NetApp per AWS/VMC

NetApp Solutions

NetApp
September 26, 2024

Sommario

NetApp per AWS/VMC

Funzionalità NetApp per AWS VMC

Scopri di più sulle funzionalità offerte da NetApp in AWS VMware Cloud (VMC), da NetApp come dispositivo di storage connesso come guest o come datastore NFS supplementare alla migrazione dei flussi di lavoro, all'estensione/diffusione nel cloud, al backup/ripristino e al disaster recovery.

Passare alla sezione relativa al contenuto desiderato selezionando una delle seguenti opzioni:

- "Configurazione di VMC in AWS"
- "Opzioni di storage NetApp per VMC"
- "Soluzioni cloud NetApp/VMware"

Configurazione di VMC in AWS

Come per i sistemi on-premise, la pianificazione di un ambiente di virtualizzazione basato sul cloud è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementazione e configurazione di VMware Cloud per AWS
- Connetti VMware Cloud a FSX ONTAP

Visualizza i dettagli "Procedura di configurazione per VMC".

Opzioni di storage NetApp per VMC

Lo storage NetApp può essere utilizzato in diversi modi, sia come congettura connessa che come datastore NFS supplementare, all'interno di AWS VMC.

Visitare il sito "Opzioni di storage NetApp supportate" per ulteriori informazioni.

AWS supporta lo storage NetApp nelle seguenti configurazioni:

- FSX ONTAP come storage connesso guest
- Cloud Volumes ONTAP (CVO) come storage connesso guest
- FSX ONTAP come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per VMC". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per VMC".

Casi di utilizzo della soluzione

Con le soluzioni cloud NetApp e VMware, molti casi di utilizzo sono semplici da implementare nel tuo AWS VMC. I casi di utilizzo sono definiti per ciascuna delle aree cloud definite da VMware:

- Protect (include disaster recovery e backup/ripristino)
- Estendi
- Migrare

"Esplora le soluzioni NetApp per AWS VMC"

Protezione dei carichi di lavoro su AWS / VMC

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

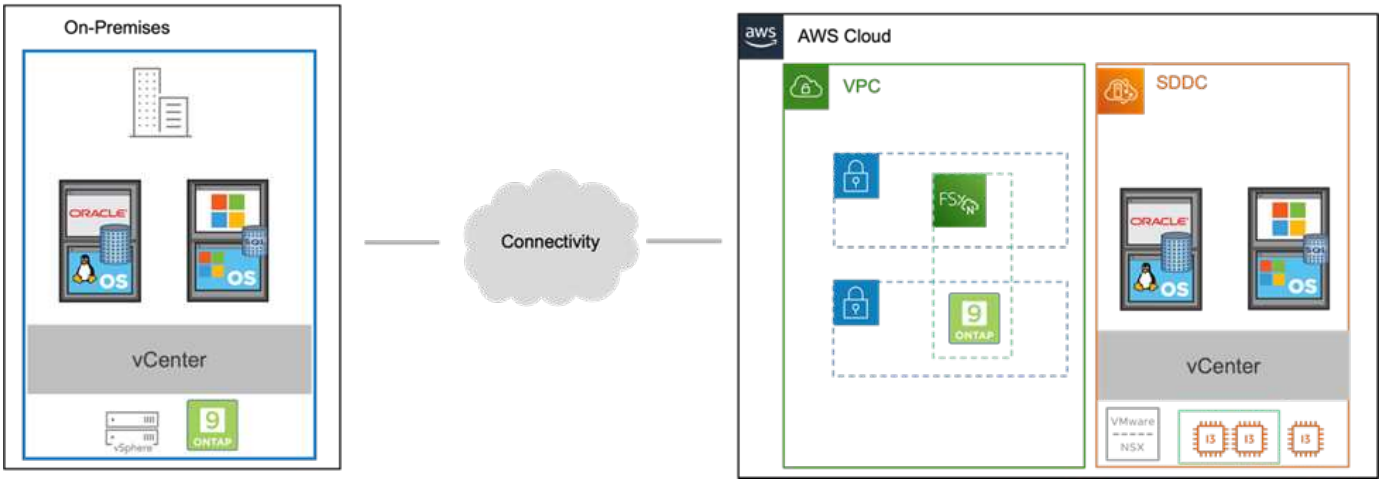
Un ambiente e un piano di disaster recovery (DR) comprovati sono fondamentali per le organizzazioni per garantire che le applicazioni business-critical possano essere ripristinate rapidamente in caso di grave interruzione del servizio. Questa soluzione si concentra sulla dimostrazione dei casi di utilizzo del DR con particolare attenzione alle tecnologie VMware e NetApp, sia on-premise che con VMware Cloud su AWS.

Autori: Chris Reno, Josh Powell e Suresh Thoppay - NetApp Solutions Engineering

Panoramica

NetApp vanta una lunga storia 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 con le opzioni di connessione guest nel cloud e le recenti integrazioni con i datastore NFS. Questa soluzione si concentra sul caso di utilizzo comunemente indicato come storage connesso al guest.

Nello storage connesso agli ospiti, il VMDK guest viene implementato su un datastore con provisioning VMware e i dati delle applicazioni vengono memorizzati su iSCSI o NFS e mappati direttamente sulla macchina virtuale. Le applicazioni Oracle e MS SQL vengono utilizzate per dimostrare uno scenario di DR, come illustrato nella figura seguente.



Presupposti, prerequisiti e panoramica dei componenti

Prima di implementare questa soluzione, esaminare la panoramica dei componenti, i prerequisiti necessari per implementare la soluzione e i presupposti della documentazione della soluzione.

"Requisiti, requisiti e pianificazione della soluzione DR"

Eseguire il 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, offre una replica dei dati ad alta velocità tra il nostro cluster AFF on-premise e FSX ONTAP. Inoltre, Veeam Backup & Replication offre funzionalità di backup e ripristino per le nostre macchine virtuali.

In questa sezione viene descritta la configurazione di SnapCenter, SnapMirror e Veeam per il backup e il ripristino.

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

Configurare le relazioni di SnapMirror e le pianificazioni di conservazione

SnapCenter può aggiornare le relazioni di SnapMirror all'interno del sistema di storage primario (primario > mirror) e ai sistemi di storage secondario (primario > vault) per l'archiviazione e la conservazione a lungo termine. A tale scopo, 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 con peering tramite VPC Amazon, gateway di transito, connessione diretta AWS o VPN AWS.

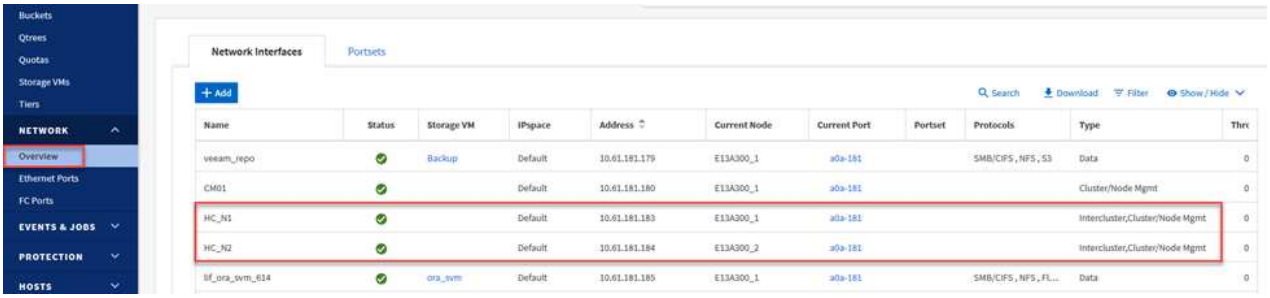
Per impostare le relazioni di SnapMirror tra un sistema ONTAP on-premise e FSX ONTAP sono necessari i seguenti passaggi:

Fare riferimento a. "FSX per ONTAP - Guida utente di ONTAP" Per ulteriori informazioni sulla creazione di relazioni SnapMirror con FSX.

Registrare le interfacce logiche Intercluster di origine e destinazione

Per il sistema ONTAP di origine residente on-premise, è possibile recuperare le informazioni LIF tra cluster da Gestore di sistema o dall'interfaccia CLI.

1. In Gestore di sistema di ONTAP, accedere alla pagina Panoramica di rete e recuperare gli indirizzi IP di tipo: Intercluster configurati per comunicare con il VPC di AWS su cui è installato FSX.



2. Per recuperare gli indirizzi IP dell'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
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

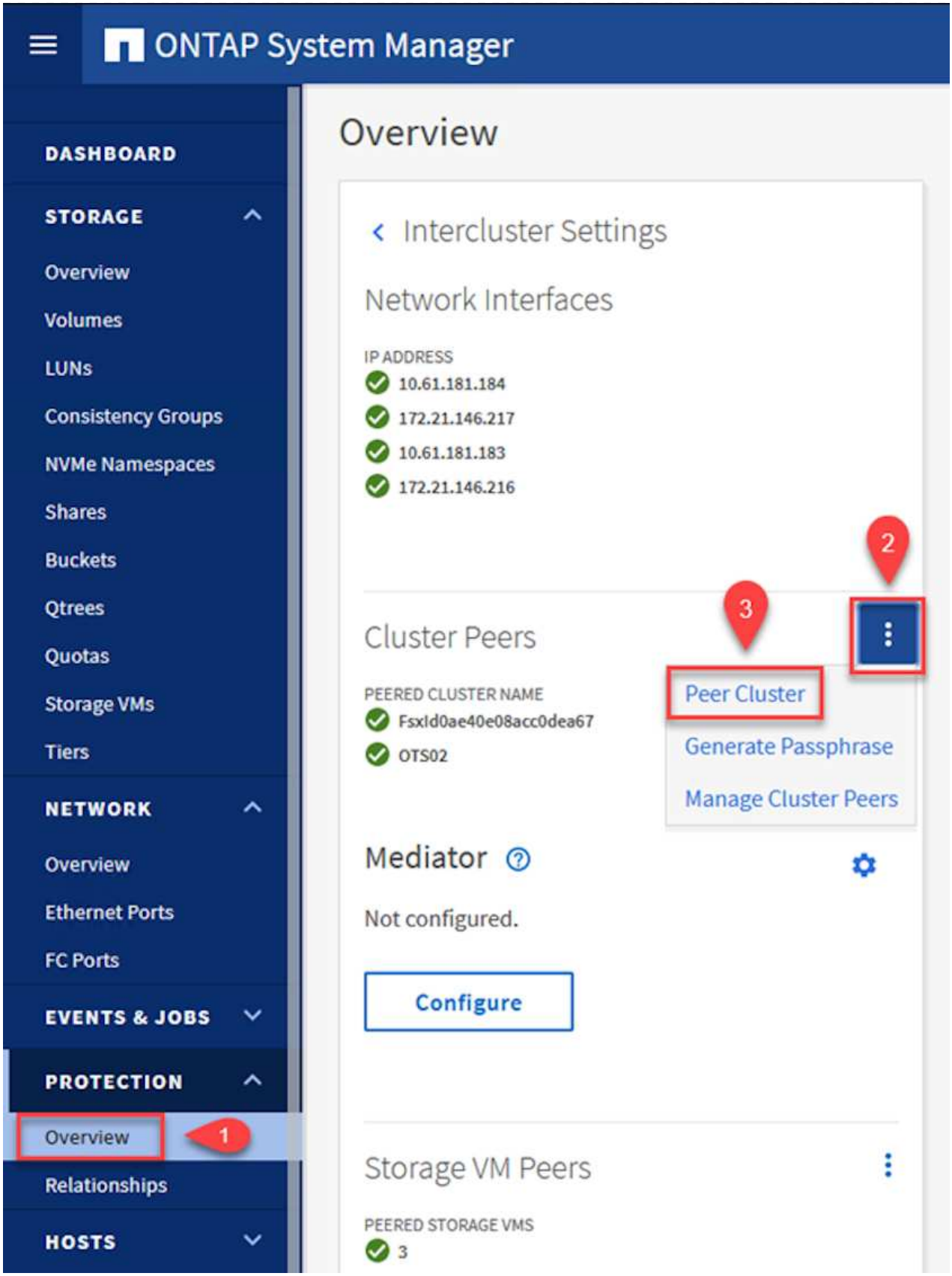
Stabilire il peering del cluster tra ONTAP e FSX

Per stabilire il peering del cluster tra i cluster ONTAP, è necessario confermare una passphrase univoca inserita nel cluster ONTAP di avvio nell'altro cluster peer.

1. Impostare il peering sul cluster FSX di destinazione utilizzando `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca da utilizzare in seguito nel cluster di origine per completare 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 Gestore di sistema di ONTAP o l'interfaccia CLI. Da Gestore di sistema di ONTAP, accedere a protezione > Panoramica e selezionare cluster peer.

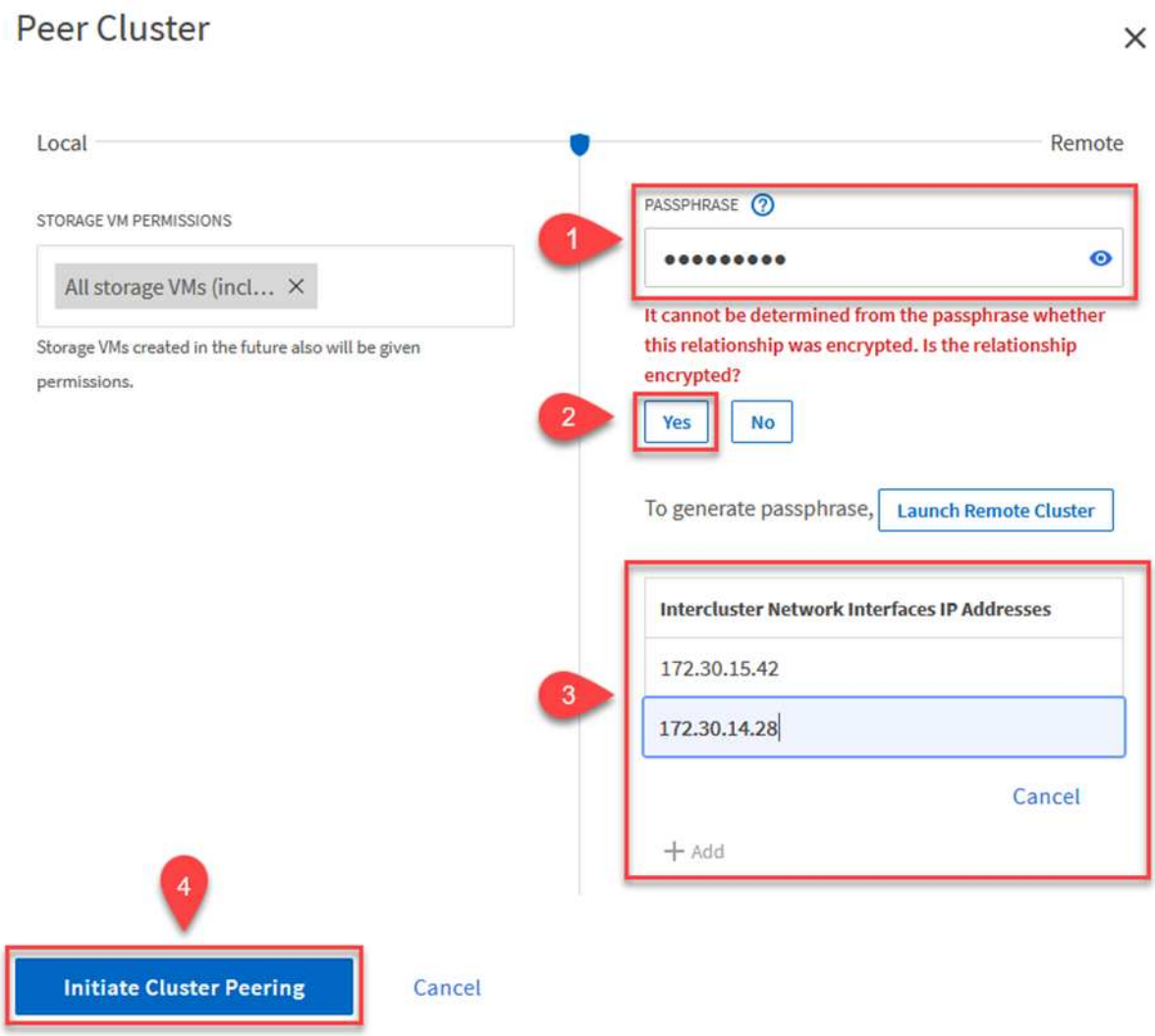


3. Nella finestra di dialogo Peer Cluster, inserire le informazioni richieste:
   a. Inserire la passphrase utilizzata per stabilire la relazione del cluster peer nel cluster FSX di destinazione.

b. Selezionare `Yes` per stabilire una relazione crittografata.

c. Inserire gli indirizzi IP LIF dell'intercluster del cluster FSX di destinazione.

d. Fare clic su Initiate Cluster peering (Avvia peering cluster) per completare 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
```

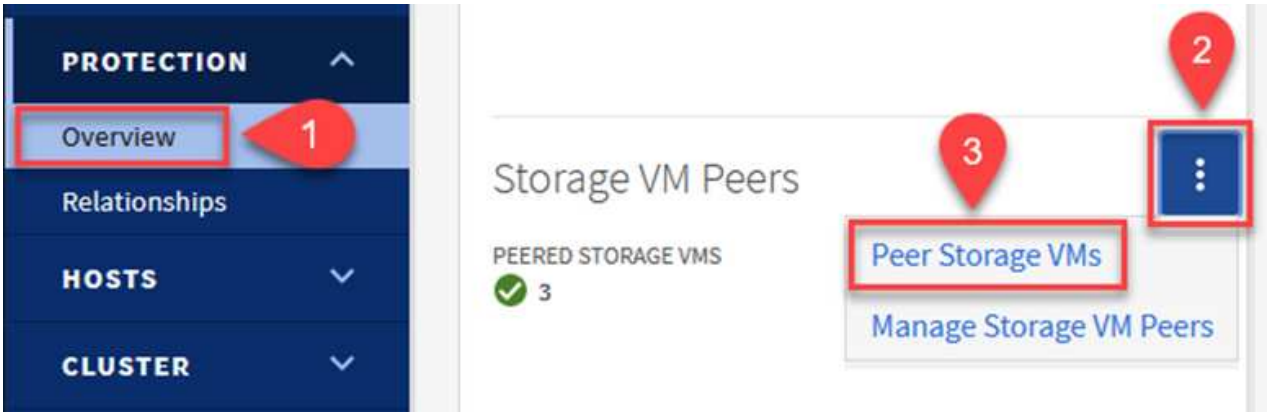
Stabilire una relazione di peering SVM

Il passaggio successivo consiste nell'impostare una relazione SVM tra le macchine virtuali dello storage di destinazione e di origine che contengono i volumi che si trovano nelle relazioni di 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 Gestore di sistema ONTAP o CLI.
3. Da Gestore di sistema ONTAP, andare a protezione > Panoramica e selezionare le VM di storage peer in peer di macchine virtuali di storage.



4. Nella finestra di dialogo Peer Storage VM, compilare i campi obbligatori:
   - La VM di storage di origine
   - Il cluster di destinazione
   - La VM di storage di destinazione

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

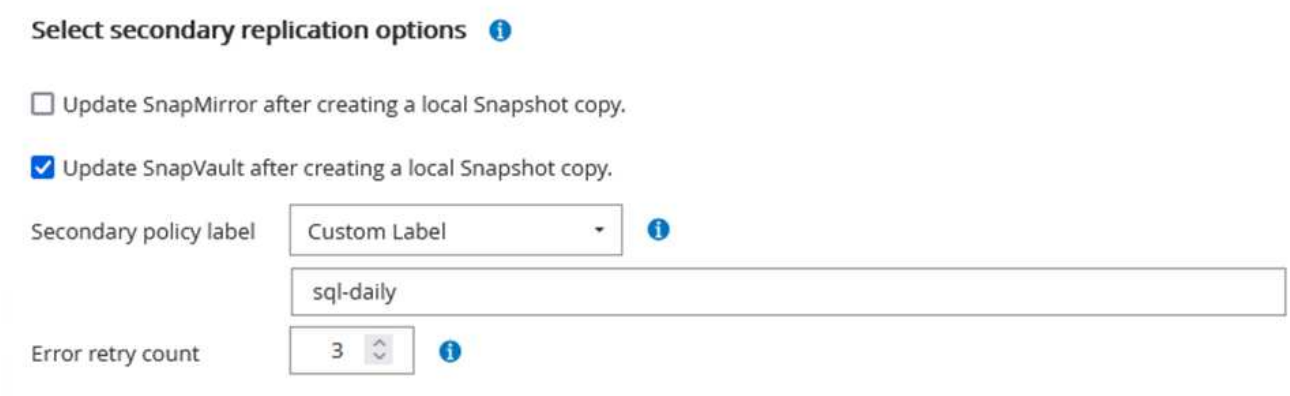
Creare un criterio di conservazione delle snapshot

SnapCenter gestisce le pianificazioni di conservazione per i backup che esistono come copie Snapshot sul sistema di storage primario. Questo viene stabilito quando si crea un criterio in SnapCenter. SnapCenter non gestisce le policy di conservazione per i backup conservati nei sistemi di storage secondari. Questi criteri vengono gestiti separatamente attraverso un criterio SnapMirror creato nel cluster FSX secondario e associato 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.

> Sullo storage secondario, queste etichette vengono associate alle regole dei criteri associate al volume di destinazione allo scopo di applicare la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutte le snapshot generate come parte di una policy utilizzata per i backup giornalieri del database SQL Server e dei volumi di log.



Per ulteriori informazioni sulla creazione di criteri SnapCenter per un database SQL Server, vedere "Documentazione SnapCenter".

È necessario innanzitutto creare un criterio SnapMirror con regole che determinano il numero di copie snapshot da conservare.

1. Creare il criterio SnapMirror sul cluster FSX.

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

2. Aggiungere regole al criterio con le etichette SnapMirror che corrispondono alle etichette dei criteri secondari specificate nei criteri SnapCenter.

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

Il seguente script fornisce un esempio di regola che è possibile aggiungere a un criterio:

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

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

Creare volumi di destinazione

Per creare un volume di destinazione su FSX che riceverà le copie Snapshot dai 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 di SnapMirror tra i volumi di origine e di destinazione

Per creare una relazione SnapMirror tra un volume di origine e un volume 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
```

