Veeam Data Platform

Die ersten 100 Tage

Ein praktischer Onboarding-Guide für IT-Administratoren

Inhalt

PHASE 1 • Tag 1—14	**7**
Meilenstein 1: Dimensionierung und Planung	7
Meilenstein 2: Bereitstellung der Veeam Software Appliance und Infrastruktur	10
Meilenstein 3: Erste Backup-Jobs	11
Meilenstein 4: Anwendungsspezifische Verarbeitung	12
PHASE 2 • Tag 15—45	**12**
Meilenstein 5: Sicherungskopie und Vault	13
Meilenstein 6: Monitoring, Alarmierung und Orchestrator-Einrichtung	14
Meilenstein 7: Deckungslücken schließen	15
Meilenstein 8: Ransomware-Bereitschaft	15
PHASE 3 • Tag 46—75	**15**
Meilenstein 9: Leistungsoptimierung und Orchestrierungspläne	17
Meilenstein 10: Wiederherstellungstests	18
PHASE 4 • Tag 76—100	**18**
Meilenstein 11: Reporting und Dokumentation	19
Meilenstein 12: regelmäßige Systemhygiene	20
Schlüsselkomponenten: Veeam Data Platform	**23**
Nützliche Links	**25**

1. Executive Summary

Veeam Data Platform ist die Grundlage Ihrer Organisation für die Resilienz gegen Ransomware und die betriebliche Kontinuität. Diese Anleitung soll IT-Teams dabei unterstützen, ihre Umgebung auf strukturierte Weise zu operationalisieren und weiterzuentwickeln. Wir sprechen hier zwar von den „ersten 100 Tagen", dies ist jedoch nur eine Metapher für einen Zeitrahmen. Jede Organisation ist unterschiedlich und kann in unterschiedlichem Tempo Fortschritte machen, aber das Ziel bleibt dasselbe: Vom anfänglichen Setup zu einem sichereren, resilienteren und besser wiederherstellbaren Zustand überzugehen. Es ist nach praktischen Meilensteinen und empfohlenen Ergebnissen strukturiert und nicht nach strengen Implementierungsanforderungen, sodass Sie sich auf die Schritte konzentrieren können, die für Ihre Umgebung und Edition am relevantesten sind.

2. Für wen gilt diese Anleitung?

Diese Anleitung richtet sich an **IT-Administratoren**, die die Veeam Data Platform implementieren, konfigurieren und operationalisieren. Es wird vorausgesetzt, dass Sie mit virtualisierter Infrastruktur (z. B. VMware vSphere, Microsoft Hyper-V oder einem anderen von Veeam Backup & Replication unterstützten Hypervisor) und grundlegender Windows Server-Administration vertraut sind. Es sind keine Linux-Kenntnisse erforderlich.

Es dient außerdem als gemeinsame Referenz für **IT-Manager**, die Umfang und Zeitpläne verfolgen, für Sicherheits- und Compliance-Stakeholder, die den Härtungsstatus validieren, sowie für Führungs- oder Beschaffungsteams, indem definiert wird, wie Erfolg am Tag 100 aussieht.

3. Was Sie bis Tag 100 erreichen werden

An Tag 100 verfügen Sie über eine stabile, gehärtete und nachweislich wiederherstellbare Umgebung, die das Ausfallrisiko reduziert und eine schnelle, zuverlässige Wiederherstellung ermöglicht — egal was passiert.

Jeder Kunde sollte bestätigen können, dass die folgenden Kontrollpunkte erfüllt sind:

- **Bereitgestellt:** Veeam Backup & Replication läuft, ist verbunden und passend dimensioniert, sodass die Backup-Fenster eingehalten werden.
- **Geschützt:** Prioritäts-Workloads werden nach einem festgelegten Zeitplan erfolgreich gesichert.
- **Abgehärtet:** Immutabilität ist lokal und/oder extern vorhanden, um gegen Ransomware zu schützen.
- **Verifizierbar wiederherstellbar:** Die Wiederherstellungstests sind abgeschlossen, dokumentiert und den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt (RTO und RPO) zugeordnet.
- **Operationalisiert:** Monitoring, Warnmeldungen, Reporting und Wiederherstellungs-Runbooks sind implementiert und Verantwortlichen zugewiesen.

4. Roadmap auf einen Blick

Diese Anleitung ist in vier aufeinander aufbauende Phasen gegliedert, die jeweils auf die Ergebnisse von Tag 100 hinführen:

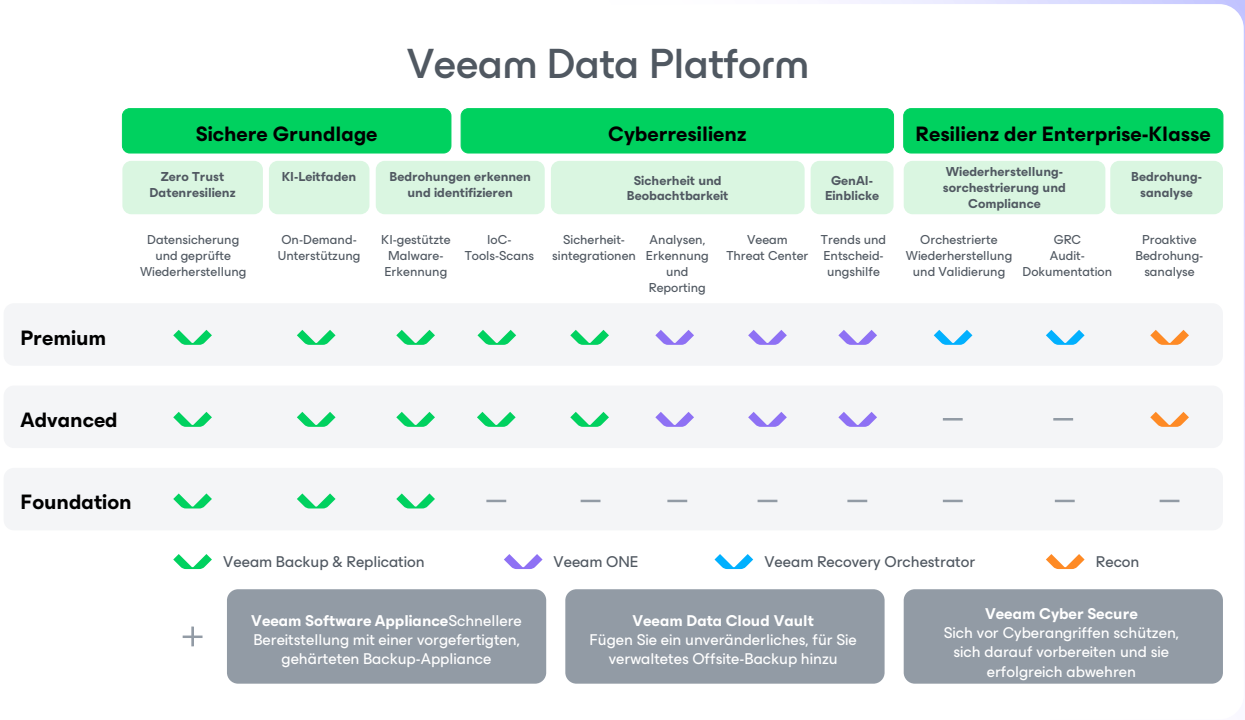
Phase	Name	Zeitrahmen	Fokus
PHASE 1	Grundlage	Tag 1—14	Ermitteln Sie die Größe der Umgebung, implementieren Sie die Veeam Software Appliance (und die Veeam Infrastructure Appliance, falls zutreffend), führen Sie die ersten Backup-Jobs aus und bereiten Sie den Veeam Recovery Orchestrator vor.
PHASE 2	Optimieren	Tag 15—45	anwendungsspezifische Verarbeitung, Backup-Copy-Job, Veeam Data Cloud Vault Offsite-Tier und Einrichtung des Veeam Recovery Orchestrator (Premium).
PHASE 3	Daten und stabiler Geschäftsbetrieb	Tag 46—75	Schließen von Schutzlücken, Aktivieren von Recon, Ransomware-Resilienz, Tuning und Erstellen von Orchestrierungsplänen (Premium).
PHASE 4	Wertnachweis	Tag 76—100	Orchestrierte Wiederherstellungstests, Reporting, Dokumentationsarchitektur und fortlaufende Hygiene.

