



TR-4931: Disaster Recovery con VMware Cloud su Amazon Web Services e Guest Connect

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Sommario

TR-4931: Disaster Recovery con VMware Cloud su Amazon Web Services e Guest Connect	1
Panoramica	1
Presupposti, prerequisiti e panoramica dei componenti	1
Esecuzione di DR con SnapCenter	1
Configurare le relazioni e le pianificazioni di conservazione SnapMirror	2
Distribuisci e configura il server Windows SnapCenter in locale	10
Distribuisci e configura Veeam Backup Server	19
Strumenti e configurazione BlueXP backup and recovery	30
Backup del database SnapCenter per il ripristino di emergenza	31
Failover	39
Ripristina le VM delle applicazioni con il ripristino completo di Veeam	42
Ripristinare i dati dell'applicazione SQL Server	55
Ripristinare i dati dell'applicazione Oracle	64
Rifasamento	70
Conclusione	70

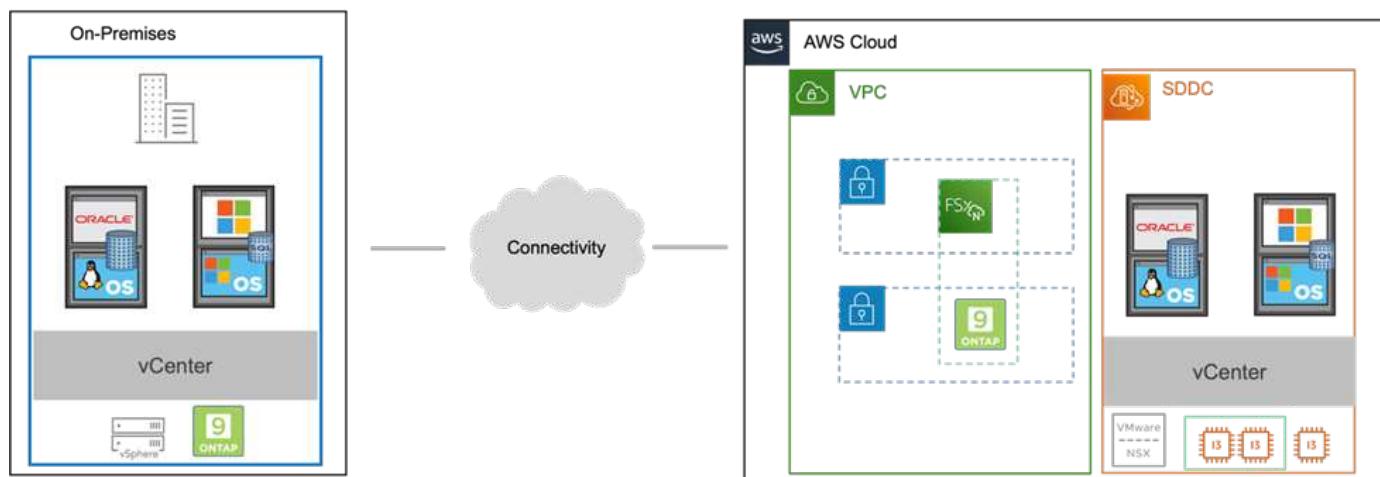
TR-4931: Disaster Recovery con VMware Cloud su Amazon Web Services e Guest Connect

Un ambiente e un piano di disaster recovery (DR) collaudati sono essenziali per le organizzazioni, per garantire che le applicazioni aziendali critiche possano essere ripristinate rapidamente in caso di un'interruzione importante. Questa soluzione si concentra sulla dimostrazione di casi d'uso DR con particolare attenzione alle tecnologie VMware e NetApp, sia in locale che con VMware Cloud su AWS.

Panoramica

NetApp vanta una lunga tradizione di integrazione con VMware, come dimostrano le decine di migliaia di clienti che hanno scelto NetApp come partner di storage per il loro ambiente virtualizzato. Questa integrazione continua anche con le opzioni connesse agli ospiti nel cloud e con le recenti integrazioni con i datastore NFS. Questa soluzione si concentra sul caso d'uso comunemente denominato storage connesso agli ospiti.

Nello storage connesso agli ospiti, il VMDK ospite viene distribuito su un datastore fornito da VMware e i dati dell'applicazione sono ospitati su iSCSI o NFS e mappati direttamente sulla VM. Per illustrare uno scenario DR, come mostrato nella figura seguente, vengono utilizzate le applicazioni Oracle e MS SQL.



Presupposti, prerequisiti e panoramica dei componenti

Prima di distribuire questa soluzione, rivedere la panoramica dei componenti, i prerequisiti richiesti per distribuire la soluzione e le ipotesi formulate nella documentazione di questa soluzione.

["Requisiti, prerequisiti e pianificazione della soluzione DR"](#)

Esecuzione di DR con SnapCenter

In questa soluzione, SnapCenter fornisce snapshot coerenti con l'applicazione per i dati delle applicazioni SQL Server e Oracle. Questa configurazione, insieme alla tecnologia SnapMirror, garantisce la replicazione dei dati ad alta velocità tra il nostro cluster AFF locale e FSx ONTAP. Inoltre, Veeam Backup & Replication offre funzionalità di backup e ripristino per le nostre macchine virtuali.

In questa sezione, illustreremo la configurazione di SnapCenter, SnapMirror e Veeam sia per il backup che per

il ripristino.

Le sezioni seguenti riguardano la configurazione e i passaggi necessari per completare un failover nel sito secondario:

Configurare le relazioni e le pianificazioni di conservazione SnapMirror

SnapCenter può aggiornare le relazioni SnapMirror all'interno del sistema di archiviazione primario (primario > mirror) e nei sistemi di archiviazione secondari (primario > vault) allo scopo di archiviazione e conservazione a lungo termine. Per fare ciò, è necessario stabilire e inizializzare una relazione di replica dei dati tra un volume di destinazione e un volume di origine utilizzando SnapMirror.

I sistemi ONTAP di origine e di destinazione devono trovarsi in reti peering tramite peering Amazon VPC, un gateway di transito, AWS Direct Connect o una VPN AWS.

Per impostare le relazioni SnapMirror tra un sistema ONTAP locale e FSx ONTAP sono necessari i seguenti passaggi:

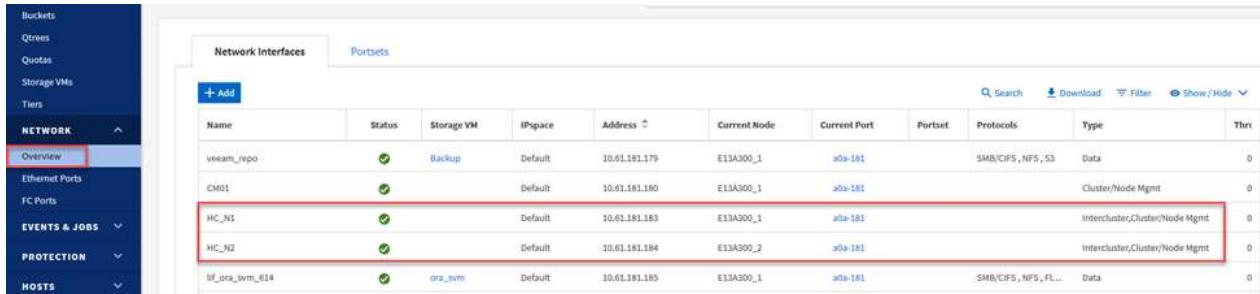


Fare riferimento al "["FSx ONTAP – Guida utente ONTAP"](#)" per ulteriori informazioni sulla creazione di relazioni SnapMirror con FSx.

Registra le interfacce logiche Intercluster di origine e destinazione

Per il sistema ONTAP di origine residente in locale, è possibile recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

1. In ONTAP System Manager, vai alla pagina Panoramica di rete e recupera gli indirizzi IP di tipo: Intercluster configurati per comunicare con l'AWS VPC in cui è installato FSx.



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thru
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster,Cluster/Node Mgmt	0
lif_ora_svm_614	✓	ora_svm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. Per recuperare gli indirizzi IP Intercluster per FSx, accedere alla CLI ed eseguire il seguente comando:

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
  Logical      Status      Network          Current      Current Is
  Vserver      Interface  Admin/Oper Address/Mask  Node        Port   Home
  -----
FsxId0ae40e08acc0dea67
  inter_1      up/up      172.30.15.42/25  FsxId0ae40e08acc0dea67-01
  inter_2      up/up      172.30.14.28/26  FsxId0ae40e08acc0dea67-02
2 entries were displayed.
```

Stabilire il peering del cluster tra ONTAP e FSx

Per stabilire il peering tra cluster ONTAP , è necessario che una passphrase univoca immessa nel cluster ONTAP di avvio venga confermata nell'altro cluster peer.

1. Impostare il peering sul cluster FSx di destinazione utilizzando `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca che verrà utilizzata in seguito sul cluster di origine per finalizzare il processo di creazione.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. Nel cluster di origine, è possibile stabilire la relazione peer del cluster utilizzando ONTAP System Manager o la CLI. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Cluster.



DASHBOARD

STORAGE ^

Overview

Volumes

LUNs

Consistency Groups

NVMe Namespaces

Shares

Buckets

Qtrees

Quotas

Storage VMs

Tiers

NETWORK ^

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS ^

PROTECTION ^

Overview

Relationships

HOSTS ^

Overview

[Intercluster Settings](#)

Network Interfaces

IP ADDRESS

✓ 10.61.181.184

✓ 172.21.146.217

✓ 10.61.181.183

✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

✓ Fsxl0ae40e08acc0dea67

✓ OTS02

[Peer Cluster](#)[Generate Passphrase](#)[Manage Cluster Peers](#)Mediator [?](#)

Not configured.

[Configure](#)

Storage VM Peers



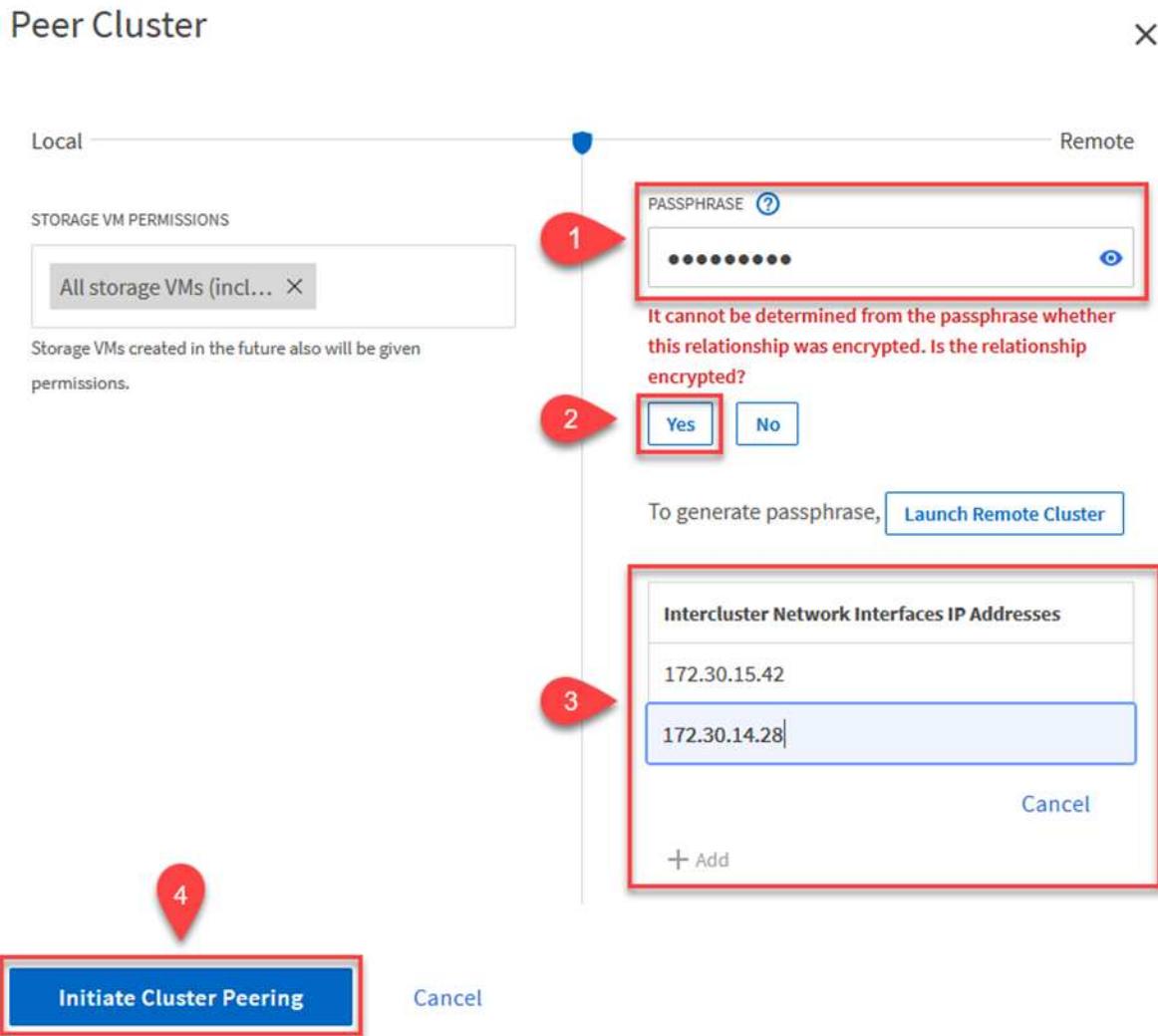
PEERED STORAGE VMs

✓ 3

3. Nella finestra di dialogo Peer Cluster, compilare le informazioni richieste:

- Immettere la passphrase utilizzata per stabilire la relazione del cluster peer sul cluster FSx di destinazione.

- b. Selezionare Yes per stabilire una relazione crittografata.
- c. Immettere l'indirizzo/gli indirizzi IP LIF intercluster del cluster FSx di destinazione.
- d. Fare clic su Avvia peering cluster per finalizzare il processo.



- 4. Verificare lo stato della relazione peer del cluster dal cluster FSx con il seguente comando:

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability  Authentication
-----  -----
E13A300                1-80-000011           Available      ok
```

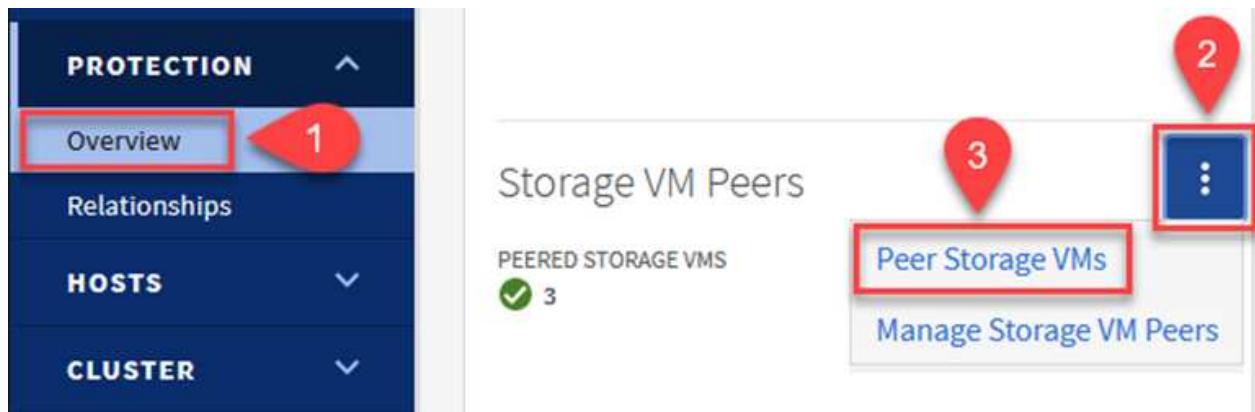
Stabilire una relazione di peering SVM

Il passaggio successivo consiste nell'impostare una relazione SVM tra le macchine virtuali di archiviazione di destinazione e di origine che contengono i volumi che saranno nelle relazioni SnapMirror.

1. Dal cluster FSx di origine, utilizzare il seguente comando dalla CLI per creare la relazione peer SVM:

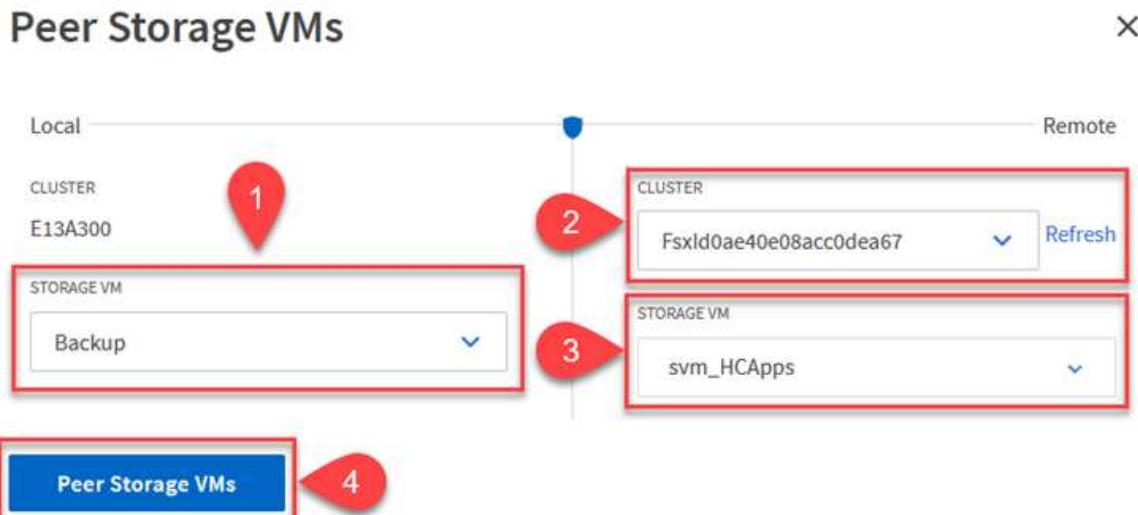
```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver  
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Dal cluster ONTAP di origine, accettare la relazione di peering con ONTAP System Manager o con la CLI.
3. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Storage VM in Storage VM Peer.



4. Nella finestra di dialogo della VM di archiviazione peer, compilare i campi obbligatori:

- La VM di archiviazione di origine
- Il cluster di destinazione
- La VM di archiviazione di destinazione



5. Fare clic su Peer Storage VM per completare il processo di peering SVM.

Creare un criterio di conservazione degli snapshot

SnapCenter gestisce le pianificazioni di conservazione per i backup presenti come copie snapshot sul sistema di archiviazione primario. Ciò viene stabilito durante la creazione di una policy in SnapCenter. SnapCenter non gestisce i criteri di conservazione per i backup conservati su sistemi di archiviazione secondari. Queste policy vengono gestite separatamente tramite una policy SnapMirror creata sul cluster FSx secondario e associata ai volumi di destinazione che si trovano in una relazione SnapMirror con il volume di origine.

Quando si crea un criterio SnapCenter, è possibile specificare un'etichetta di criterio secondaria che viene aggiunta all'etichetta SnapMirror di ogni snapshot generato quando viene eseguito un backup SnapCenter.



Nell'archiviazione secondaria, queste etichette vengono abbinate alle regole dei criteri associati al volume di destinazione allo scopo di imporre la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutti gli snapshot generati come parte di un criterio utilizzato per i backup giornalieri del database SQL Server e dei volumi di registro.

Select secondary replication options

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label

sql-daily

Error retry count

3



Per ulteriori informazioni sulla creazione di criteri SnapCenter per un database SQL Server, vedere ["Documentazione SnapCenter"](#).

Per prima cosa devi creare un criterio SnapMirror con regole che stabiliscano il numero di copie snapshot da conservare.

1. Creare la policy SnapMirror sul cluster FSx.

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Aggiungere regole alla policy con etichette SnapMirror che corrispondono alle etichette della policy secondaria specificate nelle policy SnapCenter.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Lo script seguente fornisce un esempio di regola che potrebbe essere aggiunta a una policy:

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



Creare regole aggiuntive per ogni etichetta SnapMirror e il numero di snapshot da conservare (periodo di conservazione).

Crea volumi di destinazione

Per creare un volume di destinazione su FSx che sarà il destinatario delle copie snapshot dai nostri volumi di origine, eseguire il seguente comando su FSx ONTAP:

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

Creare le relazioni SnapMirror tra i volumi di origine e di destinazione

Per creare una relazione SnapMirror tra un volume di origine e uno di destinazione, eseguire il seguente comando su FSx ONTAP:

```
FSx-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

Inizializza le relazioni SnapMirror

Inizializza la relazione SnapMirror. Questo processo avvia un nuovo snapshot generato dal volume di origine e lo copia nel volume di destinazione.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Distribuisci e configura il server Windows SnapCenter in locale.

