

Veeam Backup & Replication

Neuerungen in v11

Veeam® Backup & Replication™ v11 ist die zentrale Plattform für ein umfassendes Datenmanagement. Sie ist so leistungsstark und flexibel, dass sie sich auf alle Phasen des Datenlebenszyklus sowie komplexe Hybrid-/Multi-Cloud-Umgebungen anwenden lässt. Dieses Dokument enthält einen Überblick über wichtige neue Features und Verbesserungen in V11.

Continuous Data Protection (CDP)

Verringern Sie Ausfälle und minimieren Sie Datenverluste bei Ihren Tier-1-Workloads mit VMware vSphere. Wiederherstellungen auf den letzten Status oder auf einen gewünschten Zeitpunkt sind dank integrierter CDP-Funktionalität in kürzester Zeit (strengste RTO und RPO) möglich.

Hier eine Auswahl der exklusiven Vorteile einer Implementierung von **Veeam CDP**:

- **Keine VM-Snapshots:** Veeam CDP erfasst alle Schreibvorgangs-E/A im Datenpfad mithilfe des *VMware-zertifizierten E/A-Filtertreibers*. Dadurch erübrigt sich das Erstellen von VM-Snapshots mittels herkömmlicher Replikationsjobs. Und dank Tracking auf E/A-Ebene werden nur geänderte Daten an den DR-Standort übermittelt. Im Gegensatz dazu stehen größere Datenblöcke virtueller Festplatten, die durch Changed Block Tracking ausgegeben werden.
- **Keine Workload- oder Hardware-Abhängigkeit:** Schützen Sie BELIEBIGE Betriebssysteme und Anwendungen, die in einer vSphere-VM ausgeführt werden können. Anders als speicherbasierte Replikation überbrückt Veeam CDP auch nicht übereinstimmende Speicher-Arrays sowie hyperkonvergente Speicherlösungen und sogar lokalen vSphere ESXi-Speicher.
- **Asynchrone Replikation:** Im Unterschied zu synchroner Replikation auf Arraybasis lässt sich Veeam CDP auf jeder Distanz einsetzen. Dank E/A-Konsolidierung beim mehrmaligen Überschreiben desselben Blocks und Komprimierung des Netzwerk-Traffics wird Bandbreite gespart.
- **Richtlinienbasierte Sicherung:** Herkömmliche Replikationsjobs müssen geplant werden, diese hier nicht. Legen Sie einfach das erforderliche RPO fest (der im Katastrophenfall maximal zulässige Umfang des Datenverlusts), die CDP-Richtlinie führt dann die Synchronisierungszyklen dem Bedarf entsprechend aus. Damit Sie nicht von Monitoring-Meldungen überflutet werden, können Sie zudem Schwellenwerte für die Übertretung von RPOs festlegen, sodass vorübergehende Verbindungsprobleme nicht gleich Alarm auslösen.

Das **NEUE Veeam® Backup & Replication™ v11** schützt vor Datenverlust und Ransomware-Schäden. Unternehmen können damit sogar das Zwanzigfache ihrer Kosten für die langfristige Archivaufbewahrung sparen. In dieser 4-in-1-Lösung greifen Backups, Replikation, Storage-Snapshots und die **NEUE** Funktion „kontinuierliche Datensicherung“ (Continuous Data Protection, CDP) in einer einzigen Plattform ineinander, um für eine schnellere und flexiblere Datensicherung, -wiederherstellung und -aufbewahrung zu sorgen. Version 11 ermöglicht bislang unerreichte Resilienz für Unternehmen jeder Größe – mit über 200 neuen Features und Verbesserungen, darunter:

- Kein Datenverlust mehr – dank **Veeam CDP**
- Schutz vor Ransomware mit unveränderlichen Backups in einem **abgesicherten Linux-Repository**
- Vermeidung von Ausfällen mit **sofortiger Wiederherstellung für NAS, Microsoft SQL und Oracle**
- Kostensenkung um mehr als das 20-Fache bei **Langzeitarchivierung in Cloud-Storage auf Amazon S3 Glacier und Azure Blob Archive**
- Einheitliche **cloudbasierte Workload-Absicherung mit AWS und Azure**
- Auslagerung komplexer Aufgaben mit **BaaS und DRaaS auf Basis von Veeam**

Ergänzen Sie **Veeam Backup & Replication v11** um Einblicke, Reports und detaillierte Daten von **Veeam ONE™ v11** in einem Enterprise-Paket namens **Veeam Availability Suite™ v11**, das alle Ihre Sicherheits- und Analyseanforderungen erfüllt.

Mit **Veeam Disaster Recovery Orchestrator v4** profitieren Sie von automatisierter Standortwiederherstellung und Tests – eine leistungsstarke Kombination zugunsten von Business Continuity mit Orchestrierung in jedem Maßstab.

Unterstützte Umgebungen

Eine detaillierte Liste der unterstützten Umgebungen finden Sie in den [Release-Hinweisen](#) zum Produkt.

- **Flexible Aufbewahrung:** Sie können jeweils eine Richtlinie für die *kurzfristige Aufbewahrung* – dank granularer RPO-Zeiträumen mit ausfallsicheren Wiederherstellungen auf einen bestimmten Zeitpunkt – und eine Richtlinie für die *langfristige Aufbewahrung* definieren – mit optionalen regelmäßigen und anwendungskonsistenten Wiederherstellungspunkten. So profitieren Sie von einer zusätzlichen Schutzebene.
- **Flexible Bereitstellungsmodelle:** Je nachdem, wie viele Daten zu sichern sind, stehen Ihnen virtuelle CDP-Proxies oder *dedizierte physische CDP-Proxies* zur Auswahl, um den Aufwand für die Datenverarbeitung von vSphere-Hosts weg zu verlagern und so die VM-Konsolidierungsquote zu verbessern. In jedem Fall ist pro vSphere-Cluster nur ein Proxy zwingend erforderlich. Zusätzliche Proxies sorgen für Redundanz und unterstützen die Skalierbarkeit.
Hinweis: „CDP-Proxy“ ist eine neue Rolle, die sich mit anderen Veeam-Komponenten einen Server teilen kann.
- **Bereitstellungsassistent:** Ein integrierter Rechner sorgt für Klarheit bei der Bereitstellung. Beim Eingrenzen der RPO-spezifisch erforderlichen Bandbreite berücksichtigt er den E/A-Verlauf aller zu sichernden VMs in der CDP-Richtlinie. Außerdem schätzt er ab, ob die aktuell verfügbaren CDP-Proxy-Ressourcen angesichts der bisherigen Austauschrate ausreichen.
- **Keine Zusatzkosten:** Veeam CDP ist Bestandteil Ihrer Universallizenz – ebenso wie bereits übliche Datensicherungsmethoden für vSphere-VMs: hostbasierte Backups oder Replikationen, agentenbasierte Backups, Backups auf Anwendungsebene und Storage-Snapshots. Wie üblich *erfordert die Verwendung mehrerer Sicherungsmethoden auf derselben VM keine zusätzlichen Lizenzen!* Sie müssen nicht mehr sorgfältig abwägen, welchen VMs Sie eine teure CDP-Lizenz von Drittanbietern zuweisen sollten. Ab jetzt kann nur noch die verfügbare Bandbreite Ihre DR-Strategieplanung einschränken!

HINWEIS: Die Funktionalität „Veeam CDP“ setzt die Bereitstellung des E/A-Filters im quell- und zielseitigen vSphere-Cluster voraus. Klicken Sie dazu mit der rechten Maustaste auf den jeweiligen Cluster in der Baumstruktur neu hinzugefügter Cluster – zu finden im Tab für die Backup-Infrastruktur.

Veeam CDP ist Bestandteil der **Veeam Universal License**. Liegt eine herkömmliche sockelbasierte Lizenz vor, ist die **Enterprise Plus** Edition Voraussetzung.

Abgesichertes Repository

Bewahren Sie Ihre Backups in abgesicherten, vor Malware und Hackerangriffen geschützten Repositories auf, in denen unveränderliche Backups die Verschlüsselung und Löschung durch Ransomware und böswillige Akteure verhindern. Das ermöglichen die folgenden Verbesserungen für Backup-Repositories auf Linux-Basis:

- **Anmeldedaten für den Einmalgebrauch:** Nur einmal verwendbare Anmeldedaten sind Voraussetzung beim abgesicherten Repository. Bei der ersten Bereitstellung und beim Installieren von Produkt-Updates werden sie vom Benutzer interaktiv angegeben, jedoch nie in der Konfigurationsdatenbank gespeichert. Hacker haben so nicht die Möglichkeit, die Anmeldedaten von einem manipulierten Backup-Server abziehen und sich damit beim Repository anzumelden.
- **Unabhängig vom SSH-Protokoll:** Alle bisherigen Anwendungsfälle für das SSH-Protokoll sind im erweiterten Transportprotokoll zusammengefasst. Demzufolge ist eine SSH-Verbindung nur bei der ersten Bereitstellung und beim Installieren von Produkt-Updates erforderlich. Somit können Kunden SSH mit interaktiver Multifaktorauthentifizierung (MFA) absichern oder den SSH-Server gleich ganz deaktivieren, um das Repository umfassend zu schützen, sogar bei Zero-Day-Lücken.

- **Unveränderliche Backups:** Mit versehentlich gelöschten Backups, Ransomware und Hackern müssen Sie sich nicht mehr herumschlagen. Sorgen Sie für die Unveränderlichkeit Ihrer Backups auf Imageebene – dank GFS sind sie über die gesamte Dauer der richtliniengesteuerten Aufbewahrung geschützt. Diese Funktion beruht auf dem nativen Linux-Feature für unveränderliche Dateien. Bei diesem wird mittels entsprechender Flags die Modifizierbarkeit und Löschung von Dateien beschränkt. Nur Benutzer mit Root-Berechtigungen können Flags entfernen, die Root-Anmeldedaten werden jedoch nicht auf dem Backup-Server gespeichert und können nicht wiederverwendet werden. Achten Sie also nur darauf, dass die Anmeldedaten nicht in einer anderen Anwendung gespeichert werden und dass die „sudoers“-Liste leer bleibt!

Aus Redundanzgründen wird der Zeitpunkt, zu dem die Unveränderlichkeit enden soll, an zwei Stellen gespeichert: Zum einen in der gesonderten Konfigurationsdatei und zum anderen im erweiterten Attribut jeder Backup-Datei. Der erste Zeitstempel wird automatisch erweitert, wenn abhängige inkrementelle Wiederherstellungspunkte zur Backup-Kette hinzugefügt werden. Um gegebenenfalls der gesetzlichen Aufbewahrungspflicht nachzukommen, kann er mittels PowerShell auch manuell erweitert (nicht aber verringert) werden. Als Bestandteil der unveränderlichen Datei bleibt der zweite Zeitstempel, wie er ist. Das Flag für die Unveränderlichkeit wird aus der Backup-Datei entfernt, wenn die lokale Zeit des Repository-Servers beide Werte überschreitet.

Eine Überprüfung durch Dritte ergab, dass V11 die US-Vorschriften für Finanzdienstleister bezüglich WORM-Speicher (Write Once, Read Many) erfüllt. Eine konforme Konfiguration für abgesicherte Repositories schützt Backup-Daten vor Manipulation und erfüllt die Kriterien für nicht erneut beschreibbaren, nicht löschbaren Speicher, wie sie in SEC 17a-4(f), FINRA 4511(c) und CFTC 1.31(c)-(d) vorgegeben sind. Die Compliance-Prüfung erfolgte durch [Cohasset Associates](#).

HINWEIS: Leider können wir keine Backup-Modi unterstützen, die Direktänderungen an Backup-Dateien in unveränderlichen Repositories umfassen. Deshalb ist Ihre Auswahl auf herkömmliche vorwärts inkrementelle Backups mit regelmäßigen Full-Backups beschränkt. Aus diesem Grund ist XFS das ideale Dateisystem für solche Repositories – dank synthetischen Full-Backups ohne Speicherplatzbedarf mittels unserer erweiterten XFS-Integration (ein v10-Feature).

