Veeam Data Platform

Primi 100 giorni

Una Guida pratica di onboarding per amministratori IT

Indice

1. Executive summary

Veeam Data Platform è il fondamento della resilienza della vostra organizzazione contro i ransomware e della continuità operativa. Questa Guida è pensata per aiutare i team IT a operazionalizzare e far evolvere il proprio ambiente in modo strutturato. Sebbene usiamo il termine "primi 100 giorni", si tratta solo di una metafora per una linea temporale. Ogni organizzazione è diversa e può avanzare a ritmi differenti, ma l'obiettivo è sempre lo stesso: passare dalla configurazione iniziale a uno stato più sicuro, resiliente e pronto al ripristino. È strutturato attorno a traguardi pratici e risultati raccomandati, piuttosto che a rigidi requisiti di implementazione, consentendoti di concentrarti sulle fasi più rilevanti per il tuo ambiente e la tua edizione.

2. A chi è destinata questa guida?

Questa Guida è destinata a**gli amministratori IT** che si occupano dell'implementazione, configurazione e operatività di Veeam Data Platform. Si presuppone che tu abbia familiarità con le infrastrutture virtualizzate (ad esempio, VMware vSphere, Microsoft Hyper-V o qualsiasi altro hypervisor supportato da Veeam Backup & Replication) e con l'amministrazione di base di Windows Server. Non è richiesta alcuna conoscenza di Linux.

Serve anche come riferimento comune per **manager IT** che monitorano l'ambito e le tempistiche, per gli stakeholder della sicurezza e della conformità che validano la postura di sicurezza, e per i team di leadership o procurement chiarendo cosa si intende per successo al giorno 100.

3. Cosa otterrai entro il centesimo giorno

Entro il giorno 100, avrai un ambiente stabile, robusto e verificabilmente ripristinabile che riduce il rischio di interruzione del servizio e consente un ripristino rapido e sicuro in qualsiasi circostanza.

Ogni cliente dovrebbe essere in grado di confermare che i seguenti punti di controllo siano stati rispettati:

- **Implementato:** Veeam Backup & Replication è in esecuzione, connesso e dimensionato per soddisfare finestre di backup.
- **Protetto:** i carichi di lavoro prioritari vengono sottoposti a backup correttamente secondo una pianificazione definita.
- **Rafforzato:** l'immutabilità è implementata a livello locale e/o remoto per difendersi dal ransomware.
- **Recuperabile in modo verificabile:** i test di ripristino sono completi, documentati e mappati agli obiettivi di RTO (Recovery Time Objective) e RPO (Recovery Point Objective).
- **Efficienza operativa:** il monitoraggio, gli avvisi, la reportistica e i runbook di ripristino sono in atto e con responsabilità assegnata.

4. Sintesi della roadmap

Questa guida è strutturata in quattro fasi sequenziali, ognuna delle quali contribuisce al raggiungimento degli obiettivi previsti per il giorno 100:

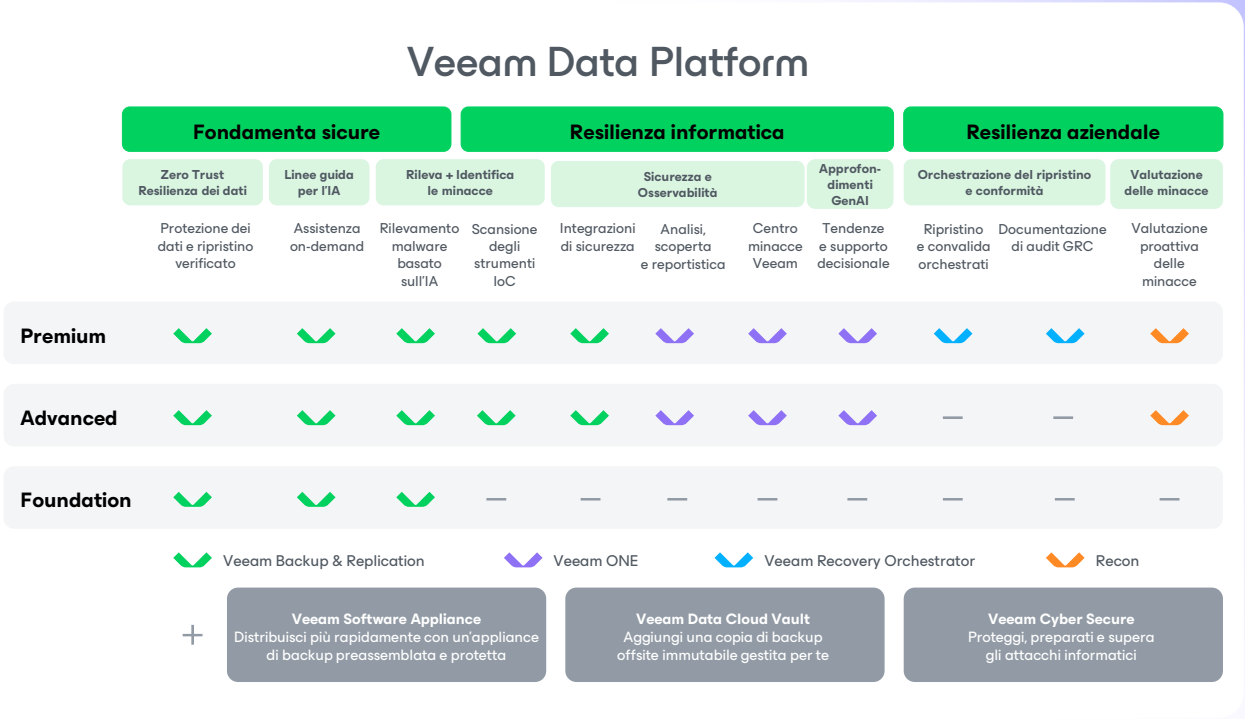
Fase	Nome	Tempistica	Focus
FASE 1	Foundation	Giorni 1—14	Dimensionare l'ambiente, distribuire Veeam Software Appliance (e Veeam Infrastructure Appliance, se applicabile), eseguire i primi job di backup, predisporre per Veeam Recovery Orchestrator.
FASE 2	Ottimizzazione	Giorni 15—45	Elaborazione application-aware, Backup Copy Job (copia del backup), livello offsite Veeam Data Cloud Vault e configurazione di Veeam Recovery Orchestrator (Premium).
FASE 3	Resilienza dei dati e dei processi aziendali	Giorni 46—75	Colmare le lacune di copertura, abilitate Recon, prepararsi al ransomware, ottimizzare e creare piani di orchestrazione (Premium).
FASE 4	Dimostrazione del valore	Giorni 76—100	Test di ripristino orchestrati, reportistica, architettura documentale e igiene operativa continua.