Distribuisci Windows SnapCenter Server in locale

Questa soluzione utilizza NetApp SnapCenter per eseguire backup coerenti con le applicazioni dei database SQL Server e Oracle. In combinazione con Veeam Backup & Replication per il backup dei VMDK delle macchine virtuali, si ottiene una soluzione completa di disaster recovery per data center on-premise e basati su cloud.

Il SnapCenter software è disponibile sul sito di supporto NetApp e può essere installato sui sistemi Microsoft Windows che risiedono in un dominio o in un gruppo di lavoro. Una guida dettagliata alla pianificazione e alle istruzioni di installazione sono disponibili sul sito ["Centro di documentazione NetApp"](#).

Il SnapCenter software può essere ottenuto presso ["questo collegamento"](#).

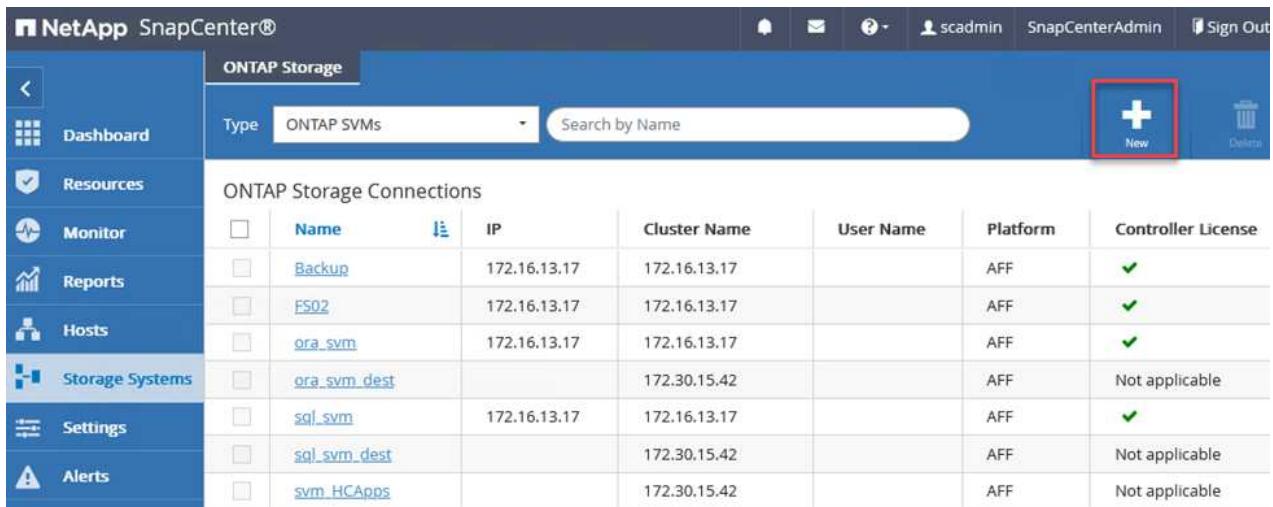
Dopo l'installazione, è possibile accedere alla console SnapCenter da un browser Web utilizzando [*https://Virtual_Cluster_IP_or_FQDN:8146*](https://Virtual_Cluster_IP_or_FQDN:8146).

Dopo aver effettuato l'accesso alla console, è necessario configurare SnapCenter per il backup dei database SQL Server e Oracle.

Aggiungere controller di archiviazione a SnapCenter

Per aggiungere controller di archiviazione a SnapCenter, completare i seguenti passaggi:

1. Dal menu a sinistra, seleziona Sistemi di archiviazione e poi fai clic su Nuovo per iniziare il processo di aggiunta dei controller di archiviazione a SnapCenter.



The screenshot shows the NetApp SnapCenter interface. The left sidebar has icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (selected), Settings, and Alerts. The main area is titled 'ONTAP Storage' with a dropdown set to 'ONTAP SVMs' and a search bar. Below is a table of 'ONTAP Storage Connections' with columns: Name, IP, Cluster Name, User Name, Platform, and Controller License. The table lists several entries, including 'Backup', 'FS02', 'ora_svm', 'ora_svm_dest', 'sql_svm', 'sql_svm_dest', and 'svm_HCapps'. The 'New' button in the top right is highlighted with a red box.

	Name	IP	Cluster Name	User Name	Platform	Controller License
	Backup	172.16.13.17	172.16.13.17		AFF	✓
	FS02	172.16.13.17	172.16.13.17		AFF	✓
	ora_svm	172.16.13.17	172.16.13.17		AFF	✓
	ora_svm_dest		172.30.15.42		AFF	Not applicable
	sql_svm	172.16.13.17	172.16.13.17		AFF	✓
	sql_svm_dest		172.30.15.42		AFF	Not applicable
	svm_HCapps		172.30.15.42		AFF	Not applicable

2. Nella finestra di dialogo Aggiungi sistema di archiviazione, aggiungere l'indirizzo IP di gestione per il cluster ONTAP locale, nonché il nome utente e la password. Quindi fare clic su Invia per iniziare l'individuazione del sistema di archiviazione.

Add Storage System

Add Storage System i

Storage System

Username

Password

Event Management System (EMS) & AutoSupport Settings

Send AutoSupport notification to storage system

Log SnapCenter Server events to syslog

 **More Options** : Platform, Protocol, Preferred IP etc..

Submit

Cancel

Reset

3. Ripetere questa procedura per aggiungere il sistema FSx ONTAP a SnapCenter. In questo caso, seleziona Altre opzioni nella parte inferiore della finestra Aggiungi sistema di archiviazione e fai clic sulla casella di controllo Secondario per designare il sistema FSx come sistema di archiviazione secondario aggiornato con copie SnapMirror o con i nostri snapshot di backup primari.

More Options

X

Platform	FAS	<input checked="" type="checkbox"/> Secondary i
Protocol	HTTPS	
Port	443	
Timeout	60	seconds i
<input type="checkbox"/> Preferred IP	i	

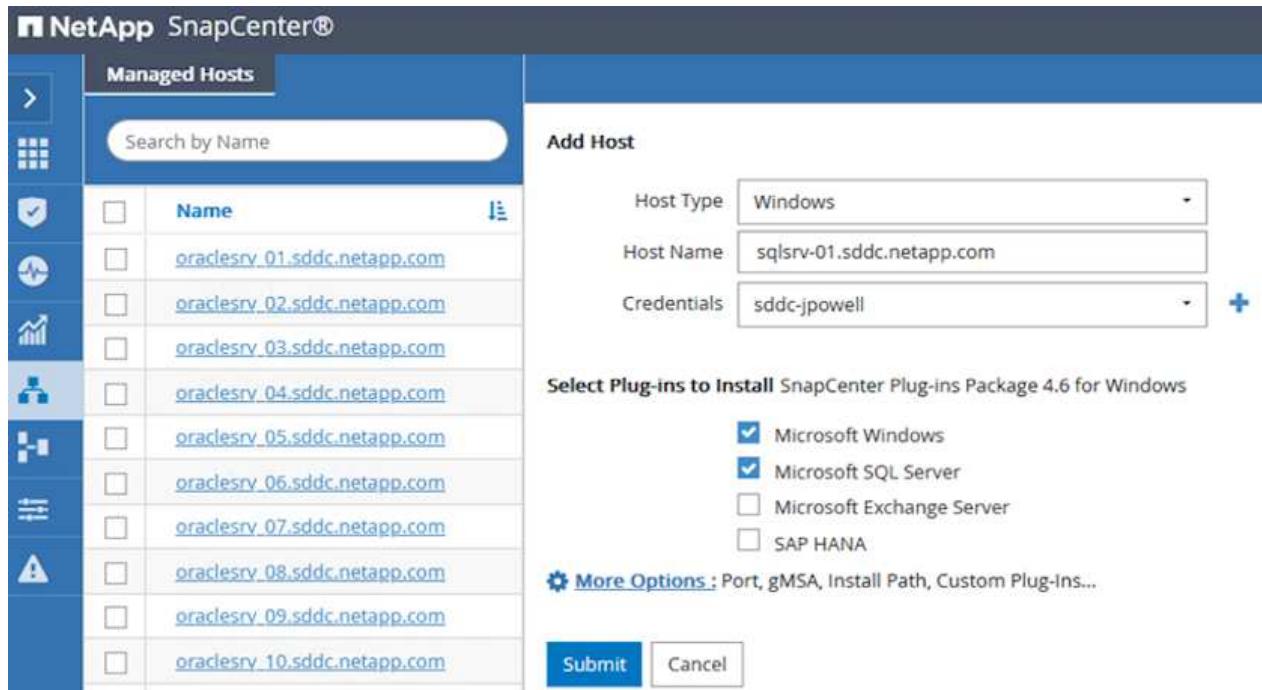
Save Cancel

Per ulteriori informazioni relative all'aggiunta di sistemi di archiviazione a SnapCenter, consultare la documentazione all'indirizzo ["questo collegamento"](#).

Aggiungi host a SnapCenter

Il passaggio successivo consiste nell'aggiungere i server applicativi host a SnapCenter. Il processo è simile sia per SQL Server che per Oracle.

1. Dal menu a sinistra, seleziona Host e poi fai clic su Aggiungi per iniziare il processo di aggiunta dei controller di archiviazione a SnapCenter.
2. Nella finestra Aggiungi host, aggiungi il tipo di host, il nome host e le credenziali del sistema host. Seleziona il tipo di plug-in. Per SQL Server, selezionare il plug-in Microsoft Windows e Microsoft SQL Server.



3. Per Oracle, compilare i campi obbligatori nella finestra di dialogo Aggiungi host e selezionare la casella di controllo per il plug-in Oracle Database. Quindi fare clic su Invia per avviare il processo di individuazione e aggiungere l'host a SnapCenter.

Add Host

Host Type	Linux	
Host Name	oraclesrv_11.sddc.netapp.com	
Credentials	root	 

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux

Oracle Database

SAP HANA

 [More Options](#) : Port, Install Path, Custom Plug-Ins...

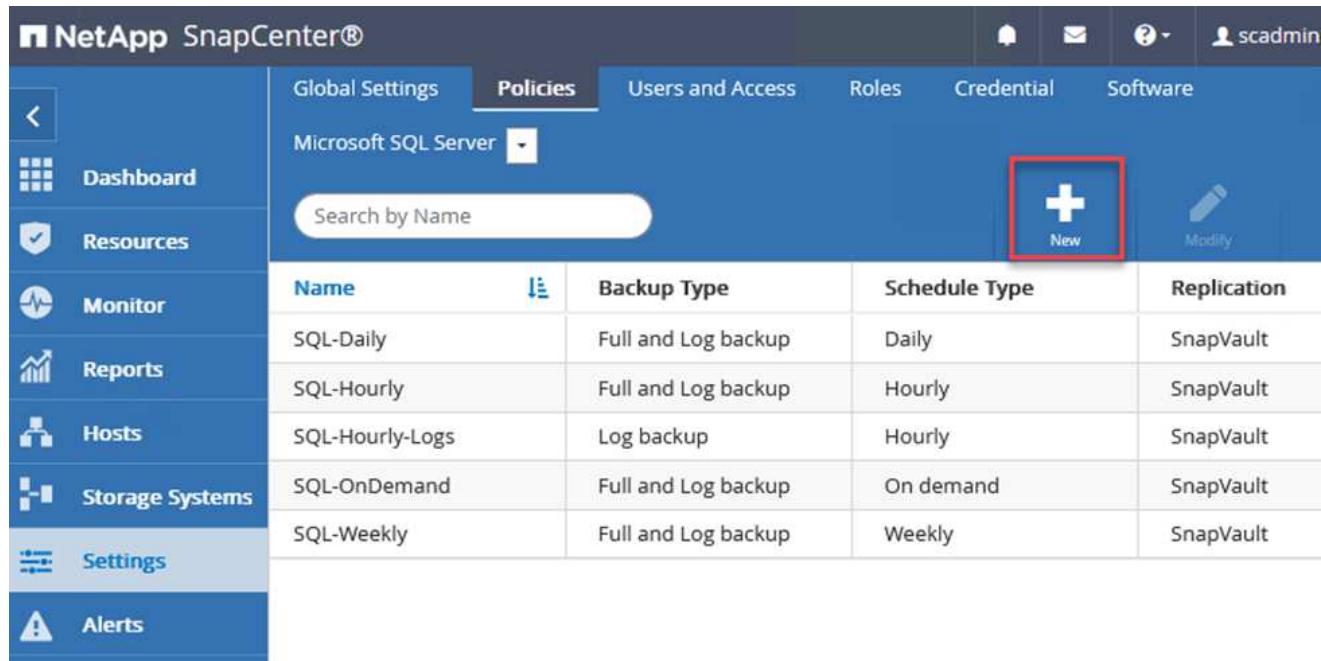
 Submit

 Cancel

Crea criteri SnapCenter

Le policy stabiliscono le regole specifiche da seguire per un processo di backup. Includono, a titolo esemplificativo ma non esaustivo, la pianificazione del backup, il tipo di replica e il modo in cui SnapCenter gestisce il backup e il troncamento dei registri delle transazioni.

È possibile accedere ai criteri nella sezione Impostazioni del client Web SnapCenter .



The screenshot shows the NetApp SnapCenter® web interface. The top navigation bar includes 'Global Settings', 'Policies' (which is the active tab), 'Users and Access', 'Roles', 'Credential', and 'Software'. A dropdown menu for 'Microsoft SQL Server' is open. Below the navigation is a search bar labeled 'Search by Name'. On the left, a sidebar lists 'Dashboard', 'Resources', 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings' (which is the active section), and 'Alerts'. The main content area displays a table of backup policies for Microsoft SQL Server:

Name	Backup Type	Schedule Type	Replication
SQL-Daily	Full and Log backup	Daily	SnapVault
SQL-Hourly	Full and Log backup	Hourly	SnapVault
SQL-Hourly-Logs	Log backup	Hourly	SnapVault
SQL-OnDemand	Full and Log backup	On demand	SnapVault
SQL-Weekly	Full and Log backup	Weekly	SnapVault

Per informazioni complete sulla creazione di criteri per i backup di SQL Server, vedere ["Documentazione SnapCenter"](#) .

Per informazioni complete sulla creazione di policy per i backup di Oracle, vedere ["Documentazione SnapCenter"](#) .

Note:

- Durante la procedura guidata di creazione dei criteri, prestare particolare attenzione alla sezione Replica. In questa sezione puoi specificare i tipi di copie secondarie SnapMirror che desideri vengano eseguite durante il processo di backup.
- L'impostazione "Aggiorna SnapMirror dopo aver creato una copia Snapshot locale" si riferisce all'aggiornamento di una relazione SnapMirror quando tale relazione esiste tra due macchine virtuali di archiviazione che risiedono sullo stesso cluster.
- L'impostazione "Aggiorna SnapVault dopo aver creato una copia Snapshot locale" viene utilizzata per aggiornare una relazione SnapMirror esistente tra due cluster separati e tra un sistema ONTAP locale e Cloud Volumes ONTAP o FSx ONTAP.

L'immagine seguente mostra le opzioni precedenti e il loro aspetto nella procedura guidata dei criteri di backup.

New SQL Server Backup Policy

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose i

Error retry count

3 i

Crea gruppi di risorse SnapCenter

I gruppi di risorse consentono di selezionare le risorse del database che si desidera includere nei backup e i criteri seguiti per tali risorse.

1. Vai alla sezione Risorse nel menu a sinistra.
2. Nella parte superiore della finestra, seleziona il tipo di risorsa con cui lavorare (in questo caso Microsoft SQL Server), quindi fai clic su Nuovo gruppo di risorse.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes the NetApp logo, 'SnapCenter®', a search bar, and user information (scadmin, SnapCenterAdmin, Sign Out). The left sidebar has a 'Resources' section selected, with other options like 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings', and 'Alerts'. The main content area has a 'Microsoft SQL Server' dropdown menu (marked with a red box and number 1) and a 'New Resource Group' button (marked with a red box and number 2). The table below lists three resource groups: SQLSRV-01, SQLSRV-02, and SQLSRV-03, each with a name, resource count, tags, policies, last backup, and overall status.

Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	05/11/2022 ...	Completed

La documentazione SnapCenter illustra dettagliatamente la creazione di gruppi di risorse per i database SQL Server e Oracle.

Per eseguire il backup delle risorse SQL, seguire ["questo collegamento"](#).

