VEEAM

10 Best Practices für Backups mit VMware vSphere

Datum: 24. Februar 2021

Veeam v11

VMware Version 7.0 U1

Hannes Kasparick

Principal Analyst, Veeam Product Management Team

Inhalt

Zusammenfassung

Die Virtualisierung von Servern ist weltweit gängige Praxis. In diesem Bereich ist VMware schon seit Jahren führend, und viele Veeam®-Kunden nutzen VMware vSphere als ihre bevorzugte Virtualisierungsplattform. Das vorliegende White Paper beschreibt Best Practices speziell für die Sicherung und Verfügbarkeit von VMware vSphere mithilfe von Veeam Backup & Replication™ 11. Es enthält auch einige Tipps und Berichte von erfahrenen Community-Mitgliedern, die ihre Sichtweise auf VMware-Backups darlegen. Ausgehend davon können Sie dann zuverlässig entscheiden, welche Backup-Strategie für Ihre Zwecke am besten geeignet ist. In diesem Whitepaper nicht enthalten sind allgemeine Best Practices für einzelne Hyper-V-, Nutanix AHV- und Veeam Agent-Funktionen.

Einführung

Backups virtueller Maschinen (VMs) auf vSphere sind nur eine von mehreren Voraussetzungen für die Verfügbarkeit von Diensten. Ohne Backup ist keine Wiederherstellung möglich, deshalb müssen Backups stets verfügbar sein — und das möglichst schnell. Als allgemeine — und wichtigste — Richtschnur für Backups kann die 3-2-1-Regel dienen.

Dies bedeutet, dass mindestens drei Kopien Ihrer Daten vorliegen sollten (d. h. die Produktionsdaten an sich sowie zwei Backup-Kopien). Die Backup-Kopien sollten auf mindestens zwei verschiedenen, voneinander unabhängigen Medien gespeichert werden, wobei die Betonung hier auf „unabhängig" liegt. Gemeint ist damit, dass keine Abhängigkeit dieser Medien aus technologischer Sicht bestehen darf. Zu guter Letzt sollte eine weitere Kopie extern und offline aufbewahrt werden, d. h. an einem Ort, an dem sie vor Naturkatastrophen, Schadsoftware und unbefugten Zugriffen geschützt ist. Beispielsweise unterstützt Veeam auch S3-Object-Lock in Veeam Backup & Replication 10 und gehärtete/unveränderliche Linux-Repositories in Version 11. Eine weitere Option für die externe Speicherung sind natürlich nach wie vor Backups auf Band.

Veeam Backup & Replication geht noch einen Schritt weiter und erweitert die 3-2-1-Regel zur 3-2-1-0-Regel, die einem neueren Ansatz folgt. Die neue Regel bietet zusätzlichen Ransomware-Schutz, indem eine Kopie sowohl extern als auch offline aufbewahrt wird. Die 0 bedeutet hier, dass bei der Wiederherstellbarkeit keine Fehler auftreten dürfen, was durch automatisierte Wiederherstellungstests mit Veeam SureBackup®- und SureReplica-Jobs möglich wird. SureBackup hat die Hauptaufgabe, logische Fehler in Backups zu erkennen, damit es bei Standard-Wiederherstellungsvorgängen nicht zu Problemen kommt. Ein solcher Fehler könnte etwa vorliegen, wenn jemand zwar Updates installiert, aber nie einen Neustart durchgeführt hat. Nach dem Neustart käme es dann zu einem fatalen Systemfehler.

In diesem Whitepaper stellen wir verschiedene Best Practices für Veeam Backup & Replication und VMware vSphere vor, die Datenverlusten und Ransomware einen Riegel vorschieben sollen. Diese Best Practices beziehen sich allerdings nur auf Veeam und VMware, andere Hypervisoren sind hier nicht Gegenstand der Betrachtung.

Zu den allgemeinen Best Practices gehören:

- Festlegen einer den geschäftlichen Anforderungen entsprechenden Backup- und Wiederherstellungsstrategie
- Korrekte Dimensionierung
- Überprüfen der VSS-Funktionsfähigkeit auf Windows-Geräten
- Bereitstellen von ausreichend Backup-Speicherplatz

Diese Best Practices gelten in jedem Fall, ob nun für VMware, Hyper-V, Nutanix AHV, Cloudprovider oder Backups physischer Server.

Zuallererst — also bevor Sie sich daranmachen, eine Lösung zu planen und zu implementieren — sollten Sie die genauen Anforderungen ermitteln. Im Idealfall erstellt ein Unternehmen eine Anforderungsliste und teilt der IT-Abteilung den benötigten Wiederherstellungspunkt (RPO) und die benötigte Wiederherstellungszeit (RTO) mit. Ist zum Beispiel nur ein Backup erforderlich oder wird auch Disaster Recovery (DR) benötigt? Ist aufgrund einer niedrigen RTO eine zusätzliche Konfiguration von Veeam-Replikationen, Veeam Continuous Data Protection (CDP) oder Storage-Snapshots erforderlich.

Anhand dieser Informationen kann dann die Hardware entsprechend dimensioniert werden, sprich: Die Anzahl der CPU-Kerne, der Speicherplatz und die Bandbreitenanforderungen für WAN, LAN und SAN können festgelegt werden. Und schließlich benötigen Sie einen Quellen- und Backup-Speicher, der die Geschwindigkeitsanforderungen erfüllen kann.

Der nächste Schritt ist dann das eigentliche Backup. Veeams anwendungsspezifische Image-Verarbeitung stellt mithilfe von Microsoft VSS sicher, dass Windows-VMs anwendungskonsistent gesichert werden. Das sogenannte „Quiescing", bei dem die VMware-Tools in den Ruhezustand versetzt werden, entfällt hier. Damit eine zuverlässige anwendungsspezifische Image-Verarbeitung gewährleistet ist, müssen die VSS-Writer der VMs ordnungsgemäß funktionieren.

1. Aktuelle Veeam- und vSphere-Version nutzen

Die neueste Version von Veeam Backup & Replication verbessert im Zusammenspiel mit VMware vSphere die Leistung und Sicherheit.

