



Il tuo percorso verso la resilienza con Veeam Kasten

Una roadmap per i tuoi primi 100 giorni e oltre.





Questa guida accompagna gli amministratori IT nell'implementazione, configurazione e operatività di Veeam Kasten for Kubernetes. Che venga installato tramite Helm o Marketplace, il percorso di implementazione è progettato per essere rapido, sicuro e accessibile. Entro il giorno 100, avrai un ambiente di backup nativo di Kubernetes con esportazioni offsite immutabili, integrato con i tuoi strumenti e applicazioni, nonché un runbook di ripristino documentato.

Il tuo viaggio di 100 giorni

FASE 1 Fondamenta Giorni 1—14	FASE 2 Rafforzare le basi Giorni 15—45	FASE 3 Ottimizzazione e rafforzamento Giorni 46—75	FASE 4 Dimostrazione del valore Giorni 76—100
M1: Dimensionamento e pianificazione	M4: Gestione centralizzata	M7: Integrazione dell'osservabilità	M10: Test di ripristino
M2: Distribuire Veeam Kasten	M5: Elaborazione application-aware	M8: Resilienza migliorata	M11: Documentazione e reportistica
M3: Primi job di backup	M6: Best practice di policy	M9: Colma le lacune di copertura	M12: Igiene operativa continua

Sintesi della roadmap

Fase	Nome	Tempistica	Focus
FASE 1	Foundation	Giorni 1—14	Pianifica l'ambiente, distribuisce Veeam Kasten ed esegui i primi job di backup.
FASE 2	Rafforza le basi	Giorni 15—45	Gestione centralizzata, elaborazione consapevole delle applicazioni e best practice sulle policy.
FASE 3	Ottimizzare e rafforzare	Giorni 46—75	Osservabilità, resilienza e DR e colmare le lacune di copertura.
FASE 4	Verifica del valore	Giorni 76—100	Test di ripristino, documentazione e manutenzione costante.



Come utilizzare questa Guida

I giorni sono linee guida, non scadenze rigide. Gli ambienti di piccole dimensioni potrebbero comprimere la Fase 1 in una settimana, mentre quelli complessi potrebbero estendere la Fase 3.

Ogni traguardo si basa sul precedente, per cui si consiglia di seguire i passaggi in ordine.

Riquadri di testo evidenziano, lungo tutto il documento, punti decisionali, opzioni di architettura e insidie comuni da tenere in considerazione.



Indice

FASE 1 • Foundation	4
Traguardo 1: Dimensionamento e pianificazione	4
Traguardo 2: Distribuzione di Veeam Kasten	7
Traguardo 3: Primi job di backup	7
FASE 2 • Rafforza le basi	9
Traguardo 4: Gestione centralizzata (MCM)	9
Traguardo 5: Elaborazione application-aware	9
Traguardo 6: Best practice per le policy	10
FASE 3 • Ottimizzare e rafforzare	11
Traguardo 7: Integrazione dell'osservabilità	11
Traguardo 8: Resilienza e DR migliorata	11
Traguardo 9: Messa a punto	13
FASE 4 • Dimostra il valore e rendi operativo	14
Traguardo 10: Test di ripristino	14
Traguardo 11: Documentazione e reportistica	15
Traguardo 12: Stabilire una cadenza continua delle pratiche di igiene	15
Appendice: Riferimento rapido	16
Componenti chiave: Integrazione con Veeam	16
Termini chiave	16



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 alla pianificazione. La maggior parte delle difficoltà legate all'implementazione di un ambiente stabile e ben protetto possono essere evitate prestando la dovuta attenzione a questa fase.

Inventario dei carichi di lavoro

- Documentare il carico di lavoro totale e il numero di Macchine virtuali (VM), l'impiego di risorse (ad esempio, dimensione del volume/numero di file) e il tasso giornaliero di variazione stimato.
- Identificare i carichi di lavoro più critici. Questi determinano i tuoi obiettivi Recovery Point Objective e Obiettivo Recovery Time Objective (RPO e RTO).
- Annotare eventuali database e carichi di lavoro che potrebbero beneficiare dell'elaborazione application-aware.