Per il backup delle risorse Oracle, seguire ["questo collegamento"](#).

Distribuisci e configura Veeam Backup Server

Nella soluzione viene utilizzato il software Veeam Backup & Replication per eseguire il backup delle macchine virtuali delle nostre applicazioni e archiviare una copia dei backup in un bucket Amazon S3 utilizzando un repository di backup scale-out (SOBR) Veeam. In questa soluzione Veeam è distribuito su un server Windows. Per indicazioni specifiche sulla distribuzione di Veeam, vedere ["Centro assistenza Veeam Documentazione tecnica"](#).

Configurare il repository di backup scalabile Veeam

Dopo aver distribuito e ottenuto la licenza del software, è possibile creare un repository di backup scalabile (SOBR) come archivio di destinazione per i processi di backup. Dovresti anche includere un bucket S3 come backup dei dati della VM fuori sede per il ripristino di emergenza.

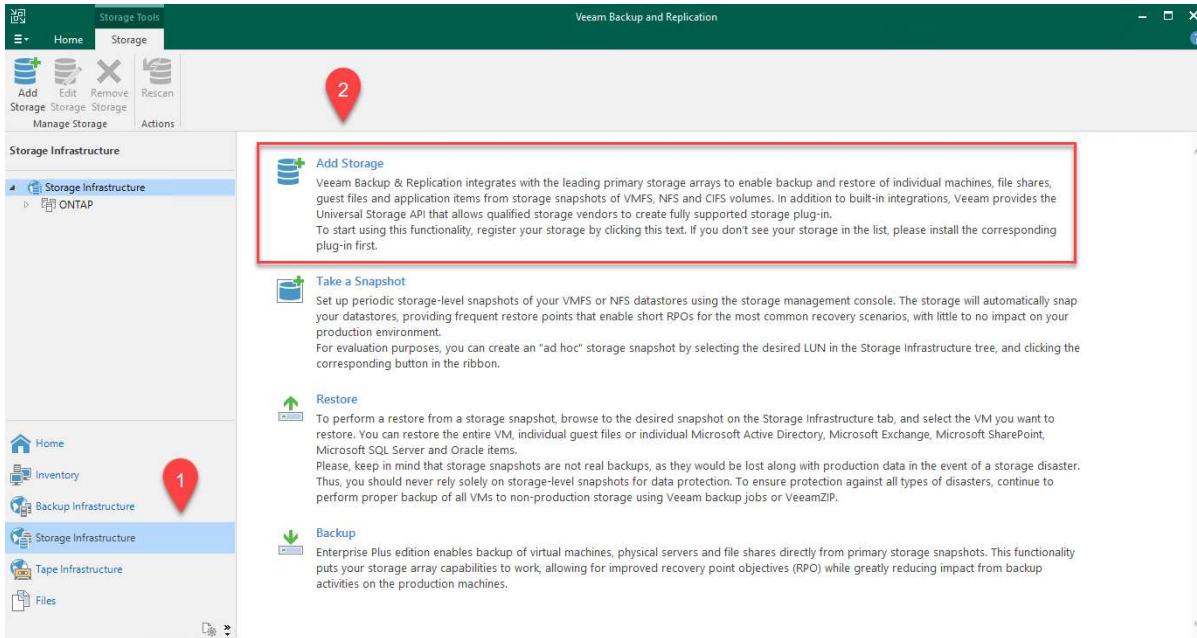
Prima di iniziare, consultare i seguenti prerequisiti.

1. Crea una condivisione file SMB sul tuo sistema ONTAP locale come archivio di destinazione per i backup.
2. Creare un bucket Amazon S3 da includere nel SOBR. Questo è un repository per i backup fuori sede.

Aggiungi ONTAP Storage a Veeam

Per prima cosa, aggiungi il cluster di storage ONTAP e il file system SMB/NFS associato come infrastruttura di storage in Veeam.

1. Apri la console Veeam ed effettua l'accesso. Vai su Infrastruttura di storage e seleziona Aggiungi storage.



2. Nella procedura guidata Aggiungi storage, seleziona NetApp come fornitore di storage, quindi seleziona Data ONTAP.
3. Immettere l'indirizzo IP di gestione e selezionare la casella NAS Filer. Fare clic su Avanti.

New NetApp Data ONTAP Storage

X

Name
Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: 10.61.181.180
Credentials	Description: Created by SDDC\jpowell at 5/17/2022 10:34 AM.
NAS Filer	Role: <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> NAS filer
Apply	
Summary	

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

4. Aggiungi le tue credenziali per accedere al cluster ONTAP .

New NetApp Data ONTAP Storage

X

Credentials
Specify account with storage administrator privileges.

Name	Credentials: HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)
Credentials	Manage accounts Add...
NAS Filer	Protocol: HTTPS
Apply	Port: 443
Summary	

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

5. Nella pagina NAS Filer, selezionare i protocolli desiderati da analizzare e selezionare Avanti.

New NetApp Data ONTAP Storage

X


NAS Filer
Specify how this storage can be accessed by file backup jobs.

Name	Protocol to use:
	<input checked="" type="checkbox"/> SMB
	<input type="checkbox"/> NFS
	<input checked="" type="checkbox"/> Create required export rules automatically
Credentials	Volumes to scan:
NAS Filer	<input type="text" value="All volumes"/> Choose...
Apply	Backup proxies to use:
Summary	<input type="text" value="Automatic selection"/> Choose...

< Previous
Apply
Finish
Cancel

6. Completare le pagine Applica e Riepilogo della procedura guidata e fare clic su Fine per avviare il processo di individuazione dell'archiviazione. Una volta completata la scansione, il cluster ONTAP viene aggiunto insieme ai filer NAS come risorse disponibili.

+
Add
Storage

✎
Edit
Storage

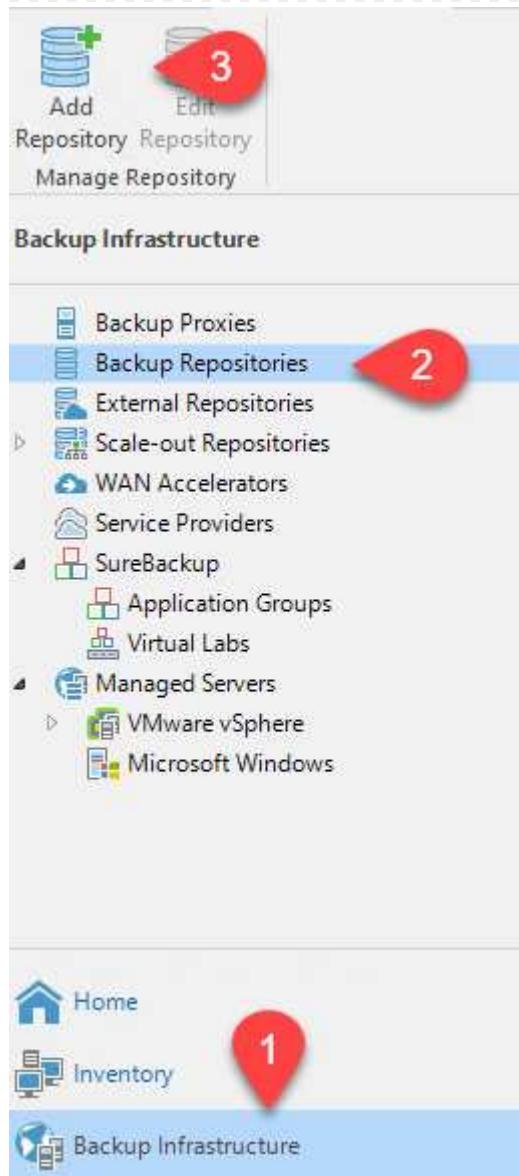
✖
Remove
Storage

⟳
Rescan
Actions

Storage Infrastructure

- ▲ Storage Infrastructure
 - ▲ ONTAP
 - E13A300
 - ▲ OTS-HC-Cluster
 - ▷ svm_nfs-A
 - ▲ svm0
 - ▷ iSCSI_Datastore
 - ▷ sqdb_vol2
 - ▷ sqldb_vol1
 - ▷ svm0_root

7. Creare un repository di backup utilizzando le condivisioni NAS appena scoperte. Da Backup Infrastructure, seleziona Backup Repository e fai clic sulla voce di menu Aggiungi repository.



8. Seguire tutti i passaggi della procedura guidata Nuovo repository di backup per creare il repository. Per informazioni dettagliate sulla creazione di repository di backup Veeam, vedere ["Documentazione Veeam"](#).

New Backup Repository

X



Share

Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

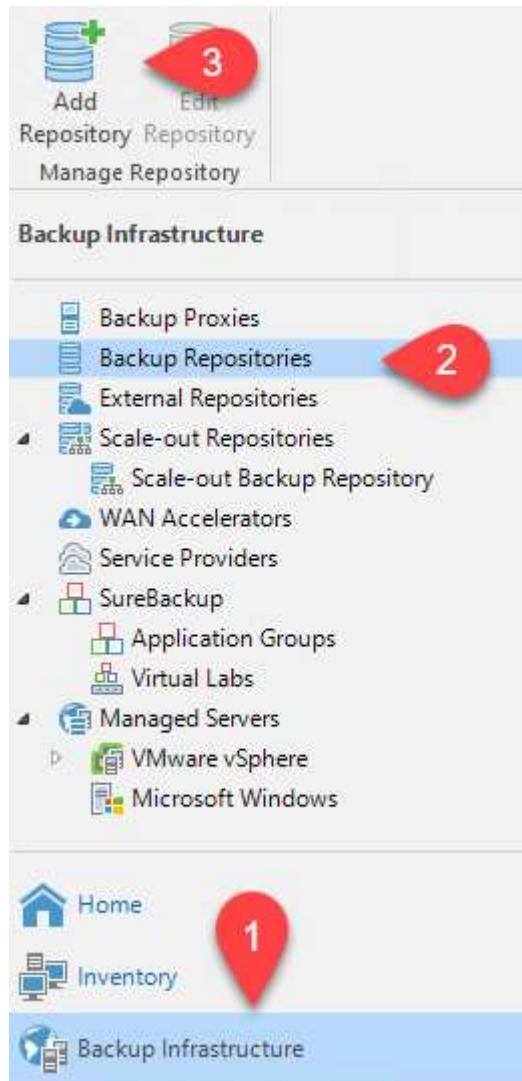
Name	Shared folder: <input type="text" value="\\172.21.162.181\VBRRepo"/> Browse...
Share	<input checked="" type="checkbox"/> This share requires access credentials: <input type="text" value="sddc\administrator (sddc\administrator, last edited: 85 days ago)"/> Add... Manage accounts
Repository	Gateway server: <input checked="" type="radio"/> Automatic selection
Mount Server	<input type="radio"/> The following server: <input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
Review	Use this option to improve performance and reliability of backup to a NAS located in a remote site.
Apply	
Summary	

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

Aggiungi il bucket Amazon S3 come repository di backup

Il passaggio successivo consiste nell'aggiungere lo storage Amazon S3 come repository di backup.

1. Passare a Infrastruttura di backup > Repository di backup. Fare clic su Aggiungi repository.



2. Nella procedura guidata Aggiungi repository di backup, seleziona Object Storage e quindi Amazon S3. Verrà avviata la procedura guidata Nuovo repository di archiviazione oggetti.

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

3. Specifica un nome per il repository di archiviazione degli oggetti e fai clic su Avanti.
4. Nella sezione successiva, fornisci le tue credenziali. Sono necessarie una chiave di accesso AWS e una chiave segreta.

New Object Storage Repository



Account



Specify AWS account to use for connecting to Amazon S3 storage bucket.

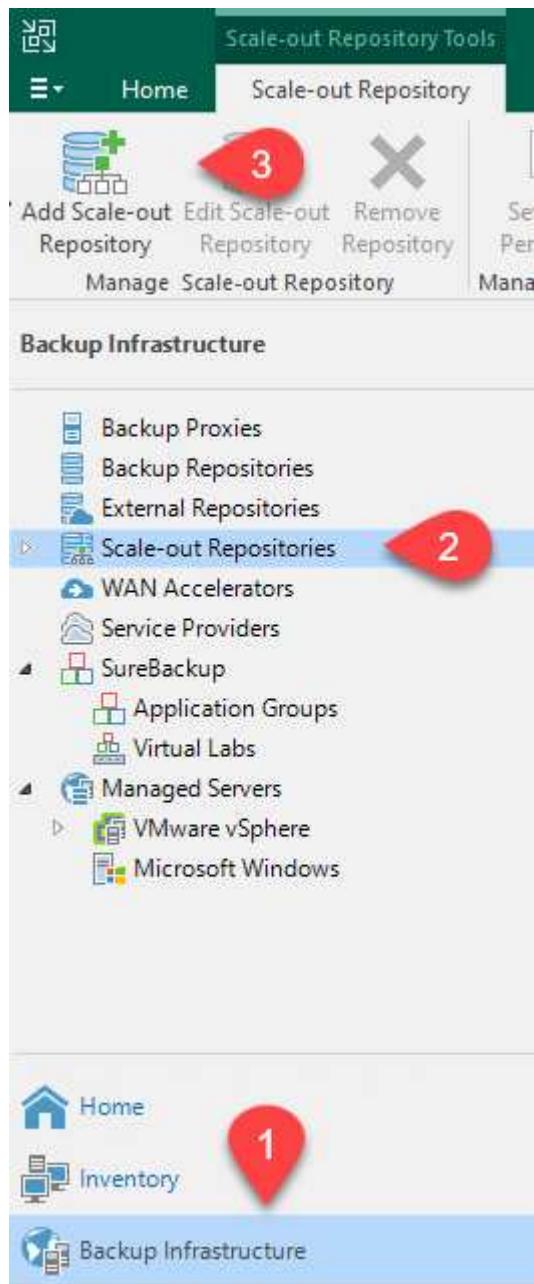
Name	Credentials:	
Account	<input type="text" value="AKIAJ4H43ZT557HXQT2W (last edited: 107 days ago)"/> Add... Manage cloud accounts	
Bucket	AWS region:	
Summary	<input type="text" value="Global"/>	
<input type="checkbox"/> Use the following gateway server: <input type="text" value="veeam.sddc.netapp.com (Backup server)"/> Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.		
< Previous Next > Finish Cancel		

5. Dopo aver caricato la configurazione di Amazon, seleziona il data center, il bucket e la cartella e fai clic su Applica. Infine, fare clic su Fine per chiudere la procedura guidata.

Crea un repository di backup scalabile

Ora che abbiamo aggiunto i nostri repository di storage a Veeam, possiamo creare l'SOBR per suddividere automaticamente le copie di backup nel nostro storage di oggetti Amazon S3 offsite per il disaster recovery.

1. Da Backup Infrastructure, seleziona Scale-out Repositories e quindi fai clic sulla voce di menu Aggiungi Scale-out Repository.



2. Nel Nuovo repository di backup scalabile, immettere un nome per SOBR e fare clic su Avanti.
3. Per il livello di prestazioni, seleziona il repository di backup che contiene la condivisione SMB residente sul tuo cluster ONTAP locale.

New Scale-out Backup Repository

Performance Tier
Select backup repositories to use as the landing zone and for the short-term retention.

Name	Extents:		
Performance Tier	<table border="1"> <thead> <tr> <th>Name</th> </tr> </thead> <tbody> <tr> <td>VBRRepo2</td> </tr> </tbody> </table>	Name	VBRRepo2
Name			
VBRRepo2			
Placement Policy			

Add... **Remove**

4. Per la politica di posizionamento, scegli Località dei dati o Prestazioni in base alle tue esigenze. Seleziona Avanti.
5. Per Capacity Tier estendiamo SOBR con l'archiviazione di oggetti Amazon S3. Ai fini del ripristino di emergenza, selezionare Copia backup in Object Storage non appena vengono creati per garantire la consegna tempestiva dei nostri backup secondari.

New Scale-out Backup Repository

Capacity Tier
Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.

Name	<input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage: <input type="text"/> Amazon S3 Repo Add...
Performance Tier	
Placement Policy	
Capacity Tier	<input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.
Archive Tier	<input checked="" type="checkbox"/> Move backups to object storage as they age out of the operational restore window Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.
Summary	Move backup files older than <input type="text"/> 14 Override...
	<input type="checkbox"/> Encrypt data uploaded to object storage Password: <input type="text"/> Add... Manage passwords

< Previous **Next >** **Finish** **Cancel**

6. Infine, seleziona Applica e Fine per finalizzare la creazione del SOBR.

Creare i processi di repository di backup scalabili

Il passaggio finale per configurare Veeam consiste nel creare processi di backup utilizzando il SOBR appena creato come destinazione di backup. La creazione di processi di backup è una normale attività del repertorio di qualsiasi amministratore di storage e in questa sede non verranno illustrati i passaggi dettagliati. Per informazioni più complete sulla creazione di processi di backup in Veeam, vedere ["Documentazione tecnica del Centro assistenza Veeam"](#).

Strumenti e configurazione BlueXP backup and recovery

Per eseguire un failover delle VM delle applicazioni e dei volumi del database sui servizi VMware Cloud Volume in esecuzione su AWS, è necessario installare e configurare un'istanza in esecuzione sia di SnapCenter Server che di Veeam Backup and Replication Server. Una volta completato il failover, è necessario configurare questi strumenti anche per riprendere le normali operazioni di backup finché non viene pianificato ed eseguito un fallback nel data center locale.

Distribuisci il server Windows SnapCenter secondario

SnapCenter Server viene distribuito nel VMware Cloud SDDC o installato su un'istanza EC2 residente in una VPC con connettività di rete all'ambiente VMware Cloud.

Il SnapCenter software è disponibile sul sito di supporto NetApp e può essere installato sui sistemi Microsoft Windows che risiedono in un dominio o in un gruppo di lavoro. Una guida dettagliata alla pianificazione e alle istruzioni di installazione sono disponibili sul sito "[Centro di documentazione NetApp](#)" .

Puoi trovare il SnapCenter software su "[questo collegamento](#)" .

Configurare il server secondario Windows SnapCenter

Per eseguire un ripristino dei dati dell'applicazione sottoposti a mirroring su FSx ONTAP, è necessario prima eseguire un ripristino completo del database SnapCenter locale. Una volta completato questo processo, la comunicazione con le VM viene ristabilita e i backup delle applicazioni possono ora riprendere utilizzando FSx ONTAP come storage primario.

