wiederherstellung zu validieren (Sandbox) oder anderweitig für Tests zu verwenden.

17.2.3 Datenkonsistenz von VMs, Datenbanken und Applikationen

Damit Sie Daten erfolgreich wiederherstellen können, müssen die Daten konsistent sein. Man unterscheidet drei Arten von Datenkonsistenz:

- **Inkonsistente Datensicherung oder korrupte Daten:** Das wäre z. B. ein auf Band gesicherter unleserlicher Datenbestand. Diese unerwünschte Form wird hier nur der Vollständigkeit halber aufgeführt. Sie wird nicht weiter erläutert.
- **Absturzkonsistente Datensicherung:** Hierbei handelt es sich um eine Sicherung einer virtuellen Maschine ohne Agenten oder Applikations-Plug-ins.
- **Applikationskonsistente Datensicherung:** Dies ist die Sicherung einer Applikation innerhalb einer virtuellen Maschine mittels Agenten oder Plug-in.

Absturzkonsistente Datensicherung

Unter einer absturzkonsistenten Datensicherung logischer oder physischer Natur versteht man die agentenfreie Sicherung einer virtuellen Maschine oder eines gesamten *VMFS-Datastores*. Eine absturzkonsistente Datensicherung kommt bei virtuellen Maschinen ohne geschäftskritische Applikationen und Datenbanken zur Anwendung oder dann, wenn es keinen spezifischen, produktabhängigen Datensicherungsagenten gibt. In vielen Anwendungsfällen genügt diese Art der Datensicherung. Dabei wird vorausgesetzt, dass die *VMware Tools* installiert sind und dass die Sicherungsapplikation oder der Sicherungsvorgang den *VSS Provider* oder den *File System Sync Driver* ansprechen kann. Beide können die Schreibvorgänge des Dateisystems eines unterstützten Gastbetriebssystems kurzfristig stilllegen, um eine

konsistente Datensicherung auf Basis der virtuellen Maschine zu ermöglichen (man spricht dann von *VM-konsistenter Sicherung*).

Applikationskonsistente Datensicherung

Von einer *applikationskonsistenten Datensicherung* ist die Rede, wenn der Datenzugriff auf die Applikation oder auf die angebundene Datenbank zum Zweck der Sicherung kurzfristig stillgelegt wird. Dazu brauchen Sie spezielle Software in Form von Datensicherungsagenten (beispielsweise *VMware Tools*) oder *Plug-ins*. Sollte eine Applikation nicht von der eingesetzten Software unterstützt werden, bietet sich alternativ ein Skript oder ein manueller Eingriff an, der die Applikationsdienste stoppt. VMware Tools bieten eine Integration in die *Microsoft Shadow Copy Services*. Diese wiederum erlauben das kurzzeitige Einfrieren eines *Microsoft SQL*-Datenbankdiensts. Das Zusammenspiel der beiden Technologien ermöglicht die Erstellung einer applikations- bzw. datenbankkonsistenten Datensicherung.

Traditionell werden auch heute noch oft geschäftskritische Applikationen für eine kurze Weile bis hin zu einer längeren Zeit stillgelegt, damit diese Daten konsistent gesichert werden können. Mit zunehmenden Datenmengen und immer geringer werdenden Datensicherungsfenstern – wenn noch vorhanden – ist diese Methode zusehends unpraktikabel. Abhilfe bieten dabei *Changed Block Tracking* (CBT) in Verbindung mit *quellbasierter Deduplikation* oder auch Snapshots.

Veeam Backup & Replication verfügt über unterschiedliche Datensicherungsagenten für (auf Windows-basierten Servern laufende) Applikationen wie zum Beispiel *Exchange*, *SQL*, *Oracle* und *SharePoint*, um nur einige zu nennen. Diese sind in der Software direkt selbst enthalten und werden bei Bedarf und entsprechender Lizenzierung aktiviert. Dabei wird die Applikation nur so lange stillgelegt, bis ein VMware-Snapshot erstellt wurde. Dieser Vorgang sollte (je nach Ausgangslage) dabei im Regelfall wenige Sekunden bis hin zu wenigen Minuten dauern, wodurch die Dauer der Stilllegung der Applikation so gering wie möglich gehalten wird.

17.2.4 Sicherung von mehrschichtigen Applikationen oder vApps

Im Aufbau komplexerer virtueller Maschinen oder vApps mit definierten *Anti-Affinity*-Richtlinien zur Lastverteilung auf unterschiedliche VMFS-Datastores gestalten sich die absturzkonsistenten Datensicherungen ungleich schwieriger. Hier scheitern Sie mit der erwähnten Methode eines Point-in-Time-Abbilds oder eines Klons der betroffenen VMFS-Datastores. Beispiele solcher Applikationen sind:

- *Microsoft Exchange*: Clientzugriff- und Postfachserver
- *Microsoft SharePoint*: Web-Frontend- und Backend-Datenbankserver
- *Webapplikationen*: Web- und Datenbankserver

Consistency Groups

Einige Speichersystemhersteller bieten zur Abbildung solcher Datensicherungsszenarien sogenannte *Consistency Groups* (CG), die mehrere *VMFS-Datastores* zu einer logischen Einheit zusammenfassen. Eine CG erlaubt das kurzfristige simultane Einfrieren (Sperren der Schreibvorgänge mehrerer VMFS-Datastores bzw. LUNs) zum Zweck einer konsistenten Datensicherung. Die absturz- sowie applikationskonsistente Datensicherung bedient sich desselben Mechanismus auf Ebene des Primärspeichersystems. Von diesem profitieren sowohl die logische als auch die physische Datensicherung.

Erkundigen Sie sich beim Hersteller, ob das in Ihrer Firma eingesetzte Speichersystem und gegebenenfalls die Datensicherungssoftware diese Funktion unterstützen.

17.3 Die fünf Prinzipien einer konsequenten Datensicherung

Eine konsequent durchgeführte Datensicherung verfolgt die Prinzipien eines *Medienbruchs*, der *Datenkopien*, einer *Indexierung* und Prüfung (*Validierung*) sowie auf organisatorischer Ebene der *Funktionstrennung*.

17.3.1 Medienbruch

Beim Medienbruch unterscheidet man den logischen vom physischen Typ. (Früher verstand man darunter meistens die Sicherung auf Band. Mittlerweile werden auch andere Medien genutzt.)

- **Logischer Medienbruch:** Eine Datensicherungsapplikation sichert Daten in einen dedizierten Bereich. Beispiel: Sie verwenden *Veeam Backup & Replication* mit einem *VMFS-Datastore*, der auf einem Primärspeichersystem im dedizierten Plattenbereich liegt. Die Vorteile sind: Verwaltung einer Speichersysteminfrastruktur und bessere Kapazitätsauslastung des Systems. Der Nachteil ist ein mittleres Risiko beim Release-Management und bei einem potenziellen Systemausfall.
- **Physischer Medienbruch:** Die Datensicherungsapplikation sichert Daten auf ein dediziertes System. Beispiel: *Veeam B&R* speichert Daten in ein dediziertes Sekundärspeichersystem. Der Vorteil ist ein geringes Risiko beim Release-Management, da für das Primär- und das Sekundärspeichersystem unterschiedliche Technologien sowie getrennte Systeme zum Einsatz kommen. Der Nachteil ist, dass zwei unterschiedliche Komponenten in der Speichersysteminfrastruktur verwaltet werden müssen, was mit höheren Kosten und Aufwänden verbunden ist.
- **Kein Medienbruch:** Die Datensicherungsapplikation verwaltet das Erstellen von Snapshots, Klonen oder replizierten Datenkopien. Die Vorteile sind die native Integration im Primärspeichersystem, bessere Kapazitätsauslastung des Systems und eine schnelle

Datenwiederherstellung. Der Nachteil ist ein hohes Risiko beim Release-Management; bei Snapshots kommt die Abhängigkeit von den Primärvolumes hinzu. Außerdem kann ein Systemausfall oder Datenkorruption einzelner Primärvolumes zum Verlust intakter Kopien führen.

17.3.2 Datenkopien

Datenkopien können Sie in mannigfaltiger Weise erstellen, entweder auf dem Primärspeicher oder auf anderen Speichersystemen. Auch die Datenträger können unterschiedlicher Art sein, wie Festplatten, Bänder oder optische Medien. Wie in Abschnitt 17.1.2 erläutert wurde, unterscheidet man zwischen logischer und physischer Datensicherung. Ein entscheidender Faktor bei der Wahl der einzusetzenden Technologien ist die Aufbewahrungsfrist der Daten. Diese kann auch gesetzlich reguliert sein. Es ist durchaus gängige Praxis, gleichzeitig die logische und die physische Datensicherung zu nutzen. Die Kosten, die aufgrund des Speicherbedarfs einer Kopie entstehen, sind dabei nicht zu unterschätzen.

Die populärsten Technologien der logischen Datensicherung sind:

- **Snapshot einer VM**
  Vorteile: Granularität auf Ebene einer VM, sehr schnelle Datensicherung und -wiederherstellung, VM-konsistent und mit VMware Tools unter Windows dateisystemkonsistent.

  Nachteile: Hoher Verwaltungsaufwand, höhere Kosten der benötigten Speicherkapazität im Vergleich zu einem Sekundärspeichersystem, bei längerer Vorhaltezeit spürbar abnehmende Performance der virtuellen Maschine.
- **Snapshot einer VM oder .vmdk-Datei (VVol-Datastores)**
  Vorteile: Granularität auf Ebene einer VM oder virtuellen Festplatte (*.vmdk*-Datei), schnelle Datensicherung und -wiederherstellung, VM-konsistent. Transparenz im Storage-Container und VVol-Datastore.

  Nachteile: Hoher Verwaltungsaufwand, Abhängigkeit von der produktiven VM. Höhere Kosten der benötigten Speicherkapazität im Vergleich zu einem Sekundärspeichersystem.
- **Snapshot eines Datastores (LUN, Dateisystem)**
  Vorteile: Schnelle Datensicherung und -wiederherstellung, VM-konsistent.

  Nachteile: Granularität und Indexierung der Datensicherung auf Ebene eines Datastores (kann bei *Storage DRS* oder *Storage vMotion* zu Inkonsistenzen in der Datensicherung führen), Abhängigkeit vom produktiven Datastore. Höhere Kosten der benötigten Speicherkapazität im Vergleich zu einem Sekundärspeichersystem.
- **Snapshot eines RDM (LUN)**
  Vorteile: Hohe Granularität, schnelle Datensicherung und -wiederherstellung, applikationskonsistent.

  Nachteil: Hoher Verwaltungsaufwand, eingeschränkt auf spezielle Agenten für Applikationen im Gastbetriebssystem, Abhängigkeit vom produktiven Datastore. Höhere Kosten der benötigten Speicherkapazität im Vergleich zu einem Sekundärspeichersystem.

- **Klon eines Datastores oder RDM**
  Vorteil: Von der Quelle unabhängige Datenkopie im selben Primärspeichersystem. Ansonsten gelten die gleichen Vor- und Nachteile wie für Snapshots von Datastores und RDMs.
- **Replikation eines Datastores oder RDM**
  Vorteil: Von der Quelle unabhängige Datenkopie in einem zweiten Primärspeichersystem, zumeist an einem anderen Standort. Ansonsten gelten die gleichen Vor- und Nachteile wie für Klone von Datastores und RDMs. Höhere Kosten der benötigten Speicherkapazität im Vergleich zu einem Sekundärspeichersystem.

Wichtig zu verstehen ist, dass logische Datensicherungen das Prinzip des Medienbruchs nicht abbilden können. Dafür bieten sie eine schnelle Datenwiederherstellung. Mit der physischen Datensicherung lässt sich ein Medienbruch abbilden. Dabei werden Datenkopien wahlweise auf den folgenden Medien angelegt:

- Datensicherung auf festplattenbasierten Sekundärspeichersystemen
- Datensicherung auf Band und optischen Medien

Die Vor- und Nachteile können Sie in Abschnitt 17.2.2, »Medien zur physischen Datensicherung«, nachlesen. Die physische Datensicherung und -wiederherstellung braucht mehr Zeit als die logische. Eine Ausnahme bietet hier *Veeam B&R* mit der *Instant VM Recovery*, doch dazu später mehr.

17.3.3 Indexierung

Eine Indexierung bzw. ein Datensicherungskatalog ist nichts anderes als die grafische Repräsentation der Datenbank einer Sicherungsapplikation, die darüber Buch führt, was zu welchem Zeitpunkt wie gesichert wurde. Moderne Sicherungsapplikationen können durchaus sowohl physische wie auch logische Datenkopien verwalten und zudem unterscheiden, welche Art von Konsistenz (VM oder Applikation) genutzt wurde.

Eine Indexierung hilft Ihnen nicht nur bei der Sicherung von Daten, sondern auch bei ihrer Restaurierung und protokolliert deren Status (Erfolg, Misserfolg, keine Sicherung). Neue virtuelle Maschinen können automatisch indiziert werden, falls die Richtlinien entsprechend gesetzt sind. So riskieren Sie nicht, mit nicht gesicherten Gastbetriebssystemen zu arbeiten.

17.3.4 Validierung

Einzig eine stetige Überprüfung garantiert die Verwendbarkeit der gesicherten Daten im Fall ihrer Wiederherstellung. Grundsätzlich unterscheidet man zwei Arten, die kombiniert am wirksamsten sind:

- Integritätsprüfung
- Validierung

Moderne festplattenbasierte Speichersysteme bieten die Möglichkeit der Integritätsprüfung sämtlicher Daten. Das geschieht auf Blockebene und garantiert nicht, dass die Daten wiederverwendbar restauriert werden können. Die Integritätsprüfung bietet aber eine zusätzliche Sicherheit, da die Daten so wiederhergestellt werden können, wie sie gesichert wurden.

Einen Schritt weiter geht die Validierung. Mit ihrer Hilfe starten Sie virtuelle Maschinen in einer isolierten Umgebung (Sandkasten) und überprüfen damit, ob die Wiederherstellung tatsächlich im Ernstfall möglich ist. Sollte ein Test fehlschlagen, können Sie noch korrigierend eingreifen.

17.3.5 Funktionstrennung

Die Funktionstrennung ist Aufgabe der Organisation. Sie muss die Voraussetzungen dafür schaffen, dass die Funktionstrennung realisiert werden kann.

Um die Funktionstrennung auch technisch umzusetzen, müssen die unten aufgelisteten Voraussetzungen erfüllt sein:

- Es muss unterschiedliche Benutzerkonten geben, die explizit einer Person zugewiesen und ihr eineindeutig zuzuordnen sind.
- Sämtliche Zugriffe auf die Systeme werden aufgezeichnet (Logging), können im Bedarfsfall ausgewertet werden und sind gemäß Unternehmensvorgaben archiviert.
- Die Systeme unterstützen den rollenbasierten Zugriff, wobei die Rollen in Form von Regeln über Zugriffsrechte hinterlegt werden. Eine oder mehrere Regeln werden Benutzern oder Gruppen zugeordnet.
- Das Arbeiten mit generellen Benutzerkonten ist unterbunden und wird nur in Spezialfällen mit Genehmigung des Managements und unter Aufsicht einer Zweitperson gestattet (beispielsweise das `root`-Konto bei Linux-Systemen).
- Sämtliche Passwörter werden regelmäßig geändert und müssen Sicherheitsrichtlinien entsprechen, die vom Unternehmen festgelegt werden.

17.4 VMware-Werkzeuge zur Datensicherung

VMware bringt von Haus aus gute Werkzeuge zur Datensicherung mit, die wir Ihnen im Folgenden vorstellen:

- *VMware Tools* (VSS-Modul für Windows-Gastbetriebssysteme)
- *VM Snapshot* (seine Funktionalität wird in Abschnitt 9.12, »VMware-Storage-Architektur«, ausführlich beschrieben)
- *Changed Block Tracking*

17.4.1 VMware Tools

Jede Installation der *VMware Tools* auf Windows-Gastbetriebssystemen bringt ein *VSS-Modul* (*Volume Shadow Copy Services*) mit. Das ist ein Modul zur Unterstützung einer automatischen Sicherung virtueller Maschinen. Dies bietet den Vorteil VM-konsistenter Snapshots. Dabei werden Dienste der Applikationen (Prozesse) unterbrochen, und die virtuelle Festplatte wird kurzfristig stillgelegt. Diesen Mechanismus machen sich viele Sicherungsapplikationen zunutze. Das VSS-Modul ist im Lieferumfang sämtlicher aktueller Versionen von Windows enthalten. Für Linux-Gastbetriebssysteme bietet *VMware Tools* leider keinen analogen Mechanismus. Es ist Drittherstellern von Sicherungsapplikationen überlassen, einen solchen zur Verfügung zu stellen.

Funktionsweise von Microsoft Volume Shadow Copy Services (VSS)

Microsoft bietet mit *VSS* einen Mechanismus zur Erstellung konsistenter Schattenkopien (*Shadow Copies*). Dieser bietet geschäftskritischen Applikationen sowie Dateisystemdiensten auf schnelle Wiederherstellung abgestimmte Lösungen. Das von *VMware Tools* mitgelieferte VSS-Modul beinhaltet einen *VSS Snapshot Provider* (VSP) und einen *VSS Requestor*. Letzterer reagiert auf Ereignisse einer externen Sicherungsanwendung. Er wird vom VMware-Tools-Dienst instanziiert, wenn ein Sicherungsvorgang angestoßen wird. Der als Windows-Dienst registrierte VSP informiert den ESXi-Server, sobald eine Applikation stillgelegt wird, um einen Snapshot der virtuellen Maschine zu erstellen. Detaillierte Informationen zu *Microsoft VSS* finden Sie unter *https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service*.

VMware Tools und Datensicherungsagenten

Vorsicht ist geboten, wenn Datensicherungsagenten von Drittherstellern innerhalb derselben virtuellen Maschine installiert sind. Falls diese auch ein VSS-Modul mitbringen, kann das mit dem Modul der *VMware Tools* konkurrieren. Das kann zur Folge haben, dass keine Datensicherung durchgeführt werden kann. Im VMware-Knowledge-Base-Artikel 1018194 wird das Symptom beschrieben (*http://kb.vmware.com/kb/1018194*). Die Lösung besteht in der benutzerdefinierten Neuinstallation von *VMware Tools* und im anschließenden Weglassen des VSS-Moduls.

Weiterführende Informationen über den Funktionsumfang von *VMware Tools* finden Sie in Abschnitt 20.12.

17.4.2 VM-Snapshots

Viele Sicherungsapplikationen machen sich die Vorteile eines *VM-Snapshots* – nach Möglichkeit in Kombination mit dem VSS-Modul von *VMware Tools* – zunutze, um auf Ebene des Speichersystems einen VM-konsistenten Snapshot eines VMFS- oder NFS-Datastores durchzuführen. Ohne *VMware Tools* ist der Snapshot absturzsicher. Das heißt, das Gastbetriebssystem kann höchstwahrscheinlich wieder anlaufen, bietet aber nicht die gleiche Qualität der Konsistenz, da das Dateisystem während des Snapshot-Vorgangs nicht stillgelegt werden kann.

Die Funktionsweise eines VM-Snapshots wird in Abschnitt 9.12 ausführlich beschrieben.

17.4.3 Changed Block Tracking

Changed Block Tracking (CBT) ist eine Technologie von VMware, die die inkrementelle Datensicherung von virtuellen Maschinen ermöglicht. Bei einer *inkrementellen* Datensicherung werden immer nur die Daten gesichert, die sich seit der letzten Datensicherung geändert haben. Das beschleunigt den Prozess der Datensicherung erheblich. CBT speichert dabei nur die zuletzt geänderten Datenblöcke und nicht etwa vollständig geänderte Dateien.

CBT ermöglicht sowohl eine inkrementelle Sicherung der virtuellen Festplatten von virtuellen Maschinen als auch deren Wiederherstellung. Voraussetzung für die Wiederherstellung mittels CBT ist allerdings, dass diese direkt in die Quell-VM erfolgt.

Voraussetzungen für CBT

- CBT läuft ab ESXi 4.0 und der Hardwareversion 7 virtueller Maschinen.
- Von der virtuellen Maschine dürfen keine Snapshots existieren.
- Um eine erfolgreiche Datensicherung mit CBT durchzuführen, muss der I/O durch den *vSphere Storage Stack* gehen (kein Support für pRDM und vRDM in den Independent Modes).
- Die virtuelle Maschine sollte zum Einrichten ausgeschaltet sein.
- Achten Sie darauf, dass die virtuelle Maschine bei ihrem Start keine VM-Snapshots enthalten sollte, damit CBT einwandfrei funktioniert. Lesen Sie dazu auch den Knowledge-Base-Artikel 1020128 unter *https://kb.vmware.com/s/article/1020128*.

CBT ist in der Grundeinstellung ausgeschaltet. Datensicherungssoftware wie VDP schaltet CBT automatisch auf zu sichernden VMs ein, sobald die Datensicherung dieser VMs angestoßen wird. CBT erstellt daraufhin eine CTK-Datei pro virtuelle Festplatte im selben Verzeichnis. In diese Datei werden die geänderten Blöcke eingetragen. Die Datensicherungssoftware speichert nach der ersten Vollsicherung nur noch diese Datei anstelle der virtuellen Maschine.

Werden virtuelle Maschinen mit *Storage vMotion* (beispielsweise *Storage DRS*) verschoben, werden die von CBT gespeicherten geänderten Blöcke verworfen, und der Prozess wird zurückgesetzt. CBT kann auch den Faden verlieren, sollte die VM gestoppt (*Power Off*) werden oder der ESXi-Host abstürzen.

17.5 Datensicherungstopologien

Dieser Abschnitt behandelt die Grundlagen von Topologien, wie sie auch in der Praxis Anwendung finden. Die Datensicherung und -wiederherstellung ist die Versicherung für Unternehmensdaten. Eine Datensicherung ist eine Kopie der Unternehmensdaten. Das Ziel einer Datensicherung ist immer die Möglichkeit einer konsistenten Wiederherstellung der benötigten Daten. Darauf muss ein Datensicherungskonzept abzielen.

Zur Wiederholung: Eine konsequent durchgeführte Datensicherung impliziert

- einen Medienbruch,
- das vollständige Erstellen von Datenkopien,
- das Führen eines Sicherungskatalogs oder Index und
- die Prüfung von Kopien sowie
- die Funktionstrennung.

Allerdings ist die Durchführung einer konsequenten Datensicherung sämtlicher Unternehmensdaten mit dem einhergehenden Datenwachstum wirtschaftlich kaum tragbar. Daher wurden Technologien entwickelt, die einen nicht unerheblichen Beitrag zur Wirtschaftlichkeit der Sicherungslösungen leisten. Weiter gilt es, eine Klassifizierung der Daten nach deren Wertigkeit über den Lebenszyklus durchzuführen. Diese sollte im Einklang mit der Kritikalität der IT-Dienste stehen, die auf diese Daten zugreifen. Diese Maßnahmen sind erforderlich für ein Unternehmen, um Datensicherung wirtschaftlich tragbar zu halten.

In vielen Unternehmen besteht bereits eine Klassifikation von IT-Diensten; sie sind in *Service Level Objectives* (SLO) definiert. Die im SLO definierten Werte beeinflussen im Zusammenspiel mit den finanziellen Möglichkeiten maßgeblich, wie Sie *IT Business Continuity* im Allgemeinen und Datensicherung im Speziellen technisch abbilden. Auch dürfen Sie nicht außer Acht lassen, dass die Wertigkeit vieler Daten über die Zeit abnimmt. Das heißt, dass Daten unterschiedlich verwaltet werden müssen (archiviert anstatt gesichert), um die IT-Infrastruktur zu entlasten. Es ist durchaus üblich und sogar notwendig, die physische und die logische Datensicherung zu kombinieren, um die SLOs vollständig abzudecken.

Die in diesem Abschnitt vorgestellten Topologien von *Veeam Backup & Replication* (*Veeam B&R*) können in Datensicherungsarchitekturen verwendet werden. Sie bilden die Grundlage einer konsequent durchgeführten Datensicherung einer virtuellen Umgebung, da sich mit jeder Topologie vier der vorgestellten Prinzipien abbilden lassen (Medienbruch, Datenkopien, Indexierung sowie Validierung).

In diesem Abschnitt stellen wir Ihnen zunächst Topologien auf Basis von *Veeam B&R* vor. Die technische Realisierung zeigen wir Ihnen in Abschnitt 17.6, »Planung einer Datensicherungsumgebung«.

Empfehlung basierend auf dem Prinzip Medienbruch

Um einen Medienbruch zu gewährleisten, empfiehlt es sich, den *Veeam B&R*-Server (was durchaus auch eine VM sein kann) und dessen Ablagepunkt für die Sicherungen getrennt vom Produktivsystem zu halten.

Sollte das aus wirtschaftlichen Gründen nicht möglich sein, müssen Sie versuchen, Ihre Architektur möglichst nahe an diesem Ideal abzubilden. Konkret heißt das: Nutzen Sie für die Sicherung zwei getrennte Speichersysteme oder zumindest ein redundant ausgelegtes System mit zwei physisch und logisch getrennten Speicherbereichen. Dies könnte z. B. ein SAN-Storage mit zwei Controllern sein, in dem 18 Festplatten in zwei Neunerblöcken der vSphere-Umgebung zwei LUNs anbieten.

17.5.1 Topologien zur lokalen Datensicherung

Veeam B&R ist ein Programm, das in einer Windows-Maschine läuft. Befindet sich diese auf einem physischen Hostsystem, wie beispielsweise auf einem HPE DL380 mit 18 Festplatten, wäre dies ein Beispiel für eine lokale Sicherung. Die Festplatten des Servers werden unter Windows eingebunden, eine oder mehrere Partitionen werden gebildet, und diese werden dann Veeam B&R als Speicher für die Datensicherungen präsentiert.

Lokale Datensicherung ist ein relativer Begriff

Veeam B&R unterscheidet dabei nicht, ob die ihm präsentierte Partition lokal oder remote vorliegt. Die Windows-»Maschine« könnte ebenso eine VM sein, der ein entsprechend großes VMDK zugewiesen ist. So könnte z. B. die Windows-VM, auf der Veeam B&R läuft, über eine kleine Systempartition und eine riesige weitere Partition verfügen, auf der eine VMDK mit 64 TB liegt.

Natürlich bietet Veeam B&R auch andere Möglichkeiten, beispielsweise die Nutzung von NFS-Datastores.