Dimensionamento e pianificazione dell'implementazione di Veeam Kasten

- Veeam Kasten ha [requisiti di sistema minimi](#) e i valori predefiniti sono generalmente sufficienti.
- Scegli il metodo di implementazione, ovvero Marketplace/Operatore (consigliato quando possibile) oppure Helm. È possibile cambiare metodo dopo l'installazione, se necessario.
- Verifica che la tua Versione di Kubernetes sia [compatibile](#) con l'ultima Versione di Veeam Kasten. Altrimenti, dovrai prima fare l'upgrade di Kubernetes oppure utilizzare una versione precedente di Kubernetes.
- Determina se questo ambiente è [fisicamente isolato](#). In tal caso, potrebbe essere necessario trasferire le immagini di Veeam Kasten in un registro locale disponibile offline tramite il marketplace del fornitore, oppure inserire il nostro registro nella whitelist.
- Pianifica la rete di backup isolando il traffico di backup su una VLAN dedicata: è una best practice di sicurezza ed è possibile con Kubernetes a seconda della CNI.

Helm VS Marketplace

Helm: Questa è la soluzione più flessibile e compatibile con tutte le distribuzioni Kubernetes.

Marketplace/Operatore: Il ciclo di vita di implementazione e upgrade è più semplice e supporta gli stessi parametri di personalizzazione di Helm. Viene comunemente utilizzato anche con Red Hat OpenShift.

Il compromesso: Potrebbe verificarsi un ritardo nella ricezione delle nuove versioni tramite il marketplace. Gli aggiornamenti sono disponibili immediatamente su Helm, ma i fornitori del marketplace spesso posticipano le nuove versioni per uno o più giorni per effettuare i test di validazione.

Architettura di storage del carico di lavoro

- **Storage compatibile con snapshot:** Veeam Kasten è compatibile con praticamente qualsiasi [driver di storage CSI](#) che supporta gli snapshot, nonché con [integrazione storage diretta](#).
- **Altri tipi di storage (ad esempio NFS generico, disco locale, ecc.):** Veeam Kasten può comunque proteggere questi carichi di lavoro, ma la mancanza di una vera capacità di snapshot influisce sull'affidabilità e sulle prestazioni dei backup. Raccomandiamo fortemente di eseguire l'upgrade all'utilizzo di volumi dotati di capacità di snapshot, ma [GSB](#) o [NFS tar](#) possono essere usati se ne accettate le limitazioni intrinseche.

Architettura dello storage di backup: panoramica delle opzioni

La scelta dello storage determina la resilienza e la disponibilità dei dati di backup. Ecco una panoramica generale dei pro e dei contro di ciascun tipo di storage di backup che puoi configurare come profilo della posizione (location).

Veeam Kasten + Veeam Vault

Le snapshot vengono esportate su uno storage di oggetti immutabile off-site e logicamente fisicamente isolato tramite Veeam Vault. Non è necessaria alcuna configurazione o manutenzione avanzata.

Veeam Kasten + Veeam Backup & Replication Repository

Gli snapshot vengono esportati nell'infrastruttura gestita di Veeam Backup & Replication, inclusi Veeam Hardened repository e Scale-Out Backup Repository (SOBR). È richiesta la modalità a blocchi.

Nota: Le versioni precedenti alla 9.x richiedono anche un piccolo profilo della posizione (location) aggiuntivo (Vault/Object/NFS/CIFS) per i metadati.

Veeam Kasten + Object Storage

Le snapshot vengono esportate su object storage (ad esempio, S3, cloud), che dovrebbe essere configurato come fuori sede e immutabile.

Veeam Kasten + NFS/CIFS

Gli snapshot esportati direttamente su NFS/CIFS sono generalmente incapaci di garantire l'immutabilità, anche su dispositivi WORM-capable, poiché sarebbe necessario il versioning per funzionare. Questa opzione è pienamente supportata, ma non è consigliata a meno che non si disponga anche di duplicati o copie immutabili in remoto.

Veeam Kasten + Profili di posizione multipli

Le snapshot vengono esportate in almeno due posizioni. Se progettata correttamente, utilizzando almeno un'opzione immutabile, questa può essere il percorso più resiliente. **Nota:** le versioni precedenti alla 9.x richiedono più criteri, utilizzando 1 profilo della posizione (location) per criterio.