Erweiterte Unterstützung für Objektspeicher

Sie können die Kosten für die langfristige Datenarchivierung und -aufbewahrung um das bis zu 20-Fache senken, manuelles Bandmanagement aufgeben und Backup-Lebenszyklen von Anfang bis Ende steuern, und zwar dank der erweiterten Unterstützung für „Hot“-Objektspeicher in Capacity Tier und Unterstützung für „Cold“-Objektspeicher in der neuen Archive Tier des Scale-Out Backup Repository™ (SOBR).

In Capacity Tier und bei der Archivierung von NAS-Dateiversionen haben Sie eine große Auswahl an Objektspeicher-Repositories. Neu dabei ist **Google Cloud Storage (GCS)**. Die native Integration erfolgt über die proprietäre GCS-Objektspeicher-API, allerdings werden noch keine unveränderlichen Backups unterstützt. Der Grund hierfür: GCS bietet nicht die Möglichkeit einer Objektsperre (Object Lock).

In Archive Tier unterstützen wir **Amazon S3 Glacier** (einschließlich Deep Archive) und mit dem neuen SOBR-Feature Archive Tier unterstützen wir **Microsoft Azure Blob Storage Archive Tier**. Im Gegensatz zum Hot-Objektspeicher in der Cloud sind diese Cold-Tiers wirtschaftlich auf den Anwendungsfall „Write Once Read Never“ (Einmal schreiben, niemals lesen) abgestimmt und eignen sich daher am besten für die langfristige Archivierung von GFS-Backups. Ihre deutlich höheren API- und Abrufkosten sowie die Abrufdauer in Stunden inspirierte uns dazu, eine eigene Archive Tier für das kosteneffiziente, dabei aber nahtlose Management des Backup-Lebenszyklus zu entwickeln.

Dies sind die Key-Features von Archive Tier:

- **Unveränderliche Backups:** Um für Compliance zu sorgen, können archivierte Backups in Amazon S3 Glacier für die gesamte richtliniengesteuerte Dauer ihrer Aufbewahrung unveränderlich gemacht werden.

- **Richtlinienbasierte Auslagerung:** Ebenso wie in Capacity Tier gibt es keine Auslagerungsjobs, die verwaltet werden müssten. Bestimmen Sie einfach ein Archivzeitfenster, das groß genug ist, um nur die Wiederherstellungspunkte, auf die Sie wahrscheinlich nie wieder (oder nur in Ausnahmefällen) zugreifen müssen, zu archivieren. SOBR, der intelligente, softwaredefinierte Speicher, kümmert sich dann ganz allein um das Verschieben der Daten über alle Ebenen hinweg. Sie müssen nur noch den täglichen SOBR-Statusreport im Blick behalten, um sicherzugehen, das alles seine Ordnung hat.
- **Kostenoptimierte Archivierung:** Aufgrund kostenintensiver APIs für Cold-Objektspeicherebenen werden ausgelagerte Datenblöcke in größere Objekte von bis zu 512 MB „umverpackt“. Dies erledigen Helper-Appliances, die in der Public Cloud über die Dauer der Archivierungssitzung automatisch bereitgestellt werden. Des Weiteren überspringen wir automatisch das Archivieren von Wiederherstellungspunkten, wenn die Aufbewahrungsrestdauer unter der geforderten Speichermindestdauer der genutzten Speicherklasse liegt. Dadurch lassen sich Strafgebühren für zu frühes Löschen vermeiden.
- **Flexible Speichermethoden:** Damit Sie weitere Kosten sparen, geht die Archive Tier-Auslagerung standardmäßig unbeschränkt inkrementell vonstatten. Pro archiviertem Wiederherstellungspunkt wird nur das Delta ab dem vorherigen hochgeladen und gespeichert. Für Richtlinien mit extrem langer Aufbewahrungsdauer bieten wir allerdings auch an, jedes vollständige GFS-Backup separat zu speichern. Dadurch vermeiden Sie einzelne jahrzehntelange Ketten an inkrementellen Backups und behalten durch Speicherklassen wie Amazon S3 Glacier Deep Archive die Gesamtkosten unter Kontrolle.
- **Eigenständige Archive:** Archivierte Backups sind nicht abhängig von externen Metadaten, sodass sie auch bei einem Verlust des lokalen Backup-Servers importiert werden können. Zudem herrscht keine Anbieterbindung, da archivierte Backups jederzeit aus dem Objektspeicher importiert und wiederhergestellt werden können. Dafür steht die Veeam Backup & Replication *Community Edition* zur Verfügung, für die keine gültige Lizenz erforderlich ist. Kurzum: Wir nehmen Ihre Daten nicht in Geiselhaft!
- **Keine Zusatzkosten:** Anders als Anbieter von Sekundärspeicher-Appliances, die Daten unbedingt in ihrer teuren lokalen Hardware halten möchten, verlangt Veeam kein Abonnement auf TB-Basis für die Datenarchivierung in Objektspeicher. Das heißt, wir erheben keine Cloud-Steuer!

SOBR Archive Tier ist Bestandteil der **Veeam Universal License**. Liegt eine herkömmliche sockelbasierte Lizenz vor, ist die **Enterprise Plus** Edition Voraussetzung.

Erweiterte Instant Recovery

Der Wegbereiter hinter Instant VM Recovery® ermöglicht die nahtlose Wiederherstellung der folgenden neuen Workloads, damit die Verfügbarkeit der Workloads in Ihrem Rechenzentrum weiter steigt:

- **Sofortwiederherstellung von Microsoft SQL Server- und Oracle-Datenbanken:** Die Datenbank lädt nicht? Entwickler haben versehentlich eine wichtige Tabelle gelöscht? Kein Problem! Sie können jede Datenbank aus dem Backup auf den letzten Status oder einen früheren Zeitpunkt auf einem beliebigen Produktivdatenbank-Server oder -Cluster (physisch oder virtuell) wiederherstellen – innerhalb von Minuten und unabhängig von der Größe.

Ausgewählte Datenbanken werden umgehend für Produktivanwendungen und Datenbank-Clients bereitgestellt und lassen sich normal ändern. Sämtliche Änderungen werden im Cache vorgehalten – das Backup selbst wird selbstverständlich nicht geändert. Währenddessen stellt Veeam Datenbankdateien automatisch und im Hintergrund im Produktiv-Speicher wieder her und synchronisiert laufend den tatsächlichen (Änderungen unterworfenen) Datenbankzustand mit dem Produktiv-Speicher.

Zum Schluss der Wiederherstellung müssen Sie veranlassen, dass die Datenbank über den Produktiv-Speicher ausgeführt wird. Das ist nach minimaler Ausfallzeit erledigt, ähnlich wie beim Neustarten einer Datenbank. Dieser Wechsel kann manuell ausgelöst oder als automatische Ausführung geplant werden – entweder sobald die Synchronisierung abgeschlossen ist oder während des nächsten Wartungszeitraums.

Im Gegensatz zur interaktiven Funktionalität für Veröffentlichungen kommt bei der Datenbank-Sofortwiederherstellung eine servicebasierte Architektur zum Einsatz und die Benutzeroberfläche des Veeam Explorer™ muss nicht ausgeführt werden. Und sollte eine Komponente der Backup-Infrastruktur während der Sofortwiederherstellung neu starten, stellt sich der „Zubringer“ Instant Recovery automatisch selbst wieder her, sobald alle erforderlichen Server erneut online sind. Bei längeren Ausfällen ab einer Stunde können Sie die Sofortwiederherstellung in der Veeam Explorer-Oberfläche selbst fortführen lassen.

Die Datenbank-Sofortwiederherstellung ist Bestandteil der **Veeam Universal License**. Liegt eine herkömmliche sockelbasierte Lizenz vor, ist eine Edition ab **Enterprise** Voraussetzung.

- **Sofortveröffentlichung von NAS-Backups:** Ein NAS- oder Dateiserver ist abgestürzt? Sie haben versehentlich eine komplette Dateifreigabe gelöscht? Kein Problem! Veröffentlichen Sie SMB-Dateifreigaben einfach aus dem Backup mit dem letzten Status oder dem Status eines früheren Zeitpunkts auf dem ausgewählten Mount-Server. Ihre Nutzer haben in dieser temporären SMB-Dateifreigabe sofort Zugriff auf ihre Daten, während Sie das Problem beheben oder Daten wiederherstellen.

Unsere V11-Betatester haben noch andere Anwendungsfälle ausgemacht: Das Aktivieren von Drittanwendungen und -skripten für den sofortigen Zugriff auf den Inhalt eines NAS-Backups zum Zweck des Data Mining und sonstiger **Datenwiederverwendung**. Übernimmt dies Backup-Speicher-Hardware, die während des Produktivbetriebs in der Regel ungenutzt bleibt, lassen sich Dateisperrungen und eine Beeinträchtigung der Produktivumgebung umgehen. Prototypen wurden von Community-Mitgliedern der folgenden Spezialgebiete entwickelt: maschinelles Lernen (ML), Suche nach personenbezogenen Daten zur Unterstützung von Compliance-Prozessen, DSGVO-Unterstützung und Malware-Erkennung (automatische Dateianalyse auf inaktive Malware anhand zusätzlicher Virenschutz-Anwendungen).

- **Sofortwiederherstellung von ALLEM in Microsoft Hyper-V:** V11 ermöglicht weitere Anwendungsfälle in der Datenwiederherstellung und -portierbarkeit, indem es BELIEBIGE physische Server, Workstations, virtuelle Maschinen und Cloud-Instanz-Backups in Microsoft Hyper-V-VMs umgehend wiederherstellt. Dabei spielt es keine Rolle, welches Veeam-Produkt das Backup erstellt hat. Schulungen und Praxisübungen sind nicht erforderlich, die Wiederherstellung geht dank der integrierten P2V/V2V-Konvertierungslogik einfach so vonstatten. Wiederherstellungen und Migrationen erfolgen mit ganz neuer Schnelligkeit und Flexibilität – so wird DR für Hybrid Clouds Realität.

Und da der Veeam-Backup-Server unter Microsoft Windows ausgeführt wird, ist der Hyper-V-Host praktisch schon in ihn integriert und zur Nutzung bereit! Wir unterstützen sogar Windows 10 Hyper-V als Ziel für diese Funktionalität, was insbesondere Managed Serviceprovidern (MSP) hilft, äußerst kostengünstige All-in-One-DR-Appliances auf Basis von Veeam und Windows 10 zu konfigurieren und bei ihren Kunden vor Ort bereitzustellen.

