



Protezione dei carichi di lavoro su GCP/GCVE

NetApp Solutions

NetApp
April 26, 2024

Sommario

- Protezione dei carichi di lavoro su GCP/GCVE 1
 - Disaster recovery coerente con l'applicazione con replica NetApp SnapCenter e Veeam 1
 - Disaster recovery applicativo con replica SnapCenter, Cloud Volumes ONTAP e Veeam 4

Protezione dei carichi di lavoro su GCP/GCVE

Disaster recovery coerente con l'applicazione con replica NetApp SnapCenter e Veeam

Autori: Suresh Thoppay, NetApp

Panoramica

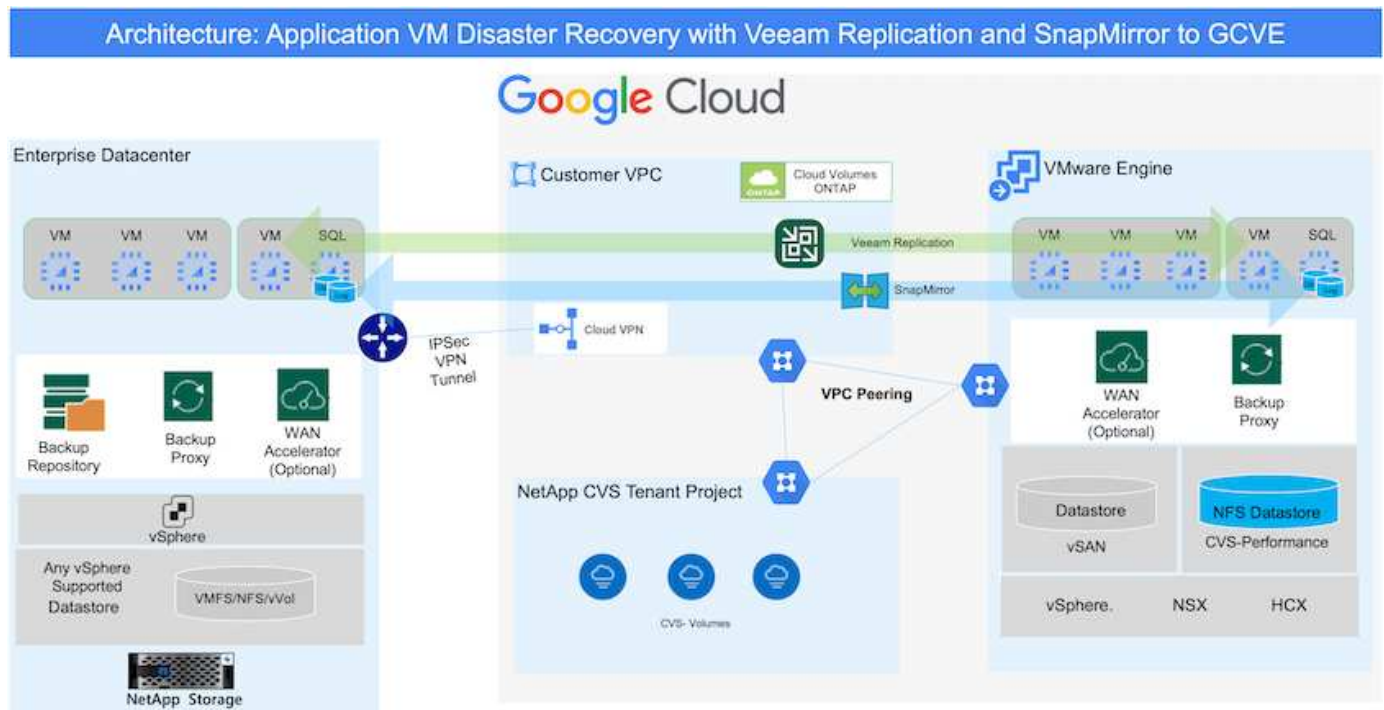
Molti clienti cercano una soluzione di disaster recovery efficace per le loro macchine virtuali applicative ospitate su VMware vSphere. Molti di loro utilizzano la soluzione di backup esistente per eseguire il recovery durante il disaster.