Le modalità di storage determinano le capacità

A seconda del tipo di storage, potresti avere le seguenti opzioni disponibili:

Modalità volume: file o blocco. Entrambi sono compatibili con Veeam Kasten (ad esempio Ceph FS o RBD).

Modalità di esportazione: file o blocco. Entrambe le modalità sono possibili con Veeam Kasten.

Se un volume è in modalità blocco, potresti essere in grado di esportare le snapshot in modalità blocco. Questa opzione offre funzionalità speciali, come CBT (quando disponibile) ed esportazione verso un repository Veeam Backup & Replication.





Utilizzo di Veeam Backup & Replication + Veeam Infrastructure Appliance (VIA) come repository con protezione avanzata

Per coloro che non dispongono di storage immutabile esistente, integrare Veeam Kasten con Veeam Backup & Replication e distribuire [VIA](#) potrebbe essere un percorso ragionevole per ottenere l'immutabilità locale.

Un repository con protezione avanzata fornisce backup locali immutabili, il che significa che il ransomware non può crittografarli o eliminarli durante il periodo di retention. Il SO è protetto contro gli accessi non autorizzati e idealmente dovrebbe essere eseguito su un server fisico protetto anziché su una VM.

Tradizionalmente, un repository con protezione avanzata richiede l'installazione e il hardening manuale di una distribuzione Linux. VIA elimina questa barriera per intero, poiché è già hardenizzato e si distribuisce tramite ISO avviabile. Può anche essere installato autonomamente su hardware compatibile o acquistato da un fornitore come dispositivo certificato.



Traguardo 2: Distribuzione di Veeam Kasten

Distribuire Veeam Kasten

- Utilizzare il [pre-flight tool](#) per verificare che i requisiti siano soddisfatti (facoltativo).
- Metodo tramite marketplace/operatore: consulta i dettagli delle istruzioni [qui](#).
- Metodo Helm: vedi i dettagli delle istruzioni [qui](#).

Integrazione dell'accesso e dell'autenticazione alla dashboard

- Per accedere alla dashboard dall'esterno, aggiungi un [Ingress o rotta](#) a Veeam Kasten.
- È una best practice integrare con il provider di autenticazione [della tua distribuzione](#) (ad esempio OpenShift Auth), ma sono possibili anche altre opzioni come LDAP diretto.
- Una volta visualizzata la dashboard di Veeam Kasten, è possibile procedere con i passaggi seguenti.

Connetti l'infrastruttura a Veeam Kasten

- Se applicabile, ([vSphere/cloud/altri](#)) aggiungi un profilo di infrastruttura per l'integrazione storage.
- Aggiungi un profilo della posizione (location) per definire la destinazione del backup.

Traguardo 3: Primi job di backup

Backup negli ambienti Kubernetes

Le snapshot di storage sono una potente funzionalità che Kubernetes comprende e può gestire nativamente, a condizione che siano supportate dal provider di storage.

Veeam Kasten sfrutta questa capacità o l'integrazione diretta per attivare snapshot che risiedono localmente sul dispositivo di storage. Veeam Kasten può quindi utilizzare queste snapshot per esportare in modo affidabile i dati in un profilo della posizione (location) esterno (ad esempio, NFS, S3, repository VBR, Vault, ecc.).

Questo metodo consente di ottenere la massima velocità e coerenza, utilizzando al contempo funzionalità e API native di Kubernetes per la massima compatibilità.

Cosa serve per iniziare?

Veeam Kasten, essendo un'applicazione nativa di Kubernetes, richiede che l'utente che la installa abbia accesso tramite kubectl all'ambiente di destinazione, privilegi di amministratore del cluster e, idealmente, anche accesso all'interfaccia di gestione della propria distribuzione, se presente.

Suggerimento: Se riscontri degli errori, puoi trovare le soluzioni sui nostri [siti Community](#) e [KB](#).



- Maggiori informazioni su [come proteggere le VM KubeVirt](#) se applicabile al tuo ambiente.
- Crea la tua prima policy di backup e impostala sul tuo profilo della posizione (location).
- Imposta una policy di retention ragionevole per iniziare: 1 snapshot locale al giorno, con esportazioni nel profilo della posizione (location) impostate per una retention di 1 giornaliera, 4 settimanali e 3 mensili.
- Programma il job per essere eseguito durante le ore di minore affluenza e verifica che non vada in conflitto con altre finestre di manutenzione.
- Esegui il job manualmente alla prima esecuzione e monitoralo fino al completamento.
- Verifica che il job si completi senza avvisi o errori prima di procedere alla Fase 2.