Weitere Verbesserungen

Neben diesen entscheidenden neuen Features bietet V11 noch mehr als 200 weitere Verbesserungen, die basierend auf Kunden-Feedback und Erkenntnissen aus Forschung und Entwicklung umgesetzt wurden. Die wichtigsten von ihnen sind hier aufgeführt:

Allgemein

Backup-Engine

V11 bringt mehr als die doppelte Backup-Leistung in Veeam-Komplettbereitstellungen auf Allzweck-Serverhardware. Kunden können beim Erstellen eines Backups somit mehr als 11 GB/s pro Knoten erreichen – sofern die primären Arrays und die Speicher-Fabric mithalten! Möglich wird diese rasante Leistungssteigerung durch mehrere Verbesserungen an der hochleistungsfähigen Server- und Speicherhardware:

- **Systemcache-Bypass:** In V11 umgehen die zieleitigen Data Mover den Betriebssystem-Cache, damit dieser nicht mit dem controllerseitigen Cache und den erweiterten E/A-Optimierungen hochleistungsfähiger RAID-Controller in Konflikt gerät. Dadurch sinkt zum einen die Auslastung der Backup-Repository-CPU und steigt zum anderen die Leistung um bis zu 50 %.
- **Ausgerichtete Schreibvorgänge:** Nicht ausgerichtete Schreibvorgänge beeinträchtigen sowohl die Auslastung des Speicherprozessors als auch dessen Leistung, daher werden Backup-Dateien in V11 in 4-KB-Datenblöcken ausgerichtet. Bei neu erstellten Repositories ist dieses Feature standardmäßig aktiviert. Für ältere Repositories lässt es sich mit dem Cmdlet [Set-VBRBackupRepository](#) massenweise aktivieren. Zur Anwendung der neuen Einstellung ist kein aktives Full-Backup erforderlich.
- **Bessere Übertragung in gemeinsam genutztem Arbeitsspeicher:** Bei Datenverarbeitungsgeschwindigkeiten gegen 100 Gbit/s hat auch moderner Arbeitsspeicher durch seine Geschwindigkeit Einfluss auf die allgemeine Datenverarbeitungsleistung. V11 optimiert die RAM-Interaktionen und beschleunigt dadurch die Datenübertragung zwischen quell- und zieleitigen Data Movers, wenn diese auf demselben Server ausgeführt werden.
- **NUMA-Unterstützung:** Um in Servern mit mehreren Prozessoren Engpässe bei internen Bussen durch sich kreuzenden Traffic der NUMA-Knoten zu vermeiden, sollten voneinander abhängige Prozesse idealerweise auf demselben Knoten stattfinden. V11 unterstützt NUMA vollständig und sorgt dafür, dass sich quell- und zieleitige Data Mover nie auf unterschiedlichen Knoten befinden.
- **Optimale Komprimierung:** Nach einer Überarbeitung der standardmäßigen Implementierung unseres Komprimierungsalgorithmus verzeichnen wir ein etwas besseres Komprimierungsverhältnis und eine deutlich bessere Dekomprimierungsleistung. Verglichen mit V10 erfolgt die Ausführung einer SQL-Abfrage nach 30 GB Daten aus einer Stack Overflow-Datenbank, die in einer sofort wiederhergestellten VM ausgeführt wird, jetzt 28 % schneller.
- **Verbesserungen am Ressourcenplaner:** Der Ressourcenplaner für die Backup-Infrastruktur wurde umfassend optimiert, sodass die Ressourcenbereitstellung um bis zu 50 % verkürzt werden kann und die Anfahrzeit eines Jobs ebenfalls deutlich kürzer ausfällt. Von dieser Verbesserung sollten vor allem Umgebungen mit einer großen Anzahl von Backup-Proxies und SOBR-Erweiterungen profitieren.

Wiederherstellungs-Engine

Nachdem wir in V10 den erweiterten Datenabruf auf die Vollexport-Funktionalität für virtuelle Bänder in Windows-Backup-Repositories angewendet und dafür sehr positive Reaktionen bekommen hatten, haben wir diese Engine nun auf Linux-basierte Repositories ausgeweitet. Tatsächlich kommt sie mittlerweile bei ALLEN Features und Funktionalitäten zum Einsatz, bei denen Backup-Dateiinhalte aus Veeam-Repositories ausgelesen werden. Die tiefgreifendsten Verbesserungen sollten sich bei hochleistungsfähiger Speicher-Hardware und bei Funktionalitäten zeigen, die massenweise Datenbewegungen beinhalten, z. B. Wiederherstellungen vollständiger Images, Backup-Kopien, Objektspeicherauslagerungen usw.

PowerShell

- **PowerShell-Modul:** Auf allgemeinen Wunsch haben wir vom PowerShell-Snap-in auf das PowerShell-Modul umgestellt, das auf jedem Rechner mit installierter Backup-Konsole verwendet werden kann. Außerdem ist es nicht mehr erforderlich, dass PowerShell 2.0 auf dem Backup-Server installiert ist, was für viele Kunden ein Problem darstellte.
- **Neue PowerShell-Cmdlets:** In V11 stehen 184 neue Cmdlets zur Verfügung, sowohl für neu hinzugefügte Funktionalitäten als auch für die erweiterte Abdeckung der vorhandenen Features, wobei der Schwerpunkt auf der Wiederherstellungsfunktionalität liegt.

RESTful API

- **RESTful API für Backup-Server:** Die aktuelle RESTful API für Veeam Backup Enterprise Manager zeigt nur Funktionen an, die in der Weboberfläche von EM verfügbar sind. Aus diesem Grund fügen wir die RESTful API nun auch dem Backup-Server selbst hinzu. Dabei werden wir uns auf die am häufigsten benötigten Funktion für die Verwaltung von Backup-Servern konzentrieren. Die neue REST API in V11 wurde für die häufigsten Anwendungsfälle unserer Kunden und Partner konzipiert: die Verwaltung von Backup-Jobs und Backup-Infrastrukturen sowie deren einfachere Bereitstellung und Migration dank Massenimport/-export. Wir möchten wissen, was Ihnen wichtig ist, damit wir uns darauf konzentrieren können. Sagen Sie uns deshalb in den F&E-Foren, welche Themen wir als Nächstes angehen sollten.

Die RESTful API ist Bestandteil der **Veeam Universal License**. Liegt eine herkömmliche sockelbasierte Lizenz vor, ist die **Enterprise Plus** Edition Voraussetzung.

Sicherheit

- **FIPS-Compliance:** Auch im Basis-Build nutzt V11 FIPS-konforme Verschlüsselungsmodule. Der FIPS-konforme Betriebsmodus ist standardmäßig deaktiviert, um die Kompatibilität mit früheren Plattformversionen zu gewährleisten, auf denen FIPS-konforme Interaktionen nicht möglich sind (z. B. VMware vSphere-Versionen vor 6.5, aufgrund ihrer Abhängigkeit von nicht FIPS-konformen VDDK-Versionen). Eine Rolle spielt aber auch, Leistungseinbußen aufgrund der durch FIPS geforderten Echtzeitprüfungen der Modulintegrität zu vermeiden. Unter „Global Options“ (Globale Optionen) im Tab „Security“ (Sicherheit) können Sie den FIPS-konformen Betriebsmodus aktivieren.

Backup

Anwendungsspezifische Verarbeitung

- **Persistenter Gastagent:** Ihnen steht nun die Option offen, den persistenten Gastagenten für Windows-basierte VMs zu nutzen. Stellen Sie ihn einfach über eine Gruppenrichtlinie oder Ihr übliches Tool für die Software-Distribution bereit. Dabei werden nur einige wenige statische Ports des Netzwerks belegt (je nach genutzter Funktionalität). Auch die Benutzerkontenverwaltung stellt einfachere Anforderungen an die Kontoberechtigungen, wenn es darum geht, im Gast einen Laufzeitprozess bereitzustellen. Gleichzeitig reduzieren sich auch der Netzwerk-Traffic und die Gast-Verarbeitungsdauer. An Gäste muss nur eine winzige Installationskomponente verteilt werden, die restlichen Komponenten stellen sich automatisch bereit (und aktualisieren sich auch so).
- **SQL Server-Integration:** Die Engine für die anwendungsspezifische Verarbeitung verwendet jetzt den nativen MSOLEDBSQL-Provider, falls dieser auf dem SQL Server vorhanden ist. Dadurch können SQL Server mit erzwungenem TLS 1.2 verarbeitet werden, ohne dass Änderungen an der Registry notwendig sind. Des Weiteren werden jetzt HA-Gruppenpräferenzen für Datenbank-Backups berücksichtigt.
- **Mehr Einblick in die SQL-Datenbanksicherung:** Die neue, experimentelle Option für SQL Server erlaubt den Abbruch einer Backup-Sitzung auf Imageebene, falls das Transaktionsprotokoll-Backup nicht initialisiert werden kann oder keine SQL-Datenbanken auffindbar sind. Mit dem Registry-Wert *AAIPSQLShowExperimentalOptions* (DWORD, 1) im Backup-Server erscheint in den Einstellungen für die anwendungsspezifische Verarbeitung das entsprechende Kontrollkästchen. In den F&E-Foren freuen wir uns über jedes Feedback zu dieser neuen Option!

Backup-Jobs

- **Jobs mit hoher Priorität:** Bestimmten Backup-Jobs können Sie jetzt eine hohe Priorität zuweisen. Solche Jobs nutzen die dedizierte Warteschlange des Ressourcenplaners, die Backup-Infrastrukturressourcen vor normalen Jobs angeboten werden. Nutzen Sie diese Einstellung zur Sicherung von Workloads, deren Backup-Startzeit unbedingt eingehalten muss, oder für regelmäßig wiederkehrende Backup-Jobs mit strengen RPO-Anforderungen.
- **GFS-Aufbewahrung im Hintergrund:** Die Aufbewahrung vollständiger GFS-Backups wird jetzt unabhängig von der Ausführung des Backup-Jobs ausgeführt – als Systemaktivität des Veeam-Repository im Hintergrund. Dadurch verschwinden abgelaufene vollständige Backups nicht länger Repository-Speicherplatz, falls der Backup-Job für längere Zeit deaktiviert wird.
- **Aufbewahrung verwaister GFS-Backups:** Die Aufbewahrungsrichtlinie gilt jetzt für GFS-Backups ohne Job. Als Grundlage dient die letzte bekannte Aufbewahrungsrichtlinie. Dadurch werden provisorische Maßnahmen unnötig, z. B. das Beibehalten überflüssig gewordener Jobs zur Sicherung einer einzelnen Dummy-Maschine.
- **Verbesserungen bei der Aufbewahrung gelöschter VMS:** Die Aufbewahrung gelöschter VMs gilt jetzt nicht mehr, wenn beim Backup-Job keine Liste der verarbeiteten Maschinen erstellt wurde. Dies soll verhindern, dass Backups infolge von vorübergehenden Infrastrukturproblemen gelöscht werden.

Backup-Copy-Jobs

Für Backup-Copy-Jobs gilt jetzt dieselbe GFS-Aufbewahrungslogik wie für primäre Backup-Jobs. Dies sorgt für Einheitlichkeit im gesamten Produkt und Kompatibilität mit neuen Features wie unveränderlichen Backups des abgesicherten Repository oder die Aufbewahrung von GFS-Backups im Hintergrund. Im Einzelnen wurden folgende Änderungen vorgenommen:

- **Zeitbasierte GFS-Aufbewahrung:** Die GFS-Aufbewahrung für Backup-Kopien basiert nicht mehr auf der Anzahl der Wiederherstellungspunkte in jeder Generation, sondern auf dem Zeitpunkt. Dadurch werden GFS-Wiederherstellungspunkte nicht kürzer als nötig aufbewahrt, selbst wenn ein GFS-Backup versehentlich manuell erstellt wird.
- **Erstellungszeitpunkt vollständiger GFS-Backups:** Full-GFS werden nun direkt am geplanten Tag erstellt und versiegelt, und nicht erst, wenn der entsprechende Wiederherstellungspunkt zum ältesten in der Kette inkrementeller Backups wird. Wir hoffen, den Prozess für unsere Kunden dadurch verständlicher gemacht zu haben.
- **Keine vierteljährlichen Backups:** In Übereinstimmung mit dem GFS primärer Backup-Jobs wird ab jetzt keine Option für vierteljährliche Backups angeboten. Laufende Quartalspläne werden beim Upgrade auf V11 in monatliche umgewandelt, wobei deren Aufbewahrungswert entsprechend steigt. Vorhandene Backup-Copy-Jobs mit aktivierter GFS-Aufbewahrung werden beim Upgrade automatisch aktualisiert.

Auch diese Verbesserungen für Backup-Copy-Jobs gibt es:

- **Repository als Quelle:** Im Sofortkopie-Modus können Sie jetzt das gesamte Repository als Quelle für Backup-Copy-Jobs auswählen.
- **Tägliche Aufbewahrung:** Bei neuen Backups, die per Backup-Copy-Job erstellt werden, können Sie die Aufbewahrung auf Basis von Wiederherstellungspunkten oder – neu – auf Basis eines Zeitpunkts wählen.

Replikationsjobs

- **Unterstützung für NFS-Repositories:** Im Assistenten für Replikationsjobs können Sie jetzt ein NFS-basiertes Backup-Repository angeben, in dem Replikat-Metadaten gehostet werden sollen.

Quick-Migration-Jobs

- **SmartSwitch-Schwellenwert:** Interne Tests ergaben, dass Quick Migration im SmartSwitch-Modus bei VMs mit sehr großem Arbeitsspeicher zu lange dauert. Teilweise sogar so lange, dass der Vorgang sinnlos wird. Ursache hierfür ist die Dauer der Übertragung des Arbeitsspeicherstatus per NFC-Protokoll. Aus diesem Grund werden wir ab V11 bei Maschinen mit mehr als 8 GB RAM eine „kalte“ Migration (per Abschaltung) erzwingen. Mithilfe des Registry-Werts `QMSmartSwitchRAMThresholdGB` (DWORD) auf dem Backup-Server können Sie den Schwellenwert außer Kraft setzen.