17.5.2 Konzepte für die Datensicherung über zwei und mehr Standorte und in der Cloud

Veeam B&R bietet darüber hinaus Möglichkeiten, Sicherungen über mehrere Standorte zu verteilen. Hierzu müssen Sie zunächst einmal unterscheiden, ob es sich dabei um eine Trennung der Standorte durch vSphere handelt oder ob eine tatsächliche logische Trennung vorliegt, die Veeam B&R ebenfalls versteht.

Nehmen wir zunächst an, dass unsere Veeam-B&R-VM innerhalb eines vSphere-Clusters, der an sich schon aus Standorten besteht, aus jedem Standort je eine LUN aus einem entsprechenden Storage bereitgestellt bekommt. Somit ist Veeam B&R nicht in der Lage, eine Unter-

scheidung zwischen lokaler und entfernter Location des Datenspeichers festzustellen. Aus seiner Sicht handelt es sich schlicht und ergreifend nur um zwei unterschiedliche Partitionen, die in Wirklichkeit schon voneinander getrennt sind. Einem solchen Konstrukt sind natürlich aufgrund der Latenzen gewisse Grenzen gesetzt.

Ähnlich sieht es aus, wenn Sie Veeam B&R »auseinanderziehen«. Anders als bei der einfachsten Installation befinden sich dann das Management, *Backup-Server* genannt, und die Worker-Komponente, *Backup-Proxys* genannt, nicht auf derselben VM, was als *Advanced Deployment* bekannt ist – im Gegensatz zum *Simple Deployment* mit nur einer VM, auf der alle Veeam-Komponenten installiert sind. So kann die *Worker-Komponente* auf einer eigenen VM liegen und die Sicherungslocation, *Backup-Repository* genannt, vorhalten.

Es gibt einen dritten generellen Fall, in dem Veeam einen Managementserver vorhält, an den wiederum die gesamten Veeam-B&R-Strukturen angehängt sind. Das ist als *Distributed Deployment* bekannt. Dieser Ansatz wird in sehr großen, sehr weit verteilten Umgebungen genutzt, meist an Organisationseinheiten gebunden, die über Länder und Kontinente verteilt sind.

Last, but not least ermöglicht Veeam B&R auch die Sicherung in die Cloud. Dabei handelt es sich im weitesten Sinne um Veeam-Komponenten, die bei einem zunächst beliebigen Serviceprovider gehostet werden können. Damit ermöglicht Veeam einfache Optionen zur Abbildung von Disaster-Recovery-Szenarien.

17.5.3 Backup vs. Replikation

Eine immer wiederkehrende Frage lautet: »Was ist eigentlich der Unterschied zwischen *Backup* und *Replikation*?«

Ganz allgemein bezeichnet *Backup* das Kopieren von Dateien oder Datenblöcken auf ein externes Speichermedium. Dabei können verschiedene Technologien zum Einsatz kommen, um sowohl die Datenmenge als auch die Backup-Zeit zu verringern, beispielsweise Kompression oder Deduplikation. Durch regelmäßige Backups werden dann entsprechende Wiederherstellungspunkte erzeugt. Dadurch entsteht eine Historie der VM, die beliebig weit in die Vergangenheit zurückreichen kann. In der Praxis wird dies durch weitere Faktoren beeinflusst: maßgeblich durch die verfügbaren Kapazitäten im Backup-Speicher, die wiederum durch den Kostenfaktor bestimmt werden.

Replikation hingegen erstellt, wie der Name schon impliziert, eine echte Eins-zu-eins-Kopie einer VM. Dies geschieht in der exakten Größe der ursprünglichen VM. Änderungen werden synchronisiert, womöglich auch wieder mit geschickt angewendeten Technologien. Letztendlich bleibt das Replikat aber exakt eine Version – die letzte Version der VM, um genau zu sein. Eine Historie wie in Backups gibt es hier entsprechend nicht.

Wie sieht dann der *Kostenfaktor* beim Vergleich zwischen Backup und Replikation aus? Da die Kosten im direkten Zusammenhang mit dem Kapazitätsverbrauch liegen, ist eine Replikation im Prinzip erst mal genauso teuer wie das Original, da sie die exakt gleiche Menge an Daten vorhält. In der Praxis wird zwar immer wieder versucht, die Kosten durch qualitativ niederwertige Infrastruktur zu drücken, z. B. indem man für die Original-VM schnellen SSD-Speicher verwendet und für das Replikat langsameren SAS- oder gar SATA-Speicher. Sinnvoll ist dies in der Regel nicht. Immerhin möchte man mit dem Replikat eine möglichst aktuelle Kopie vom Original haben, um im Disaster-Fall »umschalten« zu können. Wenn das Replikat dann nicht die gewohnte Performance bringt, sind die Anwender enttäuscht, und das eigentliche Ziel der Replikation wird verfehlt.

Betreibt man eine gut durchdachte Backup-Strategie, könnte man durchaus argumentieren, dass eine Replikation nicht zwingend erforderlich ist. Anders herum ist dies allerdings nicht möglich, da eine Replikation Backups nie ersetzen kann.

Backups verfolgen eine andere Strategie: Der Fokus liegt hier auf einer der VM, der Applikation oder den Daten angemessenen Granularität sowie Vorhaltedauer. Immerhin möchte man womöglich Daten noch Jahre später wiederherstellen können. Mit geschickten Verfahren wird versucht, die verbrauchten Kapazitäten so gering wie möglich zu halten. So kann man z. B. von einer VM für jeden Tag einer Woche ein Backup haben, dessen Kapazität aber nicht, wie es im Fall einer Replikation wäre, das Siebenfache der ursprünglichen Größe verbraucht. Stattdessen wird die Größe der Daten geschickt verringert. Später beim Wiederherstellen müssen die vorhandenen Backups dann erst einmal »zusammengesetzt« werden; das heißt, Kompression, Deduplikation und verschiedene inkrementelle Verfahren müssen so aufbereitet werden, dass schlussendlich die VM in dem Zustand des definierten Wiederherstellungszeitpunkts entsteht.

17.6 Planung einer Datensicherungsumgebung

In diesem Abschnitt beschreiben wir die Funktionsvielfalt von *Veeam Backup & Replication*. Das Produkt läuft als VM und kann somit einfach in Ihre vSphere-Umgebung integriert werden. Ein Einsatz auf einem physischen Server ist auch möglich.

An dieser Stelle sei die größte Einschränkung vom Veeam – bzw. von allen Backup-Tools, die vSphere-basierende Technologie mittels Snapshots nutzen – erwähnt: Während eines Backup-Jobs kann keine gleichzeitige Wiederherstellung stattfinden. Dies liegt schlichtweg an den Snapshots, die von vSphere erstellt werden. Sollten Sie also Use Cases haben, in denen Sie sowohl ein Backup als auch eine gleichzeitige Wiederherstellung gewährleisten müssen, ist es erforderlich, auf andere Technologien (z. B. ein filebasiertes Backup) ausweichen.

17.6.1 Funktionsübersicht zu Veeam Backup & Replication

Für Ihre Planung finden Sie in Tabelle 17.4 eine Auflistung der Eigenschaften von Veeam B&R.

Eigenschaft	Veeam Backup & Replication
Maximale Anzahl der VMs	abhängig von der Größe der VMs
Backup-Proxys	abhängig von der Größe der Infrastruktur
Maximale Kapazität (native Speicherressourcen)	skaliert mit Speichersystem
Deduplikation	✓
Change Block Tracking	✓
Microsoft Exchange	✓
Exchange Single Mailbox Restore	✓
Microsoft SharePoint	✓
Microsoft SQL	✓
Flexibler Zeitplaner und Aufbewahrungsfristen	✓
Simple sowie komplexere Aufbewahrungsfristen	✓ Mittels Backup-Copy-Jobs sind auch Wochen- und Monatssicherungen etc. (*GFS*) möglich.
Granulare *.vmdk*-Dateisicherung und -wiederherstellung	✓
Wiederherstellung einzelner Dateien innerhalb der VM	✓
Flexible Platzierung von Speicherressourcen	✓
Automatisierte Überprüfung der Datensicherungen	✓
vSphere-Integration	✓
Wiederherstellung in einem Schritt	✓
Instant Recovery	✓

Tabelle 17.4 Funktionsumfang von »Veeam Backup & Replication«

17.6.2 Generelle Ressourcenplanung

Die Planung der Ressourcen ist natürlich ein sehr umfangreiches Thema, und es ist unmöglich, alle möglichen Fälle anzusprechen. Deswegen versuchen wir an dieser Stelle, die wichtigsten Grundlagen bei der Ressourcenplanung zu erklären.

Machen wir es uns zunächst einfach und beschreiben wir die Replikation. Wie schon erwähnt, handelt es sich bei einer Replikation um eine Eins-zu-eins-Kopie, die so oft wie möglich und nötig mit dem Original synchronisiert wird. Dabei verbraucht die Replikation exakt die gleichen Ressourcen wie das Original. Entsprechend müssen Sie für ein Replikat die gleiche Menge an CPU, RAM und vor allem Speicher vorhalten.

Bei Backups sieht die Sache anders aus. Ein Backup wird anders als ein Replikat nicht dazu genutzt, beim Ausfall des Originals den Betrieb weiterhin zu gewährleisten. Deswegen müssen Sie CPU und RAM als Ressourcen kaum berücksichtigen. Hingegen kommt dem Speicher eine massive Bedeutung zu. Hier ist es zunächst einmal notwendig, die Art des Backups über die Use Cases zu definieren.

- Wie oft muss ein Backup von einer VM erstellt werden?
- Wie viele Backups werden benötigt?
- Sind zusätzliche Wochen- oder Monatssicherungen etc. mit längeren Aufbewahrungszeiten notwendig?
- Werden Backup-Kopien erstellt und, wenn ja, wo werden diese gespeichert?

In vielen Fällen lässt sich die Frage nach der Häufigkeit der Backups einfach beantworten: einmal täglich. Prominente Gegenbeispiele sind oftmals Server mit Datenbanken oder anderen kleineren sich rapide ändernden Daten. Nehmen wir aber zunächst an, dass alle VMs mit einem täglichen Backup ausreichend gesichert wären, dann ist die zweite Frage nach den Voll-Backups zu klären. Auch hier können Sie in vielen Fällen davon ausgehen, dass abgesehen von dem ersten Voll-Backup im weiteren Betrieb nur noch inkrementelle Backups notwendig sind und dass bei Bedarf mit sogenannten synthetischen Voll-Backups operiert werden kann. In einem solchen Fall wird beispielsweise eine VM, die bisher 100 GB Speicherplatz verbraucht und jeden Tag ein weiteres Gigabyte an Daten erzeugt, bei einer Vorhaltedauer von 14 Tagen 114 GB im Backup-Speicher verbrauchen. Dabei betrachten wir natürlich noch nicht die Kompression oder Deduplikation.

Best Practices zur Kompression und Deduplikation

Immer wieder ein heißes Diskussionsthema ist, wie viel Datenreduktion man bei Kompression und Deduplikation erwarten kann. Je nach Hersteller werden hier sehr unterschiedliche Werte genannt, und selbst diese sind meist nur grobe Schätzwerte, was man dann gegebenenfalls im Kleingedruckten nachlesen kann.

Dies liegt vor allem an der Beschaffenheit Ihrer Daten. Einige Daten, mit immer wiederkehrenden Mustern, lassen sich leicht und effizient deduplizieren, andere hingegen nicht.

Deswegen ist es in der Praxis wichtig, entweder sehr konservativ mit solchen Schätzungen umzugehen oder durch echte Tests mit den eigenen Daten korrekte Werte für Kompression und Deduplikation herauszufinden. In jedem Fall sollten Sie bei sehr hohen Werten der Datenreduktion (z. B. 500:1) hellhörig werden, denn dies ist in der Praxis nicht realistisch.

Für die Beispielrechnung nutzen wir den *Restore Point Simulator*, der eine sehr gute Schätzung für die zu erwartende Kapazität berechnet (siehe Abbildung 17.2). Sie finden das Tool unter *https://rps.dewin.me*.

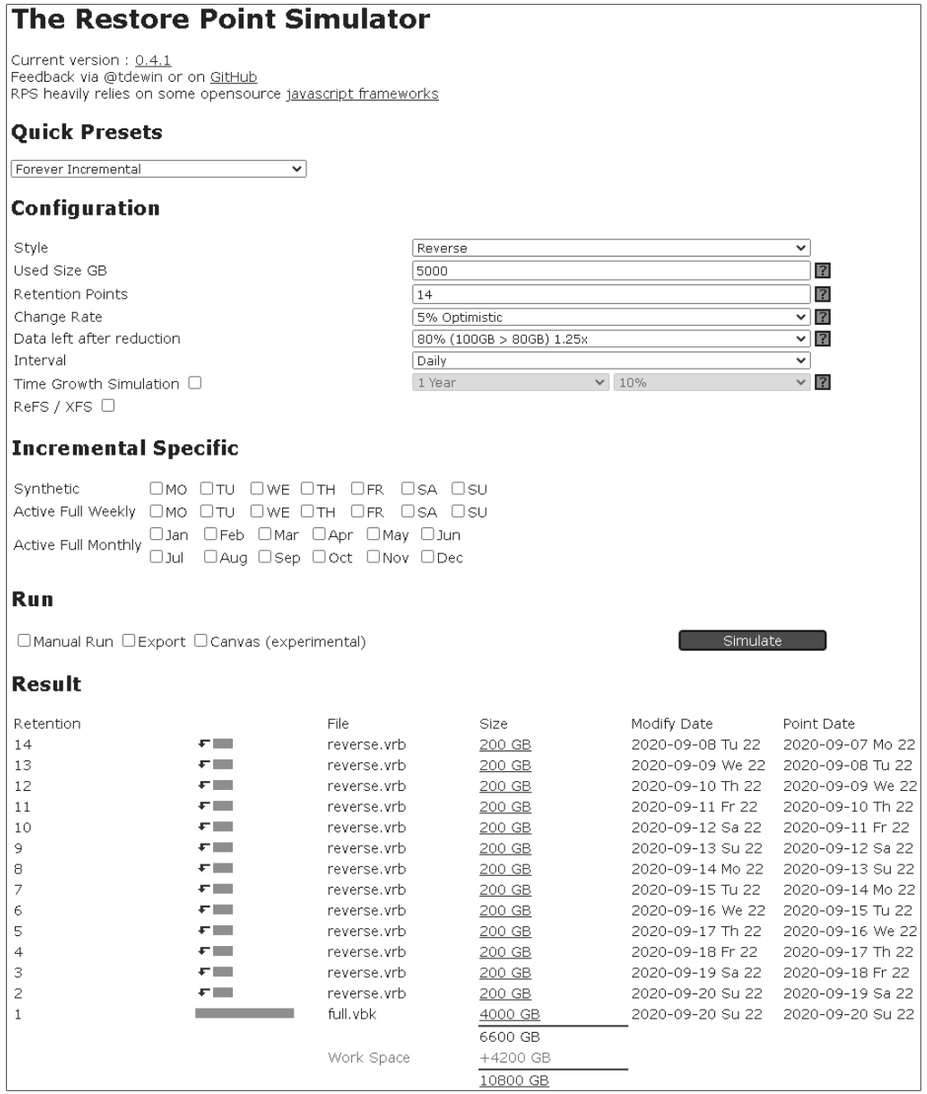


Abbildung 17.2 Beispielrechnung 1

Unser Beispiel geht von einer Infrastruktur aus, in der ein Nettodatenverbrauch von 5 TB gegeben ist und diese Daten 14 Tage vorgehalten werden sollen. Wir nutzen als Voreinstellung unter Quick Presets die Option forever incremental und wählen als Style die Einstellung Reverse. Als Änderungsrate nehmen wir optimistisch nur 5 % an.

Forever incremental bedeutet, dass wir einmal ein Voll-Backup schreiben, nämlich das erste Backup, und anschließend nur noch die Änderung. Reverse bedeutet, dass Veeam als letztes Backup das »volle Backup« synthetisiert. Dies ist insofern sinnvoll, als somit das letzte Backup auch immer am schnellsten herzustellen ist.

Im Gegenzug wird bei der Datenreduktion durch Kompression und Deduplikation nur 100:80 angenommen, also eine Reduktion um 20 % bzw. der Divisor 1,25.

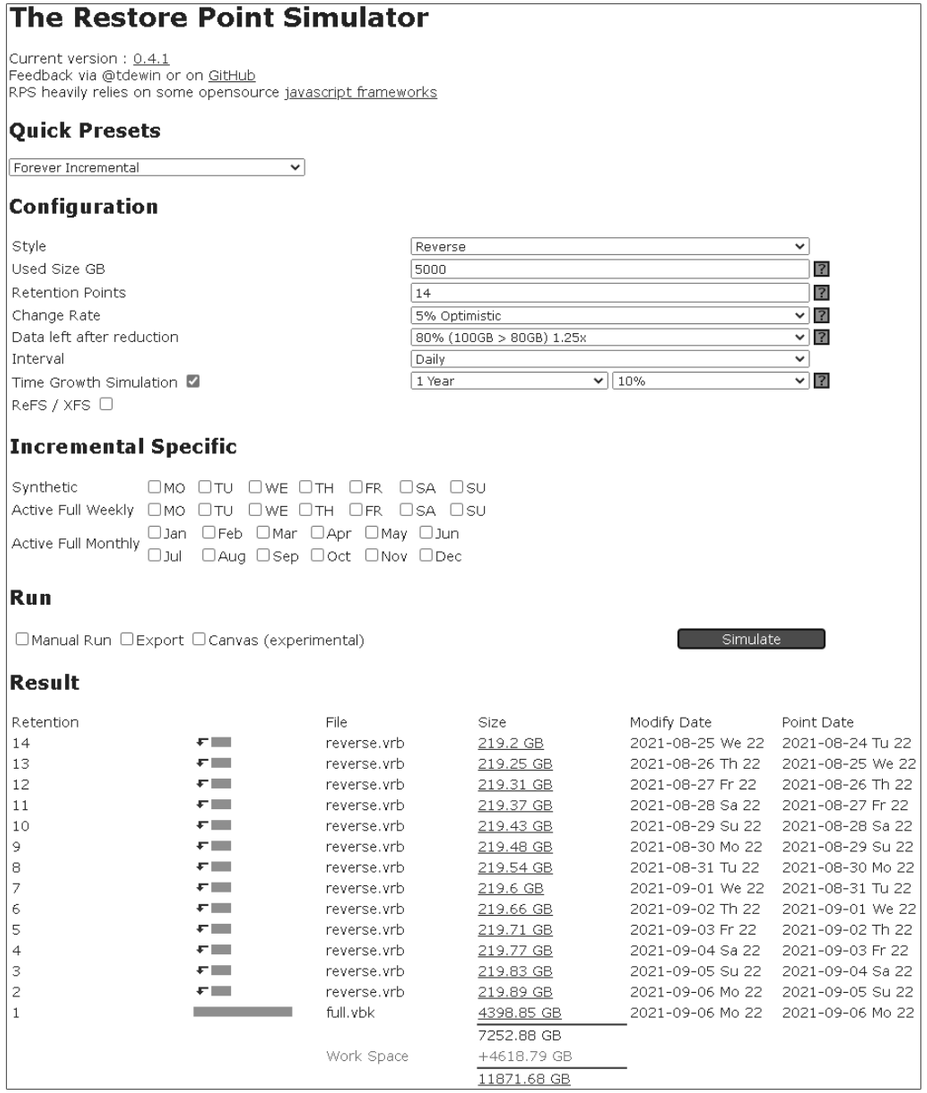
Abbildung 17.2 zeigt uns, dass insgesamt auf dem Backup-Speicher mit 6,6 TB zu rechnen ist, wobei ein sogenannter *Work Space* von 4.200 GB hinzukommt, der von Veeam für die entsprechenden Prozesse benötigt wird. Es ist sehr sinnvoll, mit einem generellen Datenwachstum zu rechnen. Bilder und Dokumente wachsen pro Datei stetig an.

Mit 10 % pro Jahr erreichen wir dann, wie in Abbildung 17.3 zu sehen, 7,25 TB plus 4,6 TB Work Space, also knappe 12 TB benötigten Backup-Speicherplatz.

Was bedeutet Veränderungsrate (Change Rate) eigentlich genau? Diese Frage wird immer wieder gestellt. Sie ist schwer zu beantworten, denn zu viele beeinflussende Faktoren sind zu berücksichtigen. Deswegen wird in der Praxis meist das einfachste Mittel verwendet, nämlich echte Kennwerte aus der Vergangenheit. Hierfür ziehen Sie schlicht die echte, verbrauchte Speicherkapazität der VMs heran und messen diese über einen längeren Zeitraum. Hierbei gilt natürlich: Je länger und detaillierter Sie messen, desto besser. Idealerweise sollte dies mit einem Tool dokumentiert werden.

Leider zeigt sich aber auch, dass in der Praxis ein großer Teil der IT-Administratoren keine echten Kennwerte für die Änderungsrate nennen kann und entsprechend auch keine genaue Vorstellung davon hat, auf welchem Niveau sich die Veränderungsrate bewegt. Dies liegt in der Natur der Aufgabenverteilung. Die Veränderungsrate ist ein Wert, der die IT-Strategie beeinflusst, und fällt damit in den Aufgaben- und Verantwortlichkeitsbereich eines IT-Architekten. Da jedoch nicht in jeder Infrastruktur ein solcher IT-Architekt im Einsatz ist und der Blickwinkel von IT-Admins oftmals einen Level unter dem des Architekten liegt, entsteht so ein blinder Fleck. Und für die IT-Strategie werden oft IT-Direktoren oder IT-Abteilungs- und Bereichsleiter herangezogen, die ebenfalls keine IT-Architekten sind, sondern Managementaufgaben wahrnehmen. In solchen Fällen werden dann gern externe IT-Architekten engagiert.

Werden Sie nun als externer Berater hinzugezogen und sind keine Tools im Einsatz, die die Änderungsrate erfassen, kann dieser blinde Fleck selbst von dem besten IT-Architekten nicht mit Sicherheit eliminiert werden. Die einzige Alternative wäre, die IT-Administratoren dazu zu verpflichten, in Sisyphusarbeit die Veränderungen der Backup-Größen zu notieren: clever, aber sehr mühselig und mit sehr hohem Zeitaufwand verbunden. Dabei geht es wohlgemerkt um Backups aus den letzten zwei bis drei Jahren, wenn sich diese überhaupt lückenlos darstellen lassen.



The Restore Point Simulator

Current version : 0.4.1
Feedback via @tdewin or on GitHub
RPS heavily relies on some opensource javascript frameworks

Quick Presets

Forever Incremental

Configuration

Style	Reverse
Used Size GB	5000
Retention Points	14
Change Rate	5% Optimistic
Data left after reduction	80% (100GB > 80GB) 1.25x
Interval	Daily
Time Growth Simulation	1 Year / 10%
ReFS / XFS	

Incremental Specific

Synthetic	MO	TU	WE	TH	FR	SA	SU	
Active Full Weekly	MO	TU	WE	TH	FR	SA	SU	
Active Full Monthly	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Run

Manual Run | Export | Canvas (experimental) | Simulate

Result

Retention		File	Size	Modify Date	Point Date
14		reverse.vrb	219.2 GB	2021-08-25 We 22	2021-08-24 Tu 22
13		reverse.vrb	219.25 GB	2021-08-26 Th 22	2021-08-25 We 22
12		reverse.vrb	219.31 GB	2021-08-27 Fr 22	2021-08-26 Th 22
11		reverse.vrb	219.37 GB	2021-08-28 Sa 22	2021-08-27 Fr 22
10		reverse.vrb	219.43 GB	2021-08-29 Su 22	2021-08-28 Sa 22
9		reverse.vrb	219.48 GB	2021-08-30 Mo 22	2021-08-29 Su 22
8		reverse.vrb	219.54 GB	2021-08-31 Tu 22	2021-08-30 Mo 22
7		reverse.vrb	219.6 GB	2021-09-01 We 22	2021-08-31 Tu 22
6		reverse.vrb	219.66 GB	2021-09-02 Th 22	2021-09-01 We 22
5		reverse.vrb	219.71 GB	2021-09-03 Fr 22	2021-09-02 Th 22
4		reverse.vrb	219.77 GB	2021-09-04 Sa 22	2021-09-03 Fr 22
3		reverse.vrb	219.83 GB	2021-09-05 Su 22	2021-09-04 Sa 22
2		reverse.vrb	219.89 GB	2021-09-06 Mo 22	2021-09-05 Su 22
1		full.vbk	4398.85 GB	2021-09-06 Mo 22	2021-09-06 Mo 22
			7252.88 GB		
		Work Space	+4618.79 GB		
			11871.68 GB		

Abbildung 17.3 Beispielrechnung 2

Entsprechend bleiben oft nur generelle Aussagen und Schätzungen übrig. Die Änderungsrate wird maßgeblich beeinflusst durch *die Art der Daten*, die *Größe der Daten*, die *Anhäufungsintensität* und die *Veränderungsrate* innerhalb bereits bestehender Daten.

Die Art der Daten lässt sich in vielerlei Hinsicht beschreiben. Je nach Erfahrung des Beschreibers schwanken die Ansätze. Eine Möglichkeit ist, die Beschreibung nach Erstellungsursache zu kategorisieren. Die üblichen Verdächtigen sind hier:

- **Office-Dokumente** wie Word, Excel, PowerPoint – also im Prinzip alles, was durch den typischen Office-Worker produziert wird.
- **Kooperationsdaten**, hauptsächlich E-Mails, denen eine besondere Betrachtung zukommt, da oftmals Teile der anderen Daten freizügig über E-Mails verschickt werden und es hier schnell zu einer Multiplikation vom Daten kommen kann.
- **Kreative Daten** mit den typischen Kandidaten Fotos, Filme und alle Dateien rund um Adobe-Produkte.
- **Technische Daten**, oftmals technische Zeichnungen unterschiedlicher Art, egal ob diese nun einen komplexen Schaltplan für eine Heizung oder das Gittermodell für ein neues Automodell darstellen.
- **Datenbanken**, die Sie besonders exakt betrachten müssen. Meist sind bei Datenbanken die Änderungsraten äußerst hoch, die Datenmenge aber eher gering. Im Vergleich zum Rechner einer Fotografin, die in einer Stunde vielleicht 100 Fotos mit einer Datengröße von 20 GB erzeugt, können sich in einer Datenbank in einer Stunde z. B. 100.000 Datensätze ändern, die auf dem Datenspeicher aber nur 150 MB verbrauchen. Die rein technischen Schwierigkeiten, die viele kleine Dateien mit sich bringen, ziehen sich über die produktive Infrastruktur natürlich bis in die Backup-Infrastruktur durch. Durch diese besondere Beschaffenheit von Datenbanken werden sie oftmals in separate Backup-Jobs gesteckt, um wesentlich kürzere Backup-Intervalle zu gewährleisten. Während die meisten Use Cases mit einem täglichen Backup abgedeckt werden, leistet man sich bei VMs mit Datenbanken oft eine sinnvolle Menge von mehreren Backups am Tag. Diese Menge kann von einer generellen, gleichmäßigen Aufteilung alle 2, 4, 6 oder 8 Stunden ausgehen oder an signifikanten Tageszeiten festgemacht sein: 06:00 Uhr, bevor die meisten Mitarbeiter den Tag beginnen, 13:00 Uhr, wenn sie in der Mittagspause sind, und 18:00 Uhr, wenn sie die Arbeit verlassen haben. Und dann gibt es natürlich noch die ganz zeitkritischen Fälle, in denen man ein nahezu kontinuierliches Backup gewährleisten möchte. Mit Veeam R&B lassen sich *Recovery Time Objectives* (RTO) und *Recovery Point Objectives* (RPO) von weniger als 15 Minuten realisieren.