Per raggiungere questo obiettivo, è necessario completare le seguenti operazioni sul server SnapCenter :

1. Configurare il nome del computer in modo che sia identico al server SnapCenter locale originale.
2. Configurare la rete per comunicare con VMware Cloud e l'istanza FSx ONTAP .
3. Completare la procedura per ripristinare il database SnapCenter .
4. Verificare che SnapCenter sia in modalità Disaster Recovery per assicurarsi che FSx sia ora l'archivio primario per i backup.
5. Verificare che la comunicazione con le macchine virtuali ripristinate sia stata ristabilita.

Distribuisci il server Veeam Backup & Replication secondario

È possibile installare il server Veeam Backup & Replication su un server Windows nel VMware Cloud su AWS o su un'istanza EC2. Per una guida dettagliata all'implementazione, vedere "[Documentazione tecnica del Centro assistenza Veeam](#)" .

Configurare il server Veeam Backup & Replication secondario

Per eseguire un ripristino di macchine virtuali di cui è stato eseguito il backup nello storage Amazon S3, è necessario installare Veeam Server su un server Windows e configurarlo per comunicare con VMware Cloud, FSx ONTAP e il bucket S3 che contiene il repository di backup originale. Deve inoltre disporre di un nuovo repository di backup configurato su FSx ONTAP per eseguire nuovi backup delle VM dopo il loro ripristino.

Per eseguire questo processo, è necessario completare i seguenti elementi:

1. Configurare la rete per comunicare con VMware Cloud, FSx ONTAP e il bucket S3 contenente il repository di backup originale.
2. Configurare una condivisione SMB su FSx ONTAP come nuovo repository di backup.
3. Montare il bucket S3 originale utilizzato come parte del repository di backup scalabile in locale.
4. Dopo aver ripristinato la VM, stabilire nuovi processi di backup per proteggere le VM SQL e Oracle.

Per ulteriori informazioni sul ripristino delle VM tramite Veeam, consultare la sezione "["Ripristina le VM delle applicazioni con Veeam Full Restore"](#)" .

Backup del database SnapCenter per il ripristino di emergenza

SnapCenter consente il backup e il ripristino del database MySQL sottostante e dei dati di configurazione allo scopo di ripristinare il server SnapCenter in caso di disastro. Per la nostra soluzione, abbiamo recuperato il database e la configurazione SnapCenter su un'istanza AWS EC2 residente nella nostra VPC. Per ulteriori informazioni sul ripristino di emergenza di SnapCenter, vedere "["questo collegamento"](#)" .

Prerequisiti per il backup SnapCenter

Per il backup SnapCenter sono richiesti i seguenti prerequisiti:

- Un volume e una condivisione SMB creati sul sistema ONTAP locale per individuare il database sottoposto a backup e i file di configurazione.
- Una relazione SnapMirror tra il sistema ONTAP locale e FSx o CVO nell'account AWS. Questa relazione viene utilizzata per trasportare lo snapshot contenente il database SnapCenter sottoposto a backup e i file di configurazione.
- Windows Server installato nell'account cloud, su un'istanza EC2 o su una macchina virtuale nel VMware Cloud SDDC.
- SnapCenter installato sull'istanza Windows EC2 o sulla VM in VMware Cloud.

Riepilogo del processo di backup e ripristino SnapCenter

- Creare un volume sul sistema ONTAP locale per ospitare il database di backup e i file di configurazione.
- Impostare una relazione SnapMirror tra locale e FSx/CVO.
- Montare la condivisione SMB.
- Recupera il token di autorizzazione Swagger per eseguire attività API.
- Avviare il processo di ripristino del database.
- Utilizzare l'utilità xcopy per copiare la directory locale del database e del file di configurazione nella condivisione SMB.
- Su FSx, creare un clone del volume ONTAP (copiato tramite SnapMirror da locale).
- Montare la condivisione SMB da FSx a EC2/VMware Cloud.
- Copiare la directory di ripristino dalla condivisione SMB a una directory locale.
- Eseguire il processo di ripristino di SQL Server da Swagger.

Eseguire il backup del database e della configurazione SnapCenter

SnapCenter fornisce un'interfaccia client Web per l'esecuzione dei comandi REST API. Per informazioni sull'accesso alle API REST tramite Swagger, consultare la documentazione SnapCenter all'indirizzo ["questo collegamento"](#).

Accedi a Swagger e ottieni il token di autorizzazione

Dopo aver navigato fino alla pagina Swagger, è necessario recuperare un token di autorizzazione per avviare il processo di ripristino del database.

1. Accedi alla pagina web dell'API SnapCenter Swagger all'indirizzo <https://< SnapCenter Server IP>:8146/swagger/>.



SnapCenter API

[Base URL: /api]

<https://snapcentersddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.

To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use https://{{SCV_hostname}}:{{SCV_host_port}}/api/swagger-ui.html

2. Espandi la sezione Autenticazione e fai clic su Provalo.

Auth

POST

/4.6/auth/login Service login

The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.

Parameters

Try it out

3. Nell'area UserOperationContext, compilare le credenziali e il ruolo SnapCenter e fare clic su Esegui.

Name	Description
TokenNeverExpires boolean (query)	Token never expires <input type="text" value="false"/>
UserOperationContext * required object (body)	User credentials Edit Value Model <pre>{ "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } }</pre> <input type="button" value="Cancel"/>
Parameter content type <input type="text" value="application/json"/>	
<input type="button" value="Execute"/>	

4. Nel corpo della risposta qui sotto puoi vedere il token. Copiare il testo del token per l'autenticazione durante l'esecuzione del processo di backup.

200 Response body

```

  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
"User": {
  "Token": "KLYxOg==tsV6EOditdAmAYpe8q5SG6wcoGaSjmE6jrNy5CsY63HQ51koZLIESRNAhpGJJ0UUQynENDgtVGDZnvx+I/ZJZIn5M1NZrj6
CLfGTApq1GmcagT08bgb5bNTx07EcdrAidzAXUDb3GyLOKtW0GdwKzSeUwKj3uVupnk1E31skK6PRBv9RS8j0qHQvo4v4RL0hhThhwPhV
9/23nFejVP/p1Ev4vrV/zeZVTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjO==",
  "Name": "SCAdmin",
  "TokenHashed": null,
  "Type": "",
  "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
  "Id": "1",
  "FullName": "SCAdmin",
  "Host": null,
  "Author": null,
  "UserName": "",
  "Domain": "",
  "Passphrase": ""
}

```

[Download](#)

Eseguire un backup del database SnapCenter

Successivamente, vai all'area Disaster Recovery nella pagina Swagger per avviare il processo di backup SnapCenter .

1. Espandi l'area Disaster Recovery cliccandoci sopra.

Disaster Recovery

GET /4.6/disasterrecovery/server/backup Fetch all the existing SnapCenter Server DR Backups.

POST /4.6/disasterrecovery/server/backup Starts the SnapCenter Server DR backup.

DELETE /4.6/disasterrecovery/server/backup Deletes the existing Snapcenter DR backup.

POST /4.6/disasterrecovery/server/restore Starts SnapCenter Server Restore.

POST /4.6/disasterrecovery/storage Enable or disable the storage disaster recovery.

2. Espandi il /4.6/disasterrecovery/server/backup sezione e clicca su Provalo.

POST /4.6/disasterrecovery/server/backup Starts the SnapCenter Server DR backup.

Starts and creates a new SnapCenter Server DR backup.

Parameters

Try it out

3. Nella sezione SmDRBackupRequest, aggiungere il percorso di destinazione locale corretto e selezionare Esegui per avviare il backup del database e della configurazione SnapCenter .



Il processo di backup non consente di eseguire il backup direttamente su una condivisione file NFS o CIFS.

Name	Description
Token * required string (header)	User authorization token TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==
SmDRBackupRequest * required object (body)	Parameters to take Backup Edit Value Model <pre>{ "TargetPath": "C:\\SnapCenter_Backups\\" }</pre>
<div style="text-align: center;"> Cancel </div> <div style="display: flex; justify-content: space-between;"> Parameter content type <div style="border: 1px solid #ccc; padding: 2px;"> application/json </div> </div>	
Execute	

Monitorare il processo di backup da SnapCenter

Accedi a SnapCenter per rivedere i file di registro quando avvii il processo di ripristino del database. Nella sezione Monitor è possibile visualizzare i dettagli del backup di ripristino di emergenza del server SnapCenter .

Job Details

SnapCenter Server disaster recovery backup

- ✓ ▾ SnapCenter Server disaster recovery backup
 - ✓ ▶ Precheck validation
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of SnapCenter Server 'SnapCenter.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_07.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_10.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-01.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_09.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'

Task Name: SnapCenter Server disaster recovery backup Start Time: 03/23/2022 10:27:11 AM End Time: 03/23/2022 10:27:47 AM

[View Logs](#) [Cancel Job](#) [Close](#)

Utilizzare l'utilità XCOPY per copiare il file di backup del database nella condivisione SMB

Successivamente è necessario spostare il backup dall'unità locale sul server SnapCenter alla condivisione CIFS utilizzata per copiare i dati SnapMirror nella posizione secondaria situata sull'istanza FSx in AWS. Utilizzare xcopy con opzioni specifiche che mantengano le autorizzazioni dei file.

Aprire un prompt dei comandi come amministratore. Dal prompt dei comandi, immettere i seguenti comandi:

```
xcopy <Source_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X  
/E /H /K  
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O  
/X /E /H /K
```

Failover

Il disastro si verifica nel sito primario

In caso di disastro che si verifica nel data center principale in sede, il nostro scenario prevede il failover su un sito secondario residente sull'infrastruttura Amazon Web Services tramite VMware Cloud su AWS. Supponiamo che le macchine virtuali e il nostro cluster ONTAP locale non siano più accessibili. Inoltre, le macchine virtuali SnapCenter e Veeam non sono più accessibili e devono essere ricostruite presso il nostro sito secondario.

Questa sezione affronta il failover della nostra infrastruttura sul cloud e tratta i seguenti argomenti:

- Ripristino del database SnapCenter . Dopo aver stabilito un nuovo server SnapCenter , ripristinare il database MySQL e i file di configurazione e attivare la modalità di ripristino di emergenza del database per consentire allo storage FSx secondario di diventare il dispositivo di storage primario.
- Ripristinare le macchine virtuali dell'applicazione utilizzando Veeam Backup & Replication. Collegare l'archiviazione S3 che contiene i backup delle VM, importare i backup e ripristinarli su VMware Cloud su AWS.
- Ripristinare i dati dell'applicazione SQL Server utilizzando SnapCenter.
- Ripristinare i dati dell'applicazione Oracle utilizzando SnapCenter.

Processo di ripristino del database SnapCenter

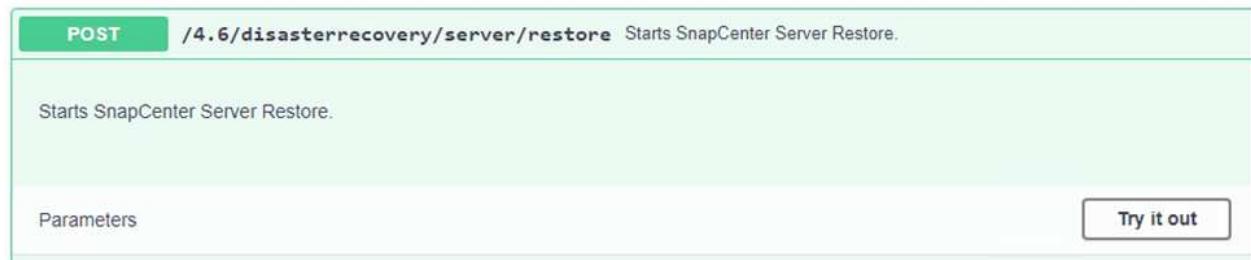
SnapCenter supporta scenari di disaster recovery consentendo il backup e il ripristino del suo database MySQL e dei file di configurazione. Ciò consente a un amministratore di mantenere backup regolari del database SnapCenter nel data center locale e di ripristinare successivamente tale database in un database SnapCenter secondario.

Per accedere ai file di backup SnapCenter sul server SnapCenter remoto, completare i seguenti passaggi:

1. Interrompere la relazione SnapMirror dal cluster FSx, rendendo il volume di lettura/scrittura.
2. Creare un server CIFS (se necessario) e creare una condivisione CIFS che punti al percorso di giunzione del volume clonato.
3. Utilizzare xcopy per copiare i file di backup in una directory locale sul sistema SnapCenter secondario.
4. Installa SnapCenter v4.6.
5. Assicurarsi che il server SnapCenter abbia lo stesso FQDN del server originale. Ciò è necessario affinché il ripristino del database abbia esito positivo.

Per avviare il processo di ripristino, completare i seguenti passaggi:

1. Accedere alla pagina web dell'API Swagger per il server SnapCenter secondario e seguire le istruzioni precedenti per ottenere un token di autorizzazione.
2. Vai alla sezione Disaster Recovery della pagina Swagger, seleziona `/4.6/disasterrecovery/server/restore` e fai clic su Provalo.



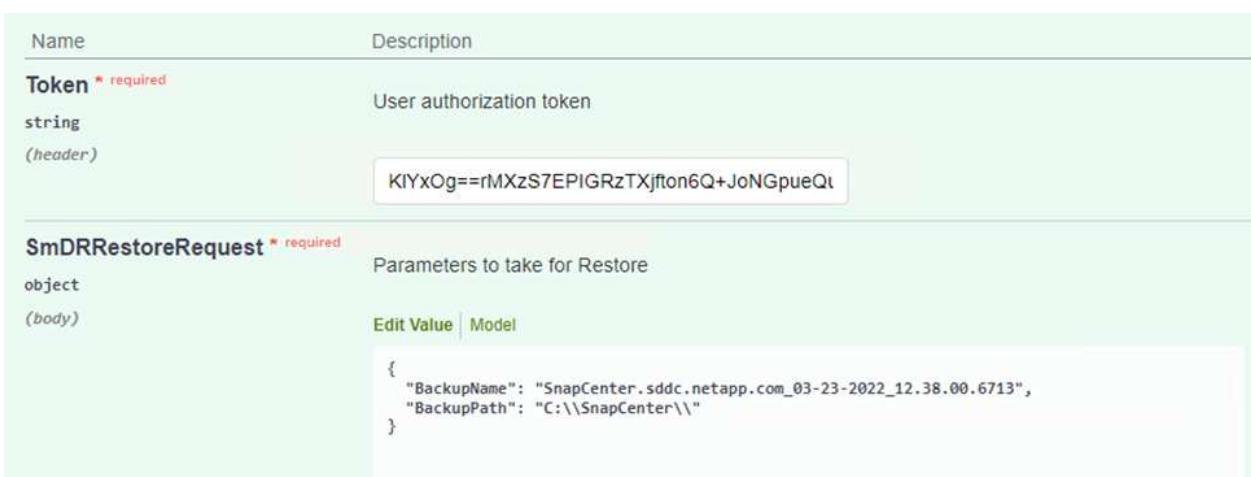
POST `/4.6/disasterrecovery/server/restore` Starts SnapCenter Server Restore.

Starts SnapCenter Server Restore.

Parameters

Try it out

3. Incolla il token di autorizzazione e, nella sezione SmDRRestRequest, incolla il nome del backup e la directory locale sul server SnapCenter secondario.



Name	Description
Token * required	User authorization token
string	
(header)	K1YxOg==rMXzS7EPIGRzTXjftn6Q+JoNGpueQI
SmDRRestoreRequest * required	Parameters to take for Restore
object	
(body)	Edit Value Model
	{ "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713", "BackupPath": "C:\\SnapCenter\\\\" }

4. Selezionare il pulsante Esegui per avviare il processo di ripristino.
5. Da SnapCenter, vai alla sezione Monitor per visualizzare l'avanzamento del processo di ripristino.

ID	Status	Name
20482	✓	SnapCenter Server Disaster Recovery
20481	✓	SnapCenter Server disaster recovery backup
20480	✗	SnapCenter Server disaster recovery backup
20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
20473	⌚	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
20472	✗	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- ✓ ▾ SnapCenter Server Disaster Recovery
 - ✓ ▾ Prepare for restore job
 - ✓ ▾ Precheck validation
 - ✓ ▾ Saving original server state
 - ✓ ▾ Schedule restore
 - ✓ ▾ Repository restore
 - ✓ ▾ Config restore
 - ✓ ▾ Reset MySQL password

6. Per abilitare i ripristini di SQL Server dall'archiviazione secondaria, è necessario impostare il database SnapCenter in modalità Disaster Recovery. Questa operazione viene eseguita separatamente e avviata sulla pagina web dell'API Swagger.
 - Passare alla sezione Disaster Recovery e fare clic su `/4.6/disasterrecovery/storage`.
 - Incolla il token di autorizzazione dell'utente.
 - Nella sezione `SmSetDisasterRecoverySettingsRequest`, modificare `EnableDisasterRecover` A `true`.
 - Fare clic su Esegui per abilitare la modalità di ripristino di emergenza per SQL Server.

Name	Description
Token <small>* required</small> string (header)	User authorization token K1YxOg==rMXzS7EPIGRzTXjton6Q+JoNGpueQu
SmSetDisasterRecoverySettingsRequest <small>* required</small> object (body)	Parameters to enable or disable the DR mode Edit Value Model { "EnableDisasterRecovery": true }



Vedere i commenti relativi alle procedure aggiuntive.