Come utilizzare questa Guida

- Segui le tappe in ordine. Saltare delle tappe, in particolare la configurazione di Scale-Out Backup Repository™ (SOBR) o di Vault, prima che i repository e i job locali siano stabili crea delle lacune che in genere emergono durante un ripristino effettivo.
- La tempistica è flessibile. I giorni sono linee guida, non scadenze rigide. Gli ambienti più piccoli possono completare la Fase 1 in meno di una settimana. Ambienti più complessi potrebbero richiedere più tempo nelle fasi successive.
- Utilizza i punti decisionali. Quando si presentano scelte architetturali (ad esempio, percorso di implementazione o strategia del repository), fai una pausa, allinea gli stakeholder e documenta la tua decisione prima di procedere.
- Salta ciò che non si applica, ma annota il motivo. Se la tua edizione non include Veeam ONE o Veeam Recovery Orchestrator, questi traguardi saranno chiaramente indicati. Analogamente, i passaggi relativi a Veeam Software Appliance e Veeam Vault sono facoltativi e rilevanti solo se questi moduli fanno parte della tua implementazione.

Panoramica di Veeam Data Platform

Prima di addentrarci nella procedura di implementazione e nelle relative modalità, iniziamo con un breve riepilogo di ciò che include la tua Veeam Data Platform. Veeam Data Platform è disponibile in tre edizioni, ognuna delle quali si basa sulla precedente:



Per la descrizione di tutti i componenti, consultare l'appendice: Appendice: Guida rapida. Componenti principali".

Prenditi un momento per confermare la tua versione.

Prima di procedere, conferma la tua edizione e fai un inventario completo di ciò che è incluso. Nella protezione dei dati, le capacità inutilizzate non sono solo valore sprecato — sono lacune in attesa di essere esposte.

Inoltre, i seguenti moduli sono disponibili in tutte le edizioni:

- **Veeam Software Appliance:** una piattaforma di implementazione pre-hardened, senza Windows, che semplifica la configurazione dell'infrastruttura e rafforza la postura di sicurezza. Non è richiesta alcuna conoscenza di Linux.
- **Veeam Vault:** archiviazione di backup immutabile e off-site fornita come servizio per proteggere i tuoi dati da ransomware e cancellazione accidentale.
- **Veeam Agents:** i Veeam Agents sono agenti software che offrono backup e ripristino a livello di immagine con la qualità Veeam per server fisici, endpoint fisici e piattaforme di macchine virtuali (VM) non supportate, gestiti centralmente dalla console di Veeam Backup & Replication.

Il percorso verso la resilienza inizia qui.

Nei prossimi 100 giorni, passerai dall'implementazione a un ambiente completamente rafforzato e verificabilmente recuperabile, procedendo passo dopo passo senza tentativi.

FASE 1 **Foundation** **Giorni 1—14**	**FASE 2** **Ottimizzazione** **Giorni 15—45**	**FASE 3** **Resilienza dei dati e resilienza dei processi aziendali** **Giorni 46—75**	**FASE 4** **Dimostrare il valore** **Giorni 76—100**
M1: Dimensionamento e pianificazione	M4: Elaborazione application-aware	M7: Colmare le lacune di copertura	M10: Test di ripristino
M2: Implementazione di Veeam Software Appliance e Infrastruttura	M5: Copia del backup, SOBR e vault	M8: Prontezza contro i ransomware	M11: Report e documentazione
M3: Primi job di backup	M6: Configurazione di monitoraggio, gestione degli avvisi e dell'orchestratore	M9: Piani di tuning delle prestazioni e piani di orchestrazione	M12: Manutenzione continua

FASE 1 • Giorni 1—14

Foundation

Obiettivo: infrastruttura dimensionata, implementata e primi carichi di lavoro protetti.

Traguardo 1: Dimensionamento e pianificazione

Prima di implementare qualsiasi cosa, dedicate del tempo al dimensionamento. Un'infrastruttura sottodimensionata è la causa più comune di finestre di backup lente e mancato rispetto degli RPO nei primi 100 giorni.

Inventario dei carichi di lavoro

- Documenta il numero totale di VM e carichi di lavoro, l'impiego di risorse (totale allocato rispetto a quello utilizzato) e il tasso giornaliero di variazione stimato.
- Identifica i carichi di lavoro critici, poiché sono questi a determinare i tuoi obiettivi di RPO e RTO.
- Annota eventuali carichi di lavoro fisici (ad es. server Windows/Linux) che richiederanno gli agenti Veeam.

Dimensionamento di Veeam Software Appliance

- Veeam Software Appliance viene fornito con Veeam Backup & Replication preinstallato, quindi la decisione principale in termini di dimensionamento riguarda l'host su cui viene eseguito.
- Requisiti minimi per le piccole e medie imprese (PMI): 8 vCPU / 16 GB di RAM (si consigliano 500 MB di RAM per ogni job concorrenti).
- Utilizza il calcolatore di dimensionamento Veeam (calculator.veeam.com) per verificare i requisiti di risorse in base al numero di carichi di lavoro e all'impiego di risorse.
- Scegli il formato di implementazione: OVA per VMware vSphere o ISO per server fisici e altri hypervisor. In entrambi i casi non è richiesta alcuna esperienza con Linux.

Architettura dello storage: scegli il tuo percorso

La scelta dello storage in questa fase determina il resto delle fasi 1 e 2. Sono disponibili tre percorsi consigliati per le PMI:

Percorso A: Veeam Software Appliance + Veeam Infrastructure Appliance come repository con protezione avanzata Veeam + Vault: Questa è la configurazione di base consigliata. Questo percorso fornisce un repository locale immutabile senza richiedere competenze Linux, oltre a copie immutabili off-site e fisicamente isolato a livello logico tramite Vault.

Opzione A: perché utilizzare un Veeam Hardened Repository fornito tramite Veeam Infrastructure Appliance?