Idealerweise teilt man anschließend die Daten nach ihrer Größe auf. Nehmen wir Folgendes an:

- **Office-Daten** von 100 GB – mit einer geschätzten Veränderungsrate von 10 bis 20 % liegt man oft schon recht gut. Hier lassen sich meist mit einer kurzen Beobachtungsdauer von einer bis sechs Wochen gute Schätzwerte ermitteln. Dies deckt Schwankungen ab, die unter der Woche entstehen, also auch beispielsweise Urlaube und Krankheiten von Mitarbeitern. Zusätzlich sollten quartals- und jahresbedingte Veränderungen berücksichtigt und idealerweise erfasst werden.

- **Datenbanken** sind, wie Sie vermutlich wissen, immer ein etwas spezielles Thema. Da verschiedene Datenbanken ihre Daten auf unterschiedliche Weise verarbeiten und natürlich auch mit sehr unterschiedlichen Daten gefüttert werden, kann es durchaus sein, dass die Änderungsrate einer Datenbank nahezu 100 % pro Tag beträgt. Dies ist natürlich nicht der Normalfall, kann in bestimmten Fällen aber durchaus passieren.

  Deswegen unterteilt man bei Datenbanken die Veränderungsrate und die Datenzuwachsrate meist in Primär- und Backup-Storage. In einem solchen Worst Case mit 100 % Änderungsrate wachsen die Daten im Primärspeicher normalerweise mit moderaten Zuwachsraten an, die im niedrigen zweistelligen Bereich liegen, was bei einer »kleinen« Datenbank von beispielsweise 10 GB nicht so viel ausmacht. Mit einer hohen Veränderungsrate wirkt sich dies aber im Backup-Speicher massiv aus.

  Nehmen wir eine Veränderungsrate von 50 % an: Somit müssen selbst bei inkrementellen Backups jeden Tag 5 GB neu gespeichert werden. Wir verwenden wieder den *Restore Point Simulator* unter *https://rps.dewin.me* und erhalten bei einer Vorhaltedauer von 30 Tagen bei zwei Backups am Tag einen Gesamtverbrauch von 305 GB plus 10,5 GB Working Space im Veeam-Backup-Repository, also das 31-Fache bzw. 3.100 % der Kapazität im Primärspeicher.
- **Daten mit signifikanten Einzelgrößen** sind meistens *kreative Daten*. Dieser Datenbestand wächst in aller Regel nur mit 3 bis 7 %. Dies liegt schlicht an der Neigung der Menschen, kreative Erzeugnisse nicht einfach wegzuwerfen, was dazu führt, dass im Verhältnis zu vielen Altdaten nur wenige neue Dateien hinzukommen. Gleichzeitig optimieren sich Arbeitsprozesse im kreativen Umfeld, weil z. B. die 1.000 Bilder eines Fotoshootings noch gefiltert werden und erst am Ende die 50 besten Bilder zur weiteren Verarbeitung dauerhaft gespeichert werden. Doch ist hier Vorsicht geboten, damit diese Prozesse nicht eine Veränderung erfahren, während die IT-Infrastruktur verändert wird, oder man muss diesen Umstand entsprechend berücksichtigen.

Ein Beispiel aus der Praxis: Eine Werbeagentur erneuert die IT-Infrastruktur. Im Zuge dessen werden nicht nur die Backup-Strukturen verändert, sondern auch die Fileserver-Struktur. Auf den alten Fileservern liegen Daten, die ca. 100 TB Speicherplatz verbrauchen. Da die neue Infrastruktur größer, schneller und besser ist – die üblichen Anpreisungen eben –, werden ca. zwei Monate, nachdem die neue Infrastruktur in Betrieb genommen wurde, alle Mitarbeiter angewiesen, von nun an ihre Daten auf den neuen Fileservern zu speichern. Daraufhin gehen auch die Mitarbeiter, die mit der Produktion von Werbefilmen beauftragt sind, dazu über, nicht nur die fertigen Filme, sondern auch alles, was *Work in Progress* ist, auf den neuen Fileservern zu speichern. Dadurch steigt die zuvor prognostizierte Datenzuwachsmenge von ca. 1,3 TB im Monat auf nunmehr 5 TB im Monat an. Die neue Infrastruktur, die auf drei Jahre Datenzuwachs ausgelegt war und dann mit entsprechenden Storage-Erweiterungen hätte skaliert werden sollen, erreicht dadurch schon nach neun Monaten Einsatz den Füllstand, der eigentlich auf drei Jahre berechnet war. Das betrifft sowohl den Primärspeicher als auch die Backup-Systeme.

Dieses Beispiel verdeutlicht, dass die benötigte Backup-Kapazität besonders im Bereich von Datenbanken und Dateien mit signifikanter Einzelgröße sehr rasch in die Höhe schießen kann. Deswegen müssen Sie bei der Berechnung bzw. der Schätzung der Backup-Speicher-Kapazität besondere Sorgfalt bei der Ermittlung der Gegebenheiten im Primärspeicher an den Tag legen und verschiedene Backup-Szenarien durchspielen.

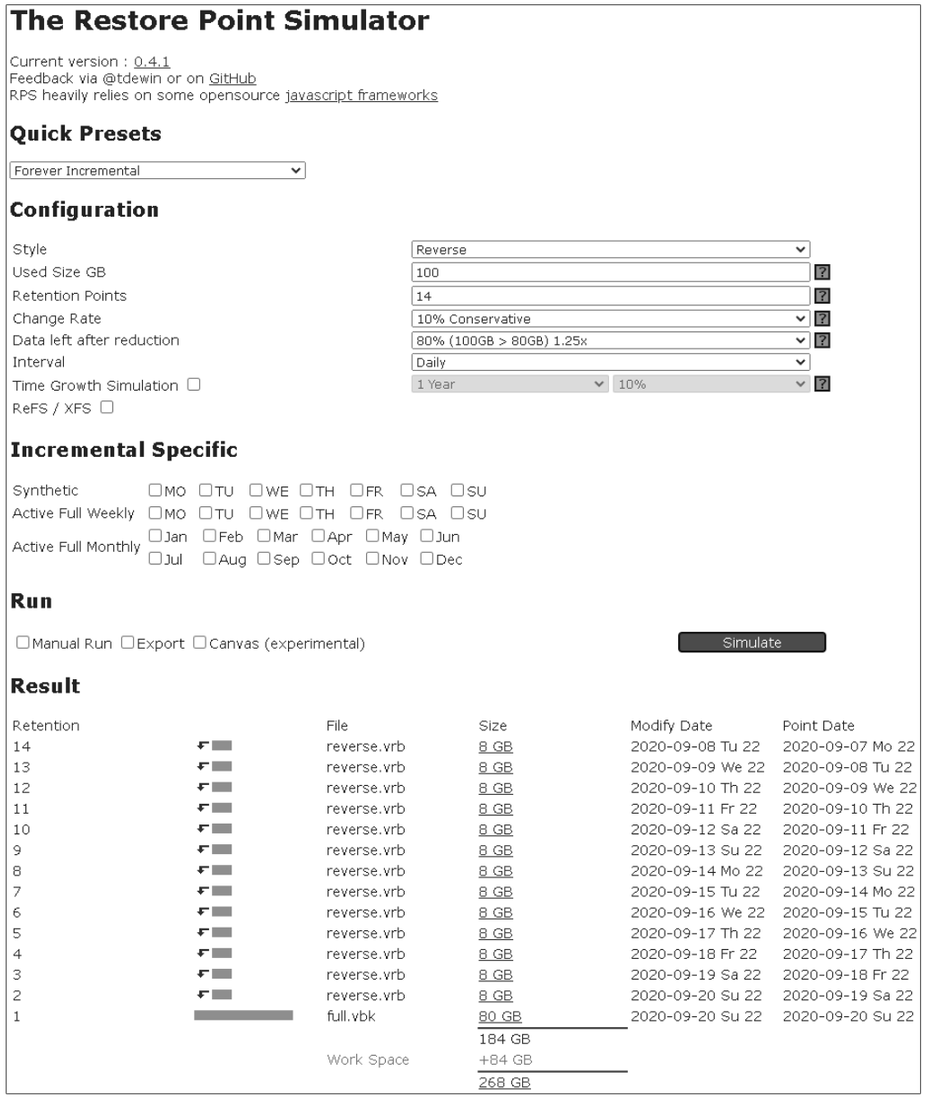


Abbildung 17.4 Restore-Point-Rechner

Sie sollten für jede Backup-Infrastruktur mit Veeam den oben vorgestellten *Restore Point Simulator* (siehe Abbildung 17.4) nutzen, um eine möglichst gute Schätzung der benötigten Ressourcen zu erhalten. Denn prinzipiell lassen sich die Backup-Repositories vom Veeam B&R zwar fast beliebig skalieren, aber Sie sollten dennoch bei der ersten Implementierung mit ausreichend Ressourcen starten, um nicht schon ein paar Monate später weitere Kapazitäten im Backup-Speicher-System nachkaufen zu müssen.

Copy-Jobs

Des Weiteren erfreuen sich die sogenannten Copy-Jobs sehr hoher Beliebtheit. Dabei werden die mit Veeam B&R erstellten Backups erneut gesichert. Gerade in einem mehrstufigen Modell erreichen Sie auf diese Weise mit Tapes, die sich immer noch hoher Beliebtheit erfreuen, den Medienbruch, ohne die Infrastruktur zusätzlich zu belasten. Nehmen wir an, dass Veeam B&R das Backup in der Nacht zwischen 02:00 Uhr und 06:00 Uhr durchführt. Anschließend könnte ein Backup-Copy-Job das neueste Backup auf Tape wegschreiben, um so eine generelle zweite Kopie auf einem physisch anderen Medium vorzuhalten. Dies ist deswegen so beliebt, weil viele Firmen nach wie vor die berüchtigten Backups der letzten zehn Jahre in einem Safe bei einer Bank vorhalten müssen. Auch hierfür bietet Veeam B&R entsprechende Möglichkeiten an, und auch hier hilft der Restore Point Simulator Ihnen, die benötigten Kapazitäten zu schätzen.

17.6.3 Deployment-Methoden

Veeam Backup & Replication teilt sich in folgende Komponenten auf:

- **Backup-Server** – Der Backup-Server ist das Konfigurations- und Kontrollzentrum. Er wird auf einem physischen Rechner oder einer virtuellen Windows-VM installiert. Neben der Koordination aller Jobs werden auch alle globalen Einstellungen hier vorgenommen.
- **Backup-Proxy** – Der Backup-Proxy befindet sich zwischen dem Backup-Server und den Infrastrukturkomponenten. Er ist sowohl für das Holen der Daten aus dem Produktions-Storage als auch für das Komprimieren, Deduplizieren, Verschlüsseln und Weitersenden an den Backup-Storage verantwortlich.
- **Backup-Repository** – Im Backup-Repository werden die Location der Backup-Daten, die VM-Kopien oder die Metadaten für Replikationsjobs gespeichert. Als Location kommen infrage:
  - Microsoft-Windows-Server, also eine »lokale« Partition
  - Linux-Server
  - CIFS/SMB-Shares
  - Dell EMC Data Domain
  - ExaGrid

  - HPE StoreOnce
  - Quantum und OEM-Partner

  Darüber hinaus sind auch Festplatten über USB oder eSATA möglich, was jedoch aufgrund der Performance wie auch der Funktionseinschränkungen nicht empfehlenswert ist. Außerdem sei erwähnt, dass ein Backup-Repository eine Singularität besitzen muss: Vermeiden Sie es auf jeden Fall, mehrere Repositories zu konfigurieren, die auf dieselbe Location zeigen und denselben Pfad nutzen!
- **Mount-Server** – Ein Mount-Server wird benötigt, um eine Wiederherstellung auf Datei- und Applikationsebene zu ermöglichen. Allerdings hat sich in der Praxis gezeigt, dass die Wiederherstellung von einzelnen Dateien idealerweise auf eine Netzwerkfreigabe geschehen sollte. Das direkte Wiederherstellen wirft neben logischen Problemen (Soll man die Datei in der Original-Location verwerfen oder ersetzen?) bei vielen kleinen Dateien auch Performanceprobleme auf. Dies liegt daran, dass jede Datei einzeln durch die gesamte vSphere-Infrastruktur übertragen werden muss, was einen Overhead produziert.
- **Guest-Interaction-Proxy** – Der Guest-Interaction-Proxy befindet sich zwischen dem Backup-Server und der VM, die gesichert werden soll. Er kümmert sich um Application-Aware- und Transaction-Log-Prozesse und auch um die Indexierung des Gastdateisystems. Durch diesen Proxy ist es dem Backup-Server möglich, mit der Gast-OS-VM zu kommunizieren, auch wenn beide in unterschiedlichen Netzen liegen
- **Scale-out-Backup-Repository** – Ein Scale-out-Backup-Repository ist eine Zusammenfassung mehrerer Backup-Repositories zu einer logischen Einheit. In diesem Pool wird entsprechend die Summe aus den einzelnen Repositories als Kapazität angeboten. Dies ist insofern nützlich, weil man nicht mehr die Backups von einem zu klein gewordenen Repository bzw. Backup-Storage auf ein neues, größeres verschieben muss. Somit hilft ein Scale-out-Backup-Repository, die generelle Skalierbarkeit der Backup-Locations so einfach wie möglich zu halten.
- **Gateway-Server** – Ein Gateway-Server ist erforderlich, wenn Sie *Dell EMC Data Domain Deduplication Appliances*, *HPE StoreOnce Deduplication Storage Appliances* oder andere verteilte Backup-Repositories nutzen.
- **WAN-Acceleratoren** – WAN-Acceleratoren sind für das globale Daten-Caching und -Deduplizieren und das anschließende Versenden an die Remote-Locations verantwortlich. Die WAN-Acceleratoren verringern durch entsprechende Optimierung die Größe der Datenpakete. Spezielle Versionen bzw. Add-on-Lizenzen von Veeam sind notwendig.
- **Log-Shipping-Server** – Diese Server sind dedizierte Komponenten für Microsoft-SQL-Server-Transaktionslogs und Oracle-Archive-Logs.
- **Tape-Server** – Viele Unternehmen entscheiden sich auch heute noch dafür, Backups auf Tapes auszulagern. Dabei steht man häufig vor der Herausforderung, dass die Veeam-B&R-Windows-Maschine als VM innerhalb der vSphere-Umgebung läuft und eine voll unterstützte Anbindung von Tape-Laufwerken oder gar Tape-Storages oftmals nicht ohne

Weiteres möglich ist. Oft scheitert dies an Legacy-Tape-Geräten und fehlenden PCI-Karten mit vSphere-Support in den ESXi-Servern. Der Tape-Server löst dieses Problem geschickt: Auf älteren Windows-PCs, in denen mit entsprechenden Schnittstellen Tape-Laufwerke verbaut oder an die Tape-Storages angeschlossen sind, wird der Veeam-Tape-Server ausgerollt. Anschließend können Sie die Tapes so ansteuern, wie man es in Legacy-Tape-Backup-Software gewohnt ist.

- **Veeam Backup Enterprise Manager** – Dies ist eine optionale Komponente, die für die Konsolidierung mehrerer Backup-Infrastrukturen in eine Weboberfläche gedacht ist. *Veeam Backup Enterprise Manager* entspricht in etwa der Funktion eines vCenters, nur eben für Veeam.

Diese Komponenten lassen sich auf unterschiedliche Art und Weise implementieren, die wir Ihnen in den nächsten Abschnitten vorstellen.

Simple Deployment

Wie der Name schon verrät, handelt es sich bei dem *Simple Deployment* um eine denkbar einfache Installation. Die oben genannten essenziellen Veeam-Komponenten werden auf einer einzigen Windows-Maschine oder VM installiert, die dann im üblichen Sprachgebrauch als *Backup-Server* bezeichnet wird.

Der Backup-Server steuert alle Jobs, agiert als Default-Backup-Proxy, ist der Speicherort für das Default- oder auch weitere Backup-Repositories und ist der Mount- bzw. Interaktions-Proxy (siehe Abbildung 17.5).

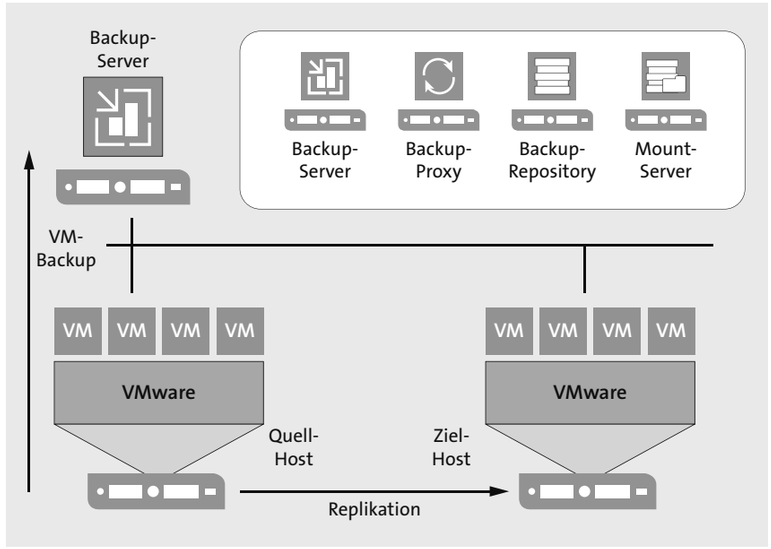


Abbildung 17.5 Schematische Darstellung eines »Simple Deployment«

Ein solches Simple Deployment eignet sich vor allem für kleinere Infrastrukturen und Testinstallationen.

Der Nachteil an einer solch einfachen Installation ist, dass alle Backups »lokal« gespeichert werden. Die Backups liegen also beispielsweise innerhalb der VM, die als Ganzes auf dem Backup-Storage liegt. Im Speziellen liegt der Nachteil hier in der Skalierbarkeit: Je nach Situation kann z. B. die Kapazität des Backup-Servers schnell ausgeschöpft sein. Handelt es sich dabei um einen Server mit internen Festplatten, bereitet dies Schwierigkeiten bei der Skalierung bzw. der Erweiterung des Backup-Storage. Für Backup-Server als VM, die dann auch noch Zugriff auf einen Shared Storage oder NFS haben, ergeben sich in der Regel keine Skalierungsprobleme. Hier muss nur sichergestellt werden, dass die Storage-Systeme, die von Veeam B&R benutzt werden, entsprechende Möglichkeiten zur Erweiterung bieten.

Advanced Deployment

Wie der Name schon vermuten lässt, stellt das *Advanced Deployment* die Erweiterung eines Simple Deployments dar (siehe Abbildung 17.6). In größeren Infrastrukturen wird die Last für einen Backup-Server schnell zu hoch. Entsprechend wird der Backup-Server nur noch als Manager eingesetzt. Die eigentliche Arbeit geschieht dann auf den Backup-Proxys, die deswegen typischerweise auch *Data Mover* genannt werden. Eine solche Installation führt unweigerlich zu der Frage, wie sich Veeam-B&R-Jobs überhaupt skalieren lassen und wie die benötigten Ressourcen berechnet werden. Lesen Sie hierzu Abschnitt 17.6.4, »Dimensionierung von Veeam Backup & Replication-Komponenten«.

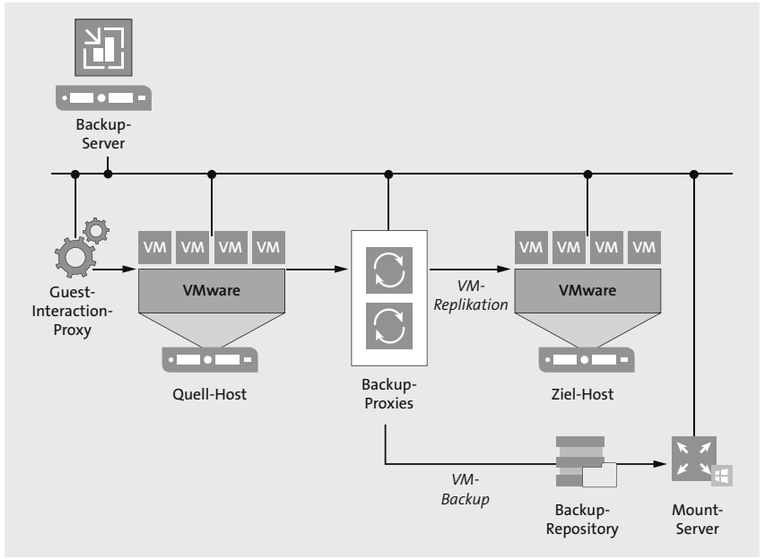


Abbildung 17.6 Schematische Darstellung eines »Advanced Deployment«, Überblick

Distributed Deployment

Die letzte Ausbaustufe einer Veeam-Backup-Infrastruktur ist eine verteilte Installation, bei der sich einfache oder erweiterte Installationen über mehrere Standorte verteilen.

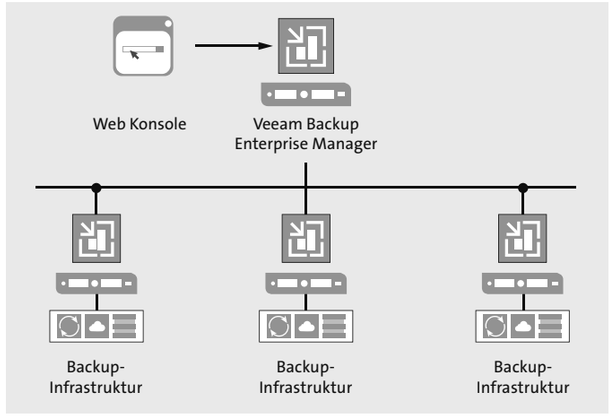


Abbildung 17.7 Schematische Darstellung eines »Distributed Deployment«

Diese werden dann über den *Veeam Backup Enterprise Manager* gesteuert. Dieser stellt über ein Webinterface, ähnlich einem vCenter, einen zentralen Anlaufpunkt zur Verwaltung aller entfernten Backup-Infrastrukturen dar, die viel zitierte *Single Pane of Glas*. Der *Veeam Backup Enterprise Manager* bietet unter anderem:

- die Bearbeitung bzw. das Klonen von Backup-Jobs über die gesamte verteilte Infrastruktur aus eine Template heraus,
- das Reporting der Jobs der letzten 24 Stunden oder 7 Tage,
- ein konsolidiertes Indexing auf diesem Server, das unter anderem die Wiederherstellung einzelner Dateien aus einem Gast-Filesystem ermöglicht, auch wenn das Backup-Repository in einer entfernten Location liegt,
- die Steuerung der Sicherheitsrollen,
- die Vereinfachung des Lizenzmanagements. An den entfernten Standorten müssen die Lizenzen nun nicht separat zugewiesen werden, stattdessen geschieht es zentral verwaltet.

Ein Veeam-Plug-in, das über den Enterprise Manager in vSphere installiert werden kann, erweitert die Ansichten und die verfügbaren Informationen. So lassen sich unter anderem nicht gesicherte VMs, Fehler oder Objektstatistiken identifizieren.

17.6.4 Dimensionierung von »Veeam Backup & Replication«-Komponenten

Für Veeam B&R werden die Ressourcen anhand der benötigten *Concurrent Tasks* im Vergleich zu der gewünschten Backup-Dauer berechnet.

In einer einfachen Installation von Veeam B&R, bei der sich alle Komponenten auf einem Server befinden, gilt:

- Ein *Concurrent Task* entspricht der Abarbeitung einer VMDK.
- Je *Concurrent Task* ist eine vCPU bzw. ein CPU-Kern erforderlich.
- 4 GB RAM plus 500 MB je *Concurrent Task* müssen pro *Concurrent Task* zur Verfügung stehen.

In einer erweiterten Installation mit Backup-Proxys benötigen diese folgende Ressourcen:

- Ein *Concurrent Task* entspricht der Abarbeitung einer VMDK.
- Je *Concurrent Task* ist eine vCPU bzw. ein CPU-Kern erforderlich
- 2 GB RAM plus 200 MB je *Concurrent Task* müssen pro *Concurrent Task* zur Verfügung stehen.

Veeam rechnet in sogenannten *Concurrent Tasks*, wobei ein solcher Task im Prinzip die Abarbeitung einer Disk, also einer VMDK ist. Als Empfehlung wird von Veeam ein Task pro CPU-Kern genannt. Nehmen wir an, Sie möchten 100 VMs mit jeweils 2 Disks sichern. Daraus ergeben sich also 200 Concurrent Tasks. Hätten Sie, wie in einem Simple Deployment, nur einen Backup-Server und hätte dieser z. B. 2 CPUs mit je 8 Kernen, also insgesamt 16 Kerne, dann würde dieser Backup-Server zunächst 16 Disks abarbeiten. Das entspricht in unserem Beispiel 8 VMs. Die anderen VMs und Disks würden in die Warteschlange geraten.

Um nun weiter in unserem Beispiel zu rechnen, nehmen wir an, dass alle 200 Disks gleich groß sind, gleich viel Kapazität verbrauchen, gleich gut im Netzwerk erreichbar sind und alle auf gleich guten Speichersystem liegen. Nehmen wir weiterhin an, dass die entsprechende Veeam-Komponente für die Abarbeitung einer Disk 10 Minuten benötigt. Bei 200 Disks geteilt durch 16 Kerne ergibt das 200 ÷ 16 = 12,5 Zeiteinheiten zu je 10 Minuten. Am Ende dauert das Backup also 125 Minuten, knapp über 2 Stunden. So weit, so gut.