Inizializzare le relazioni di SnapMirror

Inizializzare 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
```

Implementare e configurare Windows SnapCenter Server on-premise.

Implementazione del server Windows SnapCenter on-premise

Questa soluzione utilizza NetApp SnapCenter per eseguire backup coerenti con l'applicazione dei database SQL Server e Oracle. Insieme a Veeam Backup & Replication per il backup dei VMDK delle macchine virtuali, questo offre una soluzione completa di disaster recovery per data center on-premise e basati sul cloud.

Il software SnapCenter è disponibile sul sito di supporto NetApp e può essere installato su sistemi Microsoft Windows che risiedono in un dominio o in un gruppo di lavoro. Una guida dettagliata alla pianificazione e le istruzioni di installazione sono disponibili all'indirizzo "Centro di documentazione NetApp".

Il software SnapCenter è disponibile all'indirizzo "questo link".

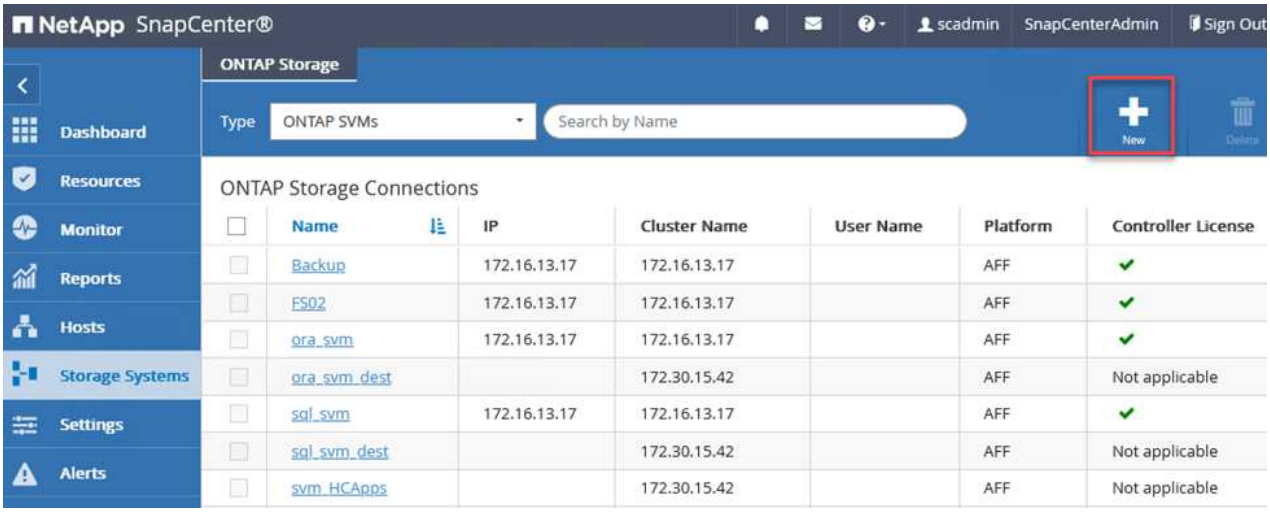
Una volta installata, è possibile accedere alla console SnapCenter da un browser Web utilizzando _ https://Virtual_Cluster_IP_or_FQDN:8146_.

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

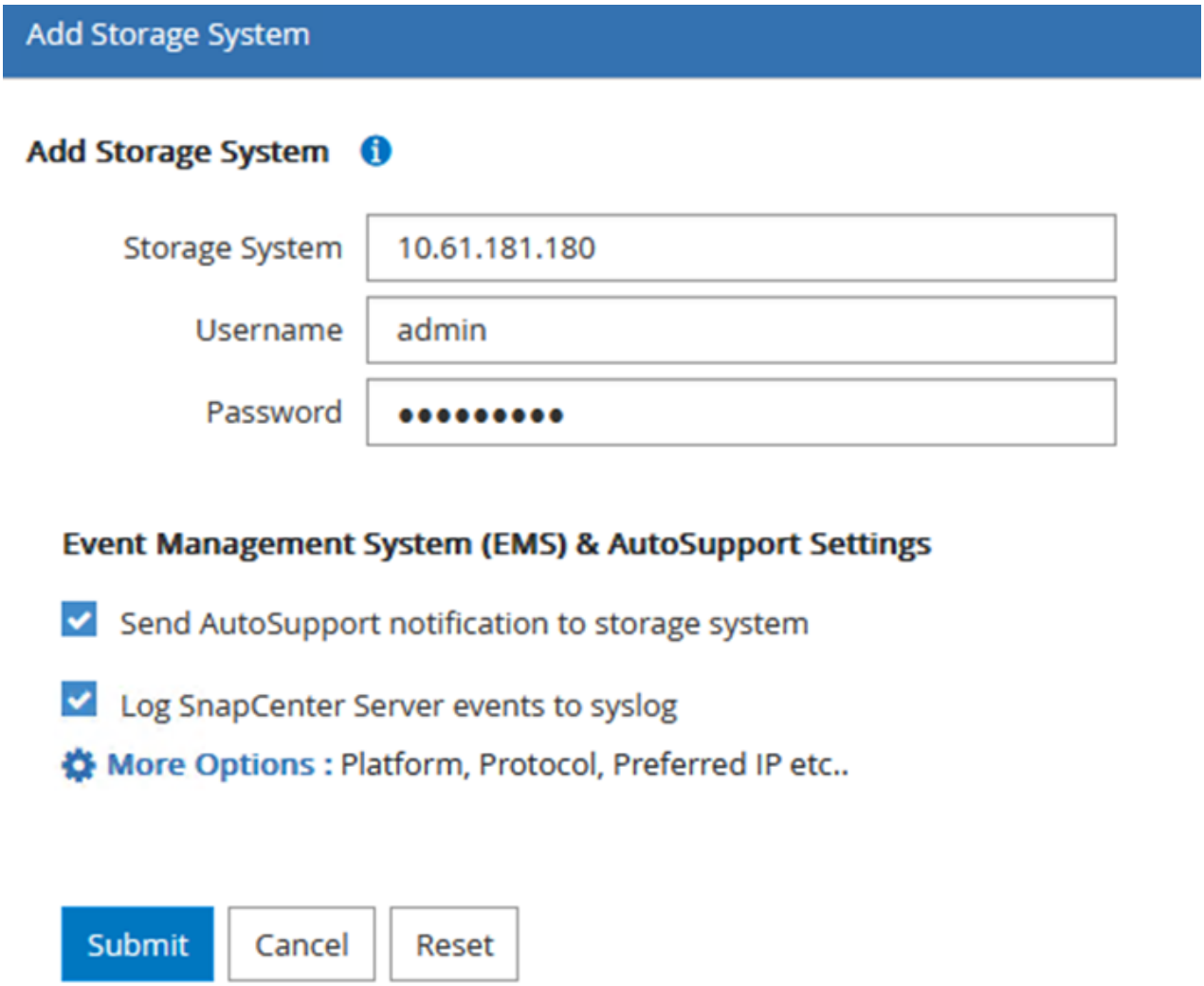
Aggiungere controller storage a SnapCenter

Per aggiungere controller di storage a SnapCenter, attenersi alla seguente procedura:

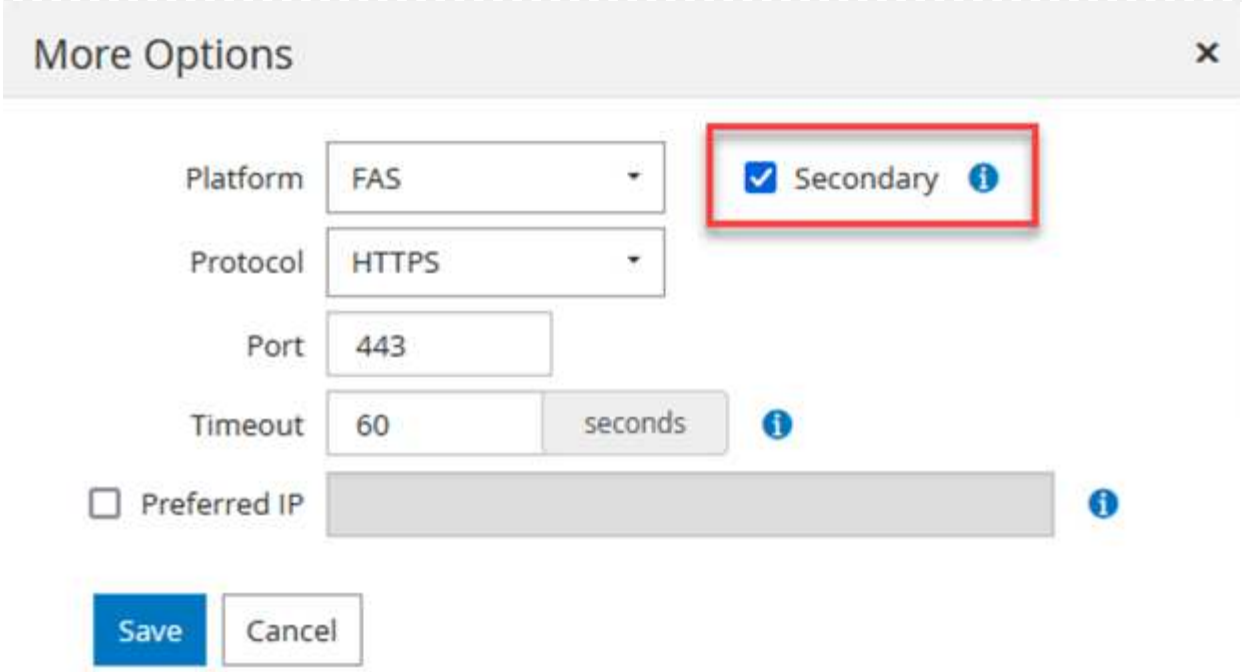
1. Dal menu a sinistra, selezionare sistemi storage, quindi fare clic su nuovo per avviare il processo di aggiunta dei controller storage a SnapCenter.



2. Nella finestra di dialogo Aggiungi sistema di storage, aggiungere l'indirizzo IP di gestione del cluster ONTAP locale on-premise e il nome utente e la password. Quindi fare clic su Submit (Invia) per avviare il rilevamento del sistema storage.



3. Ripetere questa procedura per aggiungere il sistema FSX ONTAP a SnapCenter. In questo caso, selezionare More Options (altre opzioni) nella parte inferiore della finestra Add Storage System (Aggiungi sistema di storage) e fare clic sulla casella di controllo Secondary (secondario) per designare il sistema FSX come sistema di storage secondario aggiornato con le copie SnapMirror o le snapshot di backup primarie.

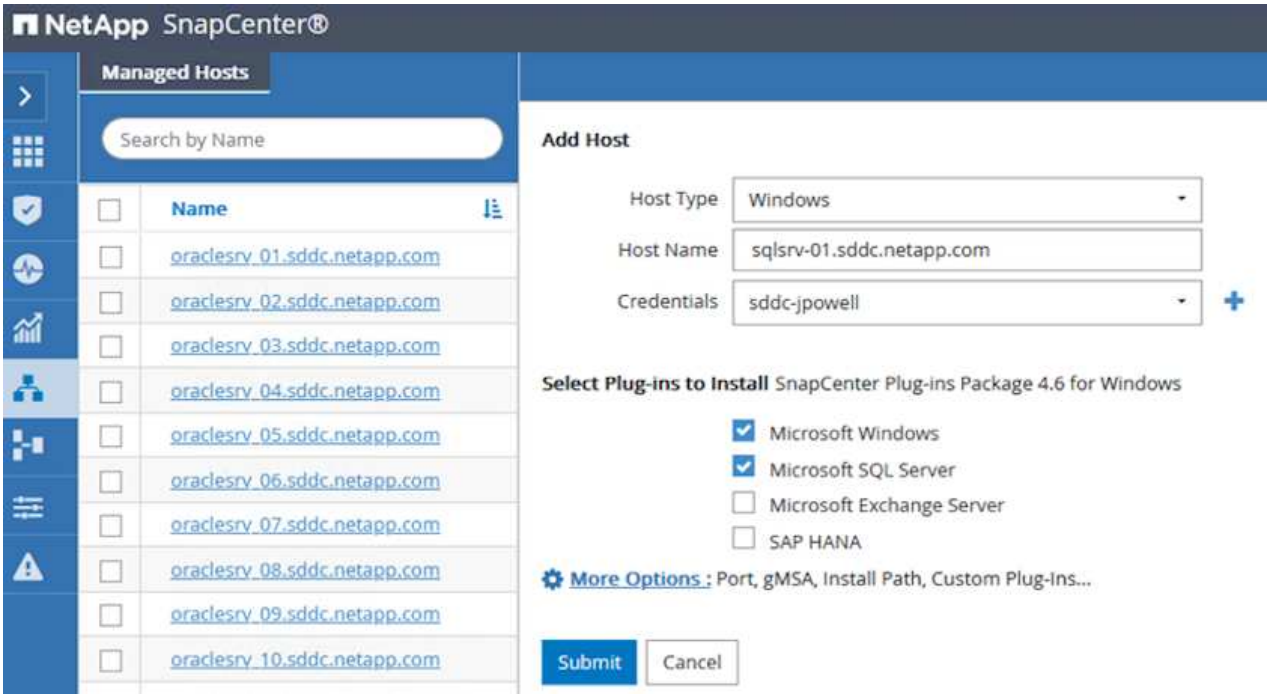


Per ulteriori informazioni sull'aggiunta di sistemi storage a SnapCenter, consultare la documentazione all'indirizzo "questo link".

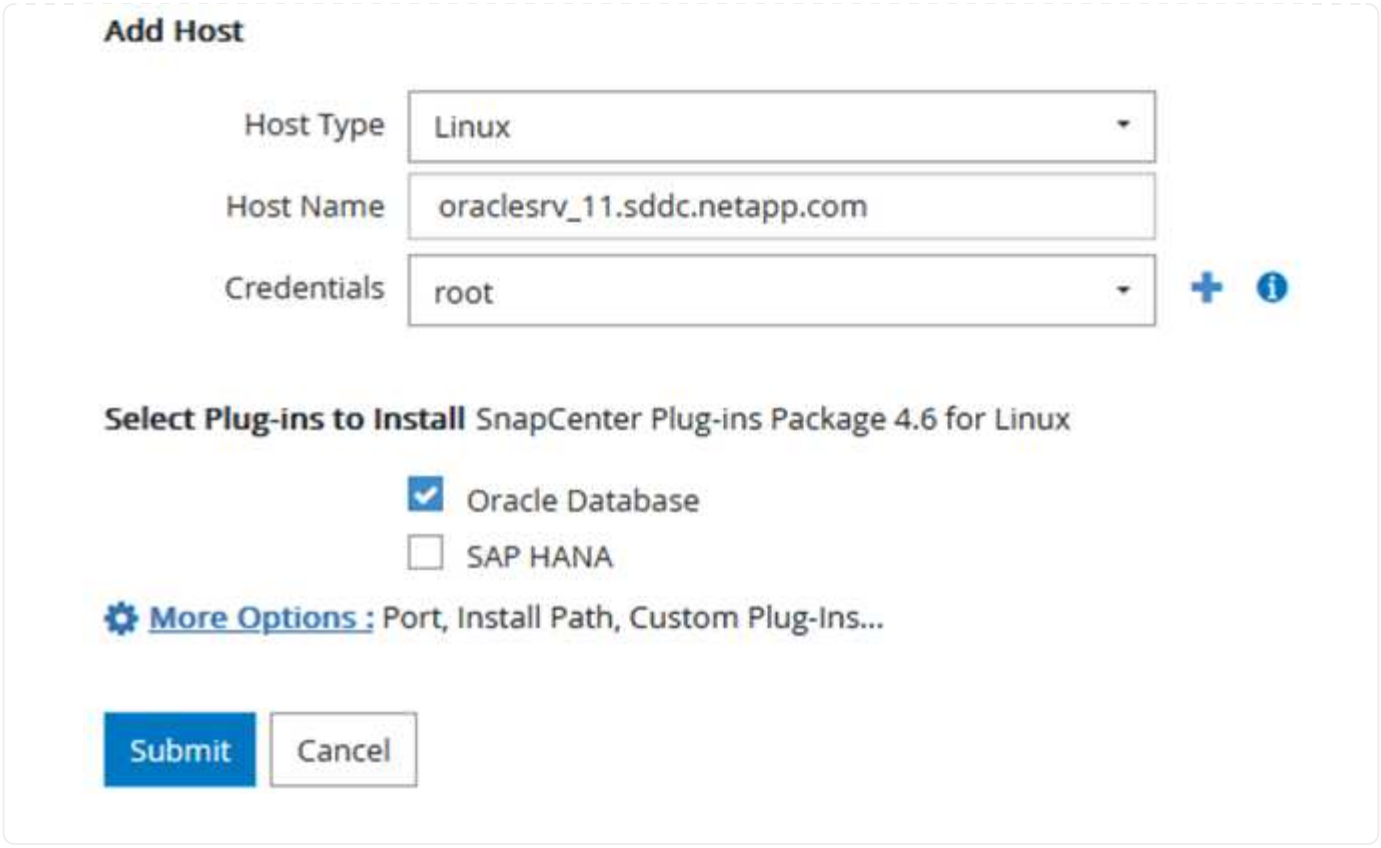
Aggiungere host a SnapCenter

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

1. Dal menu a sinistra, selezionare host, quindi fare clic su Aggiungi per avviare il processo di aggiunta dei controller di storage a SnapCenter.
2. Nella finestra Add hosts (Aggiungi host), aggiungere il tipo di host, il nome host e le credenziali del sistema host. Selezionare il tipo di plug-in. Per SQL Server, selezionare il plug-in Microsoft Windows e Microsoft SQL Server.



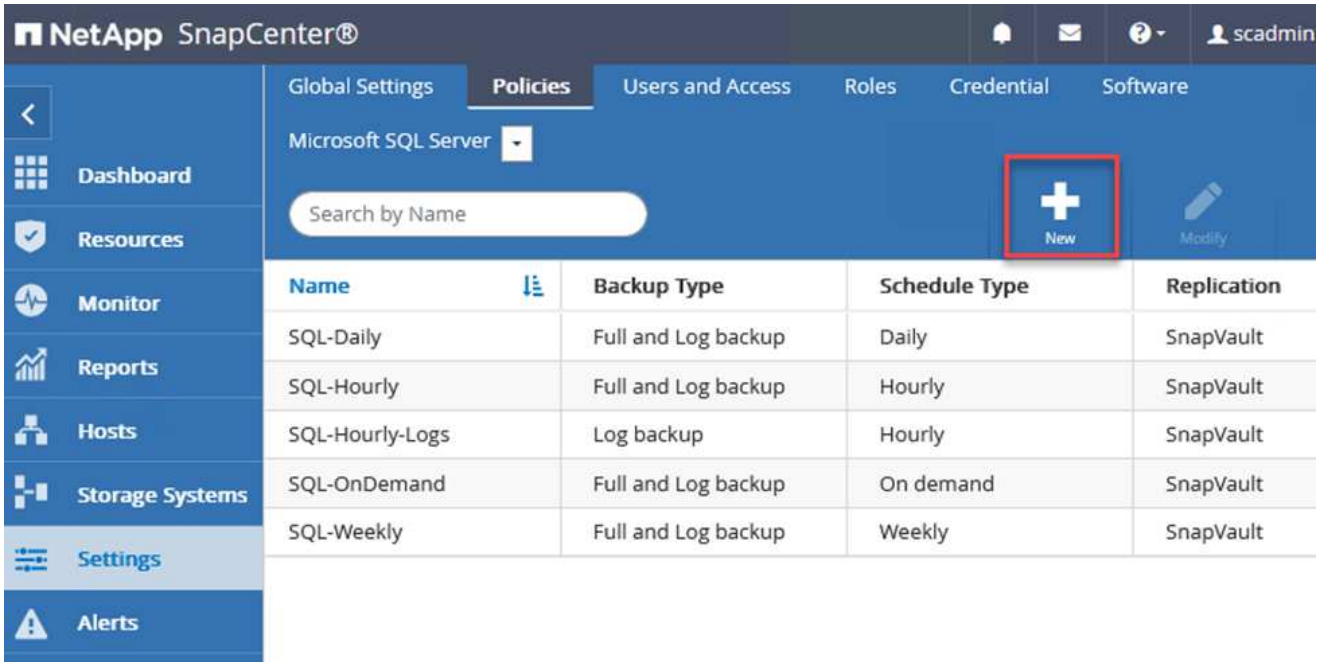
3. Per Oracle, compilare i campi obbligatori nella finestra di dialogo Add host (Aggiungi host) e selezionare la casella di controllo per il plug-in Oracle Database. Fare clic su Submit (Invia) per avviare il processo di rilevamento e aggiungere l'host a SnapCenter.


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

Creare policy SnapCenter

I criteri 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 log delle transazioni.

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



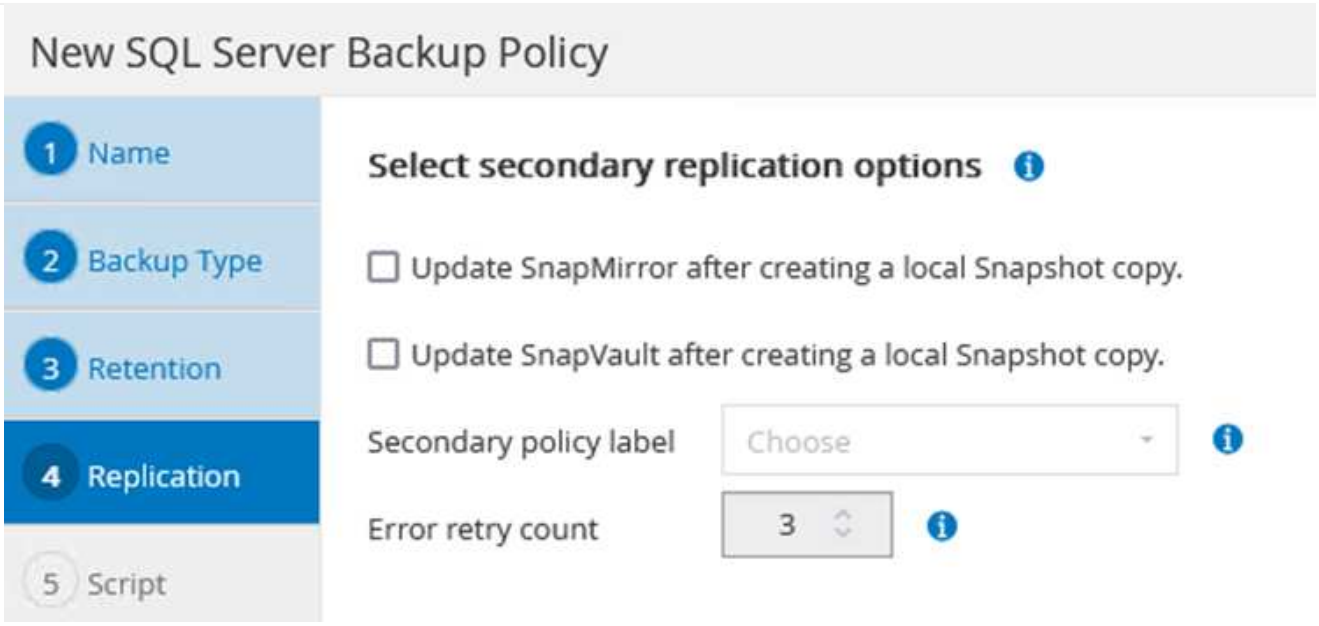
Per informazioni complete sulla creazione di criteri per i backup di SQL Server, vedere "Documentazione SnapCenter".

Per informazioni complete sulla creazione di policy per i backup Oracle, vedere "Documentazione SnapCenter".

Note:

- Durante la creazione guidata dei criteri, prendere nota della sezione Replication (Replica). In questa sezione vengono descritti i tipi di copie SnapMirror secondarie che si desidera eseguire durante il processo di backup.
- L'impostazione "Update SnapMirror after creating a local Snapshot copy" (Aggiorna SnapMirror dopo la creazione di una copia Snapshot locale) fa riferimento all'aggiornamento di una relazione SnapMirror quando tale relazione esiste tra due macchine virtuali di storage che risiedono sullo stesso cluster.
- L'impostazione "Aggiorna SnapVault dopo la creazione di una copia snapshot locale" viene utilizzata per aggiornare una relazione SnapMirror esistente tra due cluster separati e tra un sistema ONTAP on-premise e Cloud Volumes ONTAP o FSxN.

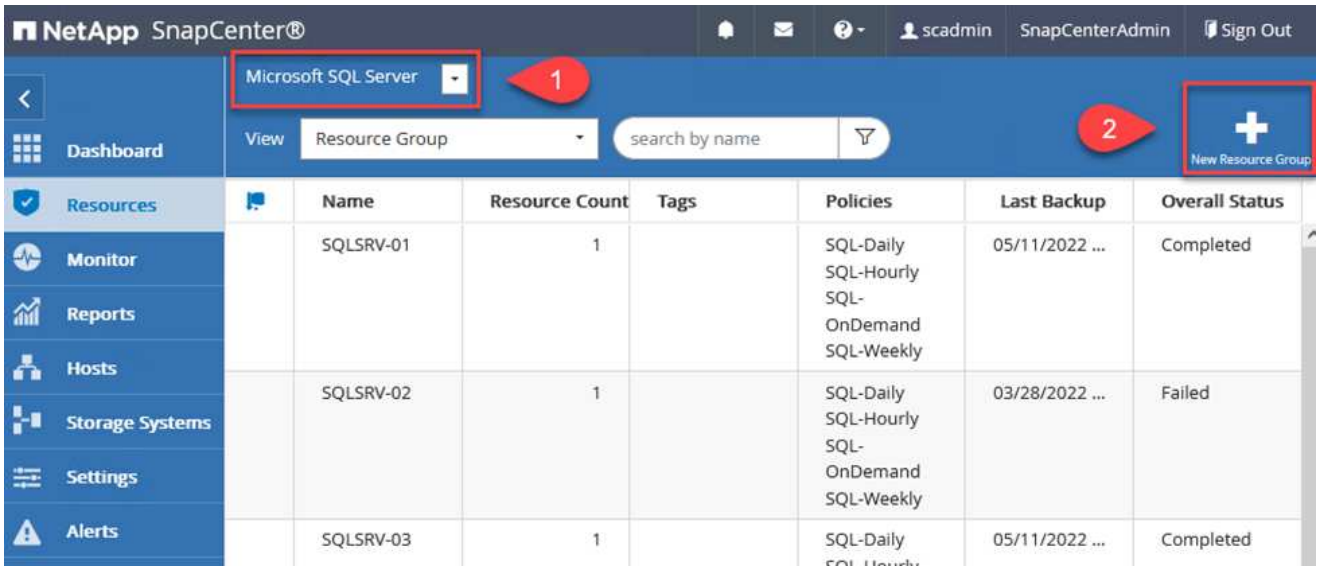
L'immagine seguente mostra le opzioni precedenti e l'aspetto della procedura guidata dei criteri di backup.



Creare gruppi di risorse SnapCenter

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

1. Accedere alla sezione risorse nel menu a sinistra.
2. Nella parte superiore della finestra, selezionare il tipo di risorsa da utilizzare (in questo caso Microsoft SQL Server), quindi fare clic su New Resource Group (nuovo gruppo di risorse).



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

Per eseguire il backup delle risorse SQL, seguire questa procedura "questo link".

Per eseguire il backup delle risorse Oracle, seguire questa procedura "questo link".

Implementare e configurare Veeam Backup Server

Il software Veeam Backup & Replication viene utilizzato nella soluzione per eseguire il backup delle macchine virtuali delle applicazioni e archiviare una copia dei backup in un bucket Amazon S3 utilizzando un repository di backup scale-out Veeeam (SOBR). Veeam viene implementato su un server Windows in questa soluzione. Per informazioni specifiche sull'implementazione di Veeam, vedere "Documentazione tecnica del centro di assistenza Veeam".

Configurare il repository di backup scale-out Veeam

Dopo aver implementato e ottenuto la licenza del software, è possibile creare un repository di backup scale-out (SOBR) come storage di destinazione per i processi di backup. È inoltre necessario includere un bucket S3 come backup dei dati delle macchine virtuali fuori sede per il disaster recovery.

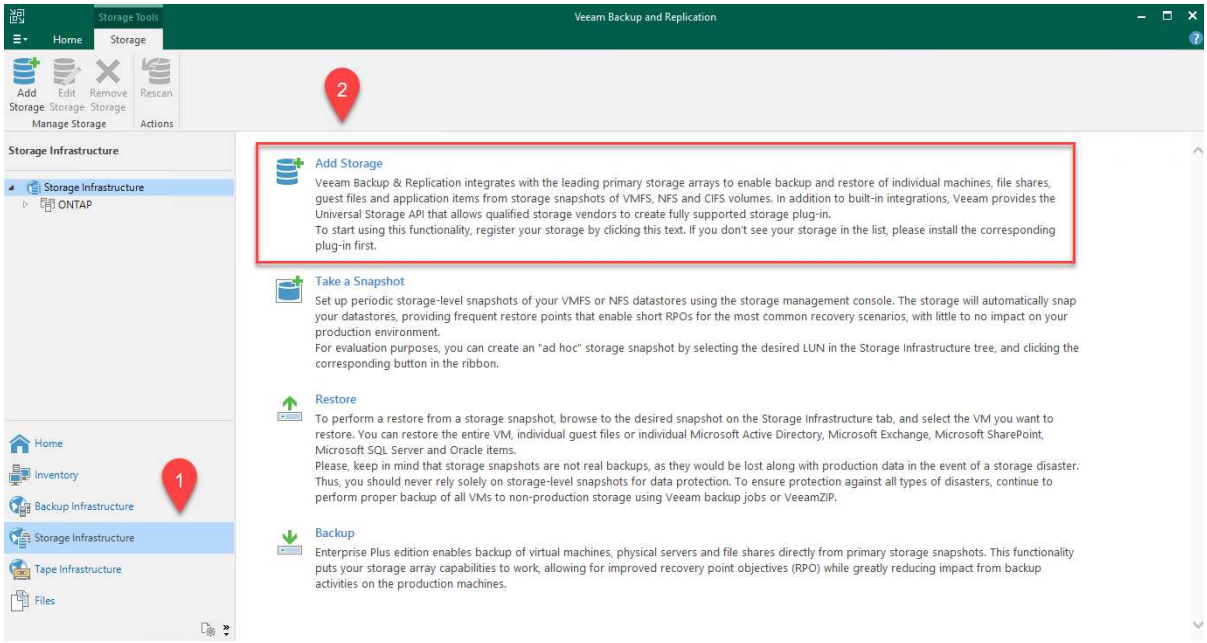
Prima di iniziare, consultare i seguenti prerequisiti.

1. Creare una condivisione di file SMB sul sistema ONTAP on-premise come storage di destinazione per i backup.
2. Crea un bucket Amazon S3 da includere nel SOBR. Si tratta di un repository per i backup fuori sede.

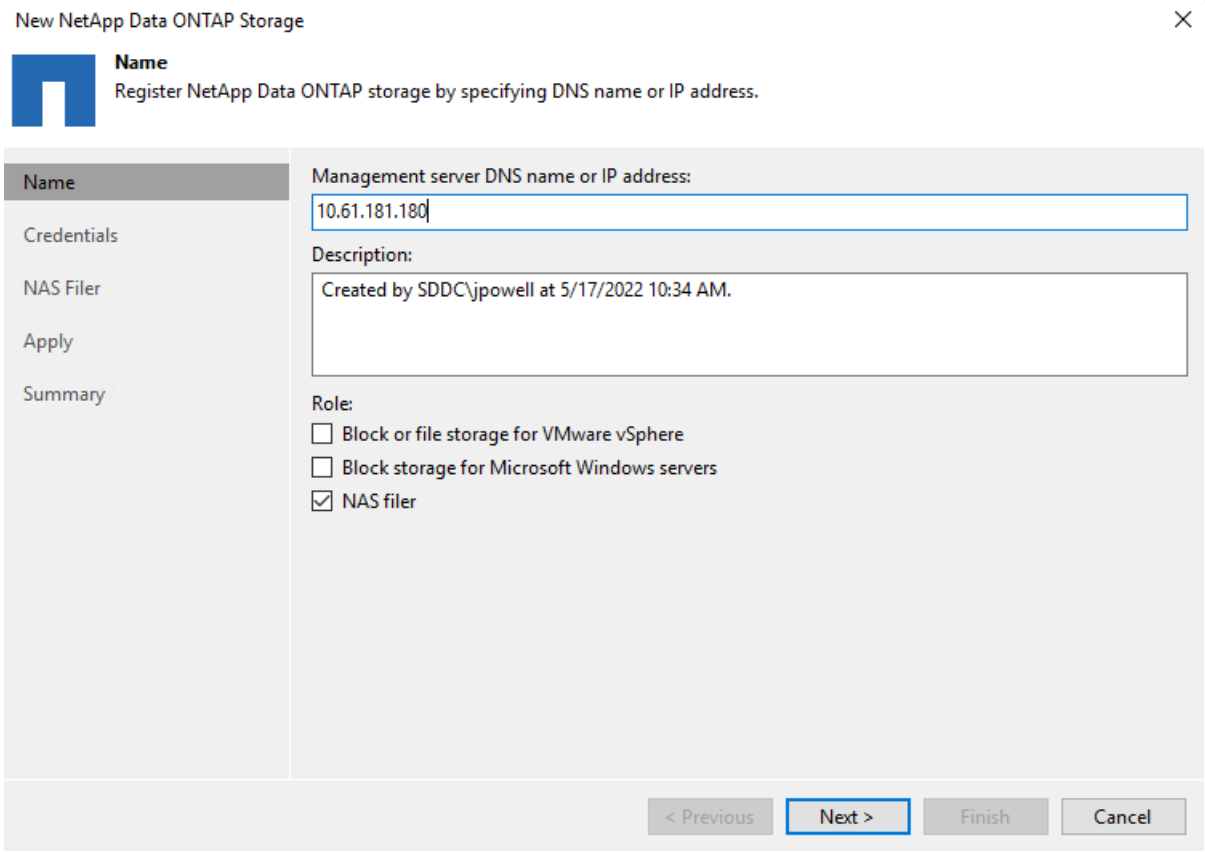
Aggiungere storage ONTAP a Veeam

Innanzitutto, aggiungere il cluster di storage ONTAP e il relativo file system SMB/NFS come infrastruttura storage in Veeam.

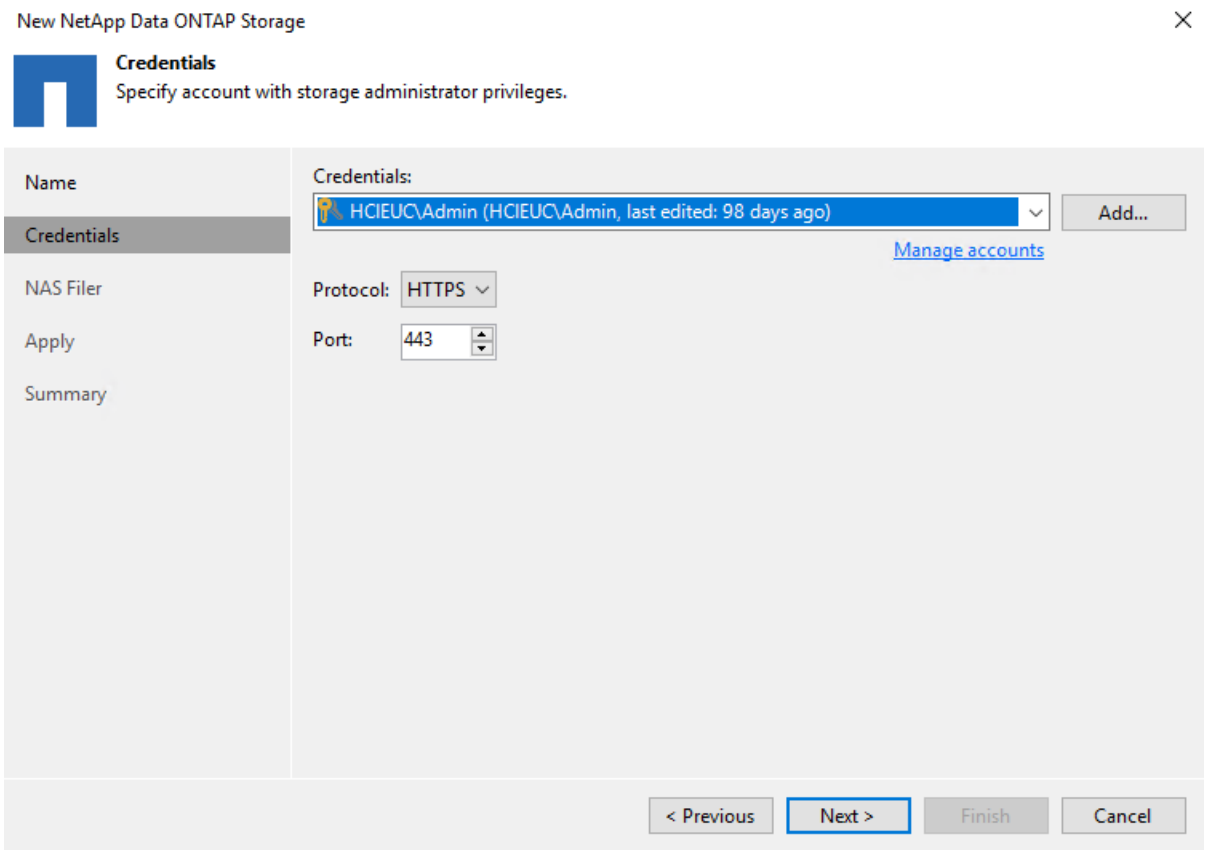
1. Aprire la console Veeam ed effettuare l'accesso. Accedere a Storage Infrastructure (infrastruttura storage) e selezionare Add Storage (Aggiungi storage).



2. Nella procedura guidata Aggiungi storage, selezionare NetApp come vendor dello storage, quindi selezionare Data ONTAP.
3. Inserire l'indirizzo IP di gestione e selezionare la casella NAS Filer (Filer NAS). Fare clic su Avanti.

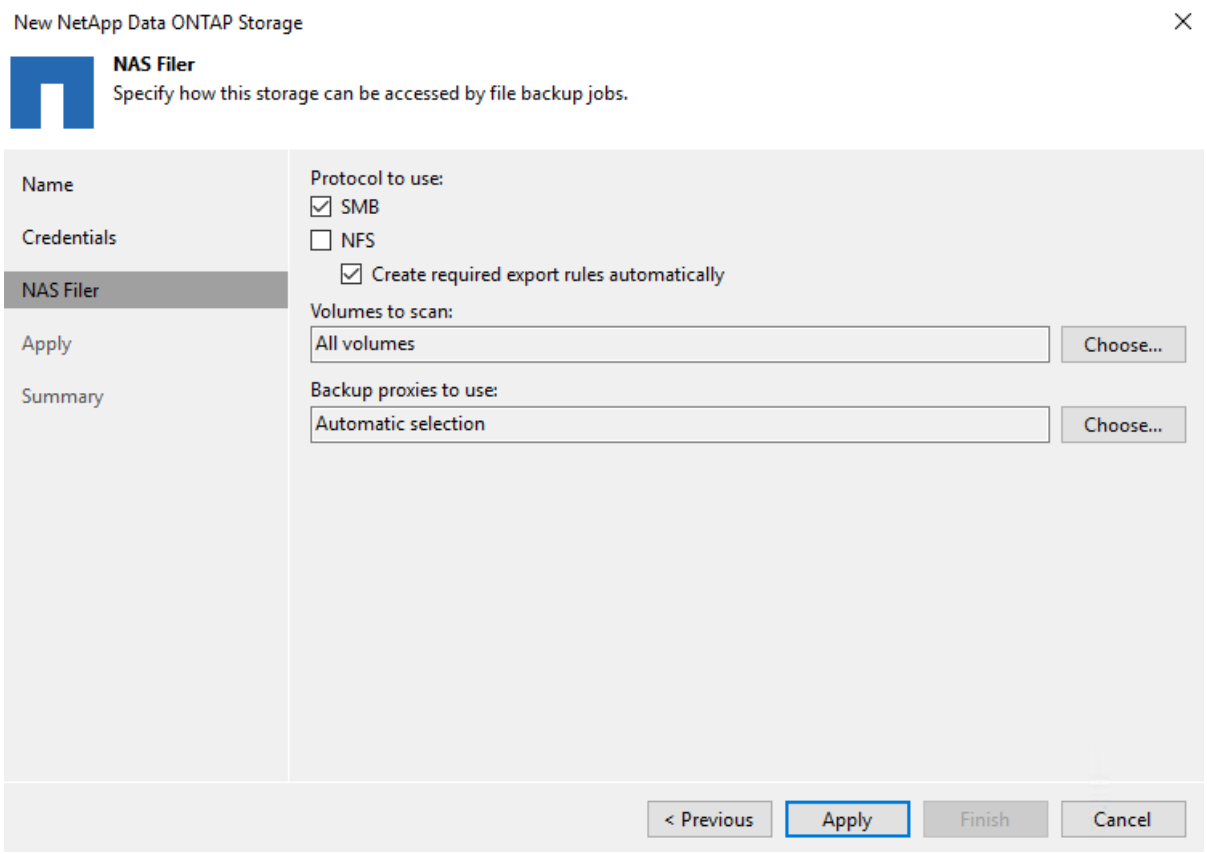


4. Aggiungere le credenziali per accedere al cluster ONTAP.

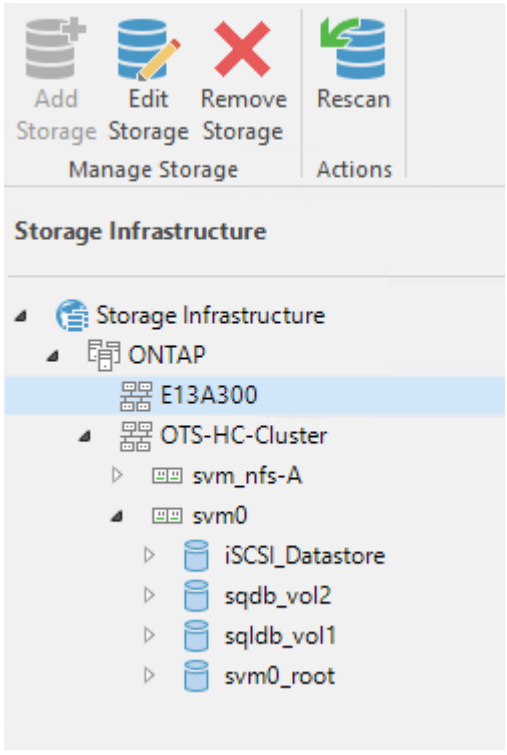


5. Nella pagina NAS Filer (Filer NAS), scegliere i protocolli desiderati per la scansione e

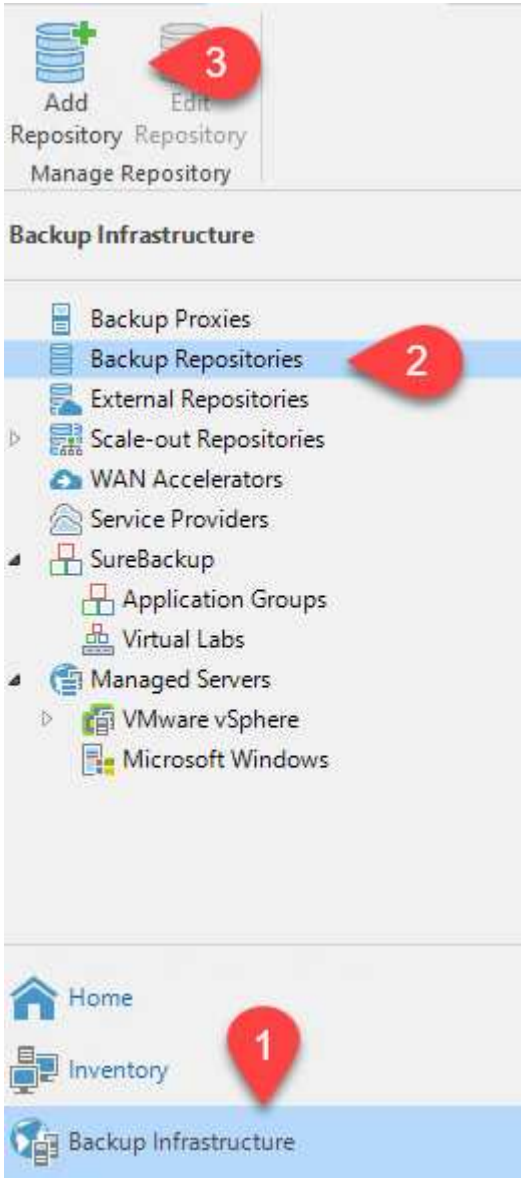
selezionare Next (Avanti).



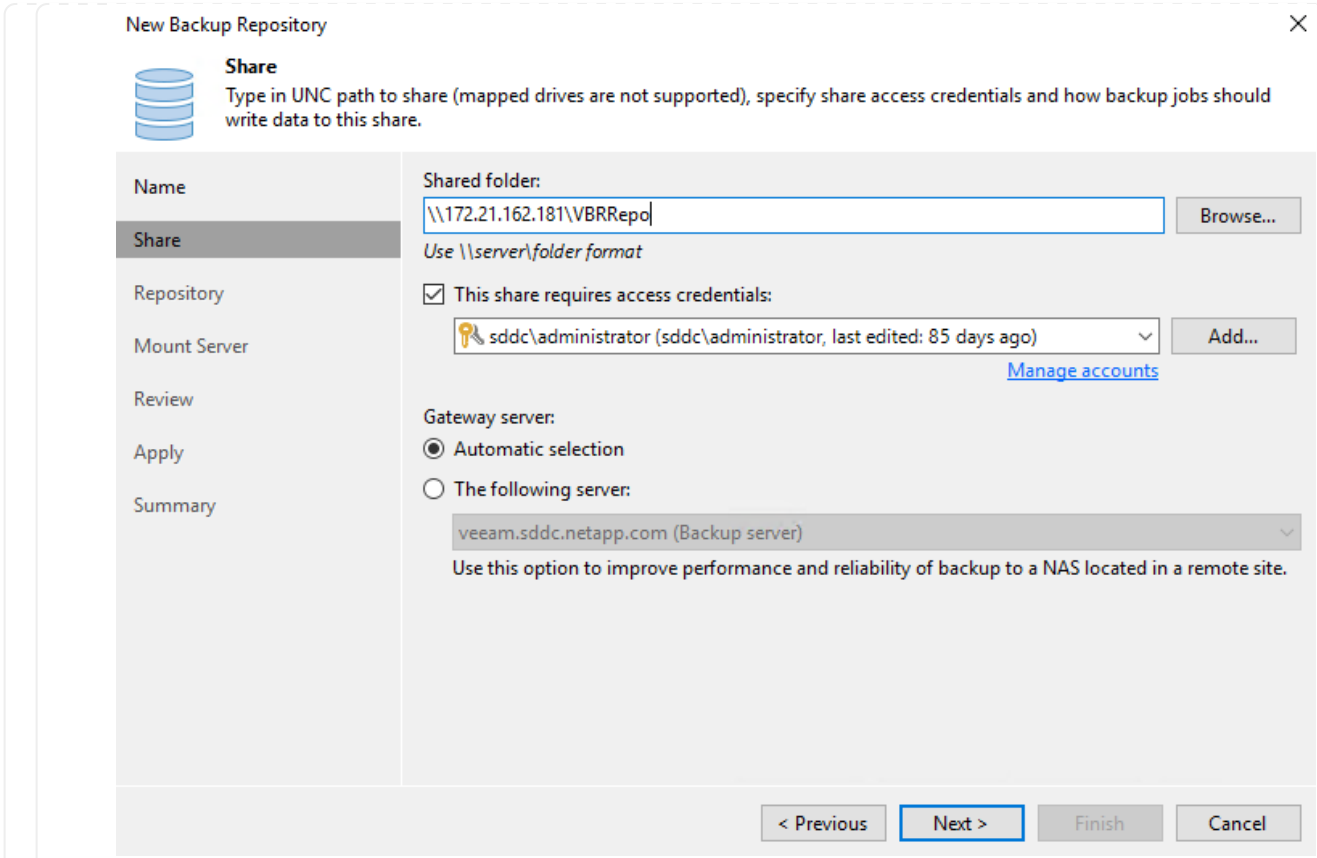
6. Completare le pagine Apply (Applica) e Summary (Riepilogo) della procedura guidata e fare clic su Finish (fine) per avviare il processo di rilevamento dello storage. Al termine della scansione, il cluster ONTAP viene aggiunto insieme ai filer NAS come risorse disponibili.



7. Creare un repository di backup utilizzando le condivisioni NAS appena rilevate. Da Backup Infrastructure (infrastruttura di backup), selezionare Backup Repository (repository di backup) e fare clic sulla voce di menu Add Repository (Aggiungi repository).



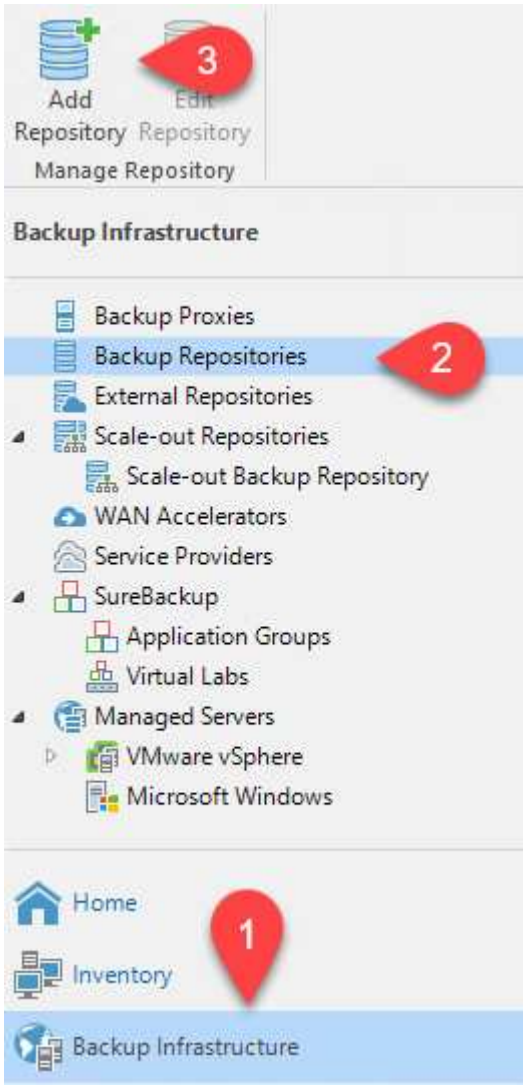
8. Seguire tutti i passaggi della procedura guidata nuovo repository di backup per creare il repository. Per informazioni dettagliate sulla creazione di repository di backup Veeam, vedere "Documentazione Veeam".


New Backup Repository
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
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

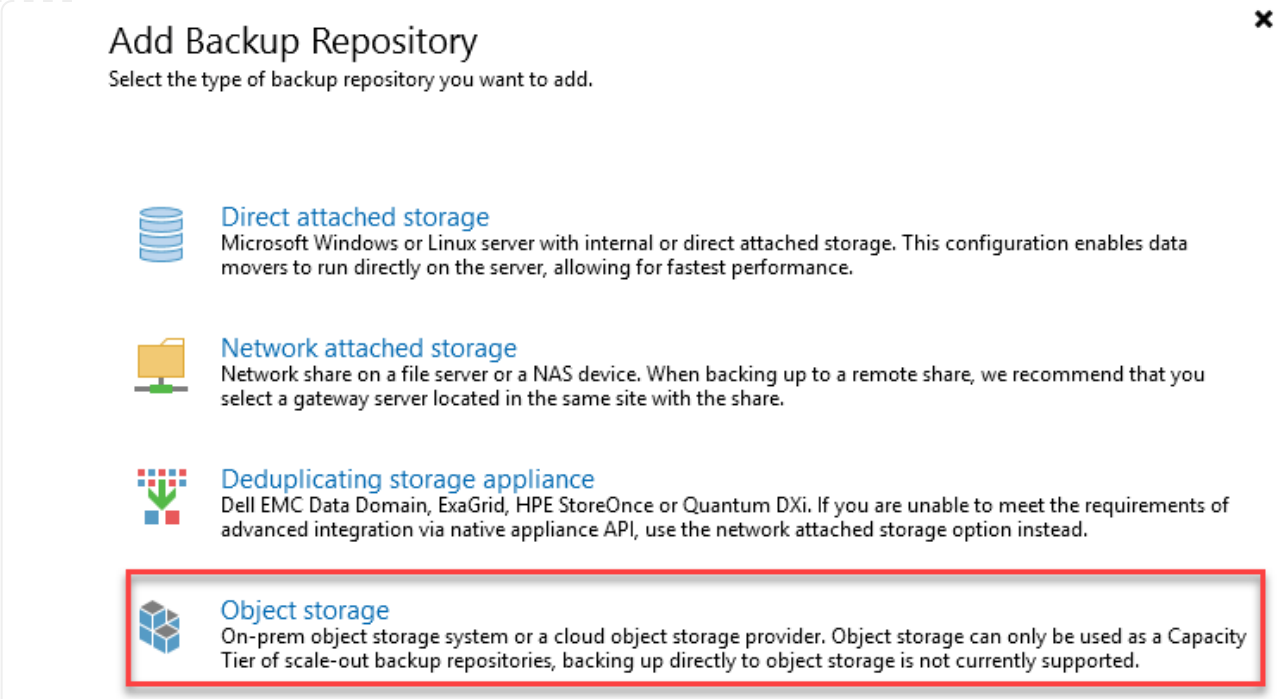
Aggiungi il bucket Amazon S3 come repository di backup

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

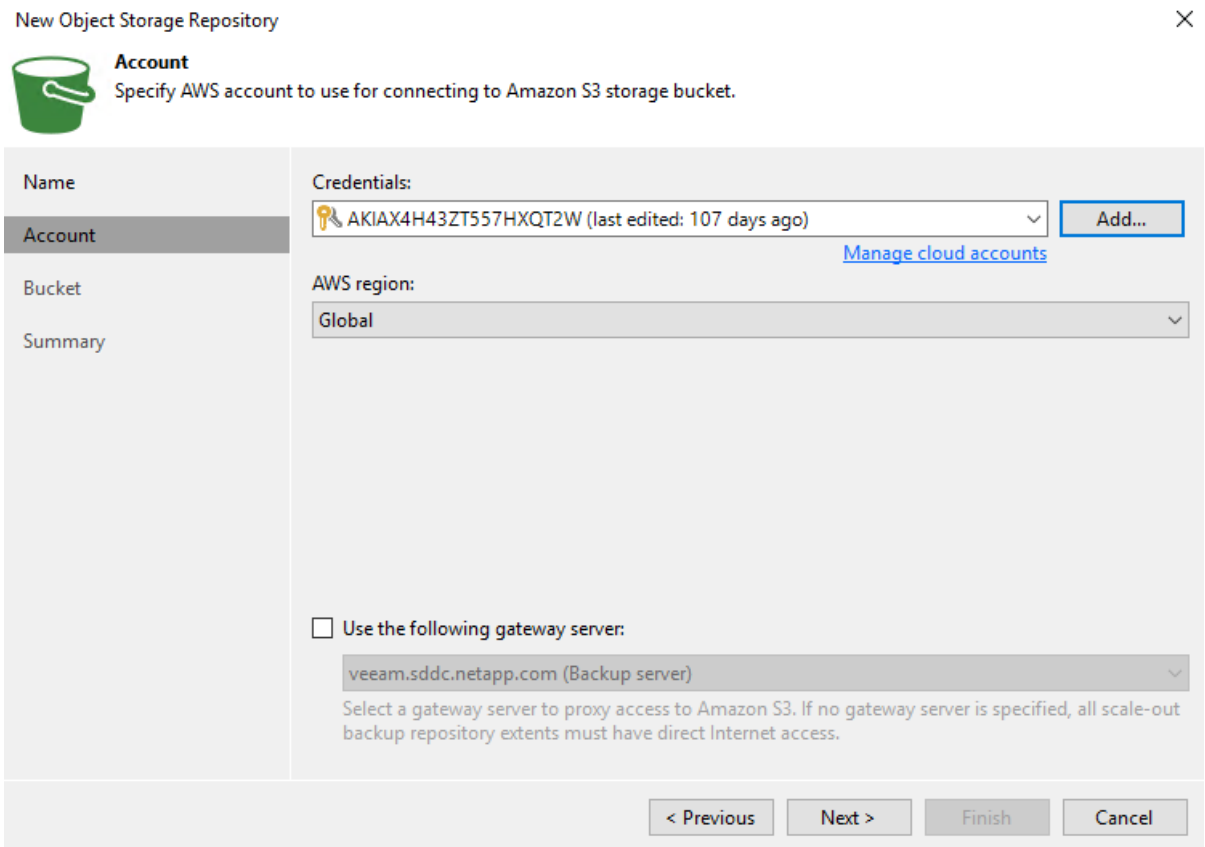
1. Accedere a infrastruttura di backup > Repository di backup. Fare clic su Add Repository (Aggiungi repository).



2. Nella procedura guidata Aggiungi repository di backup, selezionare Archivio oggetti, quindi Amazon S3. Viene avviata la procedura guidata nuovo archivio oggetti.



3. Fornire un nome per il repository di storage a oggetti e fare clic su Next (Avanti).
4. Nella sezione successiva, fornire le credenziali. Sono necessari una chiave di accesso AWS e una chiave segreta.

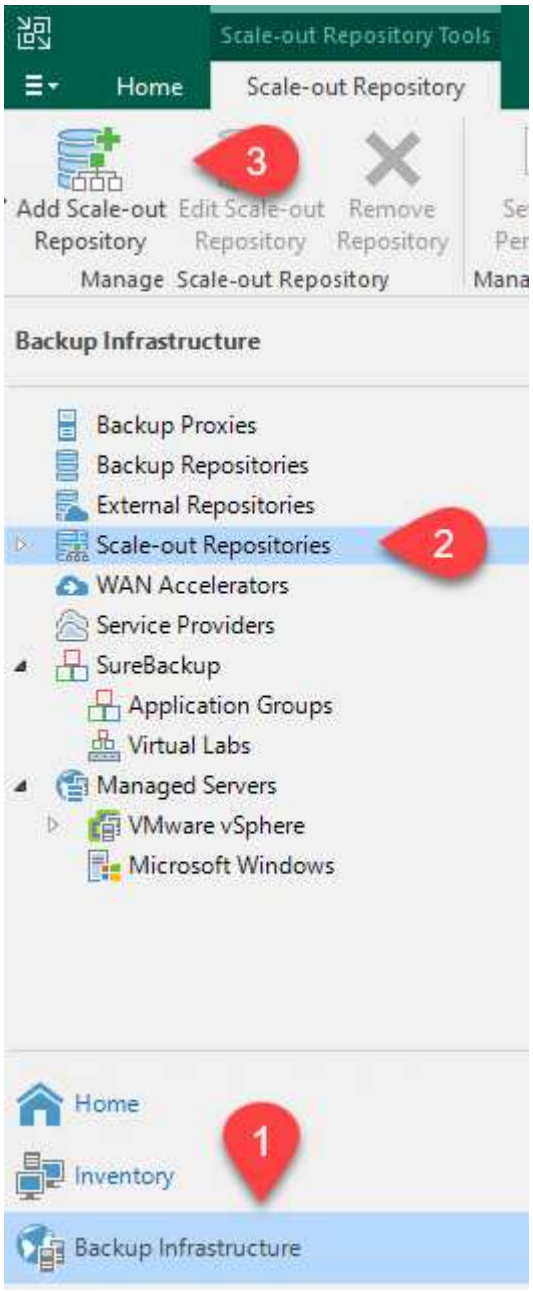


5. Una volta caricata la configurazione Amazon, scegliere il data center, il bucket e la cartella e fare clic su Apply (Applica). Infine, fare clic su fine per chiudere la procedura guidata.

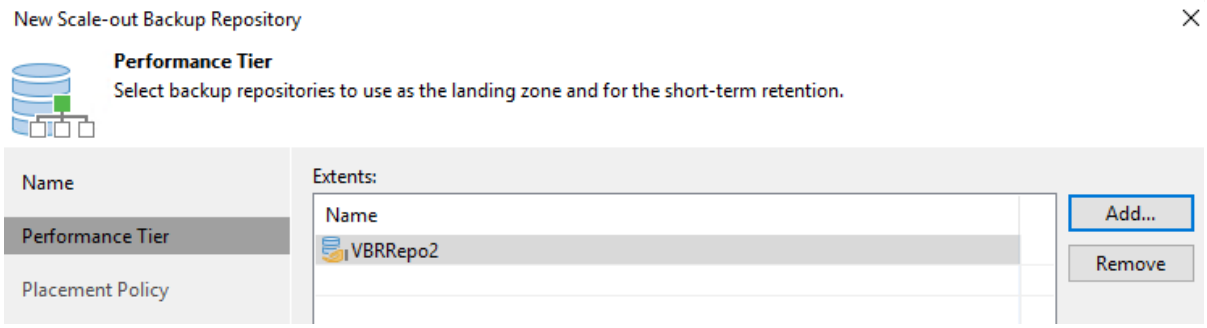
Creare un repository di backup scale-out

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

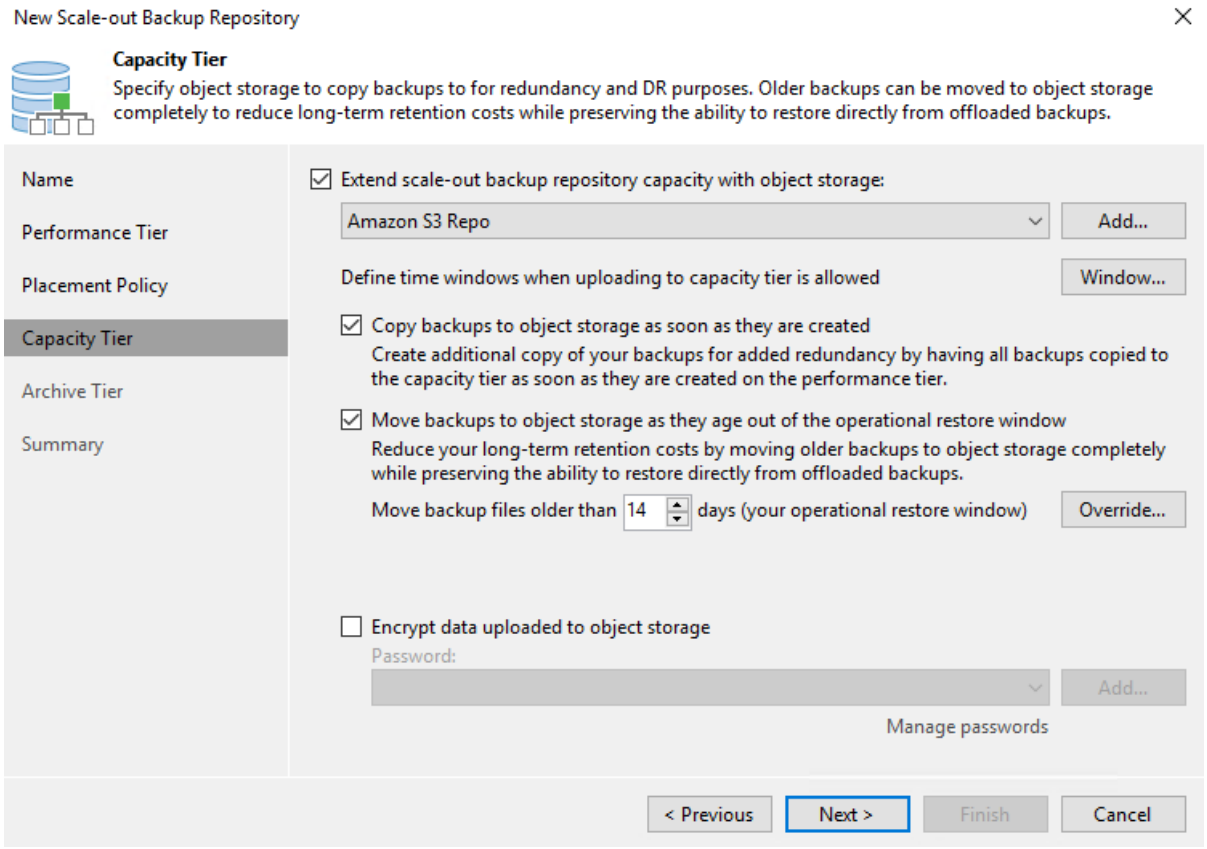
1. Da Backup Infrastructure (infrastruttura di backup), selezionare Scale-out Repository (repository scale-out), quindi fare clic sulla voce di menu Add Scale-out Repository (Aggiungi repository scale-out).



2. Nel nuovo repository di backup scale-out, immettere un nome per il SOBR e fare clic su Avanti.
3. Per il livello di performance, scegliere il repository di backup che contiene la condivisione SMB che risiede nel cluster ONTAP locale.



4. Per la policy di posizionamento, scegli la localizzazione dei dati o le performance in base ai tuoi requisiti. Selezionare Avanti.
5. Per il livello di capacità estendiamo il SOBR con lo storage a oggetti Amazon S3. Ai fini del disaster recovery, selezionare Copy Backup to Object Storage (Copia backup su storage a oggetti) non appena vengono creati per garantire la consegna tempestiva dei backup secondari.



6. Infine, selezionare Apply (Applica) e Finish (fine) per finalizzare la creazione del SOBR.

Creare i processi di repository di backup scale-out

L'ultima fase della configurazione di Veeam consiste nella creazione di processi di backup utilizzando il SOBR appena creato come destinazione di backup. La creazione di processi di backup è una parte normale del repertorio di qualsiasi amministratore dello storage e non viene descritta la procedura dettagliata. Per informazioni più complete sulla creazione di processi di backup in Veeam, vedere "Documentazione tecnica del Centro assistenza Veeam".

Configurazione e strumenti di backup e recovery di BlueXP

Per eseguire un failover delle macchine virtuali applicative e dei volumi di database sui servizi di volume cloud VMware in esecuzione in AWS, è necessario installare e configurare un'istanza in esecuzione del server SnapCenter e del server di backup e replica Veeeam. Una volta completato il failover, è necessario configurare questi strumenti per riprendere le normali operazioni di backup fino a quando non viene pianificato ed eseguito un failback al data center on-premise.

Implementare il server Windows SnapCenter secondario

Il server SnapCenter viene implementato nell'SDDC cloud VMware o installato su un'istanza EC2 che risiede in un VPC con connettività di rete all'ambiente cloud VMware.

Il software SnapCenter è disponibile sul sito di supporto NetApp e può essere installato su sistemi Microsoft Windows che risiedono in un dominio o in un gruppo di lavoro. Una guida dettagliata alla pianificazione e le istruzioni di installazione sono disponibili all'indirizzo "Centro di documentazione NetApp".

Il software SnapCenter è disponibile all'indirizzo "questo link".

Configurare il server secondario Windows SnapCenter

Per eseguire un ripristino dei dati applicativi mirrorati in FSX ONTAP, è necessario prima eseguire un ripristino completo del database SnapCenter on-premise. Una volta completato questo processo, la comunicazione con le macchine virtuali viene ristabilita e i backup delle applicazioni possono ora riprendere utilizzando FSX ONTAP come storage primario.

A tale scopo, è necessario completare i seguenti elementi sul server SnapCenter:

1. Configurare il nome del computer in modo che sia identico al server SnapCenter on-premise originale.
2. Configurare il networking per comunicare con VMware Cloud e l'istanza di FSX ONTAP.
3. Completare la procedura per ripristinare il database SnapCenter.
4. Verificare che SnapCenter sia in modalità di disaster recovery per assicurarsi che FSX sia ora lo storage primario per i backup.
5. Verificare che la comunicazione con le macchine virtuali ripristinate sia stata ristabilita.

Implementare il server di replica Veeam Backup & secondario

È possibile installare il server Veeam Backup & Replication su un server Windows in VMware Cloud su AWS o su un'istanza EC2. Per informazioni dettagliate sull'implementazione, vedere "Documentazione tecnica del Centro assistenza Veeam".

Configurare il server di replica di Veeam Backup & secondario

Per eseguire un ripristino delle macchine virtuali di cui è stato eseguito il backup sullo 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 macchine virtuali dopo il ripristino.

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

1. Configurare il networking per comunicare con VMware Cloud, FSX ONTAP e il bucket S3 contenente il repository di backup originale.
2. Configura una condivisione SMB su FSX ONTAP per diventare un nuovo repository di backup.
3. Montare il bucket S3 originale utilizzato come parte del repository di backup scale-out on-premise.
4. Dopo il ripristino della macchina virtuale, stabilire nuovi processi di backup per proteggere le macchine virtuali SQL e Oracle.

Per ulteriori informazioni sul ripristino delle macchine virtuali utilizzando Veeam, vedere la sezione "Ripristinare le macchine virtuali dell'applicazione con il ripristino completo di Veeam".

Backup del database SnapCenter per il disaster recovery

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 di SnapCenter su un'istanza di AWS EC2 che risiede nel nostro VPC. Per ulteriori informazioni su questo passaggio, vedere "questo link".

Prerequisiti per il backup di SnapCenter

Per il backup di SnapCenter sono necessari i seguenti prerequisiti:

- Un volume e una condivisione SMB creati sul sistema ONTAP on-premise per individuare i file di database e di configurazione di cui è stato eseguito il backup.
- Una relazione SnapMirror tra il sistema ONTAP on-premise e FSX o CVO nell'account AWS. Questa relazione viene utilizzata per trasportare lo snapshot contenente il database SnapCenter di cui è stato eseguito il 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 di Windows EC2 o sulla macchina virtuale in VMware Cloud.

Riepilogo del processo di backup e ripristino di SnapCenter

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

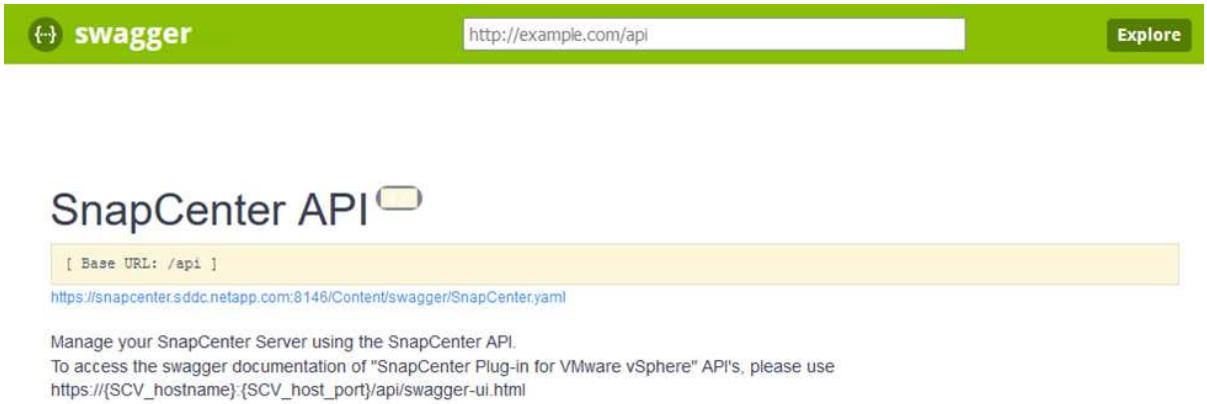
Eseguire il backup del database e della configurazione di SnapCenter

SnapCenter fornisce un'interfaccia client Web per l'esecuzione dei comandi API REST. Per informazioni sull'accesso alle API REST tramite Swagger, consultare la documentazione di SnapCenter all'indirizzo "questo link".

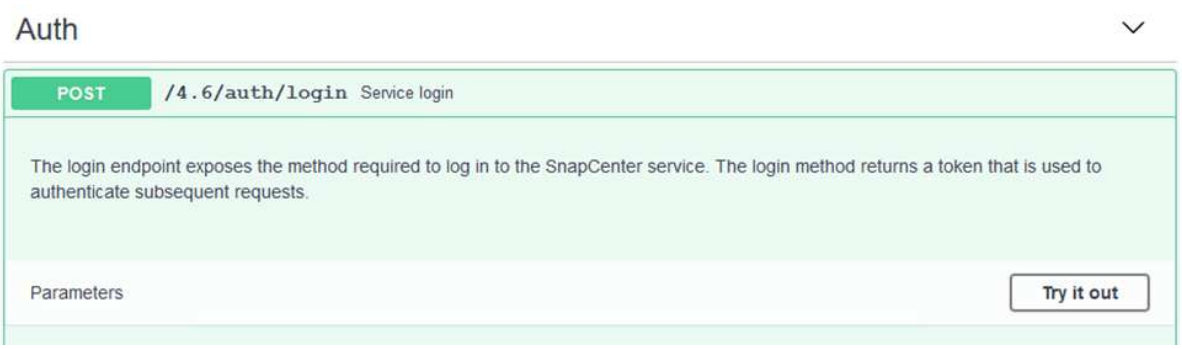
Accedere a Swagger e ottenere il token di autorizzazione

Una volta aperta la pagina Swagger, è necessario recuperare un token di autorizzazione per avviare il processo di ripristino del database.

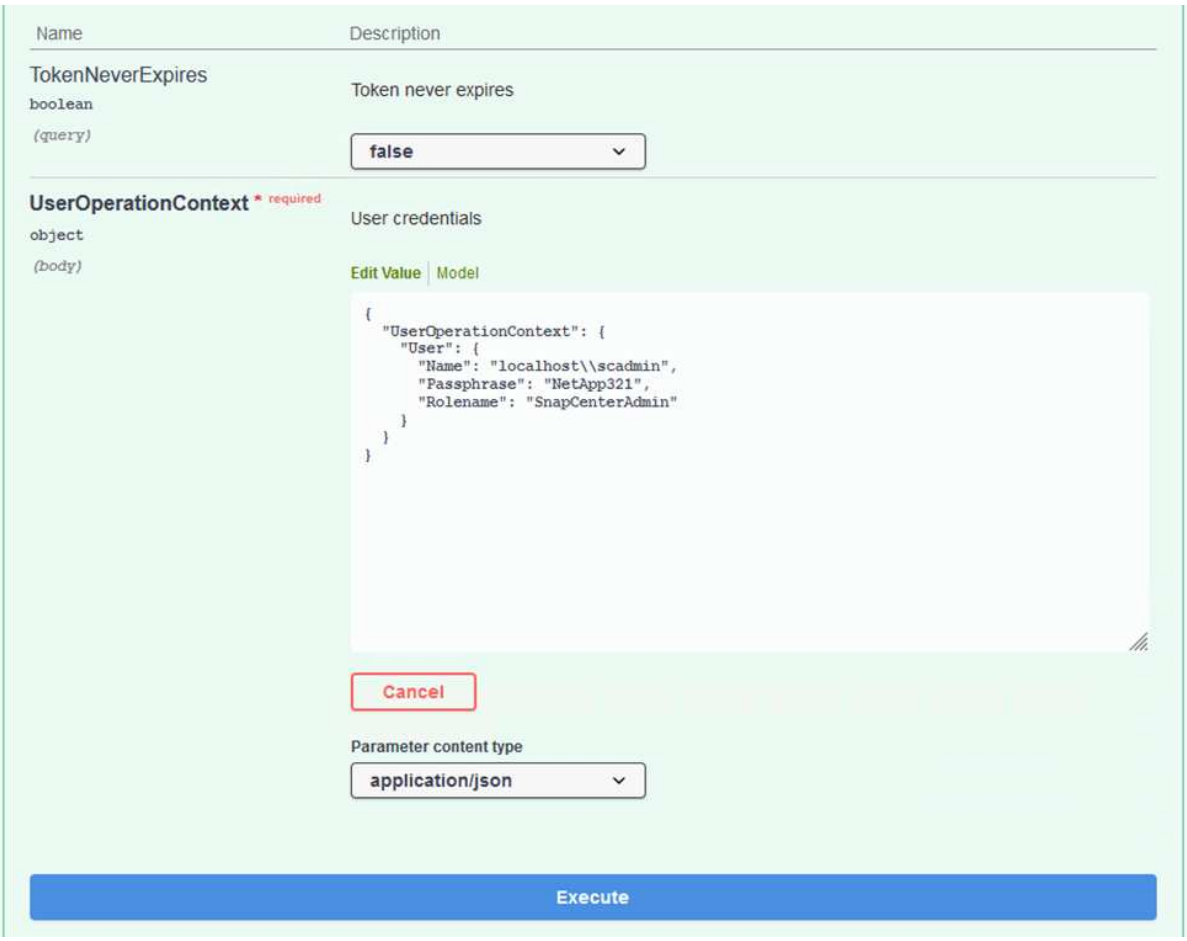
1. Accedere alla pagina Web dell'API di swagger SnapCenter all'indirizzo */https://<SnapCenter Server IP>:8146/swagger/*.



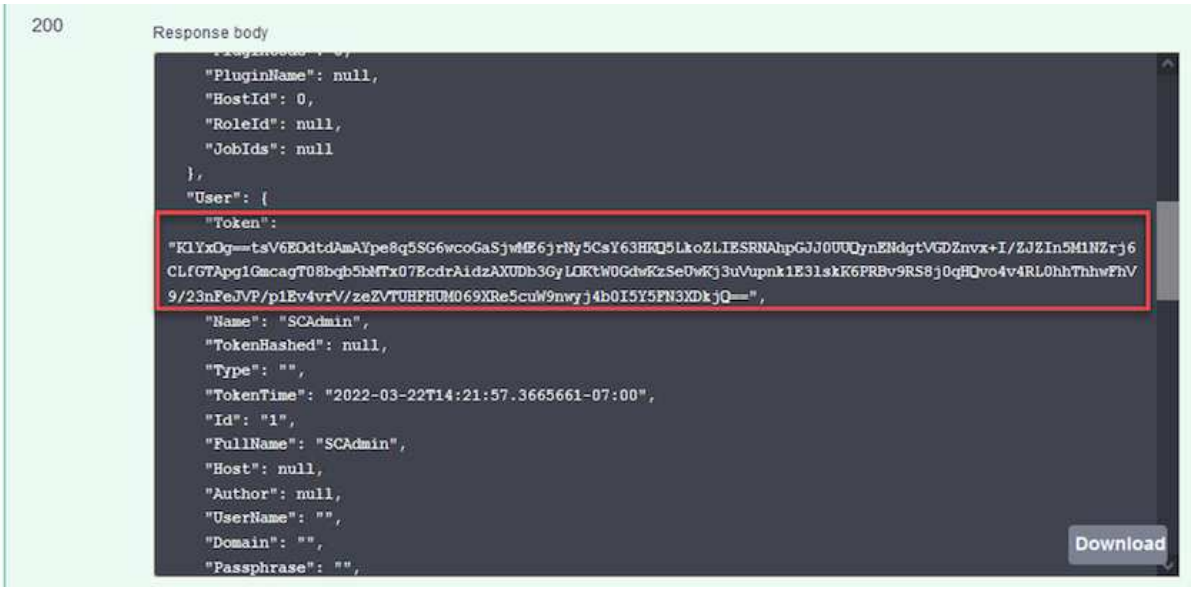
2. Espandere la sezione Auth e fare clic su Provalo.



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



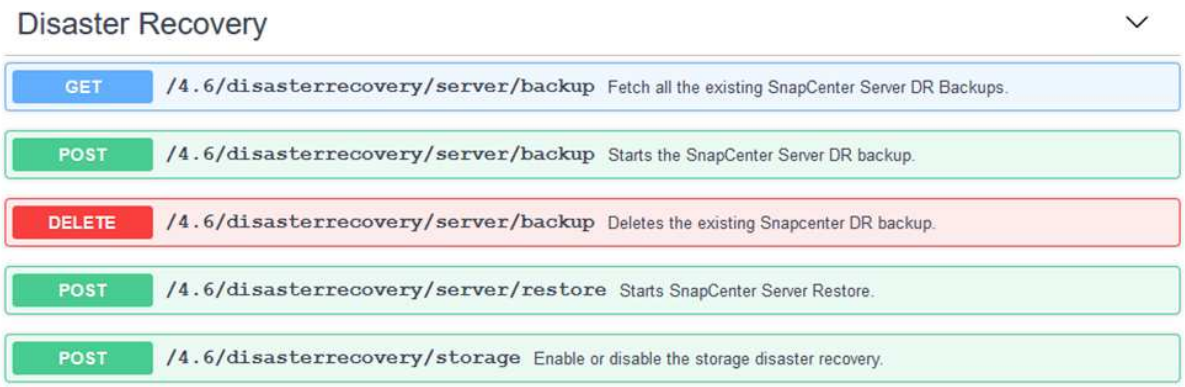