Un repository con protezione avanzata di Veeam offre backup locali immutabili. Il ransomware non può crittografarli o eliminarli durante il periodo di retention.

Tradizionalmente, un repository Linux immutabile richiede un Server Linux dedicato e un hardening manuale del SO. Veeam Infrastructure Appliance elimina completamente tale barriera. Viene fornito con sicurezza rafforzata, distribuito tramite OVA o ISO e non richiede competenze Linux per l'implementazione o la gestione.

Veeam Infrastructure Appliance è un'appliance a ruolo unico. Ciascuna istanza viene eseguita come repository con protezione avanzata Veeam o come proxy di backup. Per le PMI senza un amministratore Linux dedicato o uno storage immutabile esistente, si consiglia di adottare un repository con protezione avanzata distribuito tramite Veeam Infrastructure Appliance come percorso consigliato per ottenere l'immutabilità locale.

Per la massima protezione, installare Veeam Infrastructure Appliance su hardware fisico. L'esecuzione di Veeam Infrastructure Appliance come appliance virtuale eredita comunque la superficie di attacco dell'hypervisor. L'immutabilità a livello di file system protegge i file di backup dagli attacchi all'interno del SO, ma un amministratore dell'hypervisor può comunque eliminare le VM, anche se i file di backup sono immutabili.

Percorso B: Veeam Software Appliance + Veeam Data Cloud Vault: Veeam Backup & Replication scrive i backup direttamente nel repository locale su Veeam Software Appliance e ne mantiene una copia off-site in Veeam Vault. Questa soluzione è ideale per micro-PMI, filiali o clienti che desiderano minimizzare la gestione dello storage locale, oltre a ottenere copie immutabili off-site e fisicamente isolate a livello logico tramite Vault. Tieni presente che, se Veeam Software Appliance viene distribuito su un'infrastruttura virtuale, non costituisce un sostituto adeguato per l'immutabilità on-site.

Percorso B: Perché Veeam Software Appliance + Vault?

Path B riduce al minimo l'amministrazione dello storage. Veeam Backup & Replication scrive i backup in un repository locale sulla stessa Veeam Software Appliance, quindi un Backup Copy Job (copia del backup) li replica fuori sede su Vault.

Lo storage locale di Veeam Software Appliance è immutabile per impostazione predefinita, quindi il percorso B garantisce comunque protezione contro il ransomware on-premises. Non è un repository con protezione avanzata formale nel senso del prodotto, quindi il Percorso A rimane la scelta più solida quando si dispone di hardware da dedicare al Veeam Infrastructure Appliance, mentre il Percorso B è la scelta giusta quando non si dispone di hardware. Come per il Percorso A, Veeam Software Appliance in esecuzione come appliance virtuale può comunque essere eliminato a livello di hypervisor, quindi distribuiscilo, ove possibile, su hardware fisico.

Il percorso B salta completamente il passaggio relativo all'appliance Veeam Infrastruttura. Se scegli questo percorso, procedi dal Milestone 2 (implementazione del Veeam Software Appliance) direttamente al Milestone 5 (Backup Copy Job (copia del backup) verso Vault).

Percorso C: Veeam Software Appliance + repository NAS/Windows esistente + Vault o storage off-site alternativo di terze parti: questo percorso sfrutta l'infrastruttura di storage esistente ed è meno robusto localmente, a meno che non vengano applicate ulteriori configurazioni. Questa soluzione è utile quando i clienti desiderano sfruttare i partner VCSP (Veeam Cloud & Service Provider) esistenti per lo storage off-site o per soluzioni alternative di storage off-site già disponibili.

Indipendentemente dal percorso:

- Valuta la possibilità di isolare il traffico di backup su una VLAN o una scheda di rete dedicata, per mantenere i dati di backup separati dalla rete di produzione.
- Rivedi la copertura della licenza per socket/carico di lavoro prima dell'implementazione.

Traguardo 2: Distribuzione di Veeam Software Appliance e infrastruttura

Distribuire Veeam Software Appliance

- Scarica Veeam Software Appliance OVA (per VMware vSphere) o ISO (per server fisici o VM su altri hypervisor supportati) dal Veeam Customer Portal (my.veeam.com).
- Per OVA: importare in VMware vSphere e avviare. Veeam Backup & Replication sarà accessibile tramite l'interfaccia di gestione dopo il primo avvio.
- Per ISO: avvia il server di destinazione (ad esempio, fisico o una VM su qualsiasi altro hypervisor supportato) dall'immagine ISO e segui la procedura guidata. Veeam Backup & Replication viene installato automaticamente.
- Completa la procedura guidata di configurazione iniziale di Veeam Software Appliance e imposta il nome host, le impostazioni di rete e le credenziali di amministratore.

Connetti l'infrastruttura a Veeam Backup & Replication

- Aggiungi la tua piattaforma di virtualizzazione all'inventario di Veeam Backup & Replication (Infrastruttura di backup > Server gestiti).
- Aggiungi almeno un proxy di backup. In ambienti di dimensioni ridotte, Veeam Software Appliance può fungere da proxy iniziale.
- Per gli ambienti VMware, configurare la modalità di trasporto Hot-Add. La VM proxy monta i dischi sorgente tramite SCSI e li legge direttamente, evitando così il percorso NBD più lento sulla rete di gestione di ESXi.

Distribuisci Veeam Infrastruttura Appliance (Percorso A)

- Scarica OVA o ISO di Veeam Infrastructure Appliance dal portale del cliente Veeam.
- Distribuisci utilizzando lo stesso processo OVA/ISO di Veeam Software Appliance. Durante la procedura guidata di configurazione, seleziona "repository con protezione avanzata" o "proxy di backup" come ruolo di destinazione.
- Una volta distribuito, aggiungi Veeam Infrastructure Appliance a Veeam Backup & Replication come Server gestito, quindi configuralo come repository di backup o proxy.
- Per il ruolo di repository con protezione avanzata, aggiungi il repository in Veeam Backup & Replication (infrastruttura di backup > repository di backup) e imposta il periodo di retention dell'immutabilità.
- Igbnora questa sezione se non stai utilizzando il Percorso B o il Percorso C (poiché non è richiesto alcun Veeam Infrastructure Appliance).