Molte volte questa soluzione aumenta l'RTO e non soddisfa le loro aspettative. Per ridurre l'RPO e l'RTO, la replica delle macchine virtuali Veeam può essere utilizzata anche da on-premise a GCVE, purché siano disponibili connettività di rete e ambiente con autorizzazioni appropriate.

NOTA: Veeam VM Replication non protegge i dispositivi storage connessi guest delle VM, come i supporti iSCSI o NFS, all'interno della VM guest. Necessità di proteggerli separatamente.

Per una replica coerente delle applicazioni per SQL VM e per ridurre l'RTO, abbiamo utilizzato SnapCenter per orchestrare le operazioni di snapmirror dei volumi di log e del database SQL.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, Veeam e Google Cloud VMware Engine (GCVE).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.



Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizza le opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.



Esistono diverse opzioni per connettere i data center on-premise a Google Cloud, che ci impediscono di delineare un workflow specifico in questo documento. Fare riferimento alla documentazione di Google Cloud per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione DR

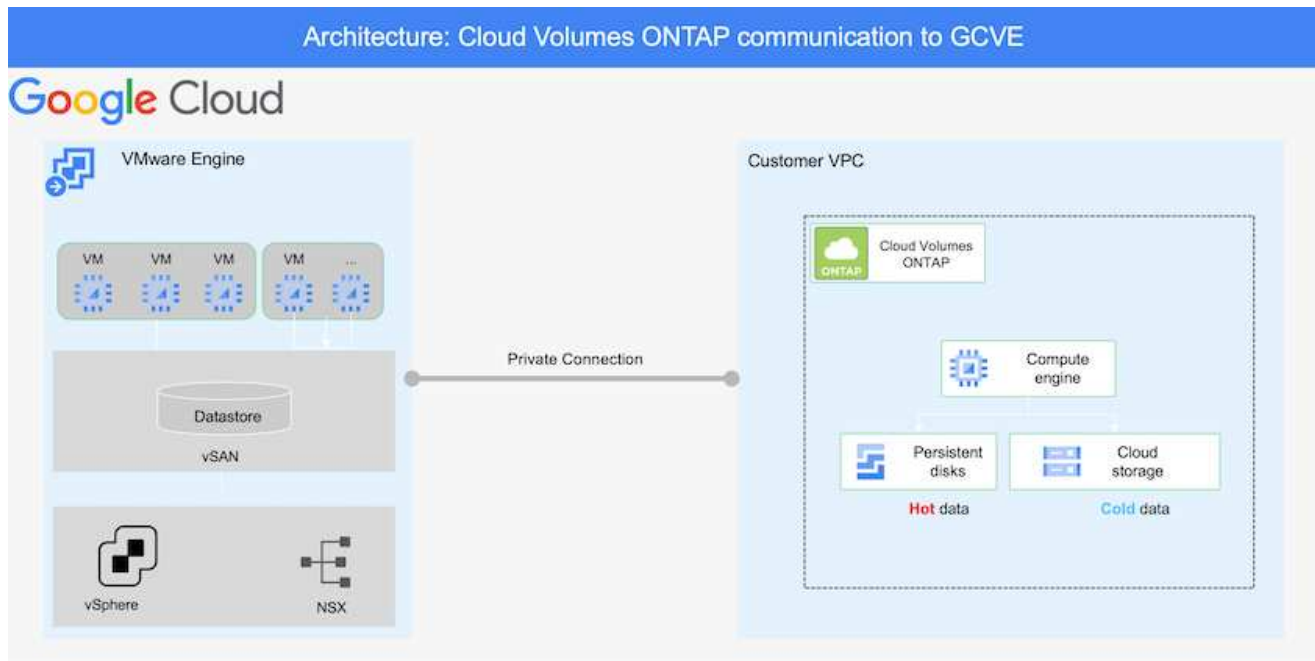
Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando BlueXP all'interno dell'abbonamento appropriato e della rete virtuale.
 - a. Configurare SnapMirror per i volumi applicativi rilevanti.
 - b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
3. Installare il software Veeam e avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Durante un evento di emergenza, interrompere la relazione SnapMirror utilizzando BlueXP e attivare il failover delle macchine virtuali con Veeam.
 - a. Ricollegare i LUN iSCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
 - b. Visualizzare le applicazioni online.
5. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Google Cloud e replicare i volumi su CVO