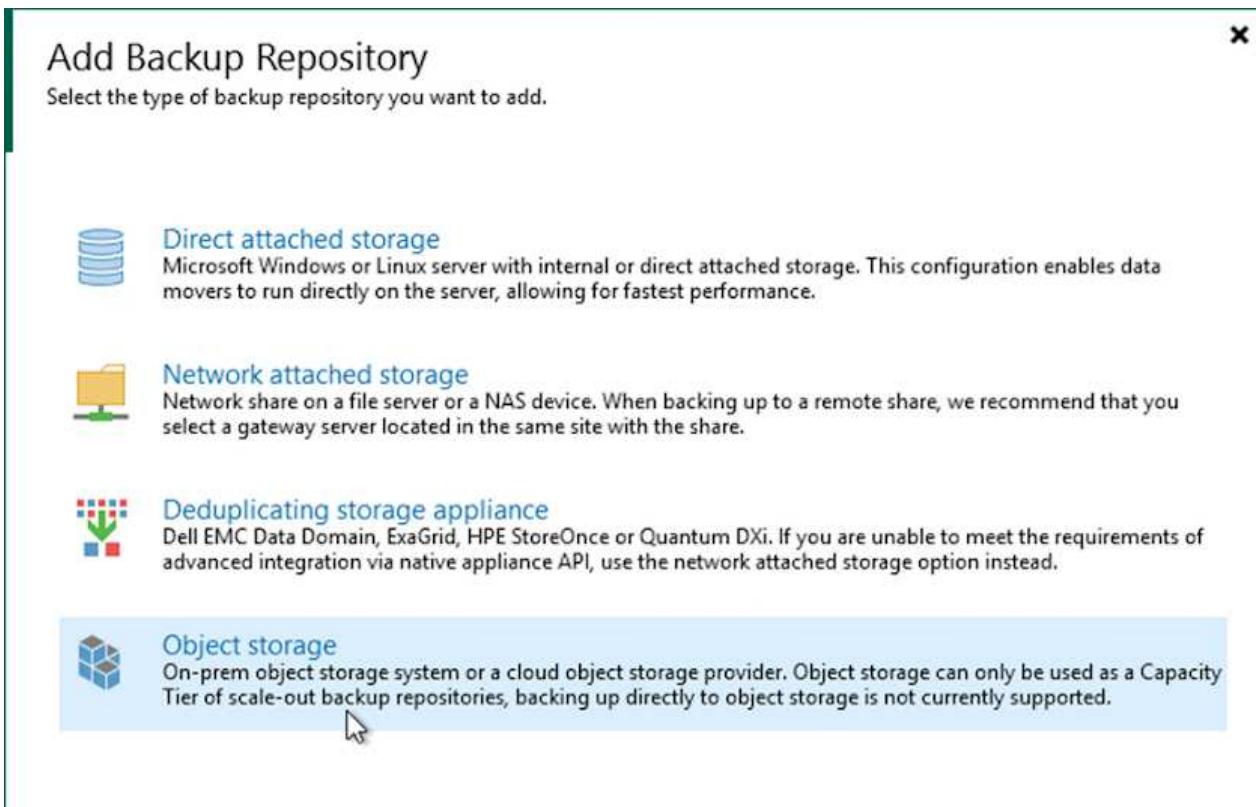
Ripristina le VM delle applicazioni con il ripristino completo di Veeam

Crea un repository di backup e importa i backup da S3

Dal server Veeam secondario, importa i backup dallo storage S3 e ripristina le VM SQL Server e Oracle nel tuo cluster VMware Cloud.

Per importare i backup dall'oggetto S3 che faceva parte del repository di backup scalabile in locale, completare i seguenti passaggi:

1. Vai a Backup Repositories e fai clic su Aggiungi repository nel menu in alto per avviare la procedura guidata Aggiungi repository di backup. Nella prima pagina della procedura guidata, seleziona Object Storage come tipo di repository di backup.



2. Selezionare Amazon S3 come tipo di Object Storage.

Object Storage

Select the type of object storage you want to use as a backup repository.



S3 Compatible

Adds an on-premises object storage system or a cloud object storage provider.



Amazon S3

Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.



Google Cloud Storage

Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.



IBM Cloud Object Storage

Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.



Microsoft Azure Storage

Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

3. Dall'elenco dei servizi di archiviazione cloud Amazon, seleziona Amazon S3.



Amazon Cloud Storage Services

Select the type of Amazon storage you want to use as a backup repository.



Amazon S3

Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.



Amazon S3 Glacier

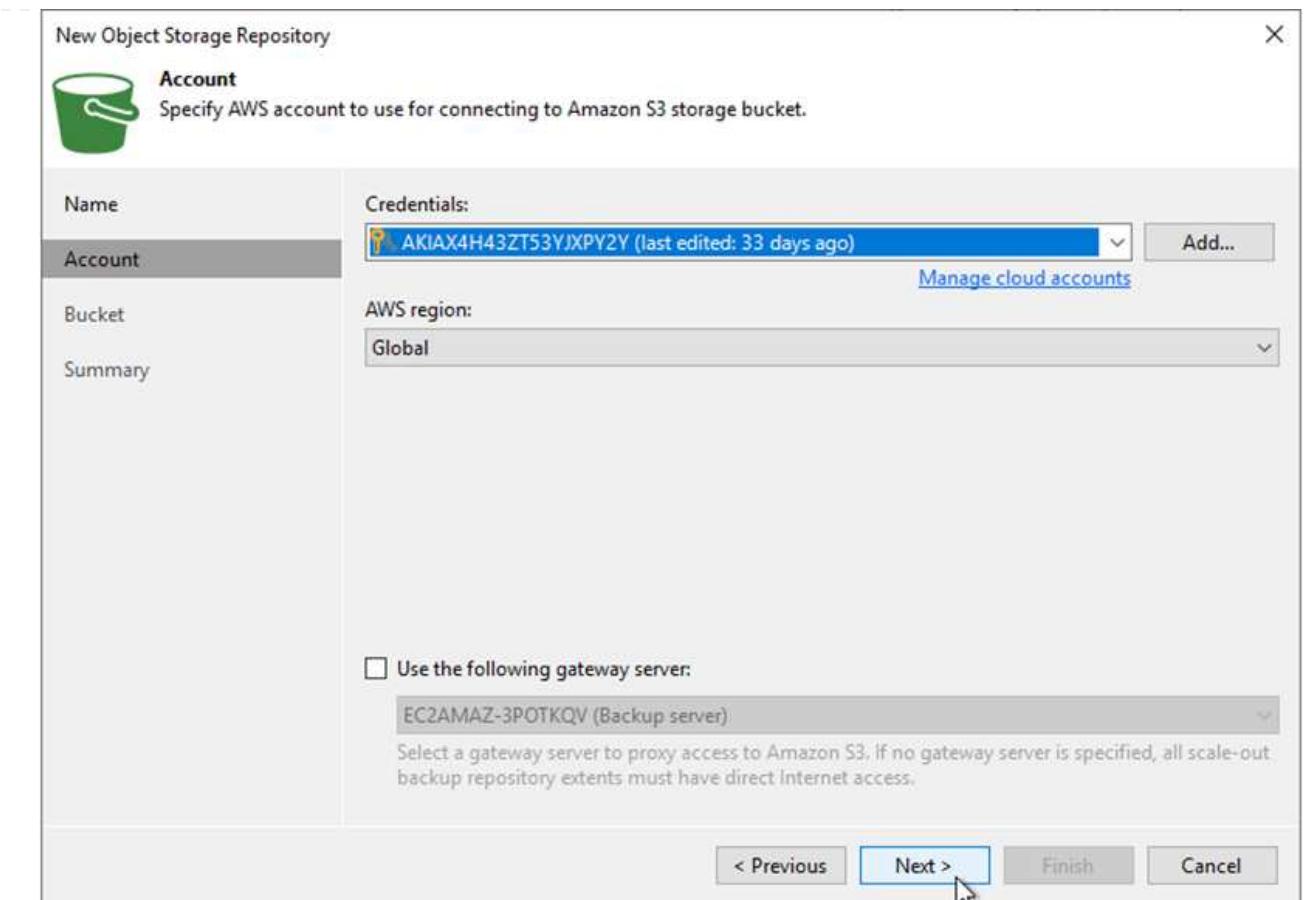
Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.



AWS Snowball Edge

Adds AWS Snowball Edge appliance to enable seeding of backups into Amazon S3 object storage.

4. Seleziona le credenziali pre-immesse dall'elenco a discesa oppure aggiungi una nuova credenziale per accedere alla risorsa di archiviazione cloud. Fare clic su Avanti per continuare.



5. Nella pagina Bucket, inserisci il data center, il bucket, la cartella e tutte le opzioni desiderate. Fare clic su Applica.

New Object Storage Repository

X



Bucket

Specify Amazon S3 bucket to use.

Name

Data center:

US East (N. Virginia)

Account

Bucket:

ehcveeamrepo

[Browse...](#)

Bucket

Summary

Folder:

RTP

[Browse...](#)

Limit object storage consumption to: 10 TB

This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.

Make recent backups immutable for: 30 days

Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.

Use infrequent access storage class (may result in higher costs)

With lower price per GB but higher retrieval and early deletion fees, this storage class is best suited for long-term storage of GFS full backups. Avoid using it for short-term storage of recent backups.

Store backups in a single availability zone (even lower price per GB, reduced resilience)

[< Previous](#)

[Apply](#)

[Finish](#)

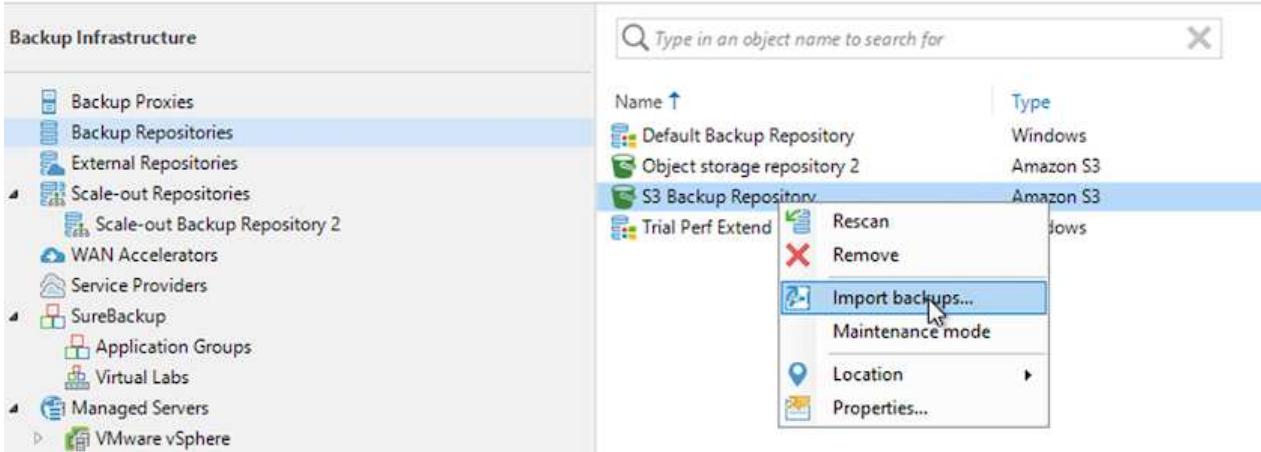
[Cancel](#)

6. Infine, seleziona Fine per completare il processo e aggiungere il repository.

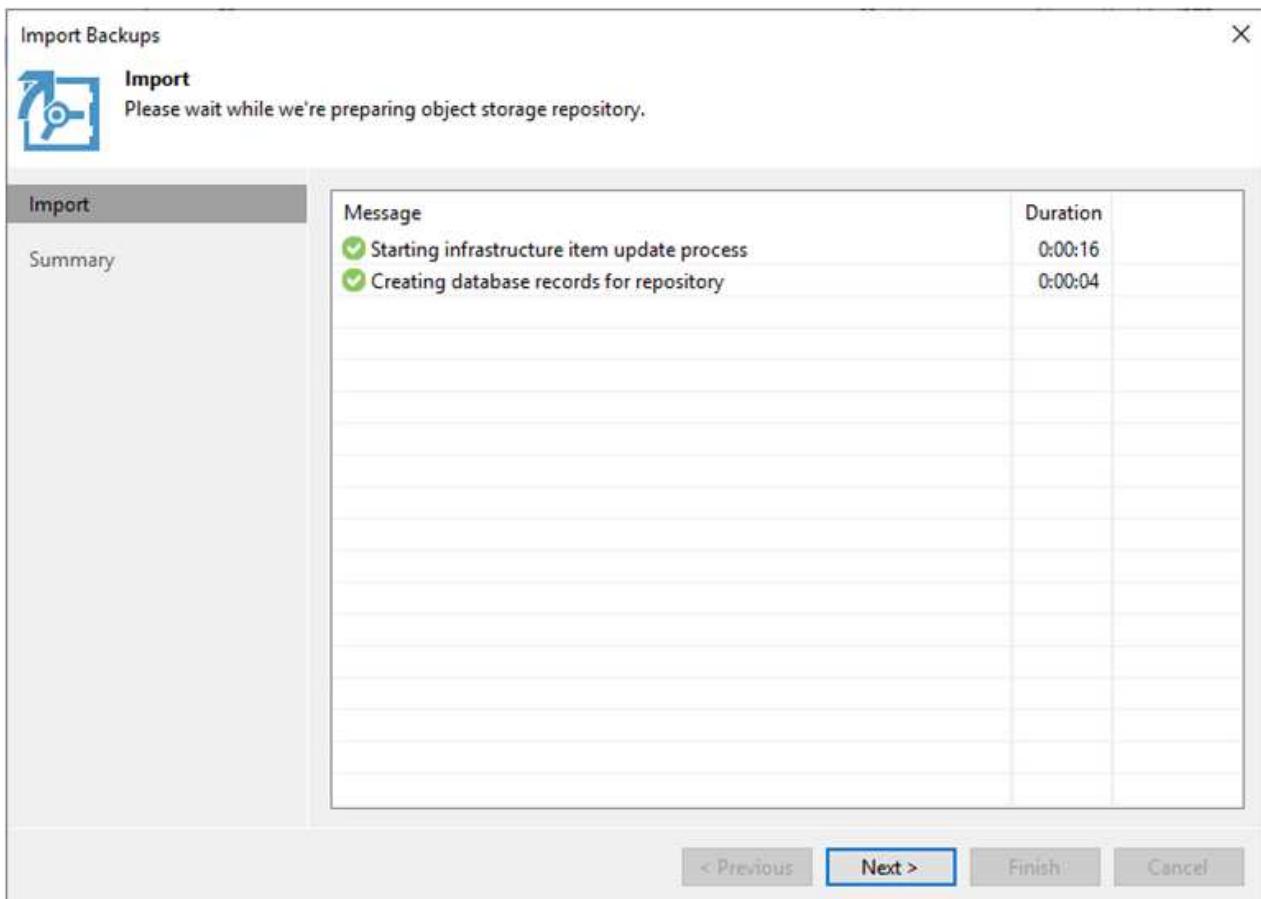
Importa backup dall'archiviazione di oggetti S3

Per importare i backup dal repository S3 aggiunto nella sezione precedente, completare i passaggi seguenti.

1. Dal repository di backup S3, seleziona Importa backup per avviare la procedura guidata Importa backup.



2. Dopo aver creato i record del database per l'importazione, selezionare Avanti e poi Fine nella schermata di riepilogo per avviare il processo di importazione.



3. Una volta completata l'importazione, è possibile ripristinare le VM nel cluster VMware Cloud.

System

X

Name: Configuration Database Resynchroniz... Status: Success
Action type: Configuration Resynchronize Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin End time: 4/6/2022 3:04:57 PM

Log

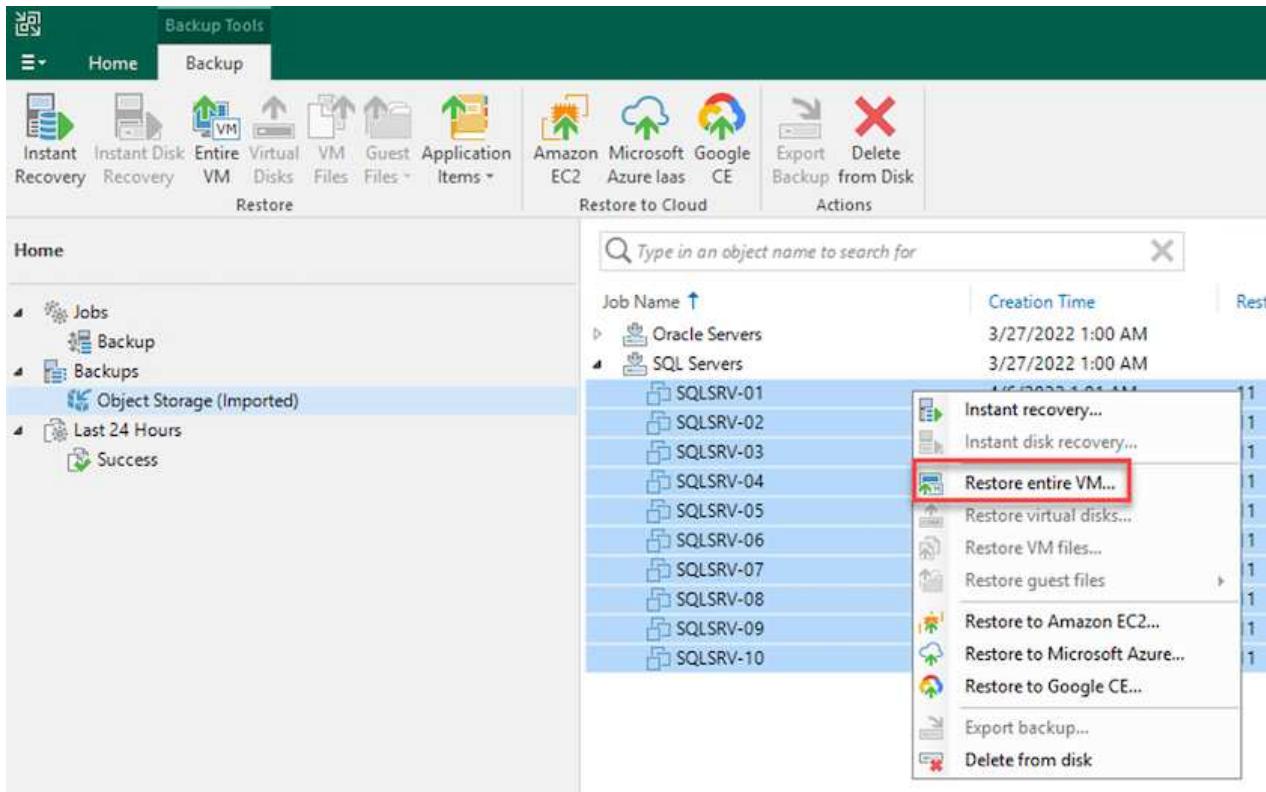
Message	Duration
✓ Starting backup repositories synchronization	
✓ Enumerating repositories	
✓ Found 1 repository	
✓ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✓ S3 Backup Repository: added 2 unencrypted	0:03:20
✓ Importing backup 2 out of 2	0:03:15
✓ Backup repositories synchronization completed successfully	