Locale VS Esportazione

Ricorda che le snapshot sono locali solo al tuo dispositivo di storage. Ciò significa:

- Non sono un vero backup.
- Più snapshot locali vengono conservate, più spazio di storage primario viene consumato.

Pertanto, è importante esportare le snapshot in un profilo della posizione (location), che può avere una policy di retention configurata indipendentemente.

Quando si esportano gli snapshot, tutti i dati vengono automaticamente deduplicati, compressi, crittografati e salvati in modo incrementale.



Il tuo primo test di ripristino: non saltarlo!

Prima di passare alla Fase 2, eseguire un ripristino su un'applicazione non critica per confermare 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.





FASE 2 • Giorni 15—45

Rafforza le basi

Obiettivo: protezione costante, copia off-site e visibilità nel tuo ambiente.

Traguardo 4: Gestione centralizzata (MCM)

Lo strumento di gestione multi-cluster (MCM) consente la visibilità e la gestione centralizzata di più cluster. Ogni cluster avrà Veeam Kasten installato per proteggere i carichi di lavoro e le istanze potranno essere unite tra loro.

- Una volta distribuito un altro cluster con Veeam Kasten, promuovere un'istanza di Kasten a primaria e utilizzare un token di join per collegarle ([istruzioni](#)). Assicurati che i certificati autofirmati siano riconosciuti come attendibili per evitare errori.
- Visualizza tutti i cluster connessi tramite la dashboard MCM.
- Definisci criteri globali e profili globali se desideri avere una configurazione coerente distribuita in tutto il tuo ambiente.
- Aggiungi la tua chiave di licenza enterprise al cluster MCM primario. Le licenze verranno distribuite automaticamente a tutti gli altri cluster senza necessità di ulteriori configurazioni.

Traguardo 5: Elaborazione application-aware

L'Elaborazione application-aware tramite Kanister Blueprints garantisce che i backup crash-consistent diventino consistenti a livello applicativo o vengano esportati logicamente. Questo è fondamentale per database come PostgreSQL, MongoDB, MySQL, Elastic e altri.

- Discuti i requisiti applicativi e le modalità di accesso con il team della tua applicazione.
- [Trova esempi di Blueprint già pronti](#) che puoi personalizzare oppure crea il tuo.
- [Aggiungi il Blueprint a Veeam Kasten.](#)
- Associa il Blueprint ai carichi di lavoro manualmente o creando un Blueprint Binding.
- Esegui un backup e un ripristino utilizzando il tuo Blueprint per verificare il ripristino end-to-end dell'applicazione.

Tipi di backup

Crash-consistent (impostazione predefinita): Questo tipo di backup acquisisce l'intero filesystem in un momento preciso, solitamente tramite snapshot dei produttori di storage. Questo metodo garantisce una maggiore coerenza dei dati rispetto alla semplice copia dei file, ma scritture durante il trasferimento o transazioni non ancora salvate potrebbero comunque andare perse.

Consistente a livello applicativo: Questo tipo di backup mette in pausa brevemente l'applicazione utilizzando i suoi strumenti nativi per assicurarsi che tutto sia scritto sul volume prima che venga creato lo snapshot.

Logico: Questo tipo di backup utilizza gli strumenti nativi dell'applicazione per creare un dump logico o esportare i dati come file. Spesso, questa operazione viene inviata a una destinazione esterna come S3 anziché sul volume stesso.

Blueprints sono [potenti](#) e infinitamente flessibili. Inoltre, grazie alla sua natura open-source, è possibile crearne uno per qualsiasi applicazione o flusso di lavoro, qualora non ne esista già uno.

Traguardo 6: Best practice per le policy

In questa fase creerai ulteriori attività per [proteggere tutti i tuoi carichi di lavoro](#) e utilizzerai impostazioni Advanced per garantirne l'affidabilità.