Nun kommen aber weitere VMs, größere Disks oder andere Anforderungen hinzu, z. B. ein kürzeres Backup-Zeitintervall. Machen wir es uns an dieser Stelle erst mal einfach und rechnen wir mit dem obigen Beispiel weiter. Wir gehen von der Vorgabe aus, dass das Backup innerhalb von 30 Minuten für die angenommene Infrastruktur durchgeführt werden muss. Wir erhöhen daher die Anzahl der Backup-Proxys, die ebenfalls mit 2 Sockets und 8 Kernen ausgestattet sind, von 1 auf 5. 4 Backup-Proxys wären zu wenig, da (200 Disks ÷ (16 Kerne × 4 Backup-Proxys)) × 10 Minuten je Disk = 31,25 Minuten sind, was über unserem Ziel von 30 Minuten liegt. Mit 5 Backup-Proxys (und wieder 2 Sockets und 8 Kernen) kommen wir auf (200 ÷ (16 × 5)) × 10 = 25 Minuten und erreichen die Vorgabe.

In der Praxis gibt es natürlich weitere Erwägungen, z. B. die tatsächliche momentan verbrauchte Kapazität der Disks oder die Geschwindigkeit der Anbindung zu den ESXi-Hosts und Speichersystemen. Gerade die Schätzung der Zeit beim ersten Backup mit Veeam oder der Voll-Backups gestaltet sich natürlich etwas schwieriger, sodass wir hier kein einfaches Beispiel errechnen können.

Allerdings können wir aus der Praxis Anmerkungen zu inkrementellen Backups machen. Mit den clever genutzten Technologien werden tägliche Backups und in sehr vielen Fällen – nach dem ersten Voll-Backup – alle Folge-Backups mit der Einstellung INCREMENTAL FOREVER oder REVERSE INCREMENTAL FOREVER durchgeführt. Da hier nur die Änderungen gesichert werden müssen, könnte man nun also fälschlicherweise meinen, dass sich die Backup-Zeit nicht nur signifikant, sondern bei entsprechend geringen Änderungsraten auf quasi 0 verringert. Dem ist aufgrund des Overheads bei der Abarbeitung der Prozesse jedoch nicht so. Je nach Leistung der gesamten Infrastruktur dauert es trotz minimaler Änderungen der Daten innerhalb einer VM in aller Regel fünf bis sieben Minuten, bis die Backups abgearbeitet sind. Beachten Sie, dass wir hier explizit nicht von »Backups schreiben« sprechen, da das tatsächliche Schreiben der Änderungsdaten innerhalb dieser fünf bis sieben Minuten teilweise nur wenige Sekunden in Anspruch nehmen kann.

Der benötigte RAM berechnet sich ähnlich mit 4 GB + 500 MB für einzelne Backup-Server und 2 GB – 200 MB für Backup-Proxys einer erweiterten Installation. Da sich die Arbeit auf die Backup-Proxys verteilt, benötigt der Backup-Server dann natürlich die genannten Ressourcen nicht mehr.

Hier sehen Sie das Ganze noch mal etwas mathematischer erklärt und von der anderen Seite aus gerechnet, um die Frage zu beantworten, wie viele Backup-Proxys benötigt werden:

- Da – Daten in MB, echter Verbrauch
- BZ – Backup-Zeitfenster in Sekunden
- D – Durchsatz, der sich aus *Da ÷BZ* ergibt
- VR – Veränderungsrate
- KV – Kerne für Voll-Backup (*Full Backup*)
- KD – Kerne für differenzielle Backups (*Incremental Backup*)

Nehmen wir folgende Infrastruktur als Grundlage unserer Berechnungen an:

- 500 virtuelle Maschinen
- 80 TB verbrauchter Speicher
- 4 Stunden gewünschtes Backup-Zeitfenster
- 10 % Änderungsrate

Da = 80 TB × 1.024^2 = 80 × 1.024 × 1.024 = 83.886.080 MB

BZ = 4 Stunden × 60^2 = 4 Stunden × 60 Sekunden je Minute × 60 Minuten je Stunde = 14.400 Sekunden

D = Da ÷ BZ = 83.886.080 MB ÷ 14.400 Sekunden ≈ 5.825 MB/s

Für Voll-Backups ist die Performance etwa viermal so hoch wie für differenzielle Backups, weswegen sich der Divisor unterscheidet.

KV = D ÷ 100 = 5.825 MB/s ÷ 100 = 58,25 ≈ 59 Kerne

Für ein differenzielles Backup haben wir mit einem Divisor von 25 gerechnet. Dafür wird der Dividend nun mit der Änderungsrate multipliziert.

KD = (D × VR) ÷ 25 = (5.825 MB/s × 0,1) ÷ 25 = 23,3 ≈ 24 Kerne

Der benötigte RAM für die Backup-Proxys errechnet sich mit 2,2 GB × *Anzahl der Kerne*, beträgt also insgesamt 59 × 2,2 GB ≈ 130 GB.

Nun verteilen wir die benötigten Ressourcen möglichst gleichmäßig. Für virtuelle Backup-Proxys müssen Sie berücksichtigen, dass wie bei jeder VM mit steigender Anzahl an vCPU womöglich ein Engpass beim Scheduling auf den physischen CPUs entsteht. Weitere Informationen hierzu finden Sie in Kapitel 20, »Virtuelle Maschinen«.

Wir rechnen deswegen nur mit 4 vCPUs: 59 Kerne ÷ 4 vCPUs sind 14,75. Es sollten also 15 Backup-Proxys mit 4 vCPUs und 9 GB RAM ausreichen. 9 GB RAM werden benötigt, da 4 vCPUs und 4 Concurrent Tasks 4 × 2,2 GB RAM, also 8,8 GB RAM entsprechen.

Sollten Sie keine Voll-Backups nutzen bzw. diese nur z. B. am Wochenende durchführen, können Sie bei der Berechnung natürlich nur die benötigten Ressourcen für differenzielle Backups heranziehen und anschließend das zu erwartende Backup-Zeitfenster für das Voll-Backup am Wochenende ermitteln. In diesem Fall würden Sie auf 24 Kerne ÷ 4 vCPU = 6 Backup-Proxys mit je 9 GB RAM kommen. Damit erreicht man das gewünschte Backup-Zeitfenster von 4 Stunden unter der Woche. Am Wochenende würde das Voll-Backup entsprechend ca. 10 Stunden dauern (4 Stunden × 60 ÷ 24, was dem Verhältnis der vCPUs in unseren beiden Berechnungsbeispielen entspricht).

Diese Art der Skalierung der Backup-Komponenten wird im Allgemeinen als *Scale-Out* bezeichnet. Entsprechend wäre z. B. in einer einfachen Installation mit einem Backup-Server, der alle Komponenten beinhaltet, die Erhöhung vom RAM, vCPUs und Speicher ein *Scale-Up*.

17.6.5 Der optimale Bereich für die Dimensionierung

Bei der Dimensionierung der Backup-Jobs müssen Sie die Art und Weise der Jobs, die Anzahl der VMs etc. berücksichtigen. Dies liegt daran, dass die im Hintergrund laufenden Prozesse teilweise sequenziell abgearbeitet werden müssen, z. B. das Auflösen der Snapshots oder das Zusammenführen des inkrementellen Backups in eine »volle« Datei, wenn man als Backup-Methode *Reverse Incremental* nutzt.

Ebenso gilt es, den Einfluss auf die Speichersysteme zu berücksichtigen. Laufen mehrere Jobs gleichzeitig ab, werden auch mehrere Snapshots gleichzeitig verwendet. Übersteigt dies die Möglichkeiten der Infrastruktur, kann es sein, dass es genauso wie auch bei vCPU-Scheduling-Problemen zu Wartezeiten kommt, bis ein entsprechender Time-Slot frei ist und ein Prozess gestartet werden kann. Auch beim Storage sollten Sie die Anzahl der gleichzeitig zu verarbeitenden Jobs berücksichtigen: Wie viel Durchsatz schafft das Backup-Repository? Wie viele gleichzeitige Tasks können gestartet werden? Schafft der echte, physische Storage im Hintergrund den Durchsatz, oder wird er z. B. durch langsame SATA-Festplatten begrenzt?

Als Faustformel werden als Maximum oft 30 VMs für ein *Job-Backup* und 300 VMs für einen Per-VM-Backup-Job genannt. Je nach Performance des Backup-Storage sollten Sie diese Zahl auf 50 bis 200 VMs verringern.

Weiterhin gibt es für die Datenbank, die Veeam B&R nutzt, einen optimalen Bereich, der bei 75 bis 100 Jobs liegt. Prinzipiell könnte Veeam mehr verarbeiten, doch auch hier hat sich gezeigt, dass Prozesse durch die Datenbank und deren Lastverteilung negativ beeinflusst werden, wenn man mehr als 100 Jobs laufen lässt.

An dieser Stelle wird sicherlich die Frage auftauchen, wie man VMs in unterschiedliche Jobs aufteilt. Wie wir schon erklärt haben, arbeitet Veeam B&R die Concurrent Tasks parallel mit den zur Verfügung stehenden Ressourcen ab. Gibt es mehr Aufgaben, als parallel abgearbeitet werden können, werden diese der Reihe nach abgearbeitet. Zusätzlich gibt es die Einschränkung, dass, während ein Job läuft, nicht gleichzeitig eine Wiederherstellung stattfinden kann, selbst wenn eine VM eigentlich schon abgearbeitet ist und nun nur noch andere VMs innerhalb des Jobs auf ihr Backup warten.

Nun könnte man geneigt sein, einfach für jede VM ein separates Backup einzurichten. Dies ist auch denkbar und bietet sogar die Möglichkeit, Backup-Jobs zu verketten, sprich, der nächste Backup-Job beginnt, nachdem der andere fertig ist. Dennoch bleiben Einschränkungen bezüglich der optimalen Nutzung: Würden Sie wirklich für jede VM einen Job verwenden wollen, müssten Sie zunächst einmal manuell entsprechend viele Jobs konfigurieren – wenn auch nicht vollständig per Hand, da Veeam die Möglichkeit bietet, Jobs zu klonen. Die entsprechende VM müssten Sie trotzdem erstellen und zudem festlegen, welcher Job der vorherige ist, nach dem der nun zu konfigurierende Job starten soll. Dies allein ist schon wesentlich aufwendiger, als für einen Backup-Job 50 VMs auszuwählen. Außerdem müssten Sie eine richtige Menge an Jobs konfigurieren, die in einem bestimmten Zeitfenster starten. Hier selbst genau die richtige Menge zu finden, die die Infrastruktur optimal nutzt – also weder zu wenig noch zu viel –, ist nahezu unmöglich. Deswegen werden in der Praxis oftmals typenähnliche VMs zusammen in einem Job konfiguriert und die Sonderfälle einzeln oder gemäß den Use Cases aufgeteilt.

Eine relativ typische Aufteilung wäre beispielsweise:

- Die Fileserver werden mit einem täglichen Backup-Job gesichert.
- Die Datenbankserver werden mit einem Backup-Job gesichert, der beispielsweise alle vier Stunden läuft.
- E-Mail-Server, die oftmals eines der wichtigsten Systeme darstellen, werden ebenfalls mit einem separaten Backup-Job gesichert, der zweimal täglich läuft.
- Besondere VMs, bei denen z. B. nicht der optimale Transportmodus beim Backup genutzt werden kann, weil es sich um ein sehr altes System handelt und kein Guest-OS-Agent verwendet werden kann, bekommen einen eigenen Backup-Job. Eine Sonder-VM kann je nach Use Case alles Mögliche sein: von VIP-VMs über Legacy-VMs bis hin zu speziellen Anwendungen, die beim Erstellen von Snapshots bitterböse reagieren, weil sich die Performance auf der VMs leicht verringert.

- Alle anderen VMs werden (je nach Jobtyp) gleichmäßig in Gruppen zu je 50 bis 200 VMs aufgeteilt.

17.6.6 Was man nicht machen sollte

Wie immer gibt es das eine oder andere Limit, das Sie nicht überschreiten sollten, und die eine oder andere Einstellung, die Sie auf gar keinen Fall nutzen dürfen. Bei Veeam sind das folgende Punkte:

- **Kompression auf »hoch« oder »extrem« stellen:** Hierfür werden mindestens zwei vCPUs je Concurrent Task benötigt. In der Ressourcenplanung führt diese Einstellung mal eben zu einer Verdopplung der benötigten vCPUs. Dabei bringt die Einstellung »hoch« gerade mal 2 % bis 10 % Platzersparnis im Backup-Speicher.
- **Applikationsserver als Backup-Server nutzen:** Dies ist eigentlich eine Selbstverständlichkeit. Dennoch passiert es immer wieder, dass Veeam B&R auf einem Server installiert wird, auf dem bereits eine andere Applikation läuft.
- **Blockgrößen:** In vorangegangenen Versionen vom vSphere haben sich unterschiedliche Blockgrößen teilweise stark ausgewirkt. Bei kleineren Blockgrößen wurde etwas mehr RAM für die Deduplikation benötigt, wenn man auf einen »lokalen« LAN-Speicher geschrieben hat, und zwei- bis viermal so viel RAM, wenn man auf ein WAN-Ziel geschrieben hat. Da die Wahl der Blockgröße mittlerweile automatisiert läuft und nicht mehr die manuell einstellbaren Möglichkeiten früherer Versionen bietet und darüber hinaus die Empfehlung bei den Einstellungen fast immer »local« für Backup-Jobs und »LAN« Replikationsjobs lautet, muss man hier nicht mehr so intensiv nachdenken. Sollten Sie auf ein WAN-Ziel schreiben wollen, wird Ihnen das Thema ohnehin noch einmal begegnen. Und was die Deduplizierung angeht, sollten Sie in der Praxis mit folgender Erwartungshaltung operieren: »Deduplizierung ist schön; wir rechnen mit nichts und freuen uns über das, was am Ende herauskommt.« Doch das ist wieder ein anderes Thema.
- **Antivirensoftware auf dem Veeam-Backup-Server** kann je nach Einstellungen zu massiven Problemen führen. Prinzipiell überwacht Antivirensoftware Schreibvorgänge, was natürlich auch alle Daten betrifft, die von Veeam B&R geschrieben werden. Entsprechend müssen Sie dafür Sorge tragen, dass Veeam B&R nicht durch diese Programme geblockt bzw. beeinträchtigt wird. Da dieses Thema mit Datensicherung nichts zu tun hat, verweisen wir an dieser Stelle auf die Veeam-KB-Artikel sowie die Dokumentation, die eine umfangreiche Liste von verwendeten Dateien, Ordnern und Ports liefert, die Sie von der Kontrolle durch Antivirensoftware ausschließen müssten.

17.7 Veeam-Backup-Repository

Um die benötigten Backup-Speicher zu planen, müssen Sie zunächst einmal genauer betrachten, welche Möglichkeiten *Veeam Backup & Replication* bietet. Dies führt uns zu den

sogenannten *Backup-Repositories*. Veeam speichert in einem solchen Repository die Backup-Dateien, VM-Kopien und Metadaten replizierter VMs. Dabei kann jeder Backup-Job nur ein Repository verwenden, die Repositories können aber mehrere Jobs annehmen. Somit besteht hier eine n:1-Beziehung von Job zu Repository. Des Weiteren lässt sich, die entsprechende Lizenz vorausgesetzt, auch ein sogenanntes *Scale-out-Backup-Repository* verwenden.

Je nach eingesetzten Features können die Anforderungen an die Backup-Infrastruktur stark variieren. Nehmen wir beispielsweise das Feature *Instant VM Recovery*. Die viel beschriebene 3-2-1-Regel für Datensicherungen werden Sie sicherlich kennen: Drei Backups an zwei unterschiedlichen Standorten, einmal besonders gesichert oder getrennt. Diese Strategie hat aber erst einmal nicht viel mit Verfügbarkeit zu tun, daher sollte man vielleicht besser Veeams *Instant VM Recovery* nutzen. Hier wird die VM aus dem Backup gebootet, der Produktionsumgebung direkt zur Verfügung gestellt und zeitgleich im Hintergrund auf den Primär-Storage kopiert. Dabei muss die Performance des Backup-Speichers höhere Ansprüche erfüllen. Wäre ein Backup-Speicher nominell nur 1/4 so leistungsfähig wie der Primär-Storage, können Sie bei der Nutzung von Instant VM Recovery davon ausgehen, dass die Performance dieser VM deutlich weniger hergibt und nur im besten Fall 1/4 der Leistung des Primär-Storage erreichen wird. Denn meist bildet sich eine Kaskade: Die übliche Anzahl der User möchte die VM natürlich direkt nutzen, während gleichzeitig der Hintergrundprozess läuft. In der Praxis hat sich gezeigt, dass die Performance dann sehr schnell weiter mit halbierten Faktoren abnimmt: 1/8, 1/16 etc. Die Begeisterung bei den Usern, IT-Administratoren und Managern wird sich deshalb sehr in Grenzen halten. Im schlimmsten Fall bleibt die VM nicht effektiv nutzbar, und der gesamte Sinn und Zweck von Instant VM Recovery würde hinfällig.

17.7.1 Verschiedene Backup-Repository-Typen

Die üblichen Kennwerte für einen Storage und somit auch für einen Backup-Storage sind immer die gleichen:

1. Gesamtkapazität
2. Schreib- und Leseleistung
3. Verfügbarkeit der Bestandteile wie Festplatten, LUNs, Controller etc.
4. Kosten-Leistungs-Faktor

Nun werden sich viele fragen, warum der Kosten-Leistungs-Faktor bei den Kennwerten des Storage genannt wird. In unserer heutigen Zeit sind der Leistung und der Kapazität kaum noch technische Grenzen gesetzt. Maßgeblicher Faktor ist und bleibt aber das einsetzbare Kapital. Hat man in den Bereichen 1, 2 und 3 Ansprüche, wird viel Kapital benötigt. Oftmals stellen Kunden zunächst eine Wunschliste mit der perfekten Lösung auf, um anschließend festzustellen, dass ihre Wünsche und ihr verfügbares Kapital nicht vereinbar sind. Anschließend begibt man sich auf die Suche nach einer schlankeren 80-%-Lösung, idealerweise für 20 % der Kosten.

Eine Möglichkeit ist es, mehrere qualitativ unterschiedliche Backup-Repositories zu verwenden. Eine häufig gewählte Variante ist ein leistungsstarkes Speichersystem mit weniger Kapazität sowie ein schwächeres System mit deutlich mehr Kapazität. Dabei werden aktuelle Wiederherstellungspunkte auf dem schnellen Speicher vorgehalten und weiter in der Vergangenheit liegende Wiederherstellungspunkte auf den schwächeren Speicher ausgelagert. In einem solchen Fall würden Sie mit einem Veeam-Backup-Copy-Job die Backups vom schnelleren zum größeren System kopieren oder, mit der entsprechenden Lizenz, ein Scale-out-Backup-Repository einrichten.

Eine weitere Stufe ist die Nutzung von extrem langsamen Speichern mit extrem hohen Kapazitäten, typischerweise Tapes. Doch dazu später mehr.

17.7.2 SMB-Backup-Repository

Da wir bereits in Kapitel 9, »Storage-Architektur«, auf unterschiedliche Arten von Speichern eingegangen sind, wollen wir an dieser Stelle nur die wichtigsten Punkte erwähnen, ohne auf die verschiedenen Vor- und Nachteile einzugehen.

Wir gehen davon aus, dass eine Windows-VM als Backup-Server, Backup-Proxy bzw. Gateway-Server verwendet wird. Auf dieser Windows-VM werden die verfügbaren Volumes dann entweder zu einer Partition zusammengefasst oder als separate Partition genutzt. Letzteres sollten Sie nur mit Bedacht tun: Die Aufteilung in separate Partitionen entsteht durch den Wunsch, eine bessere Lastverteilung zu erreichen. Allerdings sind einer einzelnen VM schon gewisse Limitierungen durch das Speichersystem auferlegt, auf dem die VMDK der VM liegt. Um dort, z. B. bei der *Queue Depth* der RAID-Karte, nicht in Schwierigkeiten zu geraten, ist es oftmals besser und auch einfacher zu berechnen, wenn man Backup-Repositories mit Backup-Proxys zusammen skaliert.

Bei der Wahl des Repository bieten die Gateway-Server oder die Backup-Jobs zwei Modi zur Auswahl: *automatisch* und die Auswahl des spezifischen Servers. Wie unschwer zu erraten ist, wird mit der Option *automatisch* die Auswahl des Backup-Repository durch die entsprechende Veeam-Komponente getroffen. Wenn Sie diese Entscheidung selbst treffen wollen, nutzen Sie in der Konfiguration das entsprechende Menü, um das gewünschte Repository auszuwählen. So können Sie z. B. Backups auf ein performanteres Speichersystem schieben und *Instant VM Recovery* nutzen. Oder Sie konfigurieren Ihre Backups explizit auf ein lokales Backup-Repository, weil eines der Backup-Repositories an einem Remote-Standort liegt. Sie möchten damit verhindern, dass die automatische Auswahl des Backup-Repository genau jenes auswählt, das sich an einem anderen Standort befindet, was die Latenzen und damit die Verarbeitungsdauer der Jobs in die Höhe schnellen ließe.

Im Fall einer automatischen Wahl wird das Load-Balancing ebenfalls automatisch durchgeführt. Hierbei gilt es zu berücksichtigen, dass pro Backup-Job nur ein Server, nämlich der *Gateway-Server*, verwendet wird, um die Daten auf ein SMB-Share zu schreiben. Bei mehreren verfügbaren Proxy-Servern ist das immer der erste, der vom Backup-Job »gefunden«

wird. Ist im Backup-Job die Option PER-VM BACKUP FILES aktiviert, werden mehrere Backup-Reihen im Hintergrund erstellt, die jede für sich wiederum möglicherweise mehrere Backup-Proxys ansprechen, von denen wiederum der erste zum Gateway-Server wird. In einem solchen Fall werden also mehrere Gateway-Server gleichzeitig angesprochen. Deswegen sollte das Netzwerk ausreichend gut ausgelegt sein, damit an dieser Stelle keine Engpässe entstehen. Außerdem ist es bei mehreren Backup-Reihen möglich, dass »der erste gefundene Backup-Proxy«, der zum Gateway-Server gemacht wird, in mehreren Reihen derselbe ist. Diesen erkennt man schnell daran, dass seine CPU- und RAM-Last wesentlich höher ist als bei den anderen Backup-Proxy-Servern.

Ein Vorteil mehrerer Backup-Reihen ist natürlich, dass mehrere Threads zu einem Speichersystem genutzt werden können. Gerade bei NAS-Speichern kann das durchaus sehr sinnvoll sein, um so die generelle Geschwindigkeit zu erhöhen, mit der Backups weggeschrieben werden können. Natürlich ist dabei zu erwähnen, dass man dies mit Bedacht tun sollte, um nicht das NAS zu überlasten. Und dass man nicht das billigste NAS dafür einsetzen sollte, ist eigentlich auch selbstverständlich.

17.7.3 Deduplication Appliances und VTL als Backup-Repository

Veeam ist in der Lage, Deduplizierungs-Appliances als Backup-Repository, Backup-Copy-Repository oder als *virtuelle Tape-Library* (VTL) zu nutzen. Solche Deduplizierungs-Appliances sind sehr vereinfacht gesagt Speichersysteme, die sich darauf spezialisiert haben, Daten anzunehmen und möglichst effizient – also mit möglichst geringem Speicherverbrauch – wegzuschreiben.

Die genaue Funktion solcher Systeme unterscheidet sich von Hersteller zu Hersteller und soll auch nicht Teil dieses Kapitels sein. Generell ist aber anzumerken, dass mit dem Vorteil des geringen Platzverbrauchs auch ein Nachteil einhergeht: Üblicherweise speichern solche Appliances auf sehr schnellen SSD- oder SAS-Festplatten einen Cache. Das können beispielsweise die »frischesten« Dateien sein, die »heißesten« Blöcke etc. Dieser Cache ist natürlich endlich, und so werden die Daten kurze Zeit später auf wesentlich langsamere Medien wie SATA-Festplatten oder Tapes geschrieben. Möchten Sie nun Daten zurückholen, die nicht im Cache liegen, kann dies entsprechend lange dauern. Sind die Daten auch noch auf mehrere Speicher verteilt, was bei Random-I/Os immer ein Thema ist, verschlimmert sich dieses Problem natürlich. Im Englischen wird dieses Phänomen *Re-hydration Process* genannt. Die »De-Hydrierung« ist dabei die Transformation der originalen Speicherblöcke in dedupliziert Speicherblöcke, und entsprechend ist die »Re-Hydrierung« die Transformation der deduplizierten Speicherblöcke in ihre originale Form. Darüber hinaus lässt sich leicht erraten, dass gerade stark I/O-lastige Prozesse für Deduplizierungs-Appliances besonders schwer zu bewältigen sind. Somit ist die Verwendung solcher Systeme für Veeams *Instant VM Recovery* denkbar ungünstig, da dieses Feature mit Abstand die meisten I/Os verursacht.

Um diese Problematik ein Stück weit zu entschärfen, gibt es für die Konfiguration von primären Backup-Jobs zwei Möglichkeiten: Storage-Hersteller bieten möglicherweise ein von

Veeam unterstütztes Produkt an. Beispiele sind hier *EMC DataDomain* mit ihrem *DDBoost*-Protokoll oder *HPE StoreOnce* mit dem *Catalyst*. Beschreibungen, wie diese optimal angesteuert werden, finden Sie in der Dokumentation der Hersteller oder in der Veeam-Dokumentation. Für Produkte aller anderen Anbieter ist die Verwendung des *Forward Incremental with Active Full*-Backups zu empfehlen. Alle anderen Backup-Modi erfordern eine Datentransformation mit signifikant höherer I/O-Last mit De-Hydrierung und Re-Hydrierung auf dem Speichersystem.