Verwenden dieser Anleitung

- Folgen Sie den Meilensteinen der Reihe nach. Wenn Sie insbesondere zu früh mit der Konfiguration des Scale-out Backup Repository™ (SOBR) oder Vault beginnen, bevor Ihre lokalen Repositorys und Jobs stabil sind, entstehen Lücken, die sich typischerweise erst bei einer echten Wiederherstellung bemerkbar machen.
- Der Zeitplan ist flexibel. Tage dienen als Orientierung, sind aber keine verbindlichen Fristen. Kleinere Umgebungen können Phase 1 innerhalb einer Woche abschließen. Komplexere Umgebungen benötigen in späteren Phasen mehr Zeit.
- Nutzen Sie die Entscheidungspunkte. Wenn Architekturentscheidungen anstehen (z. B. Bereitstellungspfad oder Repository-Strategie), halten Sie inne, stimmen Sie sich mit den Stakeholdern ab und dokumentieren Sie Ihre Entscheidung, bevor Sie fortfahren.
- Überspringen Sie, was nicht zutrifft, aber notieren Sie, warum. Wenn Ihre Edition Veeam ONE oder Veeam Recovery Orchestrator nicht umfasst, werden diese Meilensteine deutlich gekennzeichnet. Ebenso sind die Schritte für Veeam Software Appliance und Veeam Vault ebenfalls optional und nur dann relevant, wenn diese Module Teil Ihrer Bereitstellung sind.

Veeam Data Platform: Überblick

Bevor wir uns mit der Bereitstellung und deren Umsetzung beschäftigen, verschaffen wir uns einen kurzen Überblick über die Bestandteile Ihrer Veeam Data Platform. Veeam Data Platform ist in drei Editionen verfügbar, die jeweils auf der letzten aufbauen:



Siehe den Anhang für Beschreibungen aller Komponenten: „Anhang: Kurzreferenz. Kernkomponenten“.

Bitte bestätigen Sie Ihre Edition.

Bestätigen Sie vor dem Fortfahren Ihre Edition und machen Sie eine vollständige Bestandsaufnahme der enthaltenen Funktionen. Im Bereich des Datenschutzes sind ungenutzte Funktionalitäten nicht nur verschwendeter Wert — sie sind Lücken, die darauf warten, aufgedeckt zu werden.

Zusätzlich sind die folgenden Module in allen Editionen verfügbar:

- **Veeam Software Appliance:** Eine pre-hardened, Windows-freie Bereitstellungsplattform, die die Einrichtung der Infrastruktur vereinfacht und die Sicherheit stärkt. Es sind keine Linux-Kenntnisse erforderlich.
- **Veeam Vault:** Unveränderbarer, externer Backup-Speicher als Service zum Schutz Ihrer Daten vor Ransomware und versehentliche Löschung.
- **Veeam Agenten:** Veeam Agenten sind Software-Agenten, die Backups auf Imageebene und Wiederherstellung auf physischen Servern, Endpunkten und nicht unterstützten Plattformen für virtuelle Maschinen (VM) ermöglichen und zentral über die Veeam Backup & Replication-Konsole verwaltet werden.

Der Weg zur Resilienz beginnt hier.

In den nächsten 100 Tagen gehen Sie von der Bereitstellung Schritt für Schritt zu einer vollständig gehärteten, verifizierbar wiederherstellbaren Umgebung über — ganz ohne Rätselraten.

PHASE 1 **Grundlage** **Tag 1—14**	**PHASE 2** **Optimieren** **Tag 15—45**	**PHASE 3** **Datenresilienz und stabiler Geschäftsbetrieb** **Tag 46—75**	**PHASE 4** **Wertnachweis** **Tag 76—100**
M1: Dimensionierung und Planung	M4: Anwendungsorientierte Verarbeitung	M7: Abdeckungs-lücken schließen	M10: Wiederherstellungstests
M2: Bereitstellung der Veeam Software Appliance und Infrastruktur	M5: Sicherungskopie, SOBR und Vault	M8: Ransomware-Bereitschaft	M11: Reporting und Dokumentation
M3: Erste Backup-Jobs	M6: Monitoring, Alarmierung und Orchestrator-Einrichtung	M9: Leistungsoptimierung und Orchestrierungspläne	M12: laufende Systemhygiene

PHASE 1 • Tag 1—14

Grundlage

Ziel: Dimensionierung der Infrastruktur, Bereitstellung und Schutz der ersten Workloads.

Meilenstein 1: Dimensionierung und Planung

Bevor Sie irgendetwas bereitstellen, nehmen Sie sich Zeit für die Dimensionierung. Eine unterdimensionierte Infrastruktur ist die häufigste Ursache für langsame Backup-Fenster und verpasste RPOs in den ersten 100 Tagen.

Workload-Inventar

- Dokumentieren Sie die Gesamtzahl Ihrer VMs und Workloads, die Kapazitäten (bereitgestellt vs. genutzt) und die geschätzte tägliche Änderungsrate.
- Identifizieren Sie Ihre kritischsten Workloads, da diese Ihre RPO- und RTO-Ziele beeinflussen.
- Berücksichtigen Sie alle physischen Workloads (z. B. Windows/ Linux-Server), für die Veeam Agents erforderlich sind.

Dimensionierung der Veeam Software Appliance

- Die Veeam Software Appliance wird mit vorinstalliertem Veeam Backup & Replication ausgeliefert; Ihre primäre Dimensionierungsentscheidung betrifft den Host, auf dem sie läuft.
- Mindestanforderungen für KMU: 8 vCPU / 16 GB RAM (empfohlen sind 500 MB RAM für jeden gleichzeitigen Job).
- Verwenden Sie den Veeam Sizing Calculator (calculator.veeam.com), um die Ressourcenanforderungen für Ihre Workload-Anzahl und Ihre Kapazitäten zu validieren.
- Wählen Sie Ihr Bereitstellungsformat: ein OVA für VMware vSphere oder ein ISO-Image für physische Server und andere Hypervisoren. Linux-Erfahrung ist so oder so nicht erforderlich.

Speicherarchitektur: Wählen Sie Ihren Weg

Die Wahl Ihrer Speicherarchitektur in diesem Stadium bestimmt den Verlauf der Phasen 1 und 2. Es gibt drei empfohlene Pfade für KMU:

Pfad A: Veeam Software Appliance + Veeam Infrastruktur Appliance als Veeam abgesichertes Repository + Vault: Dies ist die empfohlene Standardlösung. Dieser Pfad bietet ein lokales unveränderbares Repository, das keine Linux-Kenntnisse erfordert, sowie off-site und logisch durch ein Air-Gap getrennte unveränderbare Kopien über Vault.

Pfad A: Warum sollte man ein Veeam abgesichertes Repository verwenden, das über die Veeam Infrastruktur Appliance bereitgestellt wird?

Ein Veeam abgesichertes Repository bietet unveränderbare lokale Backups. Das bedeutet, dass Ransomware die Backups während der Aufbewahrungsfrist weder verschlüsseln noch löschen kann.