Il primo passo è configurare Cloud Volumes ONTAP su Google Cloud ("cvo") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritenzioni di snapshot.



Per istruzioni dettagliate di esempio sull'impostazione di SnapCenter e la replica dei dati, fare riferimento a. ["Configurazione della replica con SnapCenter"](#)

[Analisi della protezione di SQL VM con SnapCenter](#)

Configurare gli host GCVE e l'accesso ai dati CVO

Due fattori importanti da prendere in considerazione durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e il tempo necessario per mantenere SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

Il servizio di volume cloud di NetApp per datastore NFS e Cloud Volumes ONTAP per database SQL e log possono essere implementati su qualsiasi VPC e deve disporre di una connessione privata a tale VPC per montare datastore NFS e connettere le macchine virtuali a LUN iSCSI.

Per configurare GCVE SDDC, vedere ["Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform \(GCP\)"](#). Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host GCVE siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e GCVE, iniziare a configurare Veeam per automatizzare il ripristino dei carichi di lavoro on-premise su GCVE (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando la funzione di replica Veeam e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Installare i componenti Veeam

In base allo scenario di implementazione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere implementati. In questo caso di utilizzo, non è necessario implementare l'archivio di oggetti per Veeam e il repository scale-out.

["Fare riferimento alla documentazione Veeam per la procedura di installazione"](#)

Per ulteriori informazioni, fare riferimento a. ["Migrazione con Replica Veeam"](#)

Configurazione della replica delle macchine virtuali con Veeam

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. ["Processo di replica di vSphere VM"](#) Nella fase di elaborazione guest della procedura guidata, selezionare Disable application processing (Disattiva elaborazione applicazioni), in quanto verrà utilizzato SnapCenter per il backup e il ripristino consapevoli dell'applicazione.

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692>

Failover di Microsoft SQL Server VM

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0>

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.
 - In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
 - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
 - Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito DR.

Disaster recovery applicativo con replica SnapCenter, Cloud Volumes ONTAP e Veeam