Wiederherstellen

API für die Datenintegration

- **Unterstützung für Linux-Ziele:** Die API für die Datenintegration (DI-API) wurde um Unterstützung für das Mounten von Backup-Inhalten direkt auf dem Linux-Server erweitert.
- **Erweiterte Plattformunterstützung:** V11 ermöglicht die durch DI-API gestützte Veröffentlichung imagebasierter Backups aller Plattformen, die Veeam unterstützt. Dies beinhaltet cloudbasierte Backups für AWS, Microsoft Azure und Google Cloud Platform sowie Nutanix AHV- und VMware Cloud Director-Backups.

Wiederherstellung auf Dateiebene (File Level Recovery, FLR)

- **Linux-FLR ohne Helper-Appliance:** Aus Linux-Dateisystemen lässt sich die Wiederherstellung auf Dateiebene jetzt folgendermaßen bewerkstelligen: Das Backup lässt sich in JEDER Linux-Maschine mounten, egal ob es sich um eine dedizierte, eine zweiseitige oder die ursprüngliche handelt (die ja das Dateisystem immer „kennt“, von dem aus die Wiederherstellung erfolgt). Dadurch wird ein vSphere- oder Hyper-V-Host für die FLR-Helper-Appliance unnötig, ebenso wie komplexe Netzwerkanforderungen und Sicherheitsfragen rund um die Appliance. Zudem können Kunden Dateien direkt in cloudbasierten VMware-Infrastrukturangeboten wiederherstellen.

HINWEIS: Die Helper-Appliance ist immer noch eine Option, z. B. für archivierte Backups mit Dateisystemen, die in der Produktivumgebung nicht mehr genutzt werden.

- **Leistungsstärkere Wiederherstellung von Linux-Dateien:** Die FLR-Leistung bei anderen Dateisystemen als denen von Windows ist jetzt bis zu 50 % höher – unabhängig davon, ob Sie die Helper-Appliance verwenden oder nicht.

Veeam Explorer for Microsoft Active Directory

- **DFS-Konfigurationswiederherstellung:** Sie können jetzt Konfigurationen des Distributed File System (DFS) im Systemcontainer wiederherstellen.

Veeam Explorer for Microsoft Teams

- **Objektwiederherstellung für Microsoft Teams:** Microsoft Teams-Objekte lassen sich direkt aus dem Backup auf Imageebene des Veeam Backup for Microsoft Office 365-Backup-Servers wiederherstellen.

Backup-Infrastruktur

Backup-Repository

- **Leistungsstärkere synthetische Full-Backups auf ReFS:** Auf ReFS sollten synthetische Full-Backups jetzt um das bis zu Zweifache schneller abgeschlossen sein. Grund hierfür ist die eingeschränkte Nutzung des relativ langwierigen Windows-API-Aufrufs, der zur Erstellung einer neuen synthetischen Full-Backup-Datei erforderlich ist.
- **Deaktivierung von ReFS-Integritätsdatenströmen:** Mithilfe des Registry-Werts *DisableRefsIntegrityStreams* (DWORD, 1) können Sie auf dem Backup-Server ReFS-Integritätsdatenströme für Veeam-Backup-Dateien deaktivieren. Zwar empfehlen wir das Deaktivieren von Integritätsdatenströmen nicht, weil Datenintegrität bei der Datensicherung alles ist, doch kommen wir mit dieser Neuerung Kunden entgegen, die diese Einstellung zum Zweck der Leistungssteigerung gern selbst übernehmen möchten.

Scale-out Backup Repository

- **VeeamZIP™ und Tiering exportierter Backups:** Mit VeeamZIP und dem Backup-Export erstellte vollständige Backups sowie verwaiste Backups werden jetzt gemäß den Richtlinien für Capacity Tier und Archive Tier genauso verarbeitet wie herkömmliche Backups. Zudem können sie auf die übliche Weise kopiert oder in Objektspeicher ausgelagert werden. Importierte Backups werden, wie auch vorher üblich, nicht abgestuft.
- **Unterstützung für schnelles Klonen:** Der SOBR-Erweiterungsplaner berücksichtigt jetzt, dass die neu erstellte synthetische Full-Backup-Datei schnell geklont werden muss. Er wird nicht mehr voraussetzen, dass die bevorzugte Erweiterung ausreichend Festplattenspeicher aufweist, um nicht schnell geklonte synthetische Full-Backup-Dateien aufzunehmen. In früheren Versionen konnte SOBR schon einmal „explodieren“, wenn bestimmte Erweiterungen ihre Kapazitätsgrenze erreichten, weil der Planer plötzlich alle synthetischen Full-Backups anderen als den standardmäßigen Erweiterungen zuschrieb.
- **Auslagerung von Vorgängen im Windows-Ereignisprotokoll:** Die Kopier- und Auslagerungsvorgänge von Capacity Tier und Archive Tier erhalten jetzt im Systemereignisprotokoll entsprechende Einträge, damit Nutzer, die mit der protokollbasierten Überwachung dieser Prozesse betraut sind, einen besseren Einblick bekommen.

Objektspeicher-Repository

- **Aufgabenbegrenzung:** Zugunsten der Kompatibilität mit lokalem Objektspeicher, der von einer Vielzahl gleichzeitiger API-Aufrufe leicht überfordert ist, können gleichzeitige Aufgaben jetzt begrenzt werden. Bei den meisten Objektspeicherangeboten der Public Cloud werden Sie diese Begrenzung eher nicht benötigen, da diese unendlich skalierbar sind. In einem Fall kann eine Beschränkung jedoch sehr nützlich sein: Wenn Sie in den Einstellungen des Objektspeicher-Repository einen Gateway-Server für den Proxy-Zugriff auf das Internet festlegen. Dann kann es nämlich sein, dass auf diesem Server je nach CPU- und RAM -Ausstattung die Rechenressourcen knapp werden, wenn er zu viele Aufgaben gleichzeitig verarbeiten muss.
- **Wiederherstellungsleistung:** Die Leistung für Wiederherstellungen von lokalem Objektspeicher auf langsamer Hardware wurde bereits einige Male gesteigert.
- **Berechtigung „ListAllMyBuckets“ unnötig:** S3- und Google-Objektspeicher-Buckets lassen sich jetzt ohne vorherige Suche manuell im Assistenten für das Objektspeicher-Repository angeben. So können Serviceprovider individuelle Buckets für ihre Kunden anlegen und Berechtigungen mittels einer IAM-Richtlinie delegieren, ohne über die Bucketnamen eine Liste ihrer Kunden preiszugeben.
- **Blockdekomprimierung vor der Speicherung:** Backup-Datenblöcke lassen sich jetzt dekomprimieren, bevor sie in Objektspeicher geschrieben werden. So können lokale Objektspeichergeräte mit integrierter Deduplizierung Veeam-Backup-Daten effizienter verarbeiten. Zum Aktivieren dieser Funktion legen Sie auf dem Backup-Server den Registry-Wert *ObjectStorageDisableCompression* (DWORD, 1) an.

Veeam Cloud Connect

- **MSP-Modus von Cloud Connect Backup:** Mit Aktivierung des Kontrollkästchens „Allow this Veeam Backup & Replication installation to be managed by the service provider“ (Diese VBR-Installation vom Serviceprovider verwalten lassen) im Serviceprovider-Assistenten des mandantenseitigen Backup-Servers werden Backup-Metadaten wie Maschinennamen im Backup-Server des Serviceproviders nicht verschleiert. Das erleichtert MSPs die Bereitstellung verwalteter Backup-Services.
- **Mandanten auf Microsoft Active Directory-Basis:** Für die einfachere Absicherung von Remote-Workstations und Laptops in Unternehmensumgebungen mit der eigenständigen Version von Veeam Agent *for Microsoft Windows* unterstützt Veeam Cloud Connect jetzt Mandantenkontingente auf Basis von Active Directory-Konten. So können Enduser ihre Active Directory-Konten dazu verwenden, Cloud-Repositories mit der Cloud Connect-Infrastruktur zu verknüpfen und den Mandanten per Active Directory zu authentifizieren. Bei der fortlaufenden Authentifizierung während Backups wird ein sekundäres Passwort verwendet, damit Backup-Auslassungen aufgrund von Passwortänderungen nicht vorkommen. Allerdings erfordert die Bare-Metal-Wiederherstellung aus einem Cloud-Repository immer die Active Directory-basierte Authentifizierung des Kontos mittels des aktuellen Passworts. Erst dadurch wird der Zugriff auf Backups gestattet. Zudem ist weder die Datensicherung noch die Wiederherstellung möglich, wenn das Active Directory-Konto gesperrt ist.
- **Mandantenevakuierung:** Mithilfe des Cmdlet „Start-VBRCLOUDTenantBackupEvacuation“ lassen sich Mandanten jetzt aus Scale-out Backup Repository-Erweiterungen evakuieren.
- **Drosselung des WAN-Beschleunigers:** Die Einstellung „Limit incoming traffic from this tenant“ (Von diesem Mandanten eingehenden Traffic begrenzen) betrifft jetzt auch Mandanten, die Daten über integrierte WAN-Beschleuniger übermitteln. Zuvor galt sie nur für den Direktübertragungsmodus.
- **RAM-Auslastung des Cloud Connect-Servers:** Die RAM-Auslastung des Cloud Connect-Servers bei eingehenden Replikationsjobs haben wir drastisch reduziert.

Der Zugriff auf Veeam Cloud Connect *for Service Providers* erfordert eine **Mietlizenz**. Wenn Sie Zugriff auf Veeam Cloud Connect *for the Enterprise* wünschen, wenden Sie sich bitte an Ihren Veeam Ansprechpartner im Vertrieb.

Plattformen

Google Cloud Platform (GCP)

- **Integration von Veeam Backup for Google Cloud Platform:** Registrieren Sie Buckets des Google Cloud Storage (GCS) mit Backups, die durch Veeam Backup for Google Cloud Platform erstellt wurden, als externe Repositories. So können Sie alle Arten von Wiederherstellungen durchführen und Ihre GCP-VM-Backups in lokale Backup-Repositories oder auf Band kopieren, um sich für die Disaster Recovery abzusichern und die 3-2-1-Regel einzuhalten.

Linux

- **Persistenter Data Mover für Linux:** Transportkomponenten werden jetzt dauerhaft bereitgestellt, wenn Sie einen Linux-Server bei Veeam registrieren. Das kommt sowohl der Leistung als auch der Skalierbarkeit zugute, da Data Mover nun nicht mehr jedes Mal zu Beginn einer Aufgabe auf den Server verschoben werden müssen. Die erforderlichen Regeln für integrierte Linux-Firewalls werden automatisch für die Dauer des Backup-Jobs erstellt (iptables, ufw und firewalld werden unterstützt).

HINWEIS: Für Linux-Hosts, die den persistenten Data Mover noch nicht unterstützen, (z. B. Speicher-Appliances mit Veeam Data Mover-Integration), nutzt V11 weiterhin den Data Mover in Laufzeit.

- **Verbesserte Sicherheit des Data Mover:** Werden Einmalanmeldedaten verwendet, wird der persistente Data Mover als eingeschränkter Nutzer ausgeführt. Grundlage ist das Set von Anmeldedaten aus der Bereitstellung. Demzufolge können Hacker potenzielle Schwachstellen der internen Data Mover-API nicht ausnutzen, um das Betriebssystem zu übernehmen.
- **Zertifikatsbasierte Authentifizierung:** Zur Authentifizierung zwischen Backup-Servern und Transportkomponenten während Backup-Aufgaben verwenden wir statt der gespeicherten Linux-Anmeldedaten eine PKI-Technologie (Public Key Infrastructure). Die Schlüsselpaare werden zum Zeitpunkt des Transport-Deployments automatisch generiert.
- **Kryptografie für elliptische Kurve:** Für ein bisher unerreichtes Maß an Sicherheit unterstützt V11 SSH-Schlüsselpaare auf Basis der Elliptic-Curve-Technologie (EC), z. B. Ed25519 oder ECDSA, um SSH-Verbindungen zu Linux-Servern aufzubauen. Wenn das Knacken eines 228-Bit-RSA-Schlüssels weniger Energie erfordert, als zum Aufkochen eines Teelöffels voll Wasser nötig ist, dann erfordert es bei einem 228-Bit-EC-Schlüssel genug Energie, um alles Wasser auf diesem Planeten zum Kochen zu bringen – das ist Sicherheit in der Größenordnung eines 2380-Bit-RSA-Schlüssels!