Veeam Backup & Replication 11 nutzt durchweg asynchrone Lese- und ungepufferte Schreibvorgänge, um Backups im Speichersystem zu schreiben. Asynchrone Lesevorgänge verbessern alle möglichen Lesevorgänge. In Version 10 kamen asynchrone Lesevorgänge bereits bei der Wiederherstellung auf Windows-Dateiebene, Instant VM Recovery™ und beim Erstellen virtueller synthetischer Full-Backups für Backup-auf-Band-Jobs zum Einsatz. In Version 11 sind nun auch alle anderen Lesevorgänge, darunter Backup-Copy-Jobs und Backup-auf-Band-Jobs, asynchron.

Ungepufferte Schreibvorgänge tragen zur Optimierung der Backup-Schreibleistung bei. In Version 10 betrug die Geschwindigkeit beim Schreiben eines Backups auf einen einzelnen Server mit 56 NL-SAS-Laufwerken rund 4 GB. Diese Geschwindigkeit haben wir in Version 11 mehr als verdoppelt, sodass 100-GB-Verbindungen nun maximal ausgenutzt werden können.

Mehr Sicherheit ist für VMware und Veeam ein Dauerthema. Mit der jeweils neuesten Version unserer Produkte stellen Sie sicher, dass Sicherheitsverbesserungen implementiert werden.

> *„Ihre technische Abteilung hat bei der Code-Optimierung in Version 11 ganze Arbeit geleistet. Mit 10 GiB/s auf einem einzelnen Server ist Veeam auf Apollo 4510 eine bahnbrechende Lösung. Schon Version 10 war eine der schnellsten Datensicherungslösungen, aber Version 11 setzt in puncto Leistung auf Enterprise-Niveau völlig neue Maßstäbe. Noch nie habe ich erlebt, dass ein Anbieter seine Leistung von einer Version zur nächsten glatt verdoppelt."*
>
> – Federico Venier, HPE Engineer

Best Practice: Halten Sie Veeam Backup & Replication und vSphere immer auf dem neuesten Stand, um von allen aktuellen Verbesserungen zu profitieren.

2. Den richtigen Backup-Modus wählen

Veeam Backup & Replication bietet drei verschiedene Übertragungsmodi zum Sichern von vSphere-VMs. Ab Version 11 unterstützt Veeam auch alle Backup-Modi für Linux-Proxys. Sollten Sie also Linux bevorzugen, ist dies die erste Entscheidung. Jeder Backup-Modus hat seine Vor- und Nachteile — ein Patentrezept gibt es daher nicht. Welcher der drei folgenden Modi für Ihre Zwecke am besten geeignet ist, hängt von Ihrer Umgebung und Ihren Anforderungen ab:

1. Netzwerkmodus (NBD)
2. Direkter Speicherzugriff, einschließlich Backups aus Storage-Snapshots
3. Virtual Appliance (Hot-Add)

In den Eigenschaften der einzelnen Proxys können die oben genannten Optionen im Abschnitt „Transport Mode“ (Übertragungsmodus) konfiguriert werden.

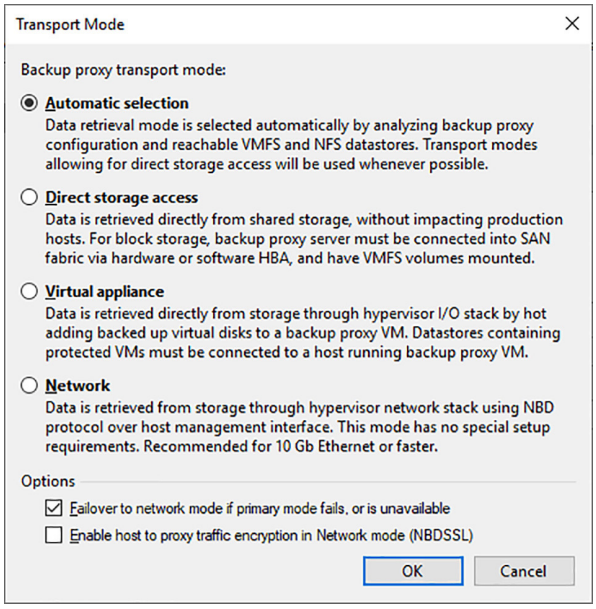


Abbildung 1: Optionen für Übertragungsmodi

Der Netzwerk- oder NBD-Modus ist die einfachste Methode, VMware-Backups vorzunehmen. Der Veeam-Proxy-Server übermittelt Backup-Daten über den ESXi-Managementport der einzelnen ESXi-Hosts. Daher ist die Einrichtung sehr einfach — zusätzlicher Speicherplatz oder eine VM-Konfiguration ist nicht erforderlich. Außerdem wächst das System mit der Anzahl der ESXi-Hosts einfach mit. Ein weiterer Vorteil: Der Administrationsaufwand ist äußerst gering. Im Gegensatz zum Hot-Add-Modus müssen keine weiteren Hot-Add-Mounts vorgenommen werden, was Zeit spart. Es werden auch keine zusätzlichen Storage-Snapshots erzeugt, z. B. Backups aus Storage-Snapshots mit integrierten Speichersystemen. Da die Koordination von VM- und Storage- Snapshots ihre Zeit dauert, ist der Netzwerkmodus für inkrementelle Backups in Umgebungen mit vielen VMs und einer niedrigen Datenaustauschrate sogar mitunter die schnellste Lösung.

Allerdings kann sich der ESXi-Managementport als Engpass erweisen, insbesondere wenn lediglich eine 1-Gbit-Schnittstelle vorhanden ist. Bei Netzwerkkarten mit 10 Gbit und mehr dürfte dies aber kein Problem darstellen.

Wird als Modus der direkte Speicherzugriff gewählt, erfolgt die Übertragung der Backup-Daten direkt vom Speichersystem auf den Veeam-Backup-Proxy. Er muss dann nicht den Umweg über den ESXi-Hypervisor nehmen. Das Protokoll hängt von der Speicherumgebung ab: in der Regel FibreChannel oder iSCSI. Der direkte Speicherzugriff hat gegenüber Hot-Add denselben Vorteil wie der Netzwerkmodus, nämlich das Entfallen zeitraubender Hot-Add-Vorgänge. Beide Modi nutzen VMware vStorage API for Data Protection (VADP).