Best practice (per la maggior parte degli scenari)

- Utilizzare più attività con etichette per selezionare le applicazioni anziché un'unica policy generica che protegga tutto.
- Usa policy basate su VM invece di quelle basate su namespace quando [proteggere le VM KubeVirt](#).
- Se desideri eseguire il backup delle risorse a livello di cluster, crea una policy separata [solo per quei](#) backup.
- Definisci una finestra di backup per garantire che i carichi di lavoro in produzione non siano influenzati durante le ore critiche.
- Valuta la possibilità di programmare i job con [scaglionamento](#) per migliorare le prestazioni.
- Configura una [protezione di backup immutabile](#).
- [Esclusioni](#) / [Filtri risorse](#) se necessario.
- (Facoltativo) [Risorse globali](#), [Impostazioni predefinite di policy](#)

Altri suggerimenti

Per i job eseguiti manualmente, a meno che non venga specificato un tempo di scadenza, tutti gli artefatti dovranno essere rimossi manualmente.

Anche se il job è stato configurato utilizzando l'ora locale, tutti gli orari vengono convertiti in UTC e le pianificazioni delle policy non cambiano con l'ora legale.

Controlla i tuoi calcoli! Il calcolo della retention non è sempre chiaro. Ad esempio, conservare 24 (in totale) snapshot orari a intervalli di 15 minuti significherebbe conservare solo 6 ore di snapshot, non 24 ore.



FASE 3 • Giorni 46—75

Ottimizzare e rafforzare

Obiettivo: colmare le lacune di protezione, migliorare RTO/RPO e accrescere la visibilità.

Traguardo 7: Integrazione dell'osservabilità

- Abilita [l'integrazione con l'osservabilità di Red Hat ACM](#), se applicabile.
- Esporta le metriche verso [sistemi di monitoraggio esterni](#) (ad esempio, Grafana, Datadog, Thanos, ecc.).
- Crea avvisi e dashboard all'interno dei tuoi sistemi di monitoraggio ([esempio di Grafana](#)).
- Abilita [Reportistica](#).

Traguardo 8: Resilienza e DR migliorata

Avere un backup di tutti i carichi di lavoro dovrebbe includere anche un backup di Veeam Kasten stesso, cosa che può essere realizzata tramite Kasten Disaster Recovery (KDR). Questo non deve essere confuso con la disponibilità di un ambiente DR o di un piano di DR, che dovrebbero essere valutati in base al livello di resilienza richiesto.

KDR (Backup del catalogo Veeam Kasten)

- Abilita [Kasten DR](#): Questo salva il catalogo dei backup di Veeam Kasten, così da poter effettuare ripristini anche se l'installazione di Kasten non è più accessibile. Questo è importante, poiché i file di backup di Veeam Kasten non sono autonomi e richiedono il catalogo e la chiave di crittografia per il ripristino.
- Imposta Kasten DR su "Esporta snapshot del catalogo locale" e salva le seguenti informazioni in una posizione sicura: passphrase, ID cluster, dettagli del profilo della posizione KDR e credenziali.



DR per i vostri carichi di lavoro

- Determina il livello di resilienza necessario in base ai valori di RTO/RPO desiderati.
- Se un RTO/RPO di 1 o più giorni è accettabile, avere solo backup e ricostruire l'ambiente secondo necessità potrebbe essere una soluzione ragionevole.
- Se i valori di RTO/RPO devono essere misurati in ore o minuti, occorre porre particolare attenzione alla definizione del piano. Di seguito vengono forniti alcuni esempi.

Configurazioni di esempio DR (secondo i requisiti di RTO/RPO necessari)