4. Nel corpo di risposta riportato di seguito, è possibile visualizzare il token. Copiare il testo del token per l'autenticazione durante l'esecuzione del processo di backup.



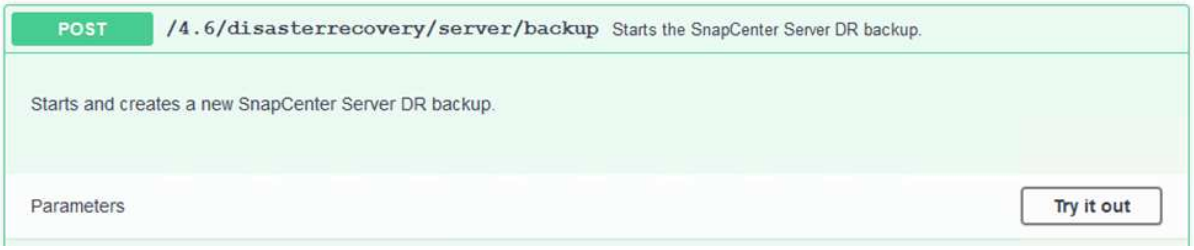
Eseguire un backup del database SnapCenter

Quindi, accedere all'area Disaster Recovery della pagina Swagger per avviare il processo di backup di SnapCenter.

1. Espandere l'area Disaster Recovery facendo clic su di essa.

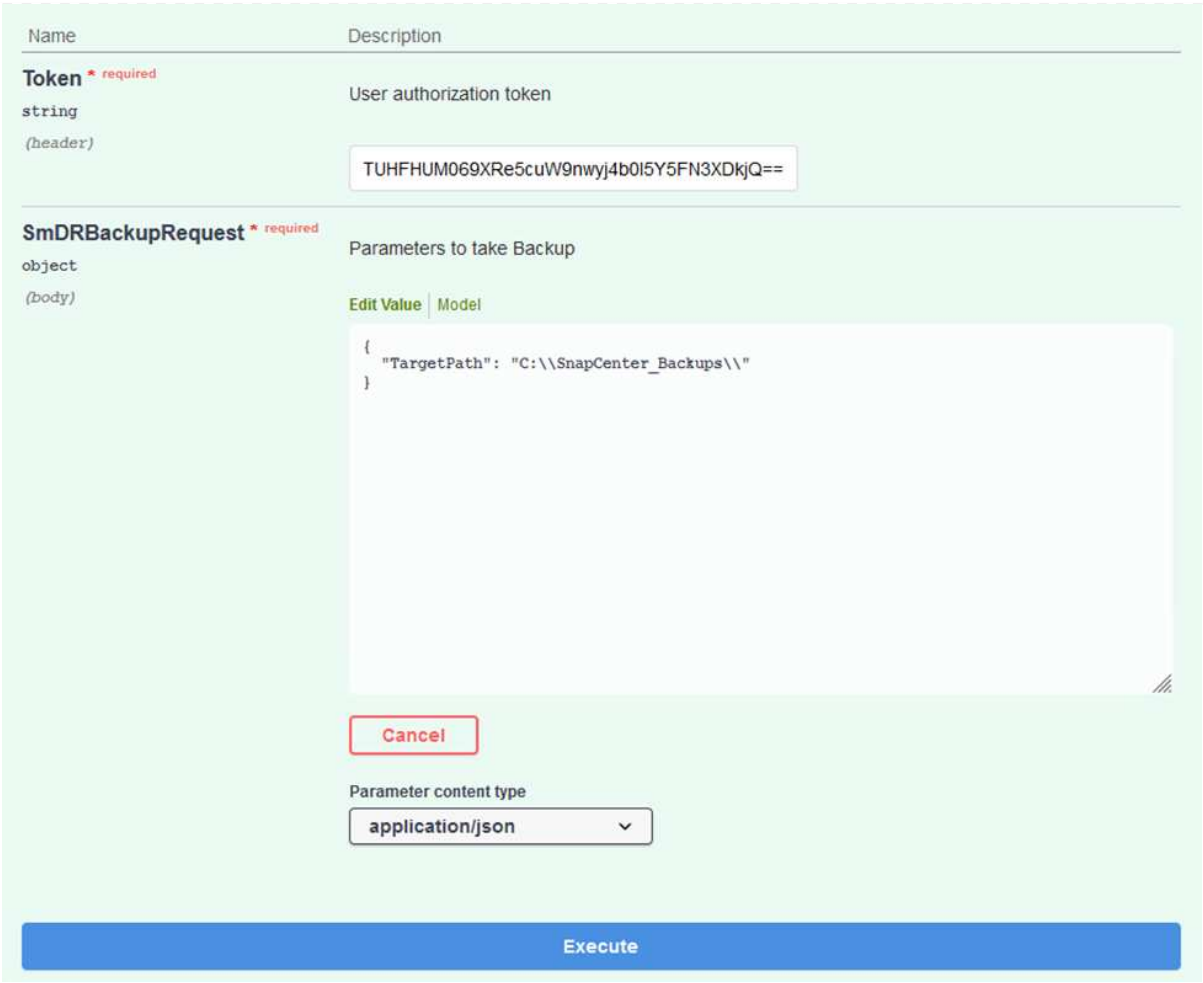


2. Espandere `/4.6/disasterrecovery/server/backup` E fare clic su Provalo.



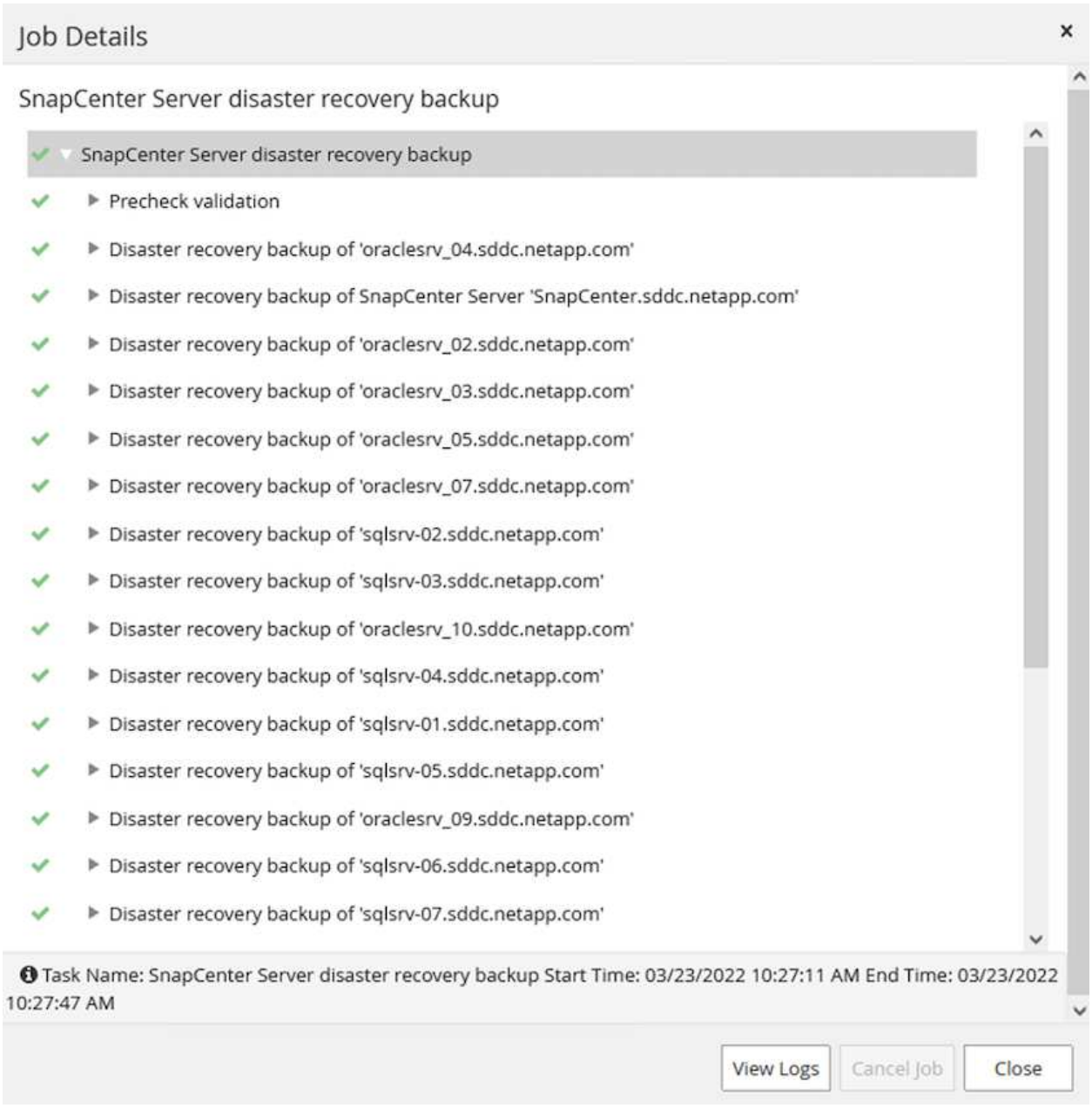
3. Nella sezione SmDRBackupRequest, aggiungere il percorso di destinazione locale corretto e selezionare Execute (Esegui) per avviare il backup del database e della configurazione di SnapCenter.

> Il processo di backup non consente il backup diretto su una condivisione file NFS o CIFS.


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

Monitorare il processo di backup da SnapCenter

Accedere a SnapCenter per esaminare i file di registro quando si avvia il processo di ripristino del database. Nella sezione Monitor, è possibile visualizzare i dettagli del backup di disaster recovery del server SnapCenter.



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

Quindi, spostare il backup dal disco locale sul server SnapCenter alla condivisione CIFS utilizzata per copiare i dati nella posizione secondaria situata sull'istanza FSX in AWS. Utilizzare xcopy con opzioni specifiche che conservano i permessi 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 primario on-premise, il nostro scenario include il failover su un sito secondario che risiede nell'infrastruttura Amazon Web Services utilizzando VMware Cloud su AWS. Supponiamo che le macchine virtuali e il nostro cluster ONTAP on-premise non siano più accessibili. Inoltre, le macchine virtuali SnapCenter e Veeam non sono più accessibili e devono essere ricostruite nel nostro sito secondario.

In questa sezione viene descritto il failover della nostra infrastruttura nel cloud e vengono trattati i seguenti argomenti:

- Ripristino del database SnapCenter. Una volta stabilito un nuovo server SnapCenter, ripristinare il database MySQL e i file di configurazione e attivare la modalità di disaster recovery per consentire allo storage FSX secondario di diventare il dispositivo di storage primario.
- Ripristinare le macchine virtuali dell'applicazione utilizzando Veeam Backup & Replication. Collegare lo storage S3 che contiene i backup delle macchine virtuali, 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

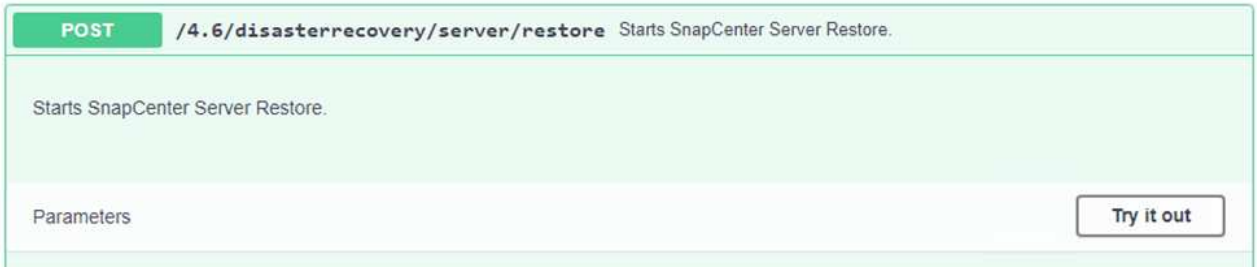
SnapCenter supporta scenari di disaster recovery consentendo il backup e il ripristino del database MySQL e dei file di configurazione. Ciò consente a un amministratore di mantenere backup regolari del database SnapCenter nel data center on-premise e di ripristinare successivamente tale database in un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

Per accedere ai file di backup di SnapCenter sul server SnapCenter remoto, attenersi alla seguente procedura:

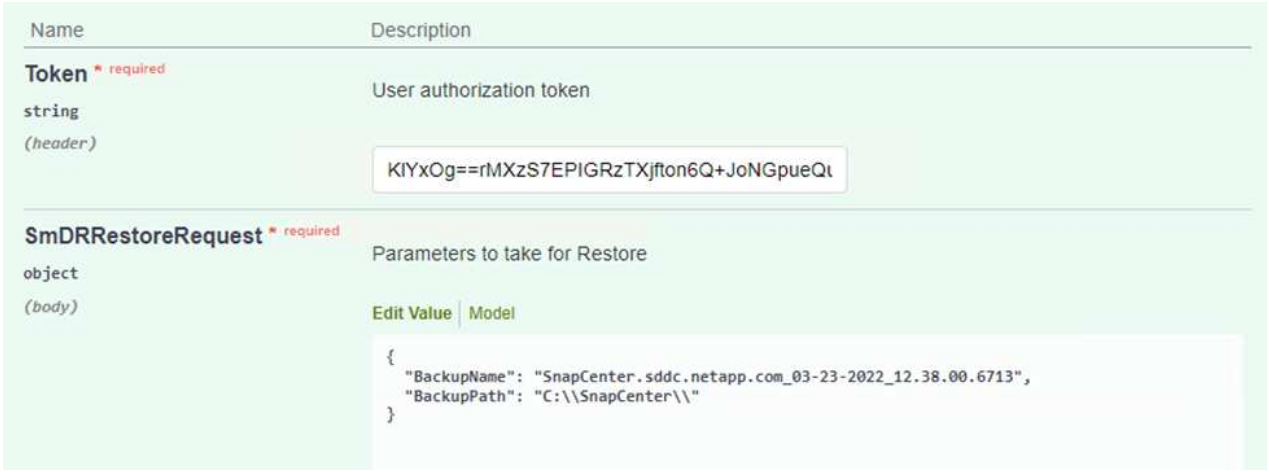
1. Interrompere la relazione di SnapMirror dal cluster FSX, che rende il volume in lettura/scrittura.
2. Creare un server CIFS (se necessario) e una condivisione CIFS che punta al percorso di giunzione del volume clonato.
3. Utilizzare xcopy per copiare i file di backup in una directory locale sul sistema SnapCenter secondario.
4. Installare SnapCenter v4.6.
5. Assicurarsi che il server SnapCenter abbia lo stesso nome FQDN del server originale. Questo è necessario per il ripristino del db.

Per avviare il processo di ripristino, attenersi alla seguente procedura:

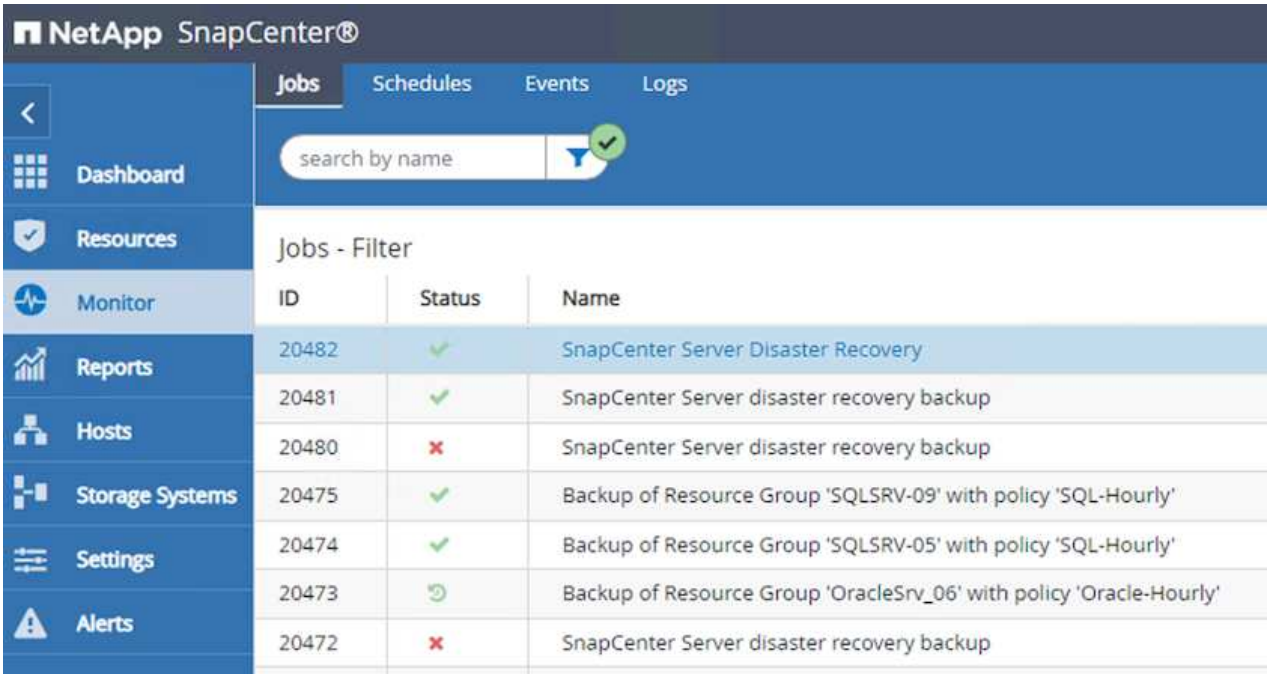
1. Accedere alla pagina Web API Swagger per il server SnapCenter secondario e seguire le istruzioni precedenti per ottenere un token di autorizzazione.
2. Accedere alla sezione Disaster Recovery della pagina Swagger e selezionare `/4.6/disasterrecovery/server/restore`E fare clic su Provalo.

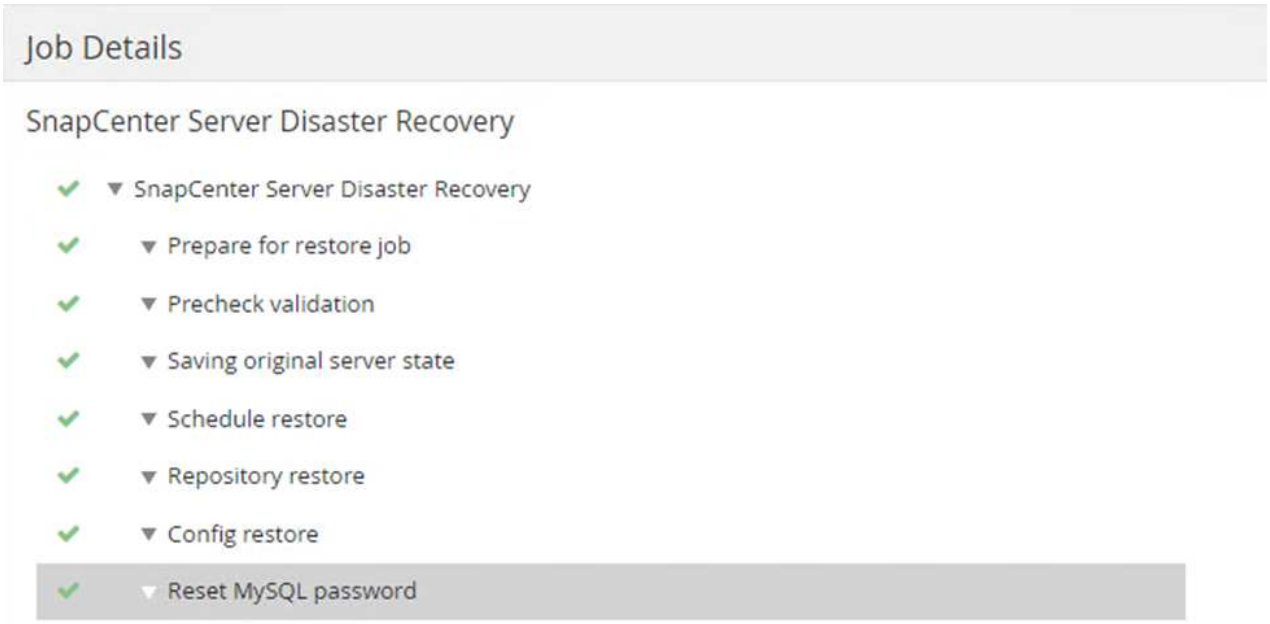


3. Incollare il token di autorizzazione e, nella sezione SmDRResterRequest, incollare il nome del backup e la directory locale sul server SnapCenter secondario.



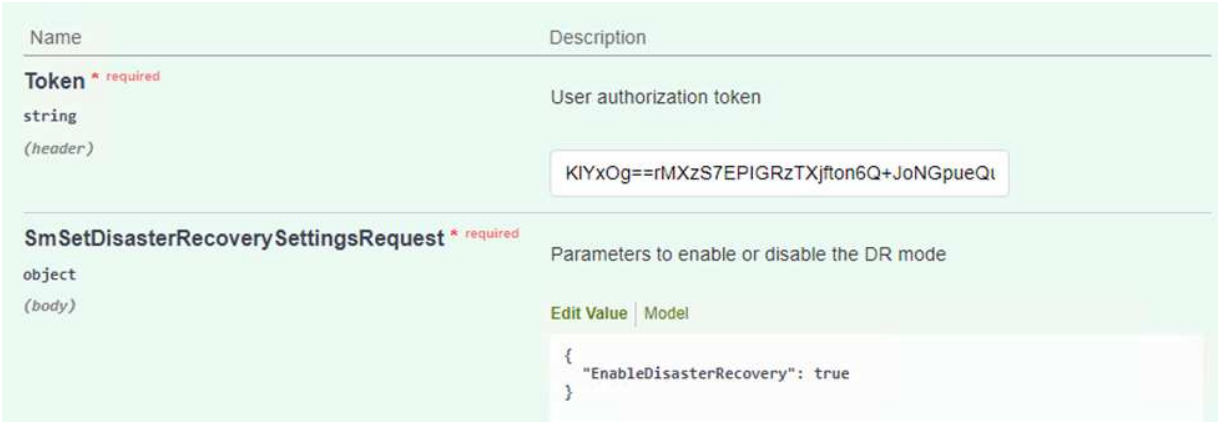
4. Selezionare il pulsante Execute (Esegui) per avviare il processo di ripristino.
5. Da SnapCenter, accedere alla sezione Monitor per visualizzare l'avanzamento del processo di ripristino.





6. Per abilitare i ripristini di SQL Server dallo storage secondario, è necessario attivare la modalità di disaster recovery nel database SnapCenter. Questa operazione viene eseguita come operazione separata e avviata sulla pagina Web API di Swagger.
   a. Accedere alla sezione Disaster Recovery e fare clic su `/4.6/disasterrecovery/storage`.
   b. Incollare il token di autorizzazione dell'utente.
   c. Nella sezione SmSetDisasterRecoverySettingsRequest, modificare `EnableDisasterRecover` a. `true`.

d. Fare clic su Execute (Esegui) per attivare la modalità di disaster recovery per SQL Server.



Vedere i commenti relativi alle procedure aggiuntive.

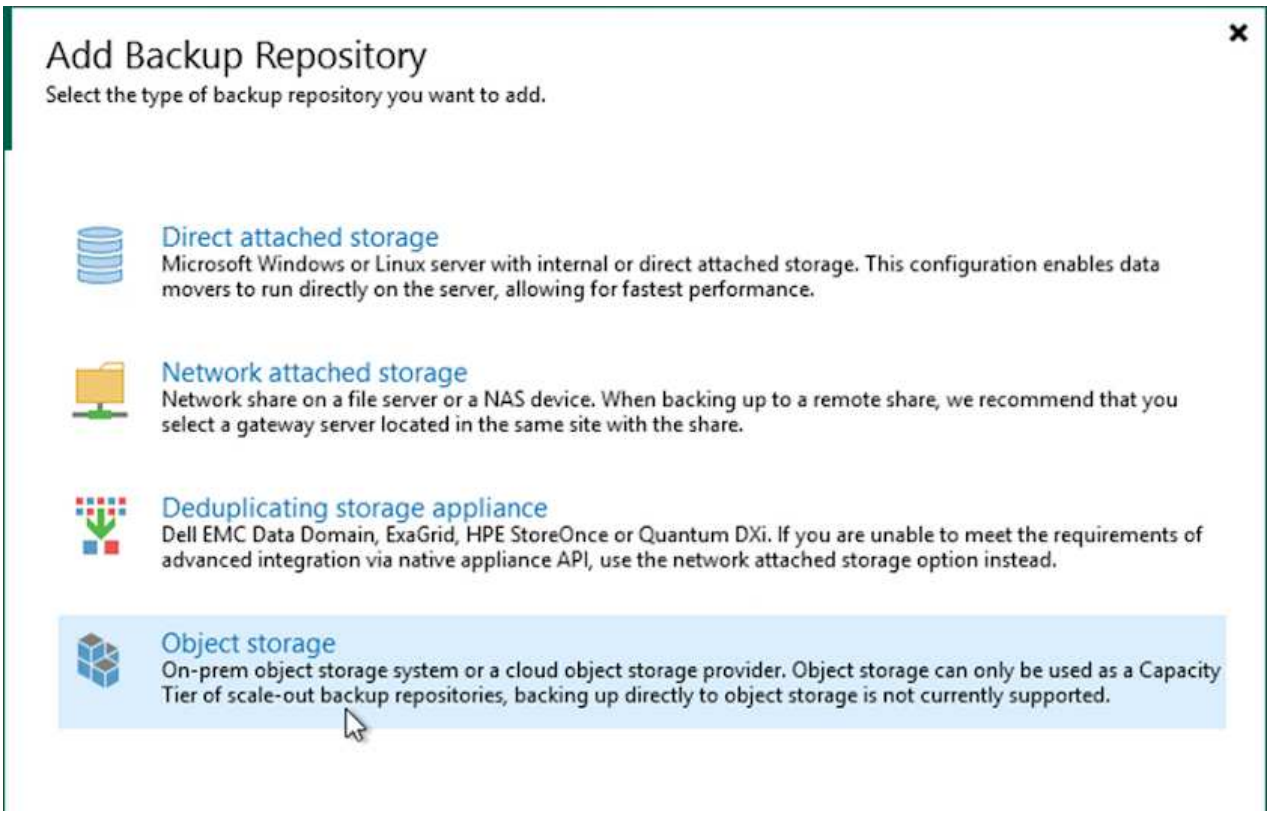
Ripristinare le macchine virtuali applicative con il ripristino completo di Veeam

Creare un repository di backup e importare i backup da S3

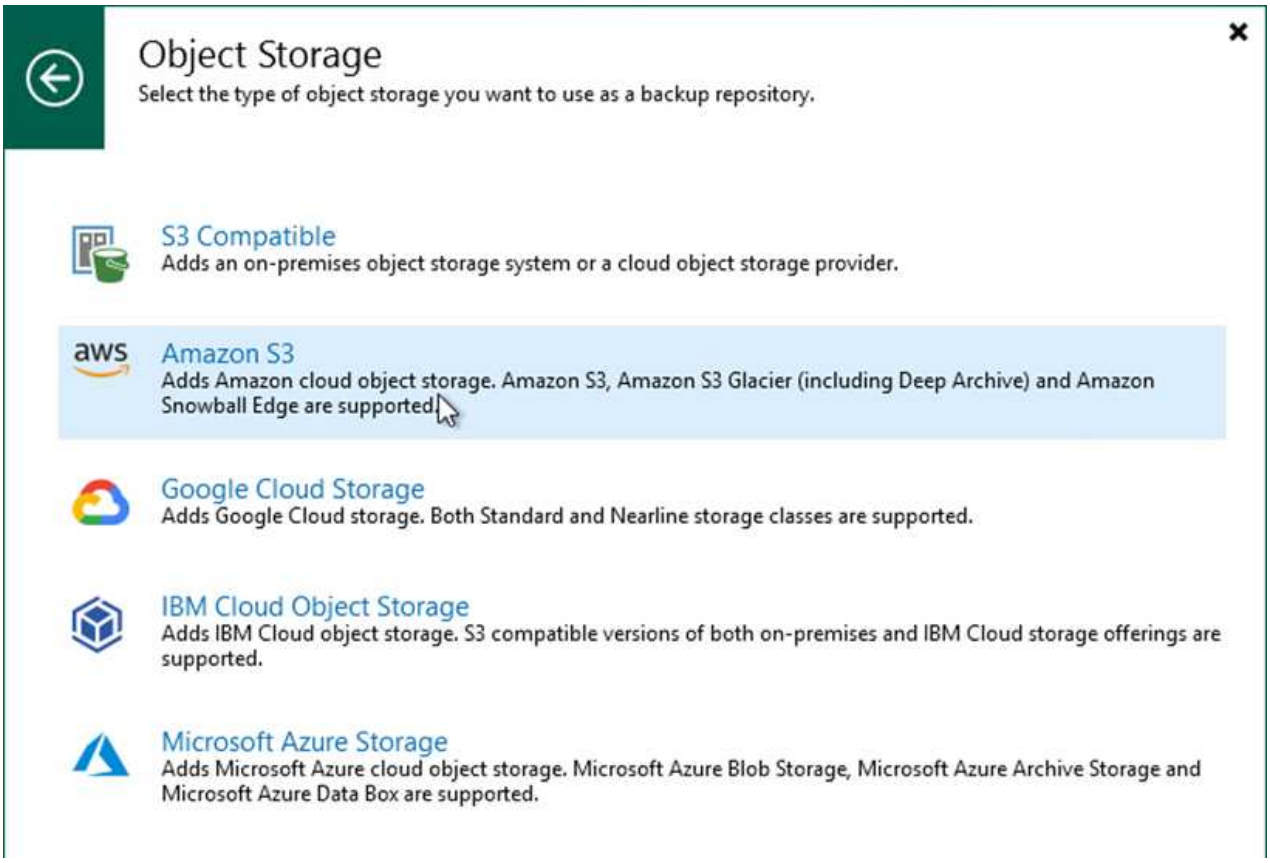
Dal server Veeam secondario, importare i backup dallo storage S3 e ripristinare le macchine virtuali SQL Server e Oracle nel cluster VMware Cloud.

Per importare i backup dall'oggetto S3 che faceva parte del repository di backup scale-out on-premise, attenersi alla seguente procedura:

1. Accedere a Backup Repository e fare clic su Add Repository (Aggiungi repository) nel menu in alto per avviare la procedura guidata Add Backup Repository (Aggiungi repository di backup). Nella prima pagina della procedura guidata, selezionare Object Storage come tipo di repository di backup.

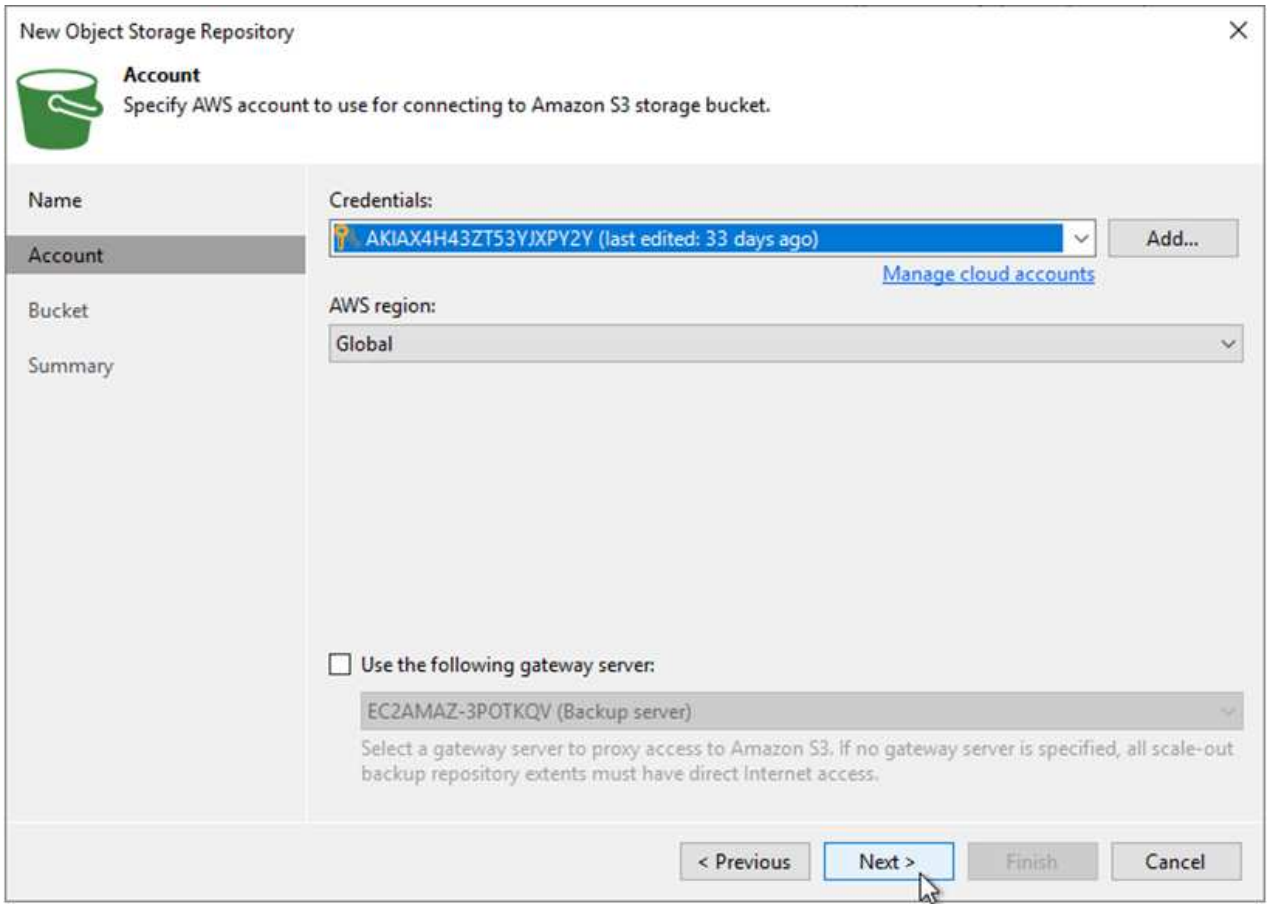


2. Selezionare Amazon S3 come tipo di storage a oggetti.

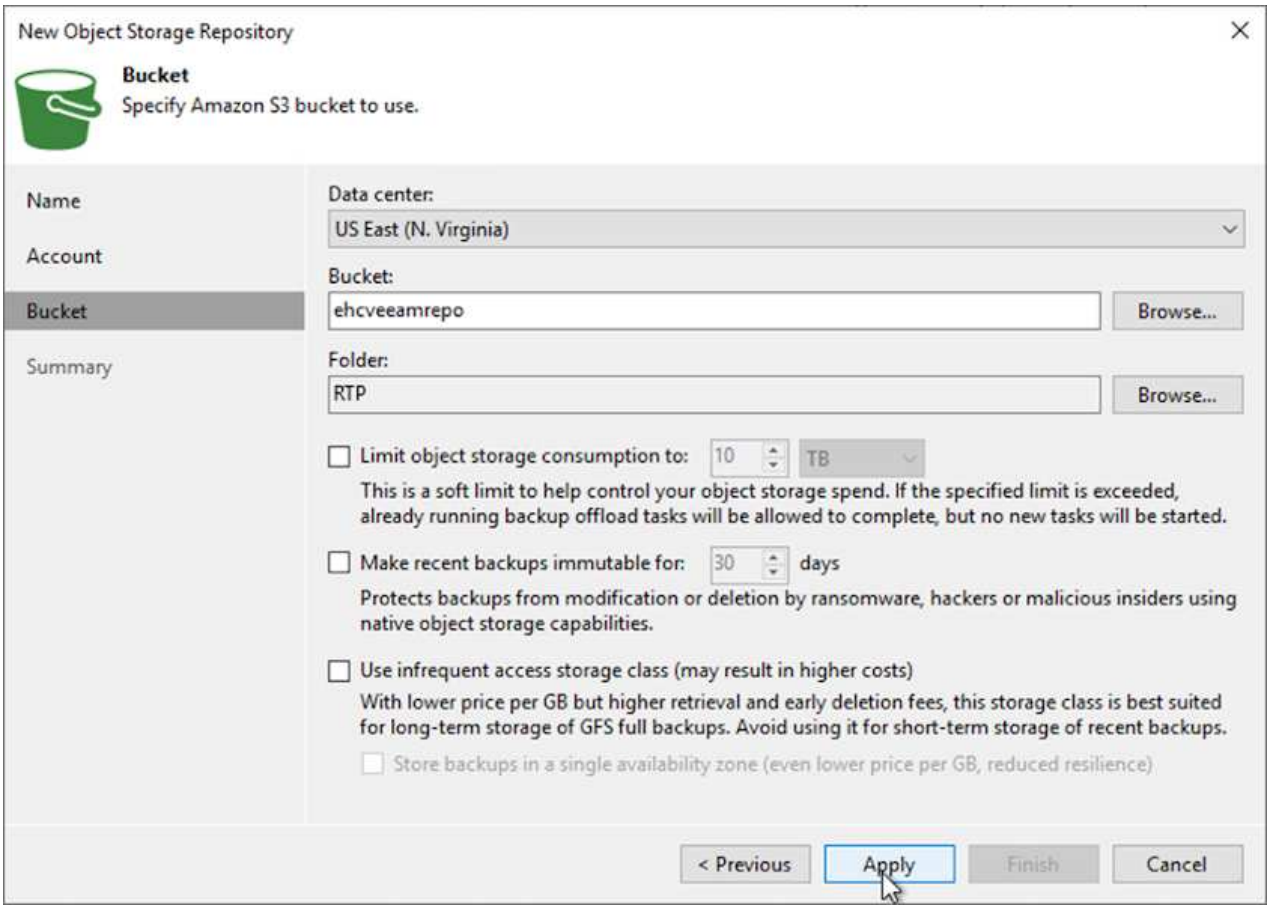


3. Dall'elenco di Amazon Cloud Storage Services, selezionare Amazon S3.

4. Selezionare le credenziali preinserite dall'elenco a discesa o aggiungere una nuova credenziale per accedere alla risorsa di storage cloud. Fare clic su Next (Avanti) per continuare.



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

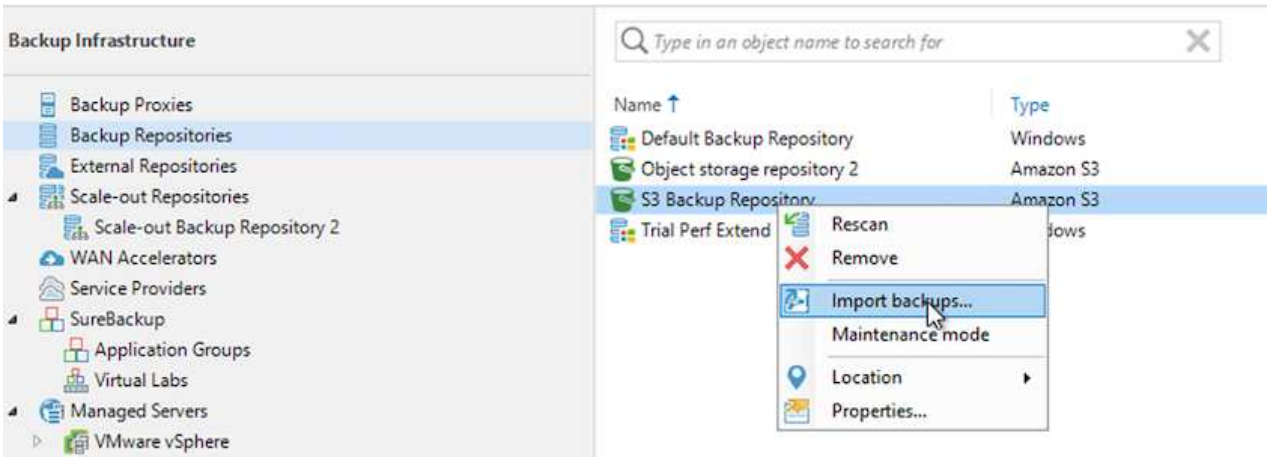


6. Infine, selezionare fine per completare il processo e aggiungere il repository.

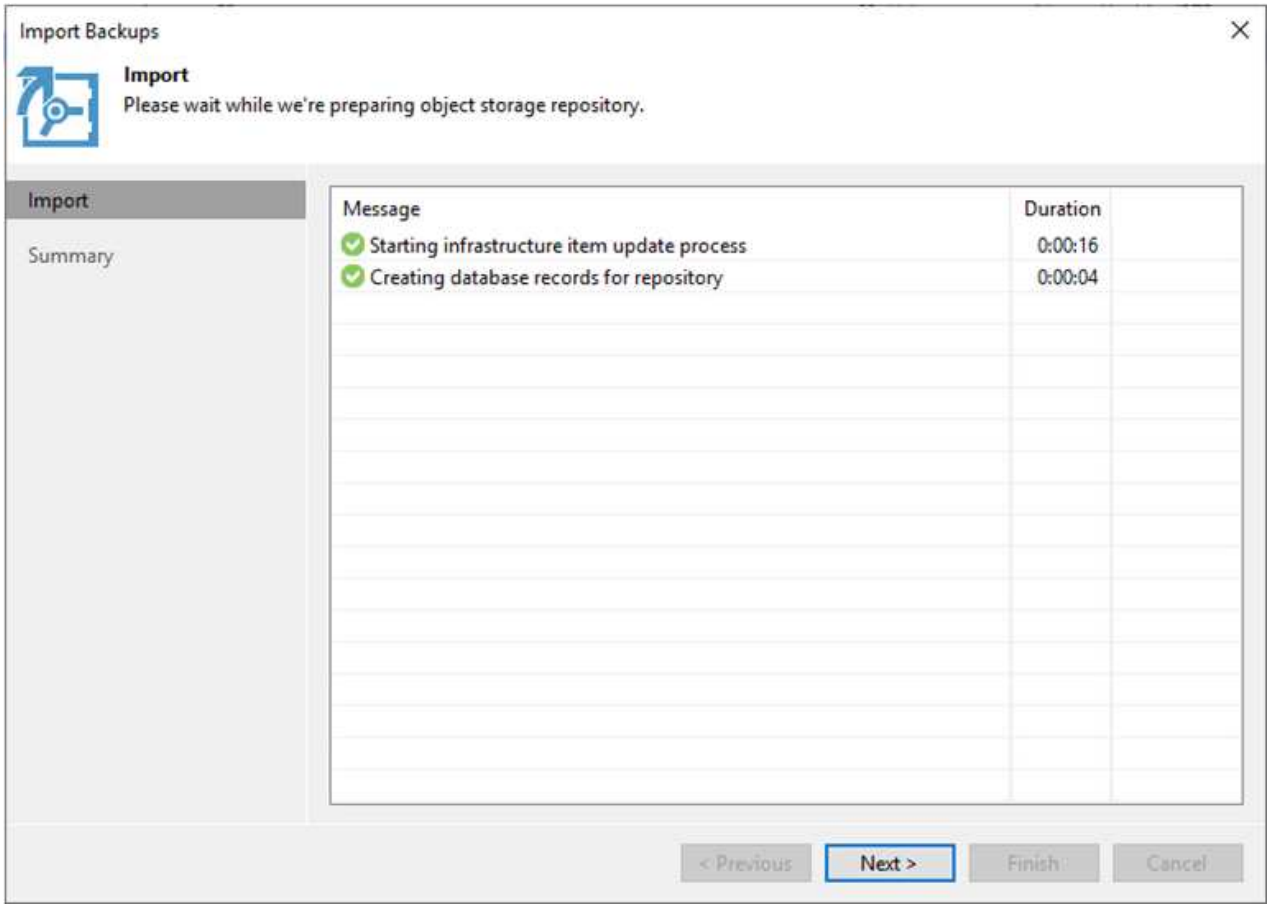
Importare backup dallo storage a oggetti S3

Per importare i backup dal repository S3 aggiunto nella sezione precedente, attenersi alla seguente procedura.

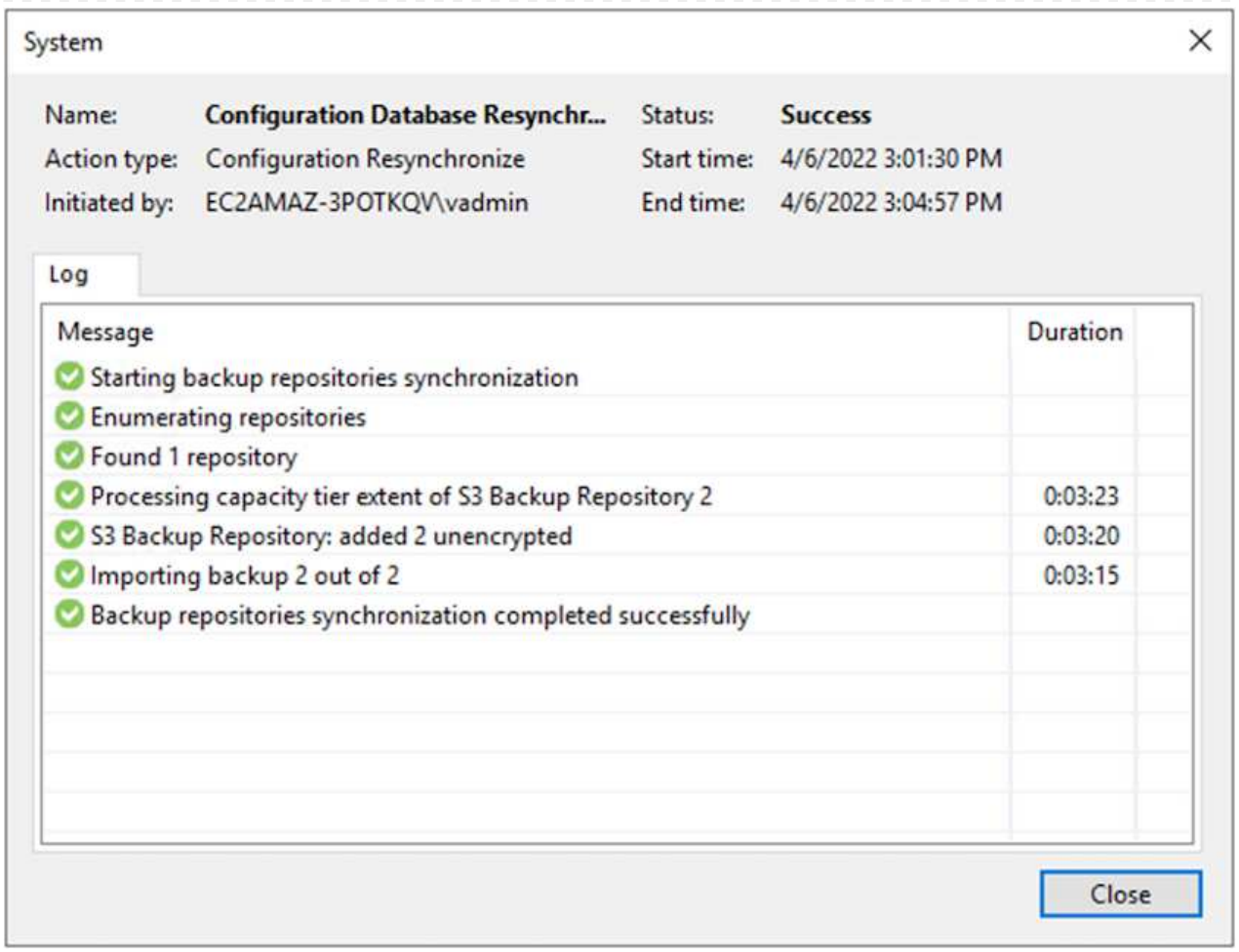
1. Dal repository di backup S3, selezionare Importa backup per avviare la procedura guidata di importazione dei backup.



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



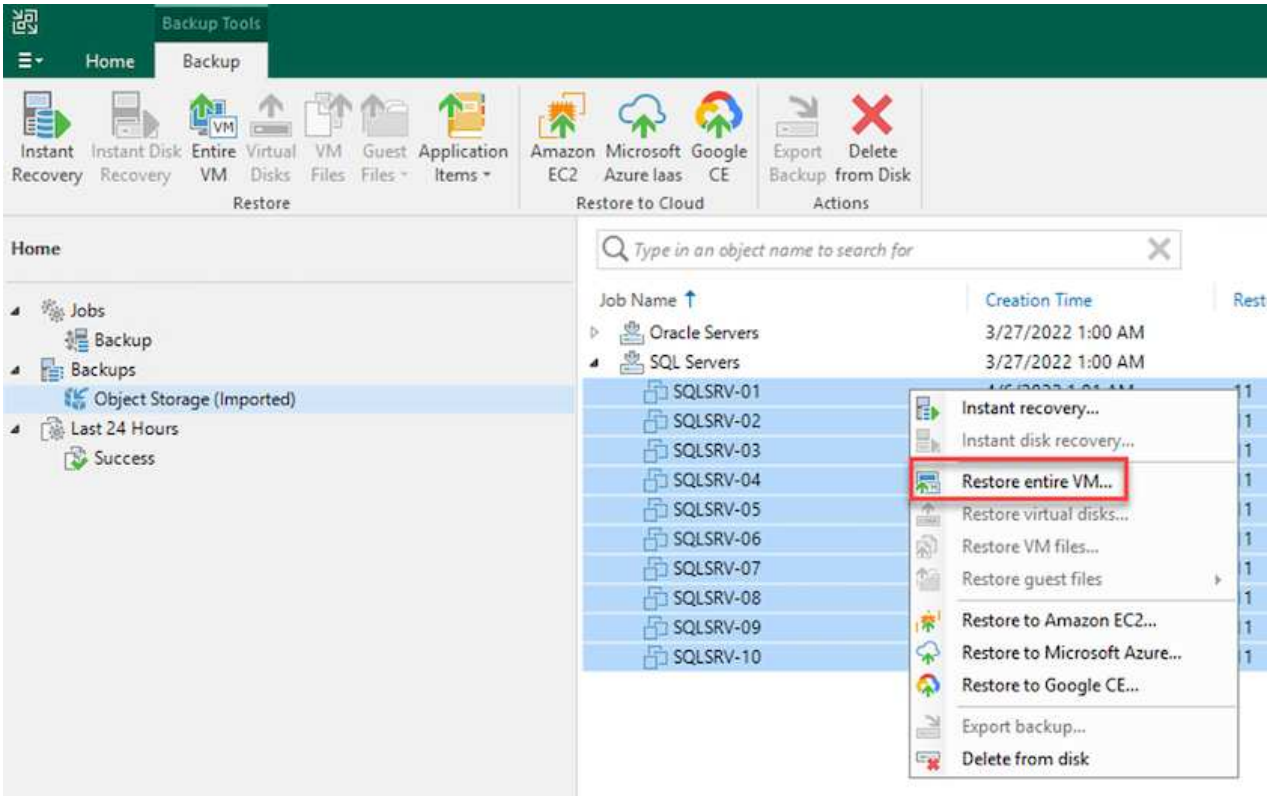
3. Una volta completata l'importazione, è possibile ripristinare le macchine virtuali nel cluster VMware Cloud.


System
Name: Configuration Database Resynchr...
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

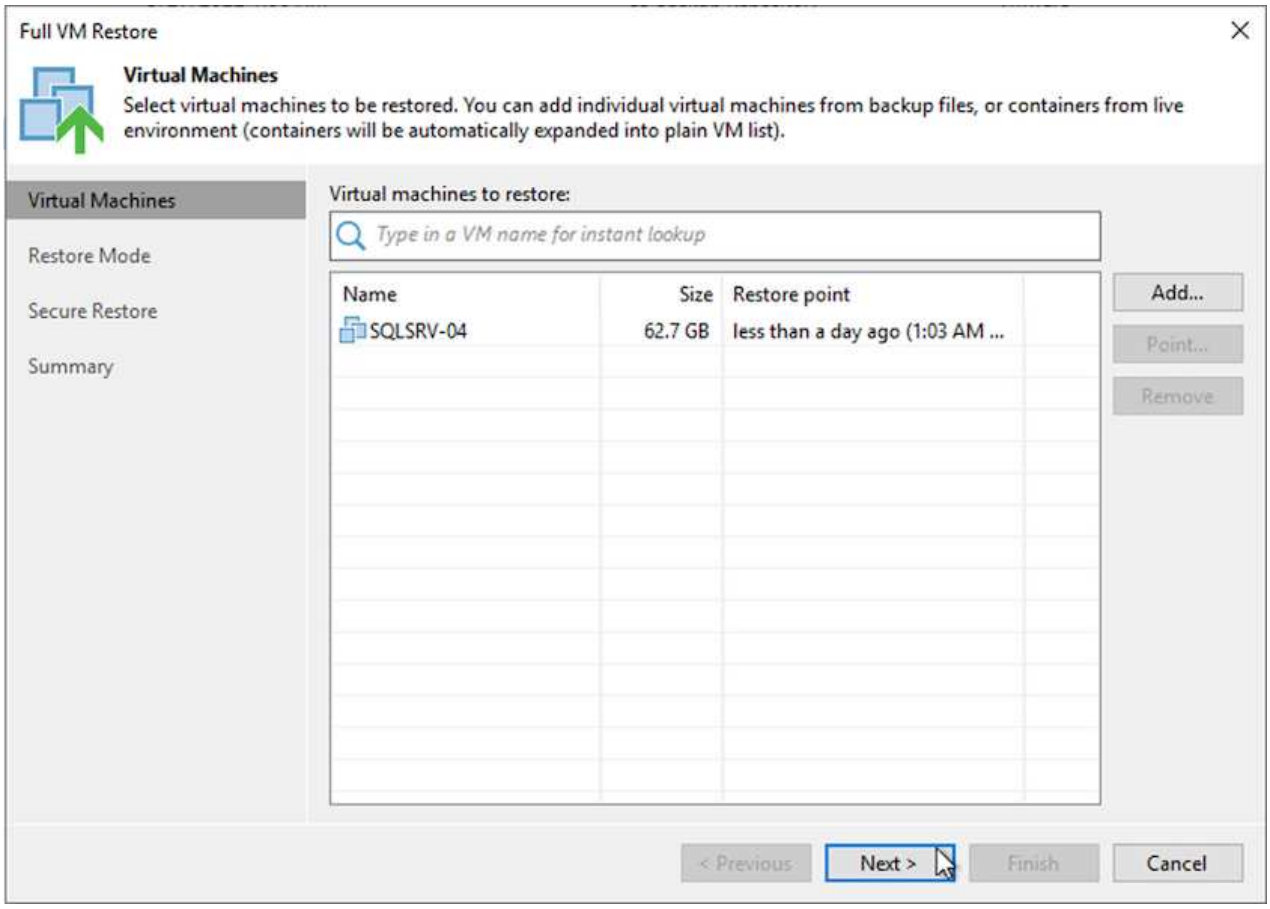
Ripristinare le macchine virtuali applicative con il ripristino completo di Veeam su VMware Cloud

Per ripristinare le macchine virtuali SQL e Oracle su VMware Cloud su cluster/dominio del carico di lavoro AWS, completare la seguente procedura.

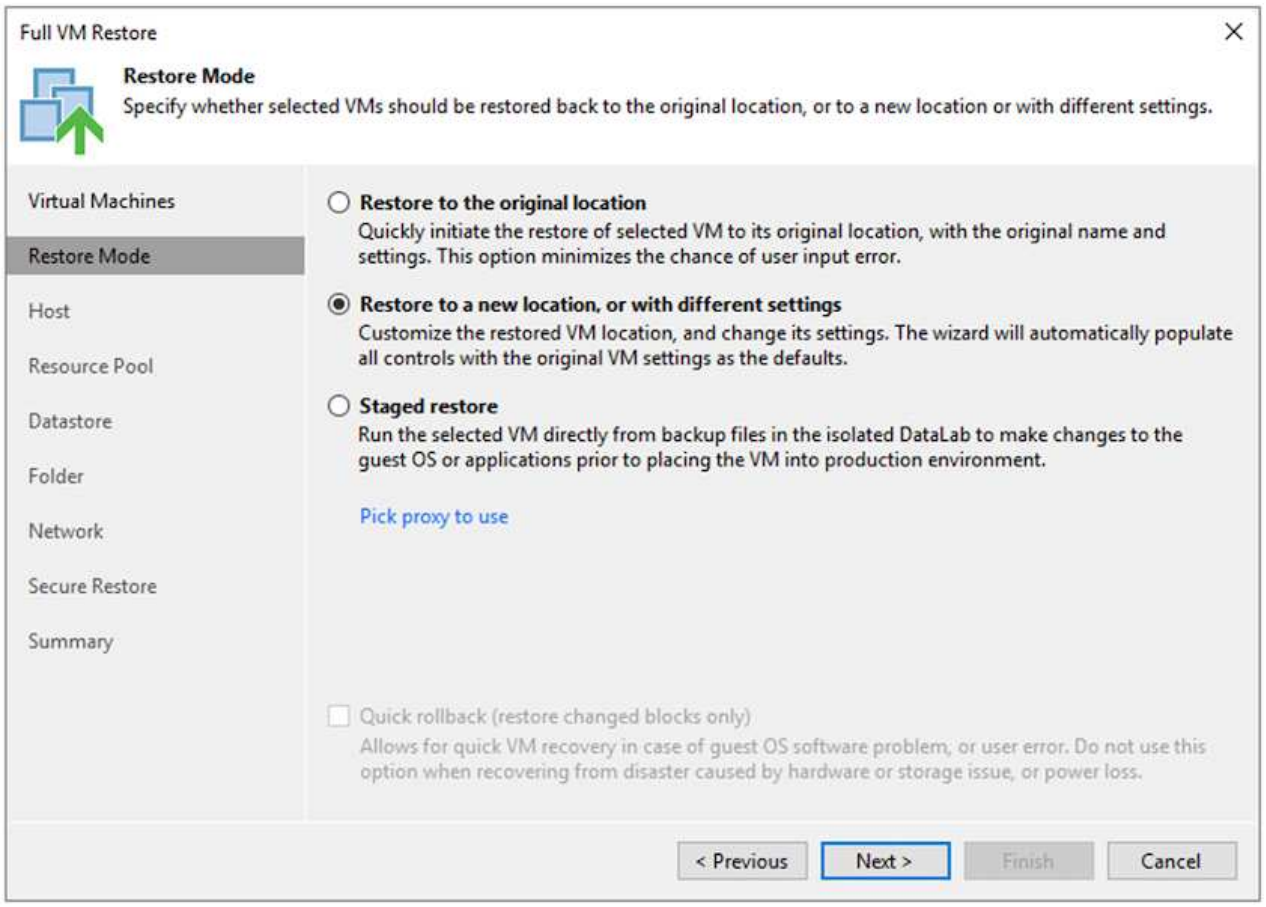
1. Dalla home page di Veeam, selezionare lo storage a oggetti contenente i backup importati, selezionare le macchine virtuali da ripristinare, quindi fare clic con il pulsante destro del mouse e selezionare Restore entire VM (Ripristina intera macchina virtuale).



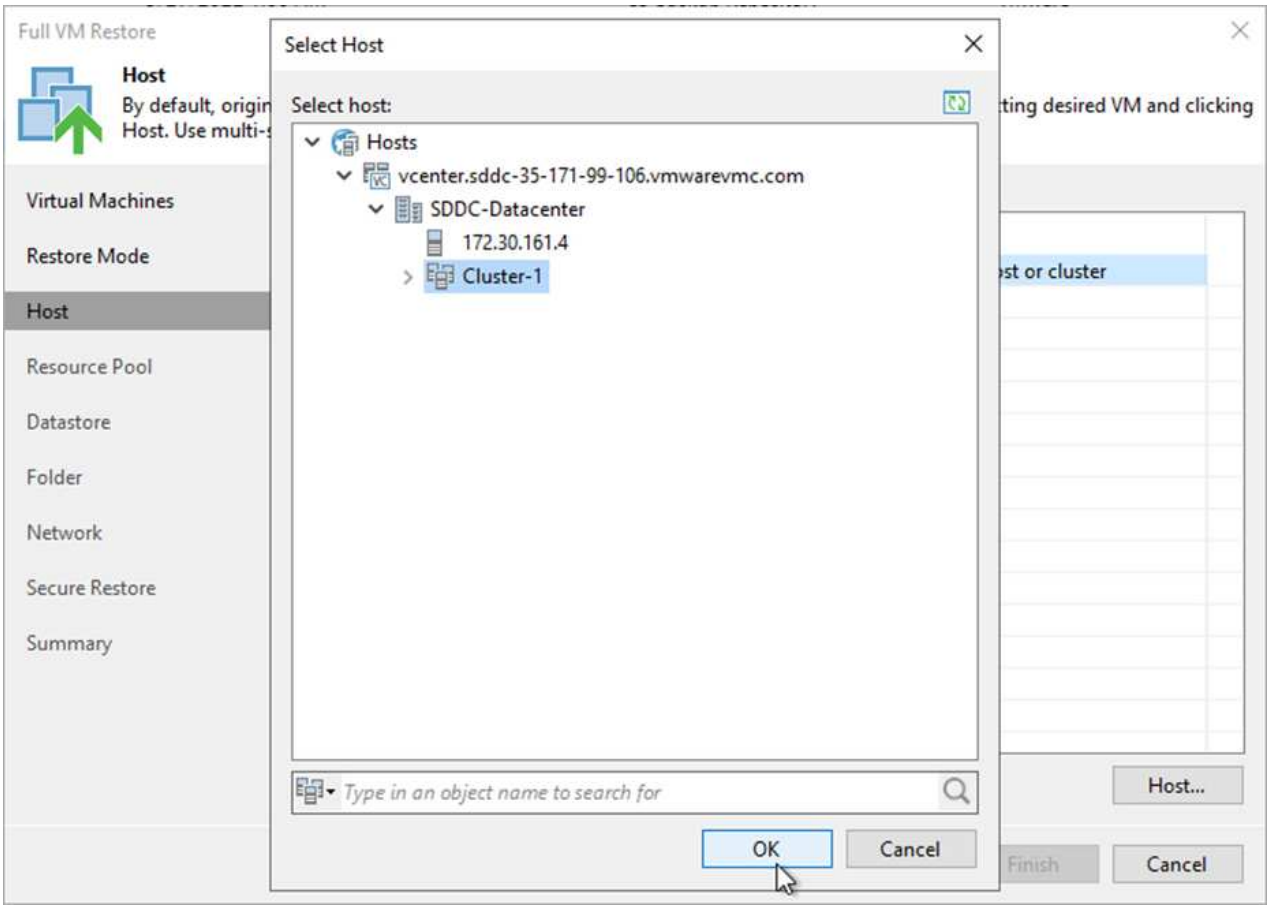
2. Nella prima pagina della procedura guidata di ripristino completo della macchina virtuale, modificare le macchine virtuali per il backup, se necessario, e selezionare Avanti.



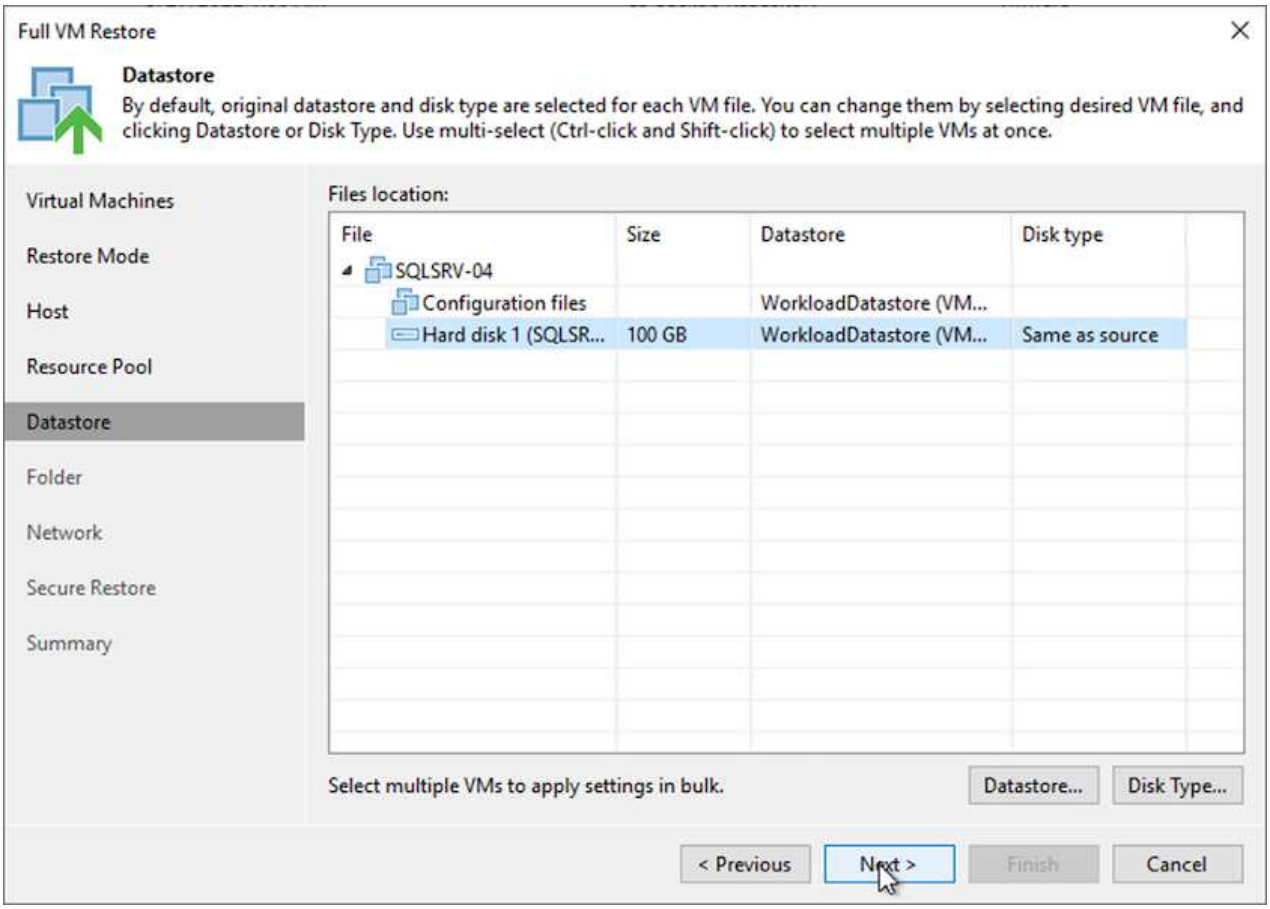
3. Nella pagina Restore Mode (modalità ripristino), selezionare Restore to a New Location (Ripristina in una nuova posizione) o with different Settings (con impostazioni diverse).



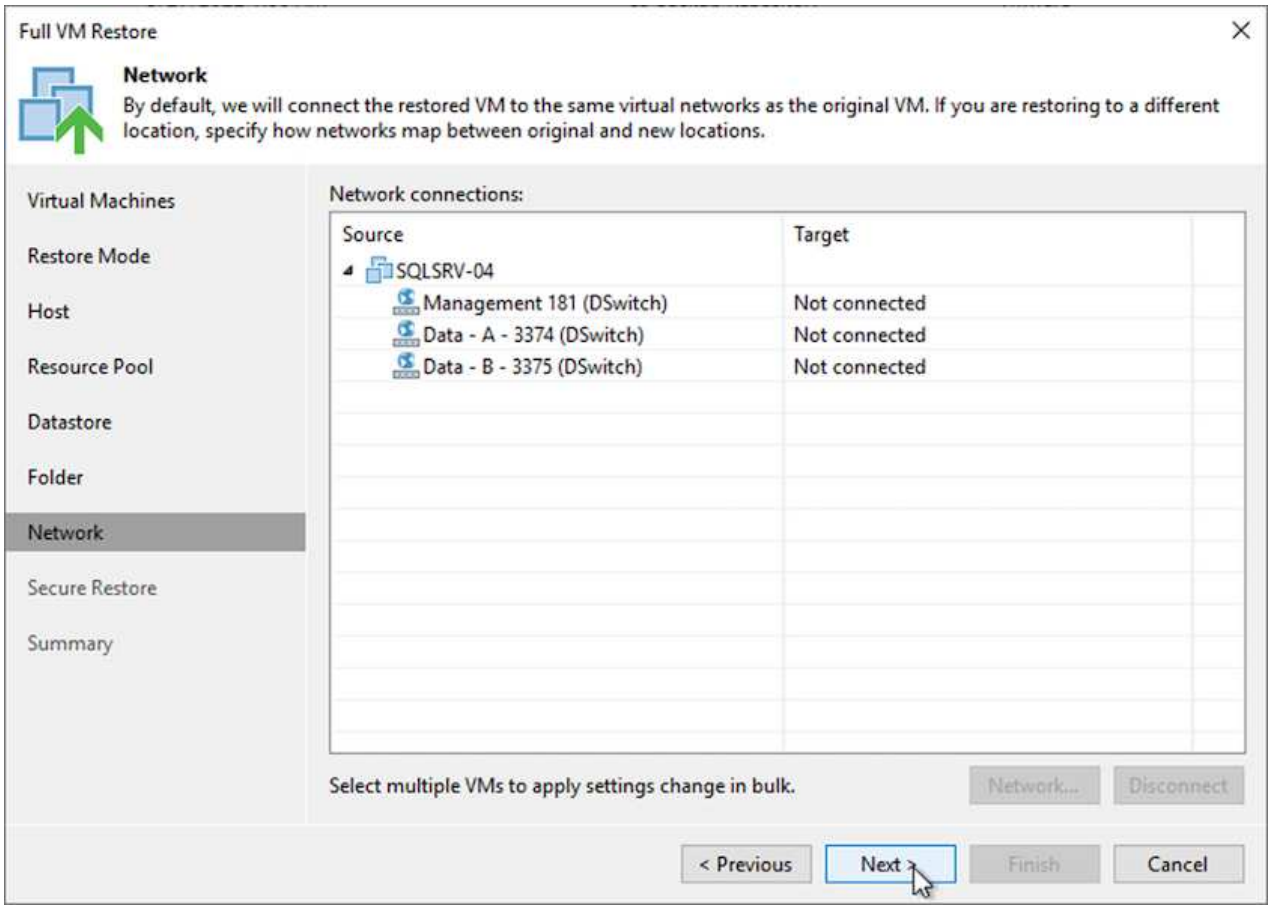
4. Nella pagina host, selezionare l'host o il cluster ESXi di destinazione su cui ripristinare la macchina virtuale.

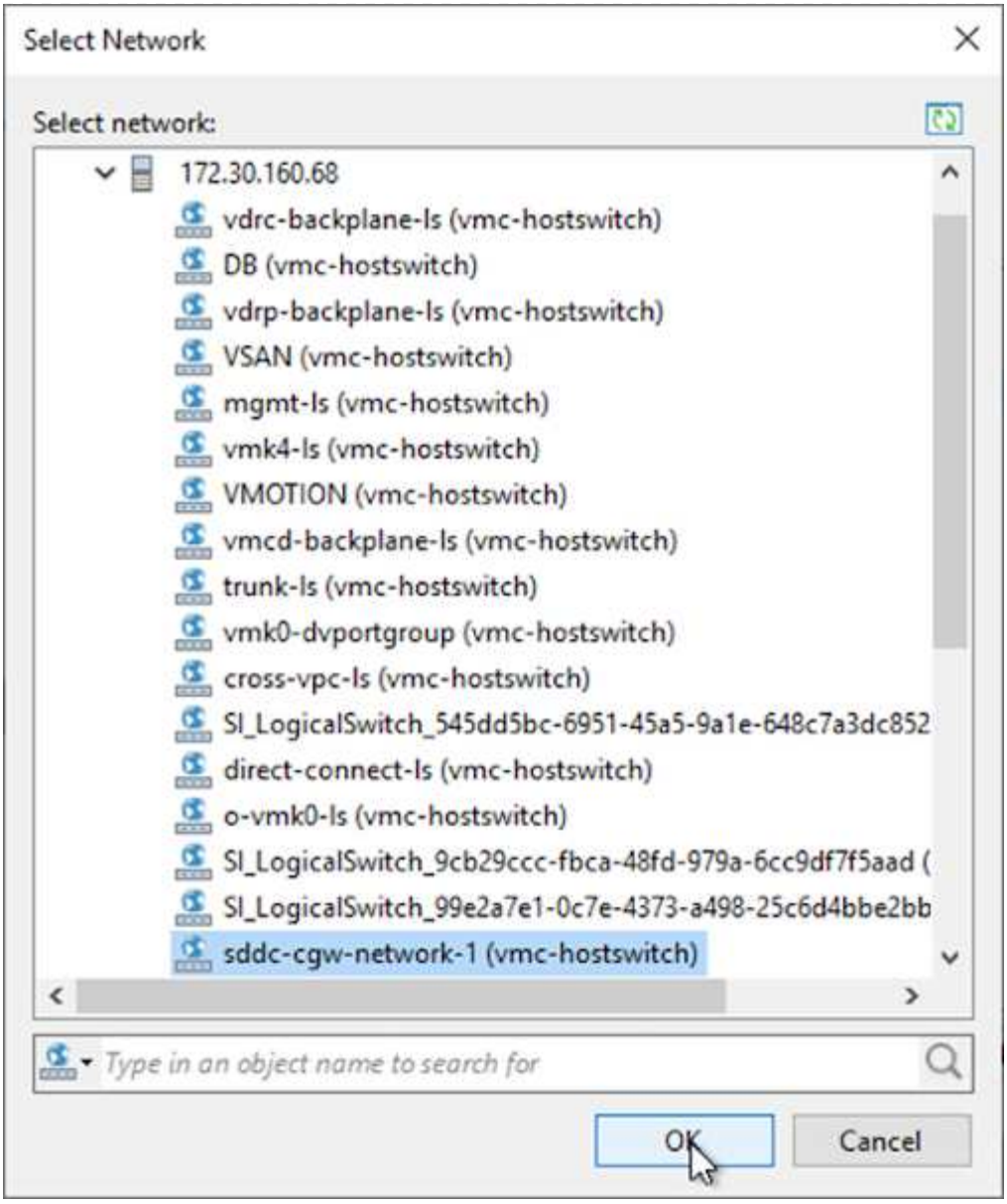


5. Nella pagina datastore, selezionare la posizione del datastore di destinazione per i file di configurazione e il disco rigido.



6. Nella pagina Network (rete), mappare le reti originali sulla macchina virtuale 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 macchina virtuale ripristinata alla ricerca di malware, esaminare la pagina di riepilogo e fare clic su Finish (fine) per avviare il ripristino.

Ripristinare i dati dell'applicazione SQL Server

Il seguente processo fornisce istruzioni su come ripristinare un SQL Server in VMware Cloud Services in AWS in caso di disastro che rende il sito on-premise inutilizzabile.

Si presuppone che i seguenti prerequisiti siano completi per continuare con le fasi di ripristino:

1. La macchina virtuale Windows Server è stata ripristinata nel VMware Cloud SDDC utilizzando il ripristino completo di Veeam.
2. È stato stabilito un server SnapCenter secondario e il ripristino e la configurazione del database SnapCenter sono stati completati seguendo la procedura illustrata nella sezione "Riepilogo del processo di backup e ripristino di SnapCenter."

VM: Configurazione post-ripristino per SQL Server VM

Una volta completato il ripristino della macchina virtuale, è necessario configurare la rete e altri elementi in preparazione per il rispristino della macchina virtuale host in SnapCenter.

1. Assegnare nuovi indirizzi IP per Management e iSCSI o NFS.
2. Unire 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 SMCore, Plug-in per Windows e Plug-in per SnapCenter Server.

> Per riscoprire automaticamente le macchine virtuali ripristinate in SnapCenter, l'FQDN deve essere identico alla macchina virtuale originariamente aggiunta a SnapCenter on-premise.

Configurare lo storage FSX per il ripristino di SQL Server

Per eseguire il processo di ripristino del disaster recovery per una macchina virtuale SQL Server, è necessario interrompere la relazione SnapMirror esistente dal cluster FSX e concedere l'accesso al volume. A tale scopo, attenersi alla seguente procedura.

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

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

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

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

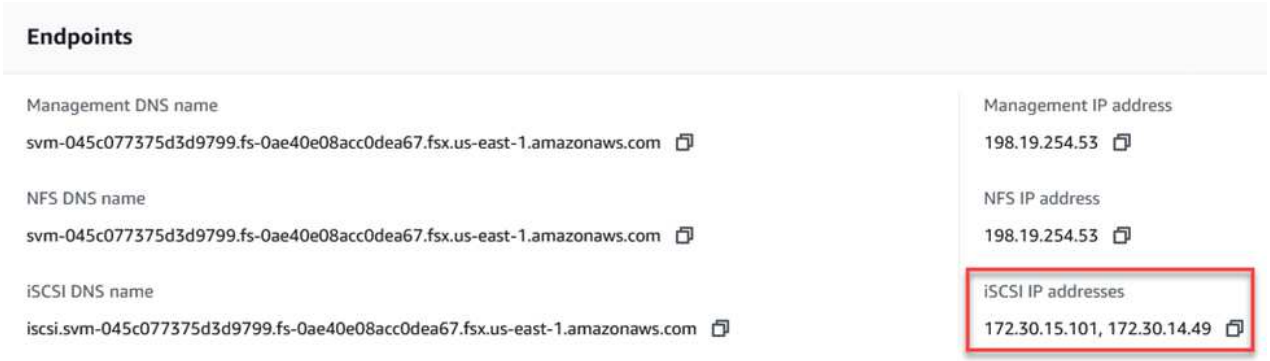
3. Infine, mappare le LUN al gruppo iniziatore appena creato:

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

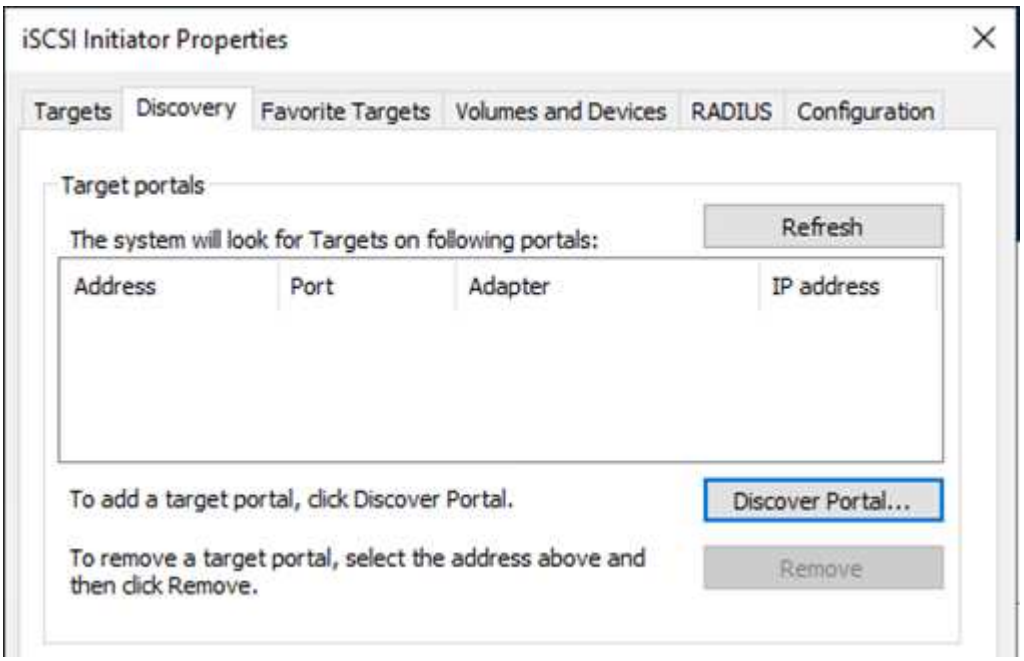
4. Per trovare il nome del percorso, eseguire `lun show` comando.

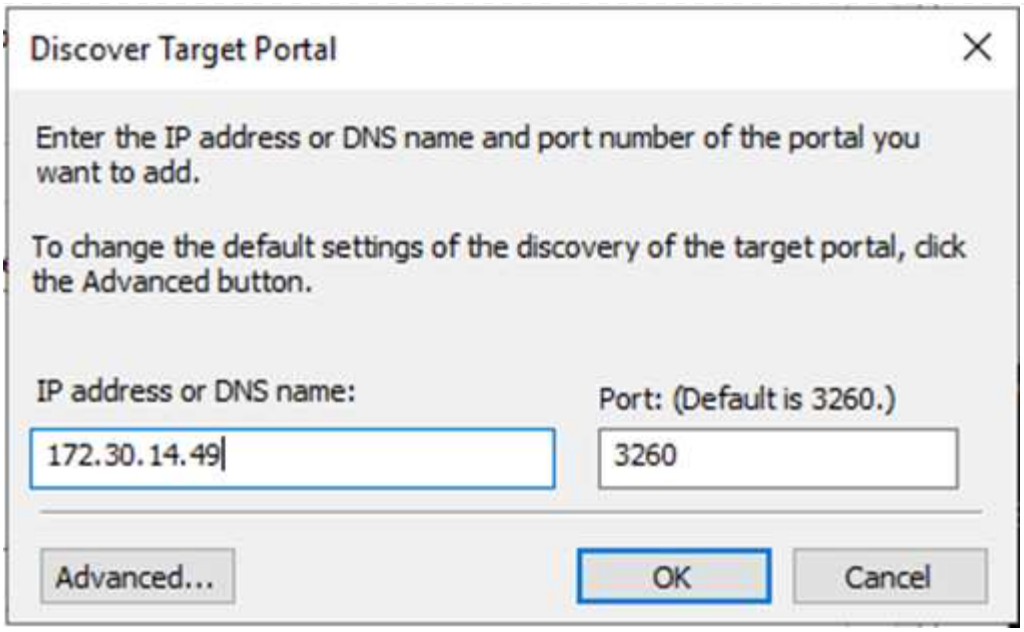
Configurare la macchina virtuale Windows per l'accesso iSCSI e rilevare i file system

1. Da SQL Server VM, configurare l'adattatore di rete iSCSI per comunicare sul gruppo di porte VMware stabilito con la connettività alle interfacce di destinazione iSCSI sull'istanza FSX.
2. Aprire l'utility iSCSI Initiator Properties (Proprietà iSCSI Initiator) e cancellare le vecchie impostazioni di connettività nelle schede Discovery (rilevamento), Favorite Targets (destinazioni preferite) e Targets (destinazioni).
3. Individuare gli indirizzi IP per l'accesso all'interfaccia logica iSCSI sull'istanza/cluster FSX. Questa opzione si trova nella console AWS in Amazon FSX > ONTAP > Storage Virtual Machines (Impostazioni > macchine virtuali di storage).

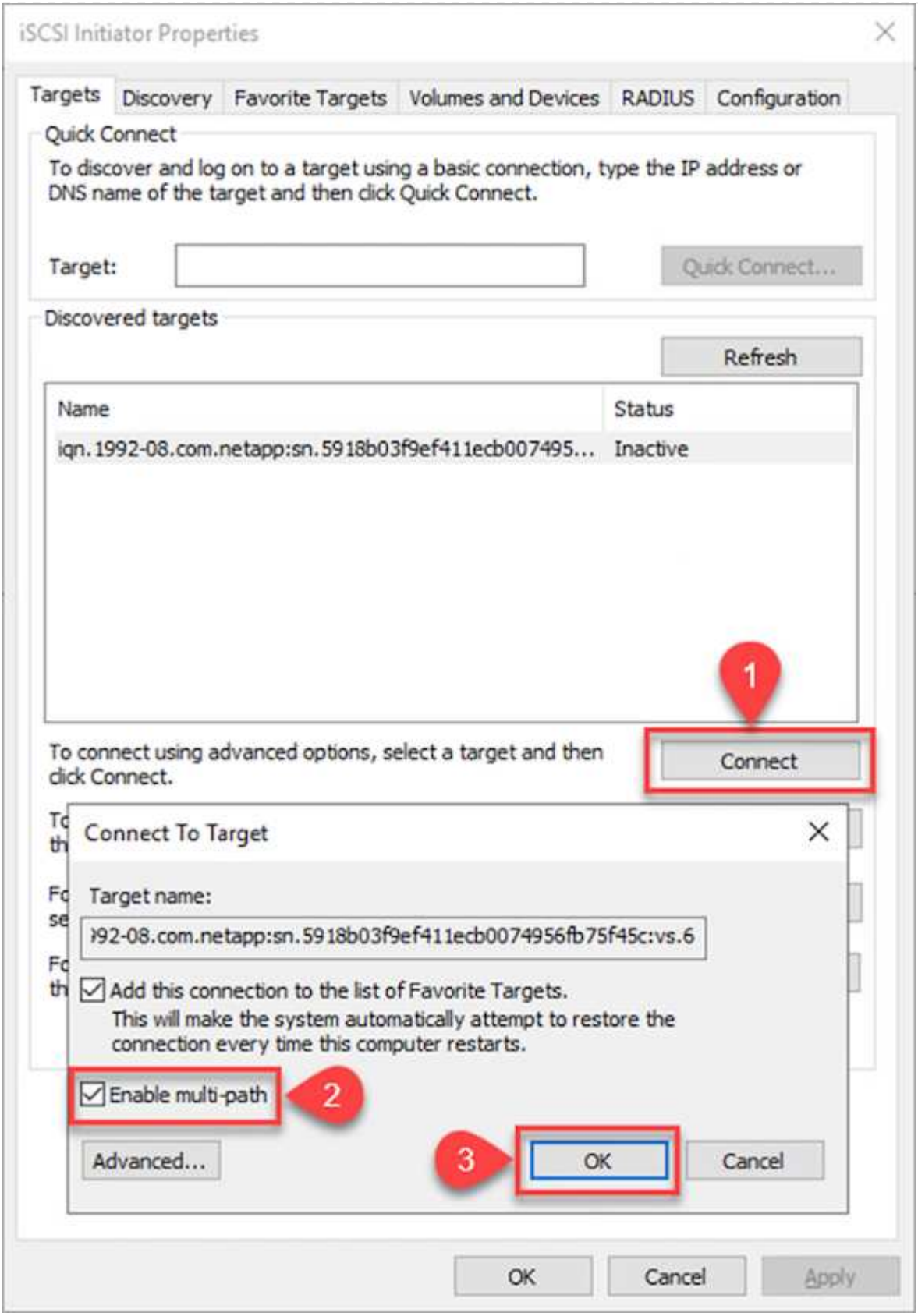


4. Dalla scheda Discovery (rilevamento), fare clic su Discover Portal (Scopri portale) e inserire gli indirizzi IP per le destinazioni iSCSI FSX.

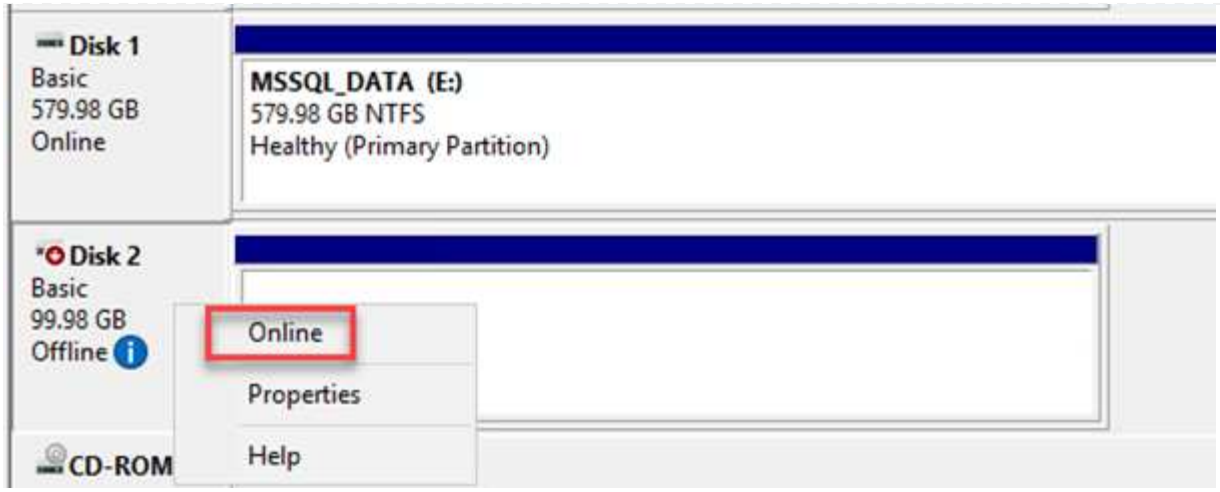




5. Nella scheda Target, fare clic su Connect (Connetti), selezionare Enable Multi-Path (attiva percorso multiplo) se appropriato per la configurazione, quindi fare clic su OK per connettersi alla destinazione.

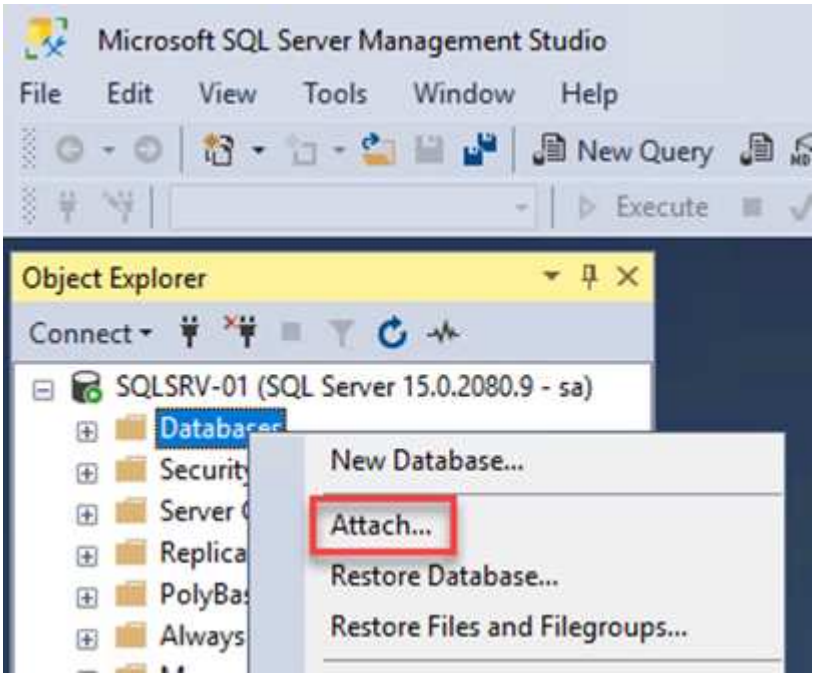


6. Aprire l'utility Gestione computer e portare i dischi in linea. Verificare che conservino le stesse lettere di unità in precedenza.

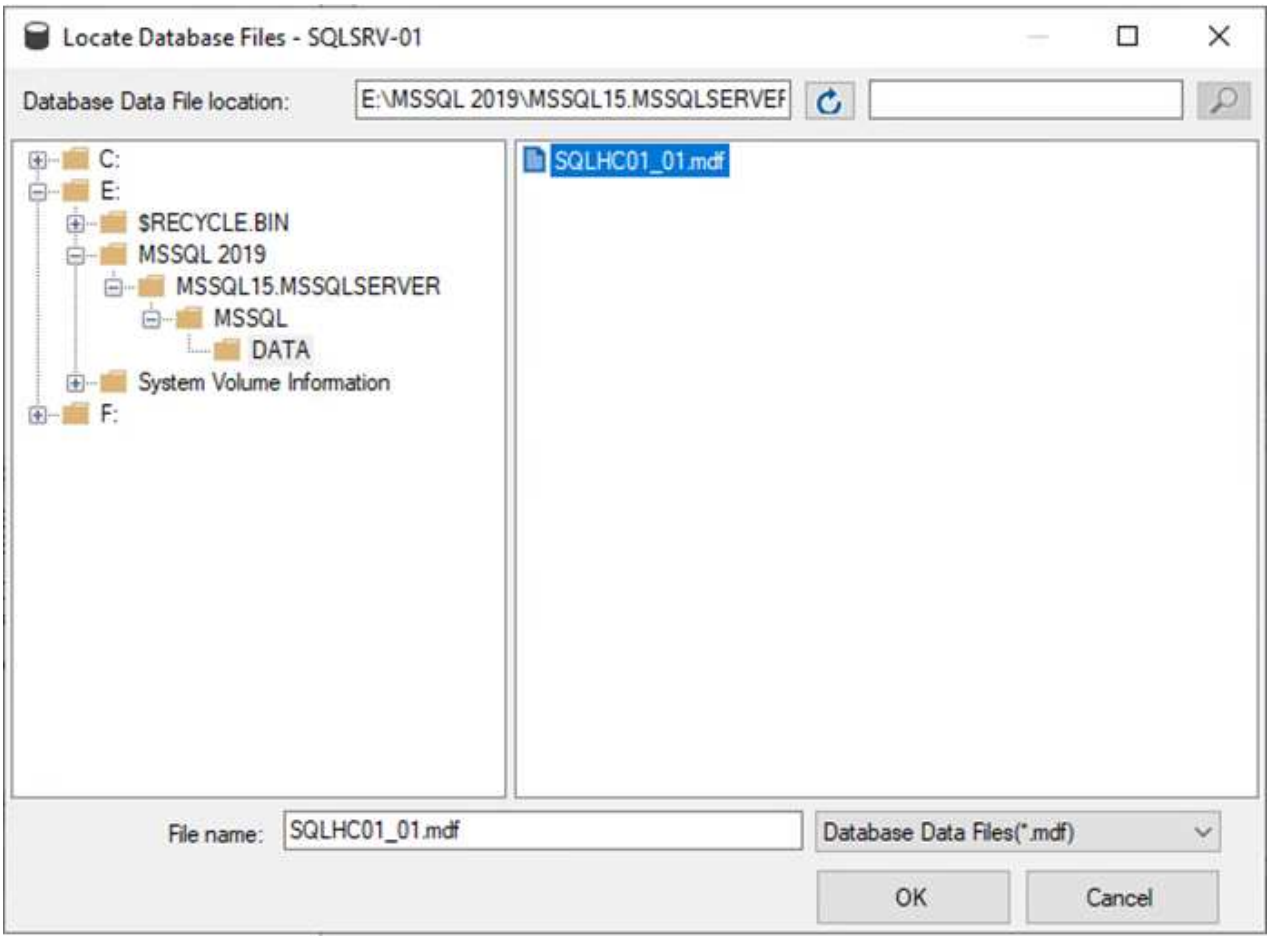

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Collegare i database di SQL Server

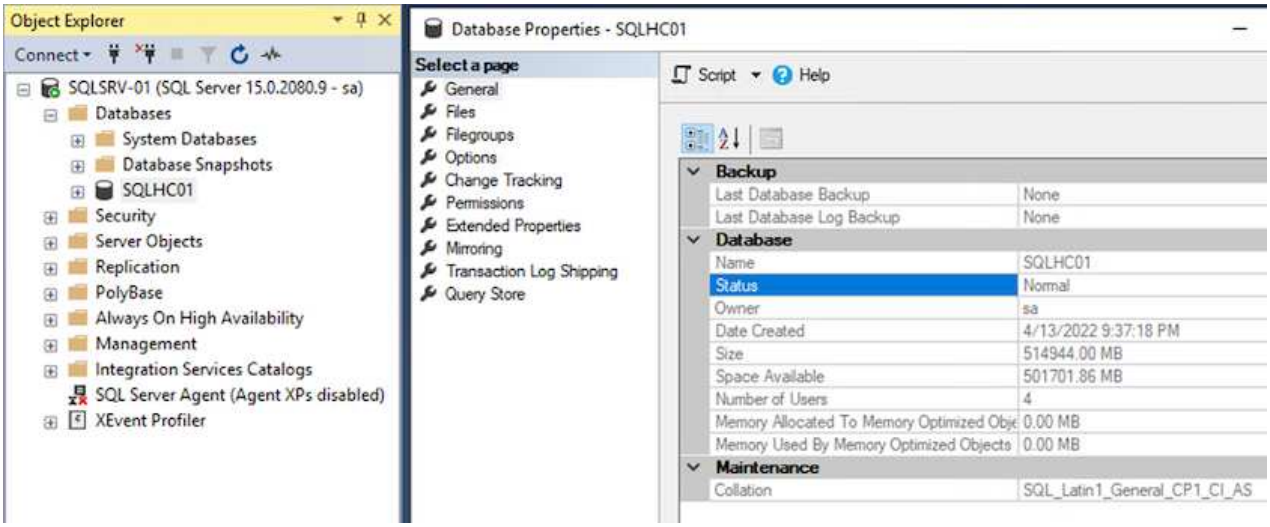
1. Da SQL Server VM, aprire Microsoft SQL Server Management Studio e selezionare Allega per avviare il processo di connessione al database.



2. Fare clic su Add (Aggiungi) e accedere alla cartella contenente il file di database primario di SQL Server, selezionarlo e fare clic su OK.



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

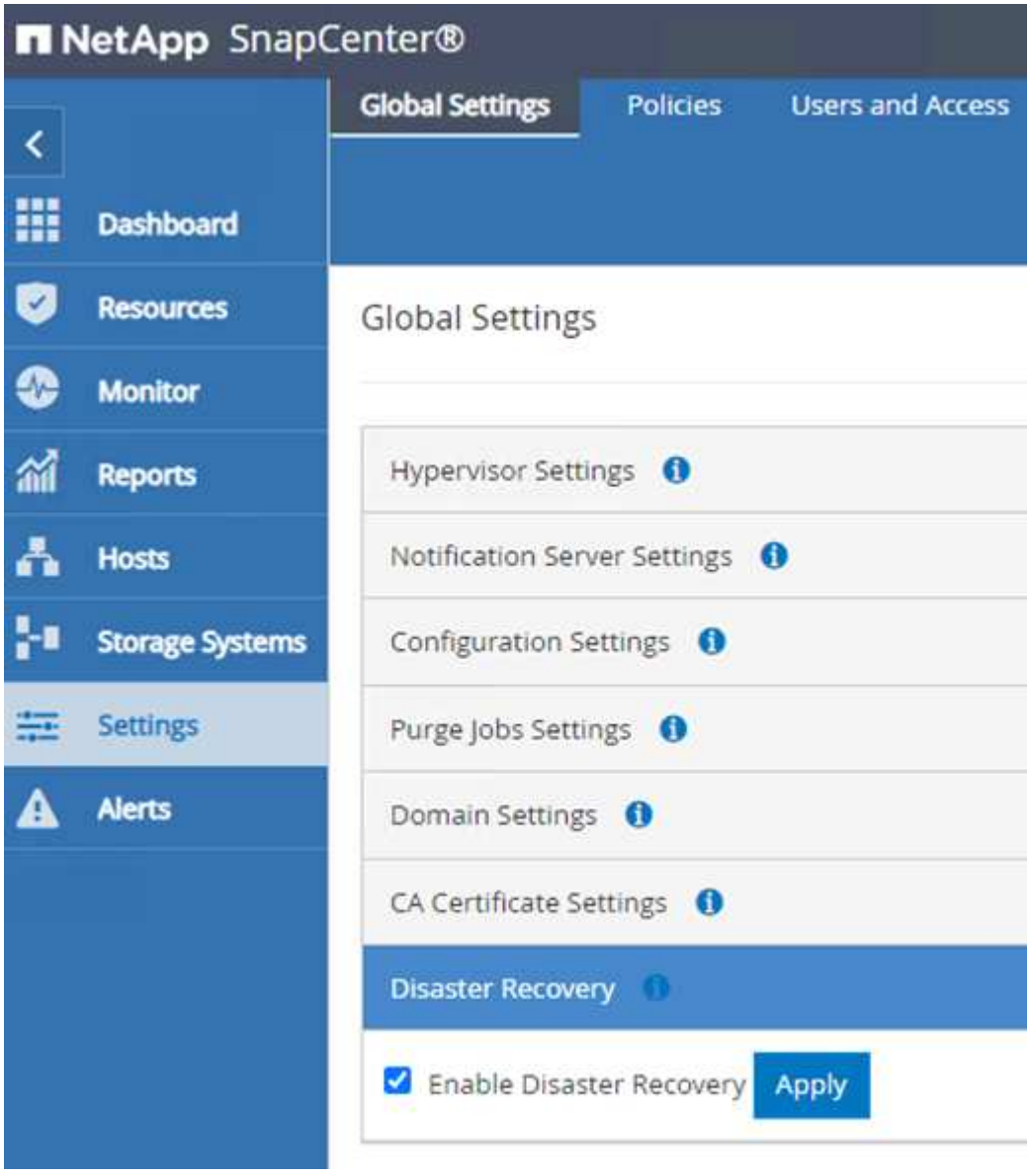


Confermare la comunicazione SnapCenter con il plug-in di SQL Server

Una volta ripristinato lo stato precedente, il database SnapCenter rileva automaticamente gli host di SQL Server. Affinché questo funzioni correttamente, tenere presente i seguenti prerequisiti:

- SnapCenter deve essere impostato sulla modalità di disaster recovery. Questa operazione può essere eseguita tramite l'API Swagger o in Impostazioni globali in Disaster Recovery.
- L'FQDN di SQL Server deve essere identico all'istanza in esecuzione nel data center on-premise.
- La relazione SnapMirror originale deve essere interrotta.
- Le LUN contenenti il database devono essere montate sull'istanza di SQL Server e sul database allegato.

Per verificare che SnapCenter sia in modalità di disaster recovery, accedere a Impostazioni dal client Web di SnapCenter. Accedere alla scheda Global Settings (Impostazioni globali) e fare clic su Disaster Recovery (Ripristino di emergenza). Assicurarsi che la casella di controllo Enable Disaster Recovery (attiva Disaster Recovery) sia attivata.



Ripristinare i dati delle applicazioni Oracle

Il seguente processo fornisce istruzioni su come ripristinare i dati delle applicazioni Oracle in VMware Cloud Services in AWS in caso di disastro che rende il sito on-premise inutilizzabile.

Completare i seguenti prerequisiti per continuare con la procedura di ripristino:

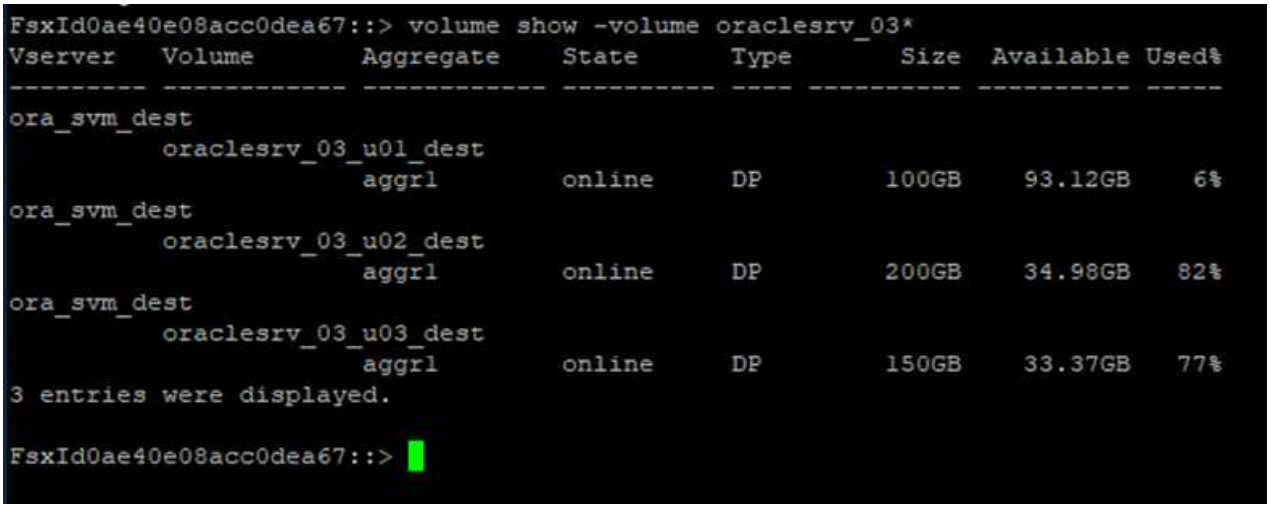
1. La macchina virtuale del server Oracle Linux è stata ripristinata su VMware Cloud SDDC utilizzando Veeam Full Restore.
2. È stato creato un server SnapCenter secondario e il database SnapCenter e i file di configurazione sono stati ripristinati seguendo la procedura descritta in questa sezione "Riepilogo del processo di backup e ripristino di SnapCenter."

Configurazione di FSX per il ripristino di Oracle - interruzione della relazione SnapMirror

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

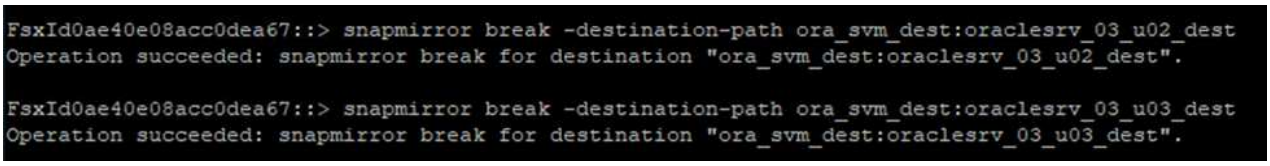
1. Dopo aver effettuato l'accesso alla CLI FSX, eseguire il seguente comando per visualizzare i volumi filtrati dal nome corretto.

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

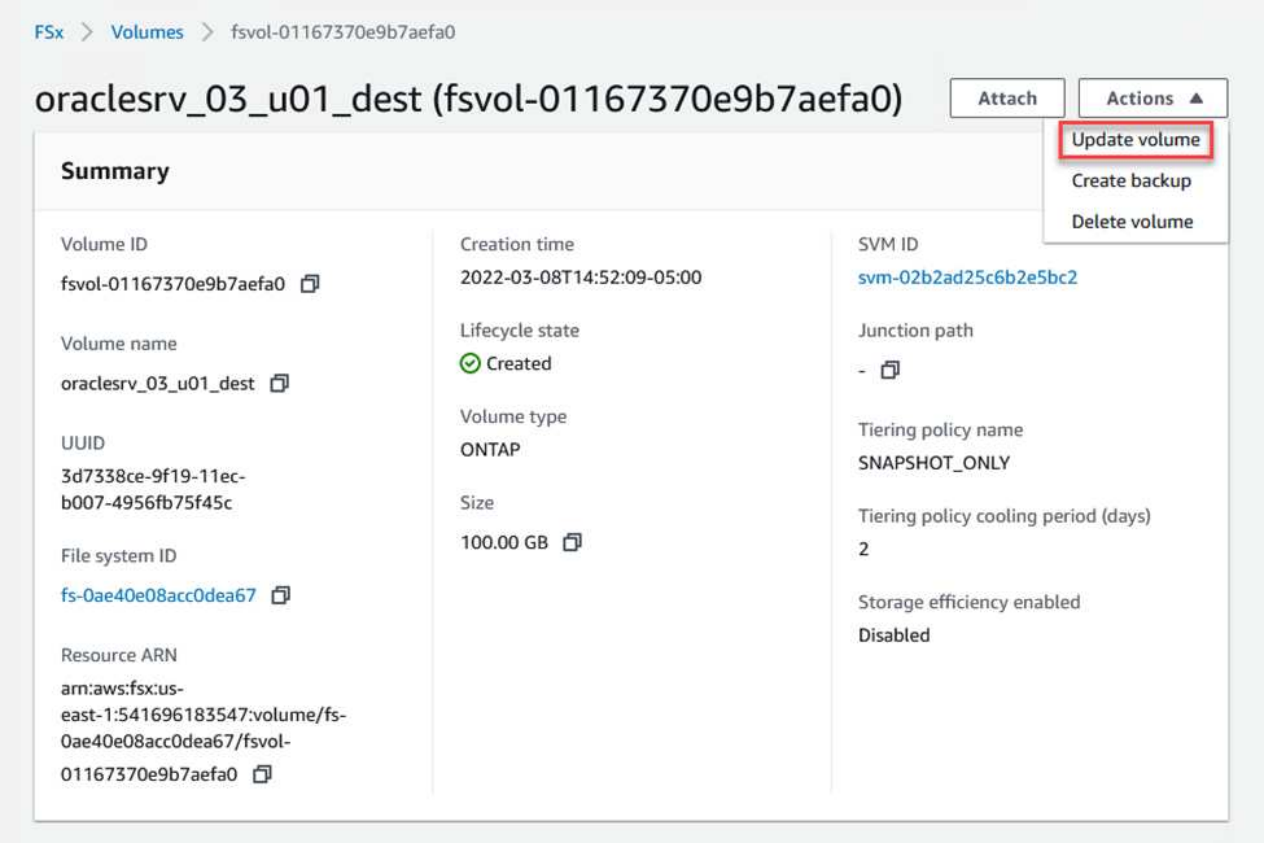


2. Eseguire il seguente comando per interrompere le relazioni SnapMirror esistenti.

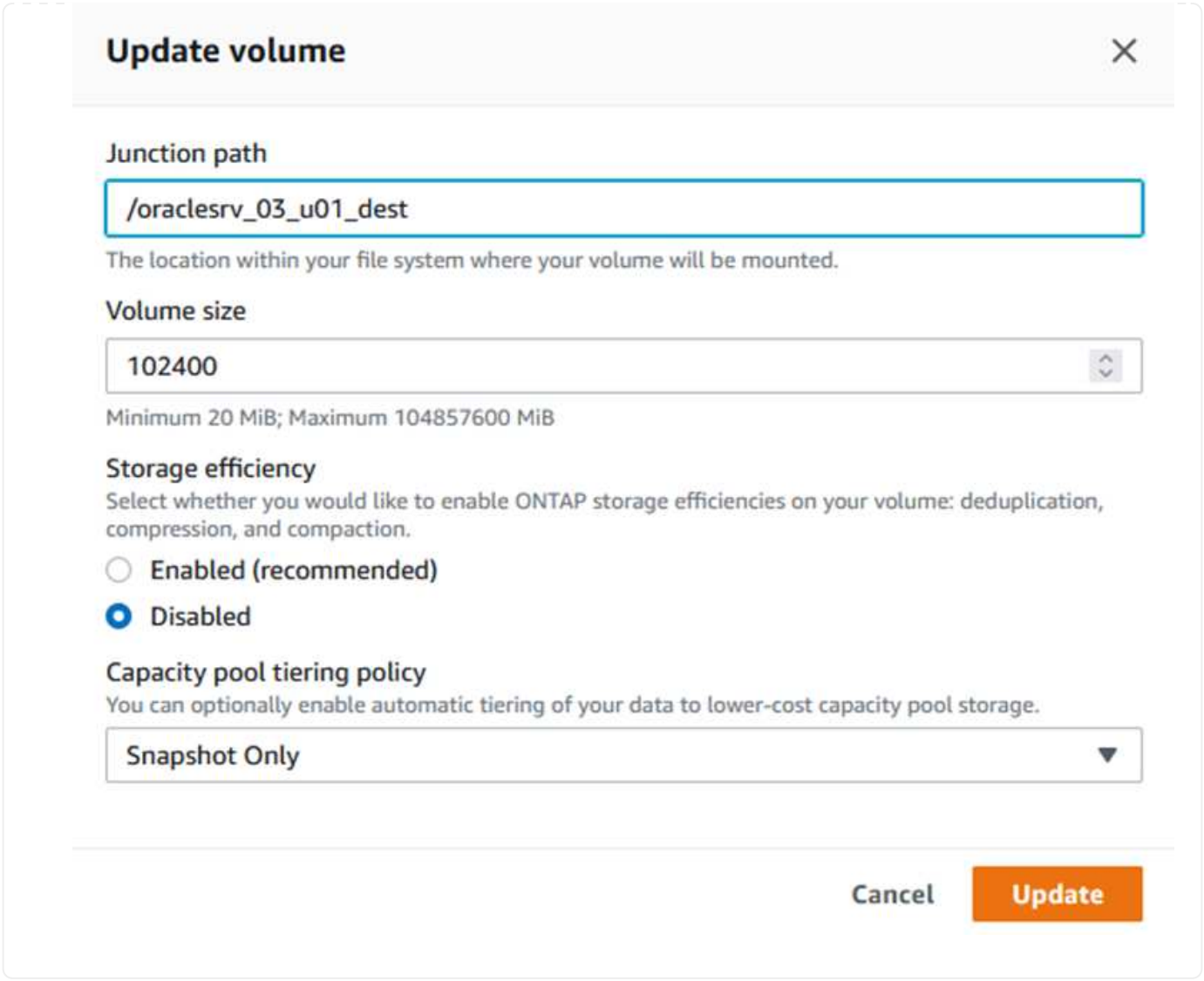
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```



3. Aggiornare il percorso di giunzione nel client Web Amazon FSX:



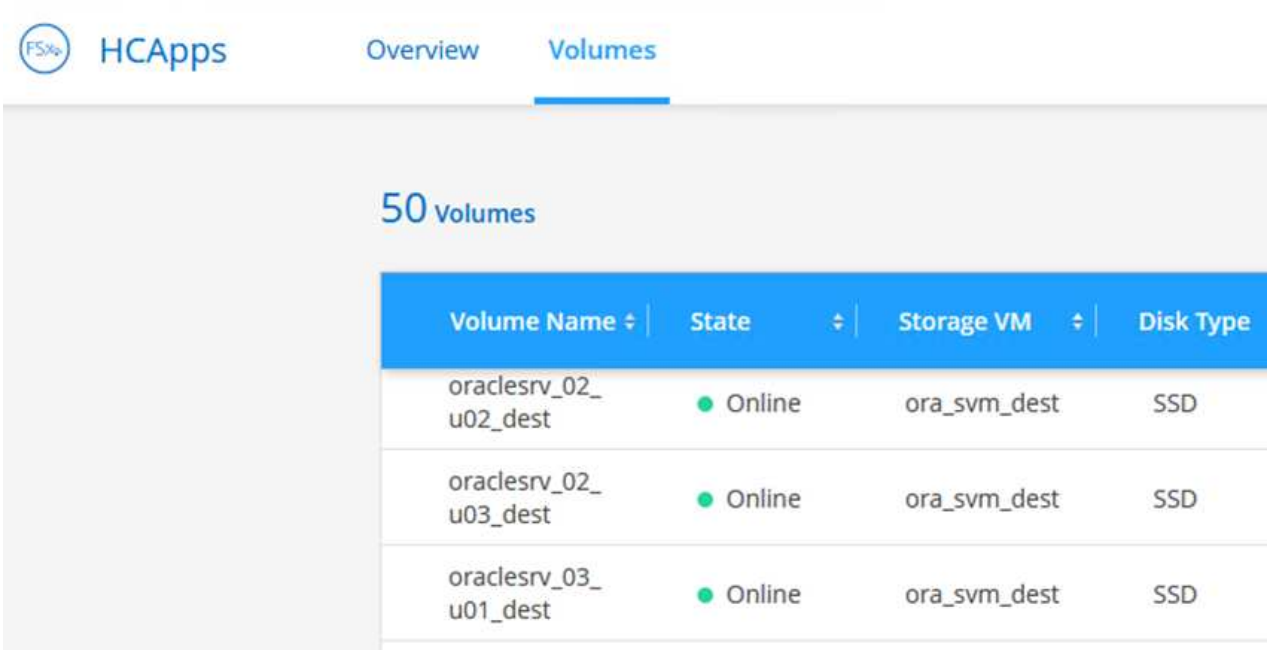
4. Aggiungere il nome del percorso di giunzione e fare clic su Update (Aggiorna). Specificare questo percorso di giunzione quando si monta il volume NFS dal server Oracle.


Update volume
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

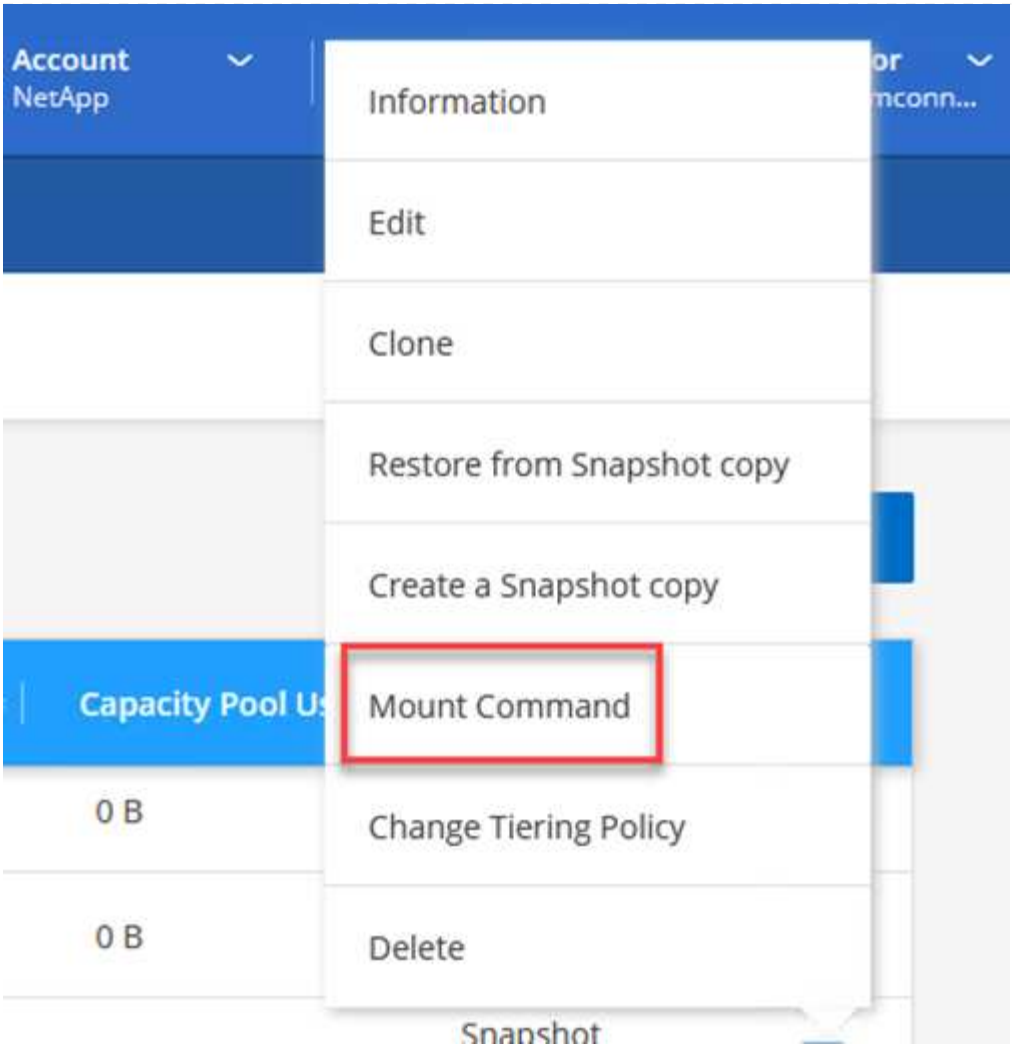
Montare volumi NFS su Oracle Server

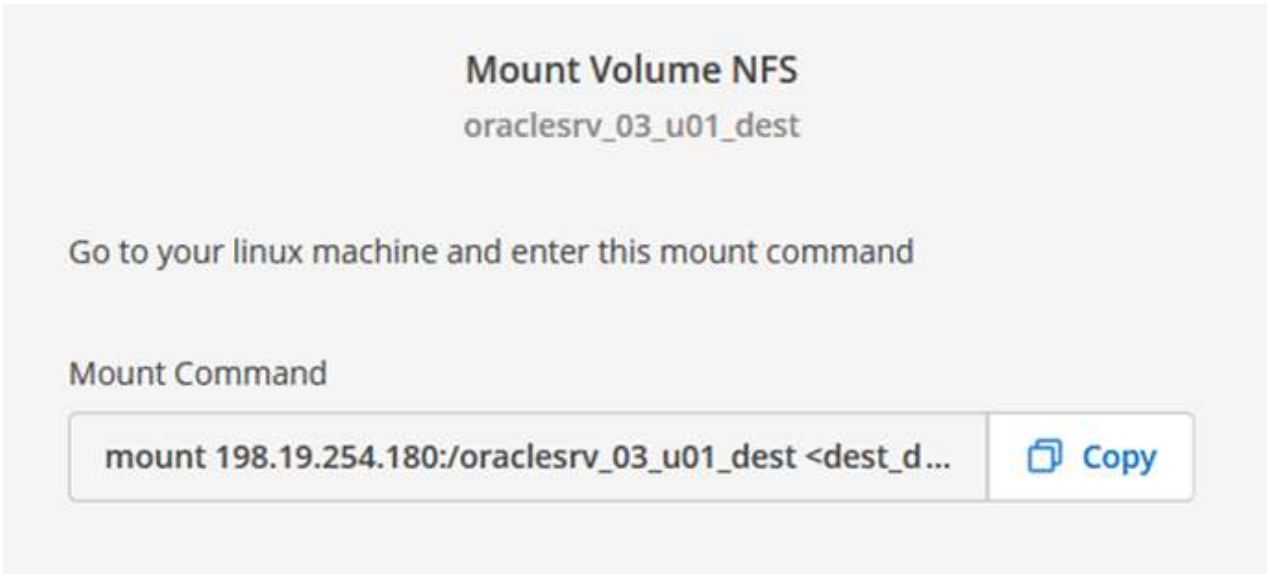
In Cloud Manager, è possibile ottenere il comando mount con l'indirizzo IP NFS LIF corretto per il montaggio dei volumi NFS che contengono i file di database e i log Oracle.

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