Microsoft Azure

- **Vollständig integriertes, Azure-basiertes Backup:** Die cloudbasierte Sicherung von Azure-Daten ist jetzt integraler Bestandteil der Veeam Backup & Replication-Konsole. Voraussetzung hierfür ist Veeam Backup for Microsoft Azure v2.
- **Unterstützung für Azure Stack HCI:** Neu hinzugekommen ist Unterstützung für die neue Hyper-Converged Infrastruktur (HCI), bei der es sich im Grunde um eine lokale Hyper-V-Infrastruktur handelt, die als [Azure-Service](#) bereitgestellt wird.
- **Wiederherstellung auf VM der 2. Generation:** Wir bieten jetzt die experimentelle Unterstützung von Direct Restore to Microsoft Azure zur Bereitstellung einer VM der 2. Generation als Ziel. Legen Sie zur Aktivierung dieser Funktionalität den Registry-Wert `AzureEnableGeneration2VMRestore` (DWORD, 1) auf dem Backup-Server an.

Nutanix AHV

- **Veeam Backup for Nutanix AHV 2.1:** Die neue Funktionalität beinhaltet die Option zum Ausschluss von Festplatten bei Backup-Jobs, eine bessere Integration mit Nutanix-Volume-Gruppen für die Wiederherstellung, Verbesserungen der Benutzeroberfläche und einiges mehr. Die vollständige Liste der neuen Features finden Sie in den zugehörigen Release-Hinweisen.

VMware vSphere

- **Sofortwiederherstellung von Festplatten erster Klasse:** Im Rahmen der Festplatten-Sofortwiederherstellung haben Anwender jetzt zwei Optionen: Wiederherstellung aus Backups als Standard-VMDK, die einer bestimmten vSphere-VM anhängt, oder Wiederherstellung als Festplatte erster Klasse, die unabhängig von vSphere-VMs verwaltet und direkt von containerbasierten Anwendungen der nächsten Generation genutzt werden kann.
- **UND für vSphere-Tags:** Sie können bereits mehrere einzelne vSphere-Tags zu einem Job-Umfang zusammenfassen und nun auch eine Kombination aus vSphere-Tags verwenden. In diesem Fall werden nur VMs verarbeitet, die alle ausgewählten Tags aufweisen (klassisches Verhalten des UND-Operators). Dieses Vorgehen erfordert allerdings eine sorgfältigere Überwachung ungesicherter VMs, beispielsweise mit Veeam ONE™, denn das Risiko, dass VMs versehentlich durch das Sicherungsraster rutschen und dann ohne aktuelle Backups sind, ist größer.
- **Zweistufiger Failback:** Damit der Failback-Zeitaufwand und damit die Ausfallzeit bei großen VMs besser einzuschätzen ist, bieten wir jetzt mehr Kontrolle über den Failback-Prozess. Im ersten und langwierigsten Prozessschritt wird die Replikat-VM weiter ausgeführt, während Hashwerte berechnet werden und die Failback-Zielmaschine in den Snapshot-Zustand vor dem Failback wiederhergestellt wird. Danach wird die Replikat-VM in den wechselbereiten Zustand versetzt und der Failback mit minimaler Ausfallzeit für die finale Deltaübertragung durchgeführt. Der Wechsel kann manuell oder automatisch erfolgen, entweder sobald das Replikat dafür bereit ist oder zu einem festgelegten Zeitpunkt während des nächsten Wartungszeitfensters.
- **Linux-Proxy-Transportmodi:** Zu den unterstützten Transportmodi zählen jetzt auch Direct Storage Access (für Block- und NFS-Speicher), Netzwerk (NBD/NBDSSL) und Backups aus Storage-Snapshots (nur für Blockspeicher). Darüber hinaus zeigt der bestehende Hot-Add-Transportmodus deutliche Leistungssteigerungen dank moderner Datenabruftechnologie, die bisher nur von Windows-basierten Proxies genutzt wurde.
- **CBT-Wiederherstellung bei Linux-Proxies:** Die Funktionalitäten für ein schnelles Rollback zu Linux-basierten Backup-Proxies wird jetzt unterstützt, um Wiederherstellungen und Failbacks vollständiger VMs am ursprünglichen Speicherort zu gewährleisten.
- **NBD-Multi-Threading:** Pro VMDK kann die Backup-Engine jetzt mehrere NBD-Verbindungen aufbauen. Dies stärkt die Leistung des Netzwerktransportmodus. Da ein ESXi-Host allerdings nur eine geringe Anzahl von NBD-Verbindungen zulässt, sorgt eine erhöhte Verbindungsanzahl auch für Bedenken hinsichtlich der Zuverlässigkeit. Unser Ressourcenplaner behält zwar die NBD-Aufgaben pro Host im Blick, damit die Grenze nicht überschritten wird, doch für uns war der marginale Leistungsvorteil nicht überzeugend genug, um dieses neue Verhalten gleich für unseren gesamten Kundenstamm freizuschalten, da auch externe NBD-Verbindungen vorliegen können. Sollten Sie die Funktionalität allerdings testen wollen, können Sie dies mit dem vollständigen unterstützen Registry-Wert `VMwareNBDConnectionsPerDisk` (DWORD) auf dem Backup-Server tun. Unsere internen Tests ergaben eine Bestleistung bei zwei NBD-Verbindungen pro Festplatte. In den F&E-Foren von Veeam würden wir gern von Ihren Ergebnissen mit dieser Funktionalität erfahren. Dies wird uns die Entscheidung erleichtern, ob wir sie in zukünftigen Updates von Anfang an aktivieren sollen.

- **Unterstützung für VMware Remote Console:** Die Funktionalität der Benutzeroberfläche, mit der sich eine VM-Konsole öffnen lässt, nutzt jetzt auch die noch sicherere VMware Remote Console. Beim ersten Versuch, eine zugehörige Funktionalität zu nutzen, erhalten Sie die Gelegenheit, die Konsole herunterzuladen und zu installieren.
- **VDDK-Versionsupdate:** VDDK 6.7 wurde auf Version 6.7.3 aktualisiert, wodurch sich unter anderem Probleme mit asynchroner NBD-E/A-Auslastung erledigen sollten.

VMware Cloud Director

- **Cloud Director-Replikation:** Der neue spezielle Replikationsjob-Typ ermöglicht es Service Providern, vApps innerhalb und zwischen Cloud Director-Instanzen (VCD) zu replizieren. Der Replikationsjob verarbeitet vApp-VMs und -Metadaten (z. B. Netzwerk- oder VM-Startreihenfolge), um eine einsatzbereite Replikat-vApp in der Cloud Director-Zielinstanz zu erstellen, die im Fall einer Katastrophe sofort genutzt werden kann.
- **Natives Cloud Director-Plug-in:** Diese neue Funktion ermöglicht es Service Providern, die Benutzeroberfläche des Cloud Director-Mandanten um die Veeam Backup & Replication-Funktionalität zu erweitern, sodass Mandanten ihre eigenen Sicherungen und Wiederherstellungen verwalten können, ohne den Komfort der Cloud Director-Webkonsole zu verlassen. Diese Integration basiert auf dem vorhandenen Cloud Director-Self-Service-Portal für Backups von Veeam.
- **Unterstützung für mehrere Cloud Director-Server:** Das Cloud Director-Self-Service-Portal für Backups unterstützt jetzt Umgebungen, in denen mehrere VCD-Server bei Veeam Backup & Replication registriert sind. So haben Sie bei der Organisationskonfiguration die Wahl, welchen VCD-Server Sie nutzen möchten.
- **Unterstützung für mehrere Konfigurationen:** Das Cloud Director-Self-Service-Portal für Backups unterstützt jetzt die Erstellung mehrerer Self-Service-Konfigurationen pro VCD-Organisation.
- **Flexiblerer Zugriff auf das Cloud Director-Portal:** Mit den Registry-Werten *vCloudPortalBackupAdminRole* (STRING) und *vCloudPortalRestoreOperatorRole* (STRING) auf dem Backup-Server können Sie benutzerdefinierte VCD-Rollen festlegen. Jeder VCD-Benutzer mit der entsprechenden Rolle kann dann für seine Organisation auf das Self-Service-Backup-Portal zugreifen – entweder als Backup-Administrator oder als Wiederherstellungsbenutzer. Bleiben diese Registry-Werte leer, ändert sich das aus früheren Versionen bekannte Verhalten nicht: Nur VCD-Benutzer mit administrativen Berechtigungen in der VCD-Organisation dürfen das Self-Service-Backup-Portal verwenden – für ihre jeweilige Organisation und in der Portalrolle des Backup-Administrators.
- **Unterstützung für Cloud Director 10.2:** Vollständige Unterstützung lokaler Installationen und cloudbasierter Bereitstellungen dank des Cloud Director-Service von VMware.

Integration von Primärspeichersystemen

Allgemein

- **Festplatten-Sofortwiederherstellung aus Storage-Snapshots:** Der Aufwand für Sofortwiederherstellungen verringert sich, wenn Sie nur die nötigen Festplatten sehr großer vSphere-VMs direkt aus speicherbasierten Snapshots wiederherstellen (z. B. nur Festplatten mit Betriebssystemen oder Daten). Sie können Festplatten aus einem Snapshot sofort auf der ausgewählten VM mounten und für andere Zwecke nutzen, beispielsweise für Vergleiche des Festplatteninhalts oder für Massenwiederherstellungen auf Dateiebene mithilfe von Drittanbieter-Tools.
- **Storage-Snapshot-Aufbewahrung auf Basis von Wiederherstellungspunkten:** Die Aufbewahrung von Wiederherstellungspunkten in Storage-Snapshots wird jetzt pro VM verarbeitet. Zuvor galten Storage-Snapshots selbst als Wiederherstellungspunkte, was in Ausnahmefällen eine Reihe von Problemen zur Folge hatte, zum Beispiel fehlgeschlagene Neuversuche, VM-Migrationen zu anderen Volumes usw.

Dell EMC VNX/VNXe/Unity/Unity XT

- **Version des Integrations-Tools:** Dell EMC Navisphere und Unisphere CLI wurden zur Unterstützung von TLS 1.2 auf die neueste Version aktualisiert.

HPE 3PAR/Primera

- **Unterstützung für 3PAR-Remote-Kopien:** Die asynchrone regelmäßige 3PAR/Primera-Replikation wird jetzt in jeder Storage-Snapshot-Integrationsfunktionalität unterstützt. Dazu zählt die Verwaltung der Storage-Snapshot-Replikation, die separate Aufbewahrung von Snapshot-Replikaten und Backups aus Snapshot-Replikaten im sekundären Array, um das primäre Array von Beeinträchtigungen durch Backup-Aktivitäten freizuhalten.
- **Mehrfachprotokoll-Unterstützung für Nimble:** Die Storage-Snapshot-Integrationsfunktionalität lässt jetzt zu, dass in Nimble Storage sowohl FC- als auch iSCSI-Protokolle in demselben Array aktiviert sind.
- **Versionsunterstützung:** 3PAR OS 3.3.1 MU5 wird unterstützt, während die Unterstützung für 3PAR-Betriebssystemversionen vor 3.2.2 und WSAPI vor Version 1.5 eingestellt wurde.

Lenovo

- **Lenovo DM-Unterstützung:** Die integrierte Storage Snapshot-Integration der Lenovo ThinkSystem DM Series wird unterstützt.