VADP ist die offizielle API von VMware für die Sicherung virtueller Maschinen. Sie weist einige Besonderheiten hinsichtlich der Backup-Performance auf, weshalb VADP in drei Veeam Backup & Replication-Konfigurationen nicht zum Einsatz kommt. Diese drei Konfigurationen sind:

- Backups aus Storage-Snapshots
- Direct NFS (mit dem direkten Speicherzugriff vergleichbar)
- Virtual Appliance (Hot-Add)

Dieser besondere Veeam-Ansatz bezüglich VADP ermöglicht eine deutliche Steigerung der Backup-Performance. Dies ist einer der Gründe für die Beliebtheit von Hot-Add. Der Hot-Add-Modus bietet aber noch weitere Vorteile. In diesem Modus wird der Veeam-Backup-Proxy als zusätzliche VM für Backups ausgeführt. Snapshots der VMs werden in der Backup-Umgebung gemountet, der Traffic läuft über das normale VM-Netzwerk. Die ESXi-Managementschnittstelle kommt dabei nicht zum Einsatz. In der Folge stellt Hot-Add eine schnelle Alternative für 1-Gbit-Netzwerke dar, bei denen der direkte Speicherzugriff nicht infrage kommt.

> *„Die Übertragungsmodi von Veeam sind dank ihrer Flexibilität und ihrem breiten Spektrum ideal für alle Arten von VMware vSphere-Umgebungen. Der Netzwerkmodus für KMU, Hot-Add für HCI und allgemeine Zwecke, der direkte Speicherzugriff und die Speicherintegration weisen beeindruckende Änderungsraten auf, haben aber nur minimale Auswirkungen auf die Produktivumgebung."*
>
> – Markus Kraus, Veeam Vanguard und VMware vExpert

Für NFS-Datastores ist der Hot-Add-Backup-Modus jedoch im Allgemeinen nicht zu empfehlen. Stattdessen sollte hier der direkte Speicherzugriff angewandt werden, was auf den Direct NFS-Modus hinausläuft. Für Direct NFS gibt es keine separate Benutzeroberflächenoption, da Direct NFS lediglich eine Variante des direkten Speicherzugriffs ist. Diese Empfehlung hat einen guten Grund: Hot-Add resultiert oft in VM-Stuns, wenn der Veeam-Proxy nicht auf demselben ESXi-Host wie die VM ausgeführt wird. Weitere Details finden Sie im Veeam-Artikel KB1681 im Abschnitt zu Umgebungen mit NFS-Datastores. Falls Sie den Hot-Add-Modus dennoch für NFS-Datastores nutzen möchten, sollten Sie folgende Regeln und Einstellungen beherzigen:

- Genau ein Hot-Add-Proxy pro ESXi-Host
- In „HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication" den Wert „EnableSameHostHotAddMode = 1" festlegen

Hinweis: Direct NFS-Backups können nur VMs ohne vorhandene Snapshots sichern. VMware empfiehlt, Snapshots so früh wie möglich zu entfernen. Sollte ein VM-Snapshot vorhanden sein, nimmt Veeam ein Failover in alternative Backup-Modi vor.

Für Backups stehen zahlreiche Optionen zur Verfügung — einen Überblick bietet die unten stehende Tabelle. Darin können Sie die Ergebnisse der einzelnen Modi ablesen und so entscheiden, welcher Modus für Sie am ehesten infrage kommt.

Mode	Operation	Time	Speed
Direct Storage Access	Full backup		
Direct Storage Access	Incremental backup		
Backup from Storage Snapshots	Full backup		
Backup from Storage Snapshots	Incremental backup		
Virtual Appliance	Full backup		
Virtual Appliance	Incremental backup		
Network	Full backup		
Network	Incremental backup		

Best Practice: Probieren Sie aus, welcher Backup-Modus am besten zu Ihrer Umgebung passt.

3. Wiederherstellungsart planen

Nachdem Sie den für Sie optimalen Backup-Modus bestimmt haben, ist nun der Wiederherstellungsmodus an der Reihe. Unabhängig davon, wie die Wiederherstellungstests im Detail ausgefallen sind, müssen die RTO-Anforderungen erfüllt sein, d. h., Sie benötigen möglicherweise leistungsstärkere Hardware. Veeam bietet zahlreiche Szenarien zur Wiederherstellung von VMs aus lokalen oder Cloudservices, physischen Maschinen, Dateien und Anwendungsobjekten. Seit Version 10 besteht zudem die Möglichkeit, imagebasierte Backups sofort in VMware wiederherzustellen.

Eine wichtige Bemerkung vorab: Wiederherstellungen unterscheiden sich je nachdem, ob Dateien und Objekte oder VMs und Laufwerke wiederhergestellt werden sollen. Dateien oder Objekte (z. B. Microsoft Exchange-E-Mails oder Microsoft Active Directory-Objekte) werden bei Veeam über das Netzwerk wiederhergestellt. Konkret bedeutet dies, dass für die Übertragung der Daten in die VM eine RPC-Verbindung (Windows) oder eine SSH-Verbindung (Linux) sowie Data-Mover-Ports erforderlich sind. Der Grund dafür: Veeam ist für VM-Backups standardmäßig agentenlos. Falls Sie die Port-Anforderungen für Windows-Backups und -Wiederherstellungen senken möchten, können Sie den neuen persistenten Veeam-Gastagenten in Version 11 nutzen.

Die Wiederherstellung ganzer VMs oder virtueller Laufwerke ist blockbasiert, da Backups über VM-Snapshots auf Blockebene erfolgen. Je nach dem gewählten Wiederherstellungsmodus macht es einen Unterschied, ob eine Thick- oder eine Thin-Provisioning-VM verwendet wird. Die Wiederherstellungsmodi entsprechen dabei den Backup-Modi (direkter Speicherzugriff, Virtual Appliance oder Netzwerk). Darüber hinaus gibt es Instant VM Recovery in Kombination mit Storage VMotion oder Quick Migration (schnelle Migration).

Der Hot-Add- und der Netzwerkmodus sind sowohl für Thick- als auch für Thin-Provisioning-VMs geeignet. Wie schon erwähnt, geht die Backup-Datenübertragung per Virtual Appliance oder Hot-Add sehr schnell vonstatten. Dasselbe gilt für die Wiederherstellung ganzer VMs oder Laufwerke per Hot-Add. In vielen Szenarien ist es ratsam, für VM- oder Laufwerkswiederherstellungen wenigstens einen Hot-Add-Proxy bereitzustellen.

Der Netzwerkmodus ist in der Regel die langsamste Wiederherstellungsmethode.