2. Dal menu delle azioni, selezionare Mount Command per visualizzare e copiare il comando mount da utilizzare sul server Oracle Linux.





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` per includere i comandi di montaggio.

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

Failback

Una volta completato con successo il processo di failover descritto in questa soluzione, SnapCenter e Veeam riprendono le funzioni di backup in esecuzione in AWS, mentre FSX per ONTAP viene ora designato come storage primario senza relazioni SnapMirror esistenti con il data center on-premise originale. Una volta ripristinato il normale funzionamento on-premise, è possibile utilizzare un processo identico a quello descritto in questa documentazione per eseguire il mirroring dei dati nel sistema di storage ONTAP on-premise.

Come indicato anche in questa documentazione, è possibile configurare SnapCenter per eseguire il mirroring dei volumi di dati dell'applicazione da FSX per ONTAP a un sistema storage ONTAP residente on-premise. Allo stesso modo, puoi configurare Veeam per replicare le copie di backup su Amazon S3 utilizzando un repository di backup scale-out in modo che tali backup siano accessibili a un server di backup Veeam che risiede nel data center on-premise.

Il failback non rientra nell'ambito di questa documentazione, ma il failback non differisce molto dal processo dettagliato qui descritto.

Conclusione

Il caso d'utilizzo 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 offrono tecnologie di mirroring dei dati comprovate che consentono alle organizzazioni di progettare soluzioni di disaster recovery che abbracciano tecnologie on-premise e ONTAP che risiedono presso i principali cloud provider.

FSX per ONTAP su AWS è una soluzione di questo tipo che consente un'integrazione perfetta con SnapCenter e SyncMirror per la replica dei dati delle applicazioni nel cloud. Veeam Backup & Replication è un'altra tecnologia ben nota che si integra perfettamente con i sistemi storage NetApp ONTAP e può fornire il failover allo storage nativo vSphere.

Questa soluzione ha presentato una soluzione di disaster recovery che utilizza lo storage Connect guest da un sistema ONTAP che ospita i dati delle applicazioni SQL Server e Oracle. SnapCenter con SnapMirror offre una soluzione semplice da gestire per proteggere i volumi delle applicazioni sui sistemi ONTAP e replicarli su FSX o CVO che risiedono nel cloud. SnapCenter è una soluzione abilitata al DR per eseguire il failover di tutti i dati delle applicazioni su VMware Cloud su AWS.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Collegamenti alla documentazione della soluzione

  "Multicloud ibrido NetApp con soluzioni VMware"

  "Soluzioni NetApp"

Backup e ripristino di Veeam in VMware Cloud, con Amazon FSX per ONTAP

Veeam Backup & Replication è una soluzione efficace e affidabile per la protezione dei dati in VMware Cloud. Questa soluzione dimostra la corretta configurazione e configurazione per l'utilizzo di backup e replica Veeam per il backup e il ripristino delle macchine virtuali dell'applicazione che risiedono su datastore NFS FSX per ONTAP in VMware Cloud.

Autore: Josh Powell - NetApp Solutions Engineering

Panoramica

VMware Cloud (in AWS) supporta l'utilizzo di datastore NFS come storage supplementare, mentre FSX per NetApp ONTAP è una soluzione sicura per i clienti che hanno bisogno di memorizzare grandi quantità di dati per le loro applicazioni cloud, in grado di scalare indipendentemente dal numero di host ESXi nel cluster SDDC. Questo servizio di storage AWS integrato offre uno storage altamente efficiente con tutte le funzionalità tradizionali di NetApp ONTAP.

Casi di utilizzo

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup e ripristino di macchine virtuali Windows e Linux ospitate in VMC utilizzando FSX per NetApp ONTAP come repository di backup.
- Backup e ripristino dei dati delle applicazioni Microsoft SQL Server utilizzando FSX per NetApp ONTAP come repository di backup.
- Backup e ripristino dei dati delle applicazioni Oracle utilizzando FSX per NetApp ONTAP come repository di backup.

Archivi dati NFS che utilizzano Amazon FSX per ONTAP

Tutte le macchine virtuali di questa soluzione risiedono su datastore NFS supplementari FSX per ONTAP. L'utilizzo di FSX per ONTAP come datastore NFS supplementare offre diversi vantaggi. Ad esempio, consente di:

- Crea un file system scalabile e altamente disponibile nel cloud senza la necessità di complesse operazioni di configurazione e gestione.
- Integrazione con l'ambiente VMware esistente, che consente di utilizzare strumenti e processi familiari per gestire le risorse cloud.
- Sfrutta le funzionalità avanzate di gestione dei dati fornite da ONTAP, come snapshot e replica, per proteggere i tuoi dati e garantirne la disponibilità.

Panoramica sull'implementazione della soluzione

Questo elenco fornisce i passaggi di alto livello necessari per configurare il backup e la replica di Veeeam, eseguire processi di backup e ripristino utilizzando FSX per ONTAP come repository di backup ed eseguire ripristini di macchine virtuali e database SQL Server e Oracle:

1. Creare il file system FSX per ONTAP da utilizzare come repository di backup iSCSI per il backup e la replica Veeam.
2. Implementare Veeam Proxy per distribuire i carichi di lavoro di backup e montare repository di backup iSCSI ospitati su FSX per ONTAP.
3. Configurare Veeam Backup Jobs per il backup di macchine virtuali SQL Server, Oracle, Linux e Windows.
4. Ripristinare le macchine virtuali SQL Server e i singoli database.
5. Ripristinare le macchine virtuali Oracle e i singoli database.

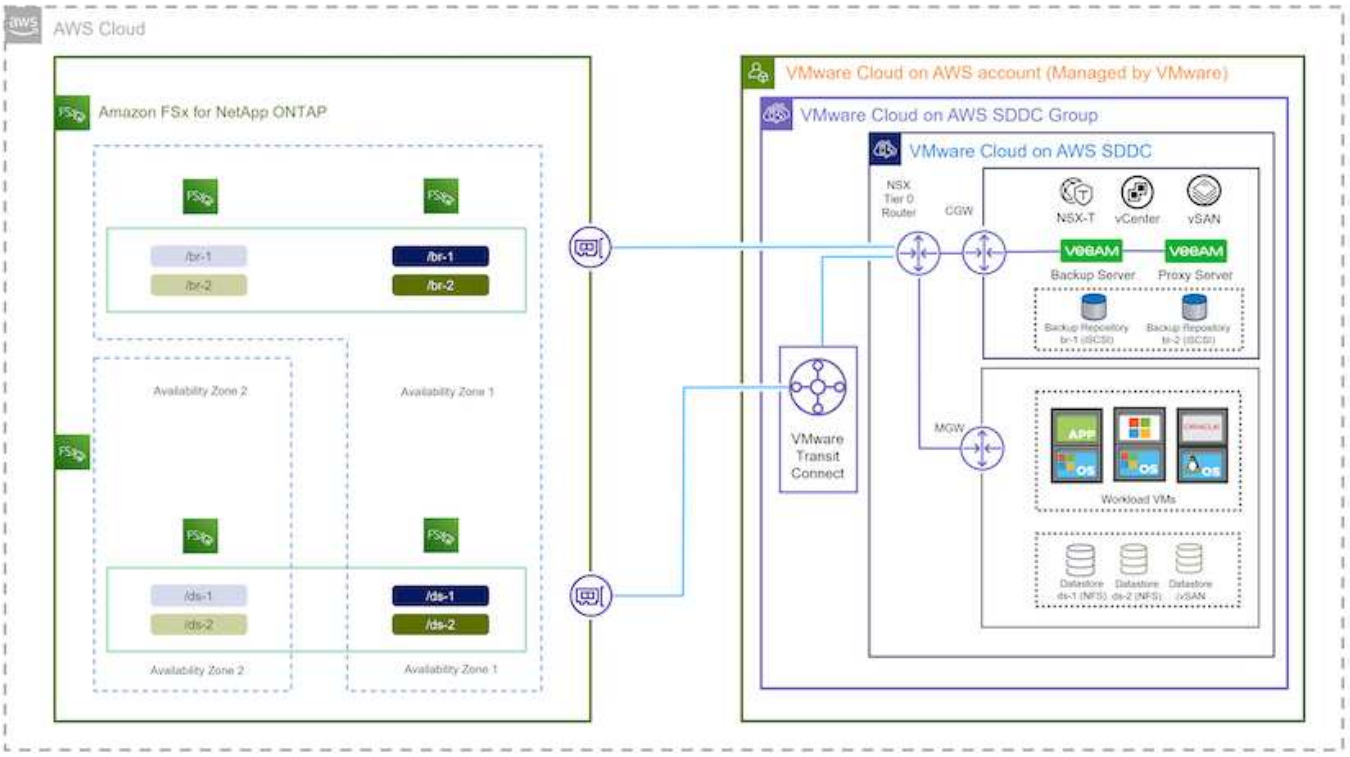
Prerequisiti

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware Cloud e situate su archivi dati NFS ospitati da FSX per NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano configurati e pronti per l'uso:

1. File system FSX per ONTAP con uno o più datastore NFS connessi a VMware Cloud.
2. Macchina virtuale Microsoft Windows Server con software Veeam Backup & Replication installato.
    - Il server vCenter è stato rilevato dal server Veeam Backup & Replication utilizzando il proprio indirizzo IP o il nome di dominio completo.
3. Microsoft Windows Server VM da installare con i componenti di Veeam Backup Proxy durante l'implementazione della soluzione.
4. Macchine virtuali Microsoft SQL Server con VMDK e dati delle applicazioni che risiedono su FSX per datastore NFS di ONTAP. Per questa soluzione avevamo due database SQL su due VMDK separati.
    - Nota: Come Best practice, i file di log delle transazioni e dei database vengono collocati su dischi separati, in quanto ciò migliorerà le performance e l'affidabilità. Ciò è dovuto in parte al fatto che i log delle transazioni vengono scritti in sequenza, mentre i file di database vengono scritti in modo casuale.
5. VM di database Oracle con VMDK e dati delle applicazioni che risiedono su FSX per datastore NFS di ONTAP.
6. VM di file server Linux e Windows con VMDK residenti su FSX per datastore NFS ONTAP.
7. Veeam richiede porte TCP specifiche per la comunicazione tra server e componenti nell'ambiente di backup. Sui componenti dell'infrastruttura di backup Veeam, le regole firewall richieste vengono create automaticamente. Per un elenco completo dei requisiti delle porte di rete, consultare la sezione Porte del "Guida utente di Veeam Backup and Replication per VMware vSphere".

Architettura di alto livello

Il test/convalida di questa soluzione è stato eseguito in un laboratorio che potrebbe corrispondere o meno all'ambiente di implementazione finale. Per ulteriori informazioni, fare riferimento alle seguenti sezioni.



Componenti hardware/software

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware Cloud e situate su archivi dati NFS ospitati da FSX per NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano già configurati e pronti per l'uso:

- Macchine virtuali Microsoft Windows situate su un archivio dati NFS FSX per ONTAP
- Macchine virtuali Linux (CentOS) situate su un archivio dati NFS FSX per ONTAP
- Macchine virtuali Microsoft SQL Server situate su un archivio dati NFS FSX per ONTAP
  - Due database ospitati su VMDK separati
- Oracle VM si trova su un archivio dati FSX per NFS ONTAP

Implementazione della soluzione

In questa soluzione forniamo istruzioni dettagliate per l'implementazione e la convalida di una soluzione che utilizza il software di backup e replica Veeam per eseguire il backup e il ripristino di macchine virtuali di file server SQL Server, Oracle e Windows e Linux in un VMware Cloud SDDC su AWS. Le macchine virtuali di questa soluzione risiedono su un datastore NFS supplementare ospitato da FSX per ONTAP. Inoltre, viene utilizzato un file system FSX separato per ONTAP per ospitare volumi iSCSI che verranno utilizzati per i repository di backup Veeam.

Passeremo a FSX per la creazione di file system ONTAP, il montaggio di volumi iSCSI da utilizzare come repository di backup, la creazione e l'esecuzione di processi di backup e il ripristino di macchine virtuali e database.

Per informazioni dettagliate su FSX per NetApp ONTAP, fare riferimento a. "Guida utente di FSX per ONTAP".

Per informazioni dettagliate su Veeam Backup e Replication, fare riferimento a. "Documentazione tecnica del

Centro assistenza Veeam" sito.

Per considerazioni e limitazioni sull'utilizzo di Veeam Backup and Replication con VMware Cloud su AWS, fare riferimento a. "VMware Cloud su AWS e VMware Cloud su supporto Dell EMC. Considerazioni e limitazioni".

Implementare il server proxy Veeam

Un server proxy Veeam è un componente del software Veeam Backup & Replication che funge da intermediario tra l'origine e la destinazione di backup o replica. Il server proxy consente di ottimizzare e accelerare il trasferimento dei dati durante i processi di backup elaborando i dati in locale e può utilizzare diverse modalità di trasporto per accedere ai dati utilizzando le API VMware vStorage per la protezione dei dati o attraverso l'accesso diretto allo storage.

Quando si sceglie un server proxy Veeam, è importante considerare il numero di attività simultanee e la modalità di trasporto o il tipo di accesso allo storage desiderato.

Per il dimensionamento del numero di server proxy e i relativi requisiti di sistema, fare riferimento a. "Veeeam VMware vSphere Best Practice Guide".

Veeam Data Mover è un componente di Veeam Proxy Server e utilizza una Transport Mode come metodo per ottenere i dati delle macchine virtuali dall'origine e trasferirli alla destinazione. La modalità di trasporto viene specificata durante la configurazione del processo di backup. È possibile aumentare l'efficienza dei backup dagli archivi dati NFS utilizzando l'accesso diretto allo storage.

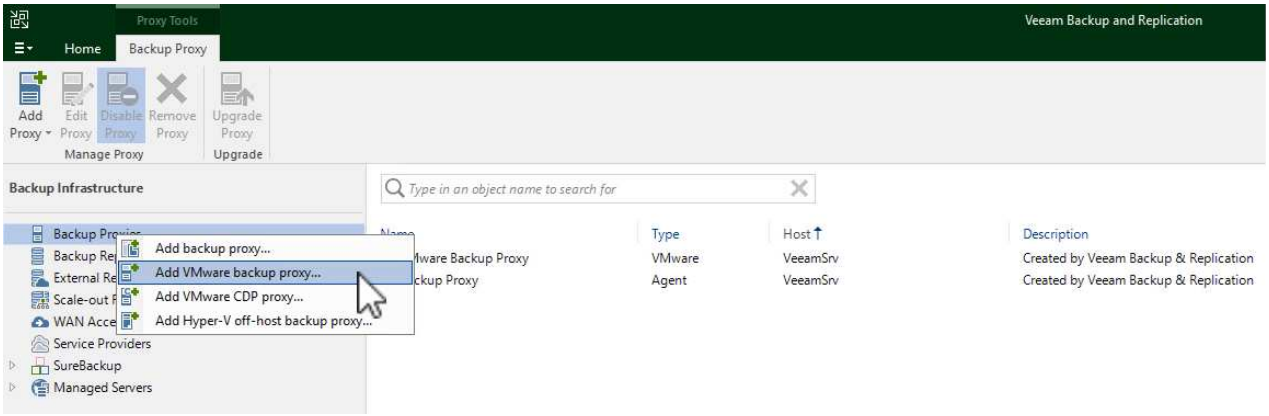
Per ulteriori informazioni sulle modalità di trasporto, fare riferimento a. "Guida utente di Veeam Backup and Replication per VMware vSphere".

Nella fase successiva verrà descritta l'implementazione di Veeam Proxy Server su una macchina virtuale Windows nel software SDDC VMware Cloud.

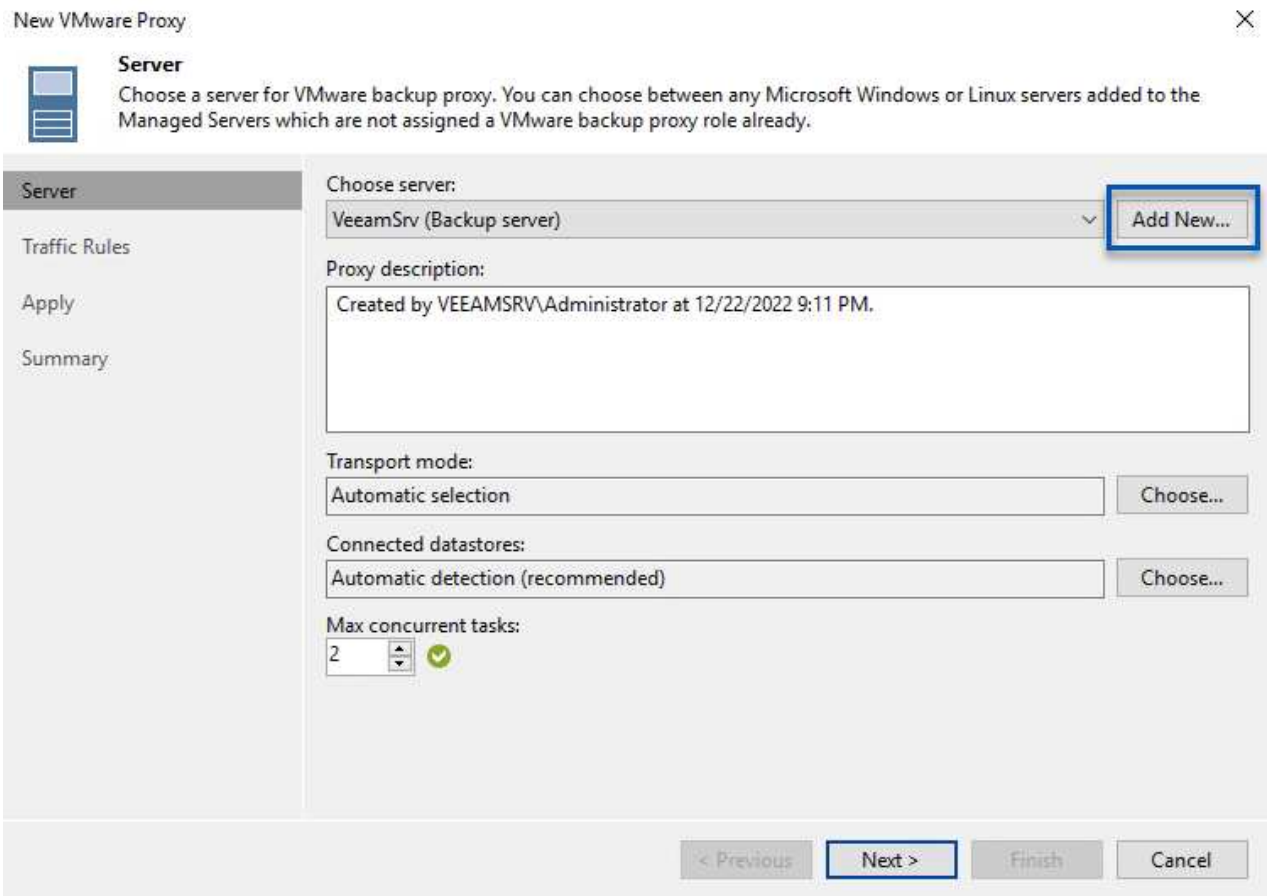
Implementare Veeam Proxy per distribuire i carichi di lavoro di backup

In questa fase, il proxy Veeam viene distribuito su una macchina virtuale Windows esistente. Ciò consente di distribuire i processi di backup tra il server di backup Veeam primario e il proxy Veeam.

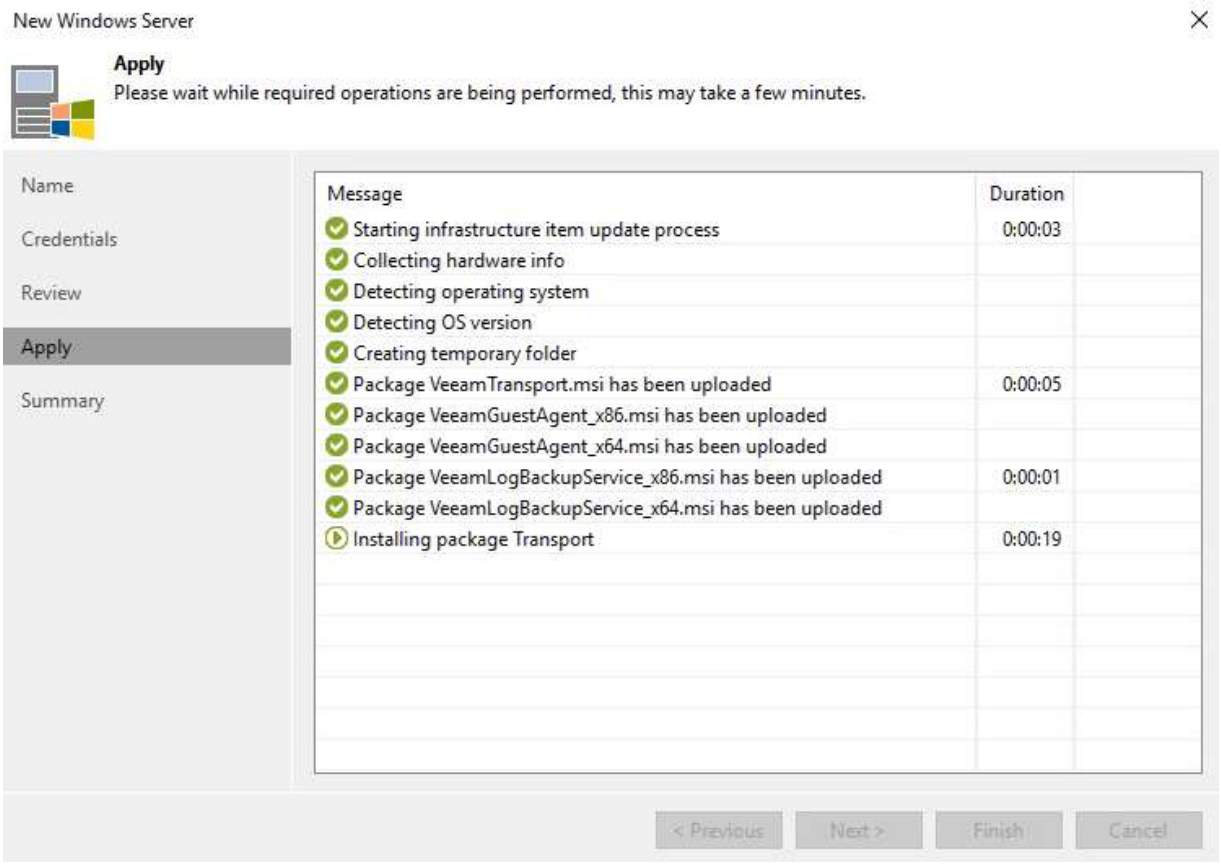
1. Sul server Veeam Backup and Replication, aprire la console di amministrazione e selezionare **Backup Infrastructure** nel menu in basso a sinistra.
2. Fare clic con il pulsante destro del mouse su **Backup Proxy** e fare clic su **Add VMware backup proxy…** per aprire la procedura guidata.



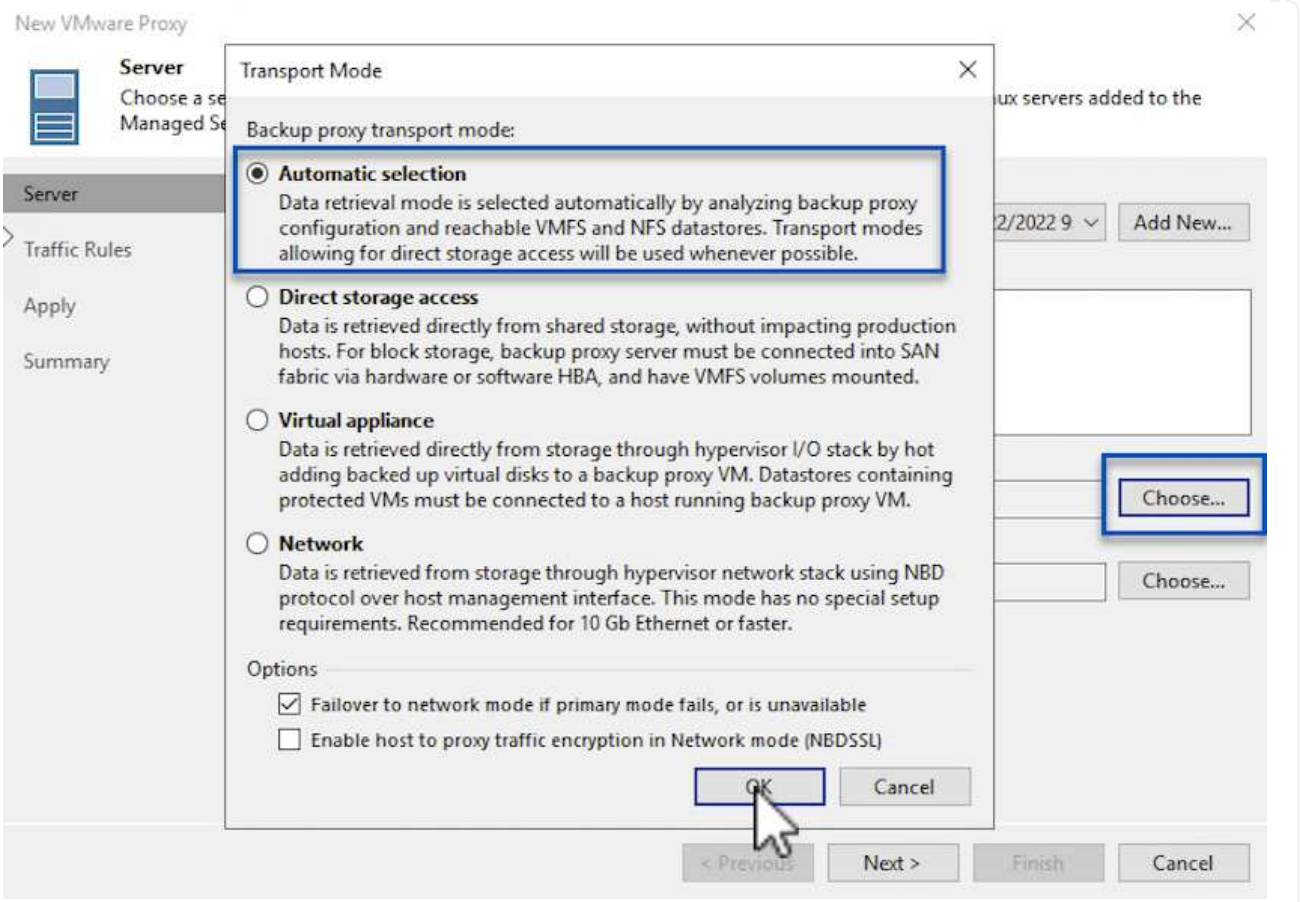
3. Nella procedura guidata **Add VMware Proxy** fare clic sul pulsante **Add New…** (Aggiungi nuovo…) per aggiungere un nuovo server proxy.



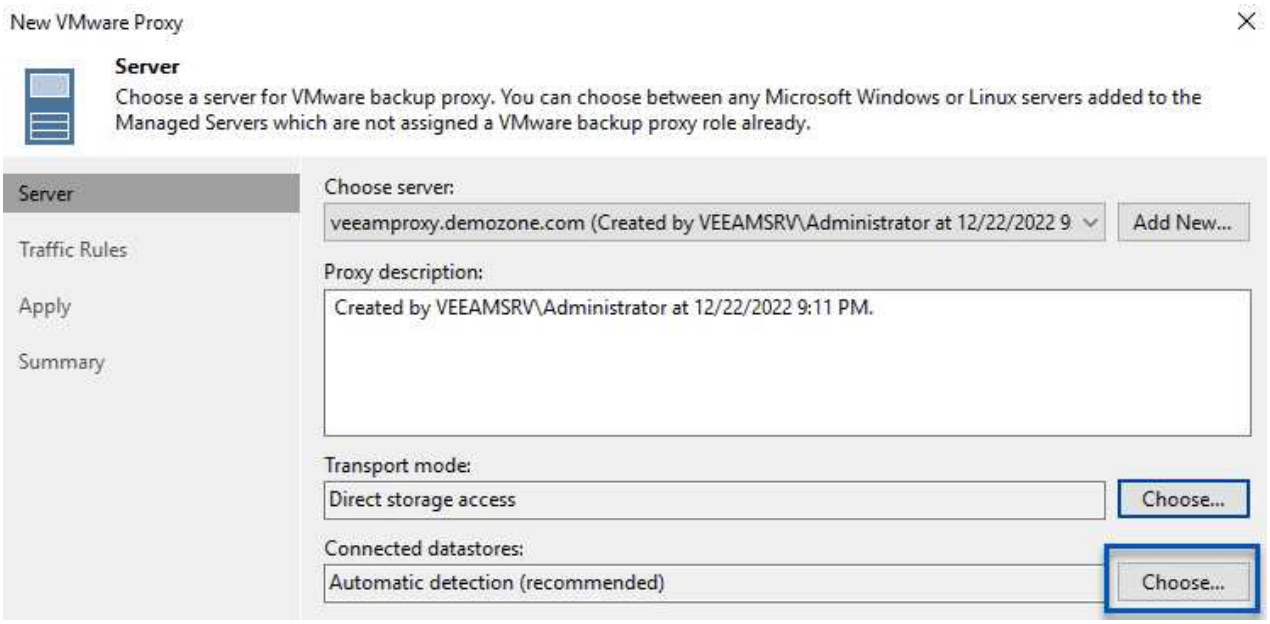
4. Selezionare per aggiungere Microsoft Windows e seguire le istruzioni per aggiungere il server:
   - Inserire il nome DNS o l'indirizzo IP
   - Selezionare un account da utilizzare per le credenziali nel nuovo sistema o aggiungere nuove credenziali
   - Esaminare i componenti da installare, quindi fare clic su **Apply** (Applica) per iniziare la distribuzione

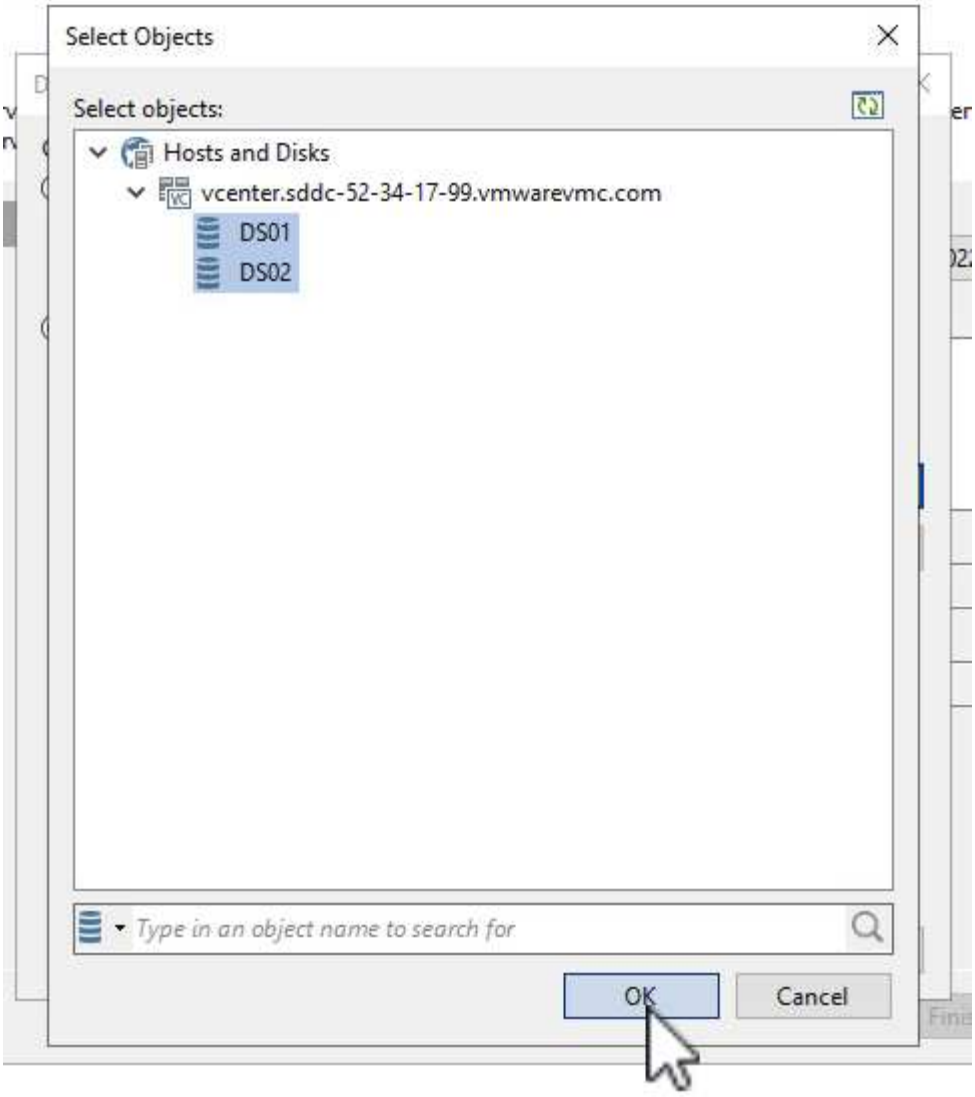


5. Nella procedura guidata **New VMware Proxy**, scegliere una modalità di trasporto. Nel nostro caso abbiamo scelto **selezione automatica**.

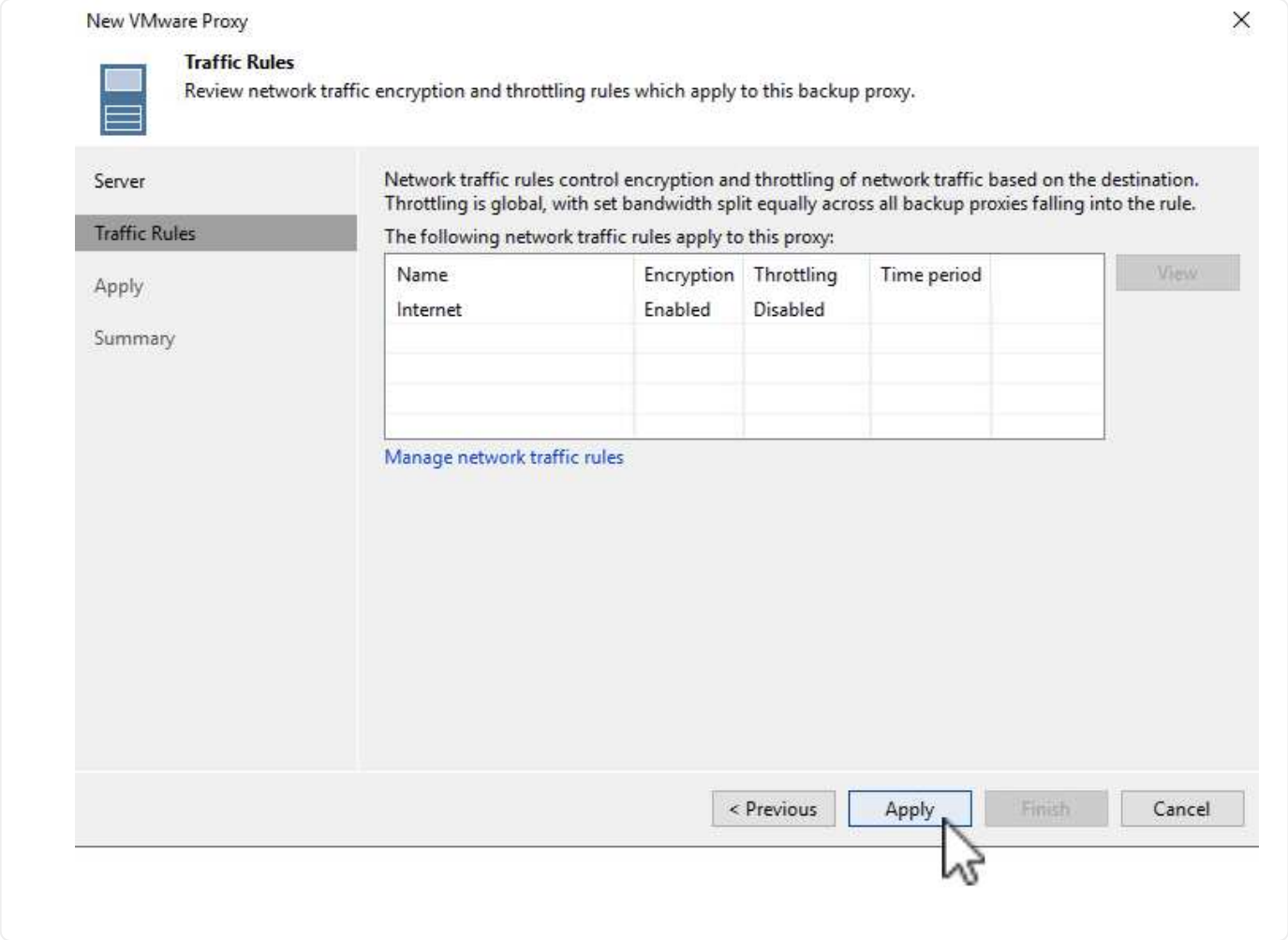


6. Selezionare gli archivi dati connessi ai quali si desidera che VMware Proxy abbia accesso diretto.





7. Configurare e applicare le regole di traffico di rete desiderate, ad esempio la crittografia o la limitazione. Al termine, fare clic sul pulsante **Apply** (Applica) per completare l'implementazione.



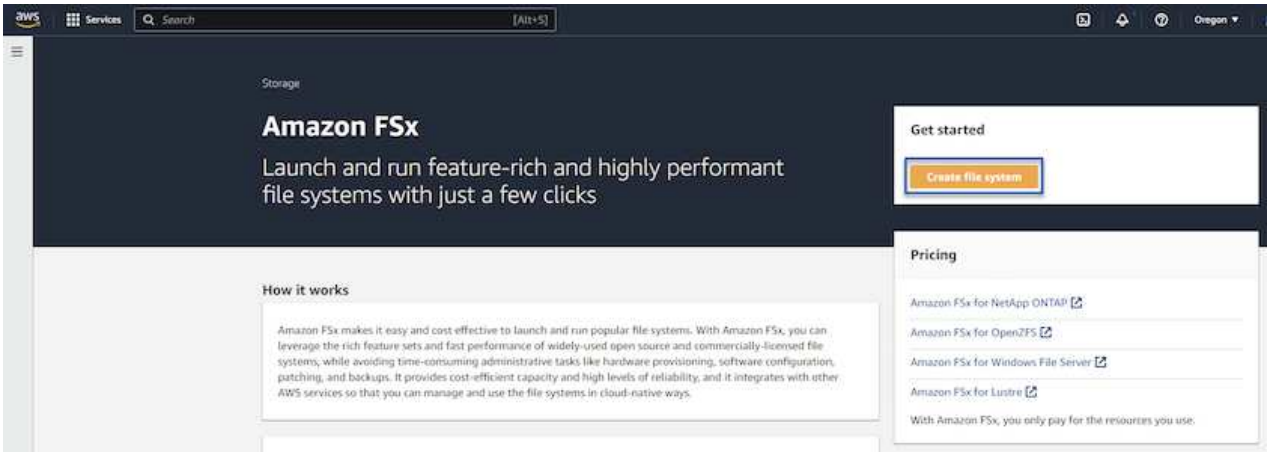
Configurare storage e repository di backup

Il server primario Veeam Backup e il server Veeam Proxy hanno accesso a un repository di backup sotto forma di storage a connessione diretta. In questa sezione viene descritta la creazione di un file system FSX per ONTAP, il montaggio di LUN iSCSI sui server Veeam e la creazione di repository di backup.

Creare FSX per il file system ONTAP

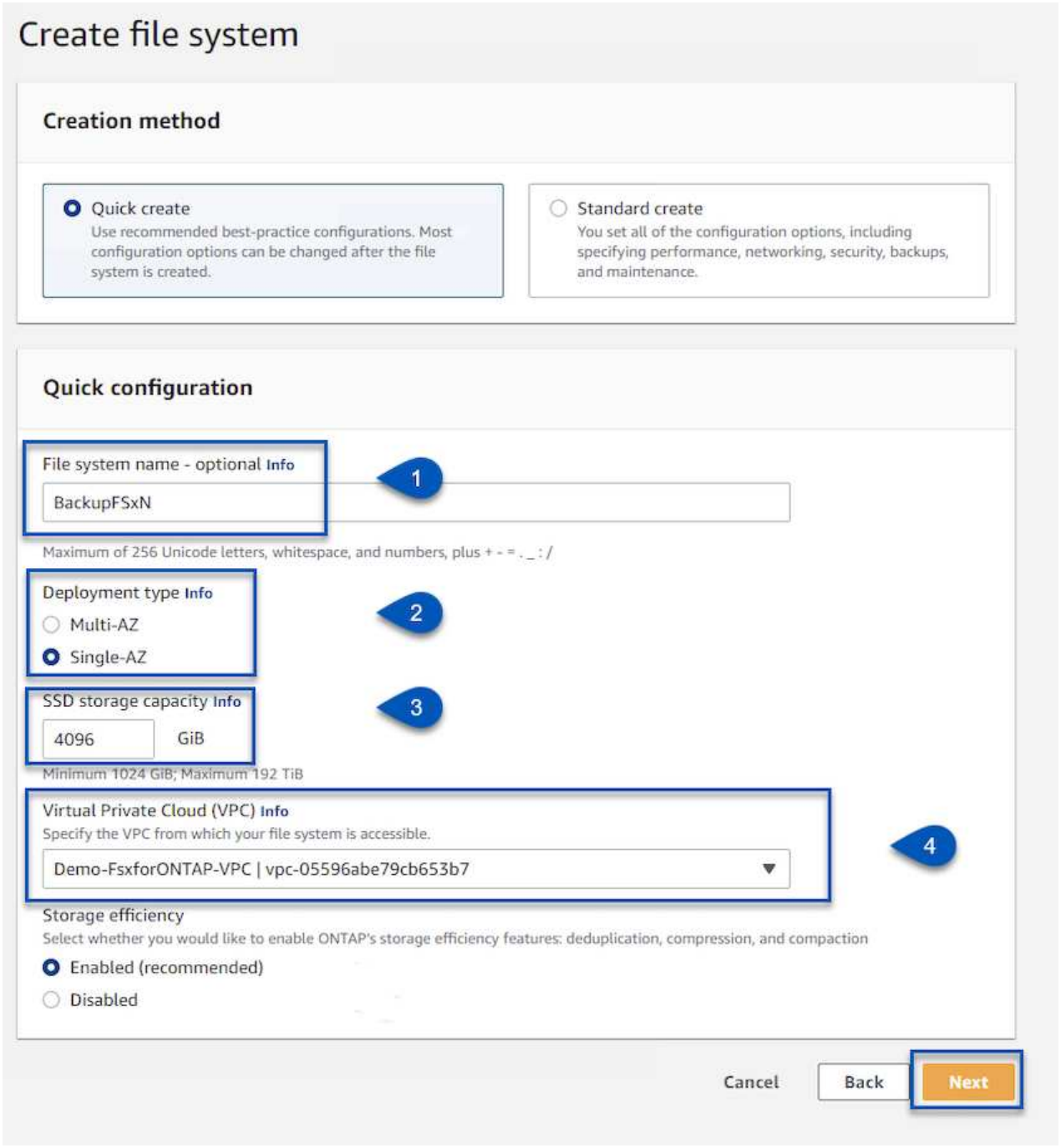
Creare un file system FSX per ONTAP che verrà utilizzato per ospitare i volumi iSCSI per i repository di backup Veeam.

1. Nella console AWS, andare a FSX e quindi a **Create file system**



2. Selezionare **Amazon FSX per NetApp ONTAP**, quindi **Avanti** per continuare.

3. Inserire il nome del file system, il tipo di implementazione, la capacità dello storage SSD e il VPC in cui si trova il cluster FSX per ONTAP. Deve essere un VPC configurato per comunicare con la rete di macchine virtuali in VMware Cloud. Fare clic su **Avanti**.



4. Esaminare le fasi di implementazione e fare clic su **Create file System** (Crea file system) per avviare il processo di creazione del file system.

Configurare e montare LUN iSCSI

Creare e configurare i LUN iSCSI su FSX per ONTAP e montarli sui server proxy e di backup Veeam. Questi LUN verranno utilizzati in seguito per creare repository di backup Veeam.

> La creazione di un LUN iSCSI su FSX per ONTAP è un processo multi-step. La prima fase della creazione dei volumi può essere eseguita nella console Amazon FSX o con la CLI NetApp ONTAP.

> Per ulteriori informazioni sull'utilizzo di FSX per ONTAP, consultare "Guida utente di FSX per ONTAP".

1. Dalla CLI di NetApp ONTAP creare i volumi iniziali utilizzando il seguente comando:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Creare LUN utilizzando i volumi creati nel passaggio precedente:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Concedere l'accesso alle LUN creando un gruppo di iniziatori contenente l'IQN iSCSI dei server proxy e di backup Veeam:

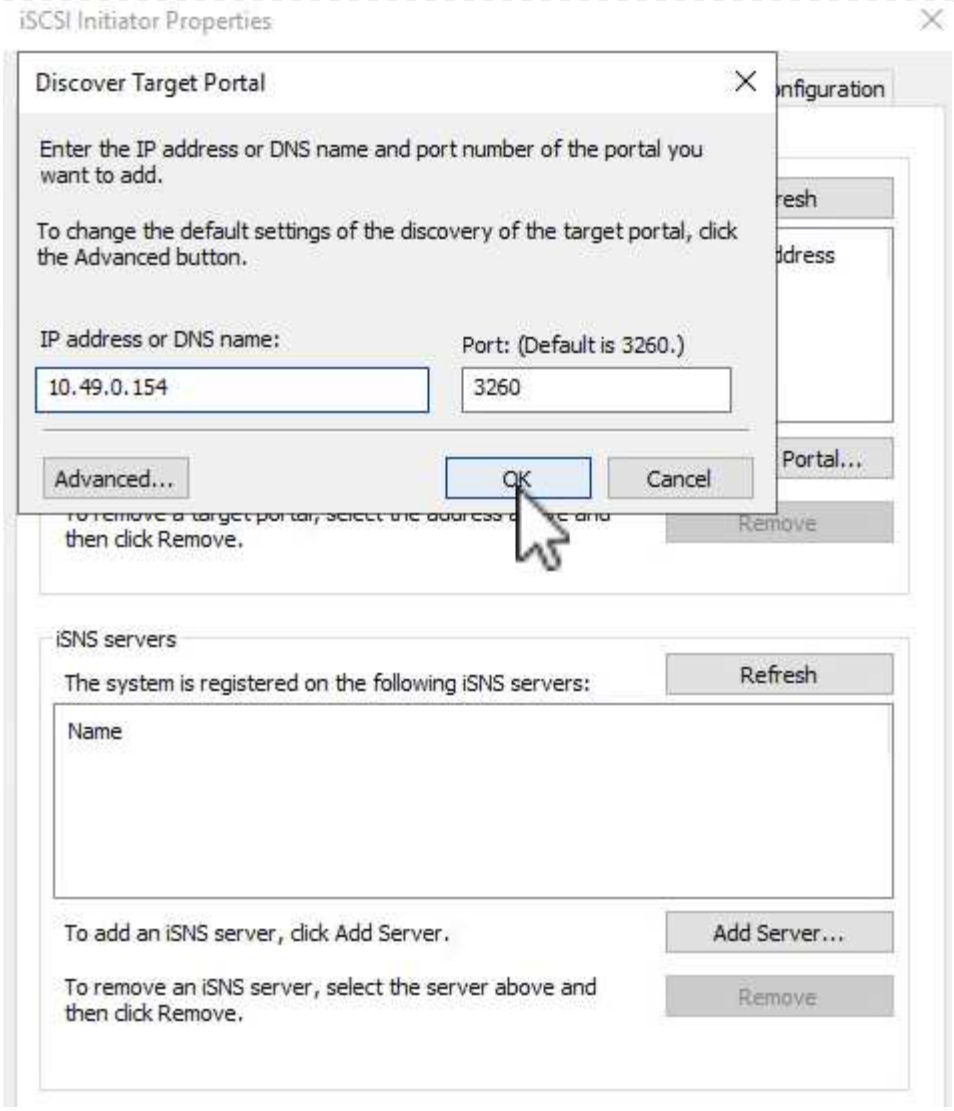
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

> Per completare il passaggio precedente, è necessario recuperare prima IQN dalle proprietà di iSCSI Initiator sui server Windows.

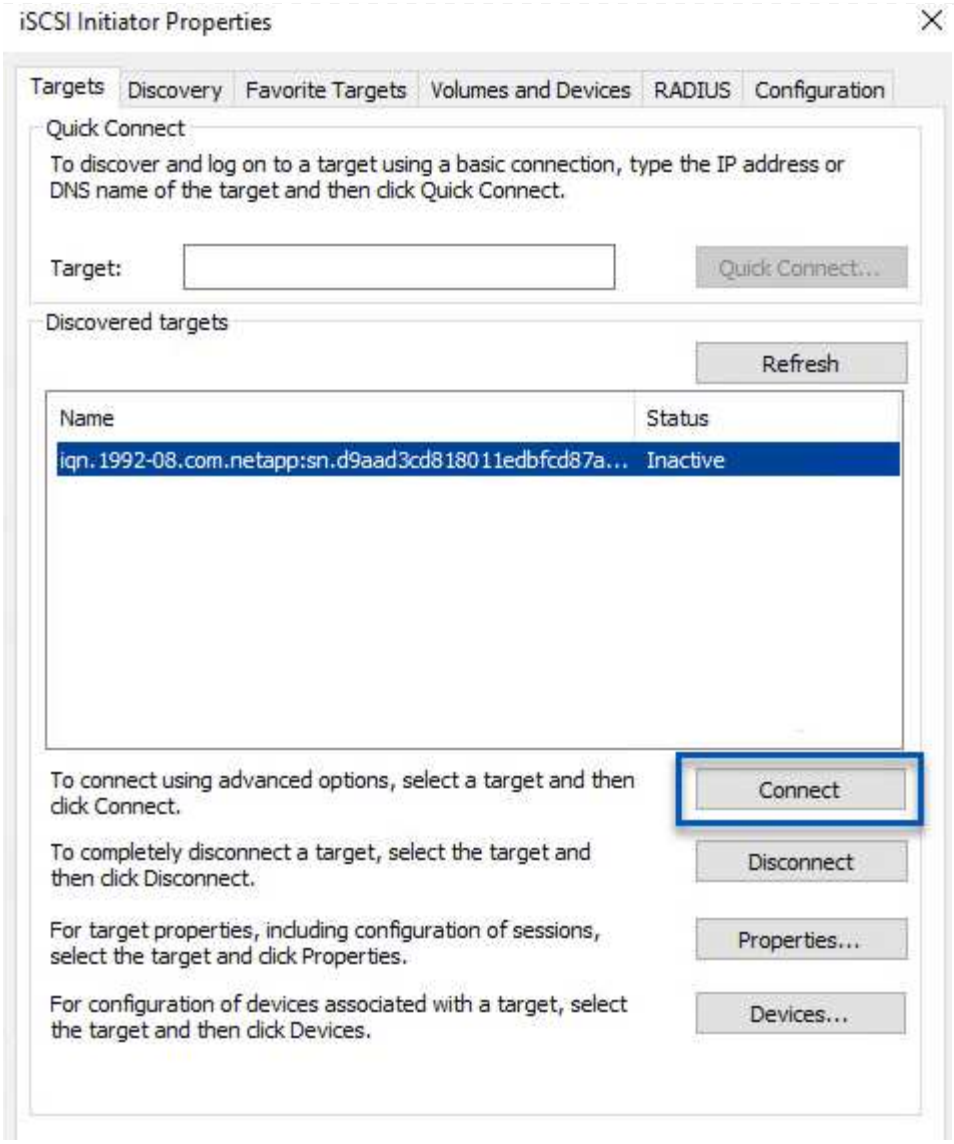
4. Infine, mappare le LUN al gruppo iniziatore appena creato:

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

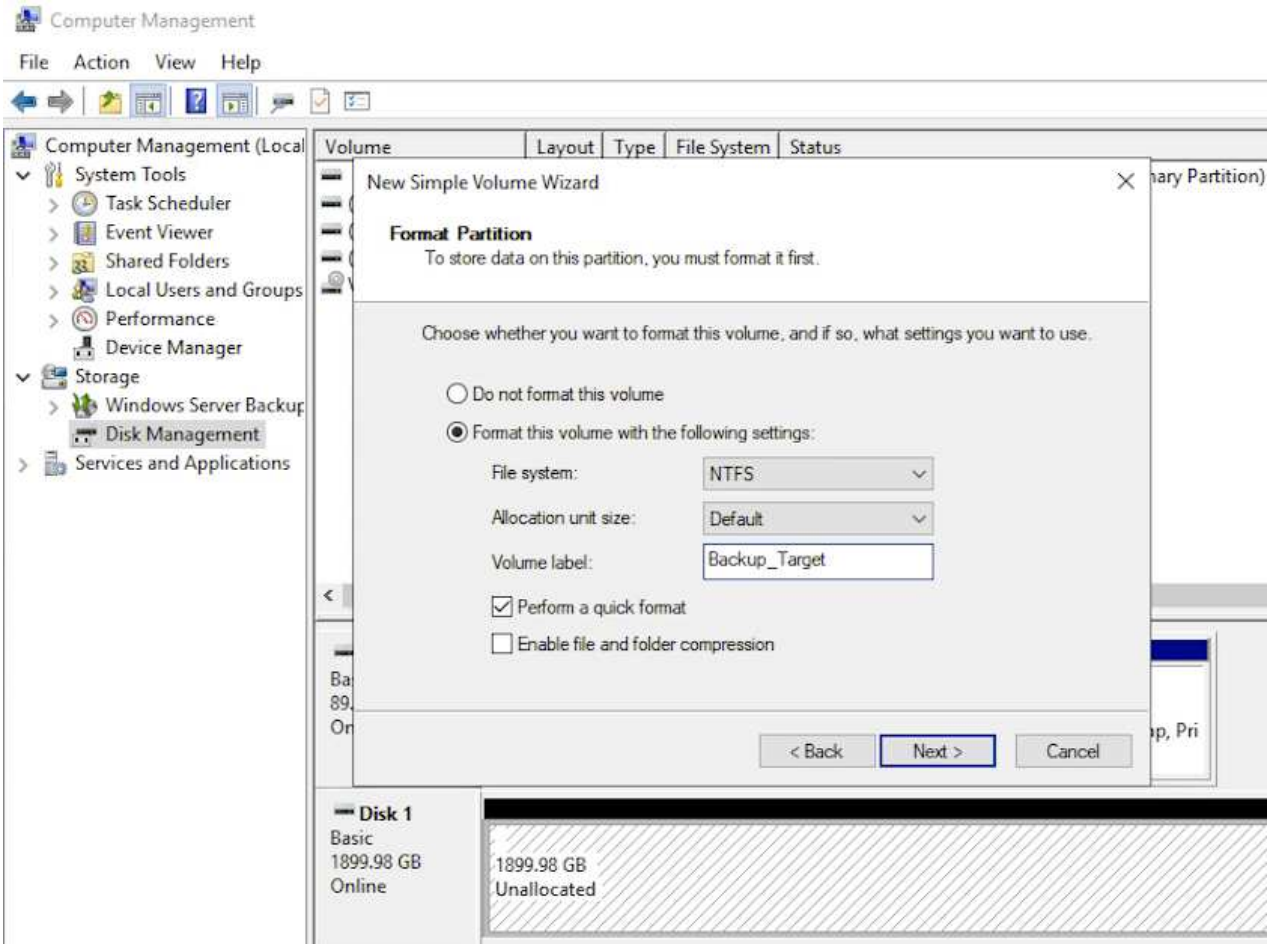
5. Per montare i LUN iSCSI, accedere a Veeam Backup & Replication Server e aprire iSCSI Initiator Properties. Accedere alla scheda **Discover** e inserire l'indirizzo IP di destinazione iSCSI.



6. Nella scheda **targets**, evidenziare il LUN inattivo e fare clic su **Connect**. Selezionare la casella **Enable multi-path** (attiva percorso multiplo) e fare clic su **OK** per connettersi al LUN.



7. Nell'utility Disk Management inizializza il nuovo LUN e crea un volume con il nome e la lettera del disco desiderati. Selezionare la casella **Enable multi-path** (attiva percorso multiplo) e fare clic su **OK** per connettersi al LUN.

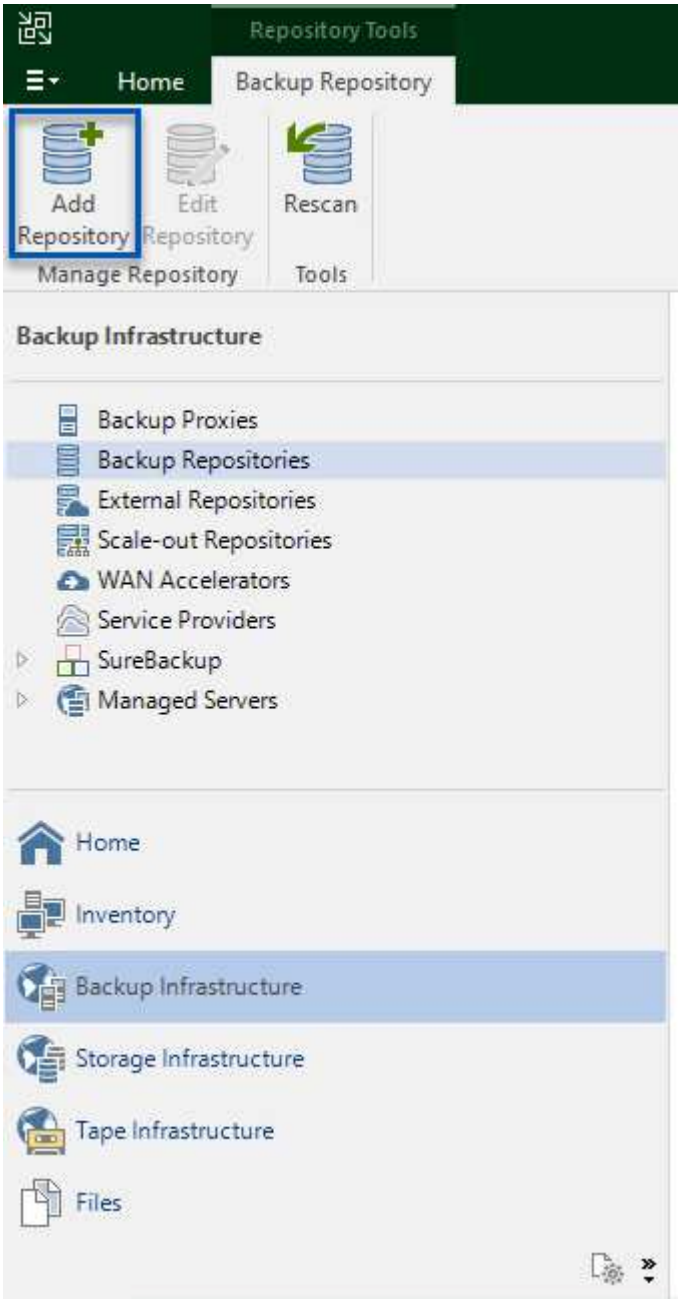