Cosa gestisce Veeam Software Appliance per te

Veeam Backup & Replication è preinstallato e pronto per la configurazione, senza necessità di configurazione manuale del SO, installazione manuale del software o applicazione di patch prima dell'implementazione.

Veeam Software Appliance viene fornito pre-hardizzato, i servizi non necessari sono disabilitati, il SO è bloccato e le best practice di sicurezza vengono applicate di default.

Distribuisci come file OVA su VMware vSphere, avvia l'immagine ISO su un server fisico oppure avvia all'interno di una VM su qualsiasi altro hypervisor supportato da Veeam. Non è richiesta esperienza con Linux.

Installa Veeam ONE

- Veeam ONE è un installer separato per Windows. Attualmente non è distribuito come parte del modello appliance.
- Installa Veeam ONE™ su una VM Windows Server o su un host fisico (consulta i requisiti minimi nella Guida all'implementazione di Veeam ONE™).
- Collega Veeam ONE a Veeam Backup & Replication e al tuo host vCenter/Hyper-V durante la procedura guidata di configurazione.
- Configura le impostazioni SMTP e di notifica e-mail immediatamente dopo l'installazione. Gli avvisi devono essere attivi fin dal primo giorno.

Traguardo 3: Primi job di backup

- Crea il tuo primo job di backup per il tuo hypervisor primario. Imposta come destinazione il Veeam repository con protezione avanzata (Percorso A), il repository locale su Veeam Software Appliance (Percorso B) o il tuo repository NAS/Windows esistente (Percorso C).
- Imposta una policy di retention sensata per iniziare: 14 punti di ripristino giornalieri, 4 settimanali, 3 mensili (GFS).
- Programma il lavoro per essere eseguito durante le ore di minore affluenza e verifica che non vada in conflitto con altre finestre di manutenzione.
- Esegui il lavoro manualmente alla prima esecuzione e monitoralo fino al completamento.
- Verifica che il lavoro si completi senza avvisi o errori prima di procedere alla Fase 2.

Test di ripristino: da non saltare!

Prima di passare alla Fase 2, eseguire un Instant VM Recovery per una VM non critica per verificare la recuperabilità.

Non sarai protetto finché non avrai verificato di poter effettuare il ripristino. Questa operazione richiede solo pochi minuti e può prevenire giorni di problemi successivamente.

Cosa gestisce per te Veeam Infrastructure Appliance

Come la Veeam Software Appliance, la Veeam Infrastructure Appliance viene fornita già rinforzata e preconfigurata per il suo ruolo assegnato. Non è richiesta alcuna gestione di Linux dopo l'implementazione.

Una singola Veeam Infrastructure Appliance è dedicata a un solo ruolo: Veeam repository con protezione avanzata o proxy di backup. Se hai bisogno di entrambi, distribuisci due appliance.

Questa appliance presenta gli stessi formati di implementazione della Veeam Software Appliance: OVA per VMware vSphere o ISO per server fisici e altri hypervisor supportati.

FASE 2 • Giorni 15—45

Ottimizzazione

Obiettivo: protezione costante, copia off-site e visibilità nell'ambiente.

Traguardo 4: Elaborazione application-aware

L'elaborazione application-aware garantisce che i backup crash-consistent diventino anche consistenti a livello applicativo. Questo è fondamentale per carichi di lavoro transazionali come SQL Server, Oracle, Exchange, Active Directory e altri carichi di lavoro applicabili.

- Abilita l'elaborazione guest nei job di backup che riguardano server applicazione Windows o Linux.
- Configura l'Elaborazione application-aware per SQL Server, Oracle, Exchange, controller di dominio Active Directory e altri carichi di lavoro applicabili.
- Imposta una politica di troncamento del log delle transazioni laddove applicabile e appropriato alle tue esigenze di ripristino.
- Dopo la prima esecuzione del job application-aware, conferma che i punti di ripristino siano contrassegnati come consistenti a livello applicativo in Veeam Backup & Replication.
- Esegui un ripristino a livello di oggetto di un database SQL (o altri carichi di lavoro applicabili) utilizzando Veeam Explorer for Microsoft SQL Server per confermare che il ripristino end-to-end dell'applicazione funzioni.

Traguardo 5: copia del backup e vault

Questo traguardo completa la tua strategia 3-2-1: una copia locale sul repository principale, più una copia immutabile off-site. Questo è il fondamento architettonico del tuo ambiente di backup.

Collega Vault

- Aggiungi Vault come repository dell'object storage in Veeam Backup & Replication (infrastruttura di backup > repository di object storage).
- Autenticati con le credenziali fornite da Veeam e scegli la tua regione.
- Verifica che l'immutabilità sia abilitata.

Backup Copy Job (copia del backup)

- Configurare i job di backup copy con una policy di retention GFS per mantenere punti di ripristino a lungo termine off-site.
- Verificare che i processi di copia di backup off-site vengano completati con successo e che gli oggetti Veeam Vault mostrino i flag di immutabilità in Veeam Backup & Replication.
- Eseguire un ripristino di prova da Vault per confermare che la copia off-site sia leggibile prima di dichiarare completata la Fase 2.

Percorso C: opzioni di destinazione off-site

I percorsi A e B puntano entrambi a Vault come destinazione per la copia off-site. Il percorso C può utilizzare Vault oppure un VCSP alternativo o un repository off-site di terze parti, se già disponibile. L'immutabilità è applicata per impostazione predefinita su tutti i dati di backup archiviati in Vault. Se si utilizza una posizione esterna a Vault, verificare che l'immutabilità o il blocco degli oggetti siano configurati su tale repository.

Traguardo 6: Monitoraggio, allertamento e configurazione dell'orchestratore

- Configura i destinatari delle notifiche di allarme in Veeam ONE: avvisi via e-mail per fallimenti dei processi e mancato rispetto degli accordi sul livello di servizio (SLA).
- Definisci gli orari di lavoro in Veeam ONE per allineare i calcoli degli SLA al tuo programma operativo.
- Rivedi le soglie di allarme predefinite: disattiva o regola gli allarmi non pertinenti al tuo ambiente per evitare l'affaticamento da allarmi.
- Esegui i tuoi primi report di Veeam ONE: report delle VM protette e report delle sessioni di lavoro.
- Esamina il report sulle VM non protette e affronta eventuali lacune individuate prima di procedere alla Fase 3.