Weiterhin ergeben sich aus der Nutzung von *Forward Incremental with Active Full*-Backups Einschränkungen, die es bei der Planung zu berücksichtigen gilt, z. B. Backup-Zeitfenster, Anzahl und Speicherverbrauch von Snapshots etc. Aus diesem Grund ist es empfehlenswert, Deduplikations-Appliances wenig oder besser gar nicht für primäre Backup-Jobs zu nutzen. Auch bei Backup-Copy-Jobs werden Transformationen vorgenommen, wenn die sogenannten synthetischen Voll-Backups verwendet werden. Entsprechend wird empfohlen, aktive Voll-Backups bei den Backup-Copy-Jobs für das Schreiben auf Deduplikations-Appliances zu verwenden.

Für die Nutzung von virtuellen Tape-Libraries (VTL) muss ein Backup-Repository ohne Kompression genutzt werden, das als Zwischenschritt vor dem Schreiben auf die VTL benötigt wird. Hierzu sollte das Backup-Repository in den erweiterten Einstellungen mit DECOMPRESS BEFORE STORING konfiguriert sein. Das gewährleistet einen effizienteren Prozess, da die Kompression, die auf Jobebene eingestellt wurde, ignoriert wird.

17.7.4 Pro-VM-Backup-Dateien

In der empfohlenen Standardeinstellung werden die Daten aus einem Backup-Job in einem *Stream* geschrieben, was sich durch einen Haken ändern lässt, wie Abbildung 17.8 zeigt.

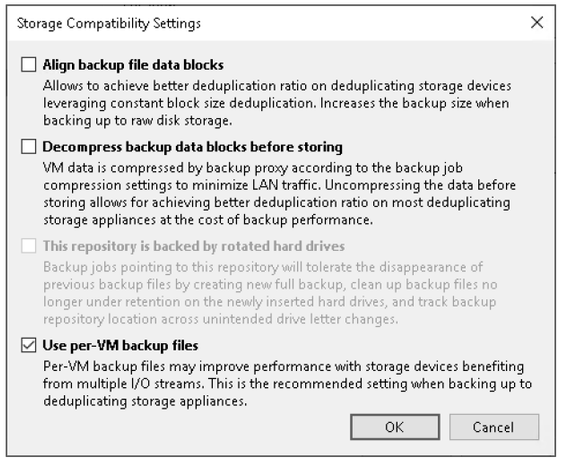


Abbildung 17.8 Die Option »Use per-VM backup files«

Dadurch sind alle Daten für mehrere VMs in einer einzigen Backup-Datei enthalten. Daraus ergibt sich eine zuvor schon angesprochene Einschränkung, da man nicht gleichzeitig das Backup und das Restore eines Jobs durchführen kann, was in der Folge einen Restore einer VM aus jenem Job verhindert, auch wenn diese schon abgearbeitet wurde.

Seit Veeam B&R ab Version 9 wird die Möglichkeit geboten, *Pro-VM-Backup-Dateien* zu schreiben. Das heißt, dass Veam je VM einen Schreibstream nutzt. Das vereinfacht das Jobmanagement erheblich. Gleichzeitig erhöht sich dadurch generell die Schreibperformance, und in bestimmten Jobmodi verbessert sich die Leistung beim Zusammenführen von Backup-Dateien. Außerdem sinkt der Speicherbedarf im Backup-Repository, das als Workspace nun nicht mehr für die Transformation der Workspaces eines Voll-Backups vorgehalten werden muss, sondern nur so viel freien Speicherplatz benötigt, um die größte Backup-Datei verarbeiten zu können.

Da die Aufteilung in mehrere Schreibstreams besonders Deduplikations-Appliances zugutekommt, wird die Einstellung entsprechend empfohlen. Darüber hinaus profitieren gerade Tape-Libraries mit mehreren Laufwerken, die jeweils nur einen Schreibstream verarbeiten können, von dieser Änderung, da nun die Schreibstreams auf alle verfügbaren Tape-Laufwerke verteilt werden können, was wiederum die Schreibleistung in Gänze verbessert und die Verarbeitungszeit verringert. In Scale-out-Backup-Repositories ist diese Einstellung standardmäßig immer aktiviert, um innerhalb eines Scale-out-Backup-Repository die Volumes ebenfalls besser ansprechen zu können. Wesentlich größer als 300 VMs sollten Backup-Jobs mit eingestelltem »Per-VM-Backup«-Dateien wie bereits erwähnt nicht werden. Dies liegt vor allem daran, dass z. B. synthetisierende Prozesse, Backup-Copy-Jobs oder Gesundheitschecks erst durchgeführt werden, nachdem alle VMs erfolgreich durchgelaufen sind, was wiederum sehr große Backup-Jobs wenig sinnvoll macht.

Bei all den Vorteilen dieses Features wollen wir aber auch die potenziellen Nachteile erwähnen. Mit multiplen Schreibstreams erreichen Sie natürlich wesentlich schneller die Grenzen Ihrer Speichersysteme. Gerade NAS-Systeme reagieren sehr ungehalten, wenn man ihnen mehr Schreibstreams aufbürdet, als sie verarbeiten können. Gehen Sie also vorsichtig vor und erweitern Sie Ihre Schreibstreams nur stufenweise. Alternativ können Sie auch in den Einstellungen von Backup-Jobs und Backup-Repositories Limits angeben. Maßgeblich ist das Concurrent-Tasks-Limit, das sich in Veeam steuern lässt.

17.7.5 Scale-out-Backup-Repositories

Veeam Scale Out Repository ist eine Zusammenfassung mehrerer einzelner Backup-Repositories und bildet damit eine übergeordnete, logische Einheit, die für Backup- und Backup-Copy-Jobs verwendet werden kann. Dies macht die Erweiterung vorhandener Backup-Repositories denkbar einfach, falls diese langsam, aber sicher volllaufen. Ähnlich wie eine Storage Extent in vSphere wird auch in Veeam eine solche Erweiterung mit einem weiteren Backup-Repository vorgenommen. Aufwendige Umzüge alter Backups entfallen damit. Wie zuvor schon erwähnt, muss eine entsprechende Lizenz vorhanden sein, und Sie benötigen natürlich mindestens zwei einfache Backup-Repositories. Auch empfiehlt es sich, die Option PER VM BACKUP FILES mit mehreren Schreibstreams beizubehalten. Es gibt allerdings Einschränkungen:

- Eine Enterprise- oder Enterprise-Plus-Lizenz ist erforderlich.
- Das Scale-out-Backup-Repository kann nicht Ziel sein für:
  - Konfigurations-Backup-Jobs
  - Replikationsjobs
  - VM-Copy-Jobs
  - Veeam-Agent-Backup-Jobs, die mit *Veeam Endpoint Backup 1.5* oder älter und *Veeam Agent for Linux 1.0 Update 1* oder älter erstellt wurden
- Sollte eines der genannten Backups schon auf einem Backup-Repository eingerichtet sein, können Sie dieses nicht für das Scale-out-Backup-Repository verwenden. Maßgeblich betrifft dies das Default-Backup-Repository, das üblicherweise bei der Installation auf der *C:*\-Partition der Windows-Maschine konfiguriert wird und sofort das Konfigurations-Backup aufnimmt. Entsprechend müssen Sie vorher die genannten Jobs auf ein anderes Ziel zeigen lassen, um dann das Backup-Repository für Scale-out verfügbar zu machen.
- Externe Laufwerke, die per USB oder eSATA angeschlossen sind, werden nicht unterstützt. Allerdings ignoriert Veeam die Einstellung THIS REPOSITORY IS BACKED BY ROTATED HARD DRIVE bei einem Extent schlichtweg und behandelt das Backup-Repository wie jedes andere.
- Sobald Sie ein Backup-Repository als Extent für ein Scale-out-Backup-Repository genutzt haben, können Sie es nicht mehr als normales Repository direkt nutzen. Ebenso können Sie es nicht für ein anderes Scale-out-Backup-Repository nutzen.
- Eine Kaskade aus Scale-out-Backup-Repositories, in der wiederum Scale-out-Backup-Repositories als Extent verwendet werden, ist nicht möglich.
- Wird ein Backup-Repository schon von *vCloud Director* verwendet, kann es nicht für ein Scale-out-Backup-Repository verwendet werden.
- Während ein laufender Prozess auf ein Backup-Repository zugreift, kann dieses nicht an ein Scale-out-Backup-Repository angebunden werden.
- Nur in der Enterprise-Plus-Lizenz sind den Scale-out-Backup-Repositories keine Limits gesetzt. Mit einer Enterprise-Lizenz sind Sie auf ein Scale-out-Backup-Repository mit drei aktiven und einem inaktiven Backup-Repository beschränkt. Das Hinzufügen eines vierten Backup-Repository verursacht Fehler bei Backup-Jobs.
- Die *Extract and Backup Validator Utilities* funktionieren nicht mit Scale-out-Backup-Repositories.
- Veeam B&R führt beim Import von Backups aus Scale-out-Backup-Repositories automatisch einen Rescan durch. Dabei dürfen sämtliche Pfade zu Ordnern und VBM-Dateien ausschließlich die alphanumerischen Zeichen a–z, A–Z, 0–9 und die Sonderzeichen _-.+= @^ enthalten. Leerzeichen dürfen nicht enthalten sein. Sind dennoch verbotene Zeichen

vorhanden, wird ein Import fehlschlagen. In einem solchen Fall müssen Sie die Sonderzeichen durch manuelles Umbenennen entfernen und einen erneuten Import durchführen.

- Veeam B&R teilt Backup-Dateien nicht auf. Das heißt, eine Backup-Datei wird immer als Ganzes auf einem Extent abgelegt.

17.7.6 Backup-File-Placement im Scale-out-Backup-Repository

Prinzipiell gibt es für Scale-out-Backup-Repositories zwei unterschiedliche Richtlinien, nach denen Dateien abgelegt werden: *Data Locality* und *Performance*. Allerdings sind diese Richtlinien nicht in Stein gemeißelt, da Veeam B&R als alles überschattende Richtlinie immer einer erfolgreichen Jobfertigstellung höchste Priorität einräumt. Dabei werden andere Richtlinien gebrochen bzw. missachtet, wenn dies eine erfolgreiche Fertigstellung eines Jobs ermöglicht. Außerdem sollten Sie bedenken, dass zum einem auf jedem Extent eines Scale-out-Backup-Repository 1 % freier Speicherplatz vorgehalten wird, um die korrekte Abarbeitung sowohl von Zusammenführungsprozessen als auch von Updates der VBM-Dateien zu gewährleisten. Zum anderen sollte ein Extent generell ausreichend Platz für Zusammenführungsprozesse vorhalten. Ist dem nicht so, könnten diese Prozesse fehlschlagen.

In der Richtlinie *Data Locality* werden die Backup-Dateien einer *Backup-Kette* (*Backup Chain*) zusammen in den gleichen Extent geschrieben. Bei der Option PER-VM BACKUP FILES sind das die Metadaten (VBM), die Voll-Backup-Datei (VBK) und die Differenzdateien (VIB). Das bedeutet auch, dass beispielsweise Dateien eines Backup-Jobs, die sich in unterschiedlichen Backup-Ketten befinden, auf alle Extents eines Scale-out-Backup-Repository verteilen können.

In der Richtlinie *Performance* werden die Voll-Backup-Dateien (VBK) und die Differenzdateien (VIB) getrennt voneinander auf unterschiedlichen Extents gespeichert. Ohne weitere Konfiguration verteilt Veeam B&R die Extents automatisch selbst, eine Spezifizierung der Extents ist aber auch möglich. Wie der Name schon verrät, erhöht dies in aller Regel die Leistung, da nun I/O-intensive Prozesse auf mehrere Extents verteilt werden. In der Praxis funktioniert das natürlich nur in Abhängigkeit von der Leistungsfähigkeit der physischen Speichersysteme. Besteht Ihr Scale-out-Backup-Repository beispielsweise aus zwei Extents, die auf der Windows-VM in zwei unterschiedlichen Volumes liegen, die wiederum in zwei unterschiedlichen VMDKs liegen, wobei die VMDKs aber auf ein und derselben LUN auf ein und demselben Array liegen, ist natürlich absehbar, dass eine echte Performancesteigerung nicht bzw. nur sehr begrenzt zu erwarten ist.

Dass alle Extents online und verfügbar sein müssen und dass eine entsprechende Netzwerkverbindung zwischen den Extents bestehen muss, damit Jobs mit dem Scale-out-Backup-Repository als Ziel erfolgreich laufen, versteht sich von selbst. Um Fälle von nicht verfügbaren Extents abzufangen, können Sie bei Voll-Backups die Option PERFORM FULL BACKUP WHEN REQURIED EXTENT IS OFFLINE aktivieren. Dadurch fallen fehlende differenzielle Dateien aus der Backup-Kette nicht ins Gewicht. Auf der anderen Seite wird dadurch natürlich die Backup-Dauer erhöht, und es wird mehr Speicher verbraucht, da nun ein Voll-Backup geschrieben wird anstelle eines weiteren inkrementellen Backups.

17.7.7 Windows-Server-Deduplikation-Share als Backup-Repository

Möchten Sie als Backup-Repository einen Windows-Fileserver mit Deduplikation nutzen, sollten Sie folgende Einstellungen vornehmen:

- Formatieren Sie Festplatten in der Konsole mit der Option `/L` für große Dateien.
- Verwenden Sie 64 KB als Cluster-Größe.
- Spielen Sie alle Patches für Windows 2012 R2 und 2016 ein, die Verbesserungen für die Deduplikation enthalten.
- Verwenden Sie aktive Voll-Backups mit Differenzdateien (Option: ACTIVE FULL WITH INCREMENTALS).
- Verteilen Sie aktive Voll-Backups über die Woche.
- Stellen Sie die Garbage Collection von wöchentlich auf täglich um.
- VBK-Dateien sollten 1 TB nicht überschreiten, da Microsoft größere Dateien offiziell nicht unterstützt. In der Praxis geht das zwar problemlos, es dauert dann nur sehr lange.
- Da *Windows Deduplikation* nur auf einem Thread läuft, können Sie mehrere Volumes einrichten, um eine bessere Performance zu erreichen. Dem steht die Tatsache entgegen, dass größere Volumes eine bessere Deduplikationsrate erreichen.
- Führen Sie die Deduplikation täglich mit einem möglichst großen Zeitfenster durch.
- Deaktivieren Sie die Veeam-Kompression und verwenden Sie als Blockgröße LAN.

17.7.8 ReFS-Volume auf einem Windows-Server

Eine weitere sehr beliebte Art des Backup-Speichers bietet ein Windows-Server mit via ReFS formatierten Partitionen. Das *Resilient File System* bietet hier das *Block Cloning*-Feature, das sich Veeam zunutze machen kann. Diese Technologie kann enorme Vorteile in Bezug auf die Speichernutzung bringen, da auch hier ähnlich wie bei der Deduplikation gleiche Datensätze nur einmalig gespeichert werden. Es muss allerdings bedacht werden, dass dieser Vorteil nur im Zusammenhang mit *Synthetic Fulls* funktioniert.

Als Beispielszenario nehmen wir an, dass wir von den 1 TB großen virtuellen Maschinen Backups für die letzten 14 Tage vorhalten wollen. Außerdem möchten wir in dem Zeitraum von jedem Samstag ein Full Backup behalten. Über den *Restore Point Simulator*, der vorhin bereits vorgestellt wurde, wird nun schnell ersichtlich (siehe Abbildung 17.9), welche enormen Vorteile Block Cloning bieten kann. Bei jedem Synthetic Full verbrauchen hier nur die veränderten Blöcke wirklich Speicherplatz auf dem Dateisystem, sämtliche auch im letzten Full Backup vorhandenen (und unveränderten) Blöcke werden verlinkt. Dadurch ist hier die Erstellung eines solchen Synthetic Fulls extrem schnell, da Veeam dies via *Fast Clone* erstellt. Die schwarzen Balken zeigen dementsprechend die Daten an, die nicht erneut geschrieben werden müssen. Wenn wir nun den Haken bei REFS / XFS entfernen würden, wäre der gesamte benötigte Speicher um ganze 1.800 GB höher.

The Restore Point Simulator

Current version : 0.4.1
Feedback via @tdewin or on GitHub
RPS heavily relies on some opensource javascript frameworks

Quick Presets

Incremental Weekly Synthetic

Configuration

Style	Incremental
Used Size GB	1000
Retention Points	14
Change Rate	10% Conservative
Data left after reduction	100% (100GB > 100GB) 1x No Compression
Interval	Daily
Time Growth Simulation	1 Year / 10%
ReFS / XFS	☑

Incremental Specific

Synthetic	☐MO	☐TU	☐WE	☐TH	☐FR	☑SA	☐SU	
Active Full Weekly	☐MO	☐TU	☐WE	☐TH	☐FR	☐SA	☐SU	
Active Full Monthly	☐Jan	☐Feb	☐Mar	☐Apr	☐May	☐Jun		
	☐Jul	☐Aug	☐Sep	☐Oct	☐Nov	☐Dec		

Run

☐Manual Run ☐Export ☐Canvas (experimental) Simulate

Result

Retention		File	Size	Modify Date	Point Date
20 (14)		full.vbk	1000 GB	2020-09-12 Sa 22	2020-09-12 Sa 22
19 (14)		incremental.vib	100 GB	2020-09-13 Su 22	2020-09-13 Su 22
18 (14)		incremental.vib	100 GB	2020-09-14 Mo 22	2020-09-14 Mo 22
17 (14)		incremental.vib	100 GB	2020-09-15 Tu 22	2020-09-15 Tu 22
16 (14)		incremental.vib	100 GB	2020-09-16 We 22	2020-09-16 We 22
15 (14)		incremental.vib	100 GB	2020-09-17 Th 22	2020-09-17 Th 22
14		incremental.vib	100 GB	2020-09-18 Fr 22	2020-09-18 Fr 22
13		full.vbk	100 GB	2020-09-19 Sa 22	2020-09-19 Sa 22
12		incremental.vib	100 GB	2020-09-20 Su 22	2020-09-20 Su 22
11		incremental.vib	100 GB	2020-09-21 Mo 22	2020-09-21 Mo 22
10		incremental.vib	100 GB	2020-09-22 Tu 22	2020-09-22 Tu 22
9		incremental.vib	100 GB	2020-09-23 We 22	2020-09-23 We 22
8		incremental.vib	100 GB	2020-09-24 Th 22	2020-09-24 Th 22
7		incremental.vib	100 GB	2020-09-25 Fr 22	2020-09-25 Fr 22
6		full.vbk	100 GB	2020-09-26 Sa 22	2020-09-26 Sa 22
5		incremental.vib	100 GB	2020-09-27 Su 22	2020-09-27 Su 22
4		incremental.vib	100 GB	2020-09-28 Mo 22	2020-09-28 Mo 22
3		incremental.vib	100 GB	2020-09-29 Tu 22	2020-09-29 Tu 22
2		incremental.vib	100 GB	2020-09-30 We 22	2020-09-30 We 22
1		incremental.vib	100 GB	2020-10-01 Th 22	2020-10-01 Th 22
			2900 GB		
		Work Space	+1050 GB		
			3950 GB		

Abbildung 17.9 »ReFS / XFS« zeigt hier, wie viel Speicherplatz bei Full Backups gespart werden kann.

Als Nachteil ist hier allerdings zu erwähnen, dass bei so erstellten Synthetic Fulls die für einen Restore benötigten Blöcke auf den Festplatten sehr weit »verstreut« liegen können, was zu starken Random-I/O führen kann und gerade bei HDDs nicht sehr effizient ist. Dadurch können Wiederherstellungen über normal via NTFS formatierte Partitionen schneller laufen.

The Restore Point Simulator

Current version : 0.4.1
Feedback via @tdewin or on GitHub
RPS heavily relies on some opensource javascript frameworks

Quick Presets

Incremental Weekly Synthetic

Configuration

Style	Backup Copy Job
Used Size GB	1000
Retention Points	7
Change Rate	10% Conservative
Data left after reduction	100% (100GB > 100GB) 1x No Compression
Interval	Daily
Time Growth Simulation	1 Year / 10%
ReFS / XFS	☑

Backup Copy Job Specific

Weekly	4
Monthly	6
Quarterly	0
Yearly	0
☐	Active Full GFS

Run

☐Manual Run ☐Export ☐Canvas (experimental) Simulate

Result

Retention		File	Size	Modify Date	Point Date
-1 -1W 6M 0Q 0Y		full.vbk	1000 GB	2020-12-12 Sa 22	2020-12-06 Su 22
-1 -1W 5M 0Q 0Y		full.vbk	500 GB	2021-01-09 Sa 22	2021-01-03 Su 22
-1 -1W 4M 0Q 0Y		full.vbk	500 GB	2021-02-13 Sa 22	2021-02-07 Su 22
-1 -1W 3M 0Q 0Y		full.vbk	500 GB	2021-03-13 Sa 22	2021-03-07 Su 22
-1 -1W 2M 0Q 0Y		full.vbk	500 GB	2021-04-10 Sa 22	2021-04-04 Su 22
-1 -1W 1M 0Q 0Y		full.vbk	500 GB	2021-05-08 Sa 22	2021-05-02 Su 22
-1 4W 0M 0Q 0Y		full.vbk	300 GB	2021-05-15 Sa 22	2021-05-09 Su 22
-1 3W 0M 0Q 0Y		full.vbk	300 GB	2021-05-22 Sa 22	2021-05-16 Su 22
-1 2W 0M 0Q 0Y		full.vbk	300 GB	2021-05-29 Sa 22	2021-05-23 Su 22
-1 1W 0M 0Q 0Y		full.vbk	300 GB	2021-06-05 Sa 22	2021-05-30 Su 22
7		full.vbk	300 GB	2021-06-08 Tu 22	2021-06-02 We 22
6		incremental.vib	100 GB	2021-06-03 Th 22	2021-06-03 Th 22
5		incremental.vib	100 GB	2021-06-04 Fr 22	2021-06-04 Fr 22
4		incremental.vib	100 GB	2021-06-05 Sa 22	2021-06-05 Sa 22
3 *W *M 0Q 0Y		incremental.vib	100 GB	2021-06-06 Su 22	2021-06-06 Su 22
2		incremental.vib	100 GB	2021-06-07 Mo 22	2021-06-07 Mo 22
1		incremental.vib	100 GB	2021-06-08 Tu 22	2021-06-08 Tu 22
			5600 GB		
		Work Space	+1050 GB		
			6650 GB		

Abbildung 17.10 Hier wird anhand der schwarzen Balken gut sichtbar, wie viel Speicherplatz durch die Verwendung einer via ReFS formatierten Partition eingespart werden kann.

Wenn man nun allerdings einen Schritt weitergeht und möchte, dass über einen Backup-Copy-Job ein *GFS* aufgebaut wird, in dem beispielsweise die letzten sieben Tagessicherungen, vier Wochensicherungen sowie sechs Monatssicherungen vorgehalten werden, kann die Speicherersparnis enorm sein, wie in Abbildung 17.10 zu sehen ist. Ohne ReFS würden hier 6.000 GB mehr an Speicherplatz verbraucht werden, wodurch wir ein fast doppelt so großes Speichersystem benötigten.

Um eine schnelle Erstellung der *Synthetic Fulls* via *Fast Clone* zu gewährleiten, sollte allerdings darauf geachtet werden, dass ein Backup-Job auch nur auf ein Repository bzw. ein Extent eines Scale-out-Repository schreibt. Wenn das nicht der Fall ist, entfällt für diese Daten die schnelle Fast-Clone-Variante, und die Erstellung des Full Backups kann somit deutlich mehr Zeit in Anspruch nehmen.

17.8 Veeam Backup & Replication installieren

Die Installation von Veeam B&R ist recht einfach. Hat man noch keine Lizenz zur Hand, empfiehlt sich der Einsatz einer Demolizenz. Hierfür melden Sie sich auf der Webseite von Veeam an, klicken auf PRODUCTS • VEEAM BACKUP & REPLICATION und dann auf den Link, der das kostenlose Testen verspricht. Neben der Weiterleitung zum Download der ISO-Datei wird Ihnen eine E-Mail mit einer Lizenzdatei zugeschickt. Diese ist zwingend notwendig, da sonst nicht alle Funktionen zur Verfügung stehen.

Wenn Sie aus der ISO-Datei heraus die Installation starten, erscheint das Installationsmenü. Mit einem Klick auf INSTALL direkt unter der Überschrift VEEAM BACKUP & REPLICATION 10A geht es los.

Akzeptieren Sie die Lizenzvereinbarung und fügen Sie anschließend im nächsten Fenster die zuvor erwähnte Lizenzdatei der Installation hinzu. Im nächsten Fenster wählen Sie die Komponenten aus, die Sie installieren wollen.

Für die erste einfache Installation nehmen Sie die Default-Settings und klicken weiter. Daraufhin überprüft Veeam, ob das System die Voraussetzungen erfüllt. Sollten Softwarekomponenten fehlen, beispielsweise *MS SQL Management Objects*, bietet Veeam die Installation an, die Sie durch einen Klick auf INSTALL durchführen. Bei der anschließenden erneuten Überprüfung sollte Veeam dann alle Voraussetzungen als erfüllt ansehen, und Sie können die Installation fortführen.

Eine letzte Übersicht erscheint, in der Sie noch den Haken für die erweiterten Einstellungen setzen können, um unter anderem die zu verwendenden Ports, die Installationsverzeichnisse sowie den SQL-Server weiter anzupassen. Anschließend starten Sie die Installation aller ausgewählten Komponenten mit einem Klick auf INSTALL.

Anders als in früheren Versionen, bei denen Veeam nur den Stand des Master-ISO-Images installierte, werden nun direkt mit der ISO-Datei auch die neuesten Updates mitgeliefert.

Entsprechend sehen Sie im Fortschrittsbalken die Installation von Updates ebenfalls. Nach der Fertigstellung sollte ein Reboot der Maschine durchgeführt werden. Anschließend können Sie über das Icon auf dem Desktop die Veeam-Applikation starten (siehe Abbildung 17.11).