8. Ripetere questa procedura per montare i volumi iSCSI sul server Veeam Proxy.

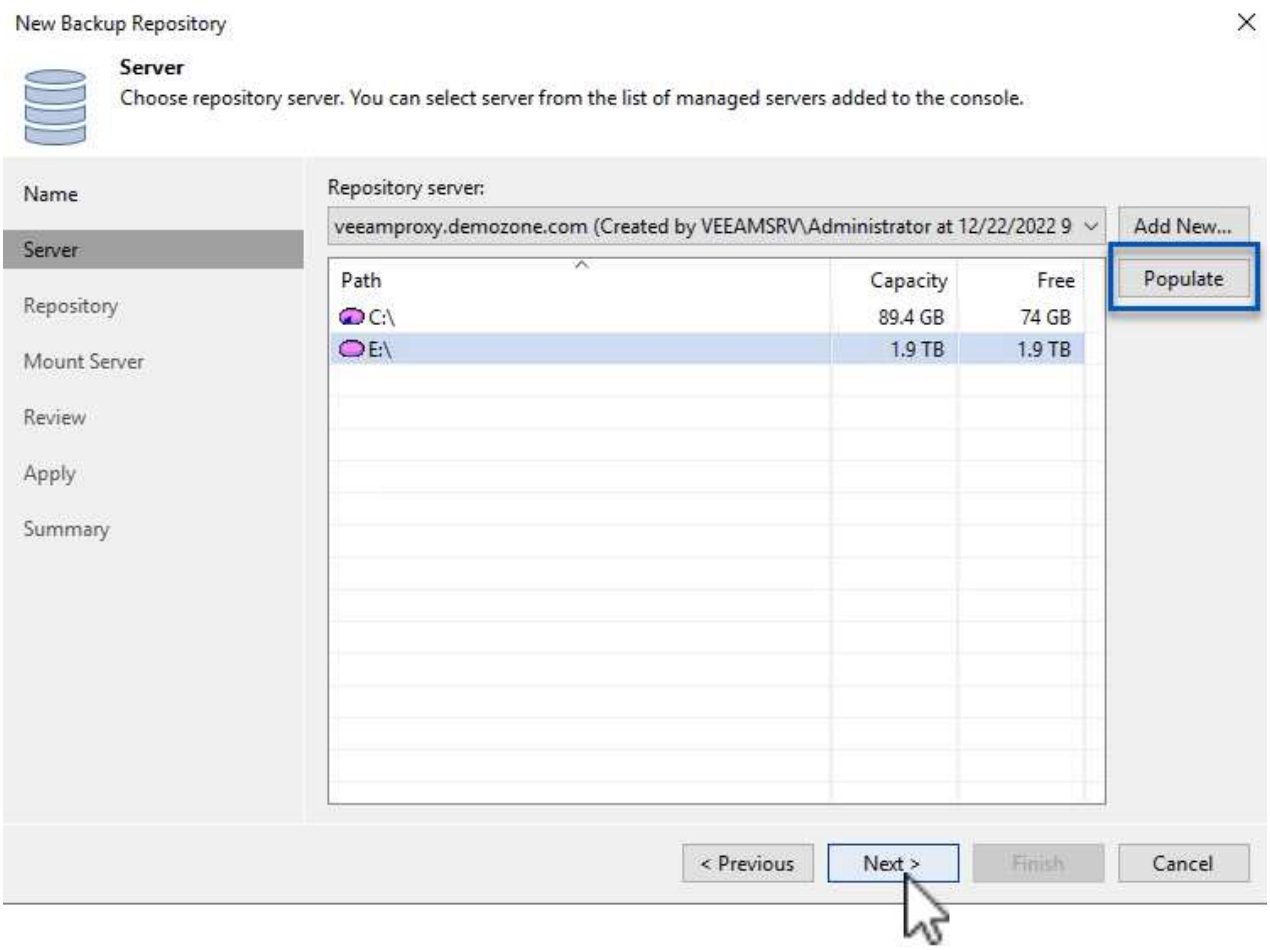
Creare repository di backup Veeam

Nella console di backup e replica di Veeam, creare repository di backup per i server Veeam Backup e Veeam Proxy. Questi repository verranno utilizzati come destinazioni di backup per i backup delle macchine virtuali.

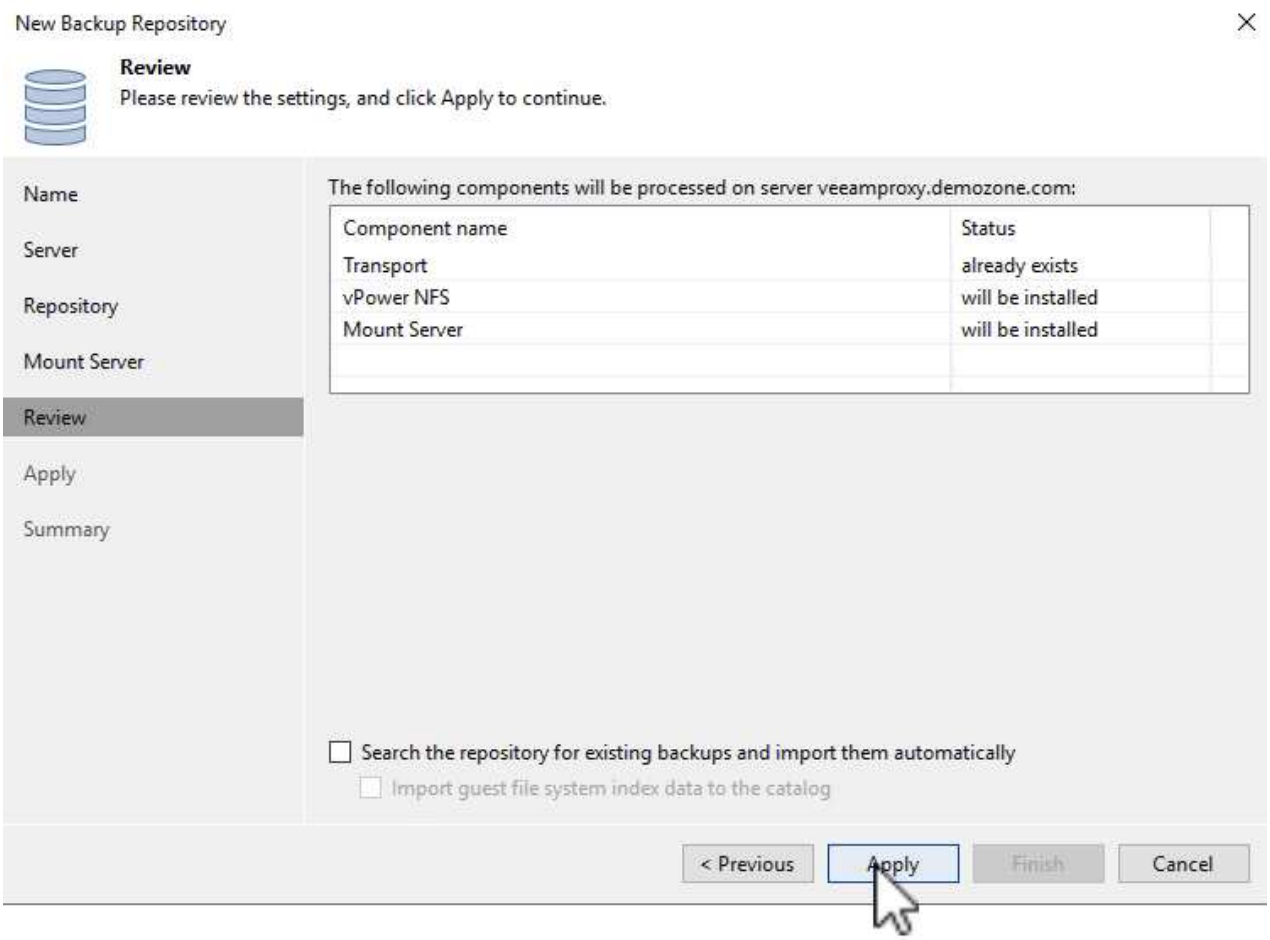
1. Nella console di backup e replica di Veeam, fare clic su **Backup Infrastructure** in basso a sinistra, quindi selezionare **Add Repository**



2. Nella procedura guidata nuovo repository di backup, immettere un nome per il repository, quindi selezionare il server dall'elenco a discesa e fare clic sul pulsante **popola** per scegliere il volume NTFS da utilizzare.



3. Nella pagina successiva, scegliere un server Mount che verrà utilizzato per montare i backup quando si eseguono ripristini avanzati. Per impostazione predefinita, si tratta dello stesso server a cui è collegato lo storage del repository.
4. Esaminare le selezioni e fare clic su **Apply** (Applica) per avviare la creazione del repository di backup.



5. Ripetere questa procedura per tutti i server proxy aggiuntivi.

Configurare i processi di backup Veeam

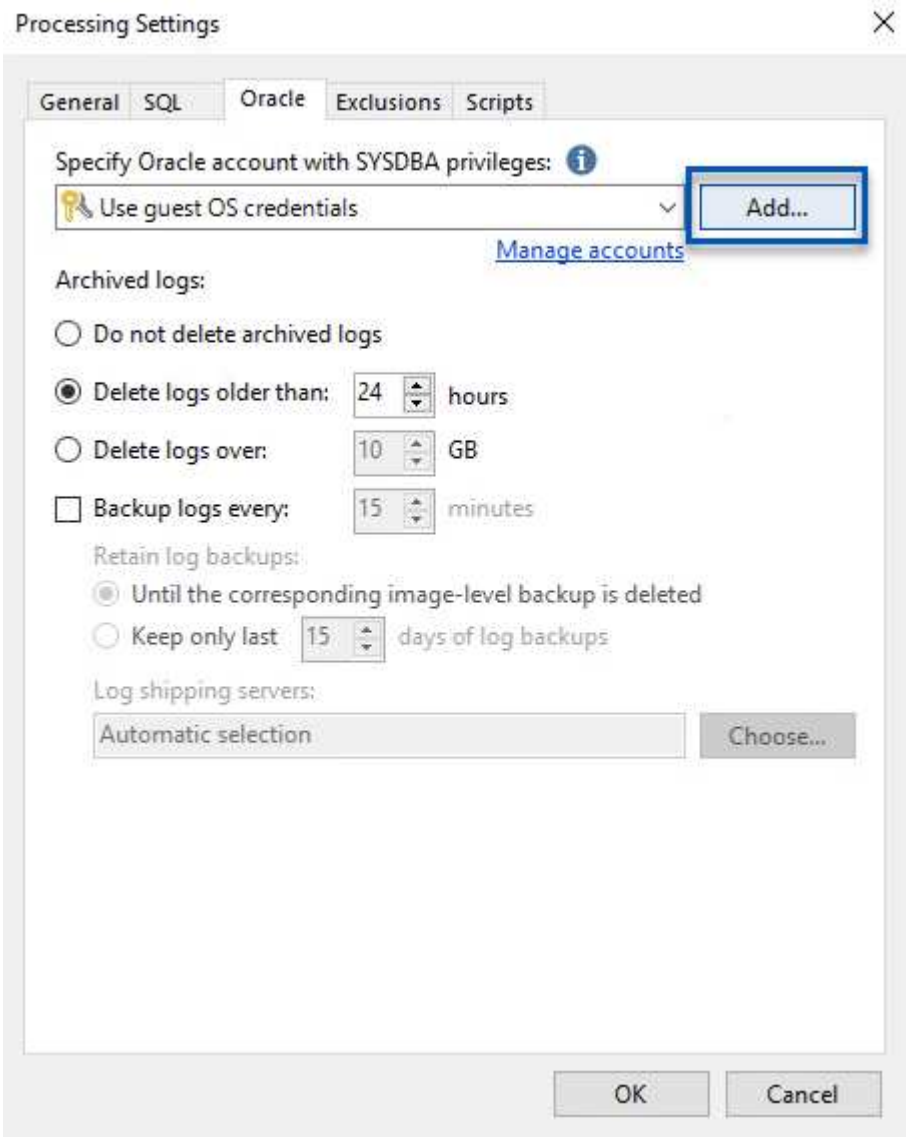
I processi di backup devono essere creati utilizzando i repository di backup nella sezione precedente. La creazione di processi di backup è una parte normale del repertorio di qualsiasi amministratore dello storage e non vengono descritte tutte le fasi qui descritte. Per informazioni più complete sulla creazione di processi di backup in Veeam, vedere "Documentazione tecnica del Centro assistenza Veeam".

In questa soluzione sono stati creati processi di backup separati per:

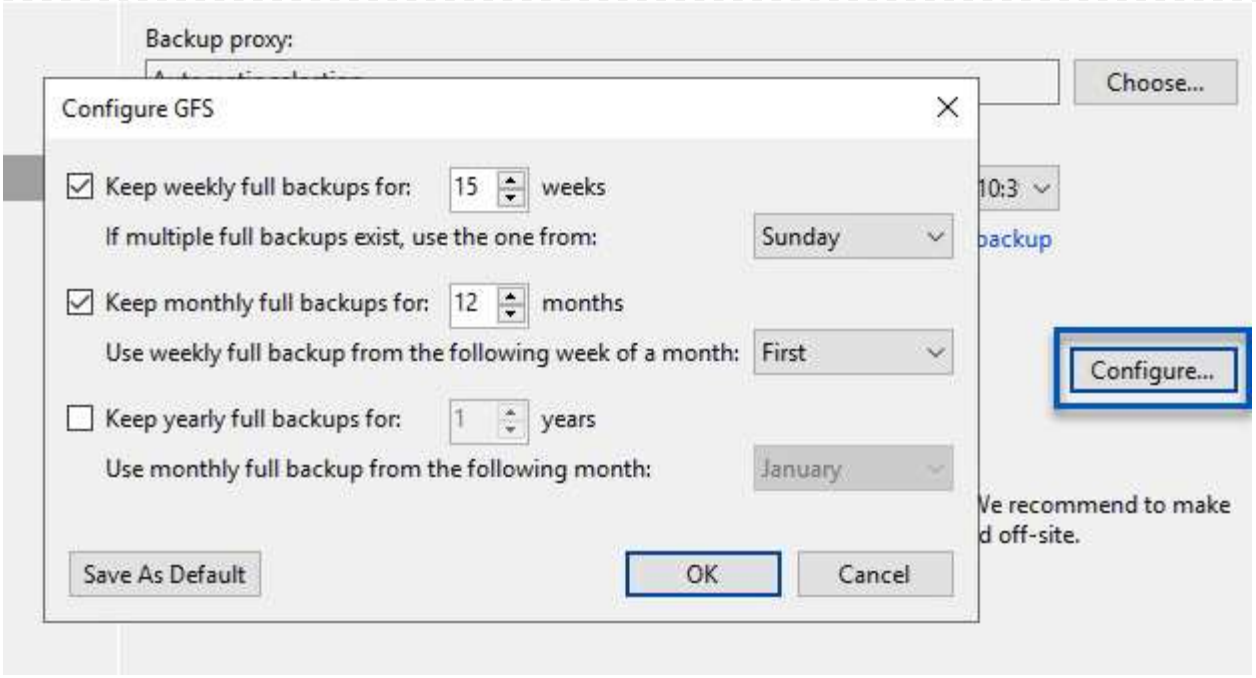
- Microsoft Windows SQL Server
- Server di database Oracle
- File server Windows
- File server Linux

Considerazioni generali per la configurazione dei processi di backup Veeam

1. Abilitare l'elaborazione basata sulle applicazioni per creare backup coerenti ed eseguire l'elaborazione del log delle transazioni.
2. Dopo aver abilitato l'elaborazione in base all'applicazione, aggiungere le credenziali corrette con privilegi di amministratore all'applicazione, poiché potrebbero essere diverse dalle credenziali del sistema operativo guest.



3. Per gestire il criterio di conservazione per il backup, selezionare **Mantieni alcuni backup completi più a lungo per scopi di archiviazione** e fare clic sul pulsante **Configura…** per configurare il criterio.



Ripristinare le macchine virtuali applicative con il ripristino completo di Veeam

Eseguire un ripristino completo con Veeam è il primo passo per eseguire un ripristino dell'applicazione. Abbiamo validato che i ripristini completi delle nostre macchine virtuali erano accesi e tutti i servizi funzionavano normalmente.

Il ripristino dei server è una parte normale del repertorio di qualsiasi amministratore dello storage e non vengono descritte tutte le fasi qui descritte. Per informazioni più complete sull'esecuzione di ripristini completi in Veeam, consultare la "Documentazione tecnica del Centro assistenza Veeam".

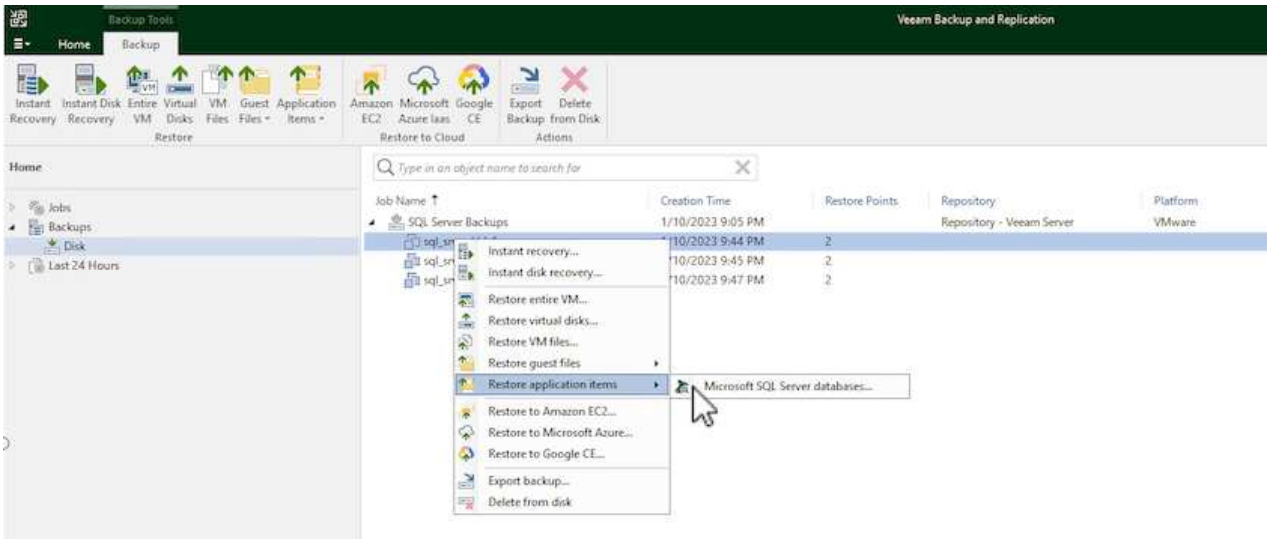
Ripristinare i database di SQL Server

Veeam Backup & Replication offre diverse opzioni per il ripristino dei database di SQL Server. Per questa convalida abbiamo utilizzato Veeam Explorer per SQL Server con Instant Recovery per eseguire ripristini dei database SQL Server. SQL Server Instant Recovery è una funzionalità che consente di ripristinare rapidamente i database di SQL Server senza dover attendere il ripristino completo del database. Questo rapido processo di recovery riduce al minimo i downtime e garantisce la continuità del business. Ecco come funziona:

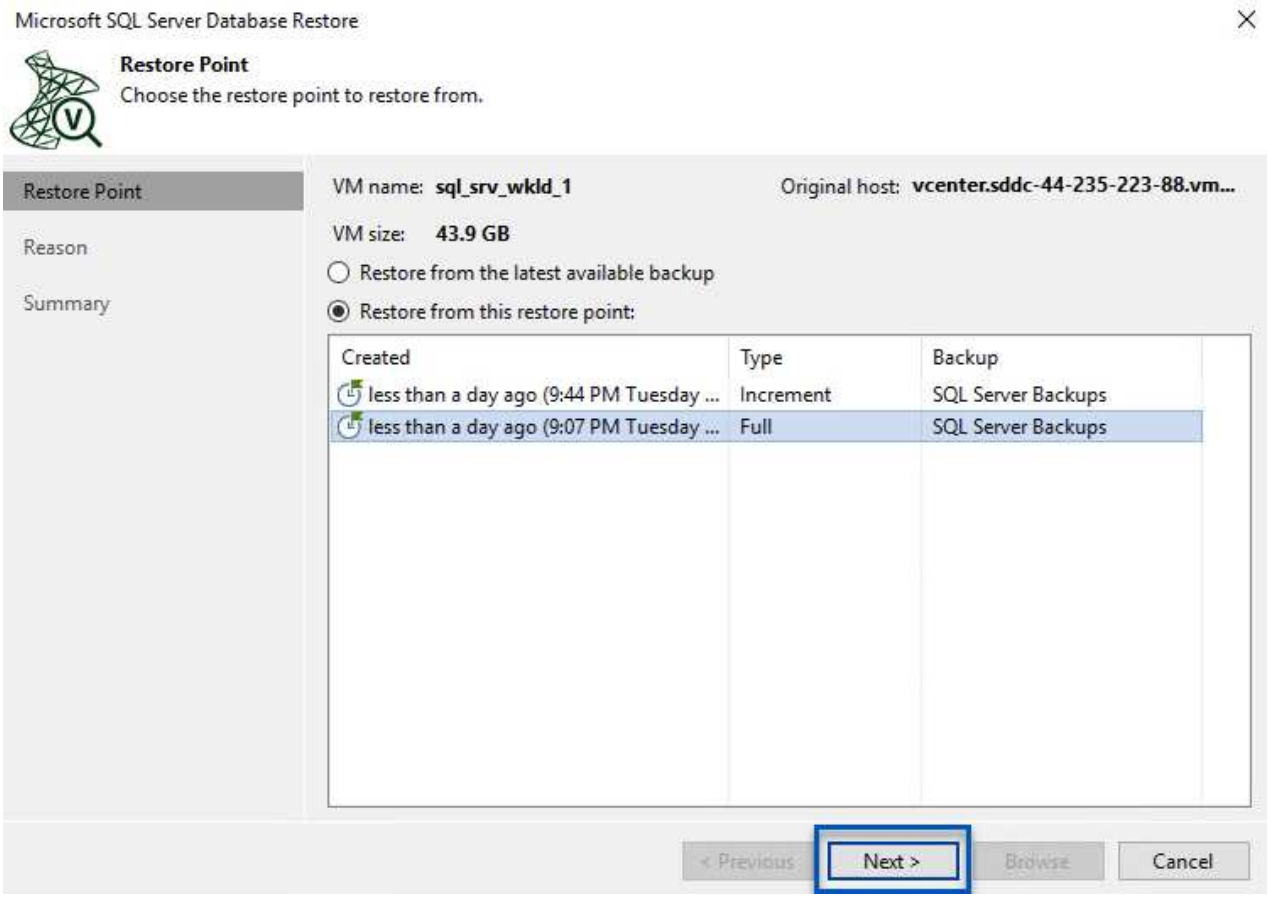
- Veeeam Explorer **monta il backup** contenente il database SQL Server da ripristinare.
- Il software **pubblica il database** direttamente dai file montati, rendendolo accessibile come database temporaneo sull'istanza di SQL Server di destinazione.
- Mentre il database temporaneo è in uso, Veeam Explorer **reindirizza le query utente** a questo database, garantendo che gli utenti possano continuare ad accedere e lavorare con i dati.
- In background, Veeam **esegue un ripristino completo del database**, trasferendo i dati dal database temporaneo alla posizione originale del database.
- Una volta completato il ripristino completo del database, Veeam Explorer **riporta le query dell'utente al database originale** e rimuove il database temporaneo.

Ripristinare il database SQL Server con Veeam Explorer Instant Recovery

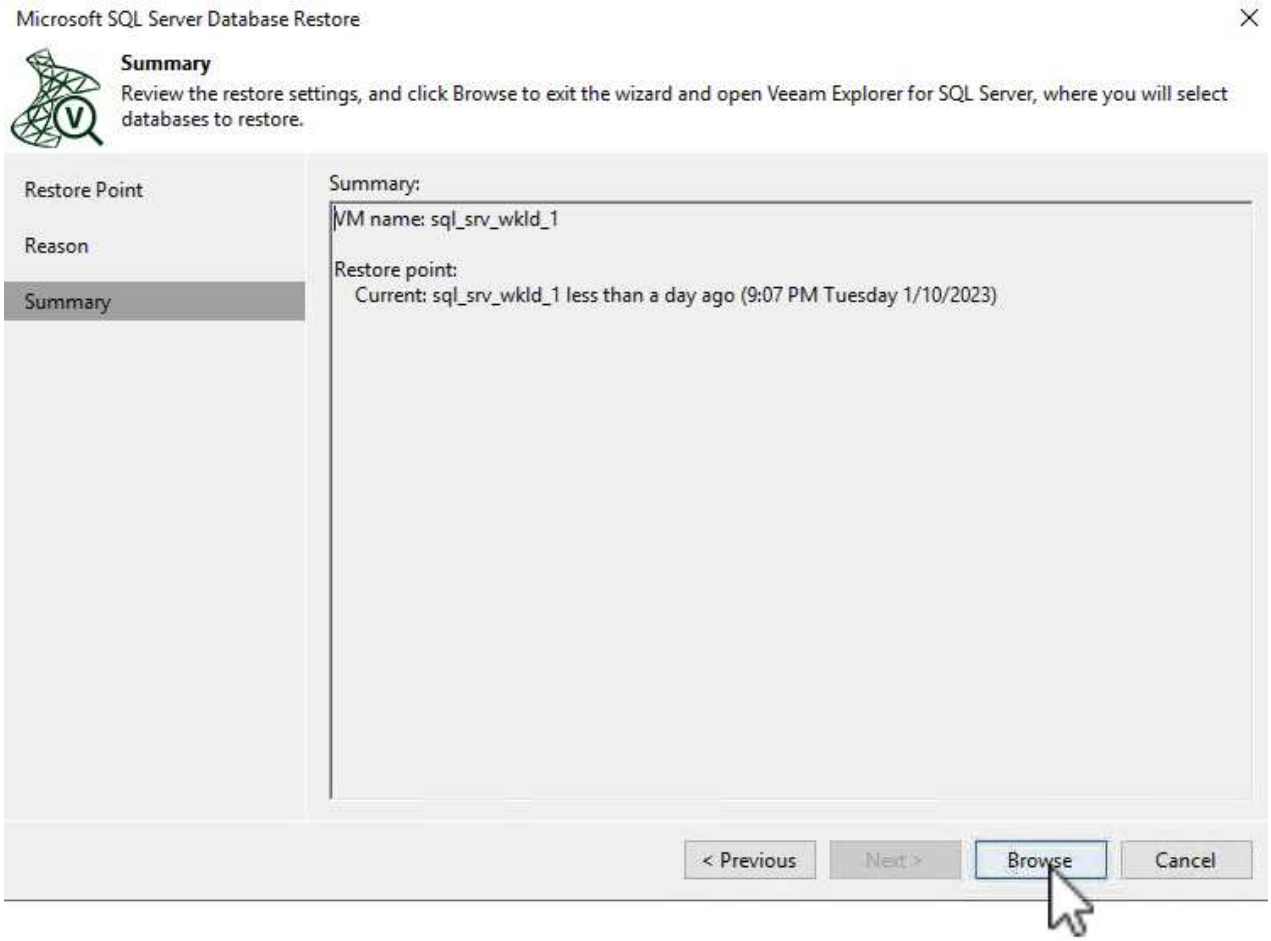
1. Nella console di backup e replica di Veeam, accedere all'elenco dei backup di SQL Server, fare clic con il pulsante destro del mouse su un server e selezionare **Restore application ITEMS** (Ripristina elementi dell'applicazione), quindi **Microsoft SQL Server Databases…** (Database Microsoft SQL Server…).



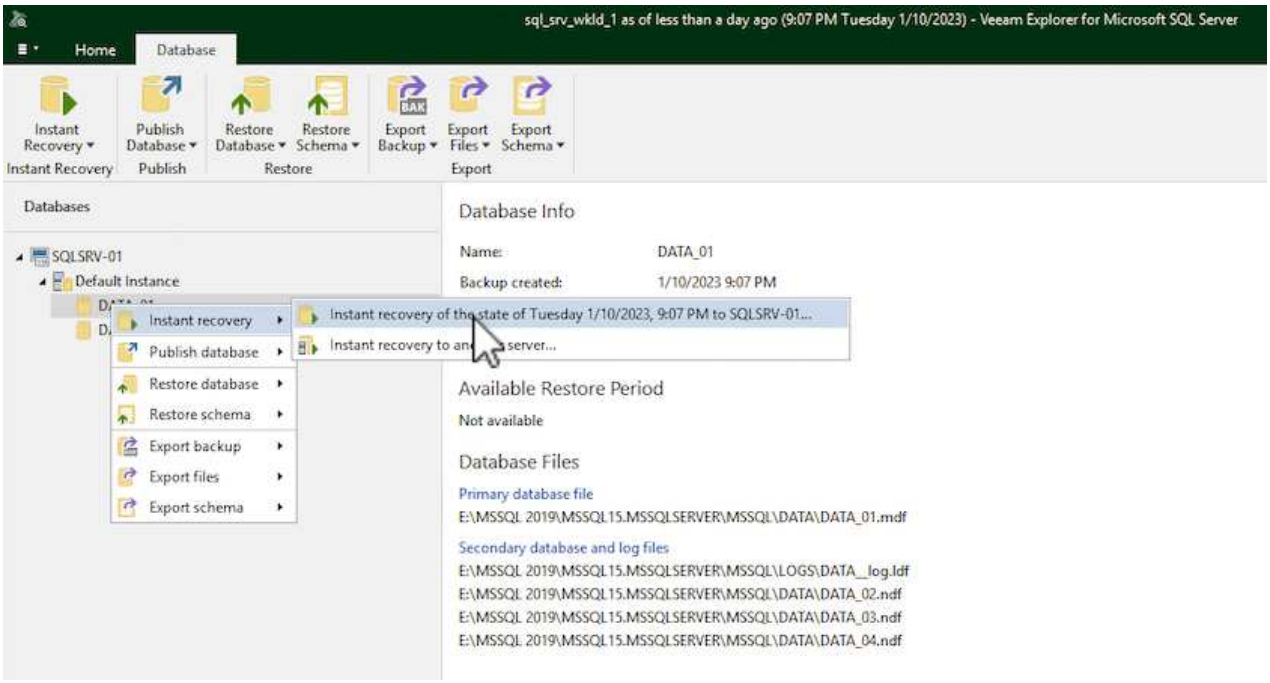
2. Nella finestra Ripristino guidato database di Microsoft SQL Server, selezionare un punto di ripristino dall'elenco e fare clic su **Avanti**.



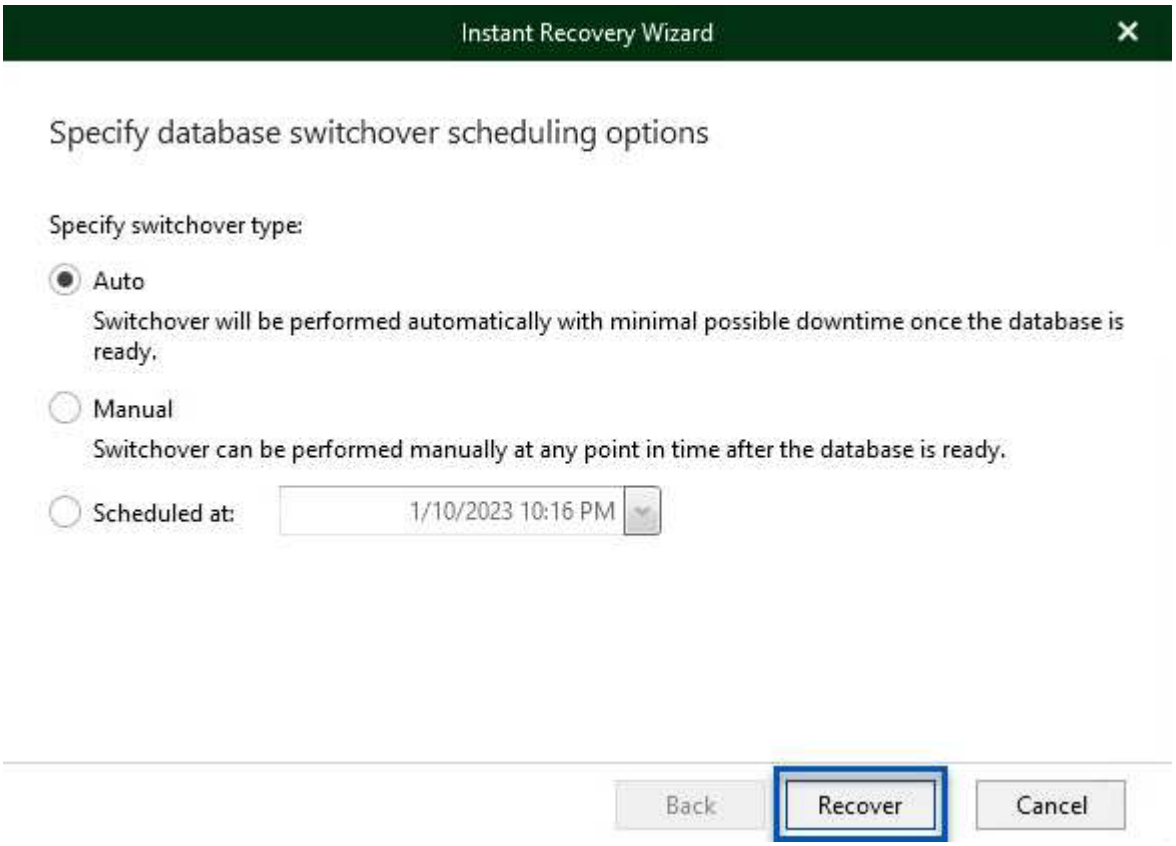
3. Inserire un valore di **Restore Reason** (motivo ripristino), se desiderato, quindi, nella pagina Summary (Riepilogo), fare clic sul pulsante **Browse** (Sfoglia) per avviare Veeam Explorer per Microsoft SQL Server.



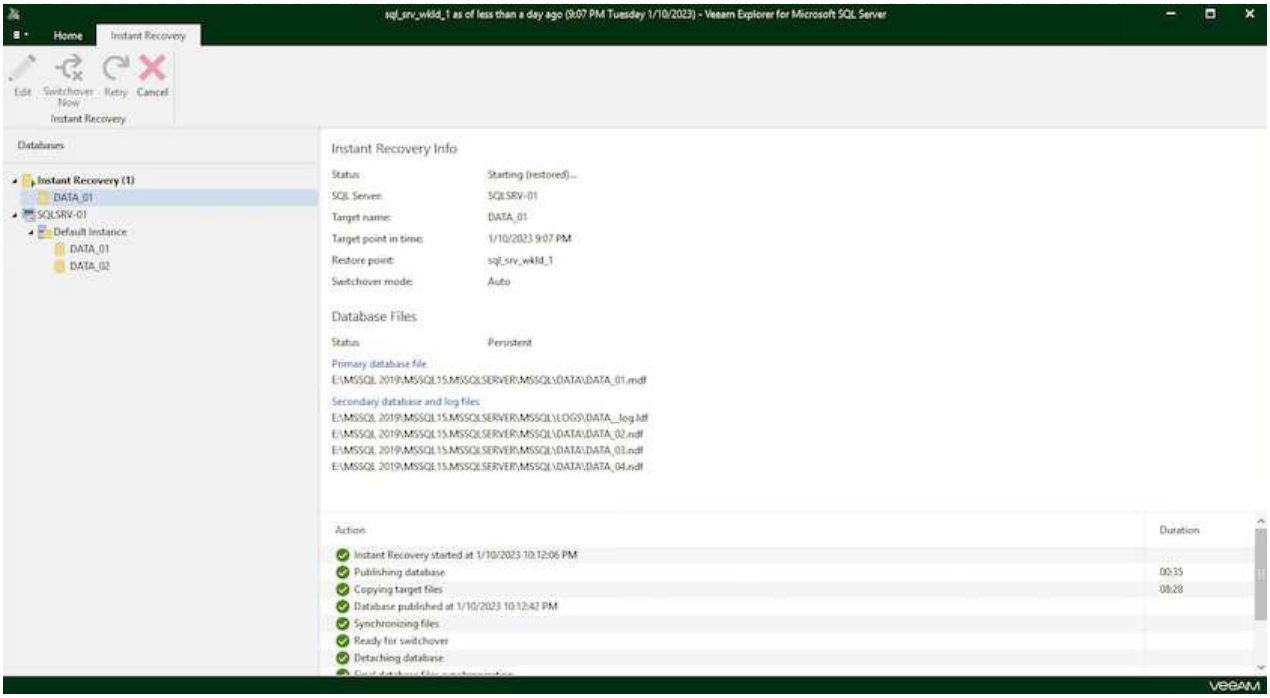
4. In Veeam Explorer espandere l'elenco delle istanze di database, fare clic con il pulsante destro del mouse e selezionare **Instant Recovery**, quindi il punto di ripristino specifico su cui eseguire il ripristino.



5. Nella procedura guidata di ripristino istantaneo, specificare il tipo di switchover. Questo può avvenire automaticamente con tempi di inattività minimi, manualmente o in un momento specifico. Quindi fare clic sul pulsante **Recover** (Ripristina) per avviare il processo di ripristino.



6. Il processo di ripristino può essere monitorato da Veeam Explorer.



Per informazioni più dettagliate sull'esecuzione delle operazioni di ripristino di SQL Server con Veeam Explorer, consultare la sezione Microsoft SQL Server nella "Guida utente di Veeeam Explorers".

Ripristinare i database Oracle con Veeam Explorer

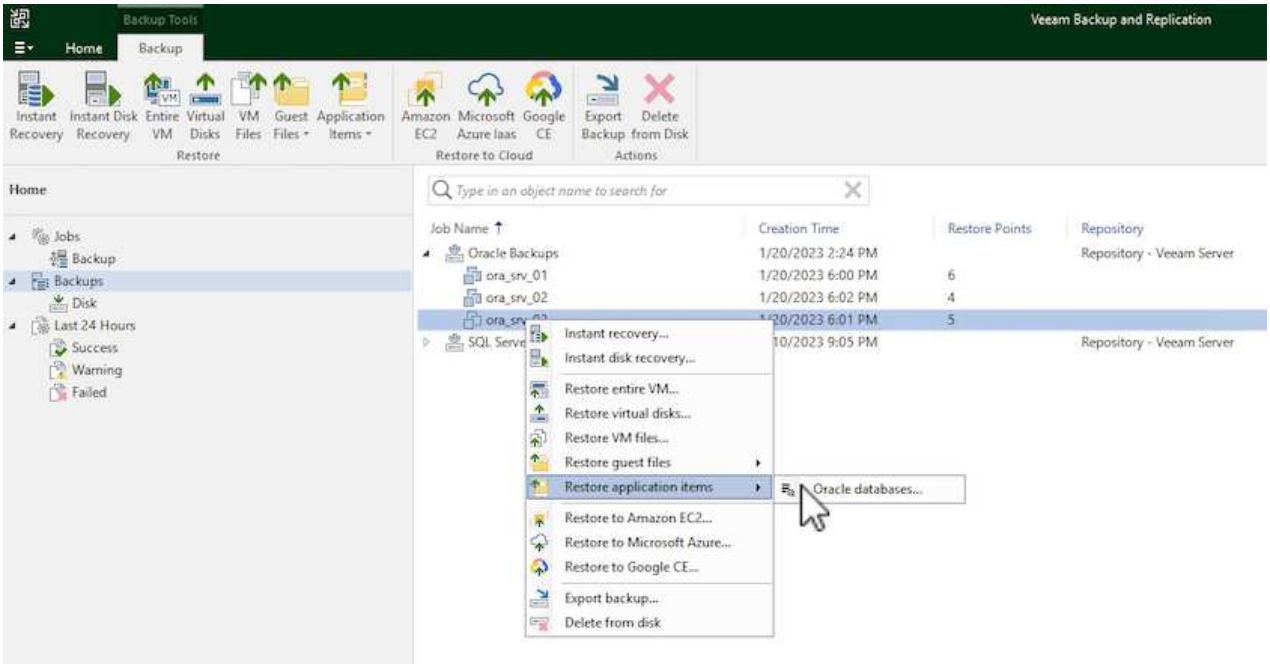
Veeeam Explorer per database Oracle offre la possibilità di eseguire un ripristino standard del database Oracle o un ripristino ininterrotto utilizzando Instant Recovery. Supporta inoltre la pubblicazione di database per un accesso rapido, il ripristino dei database Data Guard e i ripristini dai backup RMAN.

Per informazioni più dettagliate sull'esecuzione delle operazioni di ripristino del database Oracle con Veeam Explorer, fare riferimento alla sezione Oracle nella "Guida utente di Veeeam Explorers".

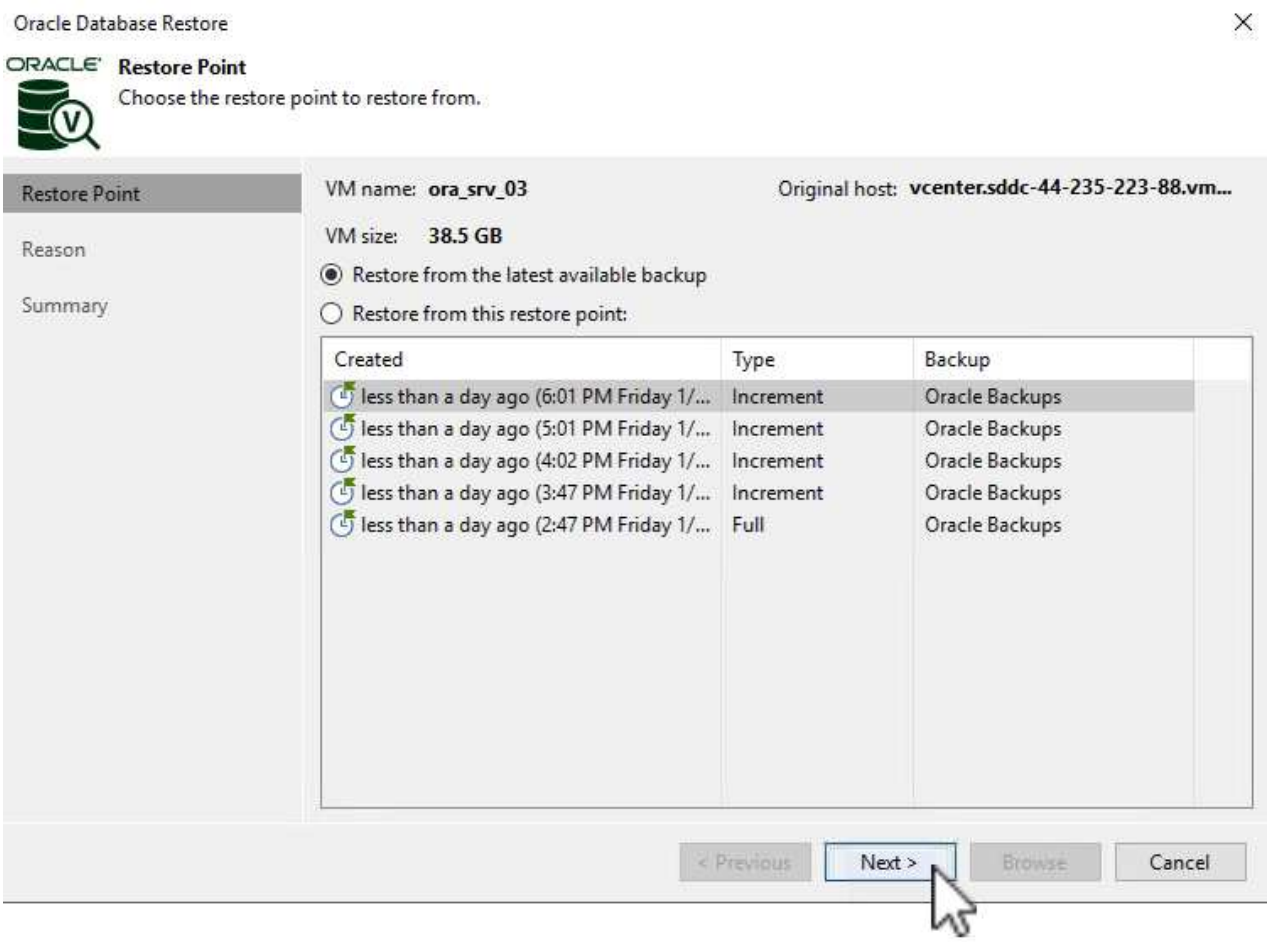
Ripristinare il database Oracle con Veeam Explorer

In questa sezione viene descritto un ripristino del database Oracle su un server diverso utilizzando Veeam Explorer.

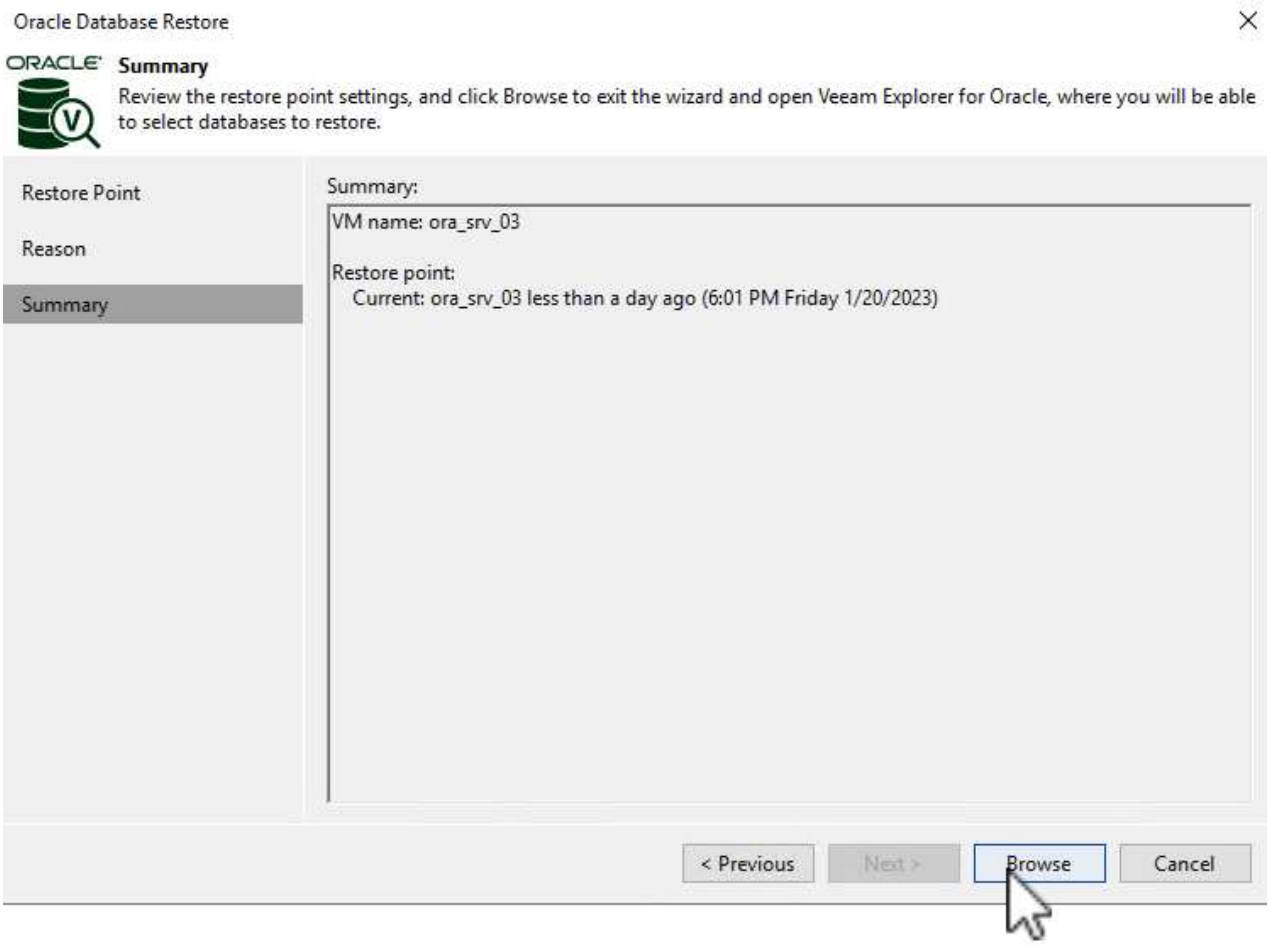
1. Nella console di backup e replica di Veeam, accedere all'elenco dei backup Oracle, fare clic con il pulsante destro del mouse su un server e selezionare **Restore application ITEMS** (Ripristina elementi dell'applicazione), quindi **Oracle Databases…** (Database Oracle…*).



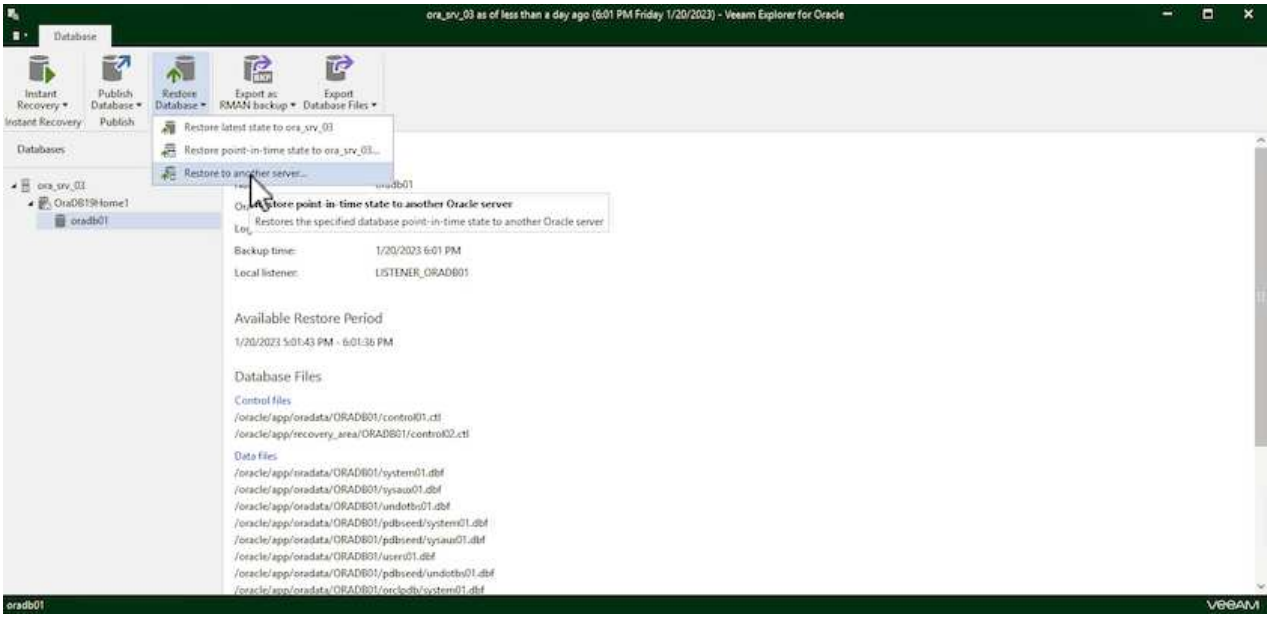
2. In Oracle Database Restore Wizard (Ripristino guidato database Oracle), selezionare un punto di ripristino dall'elenco e fare clic su **Next** (Avanti).



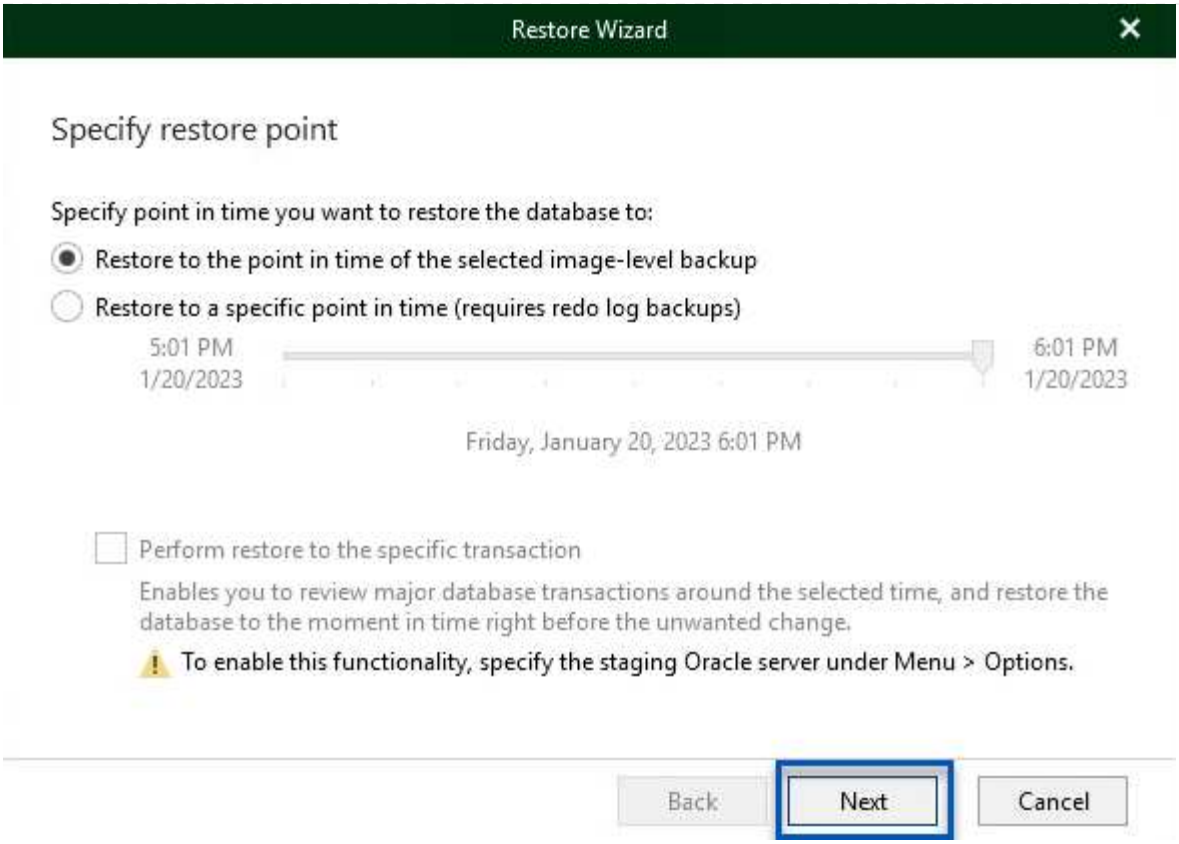
3. Inserire un **Restore Reason** (motivo ripristino), se desiderato, quindi, nella pagina Summary (Riepilogo), fare clic sul pulsante **Browse** (Sfoglia) per avviare Veeam Explorer per Oracle.



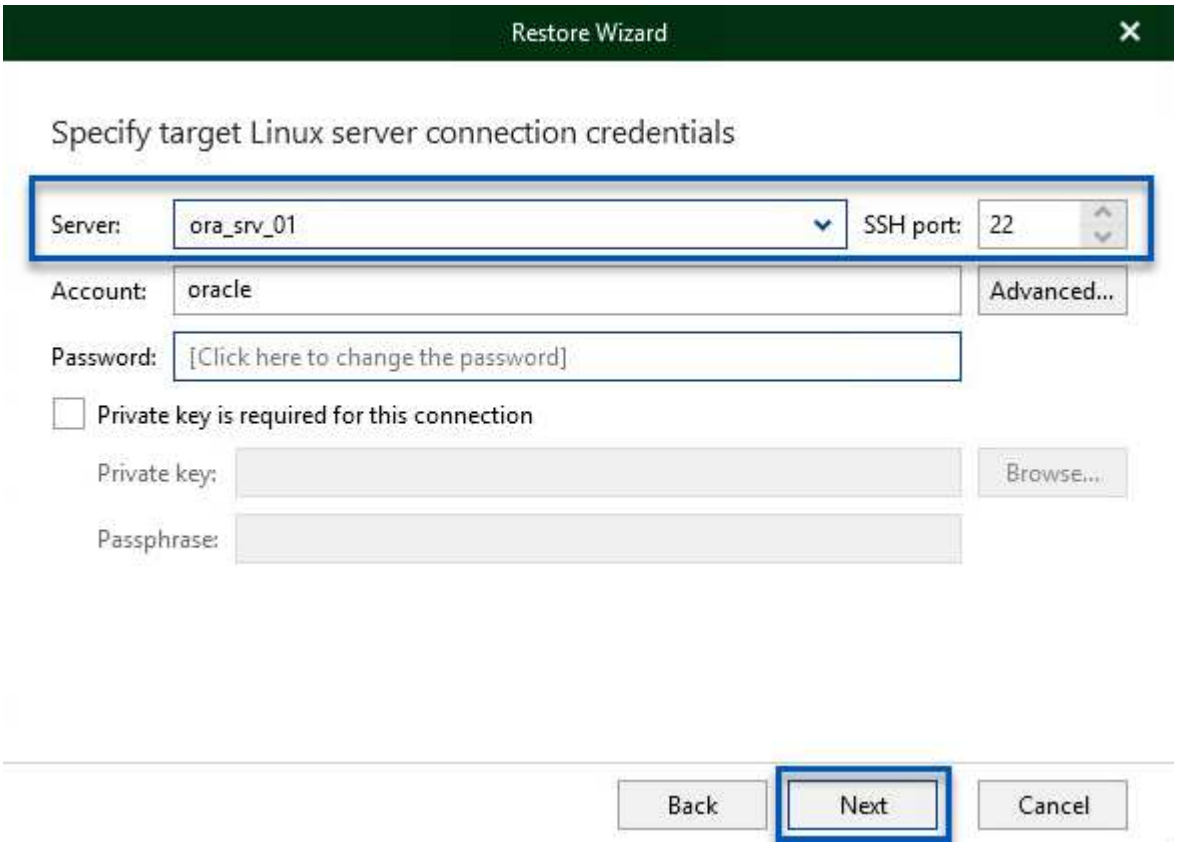
4. In Veeam Explorer espandere l'elenco delle istanze di database, fare clic sul database da ripristinare, quindi selezionare **Ripristina database** dal menu a discesa in alto. Selezionare **Ripristina su un altro server…**.



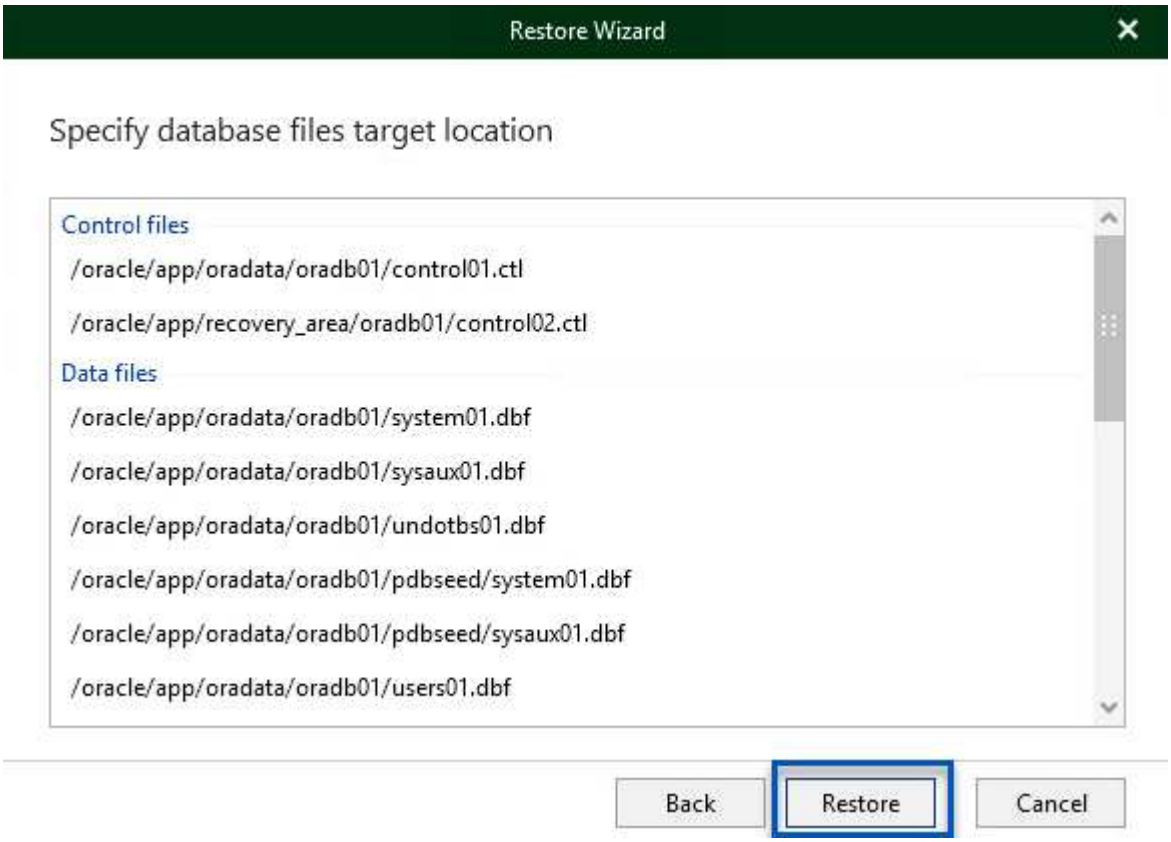
5. Nella procedura guidata di ripristino, specificare il punto di ripristino da cui eseguire il ripristino e fare clic su **Avanti**.



6. Specificare il server di destinazione in cui verrà ripristinato il database e le credenziali dell'account, quindi fare clic su **Avanti**.



7. Infine, specificare il percorso di destinazione dei file di database e fare clic sul pulsante **Restore** per avviare il processo di ripristino.

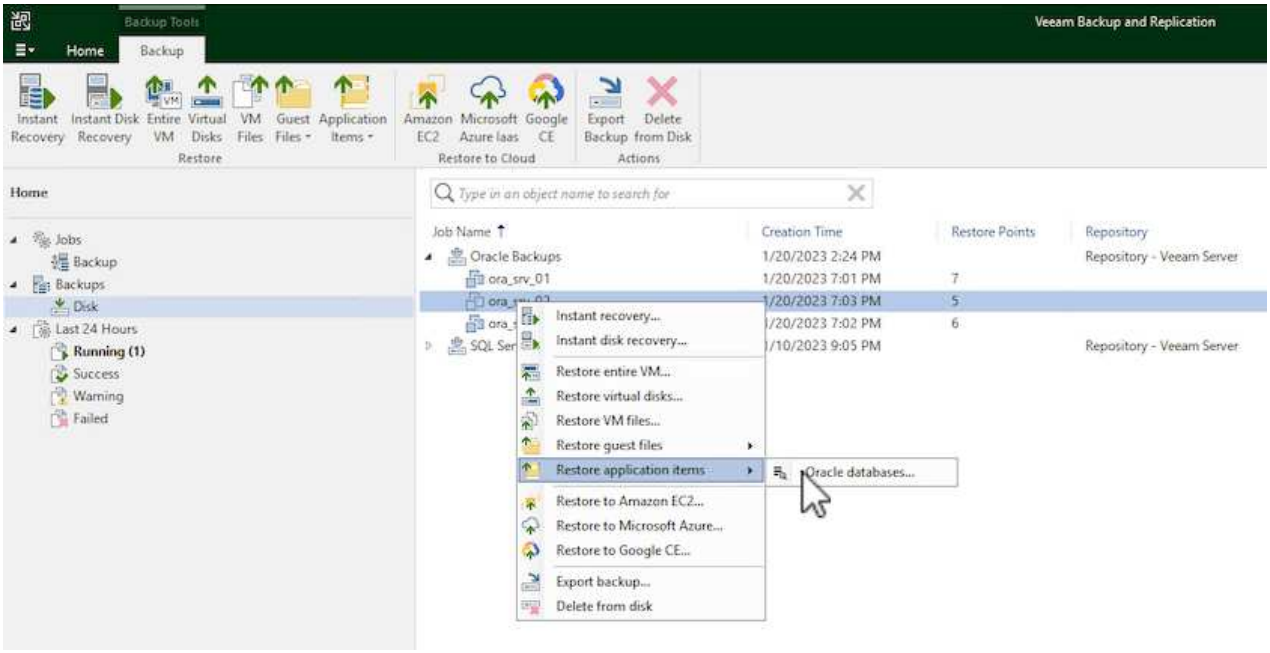


8. Una volta completato il ripristino del database, controllare che il database Oracle venga avviato correttamente sul server.

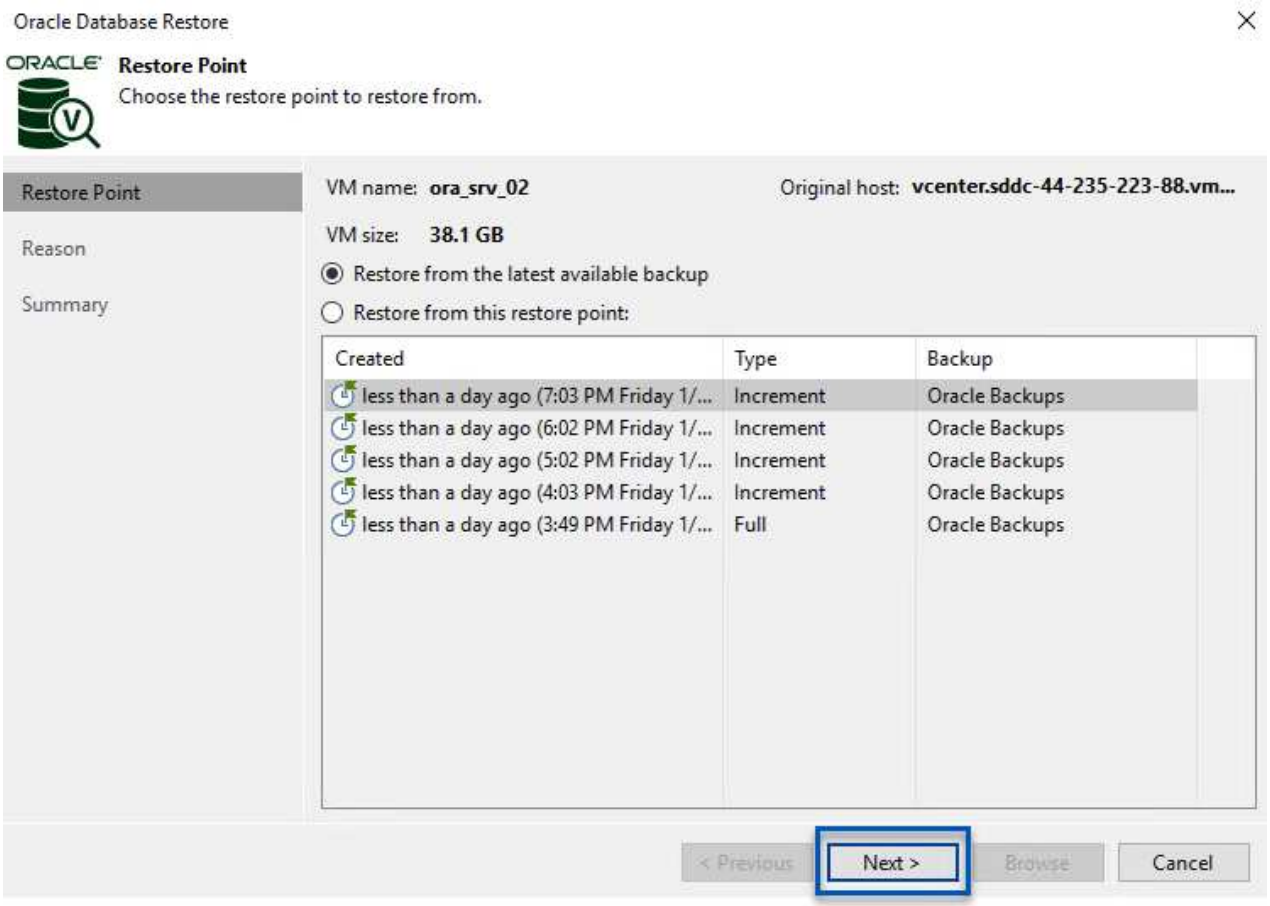
Pubblicare il database Oracle su un server alternativo

In questa sezione viene pubblicato un database su un server alternativo per un accesso rapido senza avviare un ripristino completo.

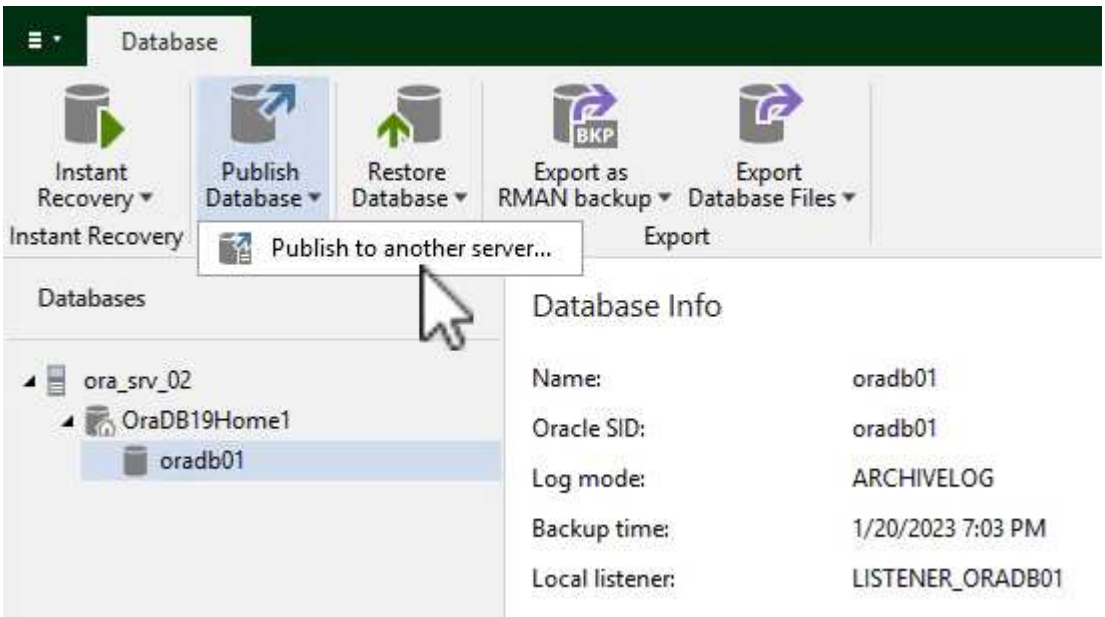
1. Nella console di backup e replica di Veeam, accedere all'elenco dei backup Oracle, fare clic con il pulsante destro del mouse su un server e selezionare **Restore application ITEMS** (Ripristina elementi dell'applicazione), quindi **Oracle Databases…** (Database Oracle…*).



2. In Oracle Database Restore Wizard (Ripristino guidato database Oracle), selezionare un punto di ripristino dall'elenco e fare clic su **Next** (Avanti).

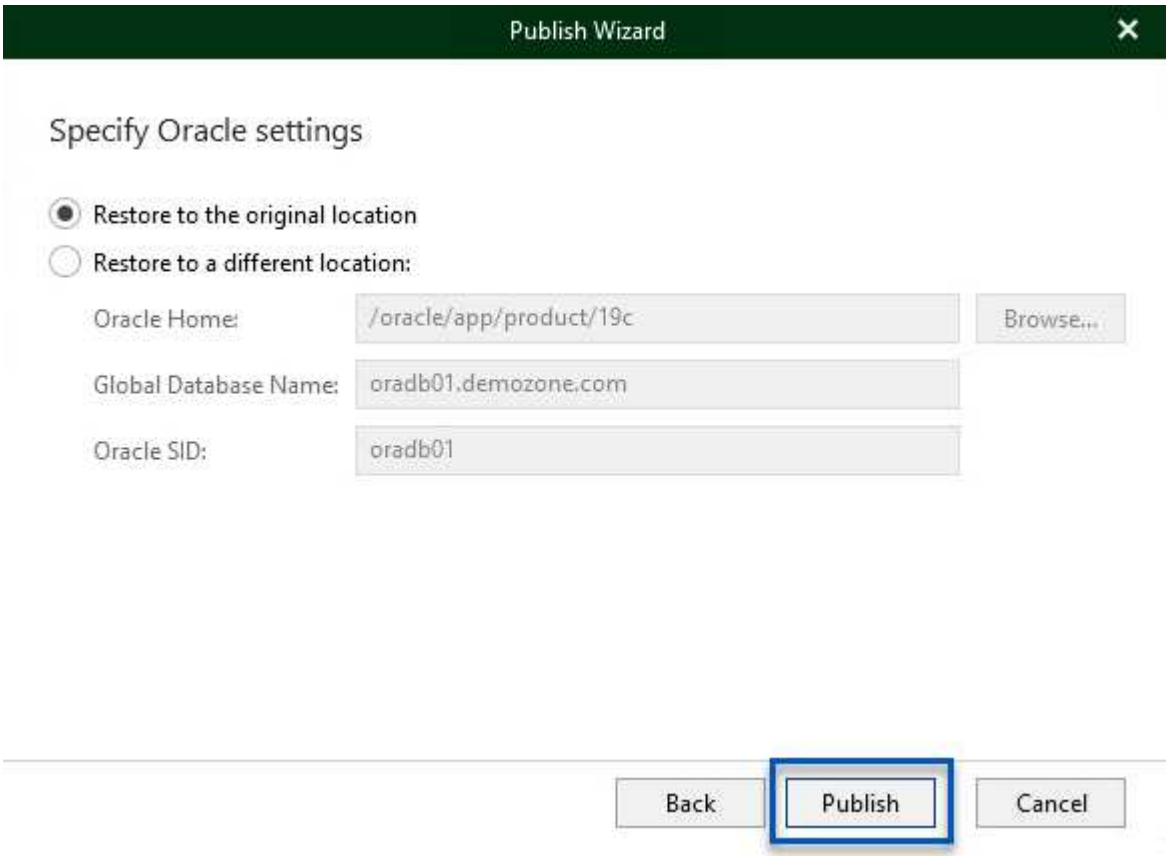


3. Inserire un **Restore Reason** (motivo ripristino), se desiderato, quindi, nella pagina Summary (Riepilogo), fare clic sul pulsante **Browse** (Sfoglia) per avviare Veeam Explorer per Oracle.
4. In Veeam Explorer espandere l'elenco delle istanze di database, fare clic sul database da ripristinare, quindi selezionare **pubblica database** dal menu a discesa in alto, quindi scegliere **pubblica su un altro server…**.



5. Nella Pubblicazione guidata, specificare il punto di ripristino da cui pubblicare il database e fare clic su **Avanti**.

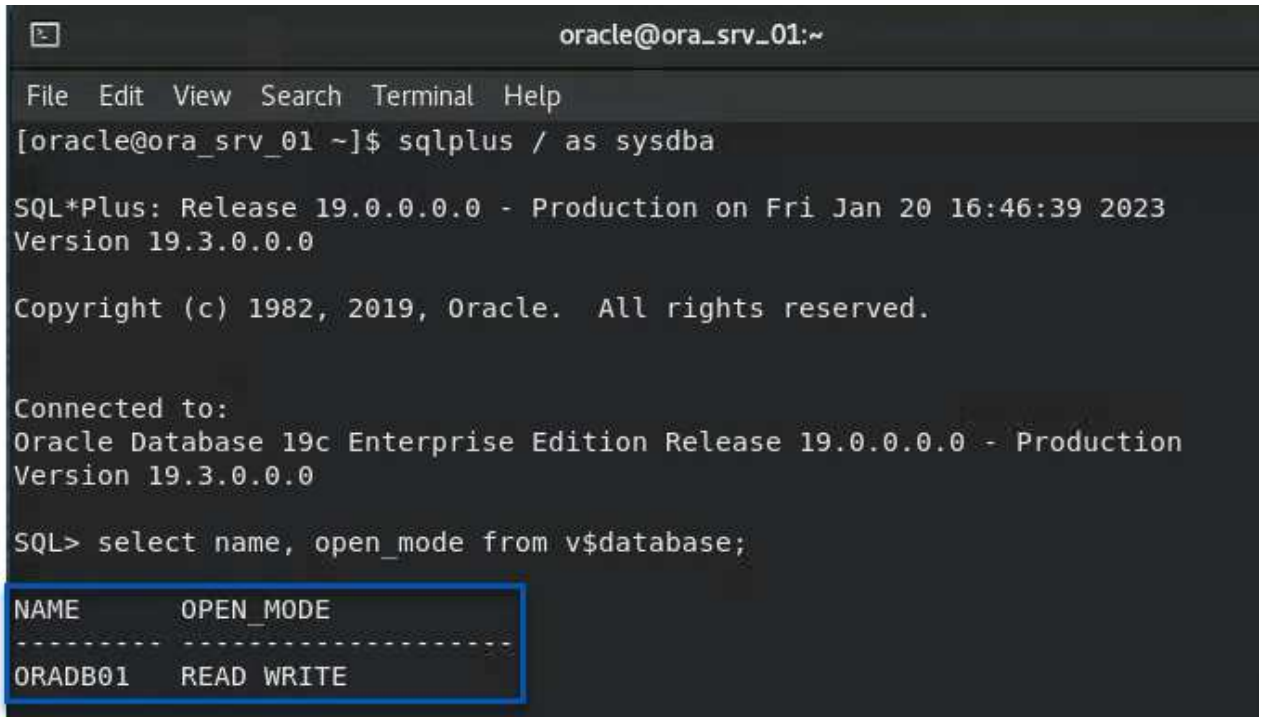
6. Infine, specificare la posizione del file system linux di destinazione e fare clic su **Publish** per avviare il processo di ripristino.



7. Una volta completata la pubblicazione, accedere al server di destinazione ed eseguire i seguenti comandi per assicurarsi che il database sia in esecuzione:

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



Conclusione

VMware Cloud è una potente piattaforma per l'esecuzione di applicazioni business-critical e l'archiviazione di dati sensibili. Una soluzione sicura per la protezione dei dati è essenziale per le aziende che si affidano a VMware Cloud per garantire la continuità del business e contribuire alla protezione dalle minacce informatiche e dalla perdita di dati. Scegliendo una soluzione di protezione dei dati affidabile e solida, le aziende possono essere sicure che i loro dati critici siano sicuri e sicuri, indipendentemente da cosa.

Il caso di utilizzo presentato in questa documentazione si concentra su tecnologie di data Protection comprovate che evidenziano l'integrazione tra NetApp, VMware e Veeeam. FSX per ONTAP è supportato come datastore NFS supplementari per VMware Cloud in AWS e viene utilizzato per tutti i dati delle macchine virtuali e delle applicazioni. Veeam Backup & Replication è una soluzione completa per la protezione dei dati progettata per aiutare le aziende a migliorare, automatizzare e ottimizzare i processi di backup e recovery. Veeam viene utilizzato insieme ai volumi target di backup iSCSI, ospitati su FSX per ONTAP, per fornire una soluzione di protezione dei dati sicura e facile da gestire per i dati applicativi residenti in VMware Cloud.

Ulteriori informazioni

Per ulteriori informazioni sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Guida utente di FSX per ONTAP"
- "Documentazione tecnica del Centro assistenza Veeam"
- "Supporto di VMware Cloud su AWS. Considerazioni e limitazioni"

TR-4955: Disaster recovery con FSX per ONTAP e VMC (AWS VMware Cloud)

È possibile utilizzare Disaster Recovery Orchestrator (DRO, una soluzione basata su script con interfaccia utente) per ripristinare senza problemi i carichi di lavoro replicati da on-premise a FSX per ONTAP. DRO automatizza il ripristino dal livello SnapMirror,

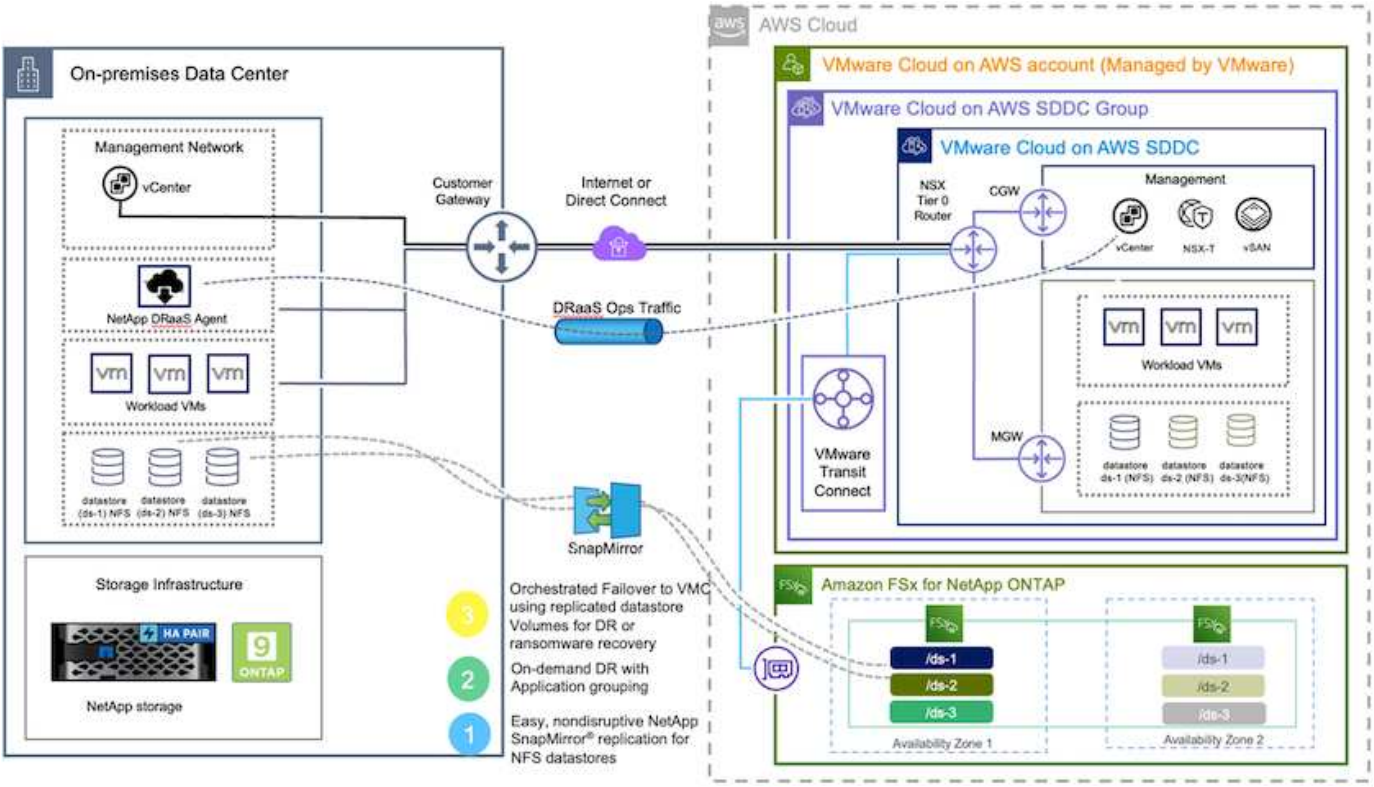
attraverso la registrazione delle macchine virtuali su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzione è inclusa in tutti gli ambienti VMC.

Niyaz Mohamed, NetApp

Panoramica

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di corruzione dei dati (ad esempio ransomware). Con la tecnologia NetApp SnapMirror, i carichi di lavoro VMware on-premise possono essere replicati su FSX per ONTAP in esecuzione in AWS.

È possibile utilizzare Disaster Recovery Orchestrator (DRO, una soluzione basata su script con interfaccia utente) per ripristinare senza problemi i carichi di lavoro replicati da on-premise a FSX per ONTAP. DRO automatizza il ripristino dal livello SnapMirror, attraverso la registrazione delle macchine virtuali su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzione è inclusa in tutti gli ambienti VMC.



Per iniziare

Implementare e configurare VMware Cloud su AWS

"VMware Cloud su AWS" Offre un'esperienza nativa del cloud per i carichi di lavoro basati su VMware nell'ecosistema AWS. Ogni VMware Software-Defined Data Center (SDDC) viene eseguito in un Amazon Virtual Private Cloud (VPC) e fornisce uno stack VMware completo (incluso vCenter Server), networking software-defined NSX-T, storage vSAN software-defined e uno o più host ESXi che forniscono risorse di calcolo e storage ai carichi di lavoro. Per configurare un ambiente VMC su AWS, seguire questa procedura "collegamento". È possibile utilizzare anche un cluster di spie pilota per scopi di DR.

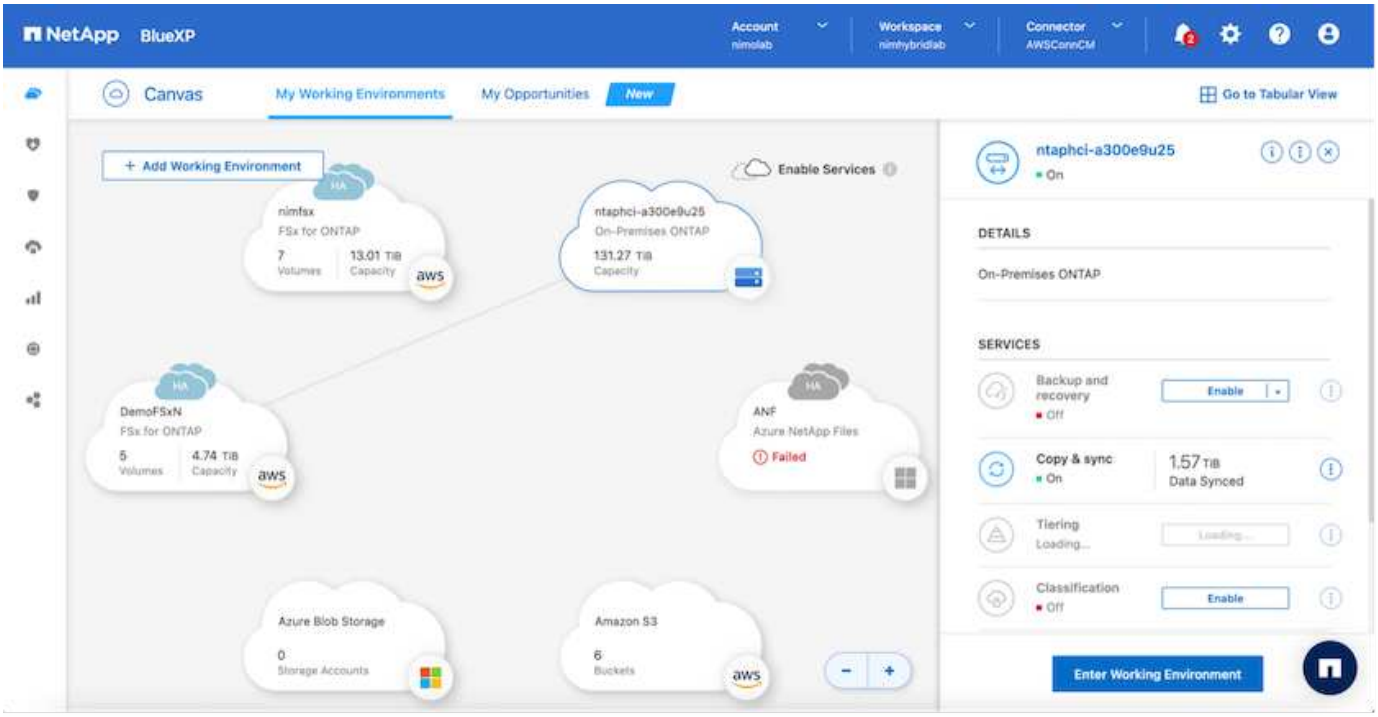
Nella versione iniziale, DRO supporta un cluster pilota-light esistente. La creazione di SDDC on-demand sarà disponibile in una release imminente.

Provisioning e configurazione di FSX per ONTAP

Amazon FSX per NetApp ONTAP è un servizio completamente gestito che offre un file storage altamente affidabile, scalabile, dalle performance elevate e ricco di funzionalità, basato sul popolare file system ONTAP di NetApp. Seguire questa procedura "collegamento" Per eseguire il provisioning e la configurazione di FSX per ONTAP.

Implementare e configurare SnapMirror in FSX per ONTAP

Il passaggio successivo consiste nell'utilizzare NetApp BlueXP e individuare FSX per ONTAP su istanza AWS e replicare i volumi datastore desiderati da un ambiente on-premise a FSX per ONTAP con la frequenza appropriata e la conservazione delle copie Snapshot di NetApp:



Seguire la procedura descritta in questo collegamento per configurare BlueXP. È inoltre possibile utilizzare l'interfaccia utente di NetApp ONTAP per pianificare la replica seguendo questo collegamento.

Una relazione SnapMirror è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a utilizzare DRO, utilizzare il sistema operativo Ubuntu su un'istanza EC2 o una macchina virtuale designata per assicurarsi di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti

- Assicurarsi che sia presente la connettività con i sistemi vCenter e storage di origine e di destinazione.
- Se si utilizzano i nomi DNS, la risoluzione DNS deve essere effettiva. In caso contrario, utilizzare gli indirizzi IP per vCenter e sistemi storage.
- Creare un utente con permessi root. È anche possibile utilizzare sudo con un'istanza EC2.

Requisiti del sistema operativo

- Ubuntu 20.04 (LTS) con almeno 2 GB e 4 vCPU
- I seguenti pacchetti devono essere installati sulla macchina virtuale dell'agente designata:
  - Docker
  - Docker-Componi
  - JQ

Modificare le autorizzazioni su `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

Il `deploy.sh` lo script esegue tutti i prerequisiti richiesti.

Installare il pacchetto

1. Scaricare il pacchetto di installazione sulla macchina virtuale designata:

```
git clone https://github.com/NetApp/DRO-AWS.git
```

   L'agente può essere installato on-premise o all'interno di un VPC AWS.

2. Decomprimere il pacchetto, eseguire lo script di implementazione e immettere l'IP host (ad esempio, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Accedere alla directory ed eseguire lo script di distribuzione come segue:

```
sudo sh deploy.sh
```

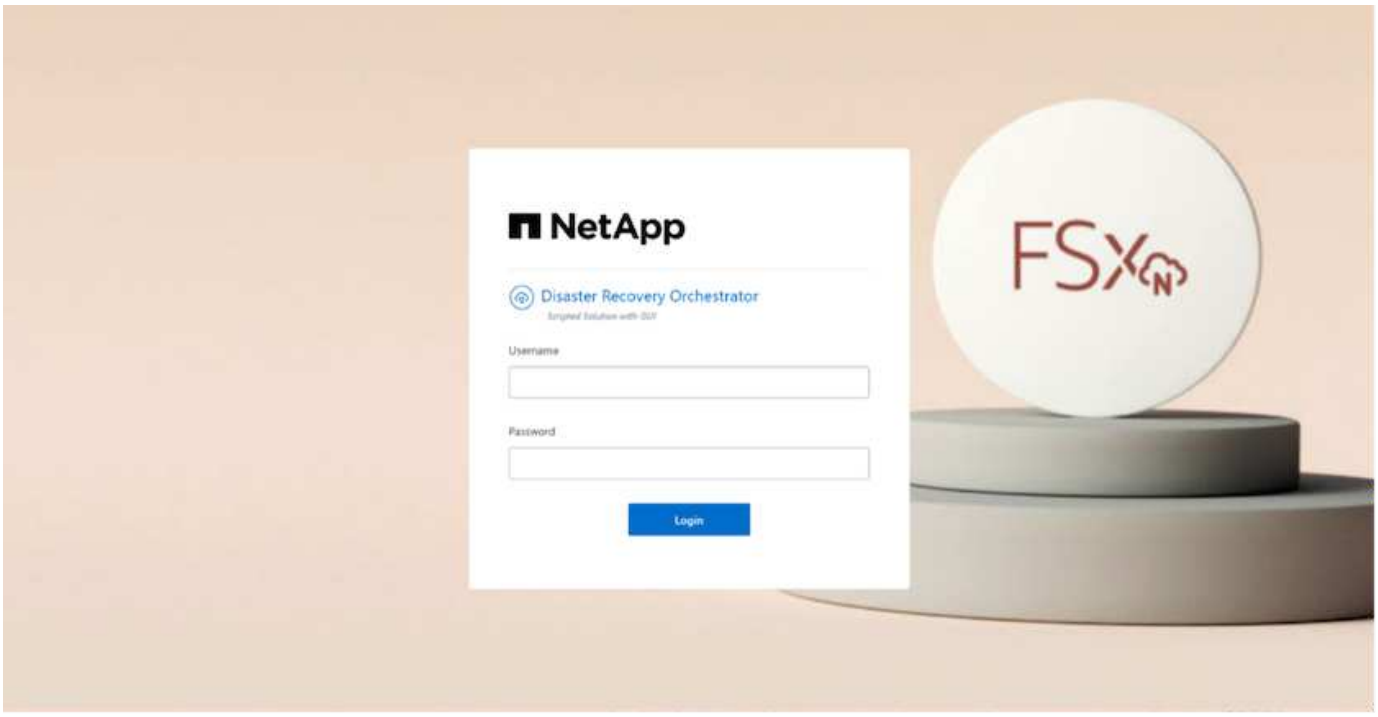
4. Accedere all'interfaccia utente utilizzando:

```
https://<host-ip-address>
```

   con le seguenti credenziali predefinite:

```
Username: admin
Password: admin
```

   La password può essere modificata utilizzando l'opzione "Change Password" (Modifica password).



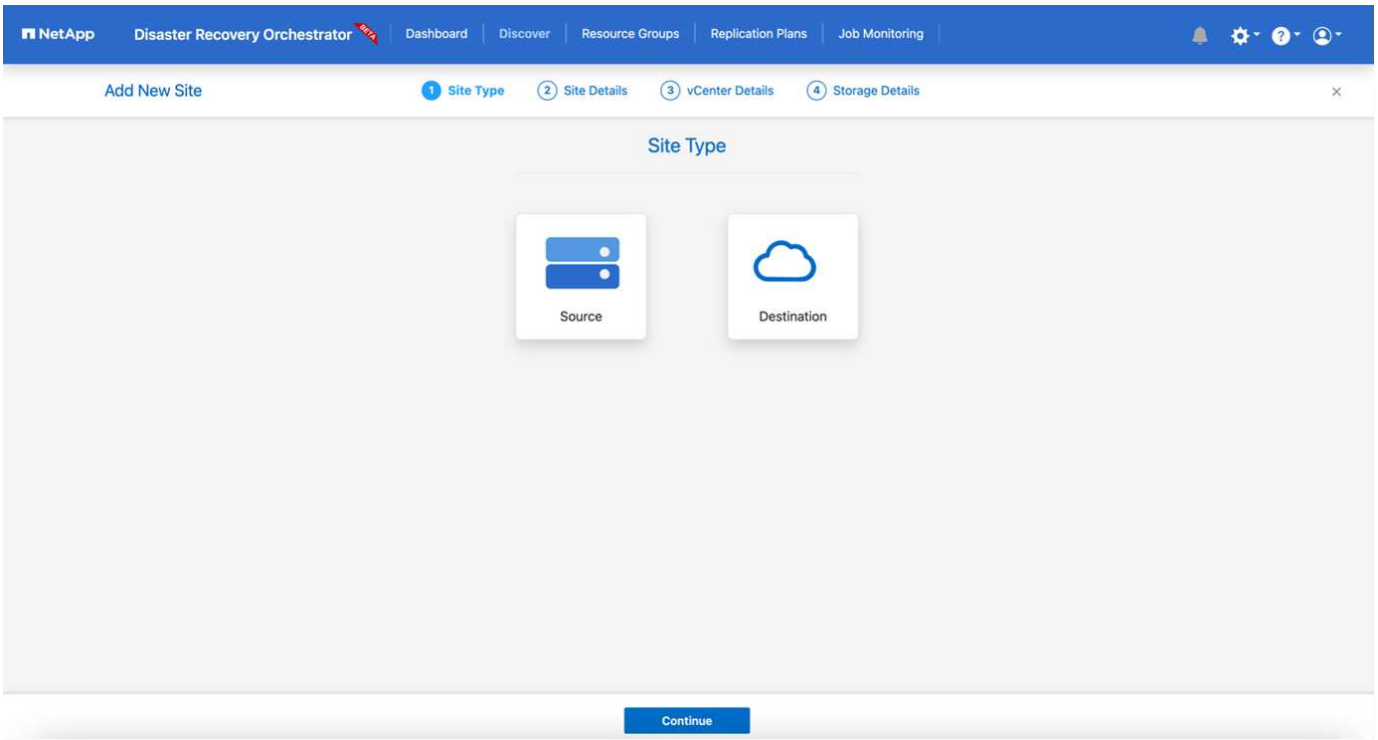
Configurazione DRO

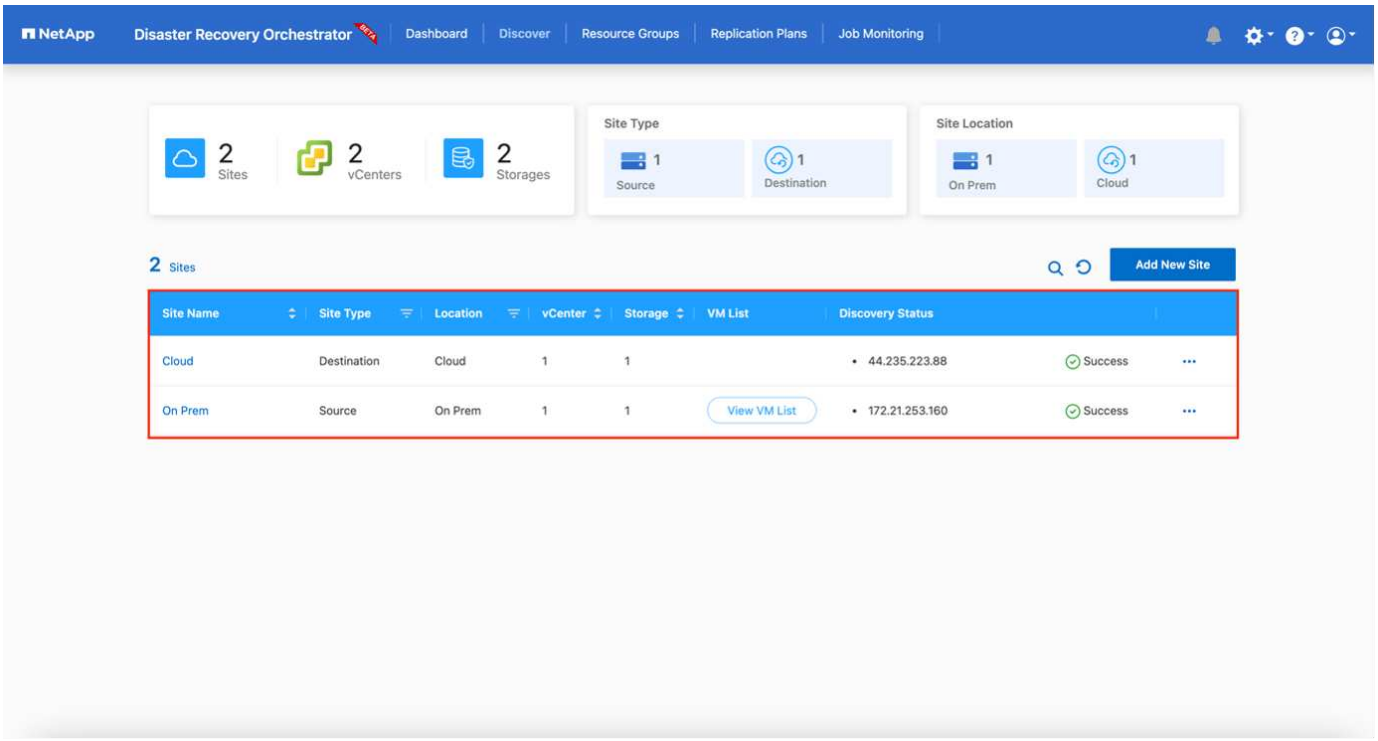
Dopo aver configurato correttamente FSX per ONTAP e VMC, è possibile iniziare a configurare DRO per automatizzare il ripristino dei carichi di lavoro on-premise su VMC utilizzando le copie SnapMirror di sola lettura su FSX per ONTAP.

NetApp consiglia di implementare l'agente DRO in AWS e anche sullo stesso VPC in cui viene implementato FSX per ONTAP (può anche essere collegato in modo peer), In modo che l'agente DRO possa comunicare attraverso la rete con i componenti on-premise e con le risorse FSX per ONTAP e VMC.

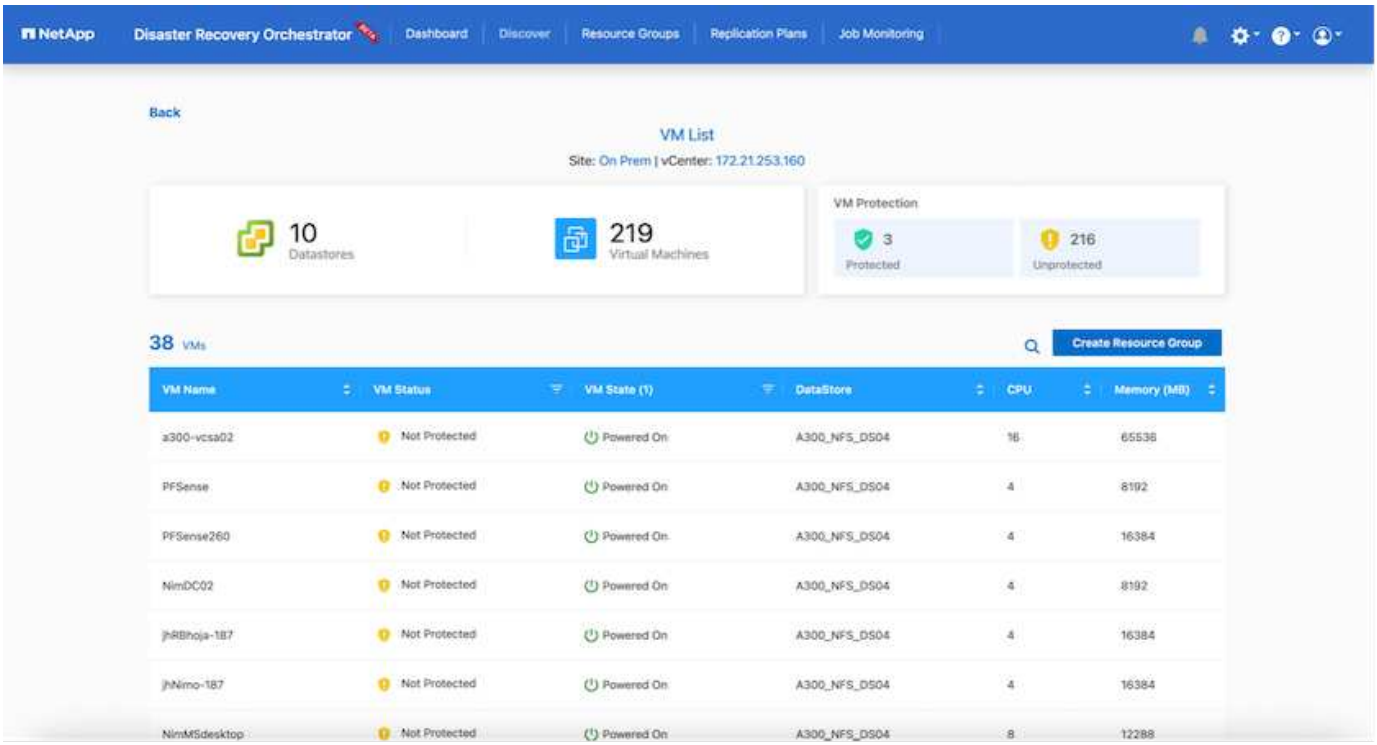
Il primo passo è scoprire e aggiungere le risorse on-premise e cloud (vCenter e storage) a DRO. Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti (admin/admin) e Add Sites (Aggiungi siti). I siti possono essere aggiunti anche utilizzando l'opzione Discover. Aggiungere le seguenti piattaforme:

- On-premise
  - VCenter on-premise
  - Sistema storage ONTAP
- Cloud
  - VMC vCenter
  - FSX per ONTAP





Una volta aggiunto, DRO esegue il rilevamento automatico e visualizza le macchine virtuali con le repliche SnapMirror corrispondenti dallo storage di origine a FSX per ONTAP. DRO rileva automaticamente le reti e i portgroup utilizzati dalle macchine virtuali e li popola.



Il passaggio successivo consiste nel raggruppare le macchine virtuali richieste in gruppi funzionali che fungono da gruppi di risorse.

Raggruppamenti di risorse

Una volta aggiunte le piattaforme, è possibile raggruppare le macchine virtuali da ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di macchine virtuali dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali delle applicazioni che possono essere eseguite al momento del ripristino.

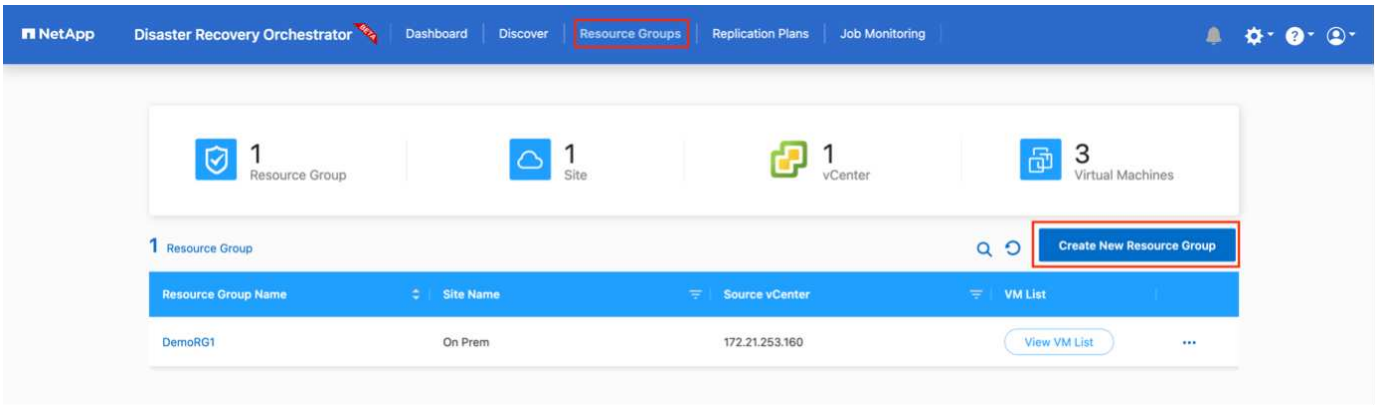
Per iniziare a creare gruppi di risorse, attenersi alla seguente procedura:

1. Accedere a **gruppi di risorse** e fare clic su **Crea nuovo gruppo di risorse**.
2. In **nuovo gruppo di risorse**, selezionare il sito di origine dal menu a discesa e fare clic su **Crea**.
3. Fornire **Dettagli gruppo di risorse** e fare clic su **continua**.
4. Selezionare le macchine virtuali appropriate utilizzando l'opzione di ricerca.
5. Selezionare l'ordine di avvio e il ritardo di avvio (sec) per le macchine virtuali selezionate. Impostare l'ordine della sequenza di accensione selezionando ciascuna macchina virtuale e impostando la relativa priorità. Tre è il valore predefinito per tutte le macchine virtuali.

   Le opzioni sono le seguenti:

   1 – la prima macchina virtuale ad accenderlo 3 – Default 5 – l'ultima macchina virtuale ad accenderlo

6. Fare clic su **Crea gruppo di risorse**.

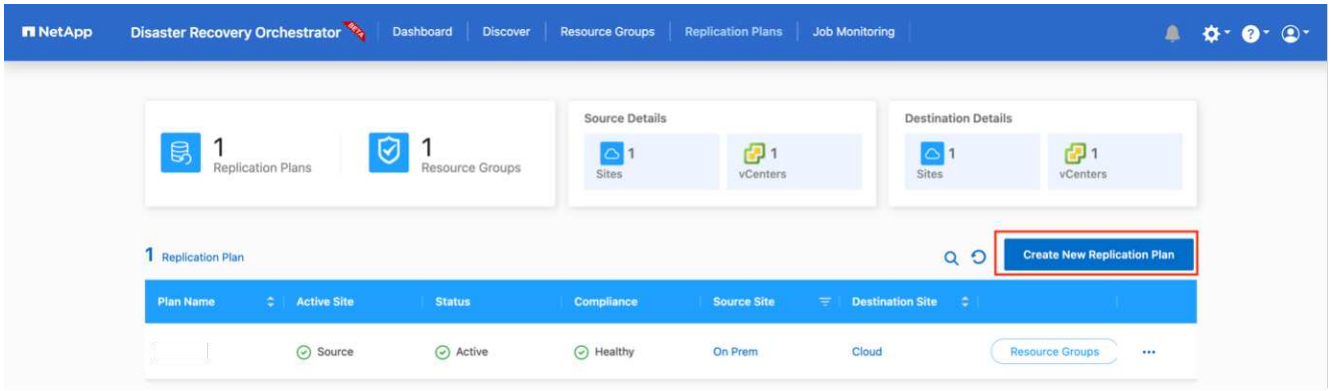


Piani di replica

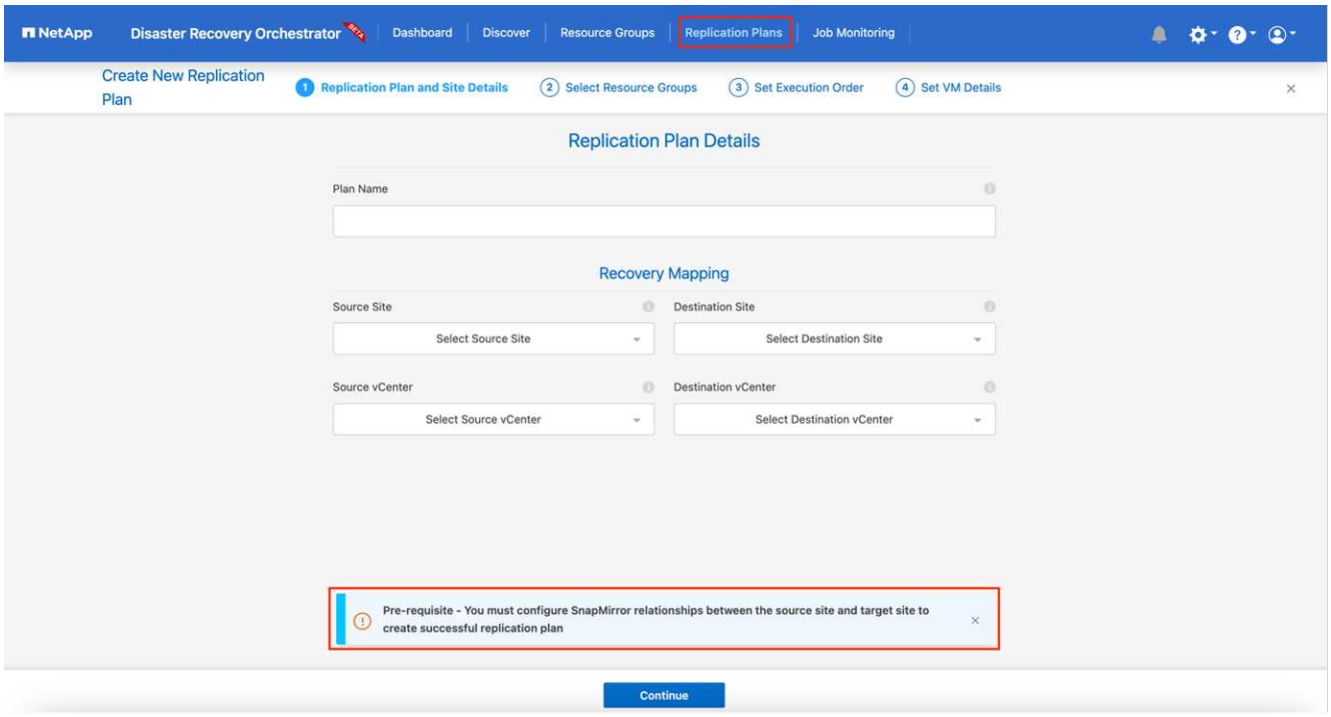
Hai bisogno di un piano per il ripristino delle applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dall'elenco a discesa e scegliere i gruppi di risorse da includere in questo piano, oltre al raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, Tier-1, Tier-2 e così via). Tali piani sono talvolta chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda **Replication Plan** (piano di replica) e fare clic su **New Replication Plan** (nuovo piano di replica).

Per iniziare a creare un piano di replica, attenersi alla seguente procedura:

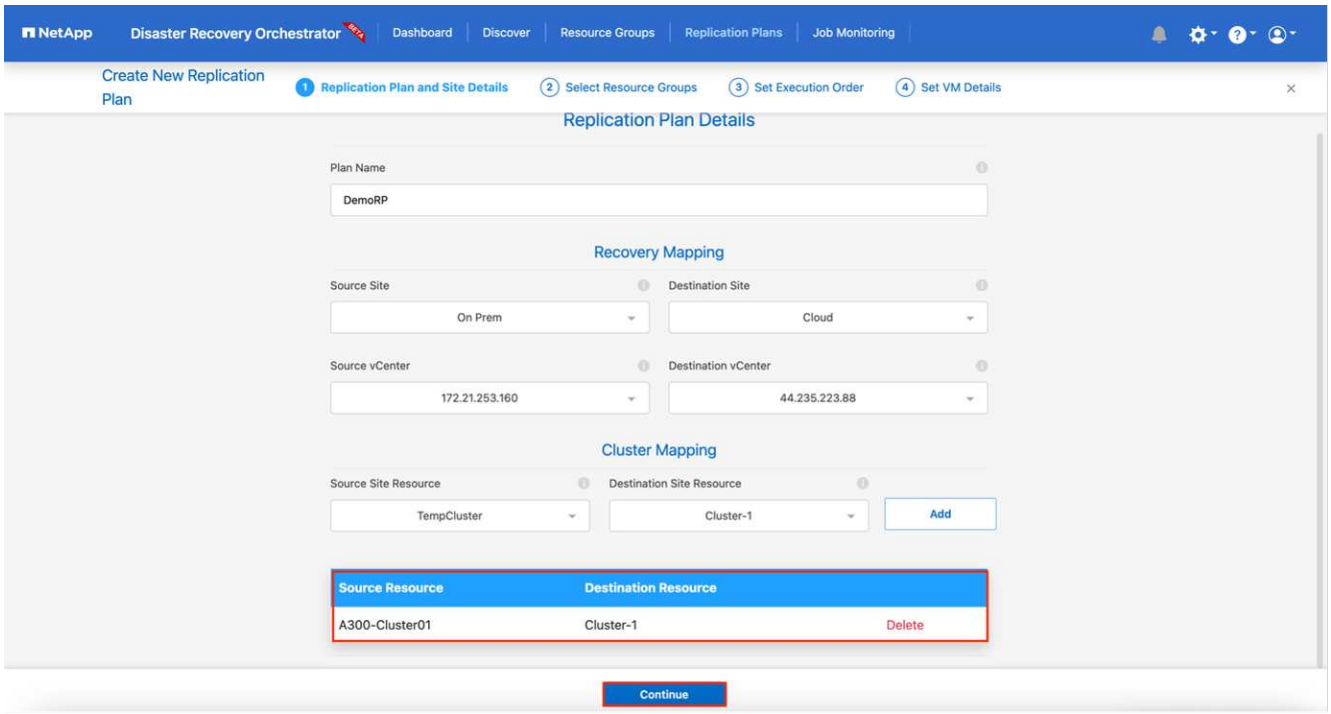
1. Accedere a **Replication Plans** e fare clic su **Create New Replication Plan** (Crea nuovo piano di replica).



2. In **New Replication Plan** (nuovo piano di replica), specificare un nome per il piano e aggiungere i mapping di ripristino selezionando il sito di origine, il vCenter associato, il sito di destinazione e il vCenter associato.

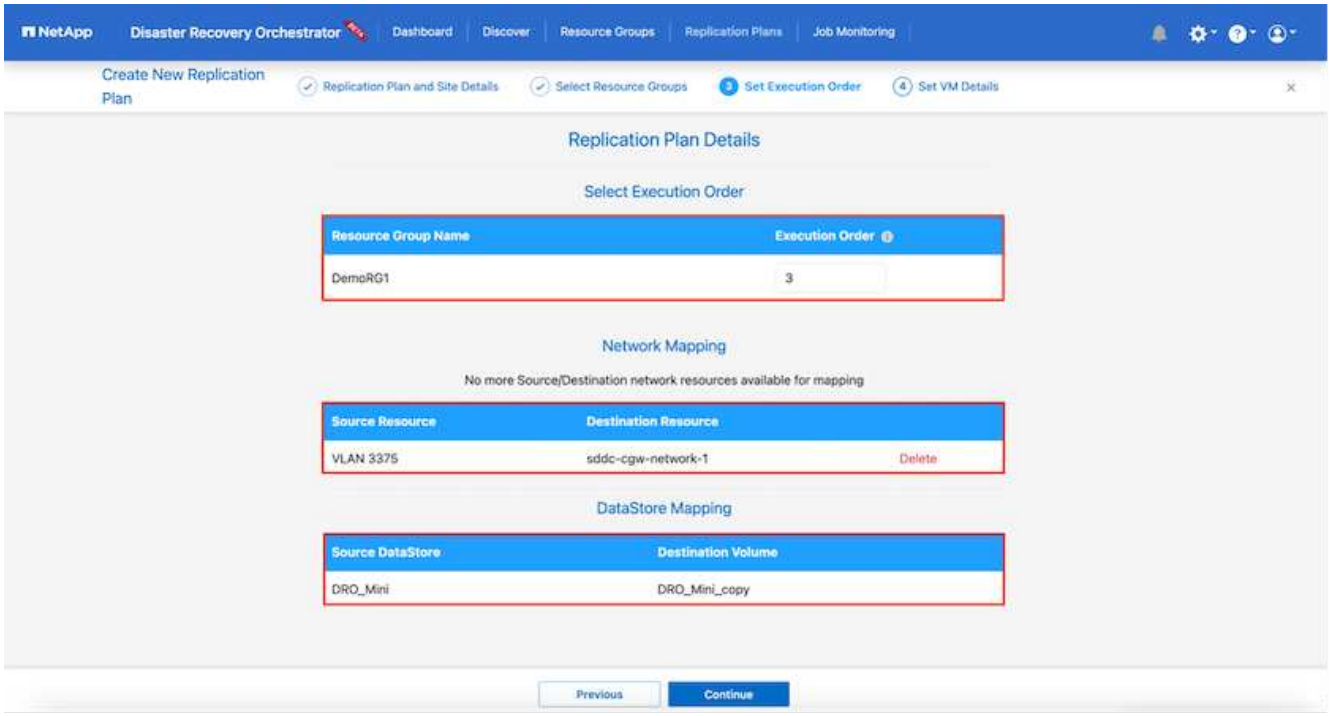


3. Una volta completata la mappatura di ripristino, selezionare la mappatura del cluster.

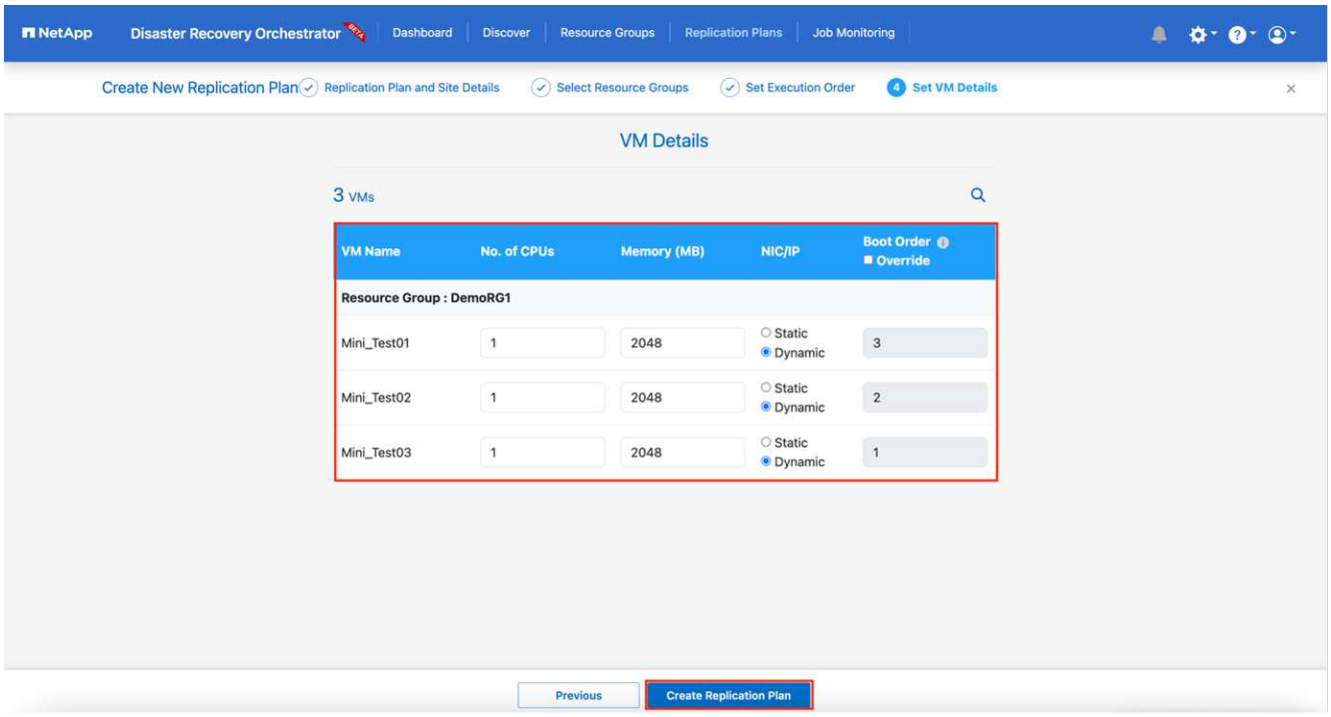


4. Selezionare **Dettagli gruppo di risorse** e fare clic su **continua**.
5. Impostare l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza di operazioni quando esistono più gruppi di risorse.
6. Al termine, selezionare la mappatura di rete per il segmento appropriato. I segmenti devono essere già sottoposti a provisioning all'interno di VMC, quindi selezionare il segmento appropriato per mappare la macchina virtuale.
7. In base alla selezione delle macchine virtuali, i mapping degli archivi dati vengono selezionati automaticamente.

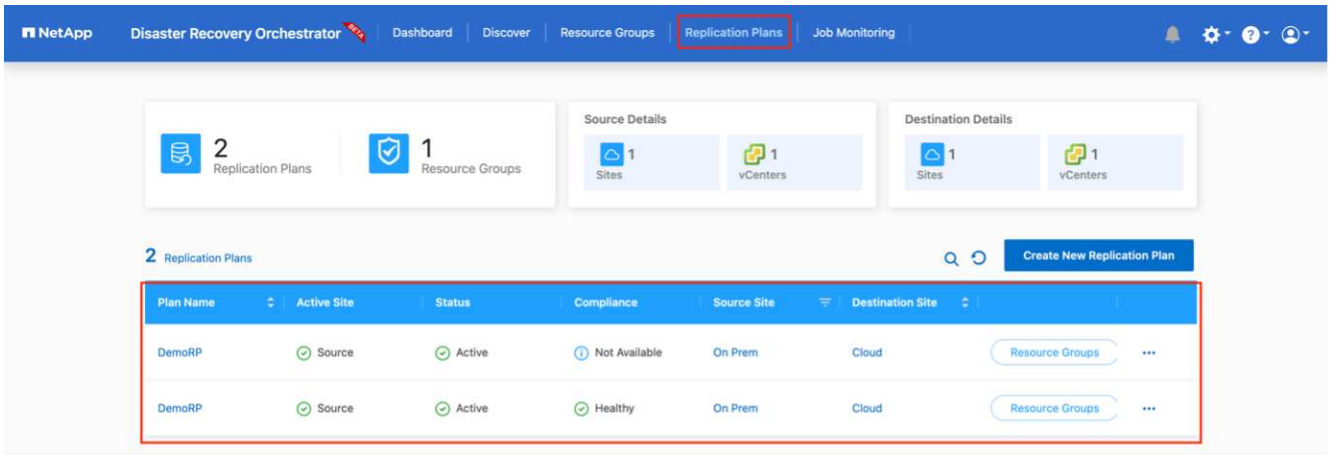
SnapMirror è a livello di volume. Pertanto, tutte le macchine virtuali vengono replicate nella destinazione di replica. Assicurarsi di selezionare tutte le macchine virtuali che fanno parte dell'archivio dati. Se non sono selezionate, vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.



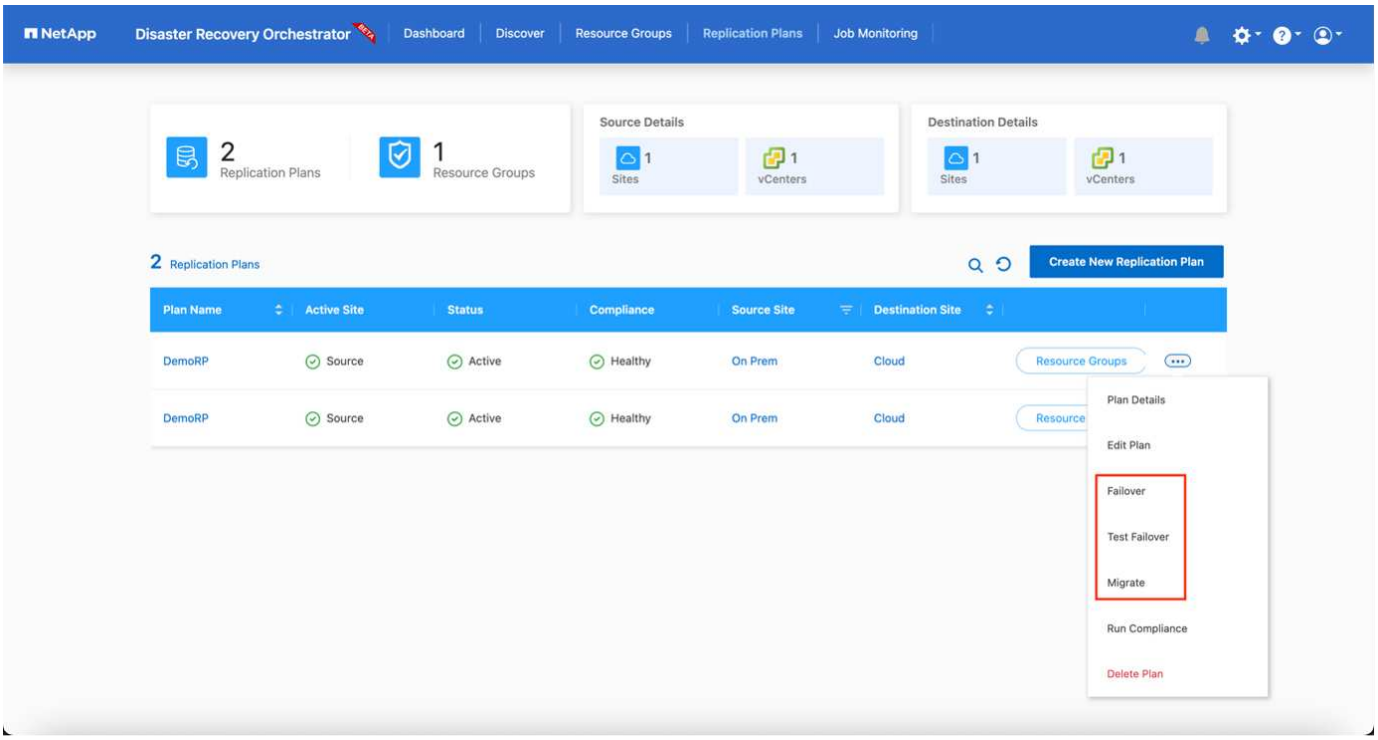
8. In base ai dettagli della macchina virtuale, è possibile ridimensionare i parametri della CPU e della RAM della macchina virtuale; ciò può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o per eseguire test di DR senza dover eseguire il provisioning di un'infrastruttura fisica VMware uno a uno. Inoltre, è possibile modificare l'ordine di avvio e il ritardo di avvio (secondi) per tutte le macchine virtuali selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche da quelle selezionate durante la selezione dell'ordine di avvio del gruppo di risorse. Per impostazione predefinita, viene utilizzato l'ordine di avvio selezionato durante la selezione del gruppo di risorse; tuttavia, in questa fase è possibile eseguire qualsiasi modifica.

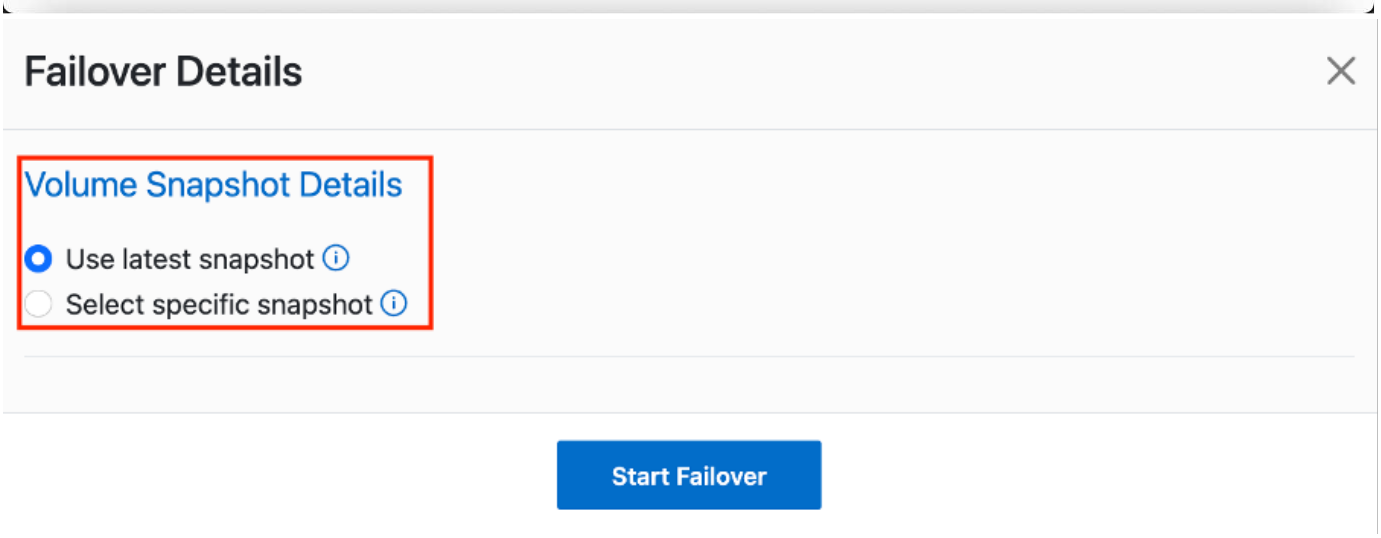


9. Fare clic su **Crea piano di replica**.

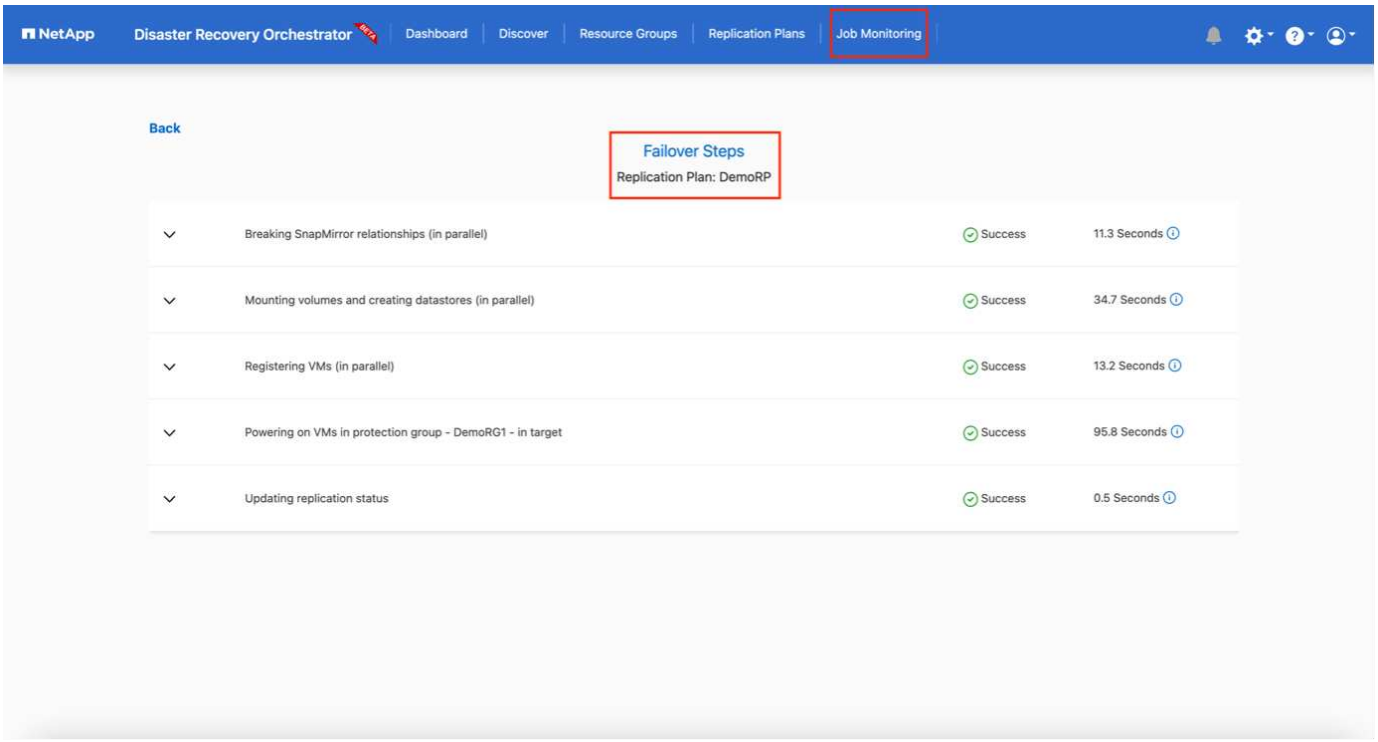


Una volta creato il piano di replica, è possibile utilizzare l'opzione di failover, l'opzione di test-failover o l'opzione di migrazione a seconda dei requisiti. Durante le opzioni di failover e test-failover, viene utilizzata la copia Snapshot SnapMirror più recente oppure è possibile selezionare una copia Snapshot specifica da una copia Snapshot point-in-time (in base alla policy di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile se si sta affrontando un evento di corruzione come ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i punti disponibili nel tempo. Per attivare il failover o verificare il failover con la configurazione specificata nel piano di replica, fare clic su **failover** o **Test failover**.

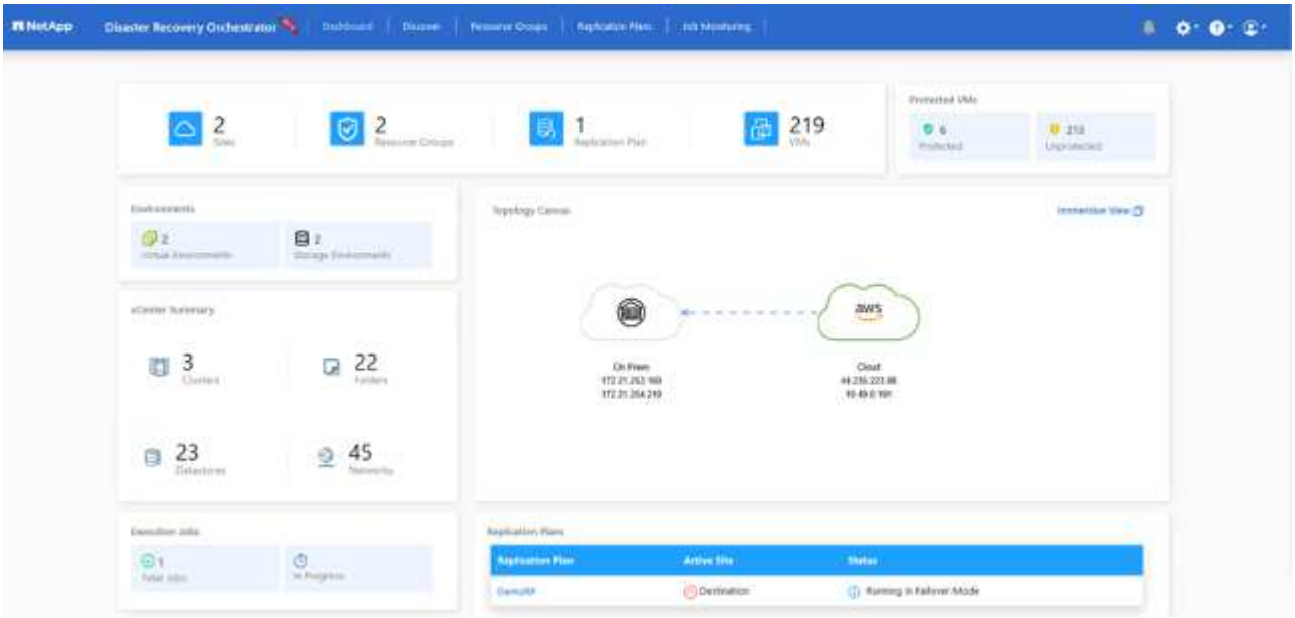




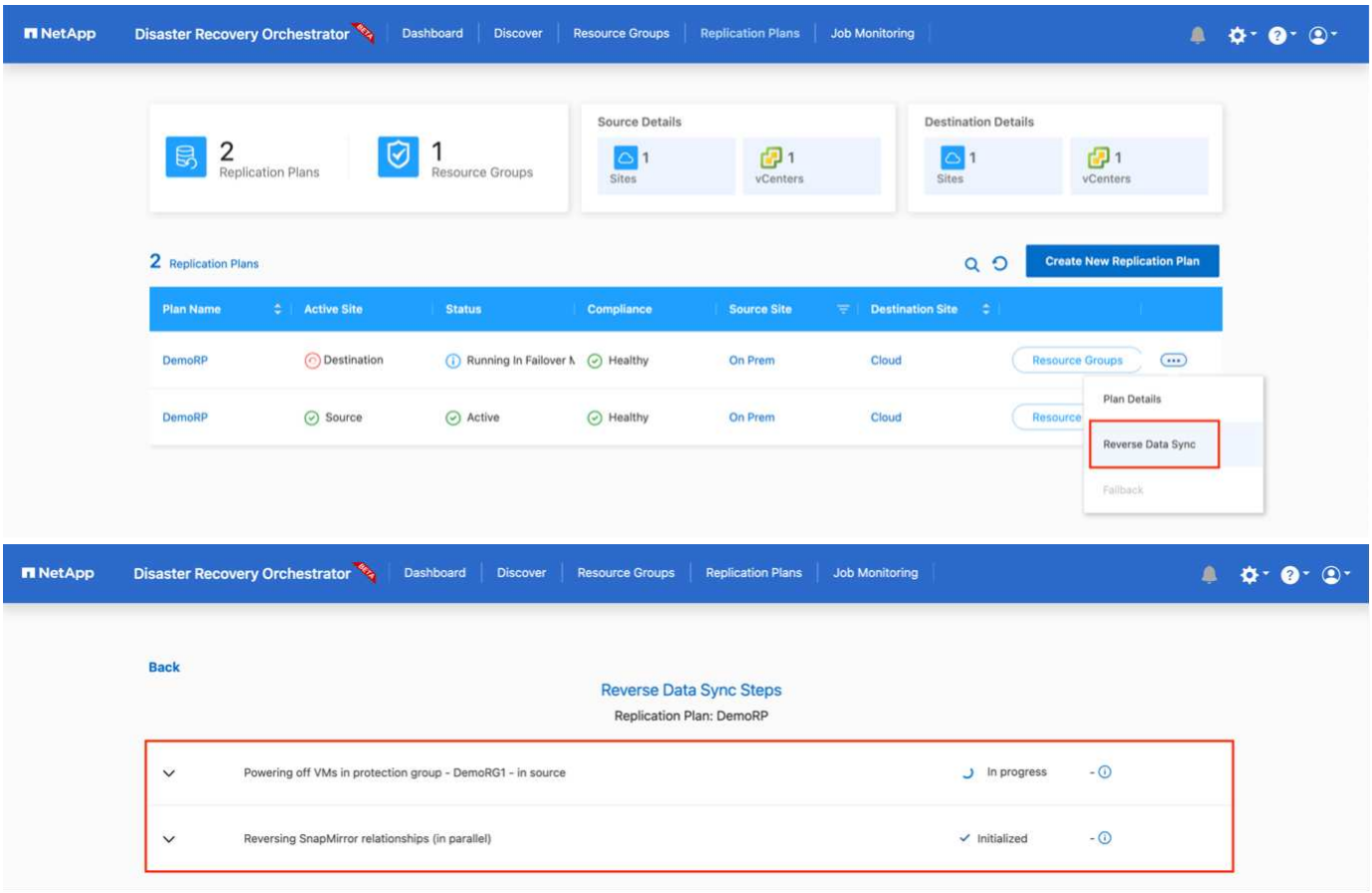
Il piano di replica può essere monitorato nel menu delle attività:



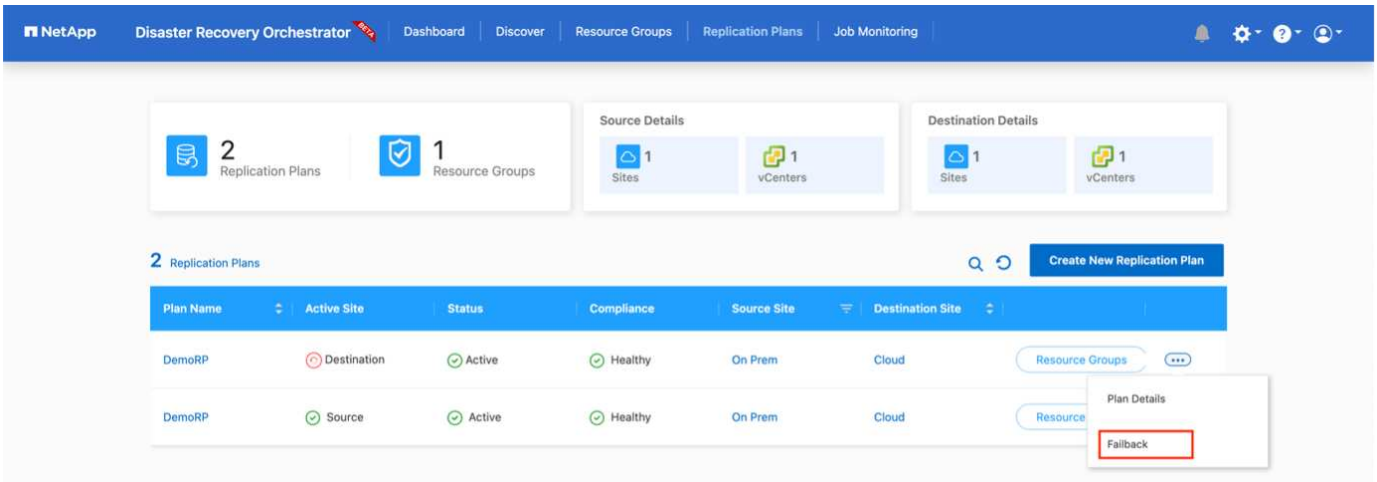
Dopo l'attivazione del failover, gli elementi ripristinati possono essere visualizzati in VMC vCenter (macchine virtuali, reti, datastore). Per impostazione predefinita, le macchine virtuali vengono ripristinate nella cartella workload.

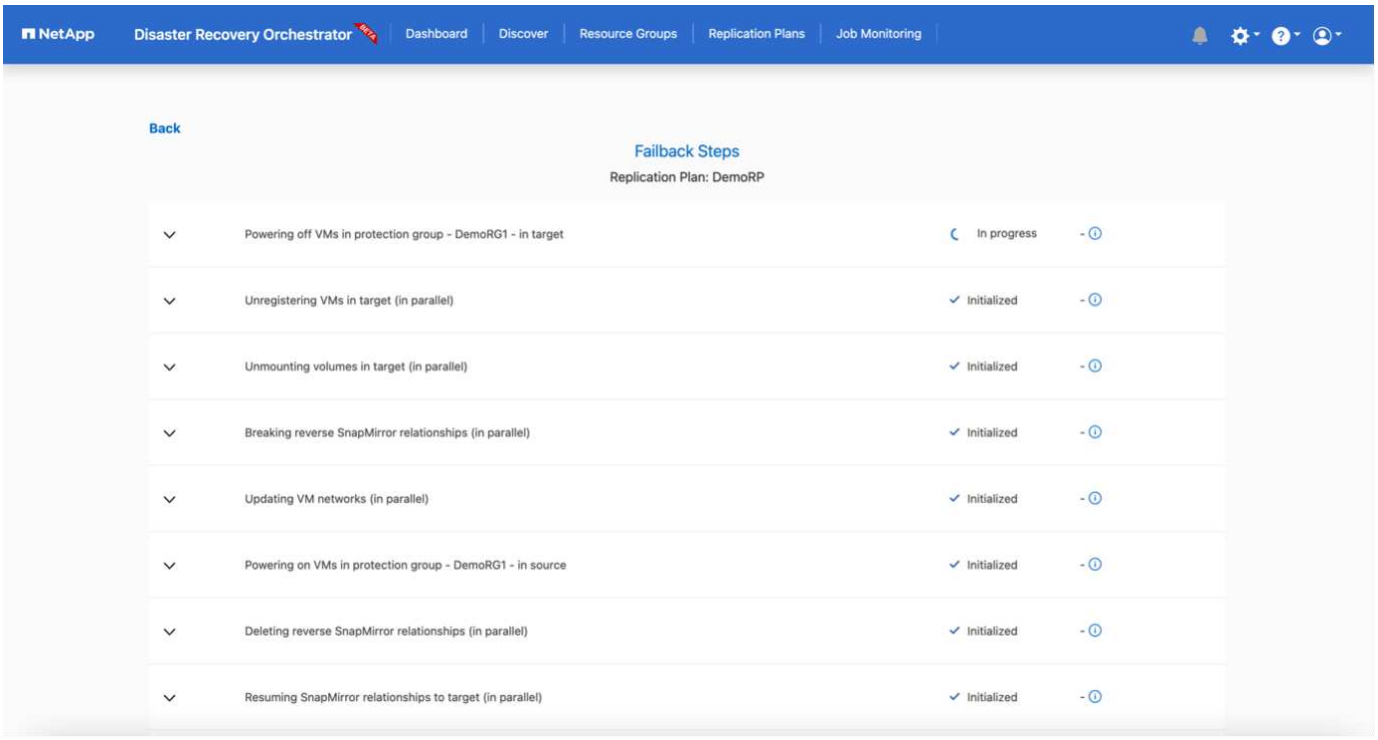


Il failback può essere attivato a livello di piano di replica. Per un failover di test, l'opzione di strappo può essere utilizzata per eseguire il rollback delle modifiche e rimuovere la relazione FlexClone. Il failback relativo al failover è un processo in due fasi. Selezionare il piano di replica e selezionare **Reverse data Sync**.

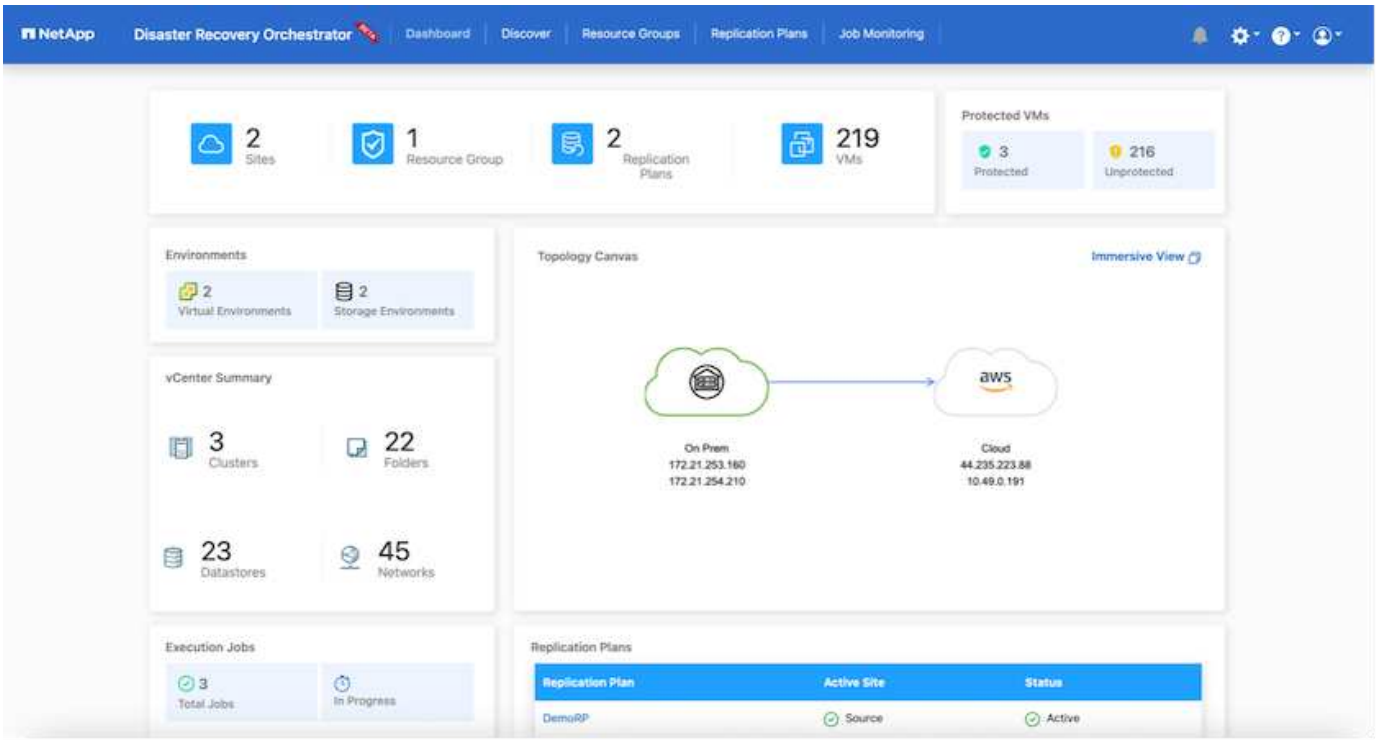


Una volta completato, è possibile attivare il failback per tornare al sito di produzione originale.





Da NetApp BlueXP, possiamo notare che lo stato di salute della replica è stato interrotto per i volumi appropriati (quelli mappati a VMC come volumi di lettura/scrittura). Durante il failover di test, DRO non esegue il mapping del volume di destinazione o di replica. Invece, crea una copia FlexClone dell'istanza SnapMirror (o Snapshot) richiesta ed espone l'istanza FlexClone, che non consuma ulteriore capacità fisica per FSX per ONTAP. Questo processo garantisce che il volume non venga modificato e che i processi di replica possano continuare anche durante i test di DR o i flussi di lavoro di triage. Inoltre, questo processo garantisce che, in caso di errori o di ripristino di dati corrotti, il ripristino possa essere pulito senza il rischio di distruzione della replica.



Recovery ransomware

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, può essere difficile per le organizzazioni IT individuare il punto di ritorno sicuro e, una volta stabilito, proteggere i carichi di lavoro recuperati da attacchi ricorrenti, ad esempio malware in sospensione o applicazioni vulnerabili.

DRO risolve questi problemi consentendo di ripristinare il sistema da qualsiasi punto in tempo disponibile. È inoltre possibile ripristinare i carichi di lavoro su reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro in una posizione in cui non sono esposte al traffico nord-sud. In questo modo, il tuo team di sicurezza è in una posizione sicura per condurre indagini legali e assicurarsi che non ci siano malware nascosti o inattivi.

Benefici

- Utilizzo della replica SnapMirror efficiente e resiliente.
- Ripristino in qualsiasi momento disponibile con la conservazione delle copie Snapshot.
- Automazione completa di tutte le fasi necessarie per ripristinare da centinaia a migliaia di macchine virtuali dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- Ripristino del workload con la tecnologia FlexClone di ONTAP che utilizza un metodo che non modifica il volume replicato.
  - Evita il rischio di corruzione dei dati per volumi o copie Snapshot.
  - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
  - Potenziale utilizzo dei dati di DR con risorse di cloud computing per flussi di lavoro che vanno oltre il DR, come DevTest, test di sicurezza, test di patch o upgrade e test di correzione.
- Ottimizzazione della CPU e della RAM per ridurre i costi del cloud consentendo il ripristino in cluster di calcolo più piccoli.

Utilizzo di Veeam Replication and FSX for ONTAP per il disaster recovery in VMware Cloud su AWS

L'integrazione di Amazon FSX per NetApp ONTAP con VMware Cloud su AWS è un datastore NFS esterno gestito da AWS e costruito sul file system ONTAP di NetApp che può essere collegato a un cluster nell'SDDC. Offre ai clienti un'infrastruttura storage virtualizzata flessibile e dalle performance elevate, che può scalare in maniera indipendente dalle risorse di calcolo.

Autore: Niyaz Mohamed - Ingegneria di soluzioni di NetApp

Panoramica

Per i clienti che desiderano utilizzare VMware Cloud su AWS SDDC come destinazione di disaster recovery, i datastore FSX per ONTAP possono essere utilizzati per replicare i dati dalle strutture on-premise utilizzando qualsiasi soluzione di terze parti validata che offre funzionalità di replica delle macchine virtuali. Aggiungendo un datastore di FSX per ONTAP, si otterrà un'implementazione ottimizzata dei costi rispetto alla costruzione di un cloud VMware su AWS SDDC con un'enorme quantità di host ESXi solo per ospitare lo storage.

Questo approccio aiuta inoltre i clienti a utilizzare cluster pilota leggero in VMC insieme ai datastore FSX per ONTAP per ospitare le repliche della macchina virtuale. Lo stesso processo può anche essere esteso come opzione di migrazione a VMware Cloud su AWS eseguendo con dignità il failover del piano di replica.

Descrizione del problema

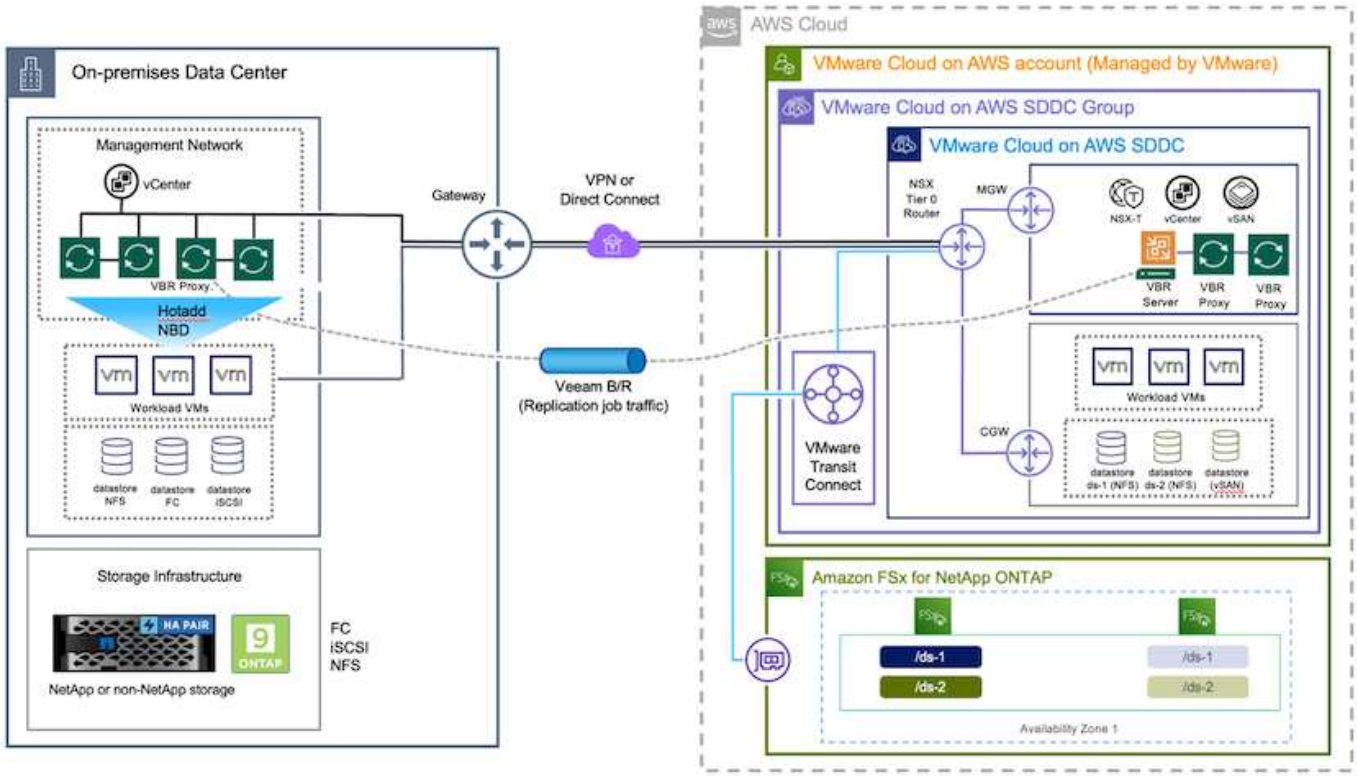
Questo documento descrive come utilizzare il datastore FSX per ONTAP e la replica di Veeam Backup per configurare il disaster recovery per le VM VMware on-premise su VMware Cloud su AWS utilizzando la funzionalità di replica delle VM.

Veeam Backup & Replication offre replica on-site e remota per il disaster recovery (DR). Quando le macchine virtuali vengono replicate, Veeam Backup & Replication crea una copia esatta delle macchine virtuali nel formato nativo di VMware vSphere sul cluster VMware Cloud di destinazione su AWS SDDC e mantiene la copia sincronizzata con la macchina virtuale originale.

La replica offre i migliori valori di RTO (Recovery Time Objective) poiché esiste una copia di una VM nello stato pronto per l'avvio. Questo meccanismo di replica garantisce l'avvio rapido dei carichi di lavoro in VMware Cloud su AWS SDDC in caso di evento di emergenza. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e le connessioni lente. Inoltre, filtra anche blocchi di dati duplicati, blocchi di dati zero, file di swap e file OS guest di VM esclusi e comprime il traffico di replica.

Per evitare che i processi di replica consumino l'intera larghezza di banda della rete, è possibile mettere in atto acceleratori WAN e regole di limitazione della rete. Il processo di replica in Veeam Backup & Replication è basato sul processo, il che significa che la replica viene eseguita configurando i processi di replica. In caso di evento di emergenza, è possibile attivare il failover per ripristinare le macchine virtuali con failover sulla copia di replica.

Una volta eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito allo stato più recente di una replica o a qualsiasi punto di ripristino valido. Ciò abilita recovery dal ransomware o test isolati, se necessario. In Veeam Backup & Replication, il failover e il failback sono passaggi intermedi temporanei che devono essere ulteriormente finalizzati. Veeam Backup & Replication offre diverse opzioni per gestire diversi scenari di disaster recovery.



Implementazione della soluzione

Gradini di alto livello

1. Il software Veeam Backup and Replication è in esecuzione in un ambiente on-premise con appropriata connettività di rete.
2. Configurare VMware Cloud su AWS, vedere l'articolo VMware Cloud Tech zone "Guida all'integrazione di VMware Cloud su AWS con Amazon FSX per l'implementazione di NetApp ONTAP" Per eseguire l'implementazione, configura VMware Cloud su AWS SDDC e FSX per ONTAP come datastore NFS. (Per scopi di DR è possibile utilizzare un ambiente pilota con configurazione minima. In caso di incidente, è possibile eseguire il failover delle macchine virtuali su questo cluster e aggiungere nodi.
3. Impostare i lavori di replica per creare repliche VM utilizzando Veeam Backup and Replication.
4. Creazione di un piano di failover ed esecuzione di un failover.
5. Tornare alle macchine virtuali di produzione una volta che l'evento di disastro è completo e il sito primario è attivo.

Prerequisiti per la replica della macchina virtuale Veeam nei datastore VMC ed FSX per ONTAP

1. Garantire che la macchina virtuale di backup di Veeam Backup & Replication sia connessa al vCenter di origine e al cloud VMware di destinazione sui cluster AWS SDDC.
2. Il server di backup deve essere in grado di risolvere i nomi brevi e di connettersi ai centri virtuali di origine e di destinazione.
3. Il datastore FSX per ONTAP di destinazione deve avere spazio libero sufficiente per archiviare VMDK di macchine virtuali replicate

Per ulteriori informazioni, fare riferimento a "considerazioni e limitazioni" "qui".

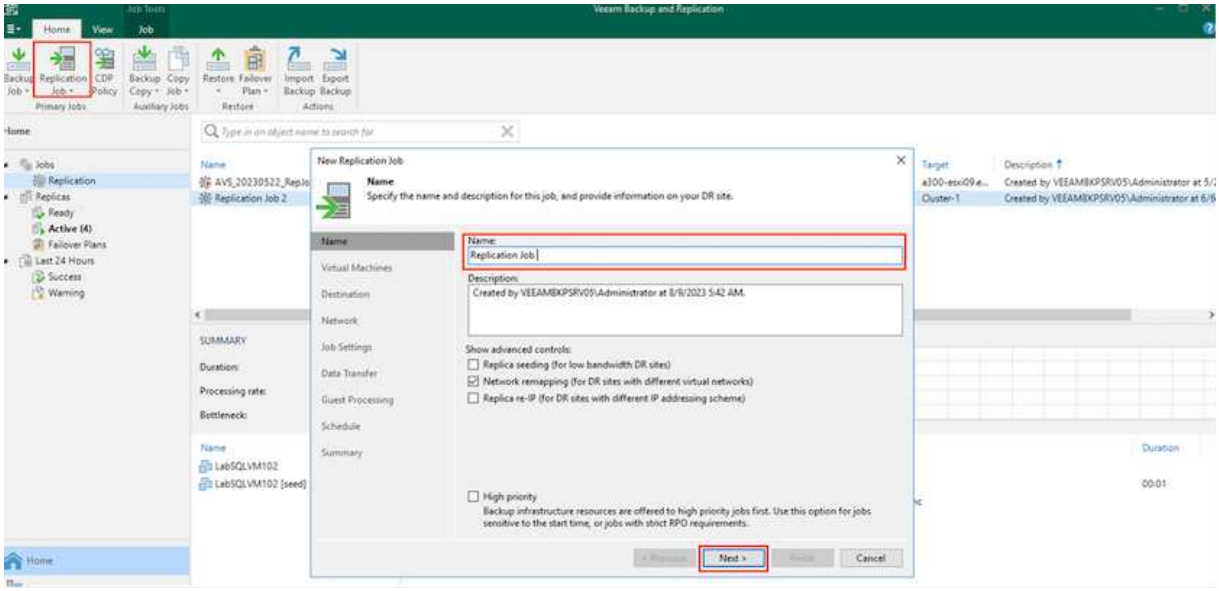
Dettagli sull'implementazione

Fase 1: Replica delle VM

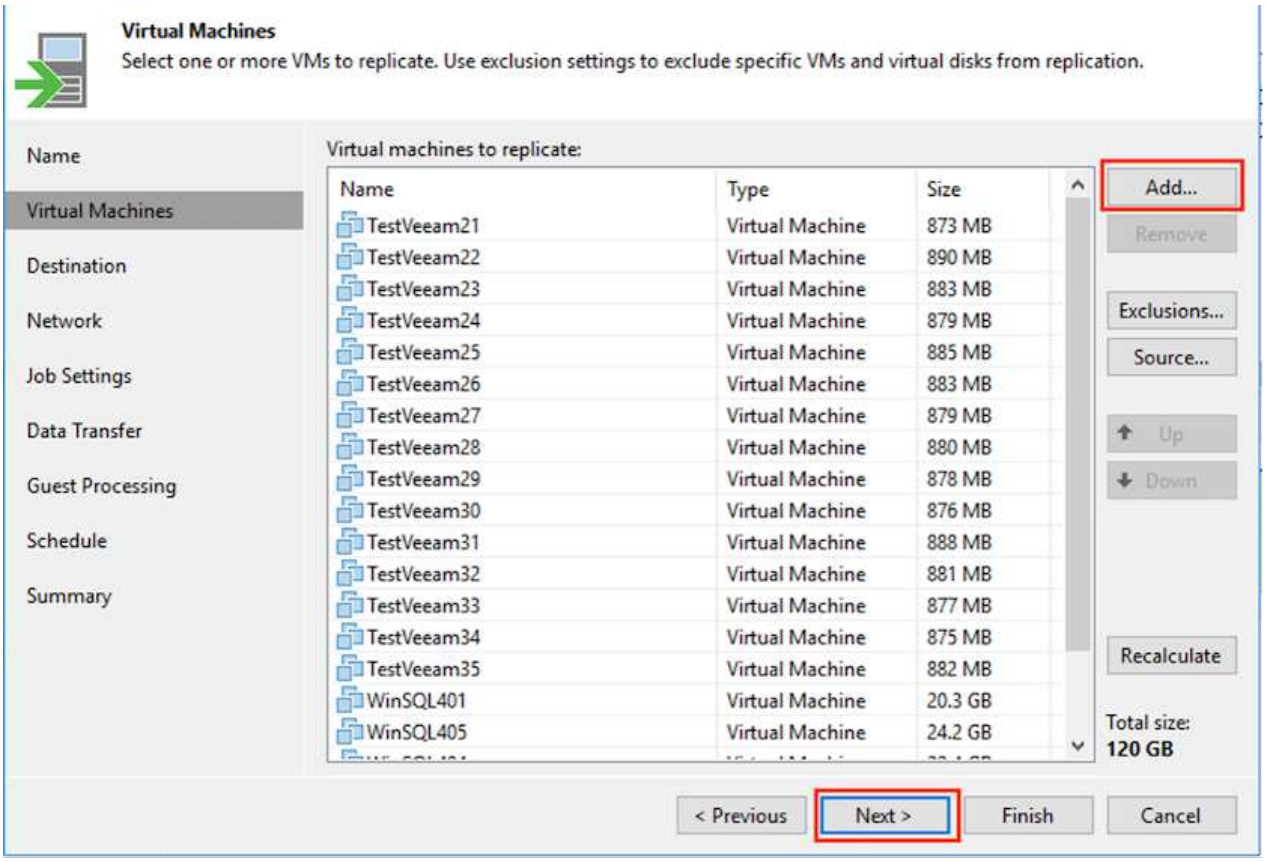
Veeam Backup & Replication sfrutta le funzionalità snapshot di VMware vSphere e, durante la replica, Veeam Backup & Replication richiede a VMware vSphere la creazione di una snapshot delle VM. L'istantanea della VM è la copia point-in-time di una VM che include dischi virtuali, stato del sistema, configurazione e così via. Veeam Backup & Replication utilizza la snapshot come origine dei dati per la replica.

Per replicare le VM, attenersi alla seguente procedura:

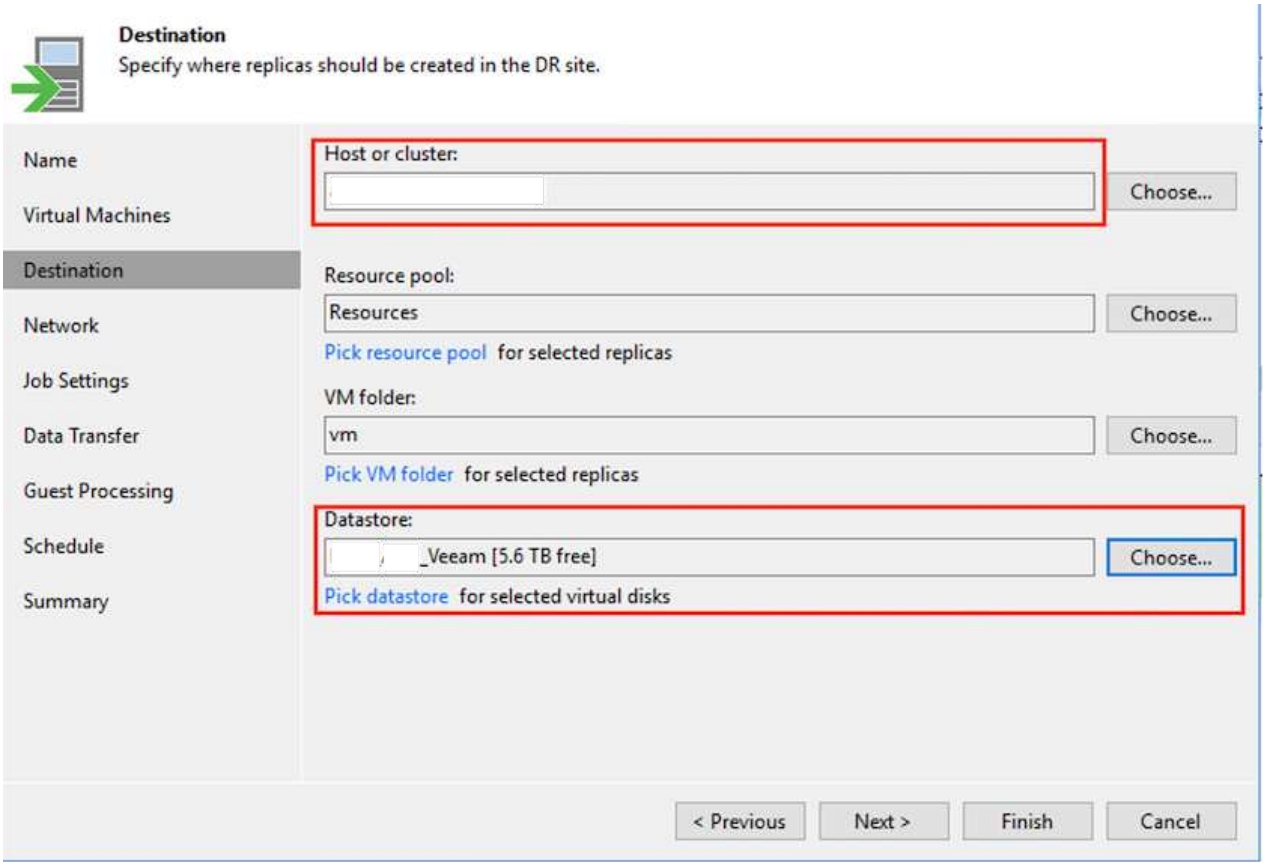
1. Apri la Veeam Backup & Replication Console.
2. Nella vista Home, selezionare processo di replica > macchina virtuale > VMware vSphere.
3. Specificare un nome di lavoro e selezionare la casella di controllo controllo avanzata appropriata. Fare clic su Avanti.
   - Selezionare la casella di controllo Replica seeding se la connettività tra on-premise e AWS ha limitato la larghezza di banda.
   - Selezionare la casella di controllo Network remapping (per i siti VMC AWS con reti diverse) se i segmenti su VMware Cloud su AWS SDDC non corrispondono a quelli delle reti dei siti on-premise.
   - Se lo schema di indirizzamento IP nel sito di produzione on-premise differisce dallo schema nel sito VMC di AWS, selezionare la casella di controllo Replica re-IP (per i siti di DR con schema di indirizzamento IP diverso).



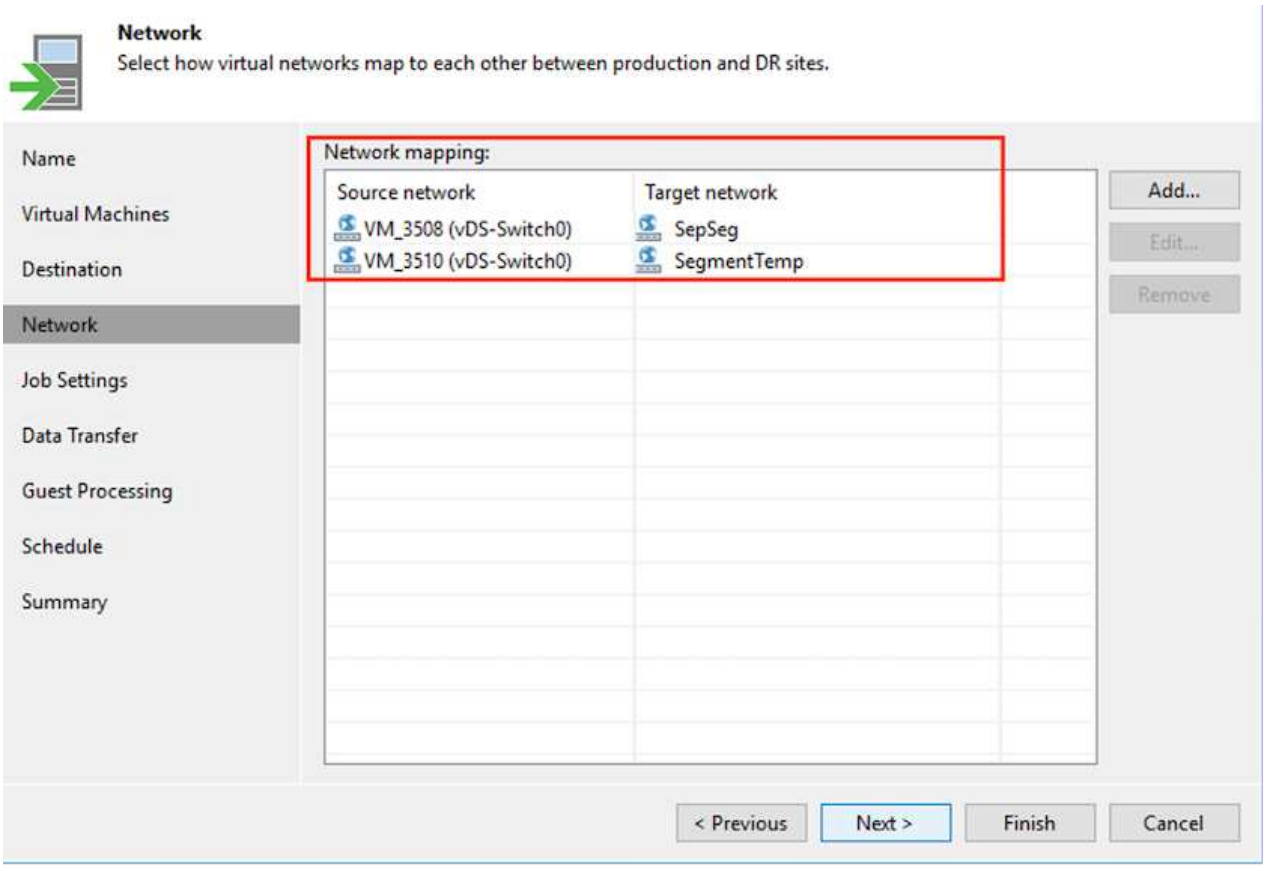
4. Seleziona le VM da replicare nel datastore FSX per ONTAP collegato a VMware Cloud su AWS SDDC nel passaggio **macchine virtuali**. Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità del datastore vSAN disponibile. In un cluster spia pilota, la capacità utilizzabile di un cluster a 3 nodi sarà limitata. Il resto dei dati può essere replicato in datastore FSX per ONTAP. Fare clic su **Aggiungi**, quindi nella finestra **Aggiungi oggetto** selezionare le VM o i contenitori VM necessari e fare clic su **Aggiungi**. Fare clic su **Avanti**.



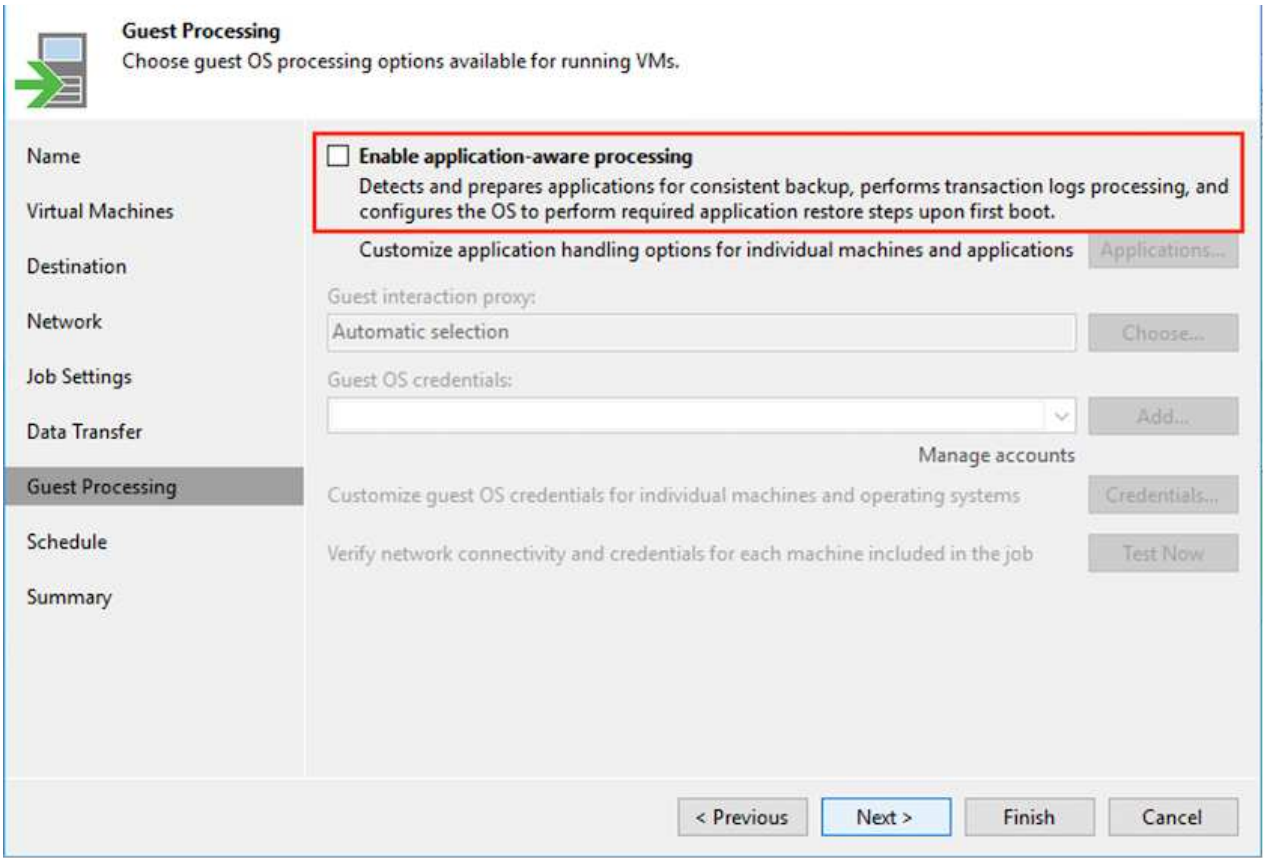
5. Quindi, seleziona la destinazione come VMware Cloud su host/cluster SDDC di AWS e il pool di risorse, la cartella VM e il datastore FSX per le repliche VM di ONTAP. Quindi fare clic su **Avanti**.



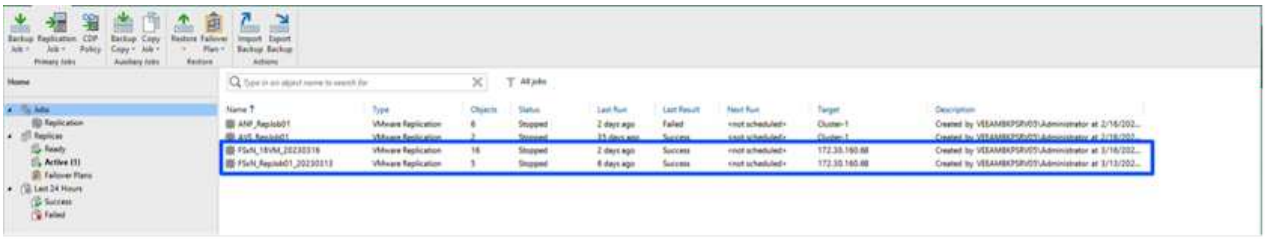
6. Nel passaggio successivo, creare la mappatura tra la rete virtuale di origine e di destinazione secondo necessità.



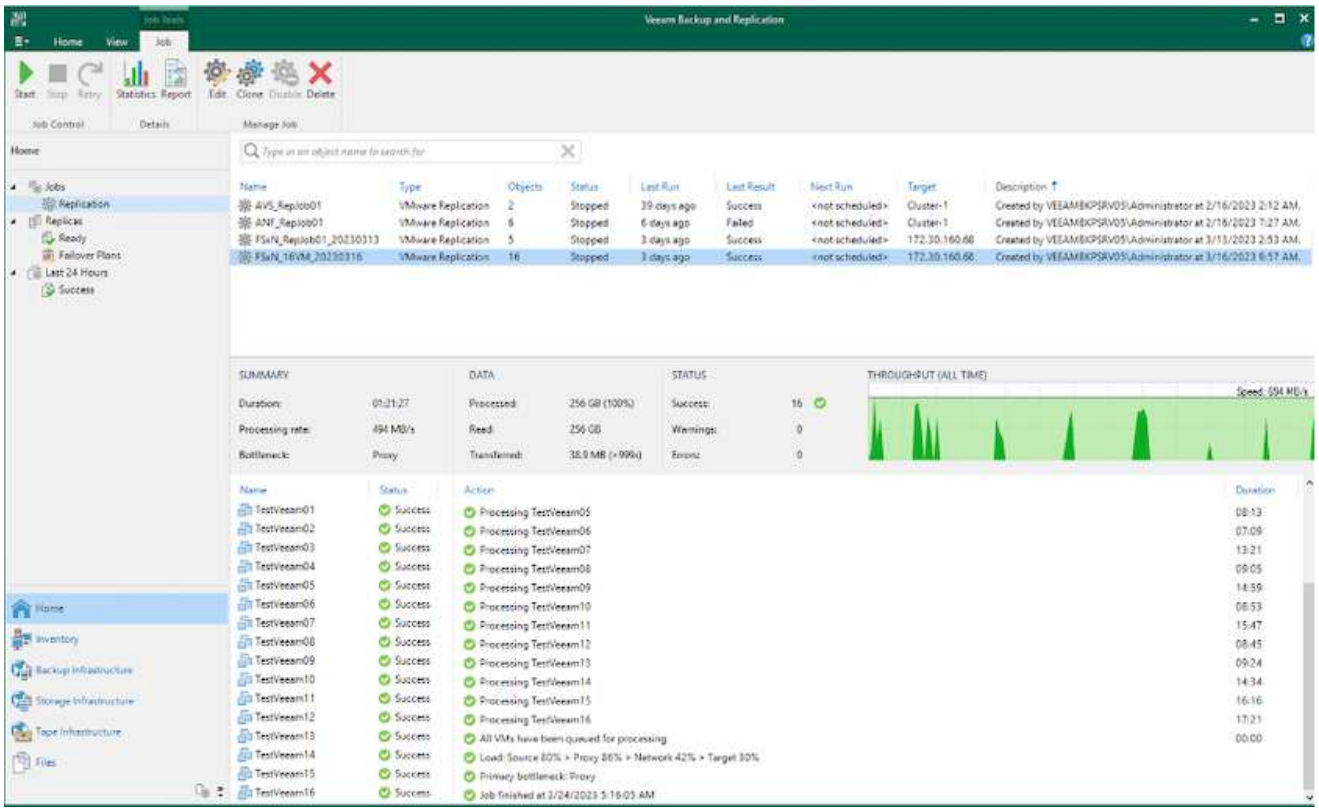
7. Nel passaggio **Impostazioni processo**, specificare il repository di backup che memorizzerà i metadati per le repliche della VM, i criteri di conservazione e così via.
8. Aggiornare i server proxy **Source** e **Target** nel passo **trasferimento dati** e lasciare selezionata l'opzione **Automatic** (impostazione predefinita) e mantenere l'opzione **Direct** (diretto) e fare clic su **Next** (Avanti).
9. Nel passaggio **elaborazione guest**, selezionare **attiva elaborazione in base alle esigenze dell'applicazione**. Fare clic su **Avanti**.



10. Scegliere la pianificazione di replica per eseguire regolarmente il processo di replica.
11. Nel passo **Riepilogo** della procedura guidata, esaminare i dettagli del processo di replica. Per avviare il lavoro subito dopo la chiusura della procedura guidata, selezionare la casella di controllo **Esegui il lavoro quando si fa clic su fine**, altrimenti lasciare deselezionata la casella di controllo. Quindi fare clic su **fine** per chiudere la procedura guidata.