Installa Veeam Recovery Orchestrator (solo versione Premium)

Salta questa sezione se la tua edizione è Foundation o Advanced. Veeam Recovery Orchestrator è incluso solo con Veeam Data Platform Premium.

- Veeam Recovery Orchestrator è un programma di installazione separato basato su Windows. Può risiedere insieme a Veeam ONE sullo stesso host Windows oppure essere eseguito su un host separato.
- Installa Veeam Recovery Orchestrator su una VM Windows Server o su un host fisico. Consulta i requisiti minimi nella Guida all'implementazione di Veeam Recovery Orchestrator.
- Durante la procedura guidata di configurazione, collega Veeam Recovery Orchestrator alla tua istanza di Veeam Backup & Replication così che possa inventariare le tue catene di backup esistenti.
- Collega Veeam Recovery Orchestrator al tuo vSphere, Hyper-V o Microsoft Azure in modo che l'esecuzione pianificata possa avviare le VM e assegnare correttamente le reti.
- Facoltativamente, collega Veeam Recovery Orchestrator a Veeam ONE per monitoraggio dei dati più completi e verifiche basate su DataLab.
- Applica la tua licenza Veeam Data Platform Premium per attivare Veeam Recovery Orchestrator.
- Configura SMTP/e-mail affinché le notifiche di esecuzione pianificata funzionino fin dal primo giorno.

FASE 3 • Giorni 46—75

Resilienza dei dati e resilienza dei processi aziendali

Obiettivo: colmare le lacune di protezione, migliorare i valori di RTO/RPO e aumentare la resilienza contro i ransomware.

Traguardo 7: Colmare le lacune di copertura

- Esegui il report delle VM non protette in Veeam ONE per affrontare tutti i carichi di lavoro non protetti prima di qualsiasi altra ottimizzazione.
- Estendi la protezione ai carichi di lavoro fisici utilizzando Veeam Agent *for Microsoft Windows* o Veeam Agent *for Linux* a seconda delle necessità.
- Esamina i programmi di lavoro per individuare eventuali conflitti e scaglionate gli orari di inizio per evitare contese tra le risorse del proxy e del repository.
- Verifica la conformità all'RPO: tutte le VM critiche stanno generando punti di ripristino entro la finestra di ripristino definita?
- Verifica che tutte le attività vengano completate entro la finestra di backup definita.

Aggiunta della capacità del proxy con un secondo VIA

Se i job di backup sono lenti o superano la finestra di backup, distribuisci una seconda Veeam Infrastructure Appliance nel ruolo di proxy.

Il modello di appliance pre-hardened rende questa operazione rapida: distribuisci l'OVA o l'ISO, registrala in Veeam Backup & Replication e i job verranno automaticamente sottoposti a bilanciamento del carico su entrambi i proxy senza necessità di configurazione manuale dei proxy.

Traguardo 8: prontezza contro il ransomware

- Veeam Data Platform Advanced e Premium includono due strumenti di sicurezza complementari. Il primo è Recon, il servizio di threat intelligence di Veeam che rileva gli IOC (Indicatori di Compromissione) e dati emergenti basati sulla risposta a incidenti reali. La seconda è scan backup, un'azione integrata in Veeam Backup & Replication. Esamina le catene di backup esistenti alla ricerca di indicatori di malware e valida l'integrità dei file, senza la necessità di una rete isolata o di avviare VM.

Avvia uno scan backup:

- Crea un job SureBackup in Veeam Backup & Replication nella sezione Home > SureBackup. SureBackup viene eseguito come job programmato e può analizzare i backup alla ricerca di malware, minacce basate su firme e integrità dei file in un unico flusso, senza richiedere una rete isolata o l'avvio di una VM per la scansione stessa.

- Collega i job di backup che vuoi coprire, così nel tempo il job SureBackup® abbraccerà tutti i tuoi dati: Veeam repository con protezione avanzata (Percorso A), repository locale Veeam Software Appliance (Percorso B), il repository NAS/Windows esistente (Percorso C) e Vault.
- Nelle opzioni di verifica, abilita la scansione malware con Veeam Threat Hunter (o una soluzione antivirus di terze parti) per verificare il contenuto del backup rispetto a un database aggiornato delle firme delle minacce.
- Nelle stesse opzioni di verifica, abilita il controllo di integrità del file per convalidare il file di backup tramite un controllo CRC e identificare eventuali blocchi danneggiati.
- Pianifica il job SureBackup® e rivedi regolarmente i risultati della sessione; esamina attentamente eventuali punti di ripristino segnalati prima di utilizzarli per il ripristino.
- Per un controllo ad hoc tra le esecuzioni programmate, vai su Home > Backups, espandi il job di backup, seleziona il carico di lavoro e scegli "Scansiona backup" dalla scheda Backup.

Installa Recon

- Installa il binario di Recon su qualsiasi host dell'infrastruttura Veeam basato su Windows o su qualsiasi host Linux a tua scelta.
- Recon può essere installato anche sui controller di dominio Windows supportati.
- Recon non può essere installato su Veeam Infrastructure Appliance. Le Veeam Infrastructure Appliance sono dedicate a un solo ruolo e pre-rafforzate.

Verifica dell'immutabilità

- Verifica che il periodo di immutabilità sul repository con protezione avanzata del tuo Veeam Infrastructure Appliance sia impostato su una finestra di retention appropriata.
- Rivedi le impostazioni di crittografia dei backup ed abilita la crittografia a riposo sui job se non già configurata.
- Genera il report "Carichi di lavoro immutabili" di Veeam ONE™ per misurare e identificare i target di immutabilità dei backup dei carichi di lavoro.

Prontezza al ripristino dal ransomware

Documenta un semplice runbook di ripristino che includa quali VM ripristinare per prime, da quali punti di ripristino e verso quale destinazione.

Identifica almeno un punto di ripristino pulitoe pre-infezionein Vault come ultimo punto di riferimento valido conosciuto.

Le copie immutabili non possono essere sovrascritte o crittografate durante il periodo di immutabilità. Questa è la tua rete di sicurezza.

Percorso A: Veeam repository con protezione avanzata più Vault.

Percorso B: storage locale di Veeam Software Appliance più Veeam Vault.

Path C: Vault più il tuo repository locale se hai configurato l'immutabilità lì.