Traditionell erfordert ein unveränderbares Linux-Repository einen dedizierten Linux-Server und eine manuelle Härtung des OS. Veeam Infrastructure Appliance beseitigt dieses Hindernis vollständig. Sie wird pre-hardened ausgeliefert, über eine OVA oder ISO bereitgestellt und erfordert keine Linux-Kenntnisse für Einrichtung oder Wartung.

Veeam Infrastruktur Appliance ist eine Single-Role-Appliance. Jede Instanz läuft entweder als Veeam abgesichertes Repository oder als Backup-Proxy. Für KMUs ohne dedizierten Linux-Administrator oder bestehenden unveränderbaren Speicher empfiehlt sich ein durch die Veeam Infrastruktur Appliance bereitgestelltes Veeam abgesichertes Repository als empfohlener Weg zur lokalen Unveränderbarkeit.

Für maximalen Schutz sollten Sie die Veeam Infrastructure Appliance auf physischer Hardware installieren. Wenn Sie die Veeam Infrastructure Appliance als virtuelle Appliance ausführen, bleibt die Angriffsfläche des Hypervisors erhalten. Dateisystembasierte Unveränderbarkeit schützt Backup-Dateien vor Angriffen innerhalb des OS, aber ein Hypervisor-Administrator kann dennoch VMs unter den unveränderbaren Dateien löschen.

Pfad B: Veeam Software Appliance + Veeam Data Cloud Vault: Veeam Backup & Replication schreibt Backups direkt in das lokale Repository auf der Veeam Software Appliance und verwaltet eine Kopie extern in Veeam Vault. Dies ist ideal für Micro-KMUs, Zweigstellen oder Kunden, die den lokalen Speicherverwaltungsaufwand minimieren möchten und zusätzlich über Vault unveränderbare Kopien extern sowie logisch durch ein Air-Gap getrennte Kopien erhalten. Denken Sie daran, dass die Veeam Software Appliance, wenn sie in einer virtuellen Infrastruktur eingesetzt wird, kein adäquater Ersatz für die Unveränderbarkeit vor Ort ist.

Pfad B: Warum Veeam Software Appliance + Vault?

Pfad B hält die Speicherverwaltung minimal. Veeam Backup & Replication speichert Backups in einem lokalen Repository auf der Veeam Software Appliance selbst, anschließend repliziert ein Backup-Copy-Job diese extern ins Vault.

Der lokale Speicher der Veeam Software Appliance ist standardmäßig unveränderbar, sodass Pfad B weiterhin Schutz vor Ransomware lokal bietet. Es handelt sich im Produktsinn nicht um ein formales Veeam abgesichertes Repository, daher bleibt Pfad A die stabilste Wahl, wenn Sie Hardware für die Veeam Infrastruktur-Appliance bereitstellen können. Pfad B ist jedoch die richtige Entscheidung, wenn Sie das nicht können. Wie bei Pfad A kann die als virtuelle Appliance ausgeführte Veeam Software Appliance weiterhin auf der Hypervisor-Ebene gelöscht werden. Daher sollte sie, wenn möglich, auf physischer Hardware bereitgestellt werden.

Pfad B überspringt den Schritt der Veeam Infrastruktur Appliance vollständig. Wenn Sie sich für diesen Weg entscheiden, wechseln Sie von Meilenstein 2 (Bereitstellung der Veeam Software Appliance) direkt zu Meilenstein 5 (Backup-Copy-Job zum Vault).

Pfad C: Veeam Software Appliance + bestehendes NAS/Windows-Repository + Vault oder alternativer Drittanbieter externer Speicher: Dieser Pfad nutzt die bestehende Speicherinfrastruktur und ist lokal weniger gehärtet, wenn keine zusätzliche Konfiguration vorgenommen wird. Dies ist nützlich, wenn Kunden bestehende Veeam Cloud & Service Provider (VCSP)-Partner für externen Speicher oder alternative externe Speicher nutzen möchten, die bereits verfügbar sind.

Ganz gleich, welchen Weg Sie einschlagen:

- Ziehen Sie in Erwägung, den Backup-Traffic auf ein dediziertes VLAN oder eine NIC zu isolieren, um Backup-Daten von Ihrem Production-Netzwerk fernzuhalten.
- Überprüfen Sie Ihre Socket/Workload-Lizenzierung vor der Bereitstellung.

Meilenstein 2: Bereitstellung der Veeam Software Appliance und Infrastruktur

Veeam Software Appliance bereitstellen

- Laden Sie die Veeam Software Appliance OVA (für VMware vSphere) oder ISO (für physische Server oder VMs auf anderen unterstützten Hypervisoren) vom Veeam-Kundenportal (my.veeam.com) herunter.
- Für OVA: Importieren Sie die OVA in VMware vSphere und starten Sie sie. Nach dem ersten Start ist Veeam Backup & Replication über die Verwaltungsoberfläche zugänglich.
- Für ISO: Starten Sie den Zielserver (z.B. einen physischen Server oder eine VM auf einem anderen unterstützten Hypervisor) von der ISO und folgen Sie der Anleitung. Veeam Backup & Replication wird automatisch installiert.
- Schließen Sie den Assistenten für die Erstkonfiguration der Veeam Software Appliance ab und legen Sie den Hostnamen, die Netzwerkeinstellungen und die Administratoranmeldedaten fest.

Verbinden Sie die Infrastruktur mit Veeam Backup & Replication.

- Fügen Sie Ihre Virtualisierungsplattform zum Veeam Backup & Replication-Inventar hinzu (Backup-Infrastruktur > Managed Server).
- Fügen Sie mindestens einen Backup-Proxy hinzu. In kleineren Umgebungen kann die Veeam Software Appliance als initialer Proxy dienen.
- Konfigurieren Sie den Hot-Add-Übertragungsmodus für VMware Umgebung. Die Proxy-VM hängt die Quellfestplatten über SCSI ein und liest sie direkt aus, wodurch der langsamere NBD-Pfad über das ESXi-Verwaltungsnetzwerk vermieden wird.

Stellen Sie die Veeam Infrastruktur Appliance bereit (Pfad A)

- Laden Sie die Veeam Infrastructure Appliance OVA oder ISO vom Veeam Kundenportal herunter.
- Verwenden Sie für die Bereitstellung denselben OVA/ISO-Prozess wie für die Veeam Software Appliance. Wählen Sie abgesichertes Repository oder Backup-Proxy als Zielrolle im Configuration Wizard aus.
- Nach der Bereitstellung fügen Sie die Veeam Infrastructure Appliance als verwalteten Server zu Veeam Backup & Replication hinzu und richten sie anschließend als Backup-Repository oder Proxy ein.
- Für die Rolle des abgesicherten Repositorys fügen Sie das Repository in Veeam Backup & Replication („Backup-Infrastruktur“ > „Backup-Repositorys“) hinzu und legen Sie den Immutabilitäts-Aufbewahrungszeitraum fest.

Was die Veeam Software Appliance für Sie übernimmt

Veeam Backup & Replication ist vorinstalliert und bereit für die Konfiguration. Es ist keine manuelle Betriebssystemeinrichtung, Softwareinstallation oder Patch-Anwendung vor der Bereitstellung erforderlich.

Die Veeam Software Appliance wird pre-hardened ausgeliefert, unnötige Services sind deaktiviert, das OS ist abgesichert und Sicherheit Best Practices werden standardmäßig angewendet.

Stellen Sie die Appliance als OVA auf VMware vSphere bereit, booten Sie das ISO-Image auf einem physischen Server oder starten Sie sie innerhalb einer VM unter jedem anderen von Veeam unterstützten Hypervisor. Es ist keine Linux-Erfahrung erforderlich.

- Wenn Sie Pfad B oder Pfad C verwenden, überspringen Sie diesen Abschnitt, da keine Veeam Infrastruktur Appliance erforderlich ist.