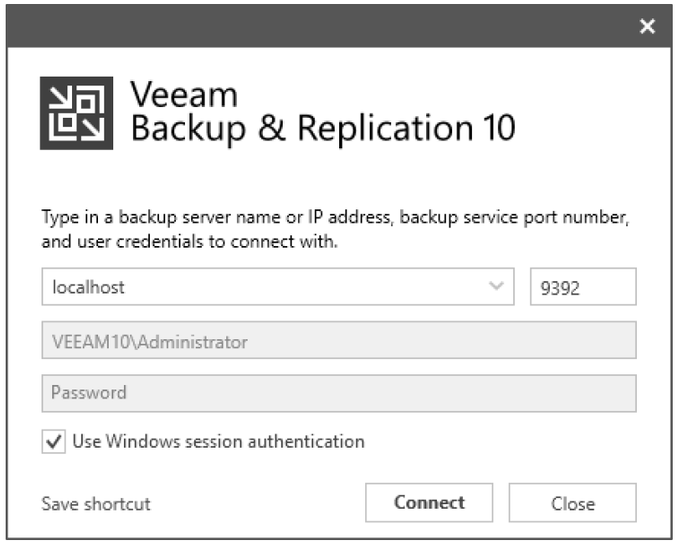


Abbildung 17.11 Das Anmeldefenster von Veeam B&R

Falls Sie nach einem Klick auf CONNECT Probleme haben, sich anzumelden, oder nach der Anmeldung andere Phänomene auftreten, die vermutlich auf Netzwerkprobleme zurückzuführen sind, sollten Sie zuerst die Windows-Firewall überprüfen. Auf der Veeam-VM, der Ziel-VM für das Backup, auf dem Backup-Repository, dem Backup-Proxy etc. kann es hier passieren, dass die Windows-Firewall noch Zugriffe blockt. In solch einem Fall sollten der Firewall die benötigten Ausnahmeregeln hinzugefügt werden.

Der übliche Startbildschirm der Veeam-Konsole erscheint. Hier sollte man ein Auge auf die Lizenzdauer und die Version haben. In der eigentlichen Konsole wird man dann direkt auf entsprechende Probleme oder Tasks aufmerksam gemacht.

17.9 Veeam richtig konfigurieren

Bevor die ersten virtuellen Maschinen gesichert werden können, muss Veeam natürlich für die jeweilige Umgebung angepasst werden. Hier starten wir nun in der Veeam-Konsole links unten im Bereich BACKUP INFRASTRUCTURE und gehen die wichtigsten Punkte in der linken Leiste durch.

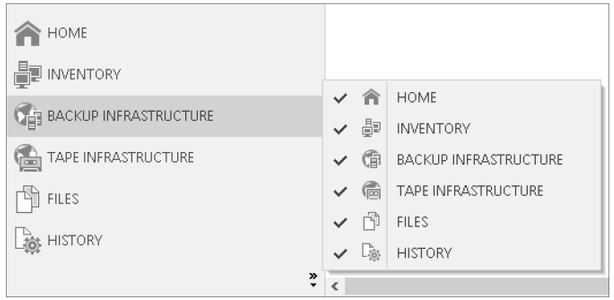


Abbildung 17.12 Falls Sie einen der nun angesprochenen Punkte nicht finden, sollten Sie über den hier markierten Button prüfen, ob der jeweilige Punkt vielleicht nicht angehakt ist.

17.9.1 Einrichtung des Backup-Proxys

Zuallererst sollten Sie einen Backup-Proxy konfigurieren. Veeam hat für VMware bereits einen Default-Proxy erstellt, der natürlich auf dem Veeam-Server selbst läuft.

Sie können einfach den vordefinierten Proxy nutzen oder auch direkt einen oder mehrere neue Proxys hinzufügen. In dem Bearbeitungsmenü eines Proxys können Sie unter anderem Feineinstellungen wie die Anzahl der maximal gleichzeitig erlaubten Tasks oder auch den gewollten Transport Mode konfigurieren.

17.9.2 Einrichtung eines Backup-Repository

Auch hier kommt Veeam bereits mit einer Vorkonfiguration. Das Default-Backup-Repository zeigt auf eine lokale Partition des Backup-Servers selbst, hier werden auch direkt automatisch Konfigurations-Backups von Veeam gespeichert. Es empfiehlt sich, daran keine Änderungen vorzunehmen und das Default-Backup-Repository nicht weiter zu nutzen bzw. für »echte« Backup-Jobs andere Backup-Repositories zu konfigurieren.

Beim Einrichten eines Backup-Repository können Sie, wie schon zuvor beschrieben, entsprechende Einstellungen bezüglich der maximalen Anzahl der Concurrent Tasks sowie der maximalen Schreib- und Leserate festlegen (siehe Abbildung 17.13). Entsprechend ihrer zuvor geplanten Zielumgebung sollten Sie hier die benötigten Einstellungen vornehmen.

Unter dem Punkt ADVANCED können Sie unter anderem auch die bereits erwähnte Option USE PER-VM BACKUP FILES auswählen, wodurch pro virtuelle Maschine eigene Sicherungsdateien erstellt werden und damit die Schreibvorgänge in mehr Streams aufgeteilt werden können.

Ebenso können Sie bei der Einrichtung eines Backup-Repository Einstellungen für den Mount-Server vornehmen oder Ports verändern. Hier gilt ebenso, dass für stark verteilte Installationen die Auswahl angepasst werden muss, um eine optimale Performance zu erreichen. Wer sich nicht sicher ist, fährt mit den Default-Settings allerdings erst einmal ganz gut.

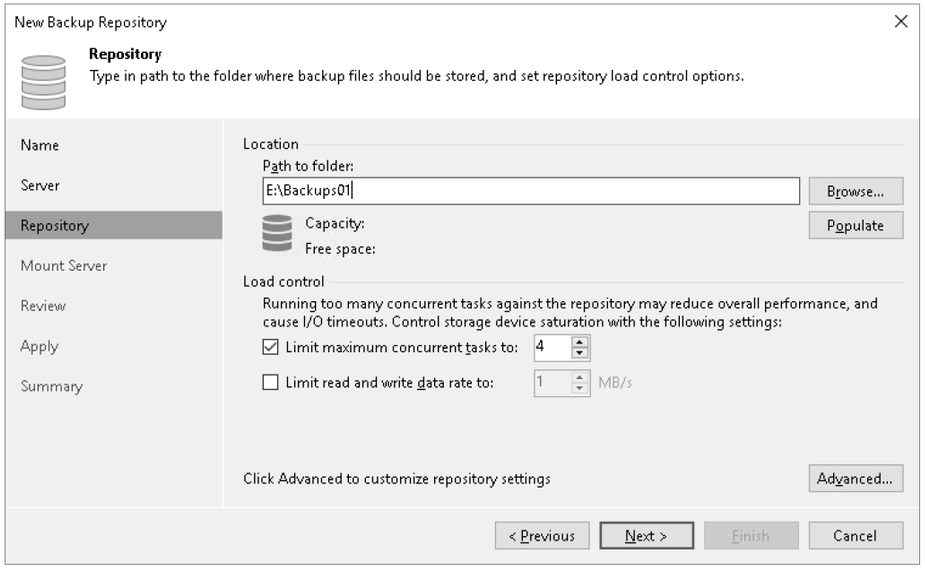


Abbildung 17.13 Einstellungen des Backup-Repository zu Location und Limits

Nachdem Sie das erste Repository erstellt haben, werden Sie auch gleich gefragt, ob Veeam seine automatischen Konfigurationssicherungen nur noch dort speichern soll. Hier sollten Sie sich überlegen, wo genau diese Konfiguration gerade für einen Worst Case am sichersten gelagert wäre.

17.9.3 Anbindung an das vCenter

Wenn Sie auf der linken Seite auf MANAGED SERVERS klicken, erscheint in der Mittelkonsole eine Auswahl der zu konfigurierenden Server. Sie wählen dort *VMware vSphere* aus und starten damit die Anbindung an das vCenter.

Geben Sie dann den DNS-Namen oder die IP-Adresse des vCenters ein und konfigurieren Sie im nächsten Fenster einen User, der sich mit den notwendigen Rechten dort anmelden darf.

Anschließend versucht Veeam, die Verbindung zum vCenter herzustellen. Wie üblich wird eine Bestätigung dazu angefordert, dass Sie dem Zertifikat vertrauen; bestätigen Sie diese (siehe Abbildung 17.14).

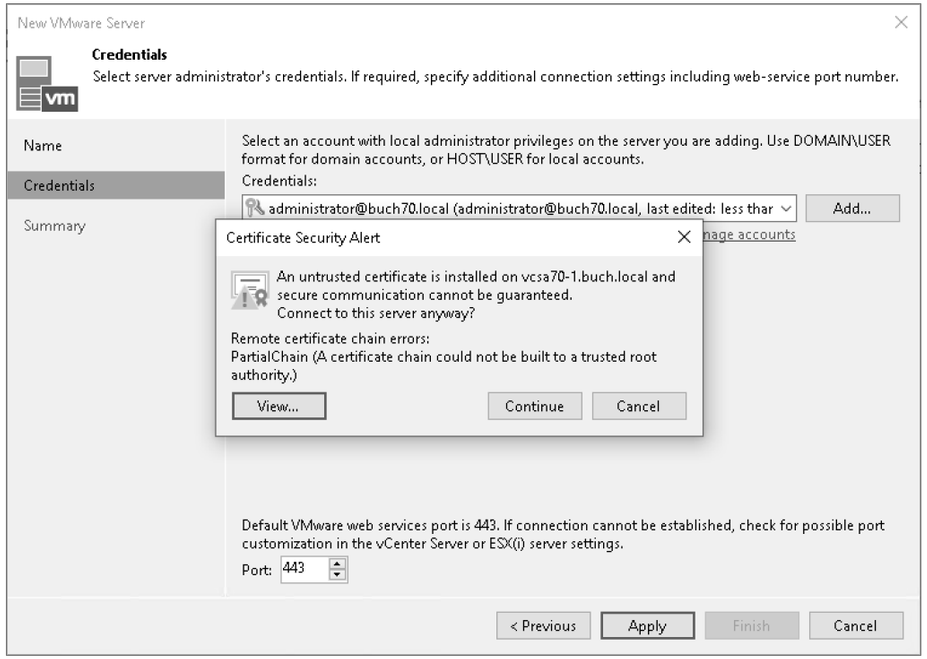


Abbildung 17.14 Mit »Continue« verbinden Sie sich mit dem vCenter und vertrauen ihm gleichzeitig.

Nachdem Sie das vCenter hinzugefügt haben, ist dieses in der Veeam-Konsole als MANAGED SERVER sichtbar (siehe Abbildung 17.15).

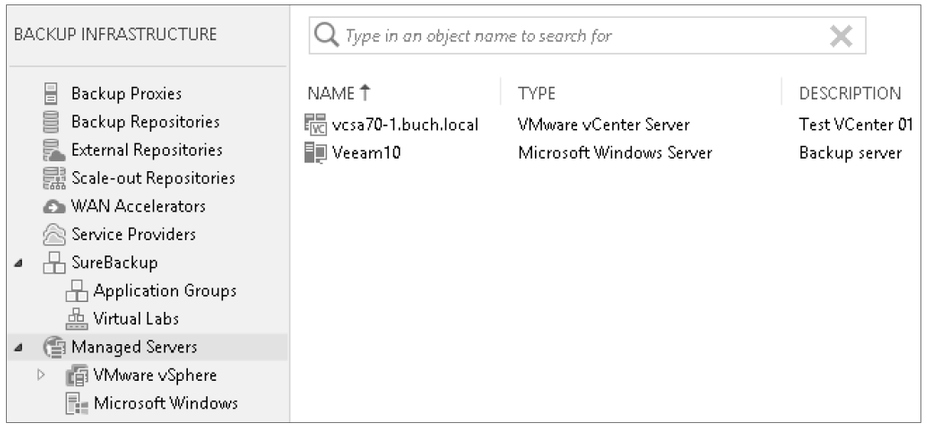


Abbildung 17.15 Veeam-Konsole nach Anbindung des vCenters

17.10 Erstellen von Backups

In diesem Abschnitt zeigen wir Ihnen, wie Sie Backup-Jobs anlegen.

17.10.1 Den ersten Backup-Job erstellen

Nachdem wir in den letzten beiden Abschnitten die Konfiguration der Backup-Komponenten abgeschlossen haben, erstellen wir nun unseren ersten Backup-Job. Andere Jobs, beispielsweise Backup-Copy-Jobs oder Replication-Jobs, verhalten sich ähnlich und unterscheiden sich nur in gewissen Details. Darüber hinaus nutzen wir diesen Absatz dafür, die komplette Konfiguration eines Backup-Jobs bebildert zu zeigen. Die technischen Feinheiten und Details zu verschiedenen Einstellungen beschreiben wir anschließend.

Abbildung 17.16 zeigt die Veeam-Konsole, wie sie erscheint, wenn Sie HOME • JOBS aufrufen. Über die Buttons in der Menüleiste der Konsole oder per Rechtklick lassen sich nun Jobs anlegen.

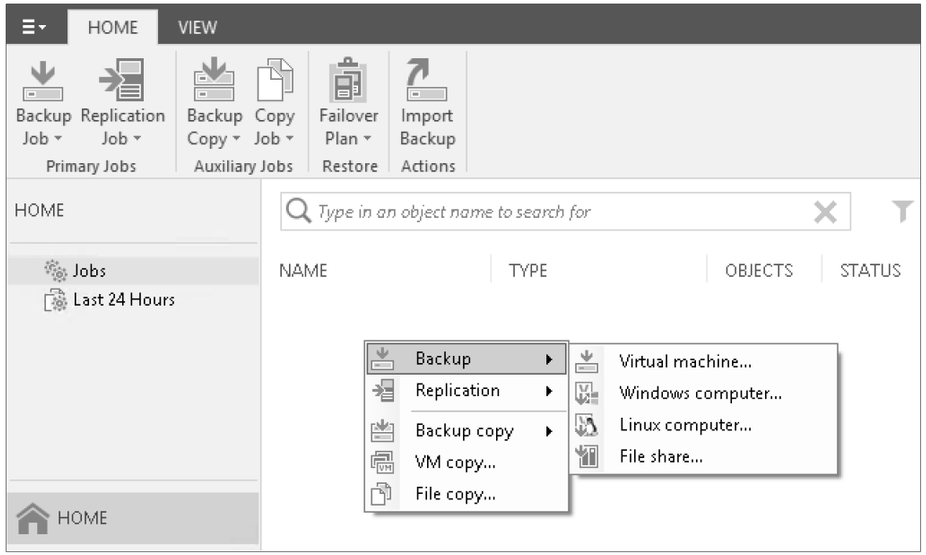


Abbildung 17.16 Erstellung unseres ersten Backup-Jobs

Wir wählen verständlicherweise BACKUP • VIRTUAL MACHINE aus und vergeben einen Namen für den Backup-Job. Es empfiehlt sich, die Namen der Backup-Jobs einfach bzw. lesbar zu halten. Mit wachsender Anzahl verliert man ansonsten schnell den Überblick.

Im Fenster aus Abbildung 17.17 wählen wir nun über ADD die Objekte aus, die in diesem Backup-Job gesichert werden sollen. Neben VMs – das ist das einfachste Objekt – können über die Icons oben rechts im Auswahlfenster auch Gruppen, Ordner, Datenspeicher, Cluster

etc. ausgewählt werden. Es dauert einen kurzen Moment, bis die Objekte aus dem vCenter gelesen sind. Wählen Sie Objektgruppen aus, können auch entsprechende Ausschlüsse konfiguriert werden.

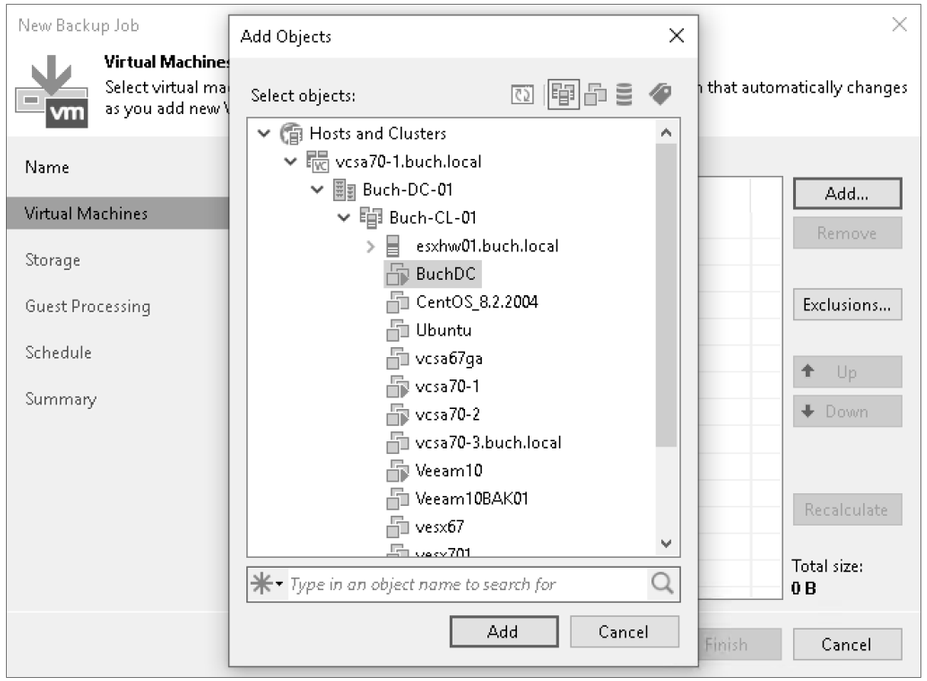


Abbildung 17.17 Auswahl der zur Sicherung vorgesehenen Objekte

Veeam versucht nun, die Objektgröße zu berechnen. Dies kann hilfreich sein, um schon an dieser Stelle festzustellen, dass die Anzahl der Objekte vielleicht die Größe eines Backup-Repository, das Sie zuvor erstellt haben, überschreitet.

Im nächsten Fenster stellen wir die STORAGE-Optionen ein (siehe Abbildung 17.18). Hier können Sie den BACKUP PROXY, das BACKUP REPOSITORY sowie die Retention Policy anpassen.

Neu ist hier unter anderem die Möglichkeit, die Vorhaltezeit nun auch in Tagen angeben zu können (RETENTION POLICY: DAYS). Früher konnte nur die Anzahl der zu behaltenden Sicherungspunkte eingestellt werden, was ein doch sehr wichtiger Unterschied ist. So wird meist dem Business gegenüber versichert, Sicherungen für einen bestimmten Zeitraum vorzuhalten und nicht eine gewisse Anzahl an Sicherungen. Hier sollte auch bei bereits bestehenden Veeam-Installationen geprüft werden, ob eine Anpassung dieser Policy nicht eine gute Idee wäre.

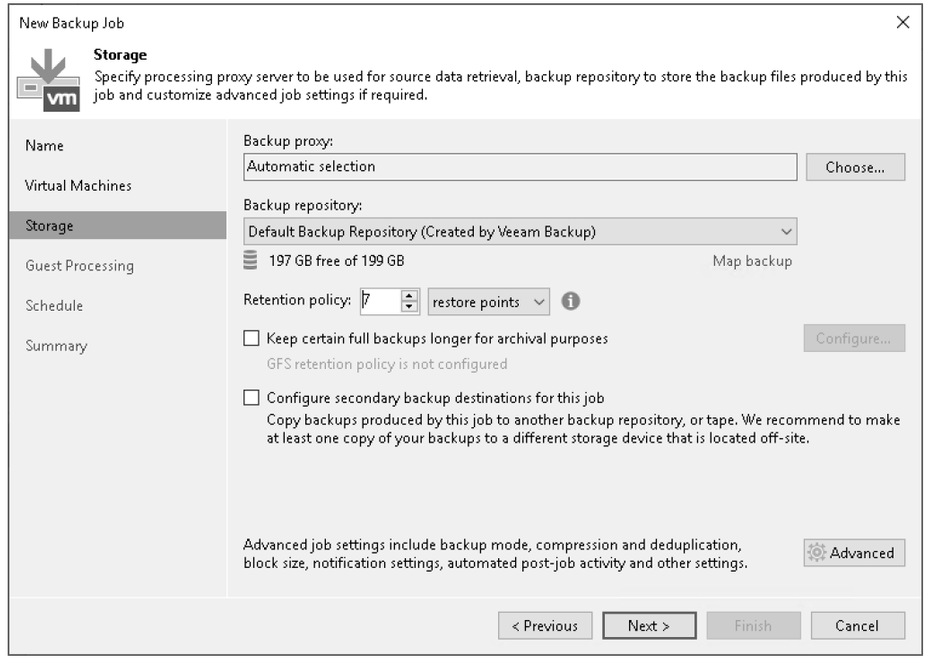


Abbildung 17.18 Einstellen des Backup-Repository und weiterer Optionen

Auch neu ist die Möglichkeit, direkt im Backup-Job ein GFS aufzubauen, dies war bisher den Backup-Copy-Jobs vorbehalten – ein weiterer Punkt, den man definitiv in seinem Zieldesign mit bedenken sollte.

Optional können Sie hier auch direkt Backup-Copy-Jobs konfigurieren (CONFIGURE SECONDARY BACKUP DESTINATIONS FOR THIS JOB) sowie erweiterte Einstellungen (ADVANCED) vornehmen.

Bei den erweiterten Einstellungen (siehe Abbildung 17.19) gibt es eine große Auswahl, die wir später detaillierter beschreiben werden. Prinzipiell sind die Einstellungen einfach zu verstehen, wenn Sie sich vorher Gedanken zu Ihrer Backup-Strategie gemacht haben.

Im Fenster GUEST PROCESSING (siehe Abbildung 17.20) können Sie die Application-Awareness und das Guest-Indexing aktivieren. Per Default sind beide nicht ausgewählt. Für die Sicherung eines Fileservers sind beide Optionen nicht zwingend notwendig. Das Indexing kommt erst dann wirklich ins Spiel, sofern Sie als Self-Service die *Veeam 1-Click Recovery* über den Enterprise Manager den Endusern anbieten möchten.

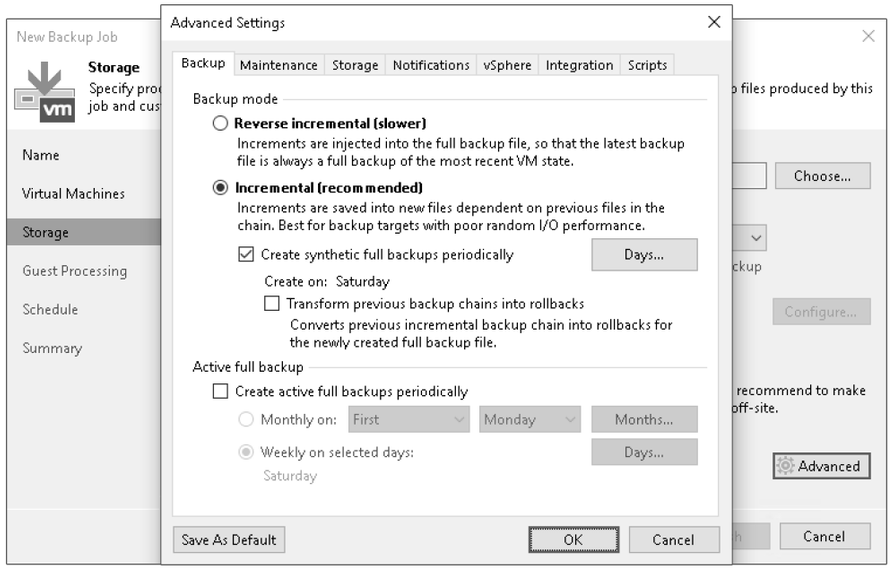


Abbildung 17.19 Die erweiterten Optionen bieten eine große Auswahl.

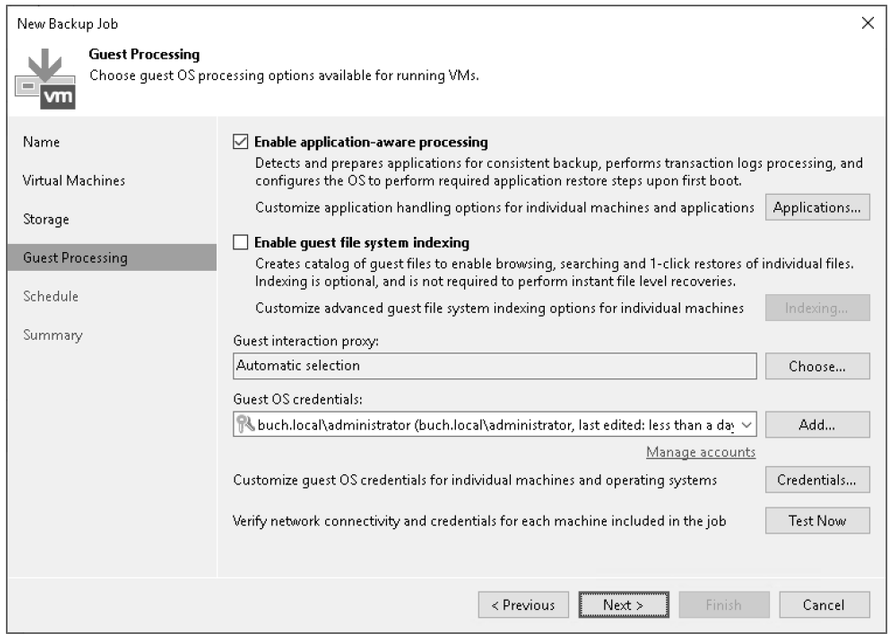


Abbildung 17.20 »Guest Processing« mit Optionen zur Application-Awareness und zum Indexing

Wenn Sie eine oder beide Optionen aktivieren, muss Veeam Zugriff auf die Gast-VM haben, und es müssen entsprechende Zugriffs-Accounts hinterlegt sein. Hier kommt Ihnen die schon angesprochene Integration mit Active Directory zu Hilfe. Sie können alternativ auch manuell einzelne Accounts definieren, was zwar ein bisschen mehr Handarbeit erfordert, aber gerade zum Beispiel bei Systemen innerhalb eines abgeschotteten Netzes meist nicht zu verhindern ist.

Klicken Sie zum Abschluss auf TEST NOW. Veeam führt dann eine Überprüfung der zur Verfügung gestellten Zugriffs-Accounts durch und testet die Zugangsdaten sowie Einstellungen. So lassen sich entsprechende Probleme direkt erkennen (siehe Abbildung 17.21). Wenn Sie diesen Schritt überspringen und die VMs des Jobs die definierten Zugriffs-Accounts nicht akzeptieren, wird das Backup fehlschlagen.