Close

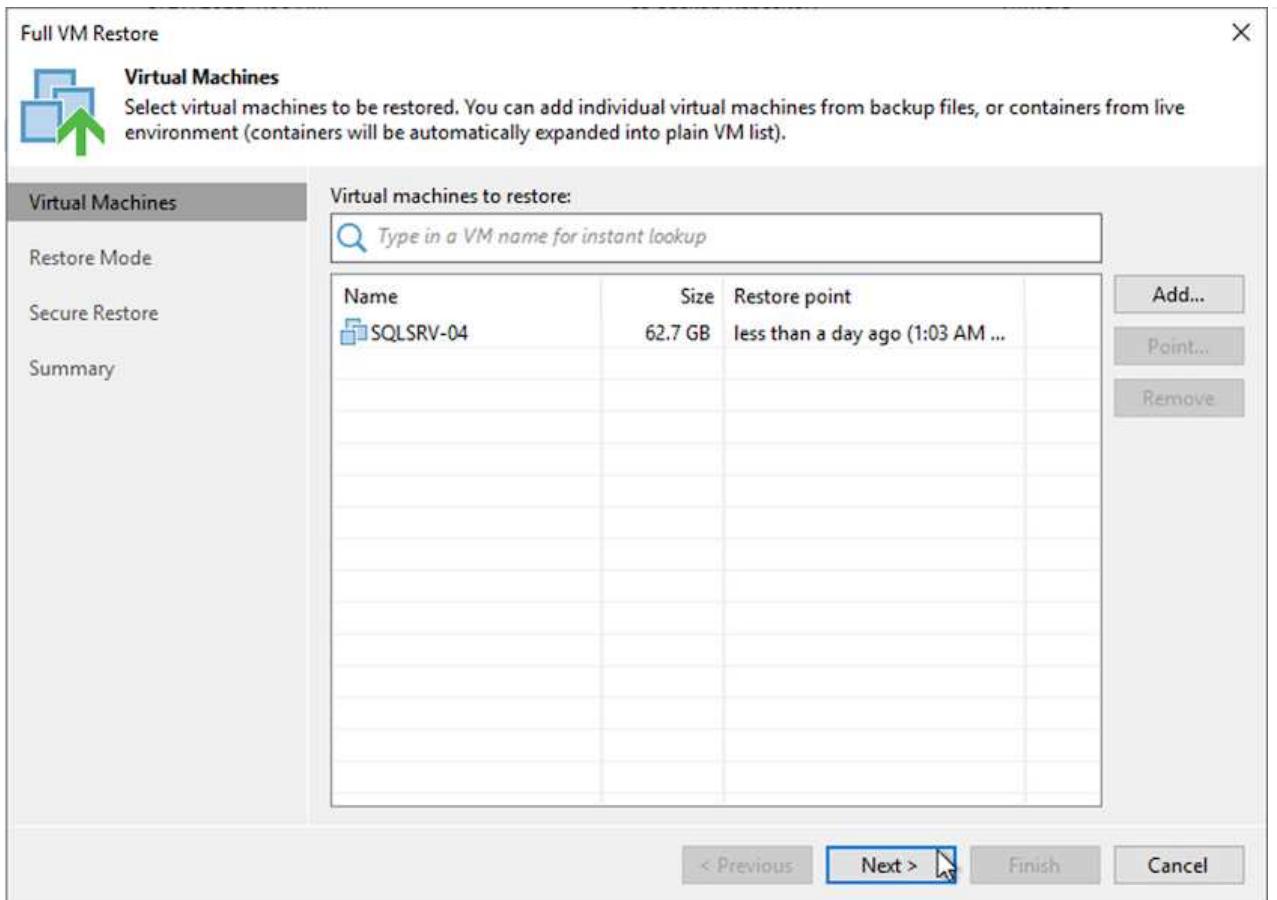
Ripristina le VM delle applicazioni con il ripristino completo di Veeam su VMware Cloud

Per ripristinare le macchine virtuali SQL e Oracle nel dominio/cluster del carico di lavoro VMware Cloud on AWS, completare i seguenti passaggi.

1. Dalla home page di Veeam, seleziona l'archivio oggetti contenente i backup importati, seleziona le VM da ripristinare, quindi fai clic con il pulsante destro del mouse e seleziona Ripristina intera VM.



2. Nella prima pagina della procedura guidata Ripristino completo della VM, modificare le VM da sottoporre a backup, se desiderato, e selezionare Avanti.



3. Nella pagina Modalità di ripristino, seleziona Ripristina in una nuova posizione o con impostazioni diverse.

Full VM Restore

 **Restore Mode**
Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines

Restore Mode **Restore to the original location**
Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.

Restore to a new location, or with different settings
Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.

Staged restore
Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.

Host

Resource Pool

Datastore

Folder

Network [Pick proxy to use](#)

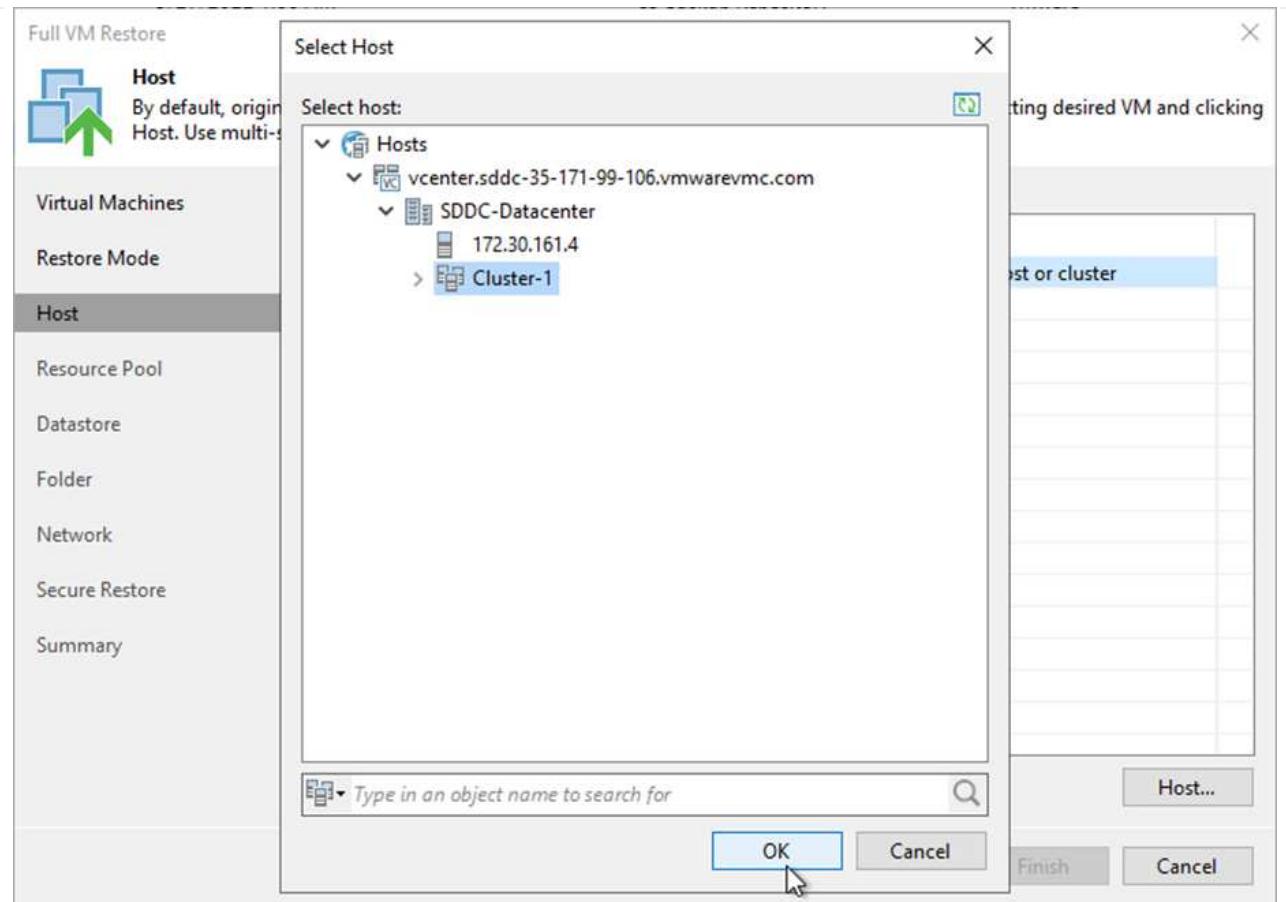
Secure Restore

Summary

Quick rollback (restore changed blocks only)
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

4. Nella pagina host, seleziona l'host o il cluster ESXi di destinazione su cui ripristinare la VM.



5. Nella pagina Datastore, selezionare la posizione del datastore di destinazione sia per i file di configurazione che per il disco rigido.

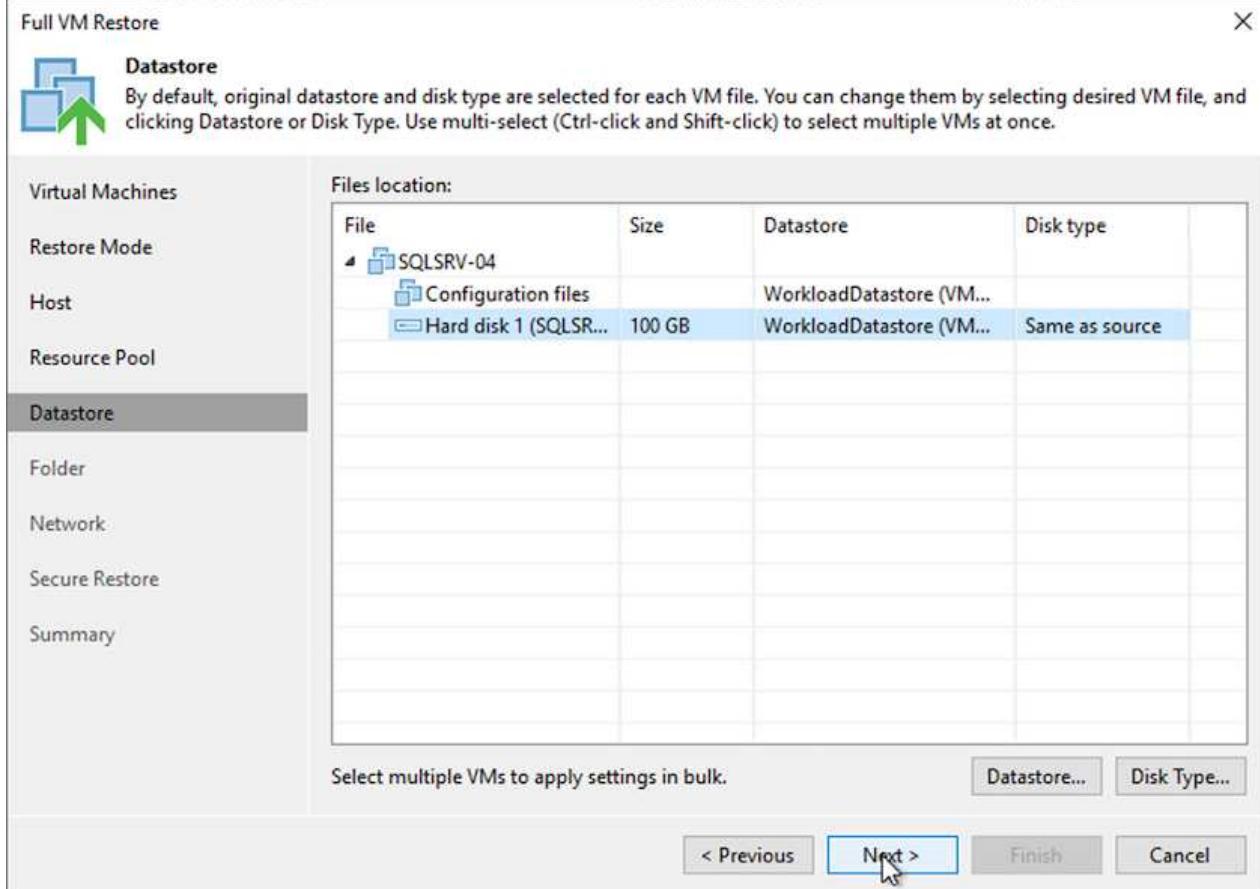
Full VM Restore

Datastore
By default, original datastore and disk type are selected for each VM file. You can change them by selecting desired VM file, and clicking Datastore or Disk Type. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.

File	Size	Datastore	Disk type
SQLSRV-04		WorkloadDatastore (VM...)	
Configuration files			
Hard disk 1 (SQLSRV-04)	100 GB	WorkloadDatastore (VM...)	Same as source

Select multiple VMs to apply settings in bulk.

< Previous **Next >** Finish Cancel



6. Nella pagina Rete, mappare le reti originali sulla VM alle reti nella nuova posizione di destinazione.

Full VM Restore



Network

By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Summary

Network connections:

Source	Target
SQLSRV-04	
Management 181 (DSwitch)	Not connected
Data - A - 3374 (DSwitch)	Not connected
Data - B - 3375 (DSwitch)	Not connected

Select multiple VMs to apply settings change in bulk.

Network...

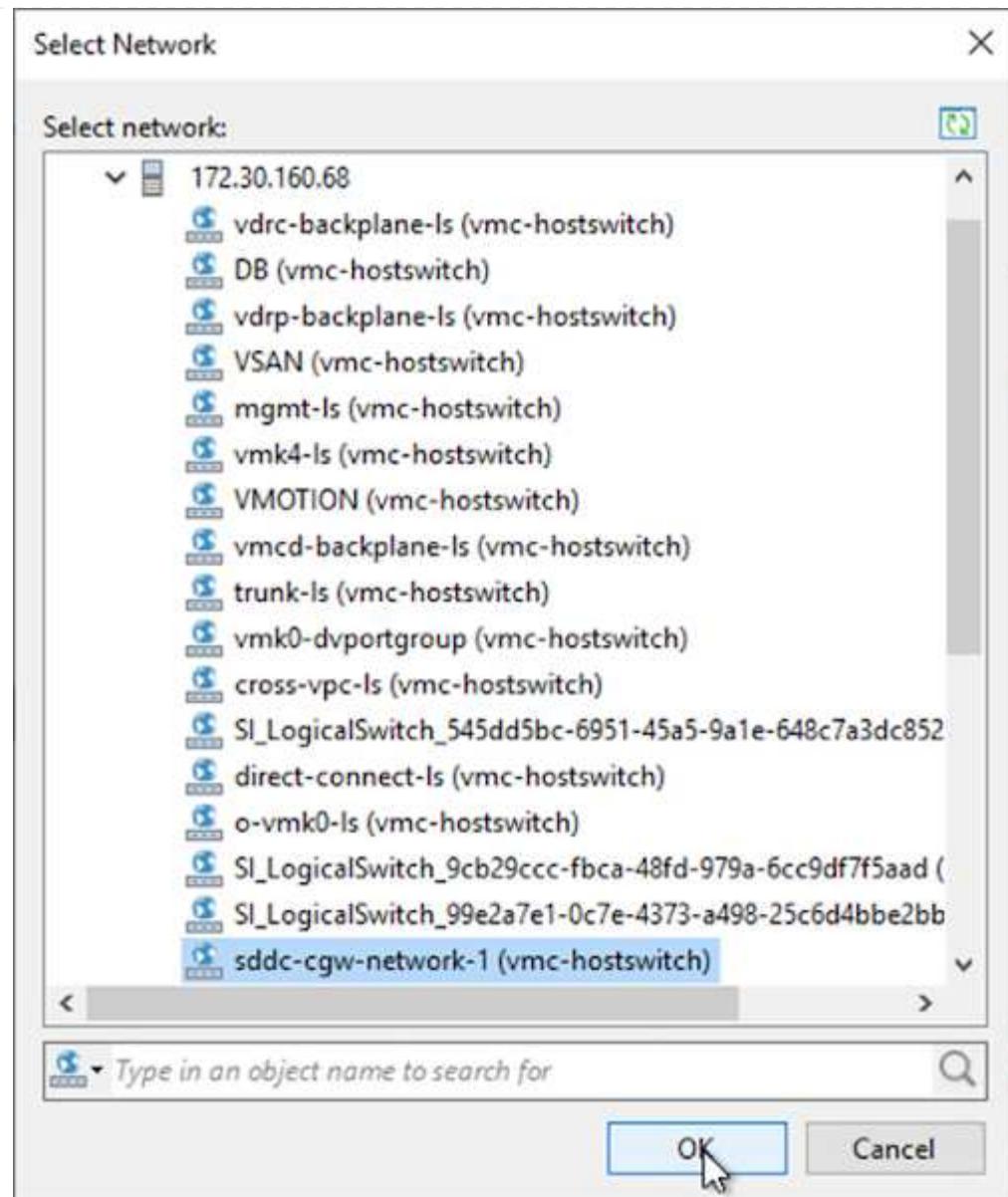
Disconnect

< Previous

Next

Finish

Cancel



7. Selezionare se eseguire la scansione della VM ripristinata per rilevare eventuali malware, rivedere la pagina di riepilogo e fare clic su Fine per avviare il ripristino.

Ripristinare i dati dell'applicazione SQL Server

La seguente procedura fornisce istruzioni su come ripristinare un SQL Server in VMware Cloud Services in AWS in caso di un disastro che renda inutilizzabile il sito locale.

Per poter proseguire con le fasi di ripristino si presuppone che siano soddisfatti i seguenti prerequisiti:

1. La VM Windows Server è stata ripristinata su VMware Cloud SDDC tramite Veeam Full Restore.
2. È stato stabilito un server SnapCenter secondario e il ripristino e la configurazione del database SnapCenter sono stati completati utilizzando i passaggi descritti nella sezione "["Riepilogo del processo di backup e ripristino SnapCenter ."](#)

VM: configurazione post-ripristino per VM SQL Server

Una volta completato il ripristino della VM, è necessario configurare la rete e altri elementi in preparazione per il nuovo rilevamento della VM host in SnapCenter.

1. Assegnare nuovi indirizzi IP per la gestione e iSCSI o NFS.
2. Aggiungere l'host al dominio Windows.
3. Aggiungere i nomi host al DNS o al file hosts sul server SnapCenter .



Se il plug-in SnapCenter è stato distribuito utilizzando credenziali di dominio diverse da quelle del dominio corrente, è necessario modificare l'account di accesso per il plug-in per il servizio Windows sulla macchina virtuale di SQL Server. Dopo aver modificato l'account di accesso, riavviare i servizi SnapCenter SMCore, Plug-in per Windows e Plug-in per SQL Server.



Per riscoprire automaticamente le VM ripristinate in SnapCenter, il nome di dominio completo (FQDN) deve essere identico alla VM originariamente aggiunta a SnapCenter in locale.

Configurare l'archiviazione FSx per il ripristino di SQL Server

Per completare il processo di ripristino di emergenza per una macchina virtuale di SQL Server, è necessario interrompere la relazione SnapMirror esistente dal cluster FSx e concedere l'accesso al volume. Per farlo, completa i seguenti passaggi.