Der direkte Speicherzugriff ist zwar sehr leistungsstark, aber die Wiederherstellungsmöglichkeiten sind hier auf Thick-Provisioning-Laufwerke beschränkt. Thin-Provisioning-Laufwerke müssten erst im laufenden Betrieb zu Thick-Provisioning-Laufwerken konvertiert werden. Der direkte Speicherzugriff ist in der Regel nicht die schnellste Wiederherstellungsoption, da er auf VADP basiert. Eine Ausnahme gilt für Wiederherstellungen mit Direct NFS — hier nutzt Veeam Backup & Replication nicht VADP.

Um eine VM oder ein Laufwerk wiederherzustellen, müssen nicht alle Daten vollständig übertragen werden. Auch eine Wiederherstellung auf Changed-Block-Tracking-Basis (CBT) ist möglich, sofern die CBT-Informationen des Produktiv-Speichers korrekt sind. Diese Option kann die Wiederherstellungszeit verkürzen. Dazu muss während der Wiederherstellung manuell die Option „Quick Rollback" ausgewählt werden.

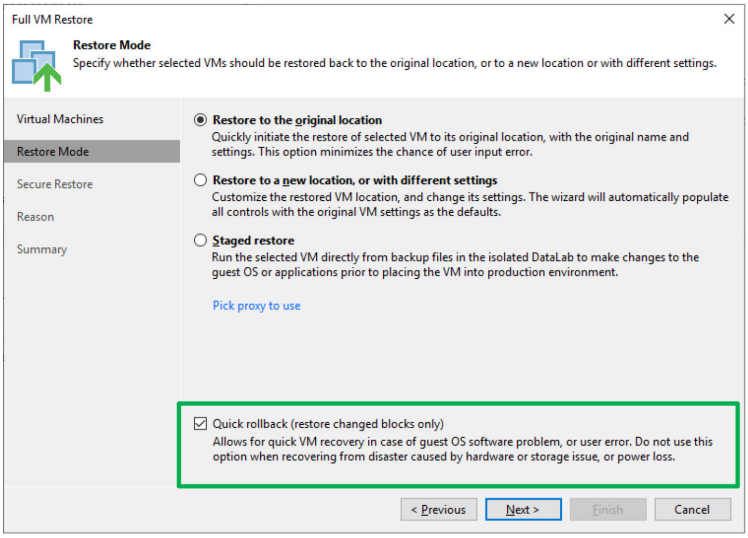


Abbildung 2: Quick Rollback basierend auf Changed-Block-Tracking-Informationen

Eine Alternative zur Wiederherstellung ganzer VMs ist Instant VM Recovery (dies gilt ebenso für die Sofortwiederherstellung von VM-Laufwerken anstelle von ganzen Laufwerken). Mit Instant VM Recovery lässt sich eine VM direkt aus dem Backup-Repository booten. Letzteres verhält sich wie ein auf einem ESXi-Host gemounteter NFS-Datastore. Die Instant VM Recovery-Leistung wurde in Version 10 deutlich gesteigert. Für die Rückübertragung der VM-Daten aus dem Repository-NFS-Datastore in den Produktiv-Datenspeicher gibt es zwei Optionen:

- Veeam Quick Migration
- VMware Storage VMotion

Für die Wiederherstellung einer vollständigen VM stehen zahlreiche Optionen zur Verfügung — einen Überblick bietet die unten stehende Tabelle. Darin können Sie die Ergebnisse der einzelnen Modi ablesen und so entscheiden, welcher Modus für Sie am ehesten infrage kommt.

Mode	Operation	Time	Speed
Direct Storage Access	Full VM restore		
Direct Storage Access	Full VM restore CBT		
Virtual Appliance	Full VM restore		
Virtual Appliance	Full VM restore CBT		
Network	Full VM restore		
Network	Full VM restore CBT		
Instant VM recovery + Storage Vmotion	Full VM restore		
Instant VM recovery + Quick Migration	Full VM restore		

Best Practice: Planen und testen Sie die Wiederherstellungsoptionen basierend auf Ihrem Speicher- und Übertragungsmodus. Wenn Sie keine NFS-Datastores nutzen, sollten Sie ersatzweise mindestens einen Hot-Add-Proxy bereitstellen.

4. Veeam Continuous Data Protection ins Disaster-Recovery-Konzept integrieren

Mit Veeam Backup & Replication können Sie im Sekundentakt VMware-VMs ohne VMware-Snapshots replizieren. Diese Funktion heißt kontinuierliche Datensicherung (Continuous Data Protection, CDP) und ermöglicht kürzere RPOs und RTOs bei der Disaster Recovery. CDP basiert auf den vSphere-APIs für die I/O-Filterung (VAIO) und ähnelt in der Anwendung der klassischen Veeam-Replikation.

Bei der CDP-Planung sollten Sie einige Dinge beachten. Wie in jedem Fall müssen Sie Hardwarekapazitäten für die Datenübertragung und die Speicherung der geänderten Daten bereithalten. Klassische Backups geschehen im 8-, 12- oder 24-Stunden-Rhythmus, wobei die Netzwerkbandbreite nur einige Male am Tag ausgenutzt wird. Beim CDP fließt hingegen ein kontinuierlicher Datenstrom. Die Bandbreite lässt sich durch Überwachung des Umfangs der Schreibvorgänge im Speicher abschätzen. Veeam wendet Komprimierung an und filtert nicht benötigte Blöcke heraus (d. h. nur die neueste Version eines Blocks, der innerhalb der RPO mehrfach geändert wurde, wird übertragen). In der Folge liegt die erforderliche Bandbreite etwas unter dem Wert, der im Speicher angezeigt wird.

Sie benötigen ausreichend Speicherplatz am Speicherort des VMware-Datastores sowie genügend I/O-Kapazität für die Wiederherstellungspunkte. Je kürzer die RPO-Zeit und je länger der Aufbewahrungszeitraum sind, desto mehr Speicherplatz braucht es. Wir empfehlen zehn Sekunden und eine längere RPO. Eine RPO von zwei Sekunden ist zwar möglich, aber der Speicherplatzbedarf und die nötige I/O-Kapazität im Ziel-Datastore sind hoch und Schreibvorgänge im Ziel-Datastore werden nicht gedrosselt. Sind im Ziel-Speichersystem auch Produktiv-VMs vorhanden, ist es ratsam, für die VM-Replikate einen eigenen Datastore zu verwenden.