NetApp

- **ONTAP 9.8-Unterstützung:** NetApp ONTAP 9.8 wird jetzt für die Storage-Snapshot-Integration unterstützt, mit Ausnahme der Verarbeitung von VMs in FlexGroup-Volumes. Hinweis: Zur Sicherung solcher VMs können Sie weiterhin herkömmliche host- oder agentenbasierte Backups nutzen.

Integration von Sekundärspeichersystemen

ExaGrid

- **Unterstützung für AD-Authentifizierung:** Bei der Registrierung von ExaGrid bei Veeam wird jetzt die Authentifizierung auf Basis von Microsoft Active Directory (AD) unterstützt.
- **SOBR-Platzierungslogik:** Angesichts der von ExaGrid angebotenen globalen Deduplizierung haben wir auf Wunsch von ExaGrid die spezielle Logik für die SOBR-Erweiterungsplanung für deduplizierenden Storage deaktiviert. SOBR legt neue vollständige Backups jetzt bevorzugt auf derselben Erweiterung ab, auf der schon das vorherige vollständige Backup platziert ist. Die bisherige Platzierungslogik können Sie wieder nutzen, indem Sie unter dem Schlüssel „HKLM\SOFTWARE\Veeam\Veeam Backup and Replication“ auf dem Backup-Server den Registry-Wert *ExaGridEnableNewFullToSameExtent* (DWORD, 1) anlegen.
- **Standardeinstellungen der Benutzeroberfläche:** Mit ExaGrid als Ziel-Repository empfehlen wir, im Backup-Job-Assistenten die Komprimierung auf „Optimal“ einzustellen. Außerdem ist die Option „Decompress backup data blocks before storing“ (Backup-Datenblöcke vor dem Speichern dekomprimieren) des Backup-Repository-Assistenten standardmäßig aktiviert, wenn ein Repository auf ExaGrid-Basis registriert wird. Mit dieser neuen Standardeinstellung kann ExaGrid effektiv deduplizieren – unabhängig vom gesicherten Workload.

Dell EMC Data Domain

- **Unterstützung des Data Domain-Betriebssystems:** DD-Betriebssystemversionen 7.1, 7.2 und 7.3 werden unterstützt, alle Versionen vor 6.1 nicht mehr. Führen Sie vor dem Upgrade auf V11 bitte ein DD-Betriebssystem-Upgrade durch.
- **Version des Data Domain Boost-SDK:** Das DD Boost-SDK wurde auf Version 7.0 aktualisiert.

HPE StoreOnce

- **Backup-Copy-Jobs als Quelle:** Backup-Copy-Jobs dienen jetzt auch als Quelle für Catalyst Copy-Jobs. Zuvor wurden nur primäre Backup-Jobs als Quelle akzeptiert.
- **Bandsicherung von Catalyst Copy-Backups:** Backup-auf-Band-Jobs unterstützen jetzt Catalyst Copy-Jobs als Quelle.
- **Leistungstärkere Integritätsprüfung:** Dank Parallelverarbeitung ließ sich die Leistung der Backup-Integritätsprüfung in Catalyst Copy-Jobs mehrfach steigern.
- **Option zur verzögerten Löschung von Backup-Kopien:** Catalyst Copy-Jobs bieten die Möglichkeit, die Löschung von Backup-Kopien aus Sekundärspeicher zu verzögern, was die Aufbewahrungsdauer auf Catalyst Copy-Zielen verlängert. Die Löschung lässt sich jetzt direkt über die Benutzeroberfläche anstatt als Registry-Einstellung steuern. Kompatibel ist diese Funktionalität mit HPE StoreOnce und HPE Cloud Volumes Backup.
- **Unterstützung für Cloud Volumes Backup:** V11 unterstützt Catalyst Copy-Jobs in HPE Cloud Volumes Backup jetzt offiziell.
- **Version des Catalyst-SDK:** Das HPE StoreOnce Catalyst-SDK wurde auf Version 4.2.4 aktualisiert, mit V11-Protokollversion.
- **Taggen von Catalyst-API-Sitzungen:** Veeam-Backup-Jobs von Dateifreigaben versehen Catalyst-API-Aufrufe jetzt mit dem eigenen VeeamNAS-Tag. Anhand dieser Information beabsichtigt der HPE-Support, Veeam-Workloads in Supportvorgängen zu kategorisieren, um eine schnellere Lösung herbeizuführen.

Quantum DXi

- **Unterstützung für Quantum FastClone:** V11 ermöglicht offiziell das schnelle Klonen in Backup-Repositories, die von entsprechend kompatiblen Quantum DXi-Modellen unterstützt werden. Bei Fragen zur Kompatibilität Ihres Speichermodells wenden Sie sich bitte an den Quantum-Support.
- **Leistungsstärkere Wiederherstellung vollständiger VMs:** Für die Wiederherstellung einer vollständigen VM gilt jetzt eine optimierte Wiederherstellungslogik, die bereits bei anderen deduplizierenden Storage-Integrationen Anwendung findet. Der Veeam-Backup-Proxy liest Daten jetzt sequenziell aus Quantum aus und schreibt sie im Zufallsmodus auf die Zielfestplatten, anstatt die Blöcke in genau der Reihenfolge wiederherzustellen, in der sie auf der Festplatte gespeichert sind.

Deduplizierende Storage-Integrationen sind Bestandteil der **Veeam Universal License**. Liegt eine herkömmliche sockelbasierte Lizenz vor, ist eine Edition ab **Enterprise** Voraussetzung.

Bandsicherung

- **Kopie auf Band:** Ausgewählte Bänder lassen sich bequem klonen, so profitieren Sie von: zusätzliche externe Kopien, Wegführen von Daten von verschleißenden Bändern oder Migration von Archiven auf moderne LTO-Laufwerke (die Migration ist sowohl zu früheren als auch zu späteren Generationen möglich). Der Backup-Server aktualisiert den Backup-Katalog mit Verweisen zu den geklonten (Ziel-)Bändern, behält aber gleichzeitig die Verweise zu den Ursprungsbändern (Quellen).
- **Bandverifizierung:** Überprüfen Sie regelmäßig Ihre archivierten Bänder darauf, ob die gespeicherten Daten noch lesbar und konfliktfrei sind. Bänder zu verifizieren kann Compliance-Gründe haben, in jedem Fall aber haben Sie davon beruhigende Gewissheit.
- **Wiederherstellung sämtlicher Bandinhalte:** Enthält eine Mediengruppe ein fehlerhaftes Band, können Sie alle Daten dieser Gruppe bequem retten, indem Sie alle noch lesbaren Dateien zu einem festgelegten Speicherort übertragen.
- **Wartungsmodus:** Damit Ihre Tape-Jobs bestimmte Bandbibliotheken oder Laufwerke vorübergehend nicht nutzen, können Sie beides in den Wartungsmodus versetzen.
- **Laufwerksgrenze pro Job:** Bei Backup-auf-Band-Jobs können Sie die Nutzung der Bandlaufwerke auf Jobebene begrenzen.
- **Erzwungene Bandlöschung:** Bei der Bandlöschung werden jetzt alle unkritischen Fehler ignoriert, z. B. mit der Blockgröße oder mit Headern, da diese bei Bändern, die gelöscht werden sollen, keine Rolle spielen.
- **Clusterspezifische Backups für Storage auf NetApp ONTAP-Basis:** Cluster Aware Backup ist eine Erweiterung des NDMP v4-Protokolls und sorgt dafür, dass der NDMP-Server eine Datenverbindung auf einem Knoten mit angeschlossenem Volume aufbauen kann. Dies optimiert den Datenfluss und verbessert die NDMP-Backup-Leistung.
- **Quellen für Backup-auf-Band-Jobs:** Mit Backup-auf-Band-Jobs lassen sich jetzt Backup-Kopien von Nutanix AHV- und Mac-Backups sowie von cloudbasierten Backups für AWS, Azure und Google verarbeiten. Dadurch können Sie Cloud-Maschinen auf Band archivieren, falls dies so Vorschrift ist.
- **Leistungsstärkere Datei-auf-Band-Jobs:** Dank einer besseren Vorverarbeitungslogik für Datei-auf-Band-Jobs, sind Backups und Wiederherstellungen von Datensätzen mit einer großen Anzahl von gesicherten Dateien und Ordnern bis zu zehnmal schneller erledigt.

- **Sicherungsumfang von Datei-auf-Band-Jobs:** Sie können jetzt die gesamte Datenquelle (Windows Server oder SMB/NFS-Dateiserver) als Quelle in Datei-auf-Band-Jobs angeben. Dadurch werden all ihre Freigaben und Exporte, auch neu hinzugefügte, gesichert. Bedingt durch diese neue Funktion wurde der Datei-auf-Band-Wiederherstellungsassistent dahingehend geändert, dass er nun Wiederherstellungen aus solchen Backups unterstützt. Im Nebeneffekt können Sie jetzt auch Massenwiederherstellungen mehrerer Dateifreigaben in einer einzigen Assistentensitzung konfigurieren.
- **Bessere Berichterstattung:** Bei der Überprüfung von Backups, Wiederherstellungen und Bändern wird jetzt eine CSV-Datei mit allen Dateien erstellt, die im Protokollordner des Jobs nicht verarbeitet werden konnten.
- **Anwenderfreundlichere Wiederherstellungen vom Band:** Die für jeden im Assistenten ausgewählten Wiederherstellungspunkt erforderlichen Bänder werden jetzt automatisch angezeigt. Das heißt, Sie müssen nicht mehr jeden einzelnen ausgewählten Wiederherstellungspunkt aufrufen – klicken Sie einfach auf „Next“ (Weiter) und warten Sie auf die Aufforderung „Insert these tapes“ (Diese Bänder einlegen).
- **Bessere Benutzeroberfläche für das Bandmanagement:** Das Dialogfeld mit Bändeigenschaften umfasst jetzt die Zeitspanne für die Reinigung von Bandmedien und das Dialogfeld mit Geräteeigenschaften umfasst jetzt die Bandbibliothek und die Laufwerkseriennummer. Nach dem erneuten Scannen eines Bands wird der Abschluss der Vorgangs vermeldet. Auf NDMP-Servern kann jetzt das Speicherort-Tag festgelegt werden. Die Kontextmenüs des Tabs für die Bandinfrastruktur wurden übersichtlicher gestaltet. Die Spaltenbreite entspricht von Anfang an dem erwarteten Inhalt.
- **LTO-9-Unterstützung:** Jede native V11-Funktionalität für die Bandunterstützung wurde mit Beispielen von LTO-9-Bandhardware getestet, die uns IBM freundlicherweise zur Verfügung gestellt hat. Wenn Bandsicherung die Zukunft ist, dann ist V11 bereit dafür!

Backup-Agenten

Agentenmanagement

- **Backups aus Storage-Snapshots:** Microsoft Windows Server, deren Volumes in unterstützten Speicher-Arrays gehostet werden, können jetzt mithilfe agentenbasierter Backup-Jobs „managed by server“ (Vom Server verwaltet) auf Basis nativer Storage-Snapshots gesichert werden. Das verlagert die Verarbeitung der Backup-Daten vom gesicherten Server zum dedizierten Backup-Proxy. Durch native Storage-Snapshots entfällt außerdem E/A-Aufwand, der sich ergibt, wenn das System über die Dauer des Backups von Software-VSS-Snapshots aus ausgeführt wird. Indem V11 diese beiden klassischen Probleme agentenbasierter Backups löst, ermöglicht es physischen Servern und Clustern LAN-freie Backups ohne Auswirkungen, wie dies auch bei VMware- und Hyper-V-VM-Backups abseits des Hosts der Fall ist. So können die Anwender auch die am stärksten ausgelasteten 24/7-Workloads sichern, ohne gegen SLAs zu verstoßen. Alle integrierten und Universal Storage API-basierten Speicherintegrationen mit iSCSI- oder FibreChannel-Konnektivität werden unterstützt. Anbieterspezifische Hardware des VSS-Providers ist nicht erforderlich.
- **Schutzgruppe für vorinstallierte Agenten:** Diese Art von Schutzgruppe (SG) erleichtert die Agenteninstallation mithilfe von Drittanbieterlösungen für die Software-Distribution, wenn die Bereitstellung über den Backup-Server wegen sicherheitsbezogenen Beschränkungen und eingeschränkter Netzwerkkonnektivität nicht möglich ist. Der SG-Assistent erstellt ein benutzerdefiniertes Paket für die Agenteninstallation, mit dem sich ein Agent mittels PKI-Authentifizierung per SG-Zertifikat automatisch mit dem Backup-Server verbindet. Der Backup-Server platziert dann einen eingehenden Agent in der Schutzgruppe, die das Installationspaket erstellt hat, und gibt ein neues persönliches Authentifizierungszertifikat aus. An dieser Stelle können Sie den Agent wie gewohnt in Backup-Richtlinien „managed by agent“ (Durch Agent verwaltet) nutzen. Für den Backup-Server besteht kein Zwang, sich über das Netzwerk mit Agenten zu verbinden, da die Agenten geänderte Richtlinieneinstellungen mehrmals am Tag selbstständig vom Backup-Server abrufen.