Veeam ONE installieren

- Veeam ONE ist ein separates Installationsprogramm für Windows. Veeam ONE wird derzeit nicht als Bestandteil des Appliance-Modells bereitgestellt.
- Installieren Sie Veeam ONE auf einer Windows Server-VM oder einem physischen Host (siehe Mindestanforderungen im Veeam ONE Leitfaden für die Implementierung).
- Verbinden Sie Veeam ONE mit Veeam Backup & Replication und Ihrem vCenter-/Hyper-V-Host im Setup-Assistenten.
- Konfigurieren Sie die SMTP/E-Mail-Benachrichtigungseinstellungen sofort nach der Installation. Warnmeldungen sollen ab dem ersten Tag aktiv sein.

Meilenstein 3: Erste Backup-Jobs

- Erstellen Sie Ihren ersten Backup-Job für Ihren primären Hypervisor. Wählen Sie das Veeam abgesichertes Repository (Pfad A), das lokale Repository auf der Veeam Software Appliance (Pfad B) oder Ihr bestehendes NAS/Windows-Repository (Pfad C) aus.
- Legen Sie zunächst eine sinnvolle Aufbewahrungsrichtlinie fest: 14 tägliche Wiederherstellungspunkte, 4 wöchentliche, 3 monatliche (GFS).
- Planen Sie den Auftrag so, dass er außerhalb der Stoßzeiten ausgeführt wird, und stellen Sie sicher, dass er sich nicht mit anderen Wartungsfenstern überschneidet.
- Führen Sie den Job bei der ersten Ausführung manuell aus und überwachen Sie ihn bis zum Abschluss.
- Vergewissern Sie sich, dass der Job ohne Warnungen oder Fehler abgeschlossen wurde, bevor Sie mit Phase 2 fortfahren.

Erster Wiederherstellungstest — nicht überspringen!

Bevor Sie zu Phase 2 übergehen, führen Sie eine Instant VM Recovery für eine nicht kritische VM durch, um die Wiederherstellbarkeit zu bestätigen.

Sie sind erst dann geschützt, wenn Sie sichergestellt haben, dass Sie wiederherstellen können. Dies dauert nur wenige Minuten und kann tagelange Probleme verhindern.

Was die Veeam Infrastruktur Appliance für Sie erledigt

Wie die Veeam Software Appliance wird auch die Veeam Infrastructure Appliance pre-hardened und für die ihr zugewiesene Rolle vorkonfiguriert geliefert. Nach der Bereitstellung ist keine Linux-Verwaltung erforderlich.

Eine einzelne Veeam Infrastruktur-Appliance übernimmt eine Rolle: entweder Veeam abgesichertes Repository oder Backup-Proxy. Wenn Sie beides benötigen, stellen Sie zwei Appliances bereit.

Dies hat die gleichen Bereitstellungsformate wie die Veeam Software Appliance: OVA für VMware vSphere oder ISO für physische Server und andere unterstützte Hypervisoren.

PHASE 2 • Tag 15—45

Optimieren

Ziel: Konsistenter Schutz, externe Kopie und Transparenz in der gesamten Umgebung.

Meilenstein 4: Anwendungsspezifische Verarbeitung

anwendungsspezifische Verarbeitung stellt sicher, dass ausfallsichere Backups auch anwendungskonsistent werden. Dies ist entscheidend für transaktionale Workloads wie SQL Server, Oracle, Exchange, Active Directory und andere relevante Workloads.

- Aktivieren Sie die Gastprozessverarbeitung bei Backup-Jobs, die Windows- oder Linux-Anwendungsserver abdecken.
- Konfigurieren Sie anwendungsspezifische Verarbeitung für SQL Server, Oracle, Exchange, Active Directory-Domänencontroller und andere relevante Workloads.
- Legen Sie eine Richtlinie zur Kürzung von Transaktionsprotokollen fest, sofern relevant und für Ihre Wiederherstellungsanforderungen angemessen.
- Stellen Sie nach dem ersten anwendungsspezifischen Backup-Job sicher, dass die Wiederherstellungspunkte in Veeam Backup & Replication. als anwendungskonsistent markiert sind.
- Testen Sie eine Item-Level-Wiederherstellung einer SQL-Datenbank (oder anderer unterstützter Workloads) mit Veeam Explorer for SQL Server, um die End-to-End-Wiederherstellung der Anwendung zu überprüfen.

Meilenstein 5: Sicherungskopie und Vault

Dieser Meilenstein vervollständigt Ihre 3-2-1-Strategie: Eine lokale Kopie auf Ihrem primären Repository, plus eine unveränderbare Kopie extern. Dies ist der architektonische Eckpfeiler Ihrer Backup-Umgebung.

Vault verbinden

- Fügen Sie Vault als Objektspeicher-Repository in Veeam Backup & Replication (Backup-Infrastruktur > Object Storage Repositorys) hinzu.
- Authentifizieren Sie sich mit Ihren von Veeam bereitgestellten Anmeldedaten und wählen Sie Ihre Region aus.
- Bestätigen Sie, dass die Unveränderbarkeit aktiviert ist.

Backup-Copy-Jobs

- Konfigurieren Sie Backup-Copy-Jobs mit einer GFS-Aufbewahrungsrichtlinie, um längerfristige Wiederherstellungspunkte an einem externen Standort zu speichern.
- Vergewissern Sie sich, dass die externen Kopieraufträge erfolgreich abgeschlossen wurden und Vault-Objekte in Veeam Backup & Replication Unveränderbarkeitskennzeichen aufweisen.
- Führen Sie eine Testwiederherstellung aus Vault durch, um sicherzustellen, dass die externe Kopie lesbar ist, bevor Sie Phase 2 für abgeschlossen erklären.

Pfad C: Optionen für Offsite-Ziele

Pfad A und B nutzen Vault als Ziel für die externe Kopie. Pfad C kann Vault oder eine alternative VCSP oder ein externes Repository eines Drittanbieters verwenden, falls Sie bereits eines eingerichtet haben. Unveränderbarkeit wird standardmäßig für alle im Vault gespeicherten Backup-Daten erzwungen. Wenn Sie ein Vault-externes Repository als Ziel verwenden, vergewissern Sie sich, dass für dieses Repository Unveränderbarkeit oder Objektsperre konfiguriert ist.

Meilenstein 6: Monitoring, Alarmierung und Orchestrator-Einrichtung

- Konfigurieren Sie die Empfänger von Benachrichtigungen in Veeam ONE: E-Mail-Benachrichtigungen für Job-Ausfälle und verpasste Service Level Agreements (SLAs).
- Definieren Sie die Geschäftszeiten in Veeam ONE, um die SLA-Berechnungen mit Ihrem Betriebsplan abzustimmen.
- Überprüfen Sie die Standard-Alarmschwellenwerte: Deaktivieren Sie Benachrichtigungen, die für Ihre Umgebung irrelevant sind, oder passen Sie sie an, um Alarmmüdigkeit zu vermeiden.
- Führen Sie Ihre ersten Veeam ONE Reports aus: Protected VMs Report und Job Session Report.
- Überprüfen Sie den Report über ungeschützte VMs und schließen Sie alle festgestellten Lücken, bevor Sie zu Phase 3 übergehen.

Installieren Sie Veeam Recovery Orchestrator (nur in der Premium Edition)

Überspringen Sie diesen Abschnitt, wenn Ihre Edition Foundation oder Advanced ist. Veeam Recovery Orchestrator ist nur in Veeam Data Platform Premium enthalten.