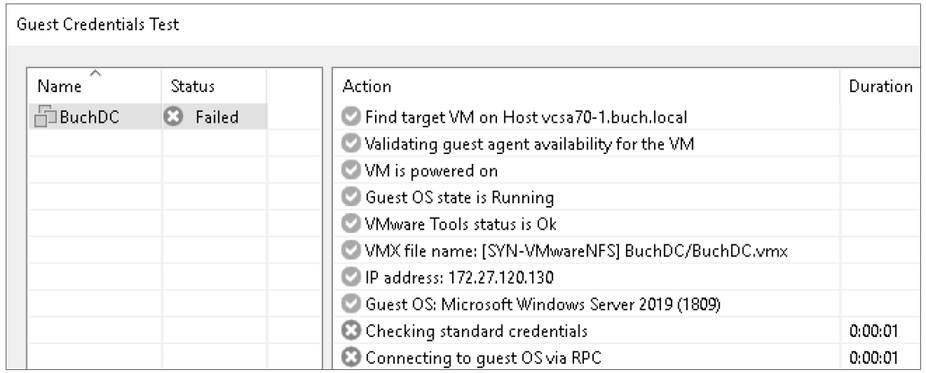


Abbildung 17.21 Ein Problem ist beim Zugriff auf das Gastbetriebssystem der VM entstanden.

> **Windows-Firewall**
>
> An dieser Stelle ist wieder der Hinweis wichtig, dass die Firewall bei Windows-VMs genau in solch einer Situation zu einem Problem werden kann, wenn nicht die entsprechenden Regeln konfiguriert sind.

Ist nun alles korrekt eingestellt und wurden die Accounts für die Anmeldung an den VMs hinterlegt, sollte das Ergebnis des Tests wie in Abbildung 17.22 aussehen. Alles funktioniert und die Angaben sind richtig.

Im Fenster aus Abbildung 17.23 definieren Sie die Backup-Zeitfenster und legen die unterschiedlichen Muster fest, nach denen der Backup-Job durchgeführt wird.

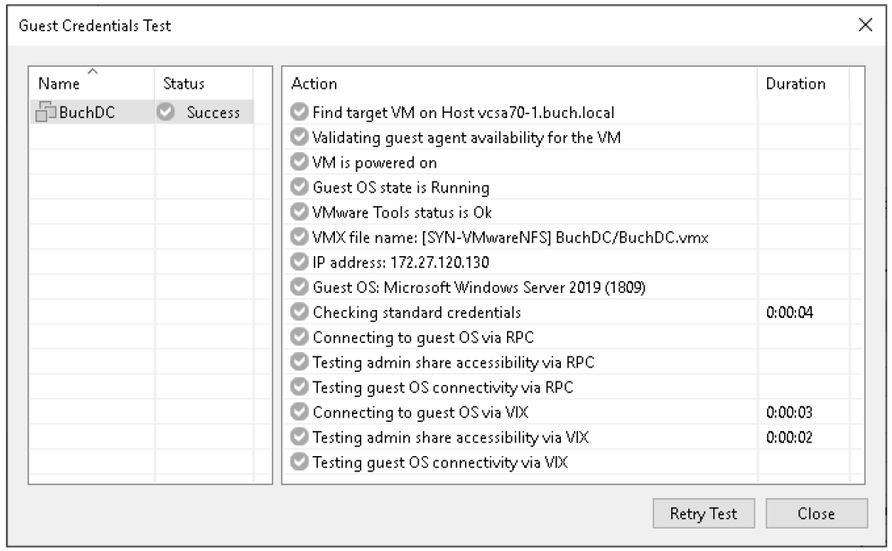


Abbildung 17.22 Wenn alle Parameter stimmen, kann sich Veeam nun korrekt am Gastbetriebssystem der VM anmelden.

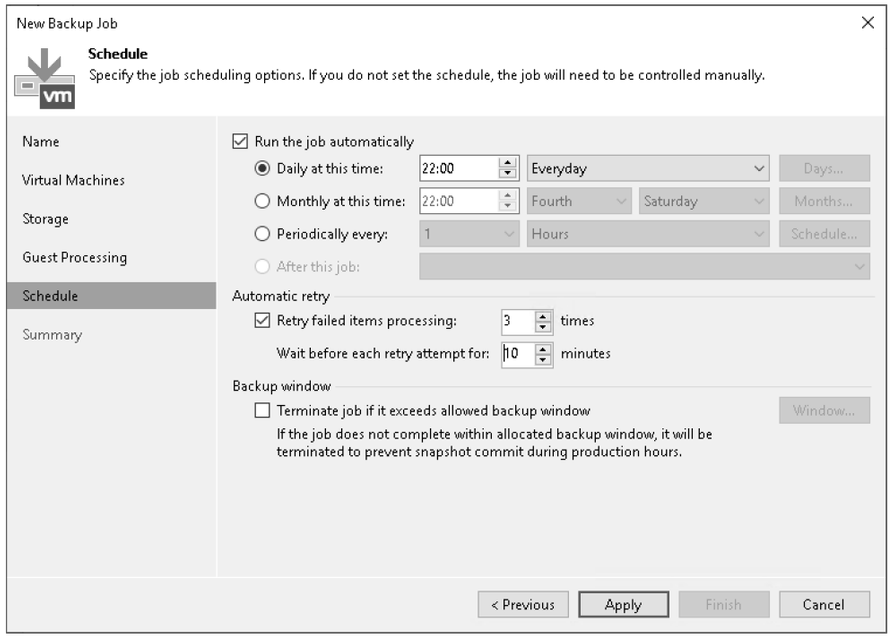


Abbildung 17.23 Einstellen des Zeitplans für die automatische Ausführung des Backup-Jobs

Es gibt die Optionen *täglich*, *monatlich*, *periodisch* (alle x Minuten, Stunden, durchgehend) oder *nach einem vorangegangenen Job*. Auch lassen sich die Anzahl der Versuche (RETRY FAILED ITEMS PROCESSING) sowie die Wartezeit dazwischen (WAIT BEFORE EACH RETRY ATTEMPT FOR) einstellen. VMs neigen unter Last dazu, nicht ausreichend schnell auf die Backup-Anfrage von Veeam zu reagieren. Veeam versucht es dann später erneut. Diese Einstellung kann große Auswirkungen auf die Dauer Ihres Backup-Jobs haben, wenn die Anzahl der Versuche und die Wartezeit entsprechend hoch eingestellt werden.

Darüber hinaus lassen sich Zeitfenster definieren, in denen keine Backups laufen dürfen (siehe Abbildung 17.24). Dies wird immer wieder gern mit der löblichen Idee genutzt, während der Produktionsphasen, also beispielsweise zwischen 8 und 20 Uhr, keine Backups durchzuführen, die den Arbeitsbetrieb beeinträchtigen könnten. In der Praxis ist es allerdings deutlich besser, wenn Sie sich gar nicht darum kümmern müssen und die Produktions- und Backup-Infrastruktur ausreichend Leistung mitbringt, um die gewünschten Zeitfenster für Backups einzuhalten.

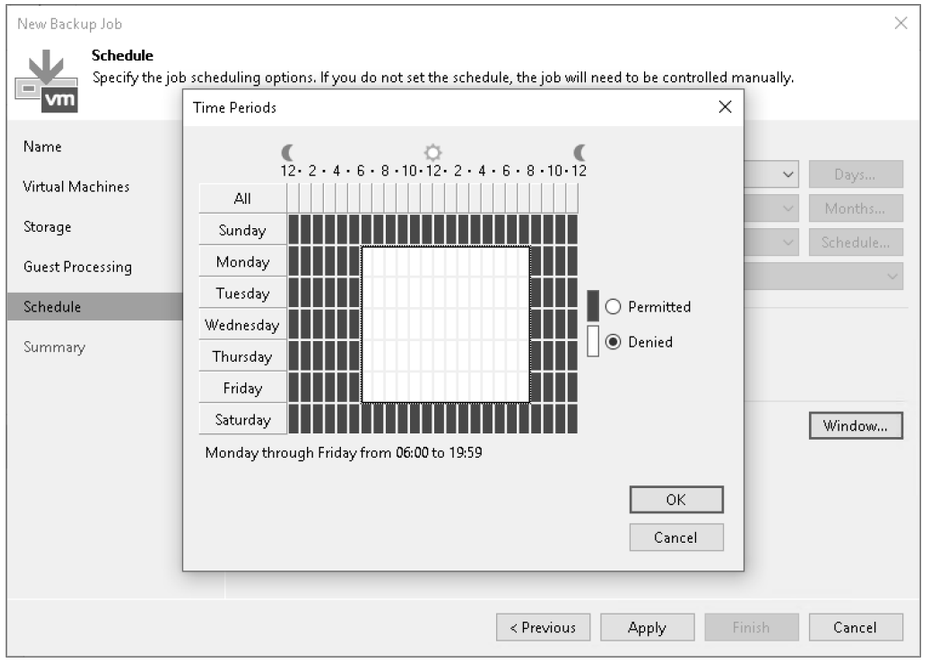


Abbildung 17.24 Zeitfenster für die Jobabarbeitung festlegen

Im letzten Fenster wird eine abschließende Übersicht präsentiert. Sie können den Backup-Job hier, wenn gewünscht, direkt starten.

Der laufende Backup-Job wird in der Veeam-Konsole angezeigt. Durch einfaches Klicken auf den Job lassen Sie sich Details anzeigen (siehe Abbildung 17.25).

Ebenso können Sie sich durch Auswahl einer VM Detailinformationen zu ihr anzeigen lassen (siehe Abbildung 17.26).

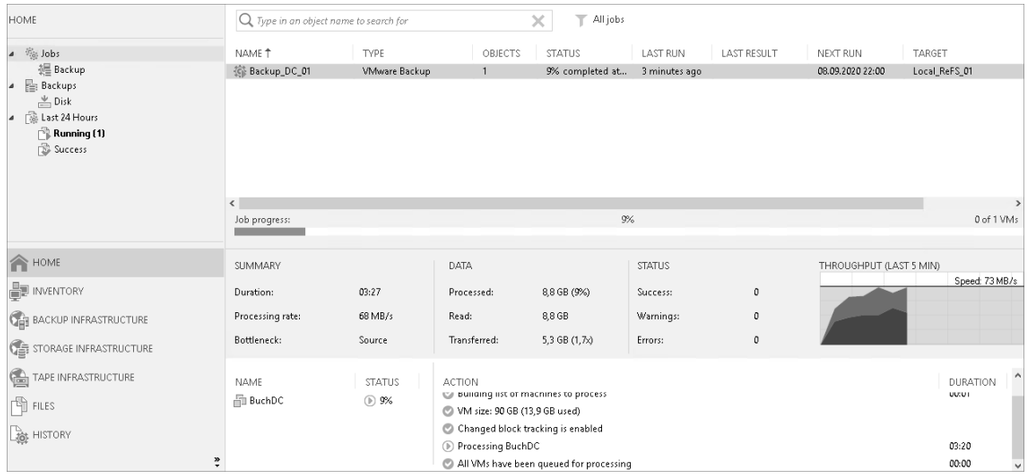


Abbildung 17.25 Backup-Job und Details

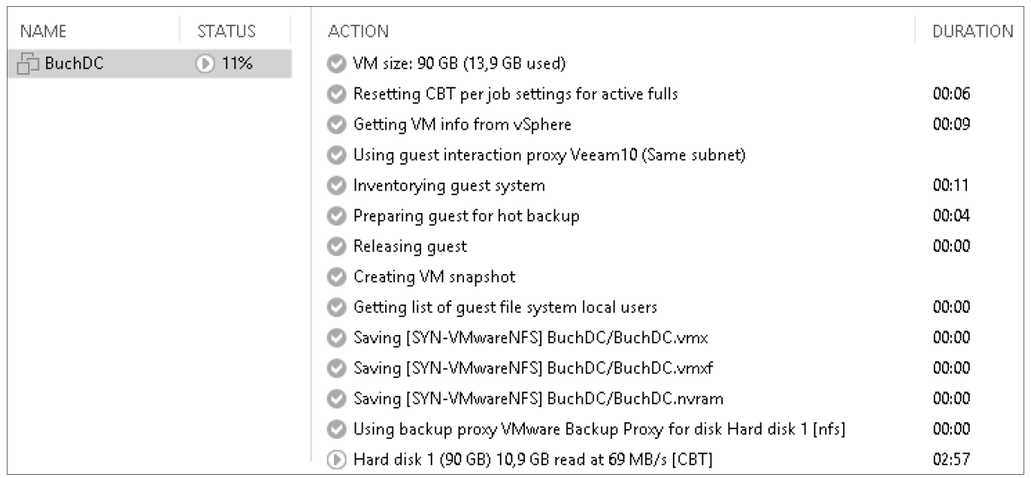


Abbildung 17.26 Details einer VM innerhalb des Backup-Jobs

Es empfiehlt sich, E-Mail-Benachrichtigungen (global für Veeam oder einzeln pro Job) einzurichten, um eine entsprechende Übersicht zu erhalten.

17.10.2 Backup-Methoden

Wie in dem einen oder anderen Beispiel bereits angesprochen, verfügt *Veeam Backup & Replication* über verschiedene Backup-Methoden, die eine Vielzahl unterschiedlicher Use Cases abdecken. Dabei erzeugen die unterschiedlichen Backup-Methoden unterschiedlich viele Schreibzugriffe auf den Produktions- und Backup-Speichersystemen, und zwar:

- **Forward Incremental** – einfache I/O-Last für die Differenz-Backups
- **Forward Incremental with Active Full (d. h. mit aktivem Voll-Backup)** – einfache I/O-Last für das gesamte Backup
- **Forward Incremental with Synthetic Full (d. h. mit synthetisiertem Voll-Backup)** – doppelte I/O-Last (einmal schreibend, einmal lesend) für die gesamte Backup-Kette
- **Reversed Incremental** – dreifache I/O-Last (zweimal schreibend, einmal lesend) für das Differenz-Backup
- **Synthetic Full with Transform to Rollbacks** – vierfache I/O-Last (zweimal schreibend, zweimal lesend) für die gesamte Backup-Kette

Dies zeigt recht deutlich, dass sich die verschiedenen Modi nicht nur vom Denkansatz her deutlich unterscheiden, sondern auch in der Last, die sie für die Speichersysteme produzieren. Sollte die Notwendigkeit bestehen, die I/O-Last zu verringern, lassen sich entsprechende Backup-Modi nutzen. Außerdem bestehen weitere Möglichkeiten in Kombination mit bestimmten Dateisystemen. So erlaubt es *Microsoft ReFS* mit Windows Server 2016 oder neuer, unnötige I/O-Last zu vermeiden.

Man unterscheidet folgende Modi:

- **Forward Incremental** – Eine der einfachsten Methoden sind vorwärts inkrementelle Backups. Die Last für Speichersysteme ist hier am geringsten. Wegen der periodisch notwendigen Voll-Backups (aktiv voll oder synthetisch, üblicherweise wöchentlich) wird mehr Speicherkapazität benötigt als bei anderen Methoden. Mit jedem neuen Voll-Backup wird eine neue Backup-Kette erzeugt, womit ältere Backups und Backup-Ketten entfernt werden können.
- **Active Full** – Die ganze VM wird gelesen (mit Ausnahme von leeren Blöcken oder Swap-Bereichen) und anschließend in einer VBK-Datei, oftmals komprimiert und dedupliziert, gespeichert. Jedes Voll-Backup erzeugt eine neue VBK-Datei. Prinzipiell ist die I/O-Last hoch, da alle Blöcke vom Speicher gelesen und anschließend auf den Backup-Speicher geschrieben werden müssen. CBT (*Changed Block Tracking*, siehe Abschnitt 17.4.3) wird hier entsprechend nicht genutzt. Insgesamt dauern solche Voll-Backups auch entsprechend länger im Verhältnis zu inkrementellen Backups.
- **Synthetic Full** – Nachdem ein neues, inkrementelles Backup geschrieben wurde, wird es mit den vorangegangenen Differenz-Backups und dem letzten Voll-Backup zu einem neuen Voll-Backup zusammengeführt oder, anders gesagt, *synthetisiert*. Ein Vorteil hierbei ist, dass die Synthetisierung im Backup-Repository stattfindet und keine I/Os im

Produktionsspeicher erzeugt. Dadurch ist es sinnvoll, mehrere kleinere Backup-Jobs mit einer geringen Anzahl von VMs zu nutzen, um die Synthetisierung zu beschleunigen. Dies funktioniert am besten mit der Option PER-VM BACKUP FILES.

- **Forever Forward Incremental** – Nach der Erstellung des ersten Voll-Backups werden nur noch inkrementelle Backups erstellt. Am Ende der Vorhaltedauer, beispielsweise nach 30 täglichen Restore-Points, wird das 31. Backup geschrieben, und das erste bzw. älteste inkrementelle Backup wird mit dem Voll-Backup zusammengeführt und anschließend gelöscht. Dies hat den Vorteil, dass nur sehr wenig Speicherkapazität verbraucht wird. Auf der anderen Seite entsteht ein Nachteil für die Wiederherstellung, da das Voll-Backup und die Differenzen zunächst zusammen »geöffnet« werden müssen. Dies macht sich besonders beim Öffnen des letzten Restore-Points bemerkbar. In unserem Beispiel muss Veeam insgesamt 31 Dateien, also eine VBK-Datei und 30 VIB-Dateien, öffnen bzw. aufbereiten, damit ein vollständiges Restore oder vielleicht sogar nur die Wiederherstellung einer einzigen Datei aus jener VM durchgeführt werden kann. Dementsprechend entsteht eine relativ hohe I/O-Last.
- **Reverse Incremental** – Nachdem ein Voll-Backup geschrieben wurde, werden anschließend nur noch inkrementelle Backups erzeugt. Allerdings wird das letzte, neueste inkrementelle Backup mit dem Voll-Backup zusammengeführt. Dadurch »bewegt« sich das Voll-Backup nach vorne und ist immer die aktuellste Backup-Datei. Auf dem Backup-Repository sind die Differenzdateien an ihrer Endung *.vrb* leicht zu erkennen (anders als die VIB-Dateien bei *Forward Incremental*). Durch diese Methode erfolgt das Öffnen des aktuellsten Restore-Points schneller, da es sich ja um das (im Prinzip synthetisierte) Voll-Backup handelt. Erst wenn Sie Restore-Points hinter dem aktuellsten auswählen, muss Veeam die VBK-Datei und die VRB-Dateien entpacken und für den User zusammen präsentieren.

17.10.3 Verschlüsselung

Veeam Backup & Replication bietet die Möglichkeit, Daten sowohl auf dem Weg zum Ziel als auch auf dem Zielspeichermedium zu verschlüsseln. Die Backup-Job- und Backup-Copy-Job-Einstellungen stellen die Verschlüsselung auf dem Zielspeichermedium ein, wenn die Daten geschrieben wurden. Entsprechend bietet sich die Verschlüsselung der Backup-Daten dort an, wo diese z. B. von externen Medien wie Tapes und mobilen Festplatten aus dem Rechenzentrum entfernt werden.

Einige Dinge gibt es bei der Nutzung von Verschlüsselung zu beachten:

- Die Verschlüsselung verhindert nicht, dass berechtigte Veeam-User Zugriff auf das Backup haben.
- Das zur Verschlüsselung genutzte Passwort sollte sicher aufbewahrt werden, und natürlich sollten Sie ein entsprechend starkes Passwort verwenden. Eine Wiederherstellung ohne das Passwort ist im Veeam möglich, erfordert aber gewisse Voraussetzungen, die

in der Veeam-B&R-Dokumentation zu finden sind (siehe dazu *https://helpcenter.veeam.com/docs/backup/vsphere/decryption_no_pass_hiw.html?ver=100* und *https://helpcenter.veeam.com/docs/backup/vsphere/decrypt_without_pass.html?ver=100*).

- Wenn Sie die Verschlüsselung aktivieren, ist zunächst ein *Active Full*-Backup notwendig.
- Natürlich wird etwas mehr CPU-Leistung bei der Erstellung verschlüsselter Backups als bei unverschlüsselten Backups benötigt. Dies macht in der Regel nicht viel aus, sollte aber berücksichtigt werden, gerade wenn der eine oder andere Backup-Proxy ohnehin schon an seiner Leistungsgrenze operiert.

Prinzipiell gelten diese Best Practices für alle Disk- und Tape-Backups. Möchten Sie diese Daten während der Übertragung verschlüsseln, ist das auch dann möglich, wenn die eigentlichen Backup-Daten im Zielspeicher später nicht verschlüsselt sind. Diese Einstellung lässt sich über die NETWORK TRAFFIC-Optionen treffen.

17.10.4 Komprimierung und Deduplikation

Wie schon zuvor erwähnt, sollten Sie sich von der Komprimierung und Deduplikation nicht zu viel versprechen: Wer das tut, wird in aller Regel schnell enttäuscht. Gerade bei der Deduplikation sollten Sie am besten mit wenig rechnen und sich über alles freuen, was am Ende dedupliziert wird. Zu diesem Thema hatten wir schon bei den unterschiedlichen Backup-Zielen in Abschnitt 17.6.2 ein paar Worte verloren. Im Folgenden soll es nun darum gehen, welche *Speicheroptimierungen* Veeam B&R anbietet:

- **Local** – Hier liest und berechnet Veeam die Daten und Hashes in 1-MB-Chunks.
- **LAN** – Empfohlen bei dateibasierten Repositories wie SMB. Veeam nutzt hier 512-KB-Chunks.
- **WAN** – Empfohlen, wenn Backups über langsame Leitungen erstellt werden oder wenn Replikation genutzt wird. Es entstehen so die kleinstmöglichen Backup-Dateien, was allerdings zulasten der Performance geht. Es werden 256-KB-Chunks genutzt.
- **Local mit mehr als 16 TB** – Wie die »normale« LOCAL-Optimierung, aber mit 4-MB-Chunks. Diese Option empfehlen wir bei sehr großen Backup-Jobs, beispielsweise bei Monster-Fileserver-VMs.

Wie üblich gilt, dass kleinere Chunks bzw. Blöcke mehr CPU und RAM verbrauchen.

Mit der Komprimierung soll die Menge der übertragenen und zu speichernden Daten verringert werden. Wie immer gilt, dass unterschiedliche Methoden unterschiedliche Auswirkungen auf die Leistung und den Verbrauch bei CPU, RAM und Speicherplatz verursachen. Es gibt folgende Optionen zur Einstellung der Kompression:

- **None** – Keine Kompression. Die Daten werden in ihrem Originalzustand belassen und in unveränderten Blöcken vom Produktions-Storage gelesen.
- **Optimal** – Dies ist die empfohlene Einstellung, die in den meisten Fällen den besten Kompromiss zwischen Backup-Größe und Joblaufzeit erreicht.

- **High** – Erreicht eine um 10 % höhere Komprimierung als die Einstellung Optimal, belastet die CPU allerdings auch ca. 10-mal stärker.
- **Extrem** – Belastet die CPU maximal und erreicht dabei meist nur maximal weitere 3 bis 5 % Kompression.
- **Dedupe-friendly** – Ist sehr CPU-freundlich und erzeugt dabei recht vorhersehbare Datenpakete, was der Deduplikation einer angebundenen Appliance zuarbeitet.

Vielleicht fragen Sie sich nun, inwieweit man sich von den empfohlenen Einstellungen entfernen sollte. Generell gilt wie immer die Unix-Regel »Wenn man nicht weiß, was man tut, sollte man es lassen«, was auch für Veeam gilt. Veeam B&R ist standardmäßig auf eine gute Balance eingestellt, und in aller Regel sollte es nicht notwendig sein, signifikante Änderungen an den Standardeinstellungen vorzunehmen.

17.10.5 Backup-Jobs

Veeam B&R hilft Ihnen bei der Erstellung eines Backup-Jobs durch einen entsprechenden Assistenten (siehe Abbildung 17.16). Zunächst werden die virtuellen Maschinen über Add Objects hinzugefügt (siehe Abbildung 17.17). Dabei sind verschiedene Ansichten der Objekte im vCenter möglich. Es dauert in der Regel einen Moment, bis die verfügbaren Objekte aufgelöst wurden und zur Auswahl bereitstehen. Es ist möglich, einzelne Objekte auszuwählen, Elternobjekte auszuwählen und Objekte auszuschließen. Üblicherweise sucht man sich die VMs zusammen, die zu einem Backup-Job zusammengefasst werden sollen. Lassen Sie bei Elternobjekten jedoch Vorsicht walten, da bestimmte verknüpfte Objekte von bestimmten Jobs nicht ausgeschlossen werden können.

Es ist sinnvoll, Gruppen ähnlicher VMs bzw. VMs gleicher Art zusammenzufassen, gerade wenn Sie bei den Einstellungen des Backup-Jobs unterschiedliche Anforderungen an die Backups der VMs abdecken müssen. Das einfachste Merkmal ist hier die Backup-Häufigkeit. Während die meisten VMs einmal täglich gesichert werden können, benötigen andere VMs kleinere Backup-Intervalle. Andere Beispiele, an denen sich sehr gut weitere Effekte festmachen lassen, sind das Betriebssystem der VMs sowie die Deduplizierungsrate.

Deduplizierung

An dieser Stelle sei erneut erwähnt, dass Sie sich nicht zu sehr auf die Deduplizierung verlassen sollten. Selbst wenn Sie alle Vorteile, die die Option per-VM backup files mit sich bringt, ignorieren können, weil sie in einem bestimmten Anwendungsfall weniger greifen, ist und bleibt eine extrem hohe Deduplizierungsrate meist ein Traum.

Das Backup lässt sich auch indirekt verwalten, indem Sie Backup-Jobs auf Containern basieren lassen. So können beispielsweise Ordner oder Pools als Elternobjekt verwendet werden. Wird anschließend eine VM in vSphere aus dem Elternobjekt entfernt, fällt sie automatisch

aus dem Backup. In der Praxis hat sich aber gezeigt, dass Backups, die so strukturiert sind, oftmals die Komplexität erhöhen oder gar nicht ohne Weiteres konfigurierbar sind. Dies liegt zum einem an der Nutzung der Ordner, denn viele Administratoren nutzen Ordner nur bedingt. Und selbst wenn eine geschickte Nutzung eines Ordners möglich wäre, müssen Sie immer die Auswirkung von Veränderungen auf das Backup berücksichtigen. Dies kann schnell dazu führen, dass man die Übersicht verliert. Das gilt besonders dann, wenn man nur eine kleine Menge von Foldern für das Backup auswählt und der Normalfall eben ein anderer ist.

Außerdem können Sie *Tags* für die Strukturierung von Backup-Jobs verwenden. Genauer gesagt, können Sie je Backup-Job exakt ein Tag verwenden. Ähnlich wie bei Ordnern gilt aber auch hier, dass eine gut strukturierte und durchdachte Vorgehensweise wichtig ist, wenn man den Überblick nicht verlieren will. So sollten Sie die Anzahl an VMs, die durch ein Tag einem Job hinzugefügt werden, im Auge behalten.