- **Besserer Export virtueller Festplatten:** Festplatten aus agentenbasierten Backups lassen sich jetzt als feste VHD/VHDX-Festplatten exportieren und in Microsoft Azure-Services mounten (bisher gab es nur die Option, Festplatten in dynamischem Zustand zu exportieren).
- **E-Mail-Benachrichtigung bei ungesicherten Hosts:** Sie können sich jetzt per E-Mail zu Hosts benachrichtigen lassen, die innerhalb einer festgelegten Anzahl von Tagen mindestens einmal nicht durch die agentenverwaltete Backup-Richtlinie gesichert wurden.
- **Entfernen aus Konfiguration:** Jetzt lassen sich Maschinen über das Kontextmenü des Hosts aus Schutzgruppen entfernen.
- **Wiederherstellungsmedien aus Backup-Kopien:** Wiederherstellungsmedien lassen sich jetzt auch aus durch Backup-Copy-Jobs erstellte Backups erstellen.
- **Veeam Agent for Microsoft Windows:** Der agentenbasierte Backup-Job-Assistent bietet jetzt die Möglichkeit, die Einstellung „Backup all volumes except excluded“ (Bis auf die ausgeschlossenen alle Volumes sichern) für den Backup-Modus auf Volume-Ebene zu konfigurieren, OneDrive-Ordner von der Verarbeitung auszuschließen und den neuen Benutzerprofil-Backup-Modus anzuwenden.

Veeam Agents

- **Veeam Agent for Microsoft Windows v5:** Die neue Funktionalität umfasst jetzt Folgendes: Unterstützung für Microsoft Windows 10 Version 20H2, breitere Microsoft .NET Framework-Versionskompatibilität, um einen Neustart nach der .NET-Installation zu vermeiden, die tägliche und GFS-Aufbewahrung für Server, Benutzerprofil-Backups auf Dateiebene, bessere Erkennung von VPN-Verbindungen, FIPS-Compliance und mehr. Die vollständige Liste der neuen Features finden Sie im zugehörigen Dokument mit Neuerungen.
- **Veeam Agent for Linux v5:** Die neue Funktionalität umfasst jetzt Folgendes: Unterstützung für neue Betriebssystemversionen, erweiterte Attributsicherung auf Dateiebene, diverse Verbesserungen an Wiederherstellungsmedien, FIPS-Compliance und mehr. Die vollständige Liste der neuen Features finden Sie im zugehörigen Dokument mit Neuerungen.
- **Veeam Agent for Mac:** Der neue Agent liefert mit Veeam Backup & Replication verwaltete Enduser-Datensicherungen für jedes macOS-Gerät, sodass Sie die Sicherung von Mac-Laptops und -Workstations nahtlos in Ihre allgemeine Datensicherungsstrategie integrieren können. Und im Gegensatz zur integrierten Apple-Software Time Machine können Sie mit Veeam Agent for Mac die 3-2-1-Regel erfüllen, indem Sie zusätzliche lokale und externe Backups mit den vertrauten Veeam-Features und -Funktionen erstellen.

Auf Basis der bewährten Agent-Engine von Veeam Agent for Linux bietet der Mac-Agent Folgendes:

- Sicherung von Anwenderdaten und Inhalten externer USB-Laufwerke
- Integration mit den Konfigurationsprofilen von MDM-Lösungen
- Lokale Benutzeroberfläche für die einfache Self-Service-Wiederherstellung auf Dateiebene durch Enduser

Plug-ins für Unternehmensanwendungen

Allgemein

- **Unterstützung für SOBR Capacity Tier:** Backups und Backup-Kopien aller Plug-ins für Unternehmensanwendungen lassen sich jetzt mit der SOBR-Funktionalität Capacity Tier in Objektspeicher kopieren oder verschieben. Backups auf Imageebene und Wiederherstellungen aus Backups, die in Objektspeicher verschoben wurden, sind vollständig transparent.
- **Leistungsverbesserungen:** In allen Aspekten haben wir die Leistung deutlich steigern können. Dies gelang uns insbesondere dank des neuen Umgangs mit Metadaten mittels backupspezifischen Metadaten-Dateien. Dadurch konnten wir die Skalierbarkeit signifikant verbessern. In der Upgrade-Dokumentation erfahren Sie mehr darüber, wie Sie vorhandene Backups in das neue Metadatenformat überführen können.
- **Sich selbst reparierende Metadaten:** In regelmäßigen Backup-Integritätsprüfungen werden alle Wiederherstellungspunkte in Abständen von sechs Stunden gescannt. Die Prüfung erstellt zudem fehlende Metadaten-Dateien neu, was erforderlich werden kann, wenn ein Backup von außen unterbrochen wird. Den Zeitraum können Sie ändern, indem Sie den Wert `DbPluginMissingMetaRegenerationAttemptIntervalMinutes` (DWORD) auf dem Backup-Server anlegen.
- **FIPS-Compliance:** Sämtliche Plug-ins für Unternehmensanwendungen verwenden jetzt FIPS-konforme Verschlüsselungsmodule.

Veeam Plug-in for Oracle RMAN

- **Unterstützung für Oracle Data Guard:** Backups von Oracle Data Guard-Bereitstellungen werden vollständig unterstützt.
- **Bessere RAC-Kompatibilität:** Oracle RAC-Installationen mit leeren „`etc/oratab`“-Dateien werden jetzt unterstützt.

Veeam Plug-in for Oracle RMAN auf AIX

Dieses neue Plug-in bietet den gleichen Funktionsumfang wie das Solaris-Pendant und wird auf dieselbe Weise installiert und konfiguriert. Unterstützt werden unter anderem die Versionen IBM AIX 6.1, 7.1, 7.2 und Oracle 11, 12, 18, 19 (ppc64-Version).

Veeam Plug-in for SAP HANA

- **Unterstützung für SAP HANA 1.0:** Neben wie bisher SAP HANA 2.0 unterstützt dieses Release jetzt auch SAP HANA Database 1.0 SPS 12 oder neuer (Installationsanleitung siehe KB2997). SAP hat dieses Plug-in offiziell für die HANA-Versionen 1.0 und 2.0 zertifiziert.

Veeam Plug-in for SAP on Oracle

Dieses neue SAP-zertifizierte Plug-in kann in SAP BR*Tools integriert werden, sodass Oracle-Datenbanken direkt in Veeam-Repositories gesichert werden können. Hierbei werden die Backup-Modi „`util_file`“ und „`util_file_online`“ unterstützt. Das Veeam Plug-in for Oracle RMAN und das Veeam Plug-in for SAP on Oracle können zusammen verwendet werden, um Backups im Modus „`rman_util`“ auszuführen. Unterstützt werden unter anderem 64-Bit-Versionen von Folgendem:

- OS: SLES 11,12 und 15; RHEL 6 und 7; Oracle Linux 6 und 7
- Oracle: 11.2 bis 19.1
- BR*Tools: 7.20 Patch 42 oder später

Plug-ins für Unternehmensanwendungen sind Bestandteil der **Veeam Universal License**. Liegt eine herkömmliche sockelbasierte Lizenz vor, ist die **Enterprise Plus Edition** Voraussetzung.

NAS-Backup

Allgemein

- **Root-Sicherungsumfang:** Sie können jetzt die gesamte Datenquelle (SMB/NFS-Dateiserver) als Quelle in Backup-Jobs für Dateifreigaben angeben. Dadurch werden all ihre Freigaben und Exporte, auch neu hinzugefügte, gesichert. Bedingt durch diese neue Funktion wurde der Wiederherstellungsassistent für Dateifreigaben dahingehend geändert, dass er nun Wiederherstellungen aus solchen Backups unterstützt. Im Nebeneffekt können Sie jetzt auch Massenwiederherstellungen mehrerer Dateifreigaben in einer einzigen Assistentensitzung konfigurieren. Außerdem werden erkannte Storage-Snapshot-Ordner automatisch ausgeschlossen, sodass Sie sie nicht mehr eigenhändig zu Ausschlusslisten für Backup-Jobs hinzufügen müssen.

HINWEIS: Mit dem Cmdlet [Convert-VBRNASBackupRootFormat](#) können Sie vorhandene Backups in das Format konvertieren, mit dem sich ein neu erstellter Backup-Job in den Root-Umfang aufnehmen lässt.

- **Bessere Leistung:** Backup-Jobs und Backup-Copy-Jobs für Dateifreigaben sind jetzt um das bis zu Zweifache schneller, weil mehrere Upload-Streams zwischen den quell- und zieleitigen Data Movers eingesetzt werden. Übertragungen in Netzwerken mit hoher Latenz profitieren davon am meisten.
- **Intelligenter Lastausgleich:** Bei mehreren Backup-Proxies erkennen und nutzen Dateifreigaben-Backup-Jobs den am geringsten belasteten Backup-Proxy (so, wie es bei VM-Backup-Jobs bereits üblich ist). Dadurch ist für eine einheitliche Lastverteilung und die Nutzung der gesamten Rechenkapazität gesorgt.
- **Warnungen zu gesperrten Dateien:** Sie bestimmen jetzt, ob Probleme bei der Verarbeitung von Dateien und Dateiattributen als Warnung im Gesamtergebnis des Dateifreigaben-Backup-Jobs verzeichnet werden sollen. Des Weiteren ist der Pfad zur Prüfdatei, die alle gesperrten Dateien auflistet, jetzt im Job-Protokoll hinterlegt.
- **Versionsspezifische Aufbewahrung:** Um die Auslastung des Backup-Repository-Speichers besser zu steuern, haben Sie jetzt die Wahl zwischen der versionsspezifischen Aufbewahrung von Dateien allein im Archiv-Repository (wie von V10 gewohnt) und einer Aufbewahrung, die Backup- und Archiv-Repositories überspannt.
- **Automatische Backup-Zuordnung für Backup-Kopien:** Der Prozess einer Backup-Kopie sucht jetzt bei der ersten Ausführung automatisch nach dem Seeding-Backup. Erkennt er eines, wird er das vorhandene Backup inkrementell fortführen.

Integration von Primärspeichersystemen

- **Integration von NAS-Filern der Enterprise-Klasse:** Mit nativen Dell EMC Isilon-, Lenovo DM- und NetApp FAS-Integrationen können Sie den gesamten Filer als Datenquelle registrieren und Dateifreigaben sichern, ohne für jede einzelne Freigabe die entsprechende Zugriffsberechtigung einzuholen. Das Backup aus solchen Datenquellen erfolgt zudem mittels sofort einsatzbereiten nativen Storage-Snapshots. So lassen sich gesperrte Dateien ohne komplexe Einrichtung und Skripte zur Snapshot-Verwaltung vermeiden.

HINWEIS: Mit dem Cmdlet [Convert-VBRNASBackupStorageFormat](#) können Sie vorhandene Backups in das Format konvertieren, mit dem sich ein neu erstellter Backup-Job in den NAS-Filer-Umfang aufnehmen lässt.

- **Native Integration von Changed File Tracking:** In V11 lassen sich Dateifreigabe-Backup-Jobs mit der Dell EMC Isilon Changelist-API integrieren, um die Speicherlast zu reduzieren und die Leistung inkrementeller Backups zu steigern. Bei dieser Maßnahme stehen gesicherte Dateifreigaben mit einer großen Anzahl an selten geänderten Unterordnern im Mittelpunkt.