- **Applicazione non protetta:** Nessun punto di ripristino (ovvero nessuna snapshot locale o esportazione).
Risultato: Nessun ripristino possibile.
- **Solo esportazione:** Le esportazioni di KDR e i punti di ripristino esportati esistono in un profilo della posizione (location) remoto.
Risultato: Per ripristinare, ricostruire innanzitutto un ambiente Kubernetes, installare Veeam Kasten, ripristinare il catalogo Kasten, quindi ripristinare le applicazioni dai punti di ripristino esportati.
- **Ambiente DR + Importazione:** Veeam Kasten è installato e una policy di importazione viene eseguita regolarmente per importare i punti di ripristino in un catalogo locale.
Risultato: I punti di ripristino sono visibili in una posizione secondaria e sono pronti per essere ripristinati. Le risorse vengono utilizzate al minimo fino a quando non sono richieste.
- **Ambiente DR + Importazione + Ripristino, scalato a zero:** Veeam Kasten è installato, la policy di Importazione + Ripristino viene eseguita regolarmente per importare i punti di ripristino nel catalogo locale e quindi ripristinare le applicazioni nell'ambiente Kubernetes. Le applicazioni vengono quindi ripristinate, ma con [Transforms](#) che impostano le repliche a 0 su tutti i carichi di lavoro.
Risultato: Le applicazioni vengono ripristinate in Kubernetes (inclusi pod, PV e tutte le risorse selezionate). Tuttavia, il numero di repliche è pari a 0, quindi il consumo di risorse è minimo finché non sono necessarie, fatta eccezione per lo storage.
- **Ambiente DR + Import + Ripristino, completo:** Veeam Kasten è installato, la policy di importazione e ripristino viene eseguita regolarmente per importare i punti di ripristino in un catalogo locale e quindi ripristinare le applicazioni nell'ambiente Kubernetes.
Risultato: Le applicazioni vengono ripristinate in Kubernetes (tramite pod, PV, tutto ciò che è stato selezionato), funzionano esattamente come in Production e sono pronte per essere utilizzate completamente.



Pianificazione dei disastri

Veeam Kasten è agnostico rispetto alla distribuzione, il che significa che può eseguire il ripristino da e verso qualsiasi distribuzione Kubernetes, anche tra distribuzioni completamente diverse, come da Tanzu ad Azure. Per poter eseguire i ripristini è necessario un ambiente Kubernetes operativo; Kasten non è in grado di avviarsi da solo. Assicuratevi di creare un piano di disaster recovery adeguato in modo da essere preparato in caso di incidente e testa regolarmente che il tuo piano soddisfi i tuoi obiettivi.

Traguardo 9: Messa a punto

- **Esamina la dashboard di Veeam Kasten:** Affronta tutti i carichi di lavoro non protetti prima di effettuare qualsiasi altra messa a punto.
- **Esamina la pianificazione dei job per individuare eventuali conflitti:** Scaglionare gli orari di inizio per prevenire contese delle risorse.
- Verifica che tutte le attività vengano completate entro la finestra di backup definita.
- **Verifica la conformità all'RPO:** Tutti i carichi di lavoro critici stanno generando punti di ripristino entro la finestra di ripristino definita?
- Verifica che tutti i carichi di lavoro vengano esportati in almeno una posizione immutabile.
- Abilitare la [Raccolta dei rifiuti](#) per rimuovere le azioni obsolete può migliorare le prestazioni del catalogo.
- Testa la procedura di upgrade! Le nuove [versioni di Veeam Kasten](#) vengono rilasciate all'incirca ogni due settimane.



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.

Test di ripristino granulare e ripristino completo

- Esegui un test di ripristino completo di uno spazio dei nomi o di ripristino di una VM da un'esportazione. Simula una perdita totale on-premises per convalidare la copia offsite.
- Test di ripristino dell'elemento applicativo: ripristina un database ed esegui query sul database per verificare che i dati siano integri.
- Test di ripristino a livello di file (se desiderato): ripristina singoli file da un export in una posizione di test.
- Metti alla prova il tuo piano di DR completo end-to-end, annota eventuali problemi da migliorare e documenta dettagliatamente il processo in modo da garantire che il tuo piano di DR e l'accesso ad esso siano disponibili.
- Registra i tempi di ripristino effettivi e confrontali con gli obiettivi RTO. Documenta i risultati.

Ripristino in ambienti diversi

Se si esegue il ripristino da/verso siti diversi, distribuzioni Kubernetes, piattaforme o altro, [Transforms](#) può essere utile per adattare automaticamente la configurazione durante il ripristino. Ad esempio, se si modificano i percorsi di rete da Production a DR, oppure se si modificano le classi di storage. Non sono necessarie modifiche manuali per avviare immediatamente i ripristini con una configurazione modificata o in un nuovo ambiente.



Best practice per il test di ripristino

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

Documenta 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.