Traguardo 9: Ottimizzazione delle prestazioni e piani di orchestrazione

- Esamina il throughput del proxy nelle statistiche delle attività di backup di Veeam Backup & Replication. Se le attività di backup sono soggette a colli di bottiglia, distribuisci una seconda Veeam Infrastructure Appliance nel ruolo di proxy.
- Verifica che la modalità di trasporto del backup sia ottimale: Hot-Add (VMware) o Direct Storage Access, ove disponibile.
- Verifica che tutti i job di backup siano stati completati entro la finestra di manutenzione definita.
- Esamina i grafici delle prestazioni di Veeam ONE™ e identifica le VM con tassi di modifica insolitamente elevati che potrebbero trarre vantaggio da attività dedicate o da pianificazioni modificate.

Crea i piani di orchestrazione iniziali (solo per l'edizione Premium)

Salta questa sezione se la tua edizione è Foundation o Advanced, oppure se non stai utilizzando un hypervisor supportato per Veeam Recovery Orchestrator.

Veeam Recovery Orchestrator trasforma il runbook di ripristino manuale in un piano eseguibile. Creare i piani ora consente alla Fase 4 di verificare automaticamente la recuperabilità, invece di ripetere i ripristini manuali.

- Identifica gli stack applicativi di livello 1 che necessitano di un ripristino orchestrato (ad esempio, controller di dominio, database principale, server applicativi principali).
- In Veeam Recovery Orchestrator, crea il tuo primo piano di ripristino che copra uno di questi stack.
- Definisci l'ordine di avvio delle VM e le dipendenze, in modo che i prerequisiti (ad esempio, DC, DNS, ecc.) vengano avviati prima dei servizi dipendenti.
- Configura le destinazioni di ripristino (ad esempio host, cluster, datastore) e mappa la rete di produzione per il failover reale, nonché una rete isolata per i test.
- Imposta gli obiettivi RTO e RPO del piano affinché Veeam Recovery Orchestrator possa segnalare eventuali deviazioni nel tempo.
- Salva il piano e rivedi la documentazione generata automaticamente con gli stakeholder prima di dichiarare completata la Fase 3.

FASE 4 • Giorni 76—100

Dimostra il valore e rendi operativo

Obiettivo: Verificare la recuperabilità, stabilire un'igiene continua e dimostrare il ritorno sull'investimento (ROI).

Traguardo 10: Test di ripristino

L'unico backup che conta è quello da cui è possibile effettuare un ripristino. La fase 4 è quella in cui dimostri — con evidenze documentate — che il tuo ambiente soddisfa i requisiti RTO e RPO.

SureBackup e scan backup

- Configura un SureBackup® Gruppo di applicazione che copra le VM più critiche (ad esempio, controller di dominio, Server applicazione principali).
- Esegui un job di SureBackup® per automatizzare la verifica dell'avvio e confermare che le VM si avviino e superino i test di heartbeat, ping e a livello di applicazione.
- Per una verifica più leggera, esegui un Scan Backup. Consente di verificare l'integrità dei file e di controllare la presenza di minacce senza avviare le VM, rappresentando un complemento pratico o un'alternativa a SureBackup® in ambienti più piccoli.

Test di ripristino granulare e completo

- Test di ripristino a livello di file e ripristinare singoli file da un backup in una posizione di test.
- Verifica il ripristino di elementi applicativi ripristinando oggetti del database SQL o utenti di Active Directory tramite Veeam Explorers™.
- Esegui un ripristino completo di VM da Vault per simulare la perdita totale on-premises e convalidare la copia off-site.
- Registra i tempi di ripristino effettivi, confrontali con i tuoi obiettivi RTO e documenta i risultati.

Best practice per il test di ripristino

Ripristinare sempre su una destinazione non di produzione e non sovrascrivere mai i carichi di lavoro in produzione durante un test.

Documentare cosa è stato ripristinato, da quale punto di ripristino, a quale destinazione e quanto tempo ci è voluto.

Questi risultati sono la prova della recuperabilità. Conservarli per verifiche di conformità, audit e report per la gestione.

Esegui piani di orchestrazione (solo Premium)

Salta questa sezione se la tua edizione è Foundation o Advanced, oppure se il tuo hypervisor non è supportato da Veeam Recovery Orchestrator. La Fase 3 ha creato il tuo primo piano di ripristino, ma la Fase 4 è dove si dimostra davvero utile.

- Esegui un test di prontezza non presidiato sul tuo piano. Veeam Recovery Orchestrator verifica la disponibilità dei punti di ripristino, la capacità della destinazione e il drift di configurazione, senza dover avviare alcuna VM.
- Esegui un test DataLab sul tuo piano. Veeam Recovery Orchestrator ripristina lo stack applicativo in una rete isolata ed esegue controlli di verifica a livello applicativo sulle VM dal vivo.
- Registra i tempi di ripristino effettivi dal test DataLab e confrontali con il target RTO impostato nella Fase 3.
- Genera il report di preparazione al ripristino di Veeam Recovery Orchestrator e archivialo insieme agli altri risultati dei test di ripristino.
- Per i carichi di lavoro non coperti da un piano di Veeam Recovery Orchestrator, ricorri ai test di ripristino manuali descritti sopra.

Traguardo 11: Reportistica e documentazione

Genera un report mensile Executive Summary di Veeam ONE™ e condividilo con il management per dimostrare lo stato di salute del backup e la copertura del backup.

- Esporta un report di inventario dei carichi di lavoro protetti per confermare l'ambito di copertura.
- Documenta l'architettura finale del backup, includendo l'elenco dei job, la struttura del repository, i ruoli del Veeam Infrastructure Appliance, le pianificazioni e le policy di retention.
- Esamina il consumo di storage di Veeam Vault e verifica che l'utilizzo sia in linea con il budget previsto.
- Archivia i risultati dei test di ripristino insieme alla documentazione dell'architettura.
- Solo per utenti Premium: genera mensilmente il report di preparazione al ripristino di Veeam Recovery Orchestrator. Monitora il punteggio di prontezza nel tempo, al variare dei carichi di lavoro e delle dipendenze.
- Solo per la versione Premium: archivia la documentazione del piano generata da Veeam Recovery Orchestrator insieme alla documentazione dell'architettura. Veeam Recovery Orchestrator rigenera automaticamente la documentazione quando i piani cambiano; pertanto, archivia nuovamente manualmente quando i piani vengono aggiornati.