- Veeam Recovery Orchestrator ist ein separater Windows-basierter Installer. Es kann zusammen mit Veeam ONE auf demselben Windows-Host betrieben werden oder auf einem separaten Host laufen.
- Installieren Sie Veeam Recovery Orchestrator auf einer Windows Server-VM oder einem physischen Host. Bitte beachten Sie die Mindestanforderungen im Leitfaden für die Implementierung für Veeam Recovery Orchestrator.
- Verbinden Sie im Einrichtungsassistenten den Veeam Recovery Orchestrator mit Ihrer Veeam Backup & Replication-Instanz, damit er eine Inventarisierung Ihrer bestehenden Backup-Ketten durchführen kann.
- Verbinden Sie Veeam Recovery Orchestrator mit Ihrer vSphere-, Hyper-V- oder Microsoft Azure-Umgebung, damit Ihre geplante Ausführung VMs starten und Netzwerke korrekt zuweisen kann.
- Optional können Sie Veeam Recovery Orchestrator mit Veeam ONE verbinden, um detailliertere Überwachungsdaten und eine DataLab-basierte Überprüfung zu erhalten.
- Aktivieren Sie Veeam Recovery Orchestrator mit Ihrer Veeam Data Platform Premium-Lizenz.
- Konfigurieren Sie SMTP/E-Mail, damit geplante Ausführungsbenachrichtigungen ab dem ersten Tag funktionieren.

PHASE 3 • Tag 46—75

Datenresilienz und stabiler Geschäftsbetrieb

Ziel: Schutzlücken schließen, RTOs/RPOs verbessern und Ransomware-Resilienz hinzufügen.

Meilenstein 7: Deckungslücken schließen

- Führen Sie den Report über nicht geschützte VMs in Veeam ONE aus, um alle ungeschützten Workloads vor allen anderen Optimierungen abzusichern.
- Schützen Sie physische Workloads bei Bedarf durch den Einsatz von Veeam Agent für Microsoft Windows oder Veeam Agent für Linux.
- Überprüfen Sie die Zeitpläne der Jobs auf Überschneidungen und staffeln Sie die Startzeiten, um Ressourcenüberlastungen bei Proxy und Repository zu vermeiden.
- Überprüfen Sie die Compliance des RPO: Erzeugen alle kritischen VMs Wiederherstellungspunkte innerhalb Ihres Ziel-Wiederherstellungsfensters?
- Bestätigen Sie, dass alle Backup-Jobs innerhalb Ihres definierten Backup-Fensters abgeschlossen werden.

Erweiterung der Proxy-Kapazität durch einen zweiten VIA

Wenn Backup-Jobs langsam ausgeführt werden oder das vorgesehene Backup-Fenster überschreiten, stellen Sie eine zweite Veeam Infrastructure Appliance als Proxy bereit.

Mit dem pre-hardened Appliance-Modell ist dies schnell möglich: Stellen Sie die OVA oder ISO bereit und registrieren Sie sie in Veeam Backup & Replication. Daraufhin werden die Jobs automatisch zwischen beiden Proxys lastverteilt, ohne dass eine manuelle Proxy-Konfiguration erforderlich ist.

Meilenstein 8: Ransomware-Bereitschaft

- Veeam Data Platform Advanced und Premium enthalten zwei ergänzende Sicherheitstools. Der erste ist Recon, der Bedrohungsinformations-Service von Veeam, der IOCs und neu auftretende Daten aus realer Reaktion auf Vorfälle bereitstellt. Das zweite ist Scan-Backup, eine produktinterne Aktion in Veeam Backup & Replication. Es untersucht bestehende Backup-Ketten auf Malware-Indikatoren und validiert die Dateiintegrität, ohne dass ein isoliertes Netzwerk oder das Booten von VMs erforderlich ist.

Führen Sie ein Scan-Backup durch:

- Erstellen Sie einen SureBackup-Auftrag in Veeam Backup & Replication unter „Home“ > „SureBackup“. SureBackup läuft als geplanter Auftrag und kann Ihre Backups in einem Durchgang auf Malware, Signaturbasierte Bedrohungen und Dateiintegrität überprüfen, ohne dass dafür ein isoliertes Netzwerk oder ein VM-Start erforderlich ist.

- Verknüpfen Sie die Backup-Jobs, die Sie abdecken möchten, sodass der SureBackup-Job im Laufe der Zeit alle Ihre Daten abdeckt: Veeam abgesichertes Repository (Pfad A), Veeam Software Appliance lokales Repository (Pfad B), das bestehende NAS/Windows-Repository (Pfad C) und Vault.
- Aktivieren Sie in den Optionen zur Überprüfung den Malware-Scan mit Veeam Threat Hunter (oder einer Antivirenlösung eines Drittanbieters), um den Backup-Inhalt anhand einer aktuellen Bedrohungssignatur-Datenbank zu überprüfen.
- Aktivieren Sie in den gleichen Überprüfungsoptionen die Dateiintegritätsprüfung, um die Backup-Datei mit einer CRC-Prüfung zu validieren und beschädigte Blöcke zu identifizieren.
- Planen Sie den SureBackup-Job und überprüfen Sie die Sessionsergebnisse regelmäßig; untersuchen Sie alle gekennzeichneten Wiederherstellungspunkte, bevor Sie sie zur Wiederherstellung verwenden.
- Für eine Ad-hoc-Prüfung zwischen den geplanten Läufen gehen Sie zu Home > Backups, erweitern Sie den Backup-Job, wählen Sie den Workload aus und klicken Sie auf „Scan Backup“ im „Backup-Tab“.

Recon installieren

- Installieren Sie die Recon-Binärdatei auf einem Windows-basierten Veeam-Infrastruktur-Host oder einem Linux-Host Ihrer Wahl.
- Recon kann auch auf entsprechenden Windows-Domain-Controllern installiert werden.
- Recon lässt sich nicht auf der Veeam Infrastruktur Appliance installieren. Veeam Infrastructure Appliances sind für eine einzelne Aufgabe ausgelegt und pre-hardened.

Unveränderbarkeitsprüfung

- Stellen Sie sicher, dass der Unveränderbarkeitszeitraum auf Ihrem abgesicherten Repository von Veeam Infrastructure Appliance auf ein angemessenes Aufbewahrungsfenster eingestellt ist.
- Prüfen Sie die Backup-Verschlüsselungseinstellungen und aktivieren Sie die Verschlüsselung bei der Speicherung für Jobs, falls noch nicht konfiguriert.
- Führen Sie den Veeam ONE „Immutable Workloads“-Report aus, um Unveränderbarkeitsziele für Workload-Backups zu messen und zu identifizieren.

Ransomware-Wiederherstellungsbereitschaft

Dokumentieren Sie ein einfaches Wiederherstellungs-Runbook, das angibt, welche VMs zuerst wiederhergestellt werden sollen, aus welchen Wiederherstellungspunkten und auf welches Ziel.

Identifizieren Sie mindestens einen sauberen, vor der Infektion erstellten Wiederherstellungspunkt im Vault als Ihren letzten bekannten guten Anker.

Ihre unveränderbaren Kopien können während der Unveränderbarkeitsperiode nicht überschrieben oder verschlüsselt werden. Dies ist Ihr Sicherheitsnetz.

Pfad A: Veeam abgesichertes Repository plus Vault.

Pfad B: Veeam Software Appliance mit lokalem Speicher plus Veeam Vault.

Pfad C: Vault plus Ihr lokales Repository, falls Sie dort Immutability konfiguriert haben.