Je nach I/O-Last und RPO-Zeit kann der Netzwerk-Traffic bei CDP sehr hoch ausfallen. MTU 9000 steigert die Leistung in 10-Gbit/s-Netzwerken um etwa 25 %. Zu empfehlen ist auch ein spezieller VMkernel-Adapter mit einem eigenen physischen Uplink (oder mehreren Uplinks). Dies verhindert Interferenzen des CDP-Traffics mit sonstigem Datenverkehr (d. h. Management-Traffic). Auf den VMkernel-Adaptern müssen keine Dienste aktiviert werden (siehe Abbildung 3). Vorhandene (verteilte) virtuelle Switches können eingesetzt werden, die Konfiguration eines speziellen vSwitch für CDP-Traffic ist dagegen nicht erforderlich.

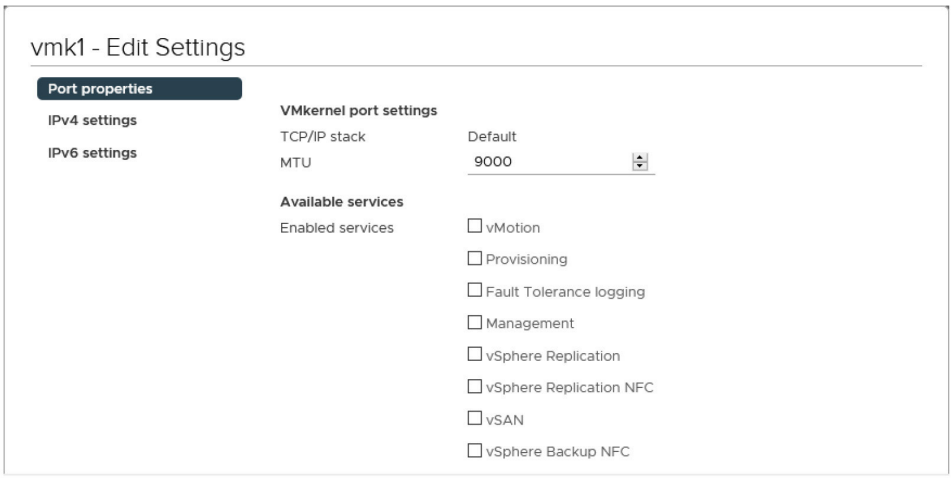


Abbildung 3: Keine aktivierten Dienste für den VMkernel-Port

Beim Proxy-Design sind ähnliche Überlegungen anzustellen wie bei Backups:

- Wenige große (physische) Proxys
- Viele kleine (virtuelle) Proxys

Aus Redundanzgründen sollte es mindestens zwei Quell- und Ziel-Proxys geben. Kommen virtuelle Proxys zum Einsatz, ist ein Proxy pro ESXi die beste Methode, den Netzwerk-Traffic zu optimieren. Darüber hinaus ist es ratsam, dedizierte Proxys für Quelle und Ziel zu verwenden. Für den Proxy-Cache empfehlen wir schnelle SSDs für gemischte Workloads.

Best Practice: Nutzen Sie für die Disaster Recovery Veeam Continuous Data Protection (CDP), sofern keine speicherbasierte Replikation eingerichtet ist.

5. VMware-Tools installieren

Für viele Vorgänge setzt Veeam Backup & Replication voraus, dass auf den VMs VMware-Tools installiert sind. Ohne diese kann Veeam Backup & Replication beispielsweise weder IP-Adressen noch die Version des Betriebssystems ermitteln. Eine erfolgreiche anwendungsspezifische Image-Verarbeitung ist so nicht möglich.

Der Grund dafür: Wenn Veeam Backup & Replication die IP-Adresse nicht ermitteln kann, lässt sich auch keine Netzwerkverbindung zur VM herstellen. Auch die Ersatzmechanismen VIX und vSphere API für die Interaktion mit dem Gastsystem funktionieren ohne VMware-Tools nicht. (Weitere Informationen zu VIX enthält Punkt 10 dieses Dokuments.) Abbildung 4 veranschaulicht dies anhand einer fehlgeschlagenen Prüfung von Gastanmeldedaten infolge fehlender VMware-Tools:

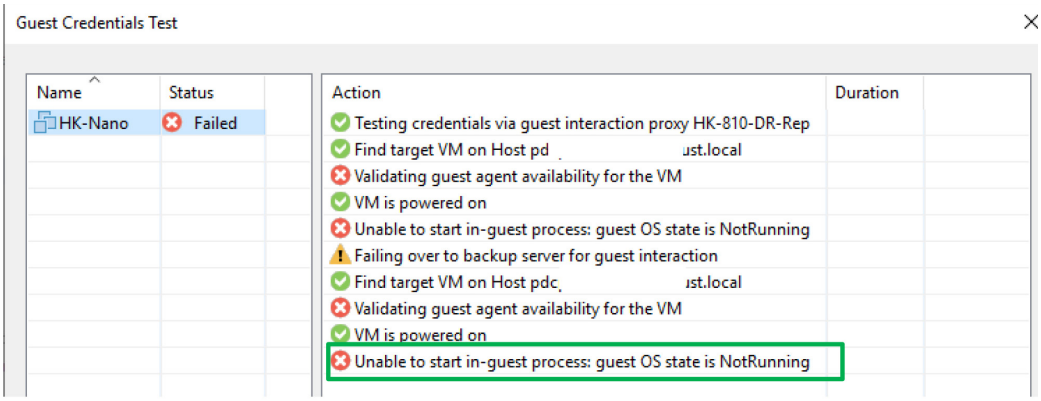


Abbildung 4: Fehlgeschlagene anwendungsspezifische Verarbeitungsprüfung

Ein weiteres Beispiel sind SureBackup-Tests. Auch Heartbeat- und Ping-Tests führen nicht zum Erfolg, wenn keine VMware-Tools vorhanden sind. Für VMware-Tools gilt daher die goldene Regel: Halten Sie die Tools immer auf dem neuesten Stand.

Best Practice: Installieren Sie VMware-Tools und halten Sie sie stets auf dem neuesten Stand.

6. Speicherbasierte Snapshots ins Sicherungskonzept integrieren

Gleich vorweg: Storage-Snapshots sind kein gleichwertiger Ersatz für Backups. Sie können aber in vielen Situationen dazu beitragen, den Datenverlust möglichst gering zu halten. Veeam Backup & Replication lässt sich zusammen mit VMware vSphere in zahlreiche Speicherlösungen integrieren. Dadurch stehen zusätzliche Datensicherungsoptionen zur Verfügung. Eine Aufzählung der Speichersysteme mit Integration finden Sie hier.