1. Per interrompere la relazione SnapMirror esistente per il database di SQL Server e i volumi di registro, eseguire il seguente comando dalla CLI di FSx:

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Concedi l'accesso al LUN creando un gruppo di iniziatori contenente l'IQN iSCSI della VM Windows di SQL Server:

```
FSx-Dest::> igrup create -vserver DestSVM -igroup igrupGroupName  
-protocol iSCSI -ostype windows -initiator IQN
```

3. Infine, mappa i LUN al gruppo di iniziatori appena creato:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igrup  
igroupName
```

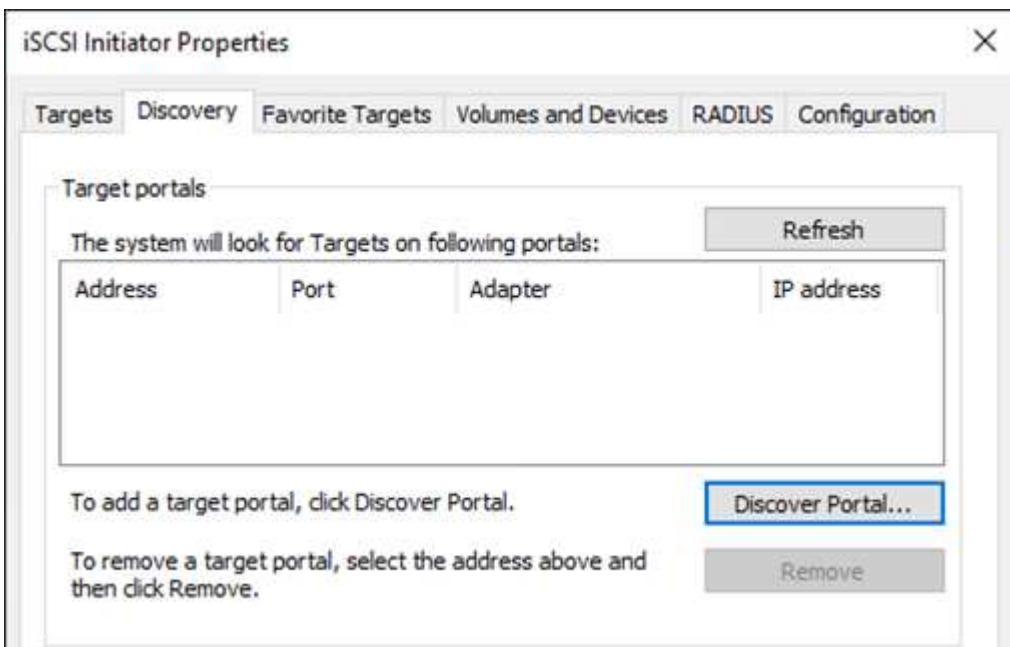
4. Per trovare il nome del percorso, eseguire il comando `lun show` comando.

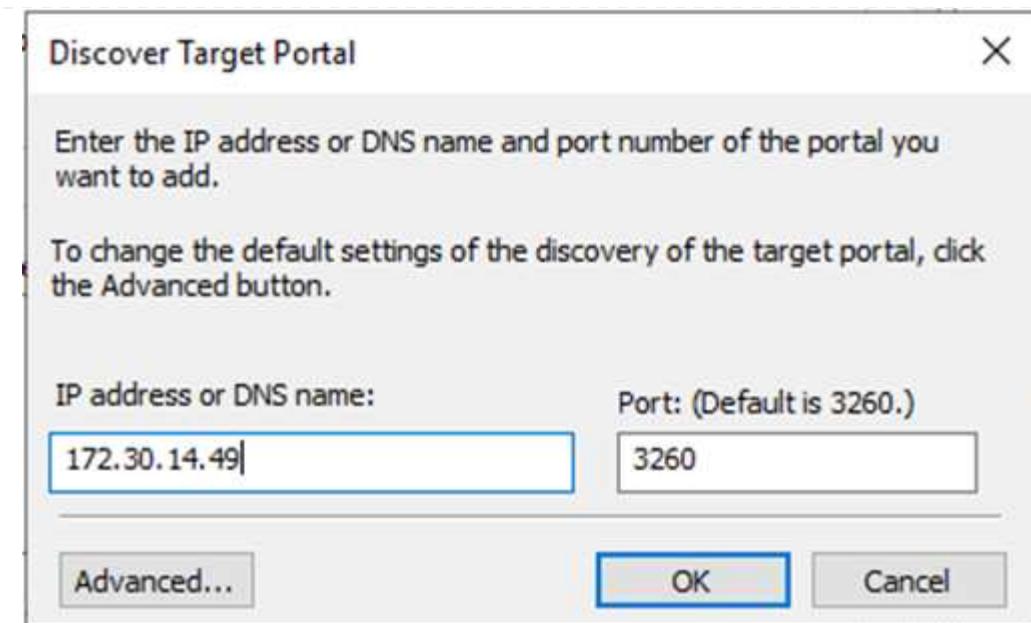
Configurare la VM Windows per l'accesso iSCSI e scoprire i file system

1. Dalla VM di SQL Server, configura la scheda di rete iSCSI per comunicare sul gruppo di porte VMware stabilito con connettività alle interfacce di destinazione iSCSI sulla tua istanza FSx.
2. Aprire l'utilità Proprietà dell'iniziatore iSCSI e cancellare le vecchie impostazioni di connettività nelle schede Rilevamento, Destinazioni preferite e Destinazioni.
3. Individuare l'indirizzo/gli indirizzi IP per accedere all'interfaccia logica iSCSI sull'istanza/cluster FSx. Questa opzione è disponibile nella console AWS in Amazon FSx > ONTAP > Storage Virtual Machines.

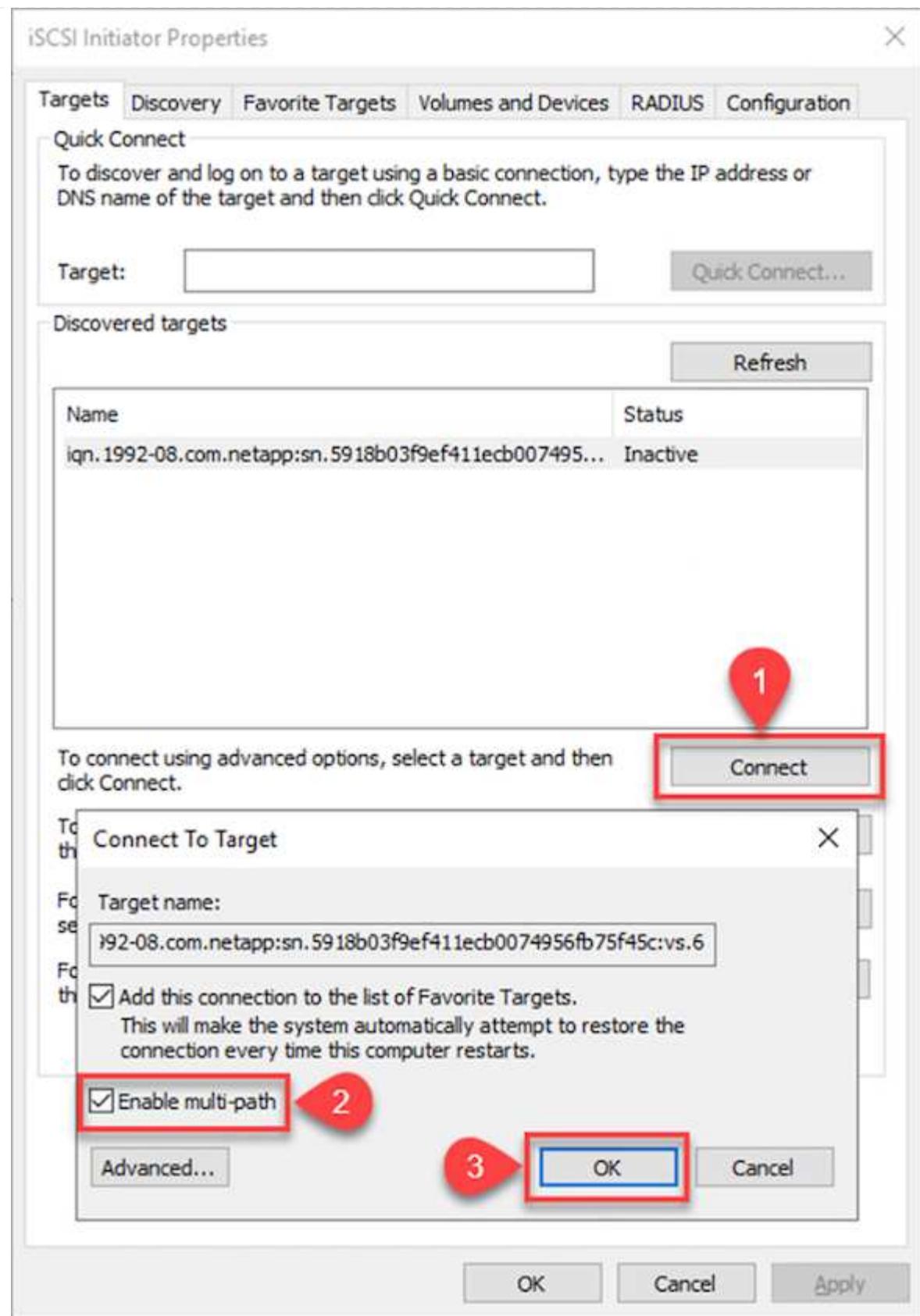
Management DNS name	Management IP address
svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	198.19.254.53
NFS DNS name	NFS IP address
svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	198.19.254.53
iSCSI DNS name	iSCSI IP addresses
iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	172.30.15.101, 172.30.14.49

4. Dalla scheda Discovery, fare clic su Discover Portal e immettere gli indirizzi IP per le destinazioni iSCSI FSx.

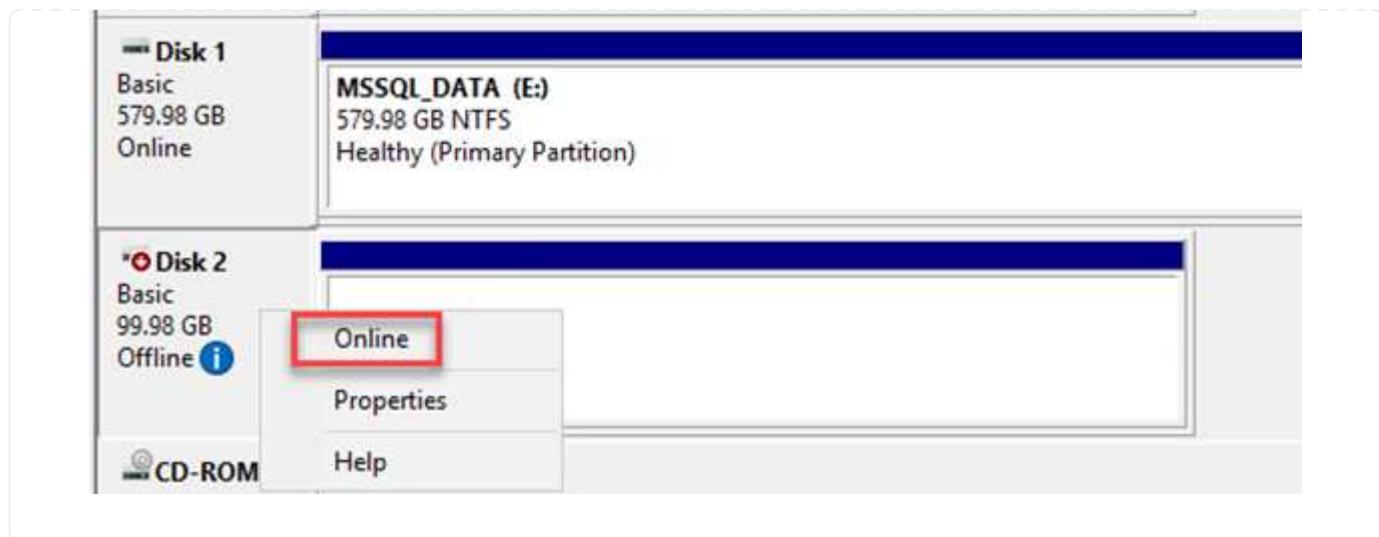




5. Nella scheda Destinazione, fare clic su Connetti, selezionare Abilita multipercorso se appropriato per la configurazione, quindi fare clic su OK per connettersi alla destinazione.

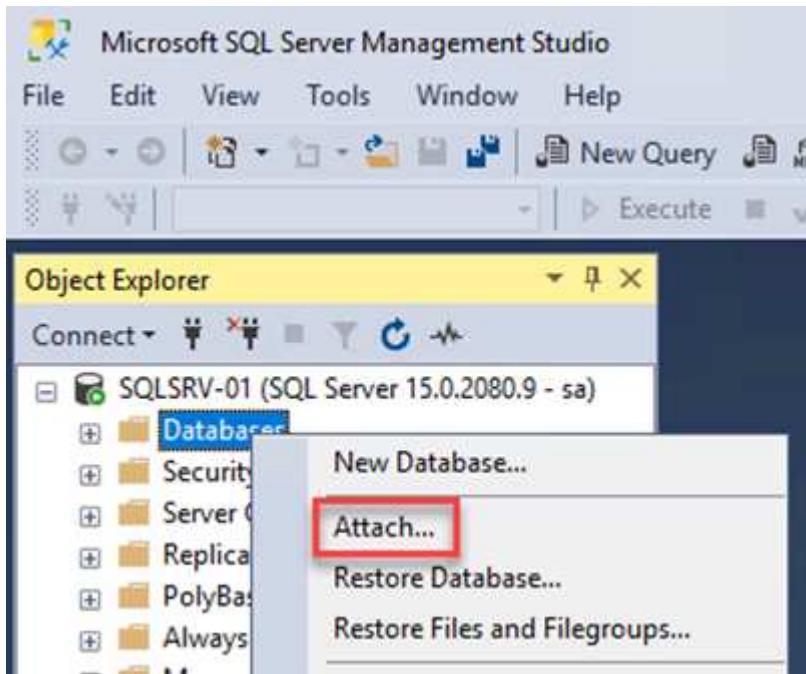


6. Aprire l'utilità Gestione computer e portare i dischi online. Verificare che mantengano le stesse lettere di unità assegnate in precedenza.

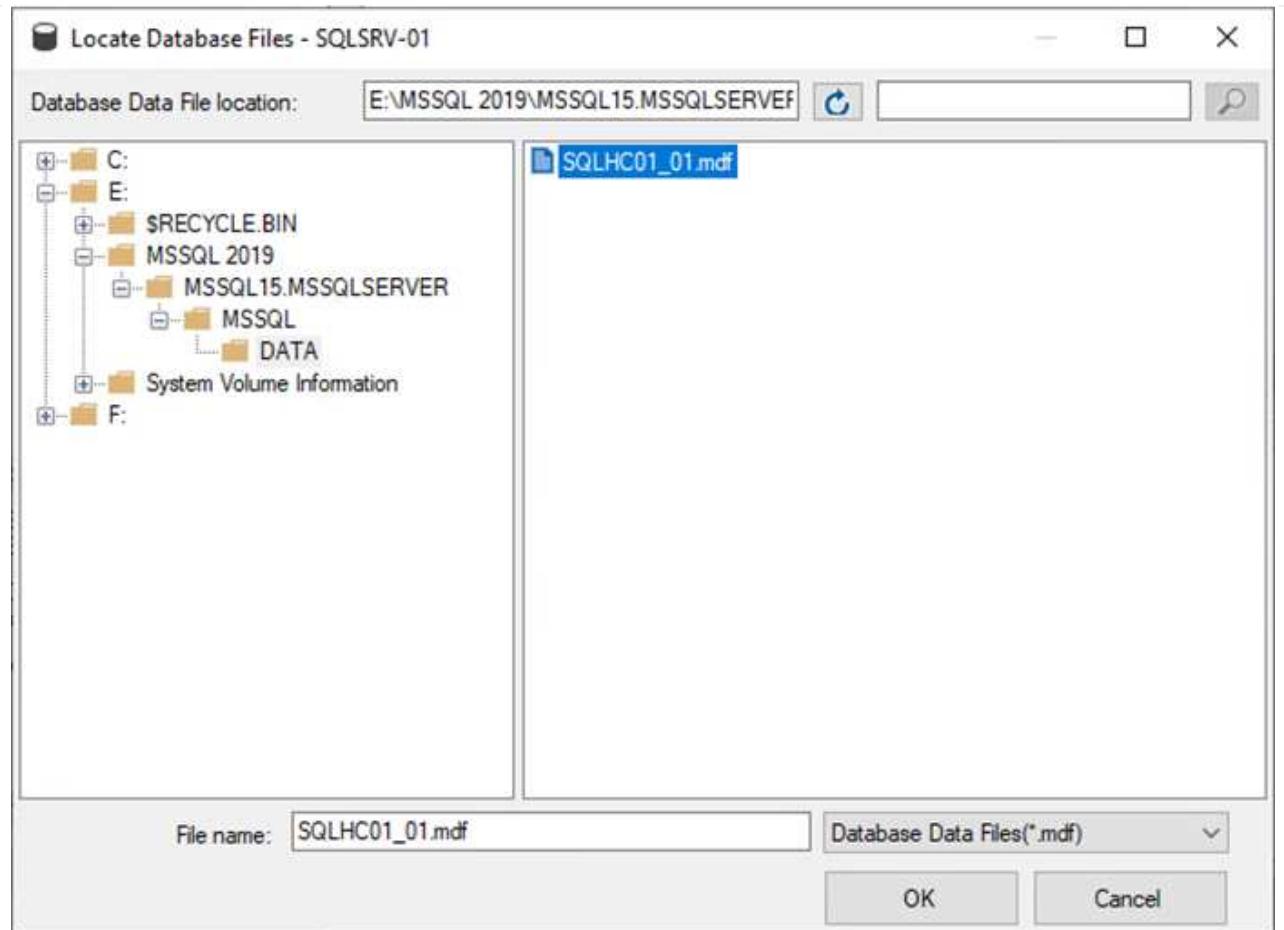


Collegare i database di SQL Server

1. Dalla VM di SQL Server, aprire Microsoft SQL Server Management Studio e selezionare Collega per avviare il processo di connessione al database.



2. Fare clic su Aggiungi e andare alla cartella contenente il file del database primario di SQL Server, selezionarlo e fare clic su OK.



3. Se i registri delle transazioni si trovano su un'unità separata, selezionare la cartella che contiene il registro delle transazioni.
4. Al termine, fare clic su OK per allegare il database.

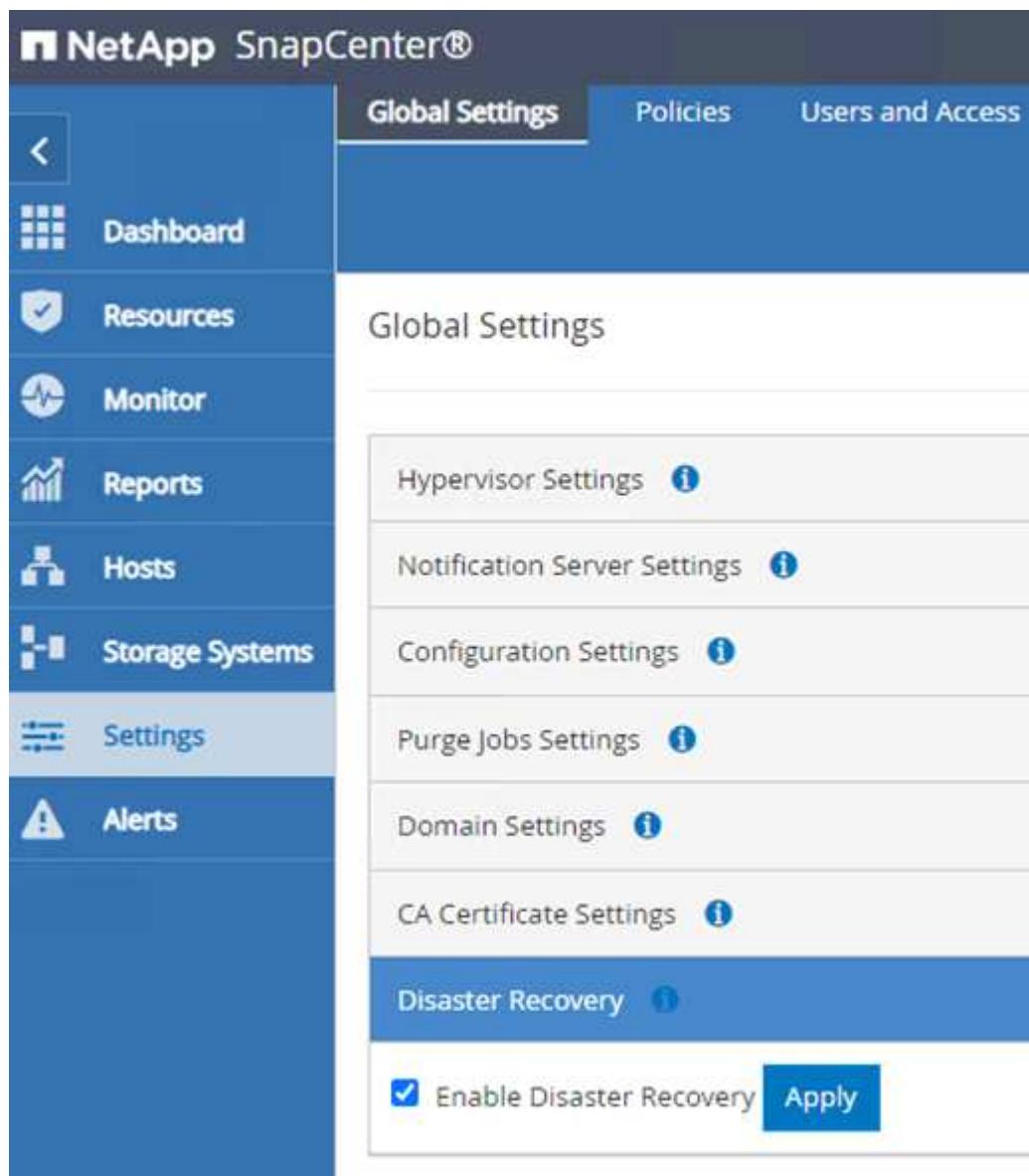
Page	Value
Name	SQLHC01
Status	Normal
Owner	sa
Date Created	4/13/2022 9:37:18 PM
Size	51494.00 MB
Space Available	501701.86 MB
Number of Users	4
Memory Allocated To Memory Optimized Obj	0.00 MB
Memory Used By Memory Optimized Objects	0.00 MB
Collation	SQL_Latin1_General_CI_AS

Conferma la comunicazione SnapCenter con il plug-in di SQL Server

Una volta ripristinato lo stato precedente del database SnapCenter , gli host di SQL Server vengono automaticamente rilevati. Per far funzionare tutto correttamente, tieni presente i seguenti prerequisiti:

- SnapCenter deve essere impostato in modalità Disaster Recover. Questa operazione può essere eseguita tramite l'API Swagger o nelle Impostazioni globali in Disaster Recovery.
- Il nome di dominio completo (FQDN) di SQL Server deve essere identico all'istanza in esecuzione nel data center locale.
- La relazione SnapMirror originale deve essere interrotta.
- I LUN contenenti il database devono essere montati sull'istanza di SQL Server e il database deve essere collegato.

Per confermare che SnapCenter è in modalità Disaster Recovery, accedere a Impostazioni dal client Web SnapCenter . Vai alla scheda Impostazioni globali e poi fai clic su Ripristino di emergenza. Assicurarsi che la casella di controllo Abilita ripristino di emergenza sia abilitata.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar has icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The 'Settings' item is currently selected. The main content area has tabs for Global Settings, Policies, and Users and Access, with 'Global Settings' selected. The 'Global Settings' page lists several sections: Hypervisor Settings, Notification Server Settings, Configuration Settings, Purge Jobs Settings, Domain Settings, and CA Certificate Settings. The 'Disaster Recovery' section is highlighted with a blue background. At the bottom of this section is a checkbox labeled 'Enable Disaster Recovery' which is checked, and a blue 'Apply' button.

Ripristinare i dati dell'applicazione Oracle

La seguente procedura fornisce istruzioni su come ripristinare i dati delle applicazioni Oracle in VMware Cloud Services in AWS in caso di un disastro che renda inutilizzabile il sito locale.

Per proseguire con i passaggi di ripristino, è necessario soddisfare i seguenti prerequisiti:

1. La VM del server Oracle Linux è stata ripristinata su VMware Cloud SDDC utilizzando Veeam Full Restore.
2. È stato stabilito un server SnapCenter secondario e il database SnapCenter e i file di configurazione sono stati ripristinati utilizzando i passaggi descritti in questa sezione "[Riepilogo del processo di backup e ripristino SnapCenter](#) ."

Configurare FSx per il ripristino di Oracle: interrompere la relazione SnapMirror

Per rendere accessibili ai server Oracle i volumi di archiviazione secondari ospitati sull'istanza FSx ONTAP, è necessario prima interrompere la relazione SnapMirror esistente.

1. Dopo aver effettuato l'accesso alla CLI di FSx, eseguire il comando seguente per visualizzare i volumi filtrati in base al nome corretto.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver      Volume      Aggregate      State      Type      Size  Available Used%
-----      -----      -----      -----      -----      -----  -----  -----
ora_svm_dest
    oraclesrv_03_u01_dest
        aggr1      online      DP      100GB    93.12GB    6%
ora_svm_dest
    oraclesrv_03_u02_dest
        aggr1      online      DP      200GB    34.98GB    82%
ora_svm_dest
    oraclesrv_03_u03_dest
        aggr1      online      DP      150GB    33.37GB    77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::> █
```