Meilenstein 9: Leistungsoptimierung und Orchestrierungspläne

- Überprüfen Sie den Proxy-Durchsatz in den Jobstatistiken von Veeam Backup & Replication. Wenn es zu Engpässen bei den Jobs kommt, stellen Sie eine zweite Veeam Infrastruktur Appliance in der Proxy-Rolle bereit.
- Stellen Sie sicher, dass der Übertragungsmodus für das Backup optimal ist: Hot Add (VMware) oder Direct Storage Access, sofern verfügbar.
- Überprüfen Sie, ob alle Backup-Jobs innerhalb Ihres definierten Wartungsfensters abgeschlossen sind.
- Überprüfen Sie die Veeam ONE Leistungsdiagramme und identifizieren Sie VMs mit ungewöhnlich hohen Änderungsraten, die von speziellen Jobs oder angepassten Zeitplänen profitieren könnten.

Erstellen Sie initiale Orchestrierungspläne (nur in der Premium-Version)

Überspringen Sie diesen Abschnitt, wenn Ihre Edition Foundation oder Advanced ist oder wenn Sie keinen unterstützten Hypervisor für Veeam Recovery Orchestrator. verwenden.

Veeam Recovery Orchestrator verwandelt Ihr manuelles Wiederherstellungs-Runbook in einen ausführbaren Plan. Durch das Erstellen von Plänen kann in Phase 4 die Wiederherstellbarkeit automatisch nachgewiesen werden, anstatt manuelle Wiederherstellungen erneut durchzuführen.

- Identifizieren Sie Tier-1-Anwendungs-Stacks, die eine orchestrierte Wiederherstellung benötigen (z. B. Domänencontroller, primäre Datenbank, primäre Anwendungsserver).
- Erstellen Sie in Veeam Recovery Orchestrator Ihren ersten Wiederherstellungsplan für einen dieser Stacks.
- Definieren Sie die Startreihenfolge Ihrer VMs und die Abhängigkeiten, damit Voraussetzungen (z. B. DCs, DNS usw.) vor den abhängigen Services gestartet werden.
- Konfigurieren Sie Wiederherstellungsziele (z. B. Host, Cluster, Datastore) und ordnen Sie das Produktionsnetzwerk für den tatsächlichen Failover sowie ein isoliertes Netzwerk zu Testzwecken zu.
- Legen Sie die RTO- und RPO-Ziele des Plans fest, damit Veeam Recovery Orchestrator Abweichungen im Zeitverlauf erkennen kann.
- Speichern Sie den Plan und prüfen Sie die automatisch erzeugte Dokumentation gemeinsam mit den Stakeholdern, bevor Sie Phase 3 als abgeschlossen erklären.

PHASE 4 • Tag 76—100

Wertnachweis und Operationalisierung

Ziel: Wiederherstellbarkeit verifizieren, laufende Systemhygiene etablieren und ROI belegen.

Meilenstein 10: Wiederherstellungstests

Das einzige Backup, das zählt, ist eines, von dem Sie wiederherstellen können. In Phase 4 weisen Sie mit dokumentierten Beweisen nach, dass Ihre Umgebung die RTO- und RPO-Verpflichtungen erfüllt.

SureBackup und Scan-Backup

- Konfigurieren Sie eine SureBackup-Anwendungsgruppe, die Ihre wichtigsten VMs umfasst (z. B. Domänencontroller und wichtige Anwendungsserver).
- Führen Sie einen SureBackup-Job aus, um die Boot-Überprüfung zu automatisieren und zu bestätigen, dass VMs starten und Heartbeat-, Ping- sowie Anwendungs-Tests durchlaufen.
- Für eine vereinfachte Überprüfung führen Sie ein Scan-Backup durch. Es validiert die Dateiintegrität und sucht nach Bedrohungen, ohne VMs zu booten, was in kleineren Umgebungen eine sinnvolle Ergänzung oder Alternative zu SureBackup darstellt.

Granulare und vollständige Wiederherstellungstests

- Testen Sie Wiederherstellungen auf Dateiebene und stellen Sie einzelne Dateien aus einem Backup zu einem Testziel wieder her.
- Testen Sie die Wiederherstellung von Anwendungsobjekten, indem Sie ein SQL-Datenbankobjekt oder einen Active Directory-Benutzer mit Veeam Explorers™ wiederherstellen.
- Testen Sie eine Wiederherstellung einer vollständigen VM aus dem Vault, um einen Totalverlust lokal zu simulieren und Ihre externe Kopie zu validieren.
- Erfassen Sie die tatsächlichen Wiederherstellungszeiten und vergleichen Sie sie mit Ihren RTO-Zielen und dokumentieren Sie die Ergebnisse.

Best Practices für Wiederherstellungstests

Stellen Sie immer auf ein Nicht-Production-Ziel wieder her und überschreiben Sie während eines Tests niemals produktive Workloads.

Dokumentieren Sie, was wiederhergestellt wurde, aus welchem Wiederherstellungspunkt, auf welches Ziel und wie lange es gedauert hat.

Diese Resultate sind Ihr Nachweis der Wiederherstellbarkeit. Bewahren Sie sie für Compliance-Überprüfungen, Audits und Management-Reporting auf.

Ausführen von Orchestrierungsplänen (nur Premium)

Überspringen Sie diesen Abschnitt, wenn Ihre Edition Foundation oder Advanced ist oder wenn Ihr Hypervisor nicht von Veeam Recovery Orchestrator unterstützt wird. In Phase 3 wurde Ihr erster Wiederherstellungsplan erstellt, aber in Phase 4 zeigt er seinen Wert.

- Führen Sie einen unbeaufsichtigten Bereitschaftstest für Ihren Plan durch. Veeam Recovery Orchestrator prüft die Verfügbarkeit von Wiederherstellungspunkten, die Zielkapazität und Konfigurationsabweichungen, ohne dabei VMs zu starten.
- Führen Sie einen DataLab-Test an Ihrem Plan durch. Veeam Recovery Orchestrator stellt den Anwendungsstapel in einem isolierten Netzwerk wieder her und führt Verifizierungsprüfungen auf Anwendungsebene gegen Live-VMs durch.
- Zeichnen Sie die tatsächlichen Wiederherstellungszeiten aus dem DataLab-Lauf auf und vergleichen Sie sie mit dem RTO-Ziel, das Sie in Phase 3 festgelegt haben.
- Erstellen Sie den Wiederherstellungs-Bereitschafts-Report mit Veeam Recovery Orchestrator und archivieren Sie ihn zusammen mit Ihren anderen Wiederherstellungstest-Ergebnissen.
- Für Workloads, die nicht von einem Veeam Recovery Orchestrator Plan abgedeckt werden, greifen Sie auf die oben beschriebenen manuellen Wiederherstellungstests zurück.

Meilenstein 11: Reporting und Dokumentation

Erstellen Sie monatlich einen Veeam ONE Executive Summary Report und teilen Sie ihn mit der Geschäftsleitung, um die Backup-Integrität und Abdeckung zu demonstrieren.

- Exportieren Sie einen InventarReport der geschützten Workloads, um den Schutzumfang zu bestätigen.
- Dokumentieren Sie Ihre finale Backup-Architektur, einschließlich Auftragsliste, Repository-Layout, Veeam Infrastruktur Appliance-Rollen, Zeitpläne und Aufbewahrungsrichtlinien.
- Überprüfen Sie den Speicherverbrauch von Veeam Vault und bestätigen Sie, dass Ihre Nutzung im Einklang mit Ihrem geplanten Budget steht.
- Archivieren Sie die Ergebnisse der Wiederherstellungstests zusammen mit der Architekturdokumentation.
- Nur für Premium: Generieren Sie jeden Monat den Wiederherstellungsbereitschafts-Report des Veeam Recovery Orchestrator. Verfolgen Sie die Bereitschaftsbewertung im Laufe der Zeit, wenn sich Workloads und Abhängigkeiten ändern.
- Nur Premium: Archivieren Sie die von Veeam Recovery Orchestrator erstellte Plandokumentation zusammen mit Ihren Architekturdokumenten. Veeam Recovery Orchestrator erstellt diese automatisch neu, wenn sich Pläne ändern. Archivieren Sie sie daher erneut, wenn die Pläne aktualisiert werden.