Dazu gehört die Möglichkeit, mit Veeam Backup & Replication Storage-Snapshots zu öffnen und Dateien und Objekte direkt aus dem Storage-Snapshot wiederherzustellen. So können Sie beispielsweise Storage-Snapshots in 15-Minuten-Intervallen einrichten, ohne dafür VM-Snapshots erstellen zu müssen. Diese viertelstündlichen Snapshots sind dann zwar keine echten Backups, da sie nicht der 3-2-1-Regel genügen, sie helfen aber durchaus dabei, die RPO-Zeiten zu verkürzen.

Hinweis: Sie haben die Wahl zwischen ausfallsicheren und anwendungskonsistenten Snapshots. Nur bei anwendungskonsistenten Snapshots wird vor dem Storage-Snapshot ein VMware-Snapshot erstellt.

Abbildung 5 zeigt Veeam Explorer™ for Storage Snapshots mit seinem ganz ähnlichen Konzept. Auf der linken Seite sind die Storage-Snapshots zu sehen, d. h. die LUNs und die Snapshots einer LUN. Rechts sind die VMs der einzelnen Storage-Snapshots abgebildet. Auf dieser Grundlage können VMs mit Instant VM Recovery oder Dateien und Anwendungsobjekte wiederhergestellt werden.

Stellen Sie sich vor, dass alle 15 Minuten ein Storage-Snapshot kritischer LUNs oder Volumes angefertigt und nach vier Stunden wieder gelöscht wird. So gehen im Ernstfall nur die Daten der letzten maximal 15 Minuten verloren — und nicht sämtliche Datenänderungen seit dem letzten nächtlichen Backup.

„Ich nutze die Speicherintegration von Veeam, die Orchestrierung von Storage-Snapshots und Backup-Jobs, in denen ich wiederum Backups aus Storage-Snapshots verwende. Dadurch, dass ich in Veeam beide Funktionen aktiviert habe, kann ich über eine einzige Konsole meine Storage-Snapshots verwalten und die Storage-Snapshot-Aufbewahrung auf meine Backup-Zeitplanung abstimmen. Diese Lösung hat sich bewährt, als ich neulich besonders kritische Daten wiederherstellen musste, die gelöscht worden waren. So konnte ich unsere Daten nahezu vollständig wiederherstellen, mit nur minimalem Datenverlust.“

– Shane Williford, Systems Architect, North Kansas City School District

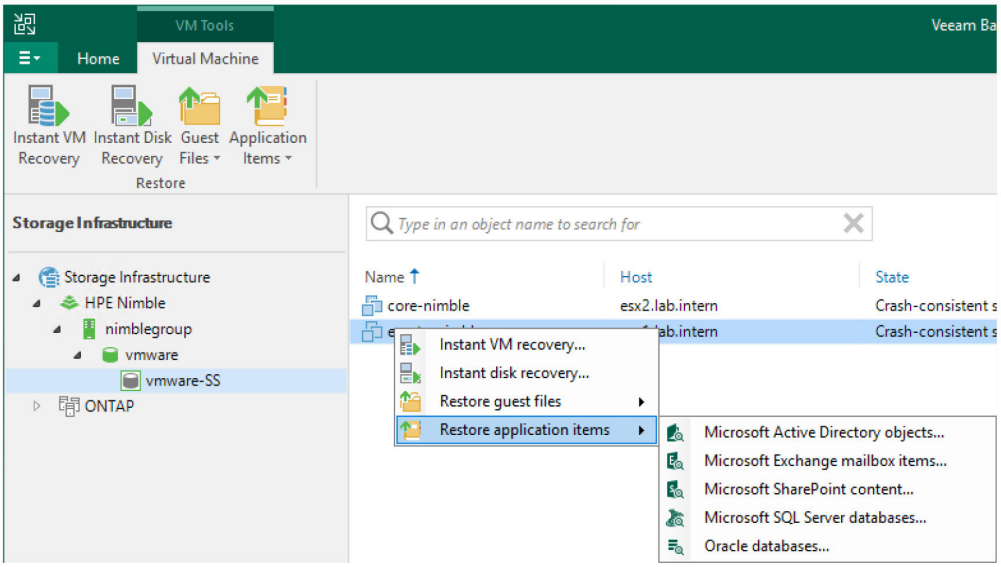


Abbildung 5: Wiederherstellung von Objekten aus Storage-Snapshots

Ein weiterer Vorteil von Speicherintegrationen ist die Möglichkeit, Backups aus Storage-Snapshots vorzunehmen. Mit Backups aus Storage-Snapshots lassen sich VMs mit hohem Transaktionsvolumen, z. B. Datenbank-Server, ohne das Risiko von VM-Stuns beim Konsolidieren der VMware-Snapshots sichern. Dies ist noch immer der Hauptgrund, warum Storage-Snapshots verwendet werden, obwohl aktuelle vSphere-Versionen deutlich besser geworden sind.

Und noch einen Vorzug bieten Backups aus Storage-Snapshots: Veeam kann so mithilfe seiner proprietären Datenabrufmechanismen klassische VADP-Backups in puncto Leistung ausstechen. Dies ist vor allem für vollständige Backups oder Backups mit hohen Änderungsraten relevant.

Best Practice: Verwenden Sie die Speicherintegration, wenn Ihre Speicherlösung Snapshots für Veeam Backup & Replication unterstützt.

7. VMware vSAN-Backup

Bei herkömmlichen Speicherprotokollen ist ein direkter Speicherzugriff oder ein Backup aus Storage-Snapshots ausgeschlossen.

Als Backup-Modi stehen in diesem Fall nur die Virtual Appliance (Hot-Add) und der Netzwerkmodus zur Verfügung. Die bessere Option ist hier der Netzwerkmodus, der inkrementelle Backups beschleunigen kann. Eine Notwendigkeit für den Hot-Add-Prozess besteht nicht. Im Hot-Add-Modus sichert Veeam Backup & Replication VMs in Relation zu den benachbarten VM-Daten. Backups erfolgen über den Proxy auf den Host mit den meisten VM-spezifischen Daten. Damit dies reibungslos funktioniert, muss pro ESXi-Host ein Hot-Add-Proxy vorhanden sein. Host-Affinität für die Proxy-VM-Regeln verhindert, dass der Distributed Resource Scheduler (DRS) von VMware diese VMs auf andere ESXi-Hosts verschiebt.