Integration von Sekundärspeichersystemen

- **Große Blobs:** Backup-Jobs und Backup-Copy-Jobs für Dateifreigaben gehen jetzt automatisch zu 1-GB-Blobs über, wenn als Ziel Speicher-Appliances für die Deduplizierung ausgewählt sind. Dadurch steigt die Skalierbarkeit bei Speichergeräten, die nur eine begrenzte Anzahl von Dateien pro Appliance (z. B. HPE StoreOnce) unterstützen, um das bis zu 20-Fache, und die Sicherung und Wiederherstellung für den gesamten Deduplizierungsspeicher verbessert sich um ein Mehrfaches.
HINWEIS: Mit dem Cmdlet [Convert-VBRNASBackupStorageFormat](#) können Sie vorhandene Jobs auf große Blobs vorbereiten.
- **Metadaten-Erweiterungen:** Wenn Sie Scale-out Backup Repositories verwenden, die ausschließlich aus langsamem Storage wie Deduplizierungs-Appliances bestehen, können Sie die Sicherung und Wiederherstellung um ein Mehrfaches leistungsstärker machen, indem Sie eine kleine, metadatenspezifische Erweiterung mit schnellem Storage einführen, der nur zum Speichern von Backup-Metadaten dient. Dieses erweiterte Feature lässt sich nur per PowerShell mit dem Cmdlet [Set-VBRRepositoryExtent](#) konfigurieren.

Benutzeroberfläche

Backup-Konsole

- **Kein lokaler Administrator erforderlich:** Benutzer der Backup-Konsole müssen auf dem System, auf dem die Konsole ausgeführt wird, nicht länger ein Konto der Gruppe lokaler Administratoren nutzen. Dies dient der Sicherheit, da nun nicht mehr allen Konsolenbenutzern Administratorrechte verliehen werden müssen. Steht ein Update der Konsole an oder erfordert ein Wiederherstellungsszenario doch lokale Administratorrechte, erhalten Sie die Gelegenheit, die Konsole unter einem administrativen Konto neu zu starten.
- **Verwaiste Backups:** Backups, denen kein Job zugewiesen ist, lassen sich jetzt viel leichter nachverfolgen – dank des neuen Waisenknotens („Orphaned“) unter „Backups“. Bisher landeten solche Backups im Knoten für importierte Backups und waren nicht voneinander zu unterscheiden.
- **Filterbasierte Job-Knoten:** Benutzerdefinierte Ansichten (ein V10-Feature) lassen sich jetzt als persistente Knoten zur Managementstruktur hinzufügen. So gelangen Sie schneller zu den von Ihnen am häufigsten genutzten Ansichten.
- **Informationen zu unveränderlichen Backups:** Im Dialogfeld mit Backup-Eigenschaften finden Sie jetzt eine Spalte mit dem Zeitpunkt, an dem die Unveränderlichkeit eines abgesicherten Repositories ablaufen wird.
- **Zeitstempel zur Aktionsprotokollierung:** Auf allgemeinen Wunsch gibt es jetzt zusätzlich zur Spalte mit der Vorgangsdauer auch eine Spalte mit den Zeitpunkten, zu denen die Vorgänge begonnen haben. Um dies anzuzeigen, klicken Sie auf den Header des Aktionsprotokolls.
- **Integration der Windows-Mitteilungszentrale:** Ab jetzt werden interaktive Benachrichtigungen anstatt als Pop-up im Systeminfobereich in der Windows-Mitteilungszentrale angezeigt, z. B. bei SQL Server-Konfigurationsdatenbanken, die drohen, zu groß zu werden (ein neues V11-Feature), bei Band-Jobs, für die noch ein Band eingelegt werden muss, und Ähnliches.
- **Verwirrende Schaltfläche umbenannt:** Die Schaltfläche „Finish“ (Fertigstellen) im letzten Schritt des Assistenten für die Wiederherstellung auf Datei- bzw. Objektebene heißt jetzt „Browse“ (Durchsuchen), damit deutlich wird, dass der Vorgang mit der Objektauswahl weitergeht. Zuvor hatten Teile des Benutzerstamms gezögert, die Schaltfläche anzuklicken, weil sie annahmen, die Wiederherstellung würde starten, ohne dass das Wiederherzustellende ausgewählt war.
- **Swagger-Konsole:** Sie können die neue interaktive Dokumentation (auf Swagger-Basis) der RESTful API für Backup-Server direkt aus dem Hauptmenü heraus öffnen.

- **Verworfenne Features:** Die Funktionalität „Transform previous backup chains into rollbacks“ (Frühere Backup-Ketten in Rollbacks umwandeln) wurde verworfen, daher enthält die Benutzeroberfläche bei neu erstellten Jobs dieses Kontrollkästchen nicht mehr. Wenn Sie diesen Backup-Modus aufgeben möchten und dabei Hilfe benötigen, schildern Sie Ihren Anwendungsfall bitte in den F&E-Foren von Veeam. Für das nächste große Release 2022 ist geplant, vollständig auf diese Funktion zu verzichten.

Enterprise Manager

- **Lokalisierung der Weboberfläche:** Für Enterprise Manager verwenden wir jetzt das branchenübliche Lokalisierungs-Framework GetText und dank unserer lokalen Mitarbeiter im Pre-Sales-Engineering ist Veeam Backup Enterprise Manager v11 schon in die folgenden Sprachen übersetzt worden: Deutsch, Chinesisch (vereinfacht), Französisch, Italienisch, Japanisch und Spanisch.
- **SSO-Anmeldung:** Die neue Anmelde-Benutzeroberfläche erfordert nicht mehr die Eingabe eines Benutzernamens. Stattdessen wird der Benutzer zur Authentifizierung direkt zum konfigurierten Identity Provider weitergeleitet. Das bedeutet, die Benutzer einer Organisation können sich bei Enterprise Manager und den zugehörigen Portalen ohne Anmeldedaten authentifizieren (z. B. in Umgebungen, in denen ausschließlich Smartcards verwendet werden).
- **SAML-Unterstützung für das Self-Service-Backup-Portal von vSphere:** Das Portal hat auch abseits der eigentlichen Zielgruppe großes Interesse geweckt, insbesondere bei Service Providern. Um dies zu unterstützen, haben wir SAML integriert, sodass Serviceprovider ihren Mandanten Zugriff auf das Portal gewähren können. Dazu müssen sie ihnen Kontingente für externe Benutzer und Gruppen zuweisen. Werden SAML-Konten verwendet, werden nur vSphere-Tags als Delegationsmodus unterstützt.
- **Verbesserte Benutzeroberfläche:** Bei der Wiederherstellung von Microsoft Exchange-Objekten wird der Postfachname neben dem Benutzernamen angezeigt, um Missverständnisse bei identischen oder ähnlich lautenden Personennamen zu vermeiden. Zudem gibt es jetzt bei der Umfangsfestlegung für die Rolle des Wiederherstellungsbenutzers eine Objektsuchfunktion.

Lizenzierung

Allgemein

- **Warum etwas ändern, das funktioniert?** V11 verwendet dasselbe Lizenzdateiformat, das es seit V10 gibt. Da solche Lizenzdateien nicht mehr an eine bestimmte Softwareversion geknüpft sind, können Sie die V10-Lizenzdatei für V11 verwenden, sofern Ihr Wartungsvertrag noch aktiv ist.
- **Automatische Lizenzaktualisierung bei der Einrichtung:** Beim direkten Upgrade aus V9 bietet Ihnen der Einrichtungsassistent die Möglichkeit, die Lizenzdatei für V11 automatisch herunterladen zu lassen. Um diese Möglichkeit zu nutzen, muss die aktuell installierte Lizenz zu Veeam-Servern hochgeladen werden. Falls Ihr Backup-Server nicht mit dem Internet verbunden ist oder falls Sie die aktuelle Lizenz lieber nicht hochladen möchten, können Sie die Lizenzdatei stattdessen aus dem [Kundenportal](#) herunterladen.
- **Automatische Lizenzaktualisierung im Produkt:** Beim Installieren einer Lizenzdatei erhalten Sie jetzt die Möglichkeit, Lizenzerweiterungen automatisch herunterladen zu lassen, sobald Sie den Vertrag verlängern oder ausweiten. Für diese optionale Funktionalität muss der Backup-Server den Veeam-Servern regelmäßig die Lizenzkennung, die Installationskennung und die Workload-Auslastung mitteilen. Wenn Sie Veeam diese Informationen nicht zukommen lassen wollen, aktivieren Sie diese Funktionalität nicht, sondern laden Sie die aktualisierten Lizenzdateien aus dem [Kundenportal](#) herunter und installieren Sie sie selbst.

- **Einfachere Lizenzverlängerung:** Sie können den Prozess für die Lizenzverlängerung jetzt direkt aus dem Dialogfeld mit Lizenzinformationen heraus starten. Per Klick auf die Schaltfläche „Renew“ (Verlängern) gelangen Sie zur Veeam-Website mit dem Anforderungsformular für die Lizenzverlängerung. Darin sind einige Informationen anhand der aktuell installierten Lizenz bereits vorausgefüllt.

Veeam Universal License (VUL)

- **Doppelte NAS-Absicherung:** Wir haben die Rabatte geprüft, die unser Vertrieb für die VUL-basierte NAS-Sicherung im Schnitt gewährt hat, und entschieden, die von einer Lizenz abgedeckte NAS-Datenmenge zu verdoppeln: von 250 auf 500 GB. Bestandteil dieser Änderung ist auch, dass Sie nun die ersten 500 GB Daten aus jeder Dateiquelle gebührenfrei sichern können (zum Vergleich: bei V10a waren es 250 GB). Die neue Kapazitätserweiterung für NAS-Backups erfordert ein Upgrade auf V11.
- **Entfernung der Starter Edition:** Diese Edition wurde im Herbst 2020 eingestellt, daher akzeptiert V11 entsprechende Lizenzdateien nicht. Bitte laden Sie eine Ersatz-Lizenzdatei für Veeam Backup Essentials™ aus dem [Kundenportal](#) herunter. Für die verbleibende Vertragslaufzeit gilt sie als kostenloses Upgrade.

Sockelbasierte Lizenzen

- **Entfernung von Produkteditionen:** Wie auch VUL werden sockelbasierte Lizenzen Nettoneukunden jetzt als einzelne, vollständig ausgestattete Edition angeboten, die bisher unter dem Namen Enterprise *Plus* lief. Bestandskunden mit sockelbasierten Lizenzen können ihre jeweilige Lizenzedition weiterhin nutzen, verlängern und erweitern. Wenn Sie Interesse an einer Funktionalität haben, die von Ihrer Produktedition nicht abgedeckt ist, wenden Sie sich an Ihren Veeam Ansprechpartner im Vertrieb. Dieser berät Sie gern zu Angeboten für das Upgrade Ihrer Sockellizenz-Edition oder die Migration zu VUL.

Community Edition

- **Jetzt mit noch mehr Features:** Die überarbeitete *Community Edition* von V11 umfasst alle neuen V11-Features und -Verbesserungen mit Ausnahme einiger weniger, für die besondere Lizenzanforderungen gelten. Benutzer dieser Edition profitieren auch von der neuen Kapazitätserweiterung für NAS-Backups: Mit der kostenlosen Lizenz lassen sich mehr als 5 TB NAS-Daten sichern, wobei die ersten 500 GB Daten pro Dateifreigabe nicht mitzählen.

Wenn möglich, führen Sie ein Upgrade auf [Veeam Backup Essentials](#) durch, und unterstützen Sie so die *Community Edition*. *Für weniger Geld als ein Besuch in einem gehobenen Restaurant kostet erhalten Sie Zugang zu ALLEN Features und Kundensupport rund um die Uhr. Ein solcher Wechsel hilft uns, hochleistungsfähige Datensicherung weiterhin denjenigen kostenlos anzubieten, die sie sich wahrlich nicht leisten können.*



Mehr auf
veeam.com/de



Kostenlose Testversion herunterladen
vee.am/backupde