Meilenstein 12: regelmäßige Systemhygiene

Bis Tag 100 sollte Ihre Umgebung stabil und vollständig dokumentiert sein. Diese Gewohnheiten sorgen dafür, dass es so bleibt:

- **Wöchentlich:** Überprüfen Sie das Veeam ONE-Dashboard zum Jobzustand und beheben Sie Fehler oder Warnungen umgehend.
- **Wöchentlich:** Überprüfen Sie den Report über ungeschützte VMs in Veeam ONE und fügen Sie Schutz für neue VMs hinzu.
- **Monatlich:** Erstellen Sie einen Executive Summary und Reports über geschützte VMs und geben Sie die Ergebnisse weiter.
- **Monatlich:** Überprüfen Sie den Vault-Speicherverbrauch und die Wachstumsrate. Achten Sie darauf, ob Sie Ihre budgetierten Kapazitäten überschreiten oder ob bevorstehende Anpassungen der Aufbewahrung anstehen.
- **Monatlich:** Vergewissern Sie sich, dass die Aufbewahrungsfristen weiterhin gelten und nicht geändert wurden.
- **Quartalsweise:** Führen Sie einen dokumentierten Wiederherstellungstest durch und rotieren Sie die Workload-Typen.
- **Quartalsweise:** Einen Scan-Backup-Lauf über jedes Repository durchführen, um nach Malware-Signaturen und Veränderungen der Dateiintegrität zu suchen.
- **Quartalsweise:** Überprüfen Sie, wer administrativen Zugriff auf Veeam Backup & Replication, Veeam ONE und Veeam Recovery Orchestrator (nur Premium) hat. Entfernen Sie den Zugriff für alle, die ihre Rolle gewechselt oder das Unternehmen verlassen haben.
- **Quartalsweise (nur Premium):** Führen Sie einen Veeam Recovery Orchestrator DataLab-Test durch und rotieren Sie, welcher Orchestrierungsplan jeweils getestet wird.
- **Quartalsweise (nur Premium):** Erstellen Sie die Plandokumentation von Veeam Recovery Orchestrator neu und archivieren Sie sie, falls sich Pläne seit der letzten Überprüfung geändert haben.
- **Monatlich:** Überprüfen Sie Recon Threat Intelligence-Updates und wenden Sie relevante Signaturen oder Regeln in Ihrer Umgebung an.

- **Jährlich:** Überprüfen Sie Ihre Backup-Architektur und Aufbewahrungsrichtlinien im Hinblick auf aktuelle Geschäftsanforderungen und neue Compliance-Verpflichtungen.
- **Jährlich:** Führen Sie eine vollständige Wiederherstellung aus dem Vault durch, um zu überprüfen, ob die externe Kopie durchgängig wiederherstellbar ist. Dokumentieren Sie das Ergebnis.
- **Jährlich:** Überprüfen Sie die Verschlüsselungseinstellungen während der Übertragung und bei der Speicherung und erneuern Sie die Schlüssel gemäß Ihrer Sicherheitsrichtlinie.
- **Bei Bedarf:** Planen Sie den Aktualisierungszyklus Ihrer Veeam-Komponenten (z. B. Veeam Software Appliance, Veeam Infrastruktur Appliance, Veeam ONE, Veeam Agents und Veeam Recovery Orchestrator, falls zutreffend) und abonnieren Sie Release-Benachrichtigungen.
- **Vor der Verlängerung:** Überprüfen Sie die Lizenznutzung, die Wachstumsprognosen und die passende Edition. Wenn das Feature-Set Ihrer Edition Ihren Anforderungen nicht mehr genügt, ist dies der richtige Zeitpunkt, um mit Ihrem Veeam-Ansprechpartner über ein Upgrade zu sprechen.

Abschließende Empfehlungen

Herzlichen Glückwunsch! Sie haben es geschafft.

In 100 Tagen sind Sie von der Bereitstellung zu einer voll funktionsfähigen Datenschutzumgebung gelangt. Ihre Workloads sind geschützt, Ihre Backups sind gehärtet und unveränderbar und Sie haben gezeigt, dass Sie Ihre Systeme nicht nur theoretisch, sondern auch nachweislich wiederherstellen können.

Das ist keine Kleinigkeit.

Jetzt verschiebt sich der Schwerpunkt vom Aufbau zur Wartung. Führen Sie Wiederherstellungen regelmäßig nach einem Testplan durch, passen Sie Richtlinien an, wenn sich Ihre Umgebung weiterentwickelt, und nutzen Sie Ihre Monitoring- und Reporting-Routine, um Abweichungen frühzeitig zu erkennen, bevor sie zum Risiko werden. Die Gewohnheiten, die Sie in Meilenstein 12 etabliert haben — Ihr wöchentlicher, monatlicher, vierteljährlicher und jährlicher Wartungsrhythmus — sorgen dafür, dass Ihre Umgebung auch lange nach Tag 100 zuverlässig bleibt. Befolgen Sie diese, übernehmen Sie Verantwortung dafür und entwickeln Sie sie weiter, während Ihr Unternehmen wächst.

Denken Sie daran, dass Tag 100 nicht die Ziellinie ist. Es ist der Ausgangspunkt. Resilienz ist ein kontinuierlicher Prozess, kein einmaliges Projekt.

Halten Sie Ihre Administratorrollen auf dem neuesten Stand, damit die richtigen Personen immer den richtigen Zugriff haben, und bleiben Sie durch das Abonnieren der Veeam Release-Hinweise und Sicherheitshinweise stets informiert, sodass Sie nie überrascht werden.

Sie müssen das nicht alleine tun

Die Communities, Lernressourcen und technischen Teams von Veeam unterstützen Sie dabei, Ihre Ziele zu erreichen. Nutzen Sie sie, während Ihre Umgebung wächst und sich weiterentwickelt! Eine kuratierte Liste von Ressourcen ist im Anhang verfügbar.

Bei Fragen oder weiteren Schritten wenden Sie sich bitte an Ihren Customer Success Account Manager oder bei technischen Fragen an Veeam Technical Support .

Anhang: Kurzreferenz

Schlüsselkomponenten: Veeam Data Platform

- **Veeam Software Appliance:** Eine vorgehärtete Appliance mit vorinstalliertem Veeam Backup & Replication. Als OVA (VM) oder ISO (physisch) bereitstellen. Dies ist der empfohlene Ausgangspunkt für alle KMU-Bereitstellungen.
- **Veeam Infrastruktur Appliance:** Eine pre-hardened Appliance, die als dedizierter Backup-Proxy oder abgesichertes Repository bereitgestellt wird. Es bietet lokale Immutabilität ohne Linux-Kenntnisse, wobei jede Appliance nur eine Rolle übernimmt.
- **Veeam Backup & Replication:** eine zentrale Backup-Engine, gehostet auf der Veeam Software Appliance. Es verwaltet Aufträge, Repositorys, Proxys und Wiederherstellungsvorgänge.
- **Veeam ONE:** Übernimmt Monitoring, Alarmierung und Reporting. Es verfügt über eine separate Windows-basierte Installation und verbindet sich mit Veeam Backup & Replication sowie Ihrem Hypervisor, um vollständige Stack-Transparenz zu ermöglichen.
- **Recon:** Dies ist der BedrohungsinformationsService von Veeam. Er zeigt Indicators of Compromise (IOCs), Bedrohungssignaturen sowie Daten zu neuen Kampagnen auf, die aus realen Reaktionen auf Vorfälle gewonnen wurden. Bestandteil der Veeam Data Platform Advanced.
- **Backup-Inhalte scannen:** Dies ist eine produktinterne Aktion, die bestehende Backup-Ketten auf bekannte Malware-Signaturen scannt und die Dateiintegrität validiert, ohne dass ein isoliertes Netzwerk oder das Booten von VMs erforderlich ist. Bestandteil der Veeam Data Platform Advanced.
- **Veeam Recovery Orchestrator:** Eine Orchestrierungsplattform, die die Disaster Recovery (DR) auf Anwendungsebene automatisiert. Sie können damit ausführbare Wiederherstellungspläne erstellen, Bereitschaftstests durchführen, DataLab-basierte Überprüfungen vornehmen und Wiederherstellungsdokumentation erstellen. Im Lieferumfang von Veeam Data Platform Premium enthalten.
- **Veeam Data Cloud Vault:** Dies stellt unveränderbaren Cloud-Objektspeicher für externe Kopien bereit. Es wird von Veeam verwaltet und erfordert kein separates Cloud-Konto.