Dadurch verkleinert sich das Backup-Fenster, während der Netzwerk-Traffic und die Latenz verringert werden. Würde man dagegen eine VM auf einem Host und den Proxy auf einem anderen Host laufen lassen, müssten im Netzwerk größere Datenmengen übermittelt werden, mit längeren Latenzzeiten und langsameren Geschwindigkeiten als Folge. Version 10 unterstützt nun auch Linux-Proxys für den Hot-Add-Modus. Mit Version 11 sind weitere Backup-Modi für Linux-Proxys hinzugekommen, darunter:

- Netzwerkmodus (NBD) zur Verwendung mit vSAN
- Direkt-SAN (NFS, iSCSI und FC)
- Backup aus Storage-Snapshots (iSCSI, FC)

Laut seiner Zertifizierung in der Kategorie Datensicherung ist Veeam Backup & Replication für vSAN sofort VMware-einsatzbereit.

Weitere Informationen sind der VMware vSAN-Hardware-Kompatibilitätsliste zu entnehmen. Kompatibilität ist auch für vSAN in VMware Cloud auf AWS gegeben.

> *„Wir sichern unsere v SAN-Infrastruktur mit je einem eigenen virtuellen Proxy pro ESXi-Host. Dementsprechend viele Proxys haben wir, die aber recht klein sind (vier vCPUs). Außerdem haben wir eine weit verteilte VSAN-Clusterkonfiguration mit weit auseinandergelegenen Rechenzentren. Mit genau einem Proxy pro ESXi-Host stellen wir sicher, dass Veeam jeder zu sichernden VM den jeweils ‚nächsten' Proxy zuweist. Dadurch vermeiden wir übermäßigen Traffic in den Verbindungsleitungen zwischen den Rechenzentren."*
>
> – Manuel Aigner, Porsche Informatik

Best Practice: Testen Sie, welcher Backup-Modus in Ihrer Umgebung am schnellsten ist. Genau ein Hot-Add-Proxy pro ESXi vermindert den vSAN-Netzwerktraffic. Allgemein zeichnet sich der Hot-Add-Modus durch höhere Durchsatzraten aus, während der Netzwerkmodus weniger Aufwand bereitet.

8. Sicherheit

Zur Verwaltung von VM-Backups und -Wiederherstellungen muss sich Veeam Backup & Replication mit vCenter verbinden. Vom Standpunkt der Sicherheit her betrachtet, ist es jedoch immer ratsam, den Berechtigungsumfang auf ein notwendiges Mindestmaß zu beschränken. VMware vCenter hält sehr umfangreiche und detaillierte Berechtigungsoptionen für Backups bereit.

Welche Berechtigungen für welchen Backup-Modus eingerichtet werden müssen, können Sie der Übersicht über die erforderlichen Berechtigungen entnehmen. Jeder Backup-Modus erfordert andere Berechtigungen. Zum Beispiel muss beim Virtual-Appliance-Modus aus Sicherheitsgründen die Option zum Entfernen der Festplatte aktiviert sein. Abbildung 6 zeigt eine dedizierte Rolle mit eingeschränkten Berechtigungen für Backups an.

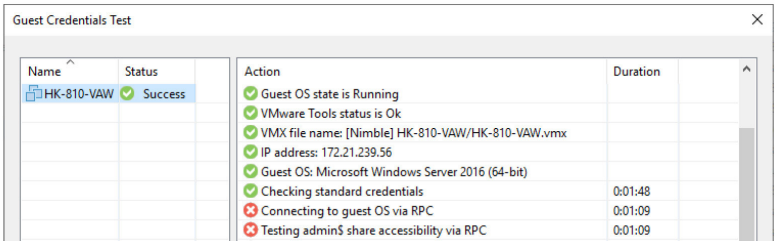


Abbildung 6: Dedizierte vSphere-Rollen für Veeam Backup & Replication

Solche Sicherheitsaspekte können die Wahl des Backup-Modus beeinflussen. Möglich ist auch eine Beschränkung bestimmter Backup-Server — sofern mehrere vorhanden sind — auf ausgewählte Standorte oder Objekte in vCenter.

Angesichts immer häufigerer Angriffe auf Backup-Server sollte die Backup-Umgebung abgesichert werden, wie im Best-Practices-Leitfaden beschrieben. Ein „abgesichertes Repository" kommt möglicherweise auch für die Speicherung unveränderlicher Backups infrage.

Best Practice: Gewähren Sie so nur so viele Berechtigungen wie unbedingt nötig.

9. Veeam Backup & Replication-Bereitstellung mit Veeam ONE planen

Die Veeam Availability Suite™ enthält Veeam ONE™, ein leistungsstarkes Planungstool für Veeam Backup & Replication-Bereitstellungen.

Veeam ONE zeigt den aktuellen Status der vSphere-Umgebung und etwaige Probleme an. Relevante Probleme könnten im Backup-Kontext beispielsweise eine hohe Speicherlatenz oder veraltete, große, verwaiste oder zu viele VM-Snapshots sein.

Veeam ONE prüft die VM-Konfiguration und gibt einen entsprechenden Bericht aus, der potenzielle Backup-Probleme auflistet.

Darin finden sich u. a. folgende typische Probleme:

- Keine VMware-Tools installiert
- Hardware-Version 4 oder früher
- Nicht backupfähige Festplatten (z. B. unabhängige Festplatten)
- Datastores mit weniger als 10 % freiem Speicherplatz
- Raw Device Mapping in VMs

Werden diese und andere Punkte im Voraus behoben, treten später beim Backup weniger Fehler auf.

Best Practice: Planen Sie mit Veeam ONE die Veeam Backup & Replication-Installation.

10. Anwendungsspezifische Backups über die VIX-API

In Punkt 4 hatten wir empfohlen, stets VMware-Tools zu installieren und auf dem neuesten Stand zu halten. Mithilfe von VMware-Tools können Veeam-Administratoren anwendungsspezifische Backups von Windows-VMs ohne direkte Netzwerkverbindung zur VM vornehmen.