Traguardo 12: cadenza continua delle pratiche di igiene

Entro il centesimo giorno, il tuo ambiente dovrebbe essere stabile e completamente documentato. Queste abitudini lo mantengono così:

- **Settimanalmente:** esamina la dashboard dello stato di salute dei tuoi job Veeam ONE e risolvi tempestivamente eventuali errori o avvisi.
- **Settimanalmente:** esamina il report delle VM non protette in Veeam ONE™ e aggiungi la protezione per eventuali nuove VM.
- **Mensilmente:** esegui un executive summary e report sulle VM protette e condividi i risultati.
- **Mensilmente:** esamina il consumo dello storage Vault e il tasso di crescita. Segnala se stai superando l'impiego di risorse previsto dal budget o se sono previsti aumenti della retention.
- **Mensilmente:** conferma che le finestre di retention siano ancora attive e non modificate.
- **Trimestralmente:** esegui un test di ripristino documentato e ruota i tipi di carico di lavoro.
- **Trimestralmente:** esegui una scansione di backup su ciascun repository per verificare la presenza di firme malware e alterazioni dell'integrità dei file.
- **Trimestrale:** verifica chi ha accesso amministrativo a Veeam Backup & Replication, Veeam ONE e Veeam Recovery Orchestrator (solo Premium). Rimuovi l'accesso a chiunque abbia cambiato ruolo o sia uscito.
- **Trimestrale (solo Premium):** esegui un test Veeam Recovery Orchestrator DataLab e alterna quale piano di orchestrazione viene esercitato.
- **Trimestrale (solo Premium):** rigenera e archivia la documentazione dei piani di Veeam Recovery Orchestrator se qualche piano è cambiato dall'ultima revisione.
- **Mensile:** esamina gli aggiornamenti di intelligence sulle minacce di Recon e applica le firme o le regole pertinenti al tuo ambiente.

- **Annualmente:** rivedi l'architettura di backup e le policy di retention in base ai requisiti aziendali attuali e a eventuali nuovi obblighi di conformità.
- **Annualmente:** esegui un ripristino completo dal Vault per verificare che la copia off-site sia recuperabile end-to-end. Documenta il risultato.
- **Annualmente:** esamina le impostazioni di crittografia durante il trasferimento e a riposo e ruotare le chiavi in conformità alla policy di sicurezza.
- **Se necessario:** pianifica la cadenza di aggiornamento dei componenti Veeam (ad esempio, Veeam Software Appliance, Veeam Infrastructure Appliance, Veeam ONE, agenti Veeam e Veeam Recovery Orchestrator, se applicabile) e iscriviti alle notifiche sui rilasci.
- **Prima del rinnovo:** esamina l'utilizzo della licenza, le proiezioni di crescita e l'adeguatezza dell'edizione. Se hai superato le funzionalità offerte dalla tua edizione, questo è il momento di discutere un upgrade con il tuo rappresentante Veeam.

Raccomandazioni finali

Complimenti! Ce l'hai fatta.

In 100 giorni, sei passato dalla fase di implementazione a un ambiente di protezione dei dati pienamente operativo. I tuoi carichi di lavoro sono protetti, i tuoi backup sono robusti e immutabili, e hai dimostrato di poter effettuare il ripristino non solo in teoria, ma anche con evidenza documentata.

Non è una cosa da poco.

Ora l'attenzione si sposta dalla costruzione alla manutenzione. Eseguite regolarmente test di ripristino, adattate le policy man mano che il vostro ambiente si evolve e utilizzate la frequenza di monitoraggio e reporting per individuare eventuali deviazioni prima che si trasformino in rischi. Le abitudini che hai stabilito nel Milestone 12 — la tua cadenza di igiene settimanale, mensile, trimestrale e annuale — sono ciò che mantiene il tuo ambiente conforme e affidabile ben oltre il Giorno 100. Segui queste abitudini, appropriati di esse e falle evolvere man mano che la tua organizzazione cresce.

Ricorda, il giorno 100 non è il traguardo. È la baseline di riferimento. La resilienza è una pratica, non un progetto.

Mantieni aggiornati i ruoli amministrativi affinché le persone giuste abbiano sempre i livelli di accesso appropriati, e rimani iscritto alle Note di release e agli avvisi di sicurezza di Veeam per non farti mai trovare impreparato.

Non devi farlo da solo

Le community, le risorse formative e i team tecnici di Veeam esistono per supportarti nel tuo percorso. Sfrutta queste risorse man mano che il tuo ambiente cresce e matura! Un elenco selezionato di risorse è disponibile in appendice.

Per domande o per i prossimi passi, contatta il tuo Account Manager del Successo del Cliente oppure l'Assistenza Tecnica Veeam per richieste tecniche.

Appendice: riferimento rapido

Componenti chiave: Veeam Data Platform

- **Veeam Software Appliance:** un'appliance pre-hardened con Veeam Backup & Replication preinstallato. Distribuire come OVA (VM) o ISO (fisico). Questo è il punto di partenza consigliato **per** tutte le implementazioni per le PMI.
- **Veeam Infrastructure Appliance:** un'appliance pre-hardenizzata distribuita come proxy di backup dedicato o repository con protezione avanzata. Offre immutabilità locale senza competenze Linux, con un solo ruolo per appliance.
- **Veeam Backup & Replication:** motore principale di backup, ospitato su Veeam Software Appliance. Gestisce job, repository, proxy e operazioni di ripristino.
- **Veeam ONE:** gestisce il monitoraggio, gli avvisi e la reportistica. Dispone di un'installazione separata basata su Windows e si collega a Veeam Backup & Replication e all'hypervisor per una visibilità completa dello stack.
- **Recon:** questo è il servizio di threat intelligence di Veeam. Fa emergere indicatori di compromissione (IOC), firme di minaccia e dati sulle campagne emergenti, desunti dalla risposta agli incidenti nel mondo reale. Incluso in Veeam Data Platform Advanced.
- **Scansione del contenuto del backup:** questa è un'azione integrata nel prodotto che analizza le catene di backup esistenti alla ricerca di firme di malware note e verifica l'integrità dei file senza richiedere una rete isolata o l'avvio di VM. Incluso in Veeam Data Platform Advanced.
- **Veeam Recovery Orchestrator:** una piattaforma di orchestrazione che automatizza il Disaster Recovery (DR) a livello di applicazione. Consente di creare piani di ripristino eseguibili, eseguire test di preparazione, effettuare verifiche basate su DataLab e generare documentazione di ripristino. Incluso con Veeam Data Platform Premium.
- **Veeam Data Cloud Vault:** questo fornisce uno storage di oggetti cloud immutabile per copie off-site. È gestito da Veeam, non è necessario un account cloud separato.