2. Eseguire il comando seguente per interrompere le relazioni SnapMirror esistenti.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Aggiorna il percorso di giunzione nel client Web Amazon FSx :

oraclesrv_03_u01_dest (fsvol-01167370e9b7aef0)

Actions ▾

- Attach
- Update volume**
- Create backup
- Delete volume

Summary

Volume ID	Creation time	SVM ID
fsvol-01167370e9b7aef0 	2022-03-08T14:52:09-05:00	svm-02b2ad25c6b2e5bc2
Volume name	Lifecycle state	Junction path
oraclesrv_03_u01_dest 	 Created	- 
UUID	Volume type	Tiering policy name
3d7338ce-9f19-11ec-b007-4956fb75f45c	ONTAP	SNAPSHOT_ONLY
File system ID	Size	Tiering policy cooling period (days)
fs-0ae40e08acc0dea67 	100.00 GB 	2
Resource ARN		Storage efficiency enabled
arn:aws:fsx:us-east-1:541696183547:volume/fs-0ae40e08acc0dea67/fsvol-01167370e9b7aef0 		Disabled

4. Aggiungere il nome del percorso di giunzione e fare clic su Aggiorna. Specificare questo percorso di giunzione quando si monta il volume NFS dal server Oracle.

Update volume

X

Junction path

/oraclesrv_03_u01_dest

The location within your file system where your volume will be mounted.

Volume size

102400



Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
 Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Snapshot Only



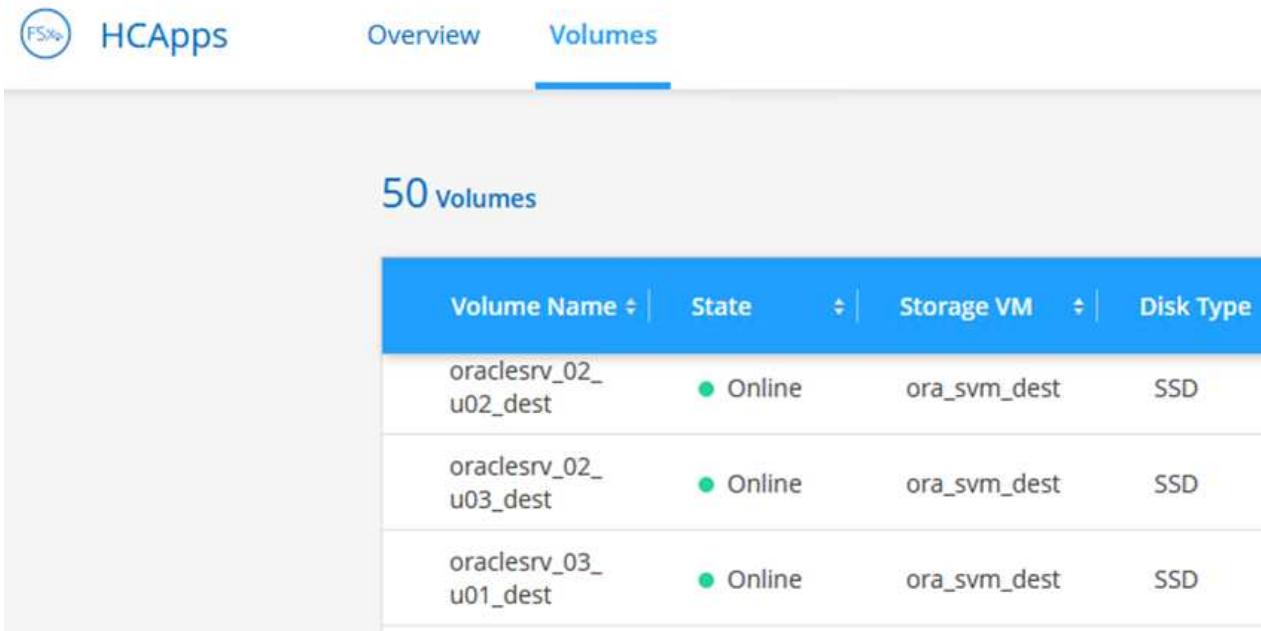
Cancel

Update

Montare volumi NFS su Oracle Server

In Cloud Manager, è possibile ottenere il comando mount con l'indirizzo IP LIF NFS corretto per montare i volumi NFS che contengono i file e i log del database Oracle.

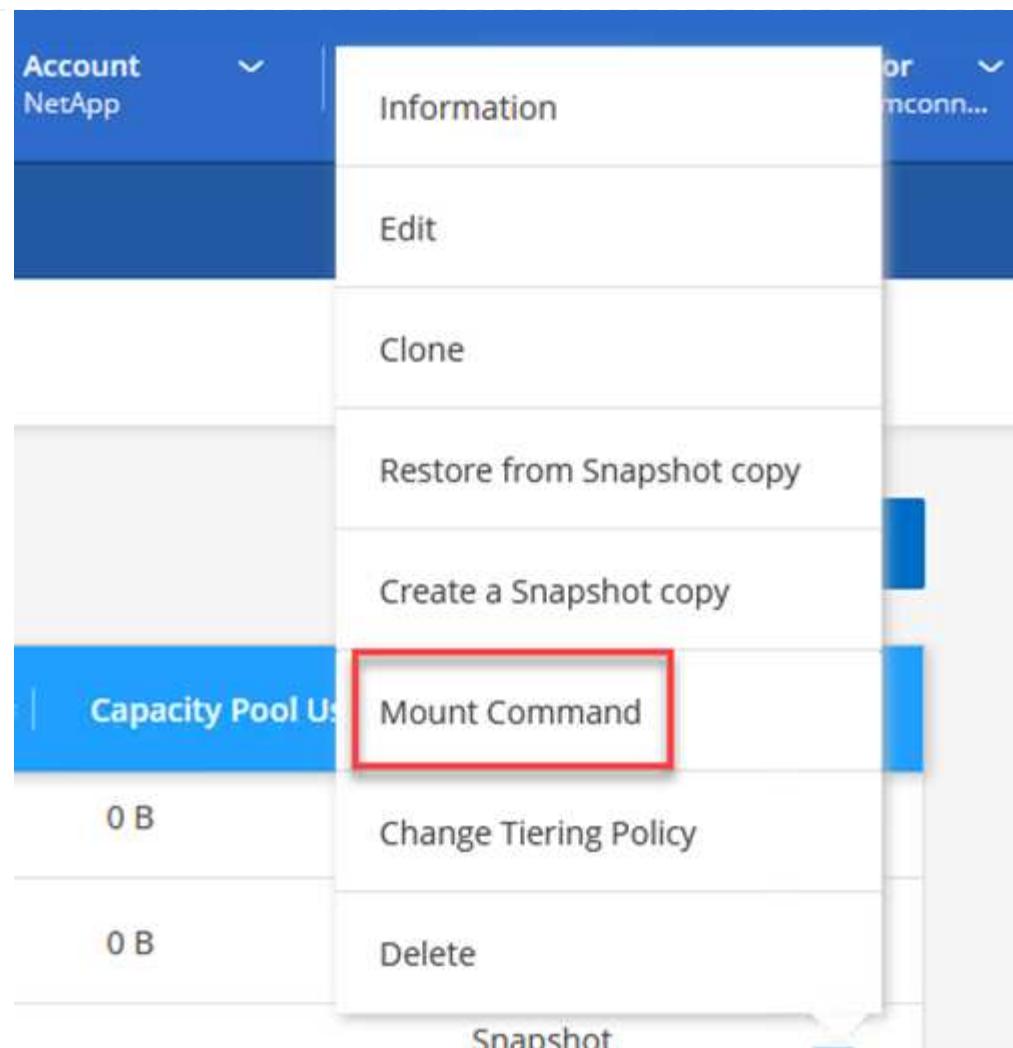
1. In Cloud Manager, accedi all'elenco dei volumi per il tuo cluster FSx.



The screenshot shows the Oracle Cloud Manager interface for FSx. The top navigation bar includes 'FSx', 'HCApps', 'Overview', and 'Volumes'. The 'Volumes' tab is selected, indicated by a blue underline. Below the navigation, a message '50 Volumes' is displayed. A table lists the volumes with the following columns: Volume Name, State, Storage VM, and Disk Type. The table contains three rows of data:

Volume Name	State	Storage VM	Disk Type
oraclesrv_02_u02_dest	Online	ora_svm_dest	SSD
oraclesrv_02_u03_dest	Online	ora_svm_dest	SSD
oraclesrv_03_u01_dest	Online	ora_svm_dest	SSD

2. Dal menu Azione, seleziona Comando di montaggio per visualizzare e copiare il comando di montaggio da utilizzare sul nostro server Oracle Linux.



Mount Volume NFS

oraclesrv_03_u01_dest

Go to your linux machine and enter this mount command

Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_d...
```

 Copy

3. Montare il file system NFS su Oracle Linux Server. Le directory per il montaggio della condivisione NFS esistono già sull'host Oracle Linux.
4. Dal server Oracle Linux, utilizzare il comando mount per montare i volumi NFS.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Ripetere questo passaggio per ogni volume associato ai database Oracle.



Per rendere persistente il montaggio NFS al riavvio, modificare `/etc/fstab` file per includere i comandi di montaggio.

5. Riavviare il server Oracle. I database Oracle dovrebbero avviarsi normalmente ed essere disponibili per l'uso.

Rifasamento

Una volta completato con successo il processo di failover descritto in questa soluzione, SnapCenter e Veeam riprendono le loro funzioni di backup in esecuzione su AWS e FSx ONTAP viene ora designato come storage primario senza alcuna relazione SnapMirror esistente con il data center locale originale. Dopo aver ripreso il normale funzionamento in sede, è possibile utilizzare un processo identico a quello descritto in questa documentazione per eseguire il mirroring dei dati sul sistema di archiviazione ONTAP in sede.

Come descritto anche in questa documentazione, è possibile configurare SnapCenter per eseguire il mirroring dei volumi di dati dell'applicazione da FSx ONTAP a un sistema di archiviazione ONTAP residente in locale. Allo stesso modo, è possibile configurare Veeam per replicare le copie di backup su Amazon S3 utilizzando un repository di backup scalabile, in modo che tali backup siano accessibili a un server di backup Veeam residente nel data center locale.

Il fallback esula dall'ambito di questa documentazione, ma differisce poco dal processo dettagliato qui descritto.

Conclusione

Il caso d'uso presentato in questa documentazione si concentra su tecnologie di disaster recovery comprovate che evidenziano l'integrazione tra NetApp e VMware. I sistemi di storage NetApp ONTAP forniscono tecnologie di data-mirroring comprovate che consentono alle organizzazioni di progettare soluzioni di disaster recovery che abbracciano tecnologie locali e ONTAP residenti presso i principali provider cloud.

FSx ONTAP su AWS è una di queste soluzioni che consente un'integrazione perfetta con SnapCenter e SyncMirror per replicare i dati delle applicazioni sul cloud. Veeam Backup & Replication è un'altra tecnologia ben nota che si integra bene con i sistemi di storage NetApp ONTAP e può fornire il failover allo storage nativo di vSphere.

Questa soluzione presentava una soluzione di disaster recovery che utilizzava l'archiviazione guest connect da un sistema ONTAP che ospitava dati di applicazioni SQL Server e Oracle. SnapCenter con SnapMirror fornisce una soluzione facile da gestire per proteggere i volumi delle applicazioni sui sistemi ONTAP e replicarli su FSx o CVO residenti nel cloud. SnapCenter è una soluzione abilitata al DR per il failover di tutti i dati delle applicazioni su VMware Cloud su AWS.

Informazioni sul copyright

Copyright © 2026 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 COMMERCIALITÀ 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.