Für ein anwendungsspezifisches Backup empfiehlt es sich, den Anwendungs-Proxy über RPC oder einen persistenten Gastagenten mit der VM zu verbinden. Dies ist auch die schnellste Methode. Falls jedoch einer Netzwerkverbindung zur VM Hindernisse im Weg stehen — etwa die Netzwerksegmentierung oder Firewalls -, kann zur Gastinteraktion auch die VIX-API oder, bei neueren vSphere-Versionen ab 6.5, die vSphere-API genutzt werden. Abbildung 7 stellt die Anmeldung über VIX dar (grüne Markierung).

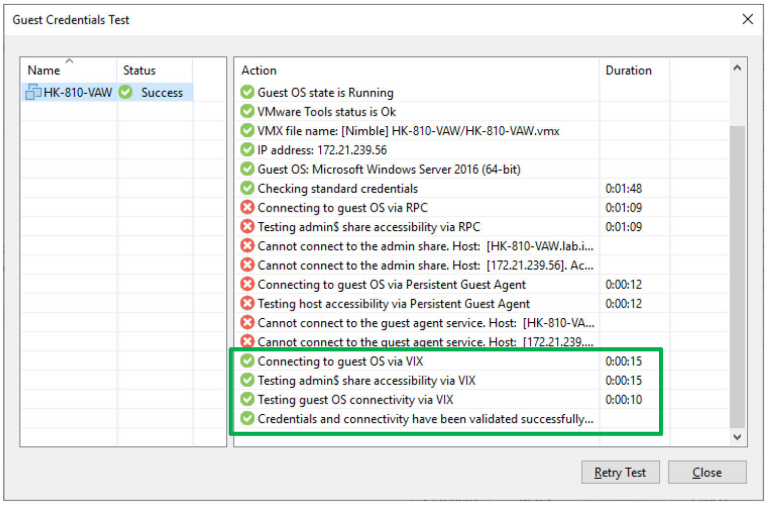


Abbildung 7: Prüfung der Gastsystem-Anmeldedaten über die VIX-API

Die VIX-API und die vSphere-API stellen allerdings gewisse Anforderungen, damit die Interaktion mit dem Gastsystem funktionieren kann. Diese Anforderungen werden im Veeam-Artikel KB 1788 ausführlich beschrieben. Im Wesentlichen gibt es zwei Anforderungen:

- Das Veeam-Benutzerkonto muss Mitglied der lokalen Administratorgruppe sein.
- Ist das Konto kein Administratorkonto, muss die Benutzerkontensteuerung von Windows deaktiviert werden.

Falls die RPC-Übertragung nicht funktioniert, dient die VIX-API oder die vSphere-API als Ersatz. In Umgebungen, in denen die meisten VMs über RPC nicht kontaktierbar sind, dauert das Backup dann länger, da Veeam zunächst versucht, eine Verbindung über RPC herzustellen. Für solche Fälle lässt sich Veeam so einrichten, dass zunächst eine VIX-Verbindung hergestellt wird; dazu muss auf dem Backup-Server oder auf dem Gastinteraktions-Proxy der folgende Registrierungsschlüssel konfiguriert werden:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veeam\Veeam Backup and
Replication\ DWORD: InverseVssProtocolOrder

Wert = 1

Zum Deaktivieren (Standardeinstellung) wird der Wert auf 0 (false)
gesetzt.
```

Wichtig ist in diesem Zusammenhang, dass die beiden Gastinteraktions-APIs bei der Wiederherstellung einige Nachteile aufweisen. Zum einen können nur Dateien wiederhergestellt werden, aber keine Anwendungsobjekte. Microsoft Active Directory-, Exchange- oder ähnliche Objekte sind also außen vor, zur Wiederherstellung solcher Objekte ist eine Netzwerkverbindung nötig. Zum anderen geht die Wiederherstellung von Dateien über das Netzwerk wesentlich langsamer vonstatten.

Apropos Geschwindigkeit: Auch der Dienst VeeamLogShipper, der SQL-Protokolle automatisch auf einer anderen Instanz sichert, kann notfalls auf VIX zurückgreifen, wenn eine Netzwerkverbindung zum Repository nicht möglich ist. Für die meisten Umgebungen dürfte dies zu lange dauern. Daher empfiehlt es sich, SQL-Protokolle über das Netzwerk zu sichern.

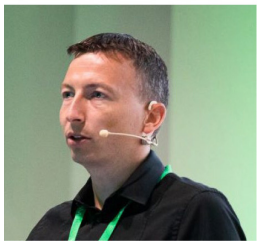
Best Practice: Behalten Sie hinsichtlich der Gastinteraktion die Nachteile der VIX- bzw. vSphere-API im Hinterkopf.

Fazit

Die Kombination aus Veeam Backup & Replication und VMware vSphere ist im Regelfall sofort einsatzbereit. Mit diesen leicht umzusetzenden Best Practices sorgen Sie aber für noch reibungslosere Abläufe.

Wenn Sie diese Best Practices in Aktion erleben möchten, testen Sie Veeam jetzt 30 Tage lang KOSTENLOS.

Über den Autor



Hannes Kasparick ist derzeit Mitglied des Produktmanagement-Teams von Veeam. Zuvor war er Senior Systems Engineer bei Veeam in der Region CEMEA. In dieser Funktion half er Kunden und Partnern dabei, mit Veeam-Produkten effektive und effiziente Backup- und DR-Lösungen zu erstellen.

Außerdem befasste er sich mit der Verwaltung von Linux- und Windows-Umgebungen sowie von Infrastrukturdiensten wie Storage, Netzwerken, Firewalls und VMware. Seine Berufserfahrung in der IT-Branche hat er in über 15 Jahren gesammelt.

Über Veeam

Veeam® ist ein führender Anbieter von Backup-Lösungen mit Cloud Data Management™. Mit der zentralen Plattform von Veeam können Unternehmen ihre Datensicherungsprozesse modernisieren, den Umstieg auf eine Hybrid Cloud beschleunigen und ihre Daten schützen. Mehr als 400.000 Kunden weltweit, darunter 82 % der Fortune 500- und 69 % der Forbes Global 2000-Unternehmen, und Kundenzufriedenheitswertungen auf dem 3,5-fachen Niveau des Branchendurchschnitts belegen eindrucksvoll Veeams Führungsposition auf dem Markt. Veeam ist ganz dem Channel verpflichtet und führt globale Partner sowie HPE, NetApp, Cisco und Lenovo als Exklusivhändler. Veeam betreibt Niederlassungen in über 30 Ländern. Weitere Informationen finden Sie unter https://www.veeam.com/de oder auf Twitter @veeam.