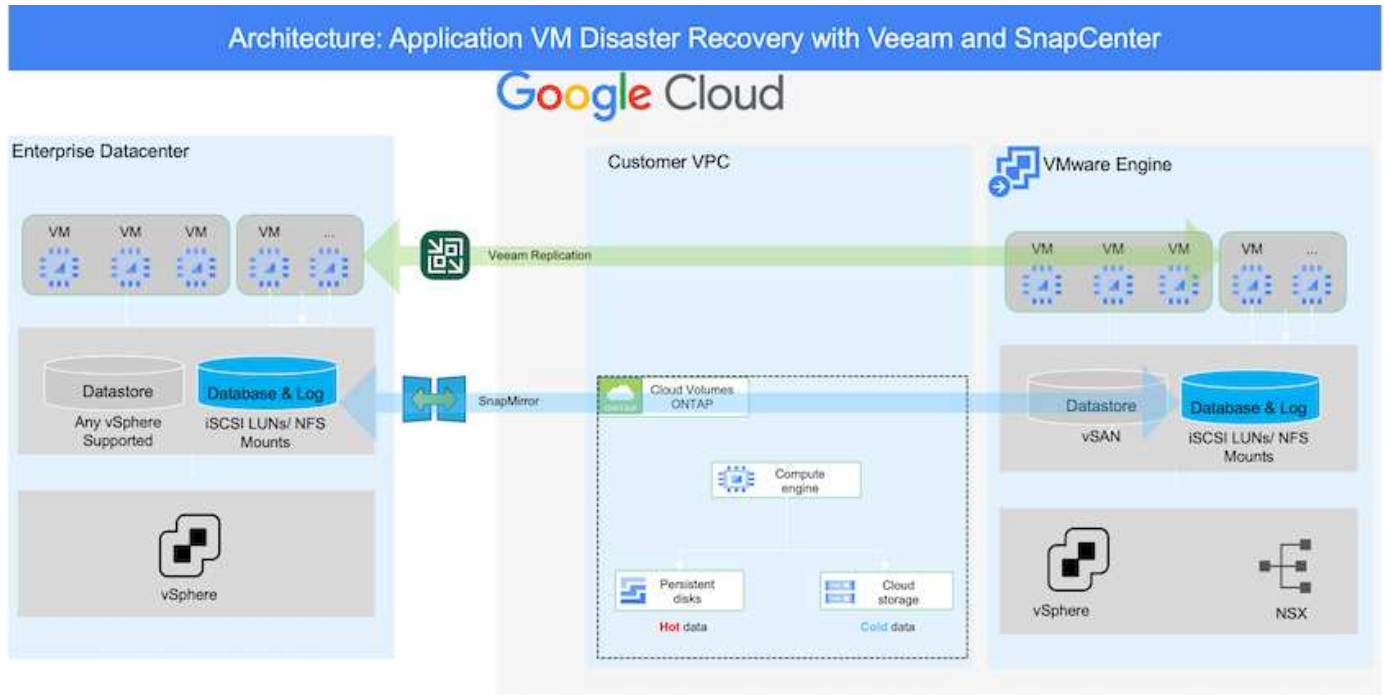
Autori: Suresh Thoppay, NetApp

Panoramica

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i workload da interruzioni del sito e eventi di corruzione dei dati come ransomware. Con NetApp SnapMirror, è possibile replicare i workload VMware on-premise che utilizzano lo storage connesso agli ospiti su NetApp Cloud Volumes ONTAP in

esecuzione su Google Cloud. Ciò riguarda i dati delle applicazioni, ma le macchine virtuali effettive. Il disaster recovery dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. A tale scopo, SnapMirror e Veeam possono essere utilizzati per ripristinare perfettamente i carichi di lavoro replicati da on-premise a Cloud Volumes ONTAP utilizzando lo storage vSAN per VM VMDK.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, Veeam e Google Cloud VMware Engine (GCVE).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.



Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizza le opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.



Esistono diverse opzioni per connettere i data center on-premise a Google Cloud, che ci impediscono di delineare un workflow specifico in questo documento. Fare riferimento alla documentazione di Google Cloud per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione DR