Termini chiave

- **Recovery Point Objective (RPO):** massima perdita di dati accettabile, misurata in tempo. Influenza la frequenza con cui vengono pianificati i backup.
- **Recovery Time Objective (RTO):** tempo massimo di interruzione accettabile prima che un carico di lavoro debba essere ripristinato.
- **GFS (Grandfather-Father-Son):** schema di retention che mantiene punti di ripristino giornalieri, settimanali e mensili.
- **Immutabilità:** dati di backup che non possono essere modificati o eliminati per un periodo di retention definito. Protegge i file di backup dalla crittografia dei ransomware.
- **Instant VM Recovery:** consente di ripristinare una VM direttamente da un backup in pochi secondi, senza dover prima copiare i dati. Eseguire sempre la migrazione allo storage di produzione dopo la convalida.
- **Piano di orchestrazione (Veeam Recovery Orchestrator):** un runbook eseguibile che definisce l'ordine, le dipendenze, le posizioni di destinazione e le mappature di rete per il ripristino di un insieme di carichi di lavoro. Sostituisce un runbook di ripristino manuale con un'automazione auto-documentata e testabile.
- **DataLabs:** ambiente di test isolato in cui Veeam Recovery Orchestrator (o SureBackup) ripristina un backup ed esegue la verifica a livello di applicazione senza influire sull'ambiente di produzione. Consente di testare il piano completo a qualsiasi cadenza.
- **Elaborazione application-aware:** elaborazione guest che crea punti di Backup uniformi tra le applicazioni per SQL Server, Oracle, Exchange, Active Directory, SharePoint, PostgreSQL e MySQL. Utilizza VSS su Windows e script di pre-freeze/post-thaw, oltre alla quiescenza nativa del database su Linux.
- **Veeam Hardened Repository:** un repository di backup basato su Linux con immutabilità garantita a livello di filesystem. Veeam Infrastructure Appliance offre un repository con protezione avanzata preconfigurato che non richiede alcuna amministrazione Linux. Object storage e object lock sono meccanismi di immutabilità separati, non sono Veeam Hardened Repositories. L'immutabilità a livello di file system protegge dagli attacchi all'interno del SO, ma non dalla distruzione a livello di VM. Un Veeam repository con protezione avanzata in esecuzione come appliance virtuale può comunque essere eliminato a livello di hypervisor; pertanto, per la massima protezione, è consigliabile distribuire Veeam Infrastructure Appliance su hardware fisico.
- **Modalità di trasporto Hot Add:** si tratta di un trasporto di backup specifico di VMware. La VM proxy esegue il Hot Add dei dischi virtuali della VM di origine e li legge tramite SCSI, evitando il percorso NBD sulla rete di gestione ESXi.

Appendice: Link utili

Il mio account

Il tuo Account Veeam è il centro nevralgico per la gestione della tua implementazione. Una volta effettuato l'accesso, è possibile scaricare prodotti e chiavi di licenza, gestire Amministratori delle richieste di supporto, contattare Veeam Support e rinnovare i contratti o aggiungere licenze.

- Accedi o crea il tuo account Veeam
- Come creare un account
- FAQ sull'accesso
- Gestione dei ruoli di amministratore delle licenze e/o dei casi

Documentazione e Download

- Centro assistenza con Documentazione tecnica, guida all'implementazione e Guide utente
- Download dei prodotti, inclusi aggiornamenti software, patch e Note di release
- Knowledge Base di Supporto con problemi comuni, passaggi di risoluzione dei problemi e soluzioni consigliate, regolarmente aggiornata da Veeam Support e dai team di ingegneria di Veeam

Apprendimento e best practice

- Webinar di onboarding in diretta: webinar di onboarding regolari in diretta dove puoi fare domande in tempo reale e ascoltare direttamente gli specialisti tecnici
- Veeam University FREE: corsi a proprio ritmo e certificazioni gratuite
- Calcolatori di dimensionamento Veeam: strumento di dimensionamento e stima online utilizzato percalcolarei requisiti di infrastruttura, storage e capacità per le implementazioni Veeam
- Procedure consigliate dagli Architetti della soluzione Veeam: guida alla progettazione e alla configurazione dell'infrastruttura basata su implementazioni reali, che vale la pena rivedere man mano che il tuo ambiente matura
- Suggerimenti pratici per Veeam Intelligence: una raccolta curata di suggerimenti efficaci per aiutarti a sbloccare tutto il potenziale di Veeam Intelligence
- Veeam Search: il portale di ricerca centralizzato di Veeam per cercare tra le risorse Veeam da un unico punto

Veeam Community

- Forum della community Veeam: connettiti con i tuoi colleghi, condividi le best practice, partecipa ai gruppi di utenti e agli eventi della community e discuti casi d'uso reali
- Forum di ricerca e sviluppo Veeam: il tuo collegamento diretto con il team di ricerca e sviluppo Veeam per discussioni sui prodotti, domande tecniche e feedback sulle funzionalità

Informazioni su Veeam Software

Veeam è l'azienda di fiducia per dati e IA, specializzata nell'aiutare le organizzazioni a garantire che i loro dati e la loro IA siano pienamente compresi, protetti e resilienti, al fine di accelerare l'adozione di un'IA sicura su larga scala. In qualità di leader di mercato nella resilienza dei dati e nella gestione della postura di sicurezza dei dati, Veeam è progettata per la convergenza di identità, dati, sicurezza e rischi legati all'intelligenza artificiale.

Con sede a Seattle e uffici dislocati in oltre 30 Paesi, Veeam protegge più di 550.000 clienti in tutto il mondo, incluso l'82% delle aziende Fortune 500.

Per saperne di più, è possibile visitare www.veeam.com o seguire Veeam su LinkedIn @veeam-software e X @veeam.