Inoltre, se si effettua un ripristino nello stesso ambiente, anche se in namespace diversi, occorre essere consapevoli che alcune risorse (in particolare i servizi di rete) potrebbero entrare in conflitto. Assicurati di rivedere la tua configurazione prima di effettuare il ripristino, ripristina in un ambiente diverso e/o utilizza [Transforms](#) per evitare conflitti.

Traguardo 11: Documentazione e reportistica

- Abilita il [Reporting](#), se non è già stato fatto.
- Documenta l'architettura finale di backup, includendo l'elenco delle politiche, le destinazioni di esportazione, 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.

Traguardo 12: Stabilire una cadenza continua delle pratiche di igiene

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

- **Settimanale:** Esamina la dashboard di Veeam Kasten e analizzare eventuali job non riusciti o con avvisi prima che si accumulino.
- **Mensilmente:** Controlla le versioni recenti di Kasten e aggiorna regolarmente il software.
- **Trimestralmente:** Esegui un test di ripristino documentato e ruota tra diversi tipi di carico di lavoro ogni trimestre.
- **Annualmente:** Rivedi la tua architettura di backup rispetto ai requisiti aziendali attuali.
- **Prima del rinnovo:** Verifica l'utilizzo delle licenze nella tua dashboard di Kasten (ad esempio, il totale tramite MCM o in ciascun cluster individualmente) per assicurarti di essere conforme ai diritti di licenza.

Passi successivi

Pronto per altro?

- [Visita Veeam University](#)
- [Scopri le storie di successo dei tuoi colleghi](#)
- [Contatta il team Customer Success](#)
- [Condividi la tua storia di resilienza dei dati con Veeam](#)





Appendice: riferimento rapido

Componenti chiave: Integrazione con Veeam

- **Veeam Software Appliance (VSA):** Un'appliance pre-hardened con Veeam Backup & Replication preinstallato. Distribuire come OVA (VM) o ISO (fisico). Può fungere da repository immutabile limitato oppure operare con altri appliance o storage di backup, inclusi VIA dedicati.
- **Veeam Infrastructure Appliance (VIA):** Un'appliance pre-hardennizzata distribuita come repository con protezione avanzata dedicato o per altri ruoli. Garantisce l'immutabilità locale senza necessità di competenze specifiche su Linux. Un ruolo per ogni appliance.
- **Veeam Backup & Replication:** Motore di backup centrale, ospitato su VSA. Gestisce job, repository, proxy e operazioni di ripristino.
- **Scale-Out Backup Repository:** Costrutto logico che combina un livello di prestazioni locale (ad es. VIA) e Capacity Tier (ad es. Vault/S3/NFS) in un'unica destinazione di backup.
- **Veeam Vault:** Storage di oggetti cloud immutabile per copie fuori sede. È gestito da Veeam, non è necessario un account cloud separato.

Termini chiave

- **RPO:** Perdita di dati massima accettabile, misurata in tempo. Influenza la frequenza con cui vengono pianificati i backup.
- **RTO:** Tempo massimo di interruzione accettabile prima che un carico di lavoro debba essere ripristinato.
- **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.
- **Veeam Hardened Repository:** Un repository di backup basato su Linux con immutabilità garantita a livello di SO. Fornito pronto all'uso da VIA, senza necessità di amministrazione Linux.
- **KubeVirt:** Un progetto open-source che consente a Kubernetes di eseguire e gestire VM insieme a carichi di lavoro containerizzati. Ciò consente alle VM di essere eseguite su piattaforme Kubernetes come OpenShift Virtualization e SUSE Harvester, che possono essere protette da Veeam Kasten.
- **Application-aware processing:** Elaborazione application-aware che crea punti di backup consistenti a livello applicativo, funzione che Veeam Kasten può realizzare grazie ai Blueprint.
- **Blueprint:** I Blueprint di Kanister sono un meccanismo open-source per descrivere attività personalizzate per la gestione dei dati a livello applicativo su Kubernetes.

Risorse utili

- [Veeam Help Center](#)
- [Portale del cliente Veeam \(download\)](#)
- [Veeam Community Forums](#)
- [Articoli KB di Veeam](#)
- [Documentazione Veeam Kasten](#)
- [Documentazione sui Blueprint di Kanister](#)

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,

Maggiori informazioni su www.veeam.com oppure segui Veeam su LinkedIn [@veeam-software](#) e X [@veeam](#).