Die Konfiguration des Zeitfensters (siehe Abbildung 17.23 und Abbildung 17.24) ist recht simpel gehalten. Es bietet unterschiedliche Einstellungsmöglichkeiten, mit denen Sie die Startzeit Ihrer Backups verwalten können. Eine weitere Option ist das Verknüpfen von Backup-Jobs. Dabei wird das Ende des einen Backup-Jobs als Startsignal für den nächsten verwendet. Auch wenn dies eine sehr angenehme und geschickte Lösung ist, sei angemerkt, dass solche Verkettungen fehleranfällig sind, wenn ein Job Probleme bereitet oder gar hängen bleibt.

Weitere Einstellungen lassen sich in Bezug auf Load-Balancing und Proxy-Affinity vornehmen. Generell empfehlen wir, Veeam entscheiden zu lassen, welcher Proxy welche Jobs machen soll. Dies ist nicht nur sehr einfach für den User, da es keine weiteren Überlegungen erfordert, sondern ist in aller Regel auch sehr effizient, da das *Intelligent Load Balancing* (ILB) von Veeam für eine optimale Verteilung sorgt. Sollte dennoch die Notwendigkeit bestehen, manuelle Einstellungen vorzunehmen, gibt es generell zwei Möglichkeiten: Zum einem können Sie mit Storage Latency Control oder Backup I/O Control die Last auf dem Speicher verringern. Zum anderen lassen sich mit Proxy Affinity-Regeln Vorgaben erstellen, wonach bestimmte Proxys nur mit bestimmten Backup-Repositories zusammenarbeiten dürfen. Dies kann sehr hilfreich sein, wenn Sie eine über mehrere Standorte verteilte Infrastruktur verwenden, da man dort offensichtlich unnötige Latenzen zwischen Proxy und Repository vermeiden und Prozesse innerhalb eines Standorts ablaufen lassen möchte.

17.10.6 Backup-Copy-Jobs

Veeam B&R führt mit *Backup-Copy-Jobs* eine zweite Stufe der Sicherung durch. Dabei werden die Dateien des »ersten« Backups, das durch die direkte Sicherung der VM bzw. ihrer Blöcke erfolgt, gelesen und gesichert. Diese Kette bringt einige Vorteile mit sich. Zum einem wird der Produktions-Storage nicht doppelt belastet. Zum anderen kann diese zweite und völlig unabhängige Backup-Kette mehrere Backup-Jobs zusammenfassen und sichern.

Damit eignen sich Backup-Copy-Jobs hervorragend zum Sichern der »Primär«-Backups auf sekundären Backup-Speichern z. B. Tapes. So lässt sich die 3-2-1-Methode leicht erreichen, denn mit dem Sichern auf Tapes wird nicht nur der Medienbruch erreicht. Gleichzeitig lassen sich diese remote lagern. Hierzu werden immer wieder gern Gruppen von Tapes zyklisch verwendet. Beispielsweise werden zwei identische Backup-Copy-Jobs konfiguriert. Im ersten Monat schreibt der erste Job die Backup-Copy auf die Tapes. Zu Beginn des zweiten Monats wird der erste Backup-Copy-Job deaktiviert, und die Tapes werden ausgetauscht. Das eine Set wird im Safe bei der Bank eingelagert, während das zweite Set in die Laufwerke gesteckt wird. Anschließend aktiviert man den zweiten Backup-Copy-Job. Im dritten Monat beginnt dieser Zyklus erneut. Man gewährleistet auf diese Weise die Off-Site-Lagerung eines kompletten Infrastruktur-Backups, das nicht älter als einen Monat ist, wobei man nur zweimal die entsprechende Tape-Kapazität vorhält. Dieses Beispiel ist wohl eines der am häufigsten vorkommenden Modelle für eine komplette Disaster-Recovery.

Da die Backup-Copy-Jobs an einen Backup-Job gekoppelt sind, verhält sich ein Backup-Copy-Job etwas anders:

- Am Anfang wird ein Gesundheitscheck der Backup-Dateien durchgeführt.
- Eine Sync-Phase prüft zunächst, ob neue Backup-Dateien vorhanden sind, und startet gemäß der konfigurierten Zeit die Synchronisation.
- Ein Backup-Copy-Job ist immer *forward incremental* und enthält deswegen eine Transformationsphase.
- Nach Beendigung des Backup-Copy-Jobs tritt dieser in eine Schlafphase, bis ein neuer Restore-Point im Backup-Job auftaucht bzw. der neue Zyklus des Backup-Copy-Jobs startet.

17.10.7 Speicherwartung bei Defragmentierung durch inkrementelle Backups

Backup-Jobs bieten unter dem MAINTENANCE-Register erweiterte Einstellungen, um die Nachteile von inkrementellen Backup-Jobs zu negieren. Die zwei schwerwiegendsten Nachteile sind die *Full Backup File Fragmentation* und die *Silent Storage Corruption*:

- **Full Backup File Fragmentation** – Die Voll-Backup-Datei-Fragmentierung entsteht im Laufe der Zeit, da die inkrementellen Backups zusammengefasst werden. Dadurch verteilen sich einzelne Fragmente möglicherweise ungünstig auf dem Backup-Speicher. Dies konnte zuvor nur durch das Schreiben periodischer Voll-Backups verhindert werden.
- **Silent Storage Corruption** – Die stille Speicherkorruption tritt dann ein, wenn ein inkrementelles Datenstück schadhaft wird, was unter Umständen alle folgenden Wiederherstellungs- und Konsolidierungsprozesse beeinflusst.

Die Option DEFRAGMENT AND COMPACT FULL BACKUP FILE, die Sie im Wartungs-Tab in den erweiterten Einstellungen finden, kann dazu genutzt werden, genau diese beiden Effekte zu verhindern. Allerdings sollten Sie sie nicht zusammen mit Deduplizierungs-Appliances nutzen, da diese von Haus aus immer stark fragmentiert sind.

Zusätzlich wurde der sogenannte *Storage-level Corruption Guard* eingeführt, der die Blöcke nach dem Backup anhand der Metadaten überprüft und bei einer Abweichung direkt repariert. Schlägt diese Reparatur fehl, wird der User darüber informiert, dass ein Voll-Backup erforderlich ist. Dieses Feature wird entsprechend für alle inkrementellen Backups empfohlen. Sollte das Backup-Speichersystem bereits über ein sogenanntes *Scrubbing* verfügen, das essenziell gesehen exakt dieses Feature darstellt, sollte es in Veeam B&R entsprechend deaktiviert werden.

17.10.8 Application-Aware Processing

Veeam ist in der Lage, Backups und Replikation mit einer Application-Awareness durchzuführen, um sogenannte *Transactionally Consistent Backup Images* zu erzeugen. Im Gegensatz zum einfachen Snapshot einer VM werden hierbei weitere systemnahe Funktionen genutzt, um die Konsistenz von Daten sicherzustellen. Dabei gibt es generell zwei Methoden: *Quiescence* mit den VMware Tools und das Veeam-eigene *App-Aware Image Processing*, das auf Microsoft VSS oder Linux-Skripten basiert. Die Eigenschaften der beiden Optionen sehen Sie in Tabelle 17.5.

Funktion	VMware-Tools-Quiescence	App-Aware Image Processing
App-Aware Backups	begrenzt	ja
Vorbereitung von VSS für spezifische Apps (z. B. Oracle)	nein	ja
App-Log-Trunkierung, z. B. für MS SQL oder Exchange	nein	ja
Ausführbare Skripte	ja, im Gast-OS	ja, zentral
Fehlermeldungen	innerhalb der Gast-OS-VM	zentral auf dem Veeam-Backup-Server
Konsistente Windows-Backups	ja	ja
Sync-Treiber für Linux	ja	nein

Tabelle 17.5 Vergleich zwischen der VMware-Tools-Quiescence und dem Veeam-eigenen Application-Aware Image Processing

Wie Sie besonders an den ersten drei aufgeführten Funktionen erkennen können, bringt Veeam einige hochinteressante Fähigkeiten mit. Mit diesen lässt sich beispielsweise eine Microsoft-SQL-Datenbank konsistent sichern oder es lassen sich Exchange-Postfächer so sichern, dass Sie später sogar einzelne Objekte wie beispielsweise eine E-Mail einfach wiederherstellen können.

Dabei geht Veeam wie folgt vor:

1. Veeam überprüft im Gastbetriebssystem, ob eine Applikation installiert ist, die Sie mit App-Awareness erfassen können.
2. Wenn nötig, werden vorab Skripte innerhalb der VM ausgeführt, um die Applikation »einzufrieren«.
3. VSS Quiescence wird durchgeführt, und anschließend wird ein Snapshot der VM erstellt.
4. Nach dem Snapshot wird die VM wieder »aufgetaut«, und eventuell vorhandene Skripte werden ausgeführt.
5. Das Backup wird erstellt und der Snapshot aufgelöst bzw. committet.
6. Log-Dateien werden mit VSS oder mit nativen Oracle-Kommandos sortiert.

Damit dieses erweiterte Quiescence funktionieren kann, sind entsprechende Zugriffsrechte innerhalb der VM nötig. Idealerweise wird hierfür ein Active-Directory-Account verwendet. An dieser Stelle ist wieder zu erwähnen, dass Sie ähnliche VMs bündeln sollten. Befinden sich ausschließlich Windows-VMs einer Domain in einem Backup-Job, können Sie Zugriffsrechte einmal vergeben, und alle VMs sind bedient. Befindet sich beispielweise zusätzlich eine Linux-VM im selben Backup-Job, die nicht ins AD integriert ist, müssen Sie die Linux-VM dediziert anpassen und Veeam spezielle Zugriffsrechte für die Abarbeitung innerhalb der VM gewähren.

Darüber hinaus sind verschiedene Ports notwendig. Für eine Windows-VM sind dies RPC inklusive dynamischer Port-Range (49152 bis 65535 für Windows 2008 und neuer), TCP/UDP auf 135, 137 bis 139 und 455. Für Linux-VMs müssen Sie den SSH-Port 22 freigeben.

17.11 Erstellen von Replikaten

Wie der Name Veeam Backup & Replication schon sagt, können Sie anstelle von Backups auch Replikate erstellen. In Abschnitt 17.5.3 haben wir die Unterschiede bereits detailliert dargestellt, weshalb wir uns zur Erinnerung auf den wichtigsten Unterschied beschränken können: Ein Replikat ist eine Eins-zu-eins-Kopie einer VM und enthält ausschließlich den letzten Status. Es ist nicht dafür gedacht, eine Historie der Daten vorzuhalten, sondern im Fall eines Ausfalls die *primäre* VM möglichst zeitnah zu ersetzen bzw. zu vertreten. Generell geht es dabei also um einen bestimmten Fall aus dem Bereich Disaster-Recovery. Nichtsdestotrotz bietet vSphere Ihnen die Möglichkeit, mehrere Restore-Points vorzuhalten. Deswegen kann es immer wieder mal vorkommen, dass sich nicht eindeutig erschließt, wann man am besten Backups und wann man Replikation einsetzt. Dies hängt auch damit zusammen, dass die Replikation ähnliche Prozesse nutzt wie das Backup und z. B. vom Typ her *forward incremental* ist.

Der wichtigste Unterschied zu Backups ist, dass die Metadaten nicht zusammen mit der Replikation auf dem Ziel gespeichert werden, sondern im Backup-Repository des Replikationsjobs verbleiben. Dies liegt maßgeblich daran, dass der Replikant nicht als eine Backup-Datei auf einem Repository liegt, sondern eine »lebende« VM ist und das Ziel am Ende ein ESXi-Host ist, lokal oder in einem entfernten Datacenter. Bleibt die Replikation lokal, bedient der Backup-Proxy bzw. der Backup-Server beide Teilnehmer: den Source-ESXi-Host und den Target-ESXi-Host.

Wird die Replikation hingegen in eine andere Location geschoben, kommunizieren zwei Backup-Proxys miteinander: einer auf der Source-Site und einer auf der Target-Site. Das dabei verwendete Backup-Repository muss auf der Source-Site zur Verfügung stehen, um die besagten Metadaten sichern zu können. Darüber hinaus ist es ebenso empfehlenswert, einen Veeam-Backup-Server auf der Target-Site einzusetzen, um einen Failover durchführen zu können. Das bedeutet auch, dass alle Operationen im Disaster-Recovery-(DR-)Fall eben durch jenen Veeam-Backup-Server auf der Target-Site bzw. der DR-Site ausgeführt werden. Um solche Failover- und Fail-Backup-Prozesse durchführen zu können, müssen beide Sites de facto autonom lauffähig sein. Das heißt, Dienste wie DNS, DHCP, AD, vCenter etc. müssen in beiden Sites unabhängig voneinander lauffähig sein.

Bei der Übertragung der Daten gibt es weitere Maßnahmen, die z. B. die Menge an zu übertragenden Daten verringern können. Darunter fällt unter anderem auch die WAN-Beschleunigung. Wir empfehlen Ihnen, sich die entsprechenden Kapitel in der Veeam-Dokumentation unter *https://helpcenter.veeam.com/docs/backup/vsphere/wan_acceleration.html?ver=100* durchzulesen.

17.12 Wiederherstellung aus Backups

Folgende Wiederherstellungstypen bezüglich einer VMware-vSphere-Umgebung sind mit Veeam B&R möglich:

- Instant VM recovery – Bootet die VM direkt aus dem Backup-Repository in die Produktionsumgebung. Dies ersetzt (wenn nicht anders eingestellt) die vorhandene VM und hat einen entsprechend hohen Impact auf primäre und Backup-Speicher, die genügend Leistung benötigen, damit diese Möglichkeit auch benutzerfreundlich abläuft.
- Restore entire VM – Wiederherstellung der gesamten VM; ersetzt die Original-VM.
- Restore Virtual disks – Wiederherstellung einzelner VM-Disks.
- Restore VM files – Wiederherstellung von VM-Dateien auf dem Primärspeicher, z. B. die *.vmx*-Datei. Hiermit sind nicht Dateien innerhalb der Gastbetriebssysteme gemeint.
- Restore guest files – Wiederherstellung von Dateien im Gastbetriebssystem, z. B. Dateien eines Fileservers, die in irgendeiner Partition liegen.

- RESTORE APPLICATION ITEMS – Wiederherstellung von Applikationsobjekten z. B. eines Benutzers innerhalb der Microsoft-AD.
- RESTORE TO MICROSOFT AZURE – Wiederherstellung der VM auf Azure.

Die Wiederherstellung von anderen Objekten, beispielsweise von Exchange- oder SQL-Objekten, verläuft ähnlich wie die Dateiwiederherstellung der Gastbetriebssysteme über einen »Explorer«. Diesen Vorgang möchten wir im Folgenden kurz demonstrieren.

In der Veeam-Konsole erreichen Sie über HOME • BACKUPS • DISK die Sicherungspunkte der zuvor erfolgreich durchgeführten Backup-Jobs. Die Buttons im Menüband am oberen Fensterrand oder ein Rechtsklick auf den Backup-Job bieten die unterschiedlichen Wiederherstellungsmethoden an (siehe Abbildung 17.27).

In diesem Beispiel möchten wir eine Datei aus einer VM wiederherstellen; die anderen Wiederherstellungsmethoden gestalten sich aber ebenso einfach und sind vergleichbar durchzuführen. Über einen Rechtsklick wählen Sie RESTORE GUEST FILES • MICROSOFT WINDOWS aus. Im Dialog aus Abbildung 17.28 werden zunächst alle verfügbaren Wiederherstellungspunkte angezeigt, von denen Sie einen auswählen und fortfahren.

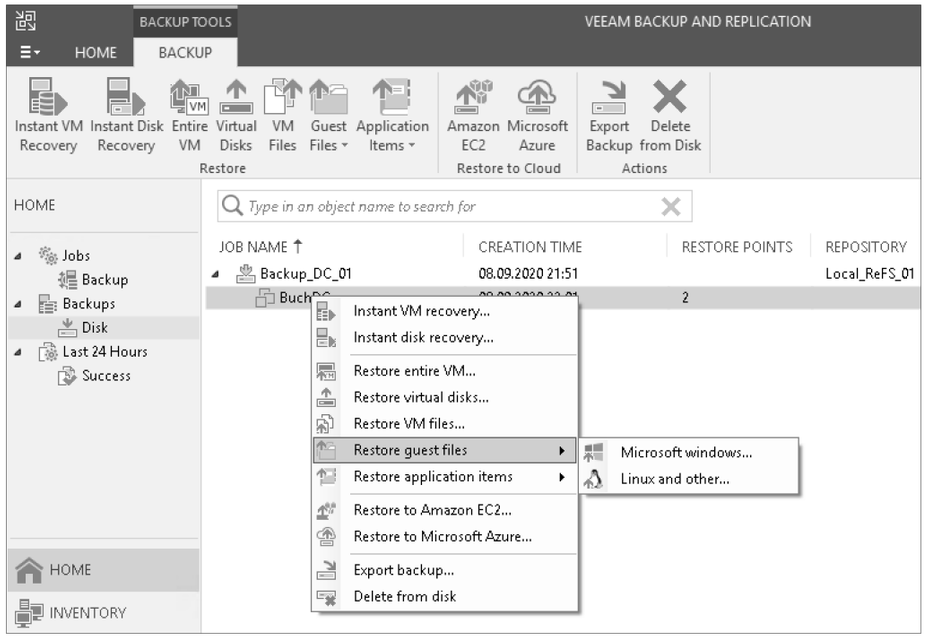


Abbildung 17.27 Wiederherstellung einer Datei aus einer VM (Restore von Gastbetriebssystemdateien)

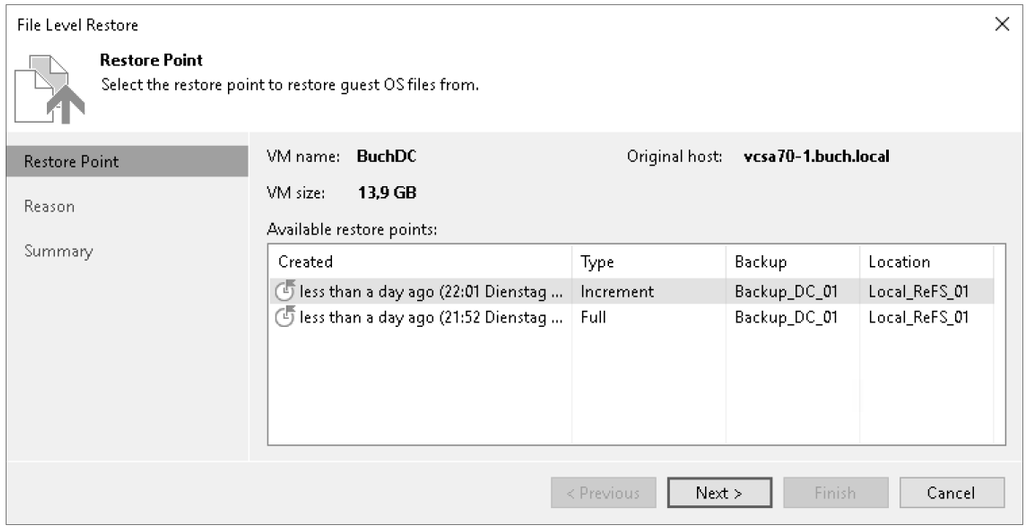


Abbildung 17.28 Einen Restore-Point zur Wiederherstellung auswählen

Sie erhalten nun die Möglichkeit, Kommentare einzufügen, oder können entscheiden, dieses Fenster für die Zukunft auszublenden. Anschließend wird die Übersicht angezeigt, in der Sie mit einem Klick auf FINISH den Vorgang beenden können (siehe Abbildung 17.29).

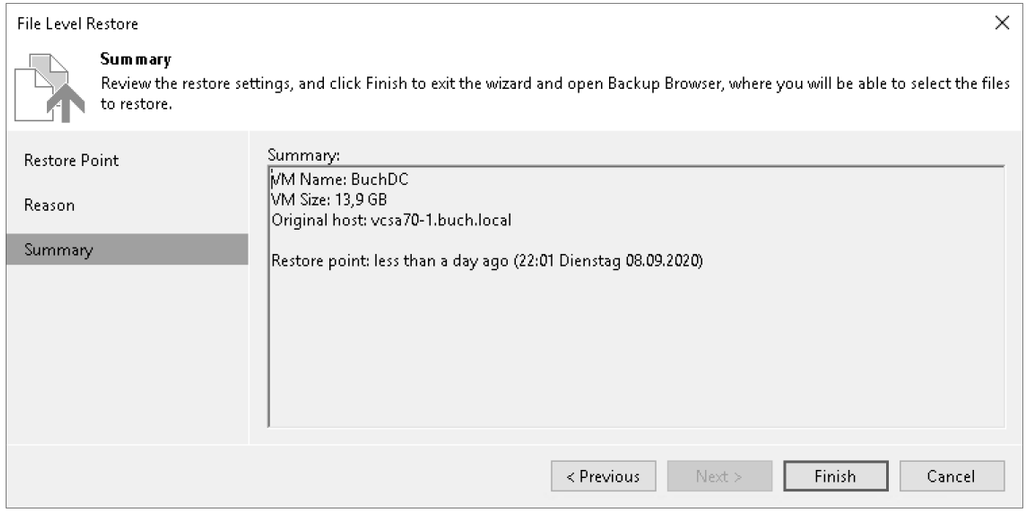


Abbildung 17.29 Der Wiederherstellungsprozess läuft. Wir müssen uns einem Moment gedulden, bis der File-Explorer erscheint.

Vielleicht wundern Sie sich jetzt darüber, dass der Vorgang so kurz ist und schon beendet wurde, denn Sie haben ja bisher keine Datei zur Wiederherstellung ausgewählt. Mit FINISH wird lediglich der Assistent beendet. Anschließend startet je nach Wiederherstellungsmethode der eigentliche Prozess. Für eine Dateiwiederherstellung aus einer VM wird eine Art »Datei-Explorer« gestartet, was je nach Größe und Menge der Backup-Daten und nach der Leistung der Backup-Infrastruktur einen Moment dauern kann. Solange der Prozess in der Veeam-Konsole angezeigt wird, müssen Sie einfach nur etwas Geduld mitbringen.

Sobald der File-Explorer auftaucht, können Sie das Filesystem der gesicherten VM durchsuchen und die gewünschten Dateien zur Wiederherstellung auswählen. Andere Explorer (z. B. für die Wiederherstellung eines Exchange-Objekts) funktionieren analog.

Sie können die Datei nun direkt wiederherstellen. Dabei kann gewählt werden, ob die Originaldatei auf der Quell-VM direkt überschrieben oder behalten werden soll, falls es sie noch gibt. Aus zwei Gründen raten wir von beiden Wegen ab:

- Zum einem gibt es ein organisatorisches Problem: Was passiert, wenn der User die aktuelle Datei noch nutzen will und die Wiederherstellung nur zum Vergleich benötigt? Ein Überschreiben wäre dann fatal.
- Zum anderen wird die wiederherzustellende Datei über den gesamten Hypervisor-Stack geschoben, was eine hohe Auslastung von vSphere zur Folge hat. Da dies für jede Datei geschieht, führen besonders viele kleine Dateien schnell zu Problemen und sorgen dafür, dass die Wiederherstellungsdauer rapide ansteigt.

Deswegen empfiehlt sich die Wiederherstellung auf ein dediziertes Netzlaufwerk oder einen Server, denn so umgehen Sie beide Probleme. Das kann am einfachsten erreicht werden, wenn Sie im Kontextmenü auf den Punkt COPY TO... klicken (siehe Abbildung 17.30).

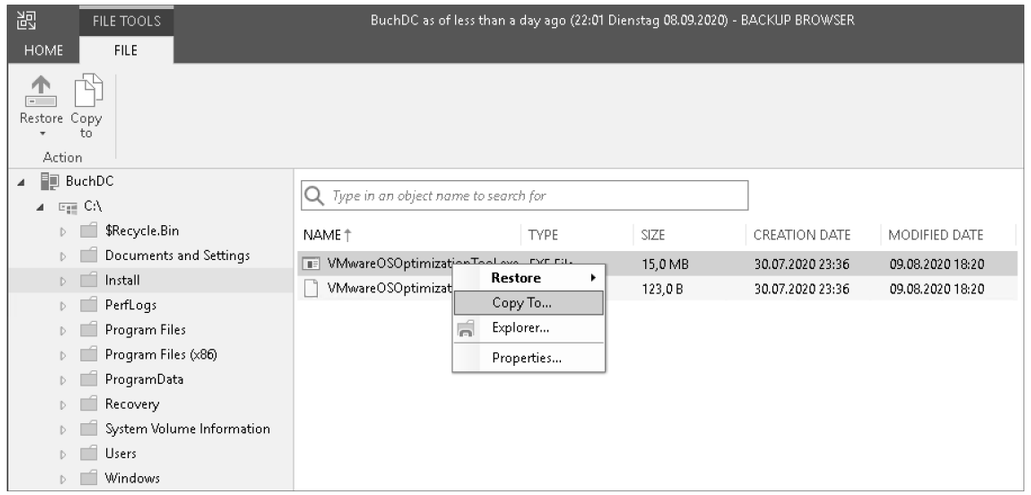


Abbildung 17.30 Die Wiederherstellung einer Datei auf ein Netzlaufwerk bietet viele Vorteile.

Sobald Sie die Datei zurückkopiert haben, ist es zwingend erforderlich, den File-Explorer wieder zu schließen, da er sonst die Backup-Datei blockiert. Bleibt er geöffnet, wird das nächste Backup zwangsläufig fehlschlagen. Durch Schließen des File-Explorer-Fensters wird das Ende des Wiederherstellungsprozesses eingeleitet. Wenige Momente später ist unter RUNNING kein aktiver Prozess mehr zu sehen.

17.12.1 Virtual Lab

Veeam verfügt über ein sogenanntes Virtual Lab, in dem Sie eine VM testweise zur Überprüfung wiederherstellen können. Hierfür erzeugt Veeam eine abgeschlossene und vom Produktionsnetzwerk getrennte Umgebung, in die die VM hochgefahren wird. Über die Veeam-Konsole können Sie sich dann testweise in der wiederhergestellten VM bewegen.

Um diese Funktion nutzen zu können, müssen Sie zuvor das Virtual Lab über BACKUP INFRASTRUCTURE • SUREBACKUP • VIRTUAL LABS einrichten. Alles Weitere verhält sich wie die Wiederherstellung einer VM, nur erfolgt diese eben in das Virtual Lab hinein.