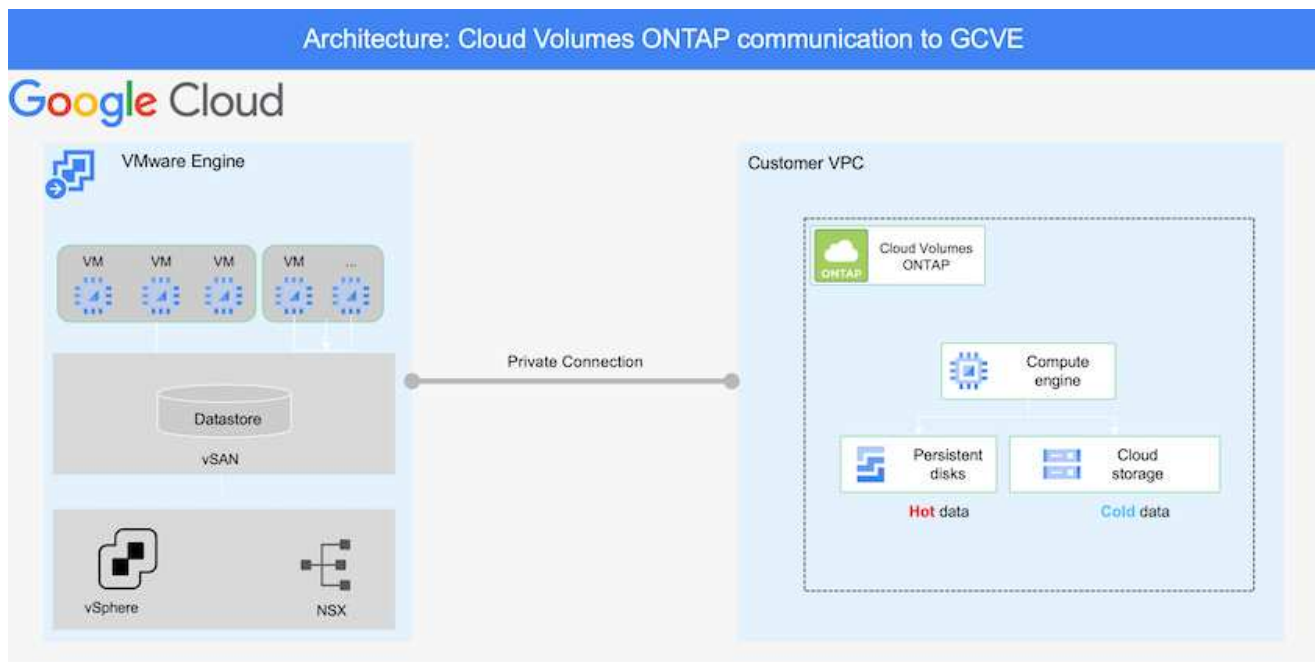
Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
 - a. Configurare SnapMirror per i volumi applicativi rilevanti.
 - b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
3. Installare il software Veeam e avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Durante un evento di disastro, interrompere la relazione SnapMirror utilizzando Cloud Manager e attivare il failover delle macchine virtuali con Veeam.
 - a. Ricollegare i LUN iSCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
 - b. Visualizzare le applicazioni online.
5. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Google Cloud e replicare i volumi su CVO

Il primo passo è configurare Cloud Volumes ONTAP su Google Cloud ("cvo") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritenzioni di snapshot.



Per istruzioni dettagliate di esempio sull'impostazione di SnapCenter e la replica dei dati, fare riferimento a. ["Configurazione della replica con SnapCenter"](#)

[Configurazione della replica con SnapCenter](#)

Configurare gli host GCVE e l'accesso ai dati CVO

Due fattori importanti da prendere in considerazione durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e il tempo necessario per mantenere SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

Cloud Volumes ONTAP può essere implementato su qualsiasi VPC e deve disporre di una connessione privata a tale VPC per consentire la connessione della macchina virtuale alle LUN iSCSI.

Per configurare GCVE SDDC, vedere ["Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform \(GCP\)"](#). Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host GCVE siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e GCVE, iniziare a configurare Veeam per automatizzare il ripristino dei carichi di lavoro on-premise su GCVE (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando la funzione di replica Veeam e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Installare i componenti Veeam

In base allo scenario di implementazione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere implementati. In questo caso di utilizzo, non è necessario implementare l'archivio di oggetti per Veeam e il repository scale-out.
https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Fare riferimento alla documentazione Veeam per la procedura di installazione"]

Configurazione della replica delle macchine virtuali con Veeam

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. ["Processo di replica di vSphere VM"](#) Nella fase di elaborazione guest della procedura guidata, selezionare Disable application processing (Disattiva elaborazione applicazioni), in quanto verrà utilizzato SnapCenter per il backup e il ripristino consapevoli dell'applicazione.

[Processo di replica di vSphere VM](#)

Failover di Microsoft SQL Server VM

[Failover di Microsoft SQL Server VM](#)

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.

- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.
 - In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
 - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
 - Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito DR.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.