Schlüsselbegriffe

- **RPO (RPO):** Maximal akzeptabler Datenverlust, zeitlich bemessen. Steuert die Häufigkeit des Backup-Zeitplans.
- **Recovery Time Objective (RTO):** Maximal akzeptable Ausfallzeit, bevor ein Workload wiederhergestellt werden muss.
- **Großvater-Vater-Sohn (GFS):** Ein Aufbewahrungsschema, das tägliche, wöchentliche und monatliche Wiederherstellungspunkte vorhält.
- **Unveränderbarkeit:** Backup-Daten, die für eine bestimmte Aufbewahrungsfrist weder verändert noch gelöscht werden können. Schützt vor der Verschlüsselung von Backup-Dateien durch Ransomware.
- **Instant VM Recovery:** Stellt eine VM innerhalb von Sekunden direkt aus einem Backup wieder her, ohne vorher Daten zu kopieren. Migrieren Sie nach der Validierung immer auf den Produktiv-Speicher.
- **Orchestrierungsplan (Veeam Recovery Orchestrator):** Ein ausführbares Runbook, das die Reihenfolge, Abhängigkeiten, Zielspeicherort und Netzwerkzuordnungen für die Wiederherstellung einer Reihe von Workloads definiert. Ersetzt ein manuelles Wiederherstellungs-Runbook durch eine auto-dokumentierte und testbare Automatisierung.
- **DataLabs:** eine isolierte Testumgebung, in der Veeam Recovery Orchestrator (oder SureBackup) ein Backup wiederherstellt und eine Überprüfung auf Anwendungsebene durchführt, ohne die Produktionsumgebung zu beeinträchtigen. Ermöglicht vollständige Testdurchläufe des Plans in jedem gewünschten Intervall.
- **anwendungsspezifische Verarbeitung:** Gastverarbeitung, die anwendungskonsistente Backup-Punkte für SQL Server, Oracle, Exchange, Active Directory, SharePoint, PostgreSQL und MySQL erstellt. Verwendet VSS unter Windows sowie pre-freeze-/post-thaw-Skripting und datenbank-natives Quiescing auf Linux-Systemen.
- **Veeam abgesichertes Repository:** Ein Linux-basiertes Backup-Repository mit Unveränderbarkeit, die auf Dateisystemebene durchgesetzt wird. Die Veeam Infrastruktur-Appliance stellt ein vorkonfiguriertes Veeam abgesichertes Repository bereit, für das keine Linux-Administration erforderlich ist. Objektspeicher und Objektsperre sind separate Unveränderbarkeitsmechanismen, nicht Veeam Hardened Repositories. Die Unveränderbarkeit auf Dateisystemebene schützt vor Angriffen auf das OS, aber nicht vor der Zerstörung auf VM-Ebene. Ein Veeam abgesichertes Repository, das als virtuelle Appliance betrieben wird, kann auf der Hypervisor-Ebene weiterhin gelöscht werden. Daher sollten Sie die Veeam Infrastruktur Appliance auf physischer Hardware bereitstellen, um maximalen Schutz zu gewährleisten.
- **Hot Add-Übertragungsmodus:** Dies ist ein VMware-spezifischer Backup-Übertragungsmodus. Die Proxy-VM fügt die virtuellen Festplatten der Quell-VM per Hot Add hinzu und liest sie über SCSI aus, wobei der NBD-Pfad über das ESXi-Verwaltungsnetzwerk vermieden wird.

Anhang: Nützliche Links

Mein Konto

Ihr Veeam-Konto ist Ihre zentrale Anlaufstelle für die Verwaltung Ihrer Bereitstellung. Sobald Sie angemeldet sind, können Sie Produkte und Lizenzschlüssel herunterladen, Case-Administratoren verwalten, den Veeam-Support kontaktieren sowie Verträge verlängern oder Lizenzen hinzufügen.

- Melden Sie sich an oder erstellen Sie Ihr Veeam-Konto
- Wie Sie ein Konto erstellen
- FAQ zur Anmeldung
- Verwaltung von Lizenz- und/oder Falladministrator-Rollen

Dokumentation und Downloads

- Help Center mit technischer Dokumentation, Bereitstellungsanleitungen und Benutzerhandbüchern
- Produkt-Downloads, einschließlich Software-Updates, Patches und Release-Hinweise
- Support Knowledge Base mit häufigen Problemen, Schritten zur Fehlerbehebung und empfohlenen Lösungen, die regelmäßig von den Veeam-Support- und Engineering-Teams aktualisiert werden

Lernen und Best Practices

- Regelmäßige Live-Onboarding-Webinare: Bei denen Sie in Echtzeit Fragen stellen und direkt von technischen Spezialisten Antworten erhalten können
- Veeam University Free: Selbstlernkurse und kostenlose Zertifizierungen
- Veeam Sizing Calculators: Online-Tool zur Größenbestimmung und Abschätzung, das zur Berechnung der Infrastruktur-, Speicher- und Kapazitätsanforderungen für Veeam-Bereitstellungen verwendet wird.
- Best Practices von Veeam Solution Architects: Leitfaden zur Infrastrukturgestaltung und Konfiguration, basierend auf realen Bereitstellungen, den Sie erneut prüfen sollten, wenn Ihre Umgebung reift
- Handlungsorientierte Anweisungen für Veeam Intelligence: eine kuratierte Sammlung effektiver Anweisungen, die Sie dabei unterstützt, das volle Potenzial von Veeam Intelligence auszuschöpfen
- Veeam Search: Das zentrale Suchportal von Veeam, mit dem Sie alle Veeam-Ressourcen von einem zentralen Ort aus durchsuchen können.

Veeam Communities (community.veeam.com)

- Veeam Community-Foren: Vernetzen Sie sich mit Fachkollegen, tauschen Sie Best Practices aus, nehmen Sie an Benutzergruppen und Community-Events teil und diskutieren Sie reale Anwendungsfälle
- Veeam R&D-Foren: Ihr direkter Draht zu Veeam R&D für Produktdiskussionen, technische Fragen und Feature-Feedback

Über Veeam Software

Veeam ist das führende Unternehmen für Daten- und KI-Vertrauen mit dem Anspruch, Organisationen dabei zu unterstützen, ihre Daten und KI vollständig zu verstehen, zu schützen und resilient zu halten, um die sichere Nutzung von KI in großem Umfang zu beschleunigen. Als Marktführer in den Bereichen Datenresilienz und Management der Datensicherheitslage (Data Security Posture Management = DSPM) ist Veeam auf die Konvergenz von Identität, Daten, Sicherheit und KI-Risiko ausgerichtet.

Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit schützt Veeam über 550.000 Kunden, darunter 82 % der Fortune 500.

Erfahren Sie mehr unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.