Una volta avviato il processo di replica, le macchine virtuali con il suffisso specificato verranno popolate nel cluster/host VMC SDDC di destinazione.



Per ulteriori informazioni sulla replica Veeam, fare riferimento a. "Come funziona la replica".

Passaggio 2: Creare un piano di failover

Una volta completata la replica o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire automaticamente il failover per le VM dipendenti una alla volta o come gruppo. Il piano di failover è il modello per l'ordine in cui le macchine virtuali vengono elaborate, inclusi i ritardi di avvio. Il piano di failover aiuta inoltre a garantire che le VM dipendenti da fattori critici siano già in esecuzione.

Per creare il piano, passare alla nuova sottosezione denominata repliche e selezionare piano di failover. Scegliere le VM appropriate. Veeam Backup & Replication cercherà i punti di ripristino più vicini a questo punto nel tempo e li utilizzerà per avviare le repliche della VM.

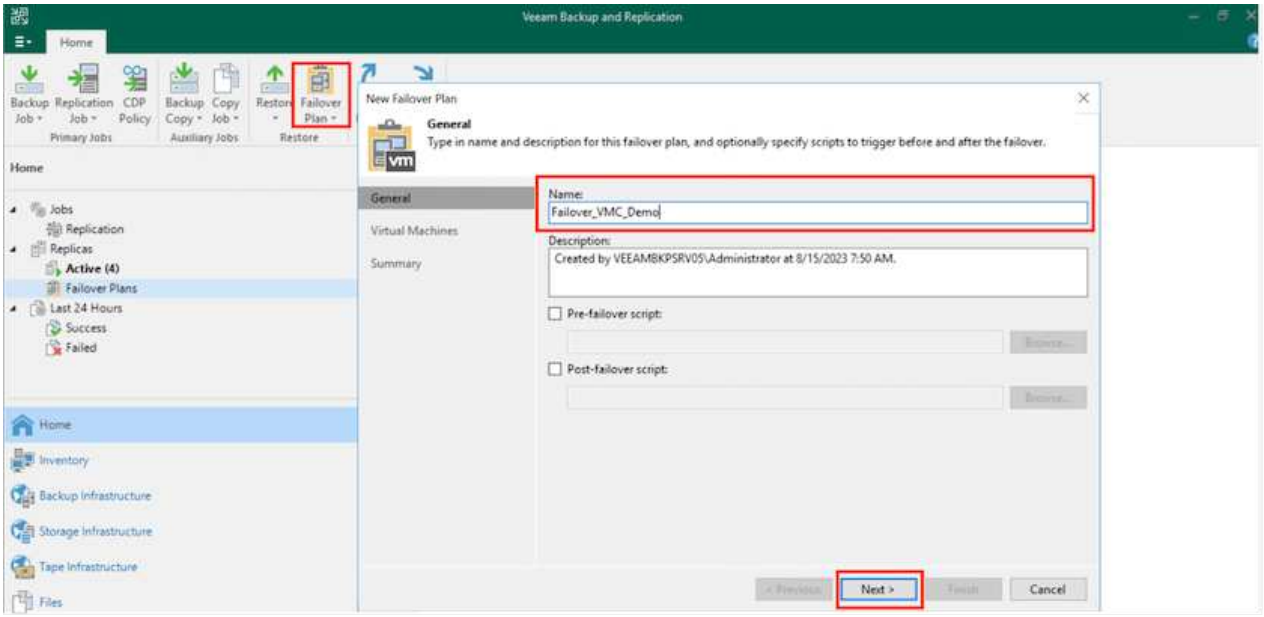
> Il piano di failover può essere aggiunto solo una volta completata la replica iniziale e le repliche della VM sono nello stato Pronta.

> Il numero massimo di VM che possono essere avviate contemporaneamente quando si esegue un piano di failover è 10.

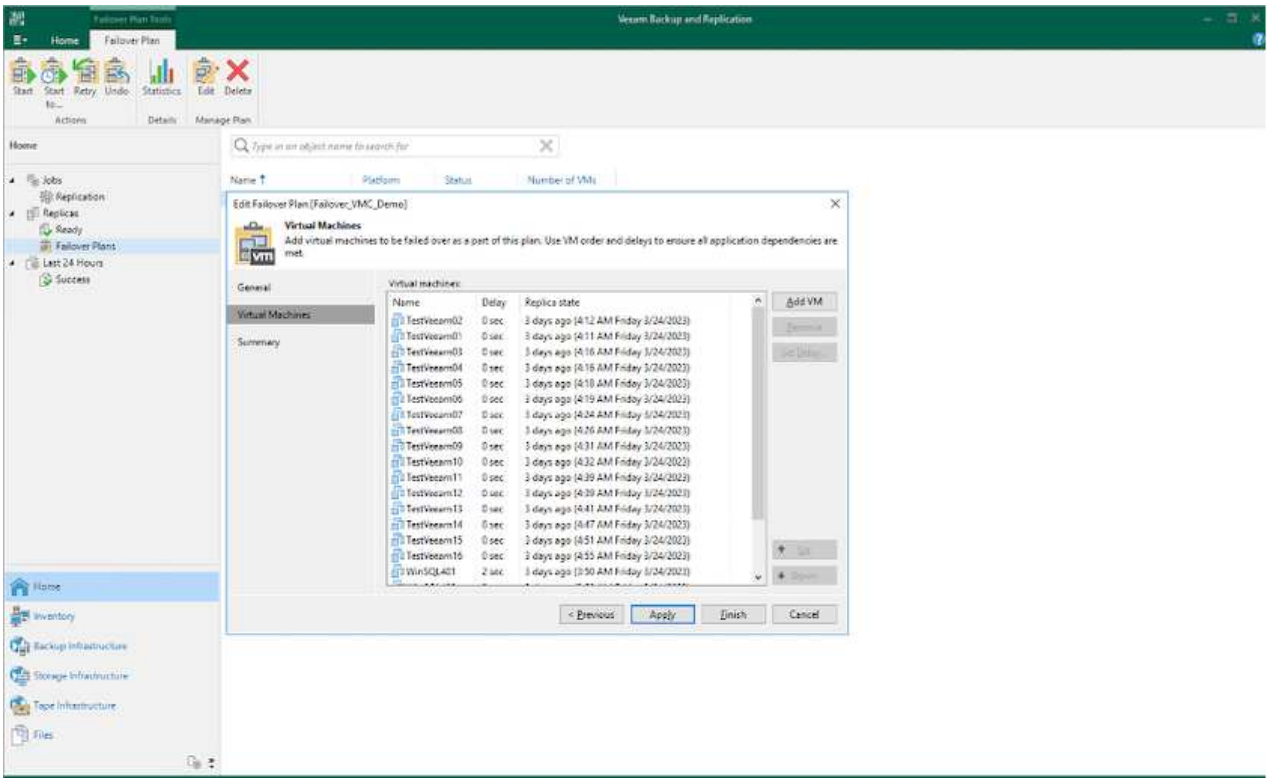
> Durante il processo di failover, le macchine virtuali di origine non verranno spente.

Per creare il **piano di failover**, procedere come segue:

1. Nella vista Home, selezionare **piano di failover > VMware vSphere**.
2. Quindi, fornire un nome e una descrizione al piano. Gli script pre e post-failover possono essere aggiunti secondo necessità. Ad esempio, eseguire uno script per arrestare le macchine virtuali prima di avviare le macchine virtuali replicate.



3. Aggiungere le VM al piano e modificare l'ordine di avvio delle VM e i ritardi di avvio per soddisfare le dipendenze delle applicazioni.



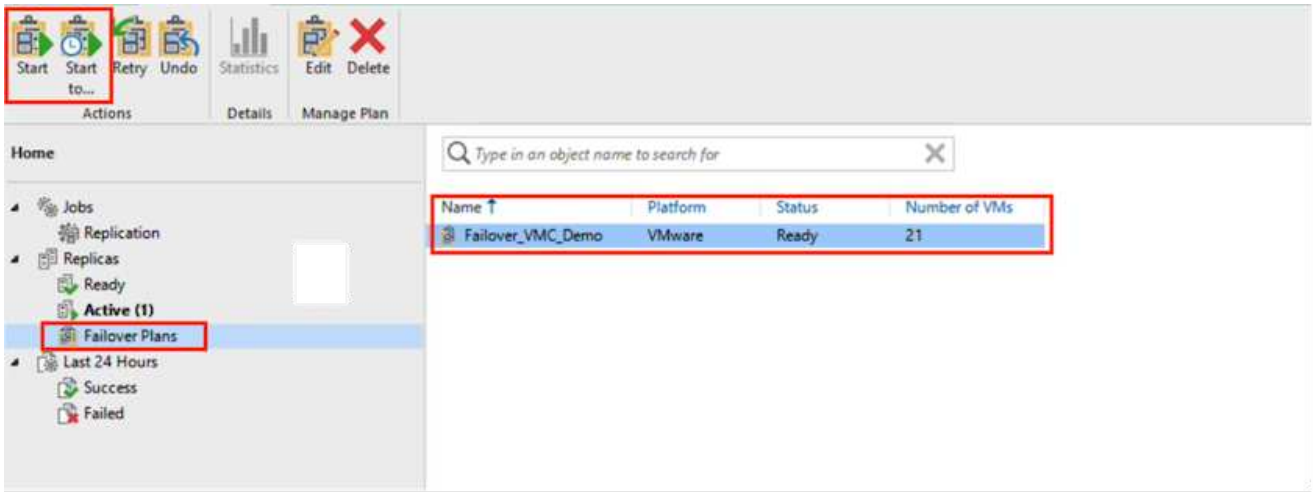
Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento a. "Creazione di processi di replica".

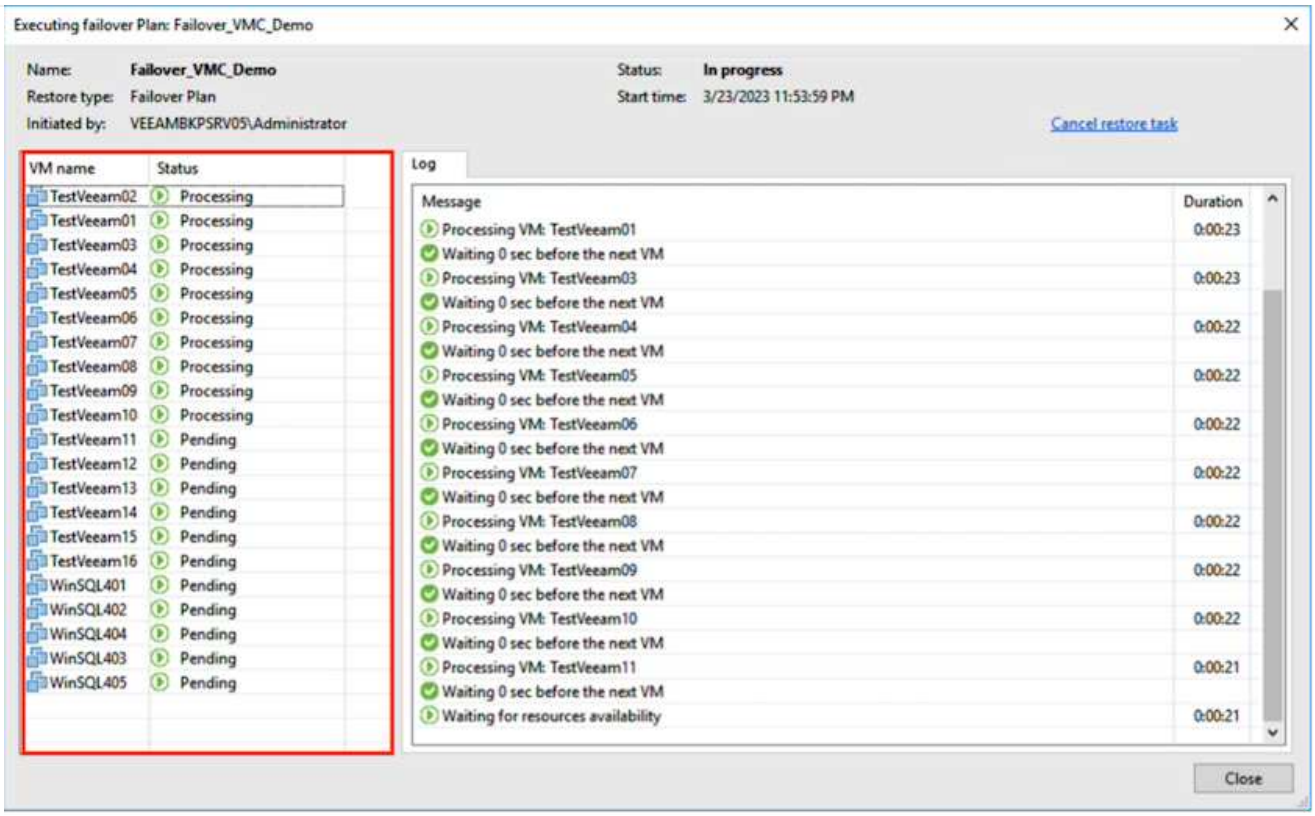
Passaggio 3: Eseguire il piano di failover

Durante il failover, la macchina virtuale di origine nel sito di produzione viene commutata alla replica nel sito di disaster recovery. Come parte del processo di failover, Veeam Backup & Replication ripristina la replica della VM al punto di ripristino richiesto e sposta tutte le attività di i/o dalla VM di origine alla replica. Le repliche possono essere utilizzate non solo in caso di disastro, ma anche per simulare esercitazioni sul DR. Durante la simulazione del failover, la VM di origine rimane in esecuzione. Una volta eseguiti tutti i test necessari, è possibile annullare il failover e tornare alla normale operatività.

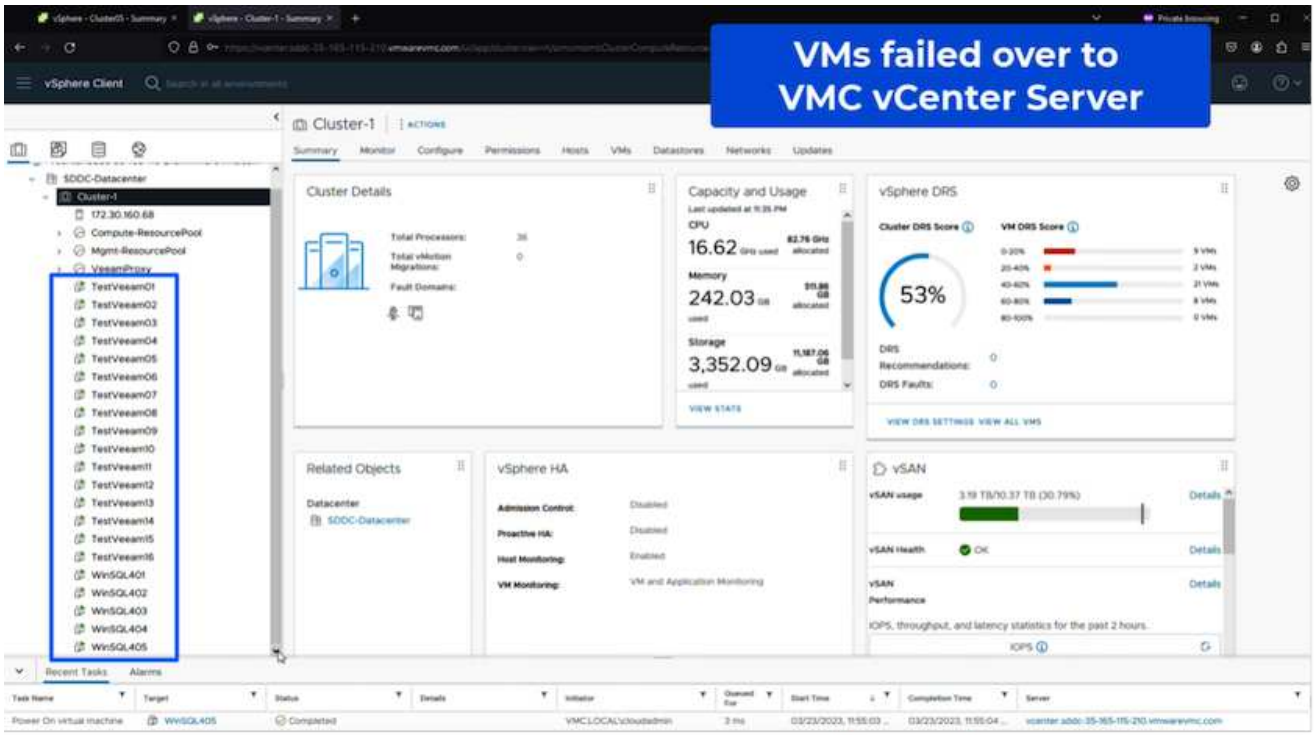
Accertarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante le procedure di DR.

Per avviare il piano di failover, è sufficiente fare clic sulla scheda **piani di failover** e fare clic con il pulsante destro del mouse sul piano di failover. Selezionare **Start**. Il failover viene eseguito utilizzando gli ultimi punti di ripristino delle repliche della VM. Per eseguire il failover su punti di ripristino specifici delle repliche della VM, selezionare **Avvia a**.

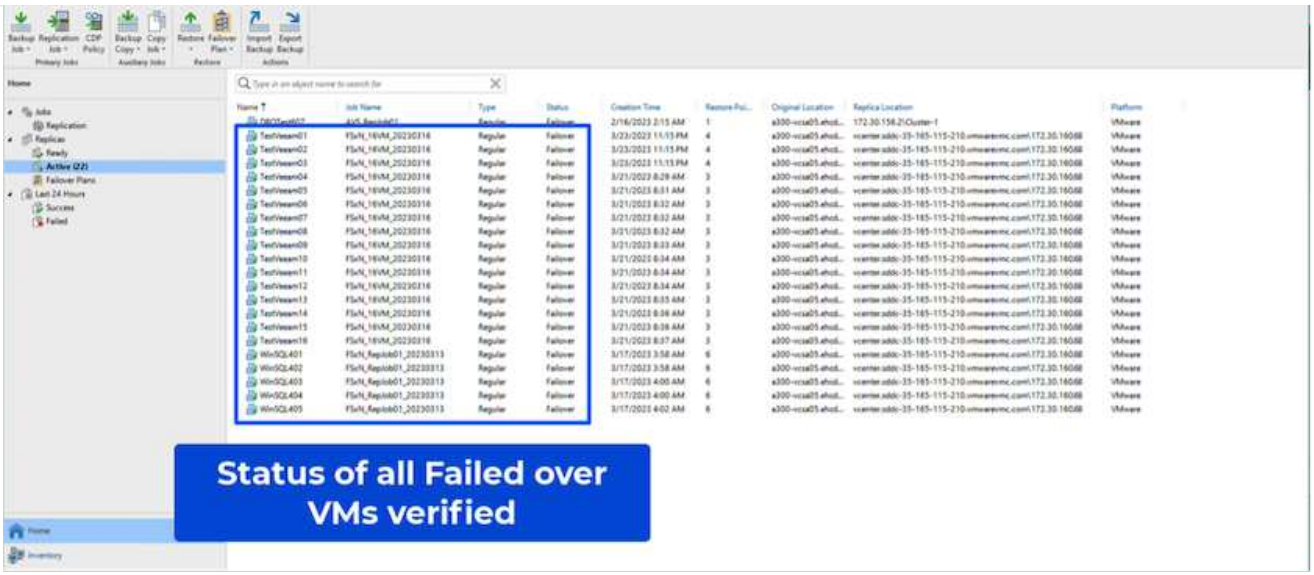




Lo stato della replica della macchina virtuale cambia da Pronto a failover e le macchine virtuali vengono avviate sul VMware Cloud di destinazione sul cluster/host AWS SDDC.



Una volta completato il failover, lo stato delle macchine virtuali passa a "failover".



Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine fino a quando la replica non viene riportata allo stato Ready.

Per informazioni dettagliate sui piani di failover, fare riferimento a. "Piani di failover".

Fase 4: Failback nel sito di produzione

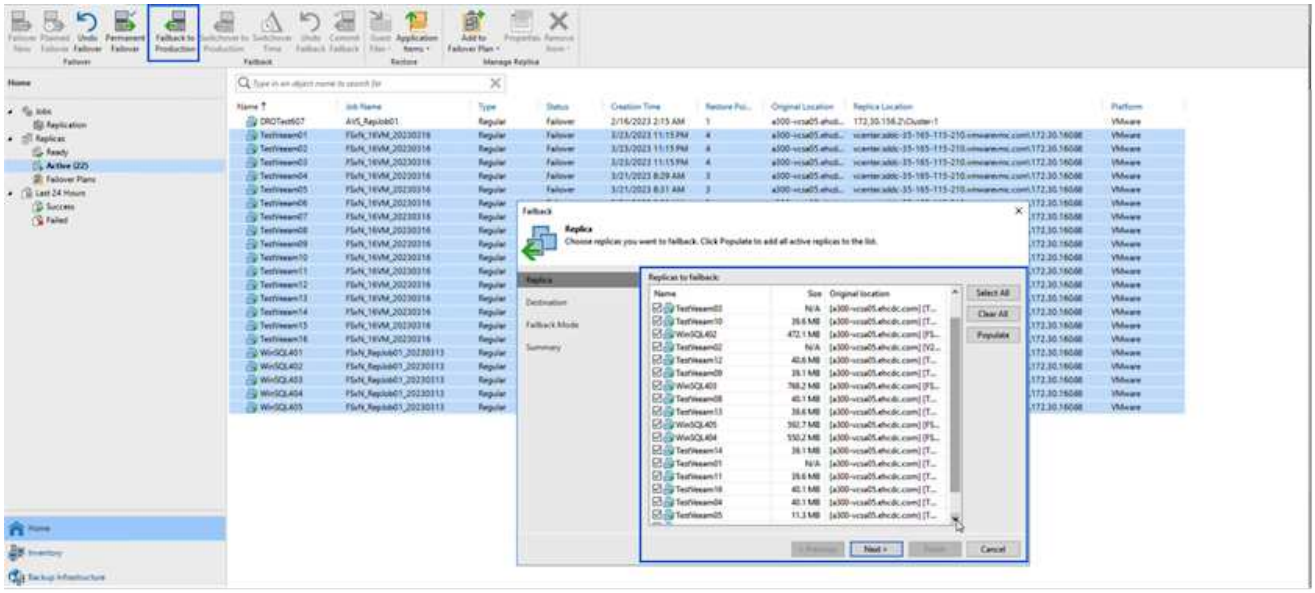
Quando il piano di failover è in esecuzione, viene considerato come una fase intermedia e deve essere finalizzato in base al requisito. Le opzioni includono:

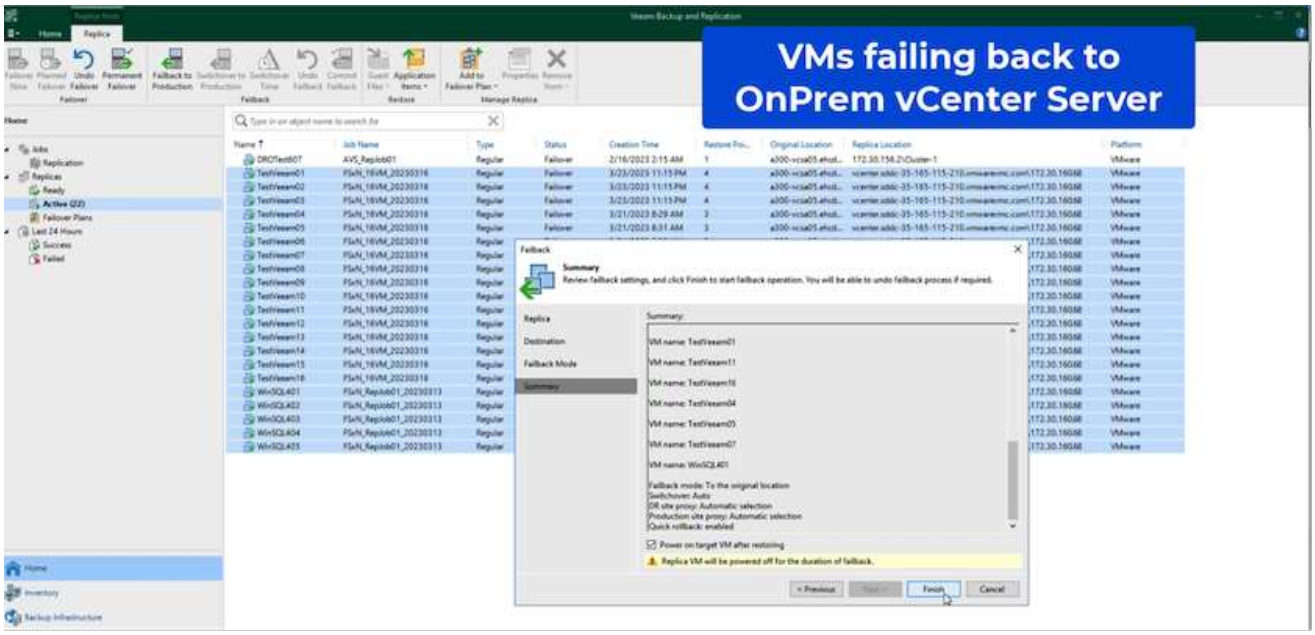
- **Failback to Production** - consente di tornare alla VM originale e di trasferire tutte le modifiche apportate durante l'esecuzione della replica della VM alla VM originale.

> Quando si esegue il failback, le modifiche vengono solo trasferite ma non pubblicate. Scegliere **Commit failback** (una volta che la VM originale è confermata per funzionare come previsto) o **Undo failback** per tornare alla replica della VM se la VM originale non funziona come previsto.

- **Annulla failover** - consente di tornare alla VM originale e di ignorare tutte le modifiche apportate alla replica della VM durante l'esecuzione.
- **Failover permanente** - consente di passare in modo permanente dalla VM originale a una replica della VM e di utilizzare questa replica come VM originale.

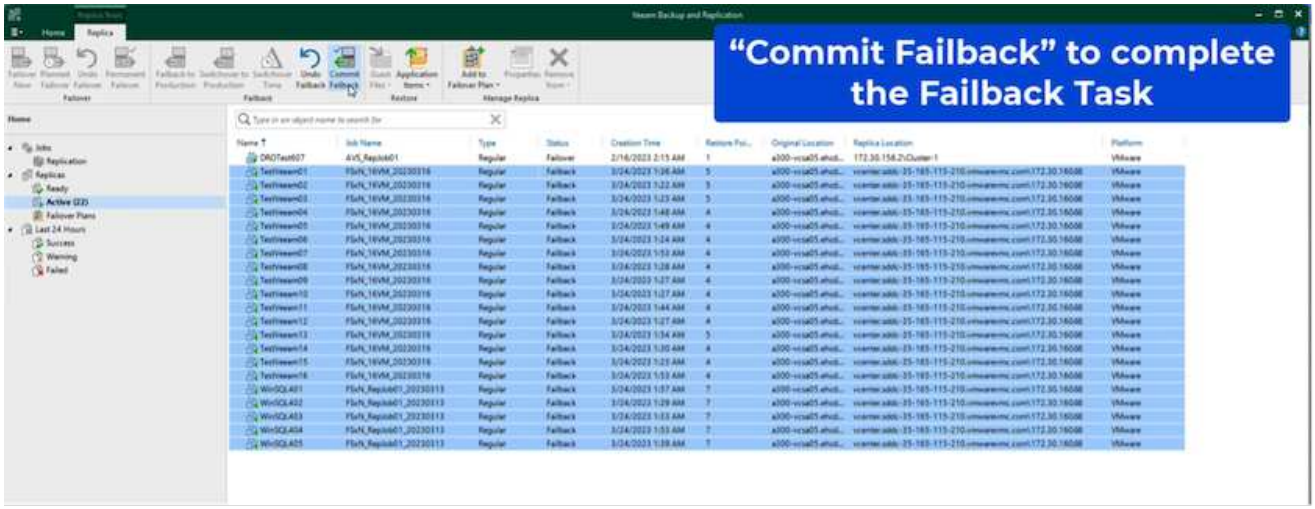
In questa demo, è stato scelto il failback in produzione. Il failback alla macchina virtuale originale è stato selezionato durante la fase di destinazione della procedura guidata ed è stata attivata la casella di controllo "accensione della macchina virtuale dopo il ripristino".

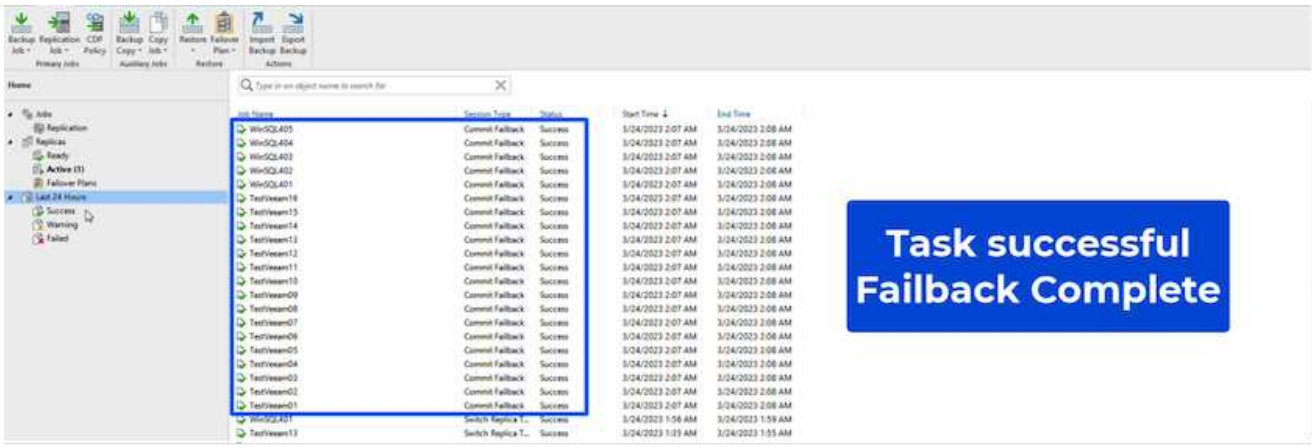




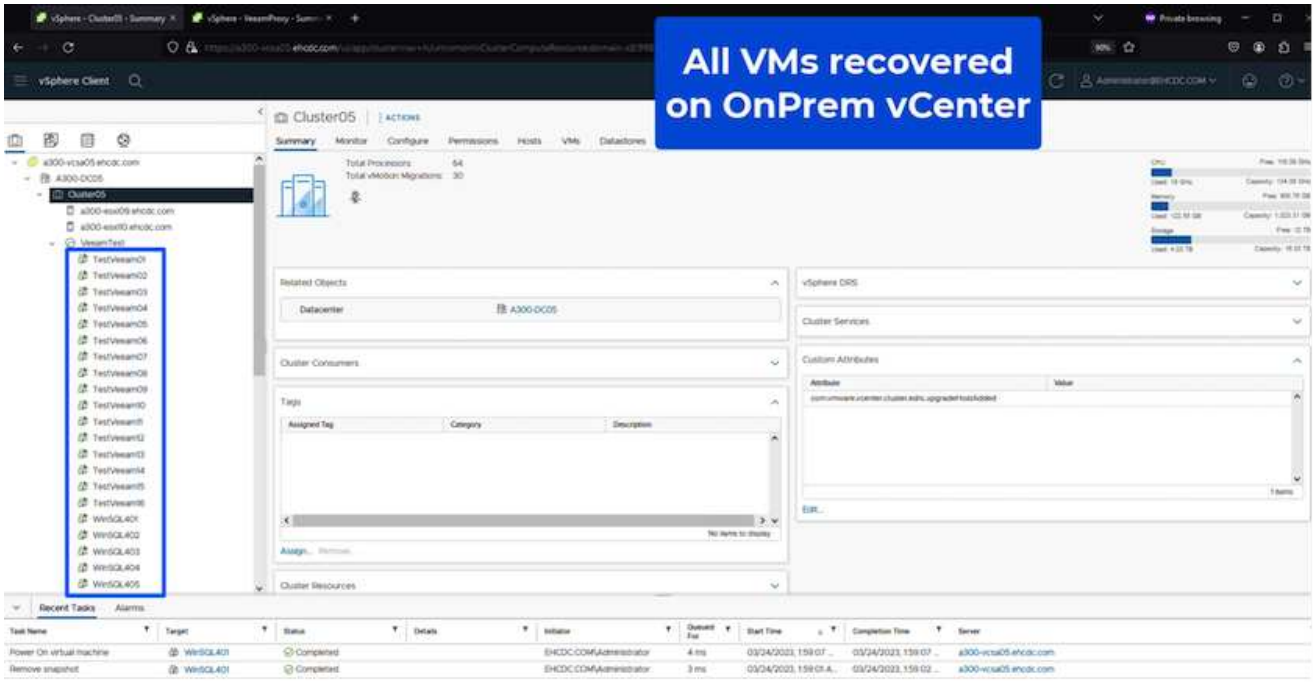
Il commit di failback è uno dei modi per finalizzare l'operazione di failback. Quando il failback viene eseguito, conferma che le modifiche inviate alla VM che ha avuto esito negativo (la VM di produzione) funzionano come previsto. Dopo l'operazione di commit, Veeam Backup & Replication riprende le attività di replica per la VM di produzione.

Per informazioni dettagliate sul processo di failback, fare riferimento alla documentazione Veeam per "Failover e failback per la replica".





Una volta eseguito il failback in produzione, le macchine virtuali vengono tutte ripristinate nel sito di produzione originale.



Conclusione

La funzionalità datastore di FSX per ONTAP permette a Veeam o a qualsiasi strumento di terze parti validato di fornire una soluzione DR a basso costo utilizzando il cluster pilota leggero e senza standing un elevato numero di host nel cluster solo per ospitare la copia della replica della VM. Questo offre una potente soluzione per gestire un piano di disaster recovery personalizzato e su misura e consente inoltre di riutilizzare i prodotti di backup esistenti in sede per soddisfare le esigenze di disaster recovery, consentendo in questo modo il disaster recovery basato sul cloud uscendo dai data center on-premise. Il failover può essere eseguito come failover pianificato o failover con un clic su un pulsante in caso di disastro e si decide di attivare il sito di DR.

Per ulteriori informazioni su questo processo, segui il video dettagliato.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

Migrazione dei carichi di lavoro su AWS / VMC

TR 4942: Migrazione dei carichi di lavoro al datastore FSX ONTAP con VMware HCX

Un caso di utilizzo comune per VMware Cloud (VMC) su Amazon Web Services (AWS), con il datastore NFS supplementare su Amazon FSX per NetApp ONTAP, è la migrazione dei workload VMware. VMware HCX è un'opzione preferita e offre diversi metodi di migrazione per spostare macchine virtuali (VM) on-premise e i relativi dati, in esecuzione su qualsiasi datastore supportato da VMware, negli archivi dati VMC, che includono datastore NFS supplementari su FSX per ONTAP.

Autore: NetApp Solutions Engineering

Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore supplementari FSX ONTAP e VMware Cloud

VMware HCX è principalmente una piattaforma di mobilità progettata per semplificare la migrazione dei workload, il ribilanciamento dei workload e la business continuity tra i cloud. È incluso in VMware Cloud su AWS e offre diversi modi per migrare i carichi di lavoro e può essere utilizzato per le operazioni di disaster recovery (DR).

Questo documento fornisce istruzioni dettagliate per l'implementazione e la configurazione di VMware HCX, inclusi tutti i suoi componenti principali, on-premise e sul cloud data center, che abilita vari meccanismi di migrazione delle macchine virtuali.

Per ulteriori informazioni, vedere "Introduzione alle implementazioni HCX" e. "Installare l'elenco di controllo B - HCX con VMware Cloud su AWS SDDC Destination Environment".

Passaggi di alto livello

Questo elenco fornisce i passaggi di alto livello per installare e configurare VMware HCX:

1. Attivare HCX per il data center software-defined (SDDC) VMC tramite VMware Cloud Services Console.
2. Scaricare e implementare IL programma di installazione di HCX Connector OVA nel server vCenter on-premise.
3. Attivare HCX con una chiave di licenza.
4. Associare il connettore VMware HCX on-premise con VMC HCX Cloud Manager.
5. Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio.
6. (Facoltativo) eseguire l'estensione di rete per estendere la rete ed evitare il re-IP.
7. Verificare lo stato dell'appliance e assicurarsi che sia possibile eseguire la migrazione.
8. Migrare i carichi di lavoro delle macchine virtuali.

Prerequisiti

Prima di iniziare, assicurarsi che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, vedere "Preparazione per l'installazione HCX". Una volta soddisfatti i prerequisiti, inclusa la connettività, configurare e attivare HCX generando una chiave di licenza dalla console VMware HCX in VMC. Dopo l'attivazione DI HCX, il plug-in vCenter viene implementato ed è possibile accedervi utilizzando vCenter Console per la gestione.

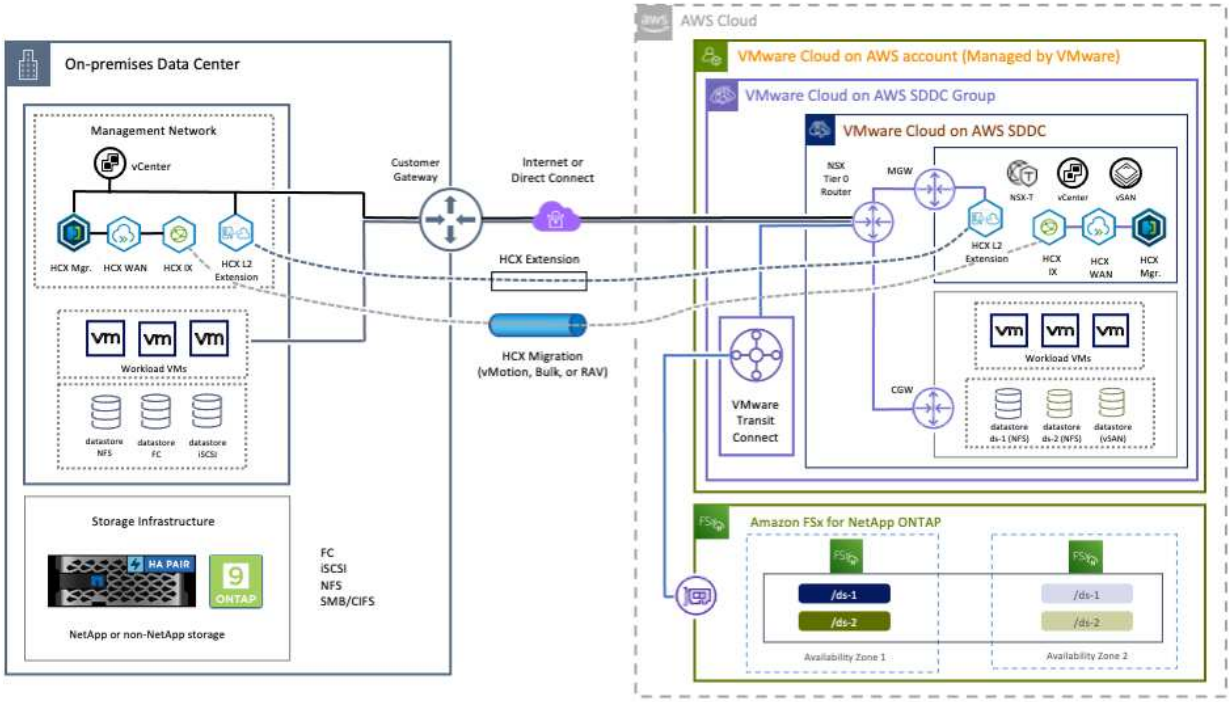
Prima di procedere con l'attivazione E l'implementazione DI HCX, è necessario completare i seguenti passaggi di installazione:

1. Utilizzare un SDDC VMC esistente o creare un nuovo SDDC in seguito "Link NetApp" o questo "Link VMware".
2. Il percorso di rete dall'ambiente vCenter on-premise all'SDDC VMC deve supportare la migrazione delle macchine virtuali utilizzando vMotion.
3. Assicurarsi di aver selezionato il necessario "porte e regole del firewall" Sono consentiti per il traffico vMotion tra vCenter Server on-premise e vCenter SDDC.
4. Il volume NFS FSX per ONTAP deve essere montato come datastore supplementare nell'SDDC VMC. Per collegare gli archivi dati NFS al cluster appropriato, seguire la procedura descritta in questa sezione "Link NetApp" o questo "Link VMware".

Architettura di alto livello

A scopo di test, l'ambiente di laboratorio on-premise utilizzato per questa convalida è stato collegato tramite una VPN sito-sito ad AWS VPC, che ha consentito la connettività on-premise ad AWS e a VMware Cloud SDDC tramite External Transit Gateway. La migrazione HCX e il traffico di estensione della rete fluiscono su Internet tra SDDC di destinazione cloud on-premise e VMware. Questa architettura può essere modificata per utilizzare le interfacce virtuali private Direct Connect.

L'immagine seguente mostra l'architettura di alto livello.



Implementazione della soluzione

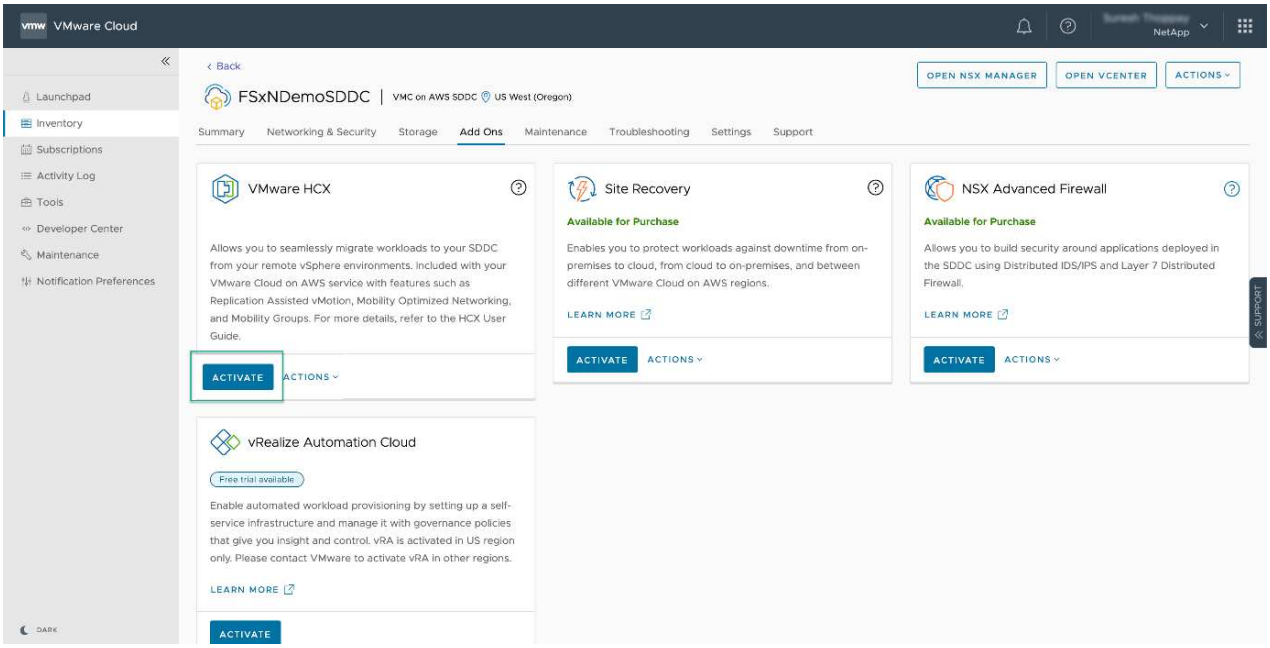
Seguire la serie di passaggi per completare l'implementazione di questa soluzione:

Fase 1: Attivare HCX tramite VMC SDDC utilizzando l'opzione Add-ons

Per eseguire l'installazione, attenersi alla seguente procedura:

1. Accedere alla console VMC all'indirizzo "vmc.vmware.com" E accedere all'inventario.
2. Per selezionare l'SDDC appropriato e accedere ai componenti aggiuntivi, fare clic su View Details (Visualizza dettagli) su SDDC e selezionare la scheda Add Ons (Aggiungi).
3. Fare clic su Activate for VMware HCX.

   Il completamento di questa fase richiede fino a 25 minuti.

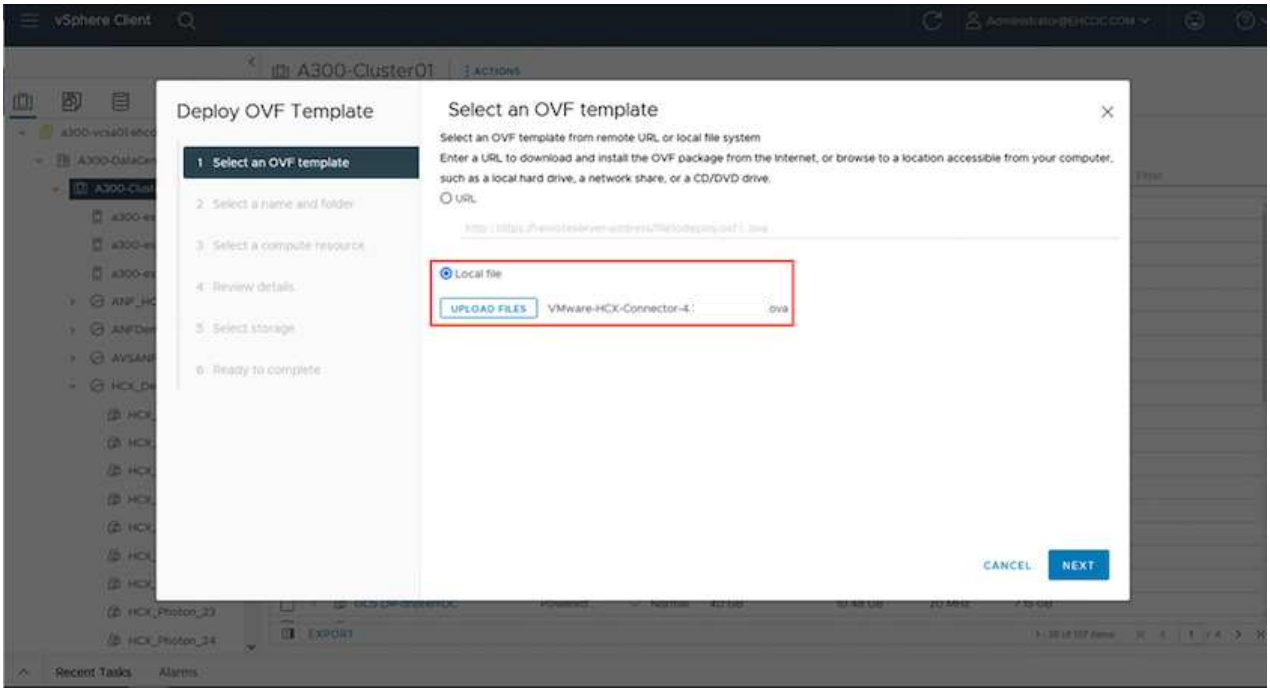


4. Una volta completata l'implementazione, convalidare l'implementazione confermando che HCX Manager e i relativi plug-in associati sono disponibili in vCenter Console.
5. Creare i firewall di Management Gateway appropriati per aprire le porte necessarie per accedere A HCX Cloud Manager.HCX Cloud Manager è ora pronto per le operazioni HCX.

Fase 2: Implementazione dell'OVA del programma di installazione nel server vCenter on-premise

Affinché il connettore on-premise comunichi con HCX Manager in VMC, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente on-premise.

1. Dalla console VMC, accedere alla dashboard HCX, accedere a Administration (Amministrazione) e selezionare la scheda Systems Update (aggiornamento sistemi). Fare clic su Request a Download link for the HCX Connector OVA image (Richiedi un link di download per l'immagine OVA
2. Dopo aver scaricato HCX Connector, implementare OVA nel server vCenter on-premise. Fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione Deploy OVF Template.

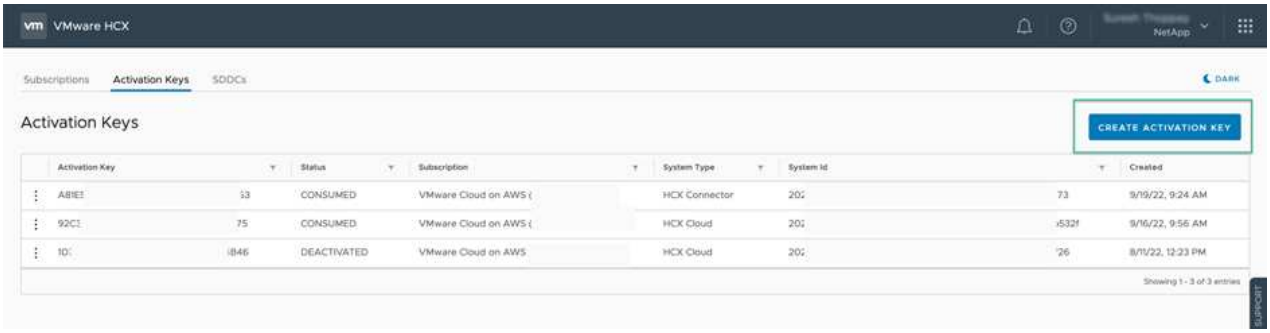


3. Inserire le informazioni richieste nella procedura guidata Deploy OVF Template (implementazione modello OVF), fare clic su Next (Avanti), quindi su Finish (fine) per implementare VMware HCX Connector OVA.
4. Accendere manualmente l'appliance virtuale.per istruzioni dettagliate, visitare il sito Web "Guida utente di VMware HCX".

Fase 3: Attivare HCX Connector con la chiave di licenza

Dopo aver implementato VMware HCX Connector OVA on-premise e avviato l'appliance, completare la seguente procedura per attivare HCX Connector. Generare la chiave di licenza dalla console VMware HCX in VMC e immettere la licenza durante la configurazione del connettore VMware HCX.

1. Da VMware Cloud Console, accedere a Inventory (inventario), selezionare SDDC e fare clic su View Details (Visualizza dettagli). Dalla scheda Add Ons (Aggiungi servizio), nel riquadro VMware HCX, fare clic su Open HCX (Apri HCX).
2. Dalla scheda Activation Keys (chiavi di attivazione), fare clic su Create Activation Key (Crea chiave di Selezionare il tipo di sistema come connettore HCX e fare clic su Confirm (Conferma) per generare la chiave. Copiare la chiave di attivazione.



> È necessaria una chiave separata per ciascun connettore HCX implementato on-premise.

3. Accedere a VMware HCX Connector on-premise all'indirizzo `"https://hcxconnectorIP:9443"` utilizzando le credenziali di amministratore.

> Utilizzare la password definita durante l'implementazione di OVA.

4. Nella sezione Licensing (licenze), inserire la chiave di attivazione copiata dal passaggio 2 e fare clic su Activate (attiva).

> Il connettore HCX on-premise deve disporre di accesso a Internet per completare correttamente l'attivazione.

5. Nella sezione Datacenter Location, specificare la posizione desiderata per l'installazione di VMware HCX Manager on-premise. Fare clic su continua.
6. In System Name (Nome sistema), aggiornare il nome e fare clic su Continue (continua).
7. Selezionare Sì, quindi continuare.
8. In Connect Your vCenter (Connetti il vCenter), fornire l'indirizzo IP o il nome di dominio completo (FQDN) e le credenziali per vCenter Server, quindi fare clic su Continue (continua).

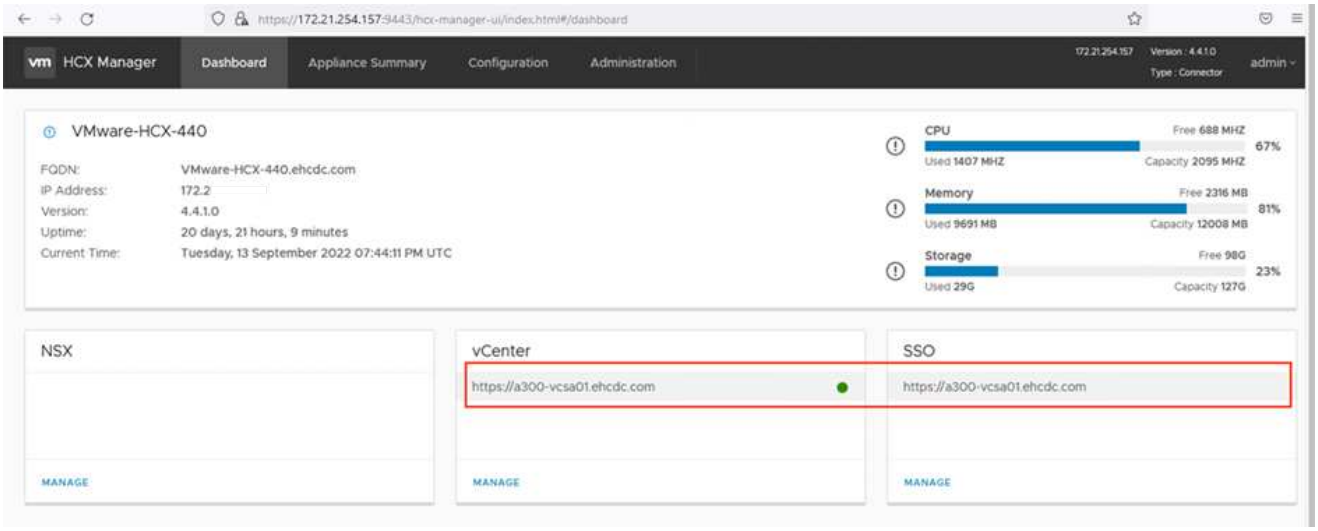
> Utilizzare l'FQDN per evitare problemi di comunicazione in un secondo momento.

9. In Configure SSO/PSC (Configura SSO/PSC), fornire l'indirizzo FQDN o IP del controller dei servizi della piattaforma e fare clic su Continue (continua).

Inserire l'indirizzo IP o l'FQDN del server vCenter.

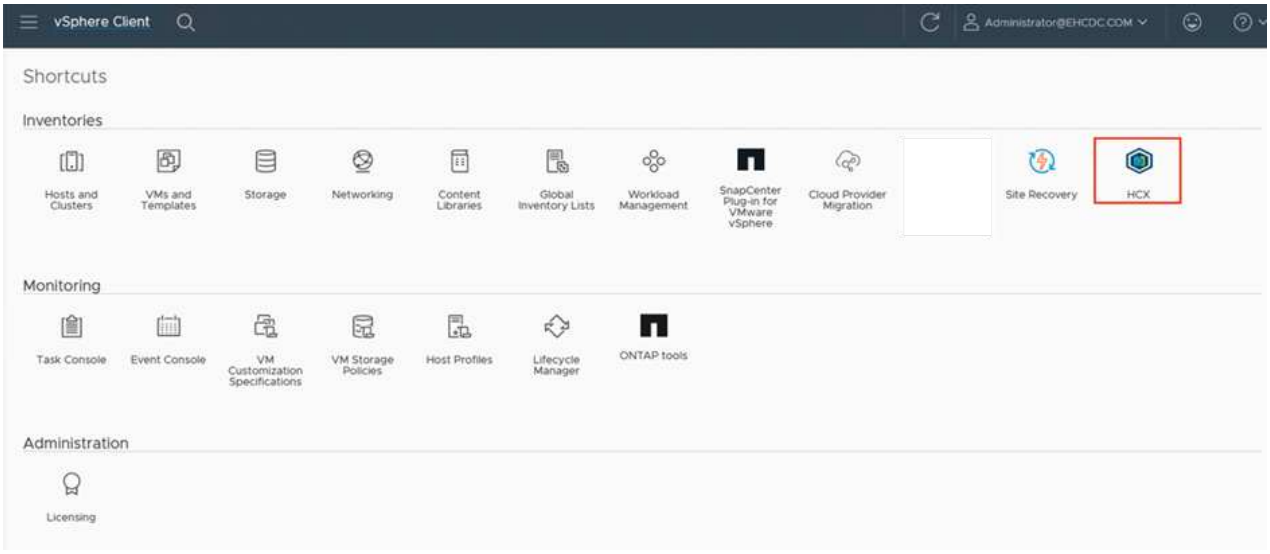
10. Verificare che le informazioni siano inserite correttamente e fare clic su Restart (Riavvia).
11. Al termine dell'operazione, vCenter Server viene visualizzato in verde. VCenter Server e SSO devono avere i parametri di configurazione corretti, che devono essere gli stessi della pagina precedente.

Questo processo richiede circa 10–20 minuti e l'aggiunta del plug-in al server vCenter.

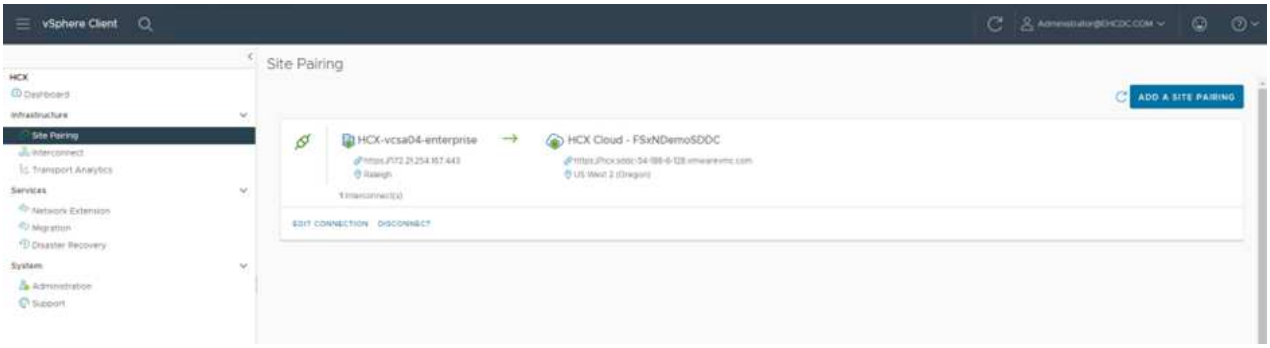


Fase 4: Associazione on-premise di VMware HCX Connector con VMC HCX Cloud Manager

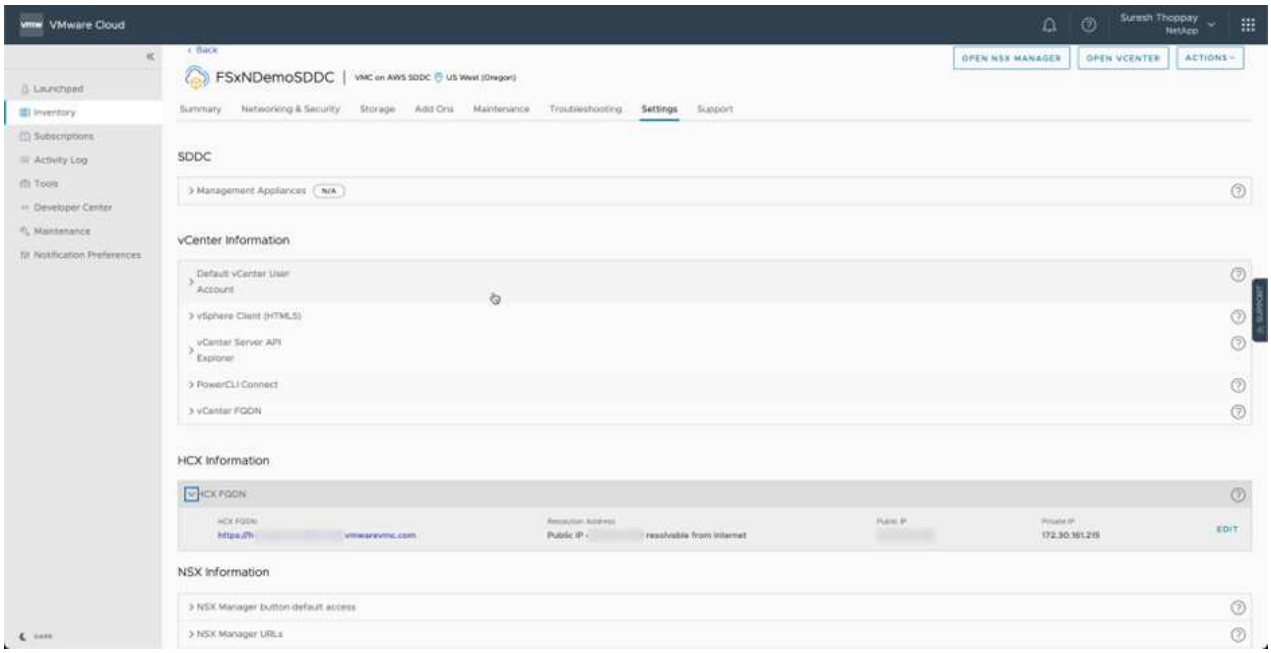
1. Per creare una coppia di siti tra vCenter Server on-premise e VMC SDDC, accedere al vCenter Server on-premise e al plug-in del client Web HCX vSphere.

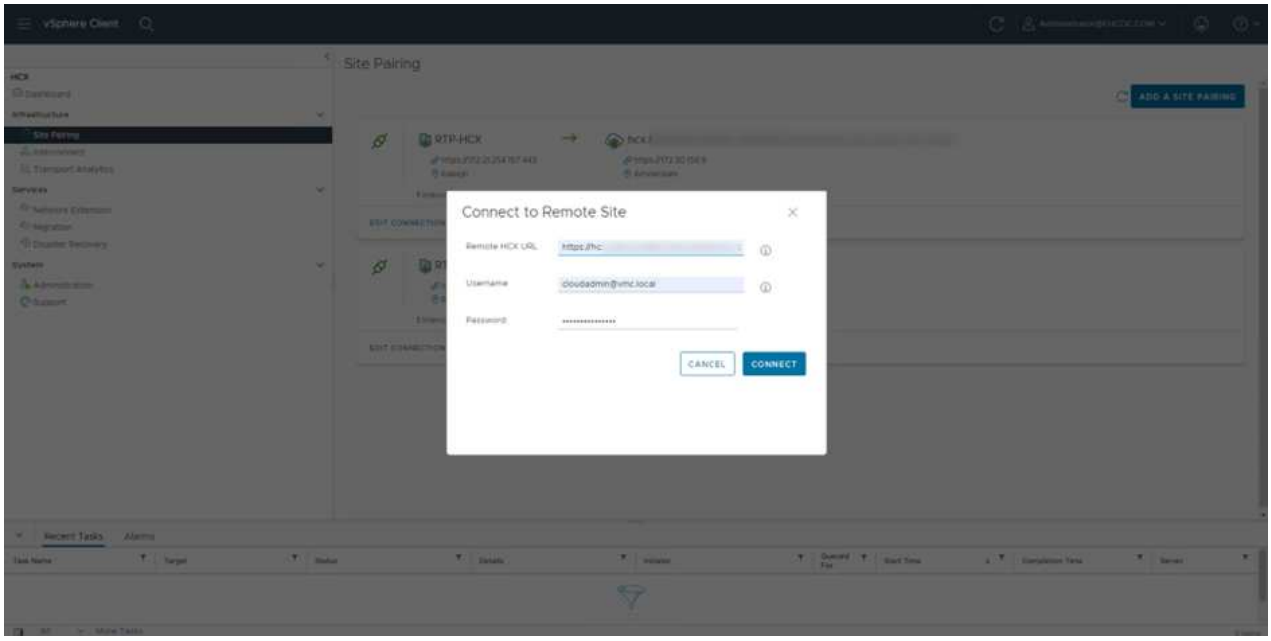


2. In infrastruttura, fare clic su Aggiungi associazione sito. Per autenticare il sito remoto, immettere l'URL o l'indirizzo IP di VMC HCX Cloud Manager e le credenziali per il ruolo CloudAdmin.



Le informazioni HCX possono essere recuperate dalla pagina Impostazioni SDDC.





3. Per avviare l'associazione del sito, fare clic su Connect (Connetti).

> VMware HCX Connector deve essere in grado di comunicare con HCX Cloud Manager IP sulla porta 443.

4. Una volta creata l'associazione, l'associazione del sito appena configurata è disponibile nella dashboard HCX.

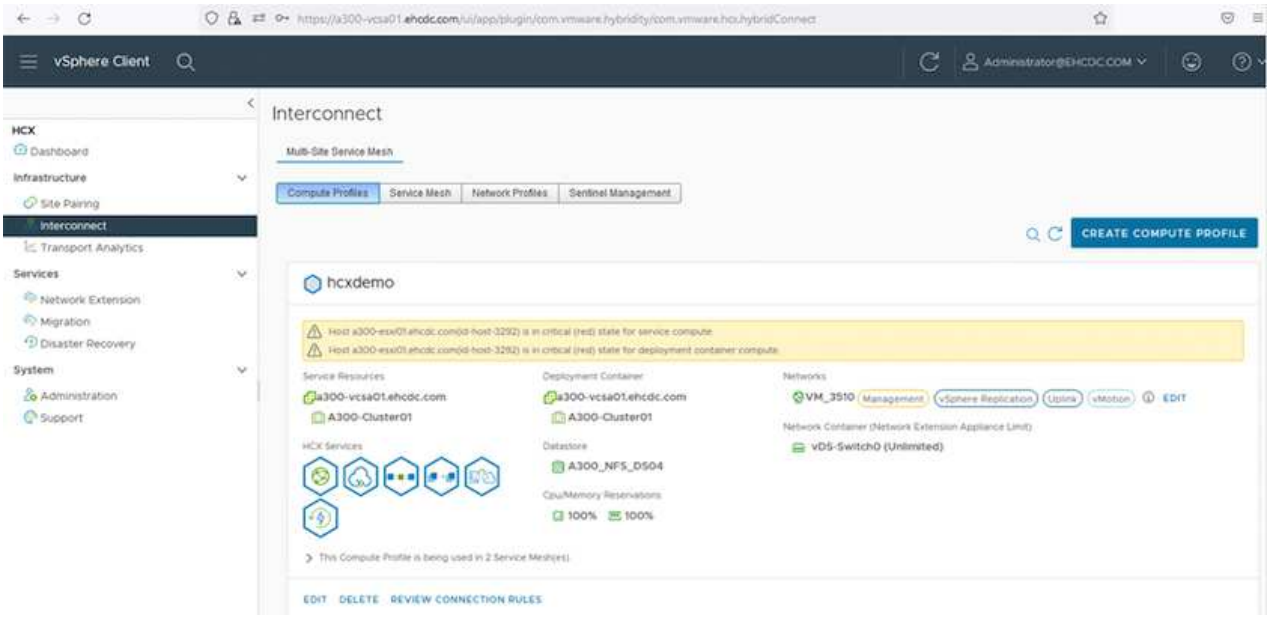
Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

L'appliance VMware HCX Interconnect (HCX-IX) offre funzionalità di tunnel sicuro su Internet e connessioni private al sito di destinazione che consentono la replica e funzionalità basate su vMotion. L'interconnessione fornisce crittografia, ingegneria del traffico e una SD-WAN. Per creare l'appliance di interconnessione HCI-IX, attenersi alla seguente procedura:

1. In Infrastructure (infrastruttura), selezionare Interconnect (interconnessione) > Multi-Site Service Mesh (Mesh servizio multi-sito) > Compute Profiles (profili di calcolo) > Create Compute Profile

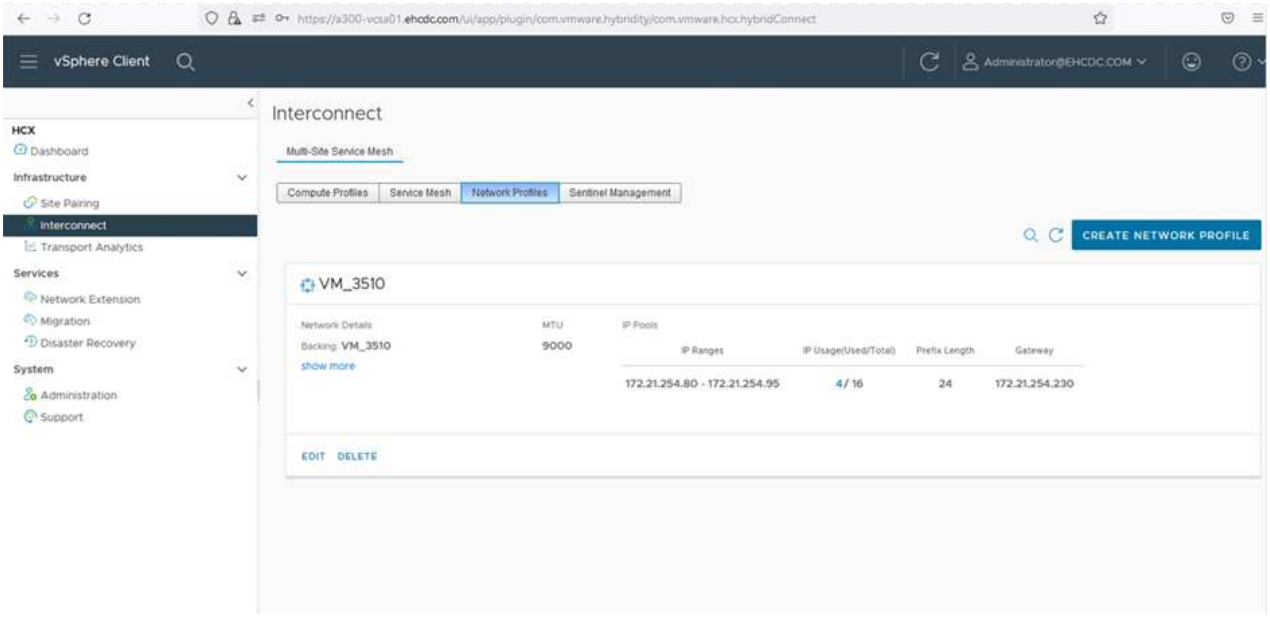
   I profili di calcolo contengono i parametri di calcolo, storage e implementazione di rete necessari per implementare un'appliance virtuale di interconnessione. Inoltre, specifica quale parte del data center VMware sarà accessibile al servizio HCX.

   Per istruzioni dettagliate, vedere "Creazione di un profilo di calcolo".



2. Una volta creato il profilo di calcolo, creare il profilo di rete selezionando Mesh servizio multi-sito > profili di rete > Crea profilo di rete.
3. Il profilo di rete definisce un intervallo di indirizzi IP e reti che VERRANNO utilizzati DA HCX per le proprie appliance virtuali.

   Questo richiede due o più indirizzi IP. Questi indirizzi IP verranno assegnati dalla rete di gestione alle appliance virtuali.

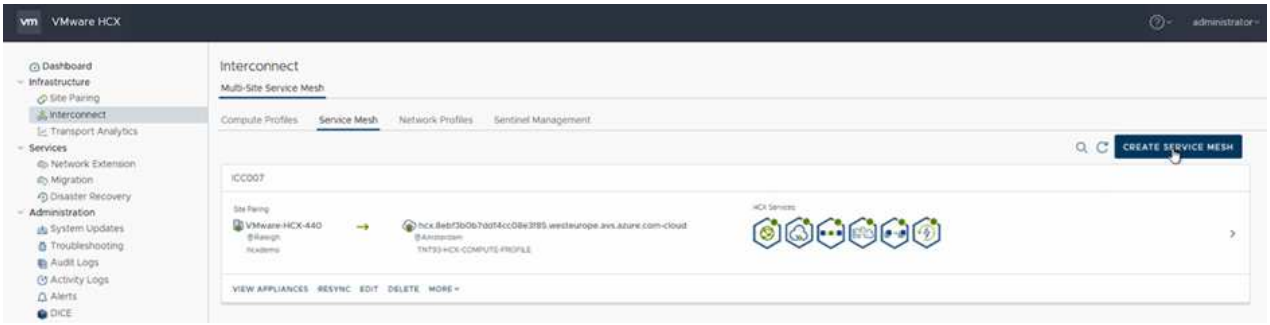


Per istruzioni dettagliate, vedere "Creazione di un profilo di rete".

Se si effettua la connessione a una SD-WAN tramite Internet, è necessario riservare gli IP pubblici nella sezione rete e sicurezza.

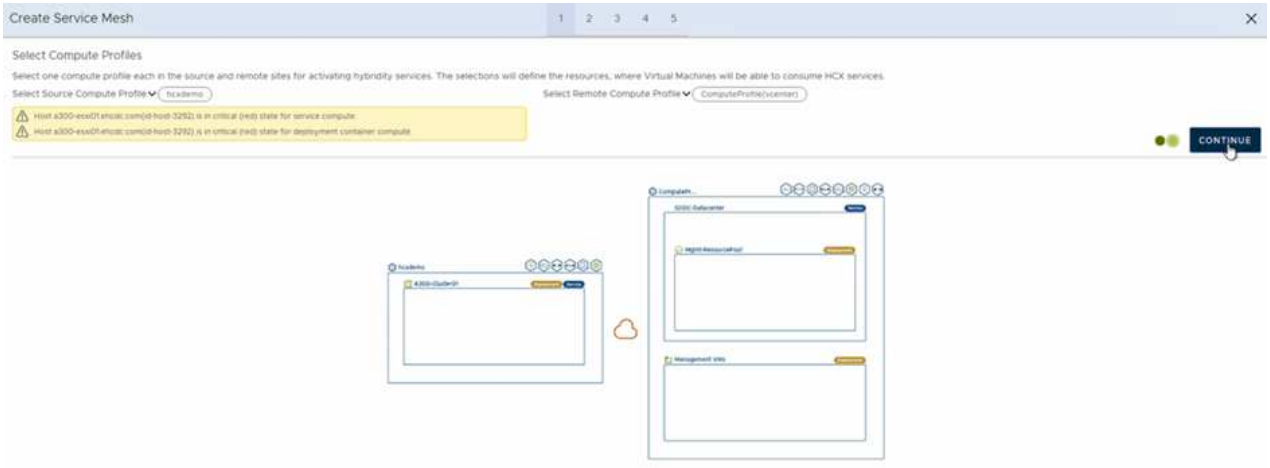
4. Per creare una mesh del servizio, selezionare la scheda Service Mesh (Mesh del servizio) all'interno dell'opzione Interconnect (interconnessione) e selezionare on-premise and VMC SDDC sites (siti SDDC on-premise e VMC).

   La mesh del servizio stabilisce una coppia di profili di rete e di calcolo locale e remoto.

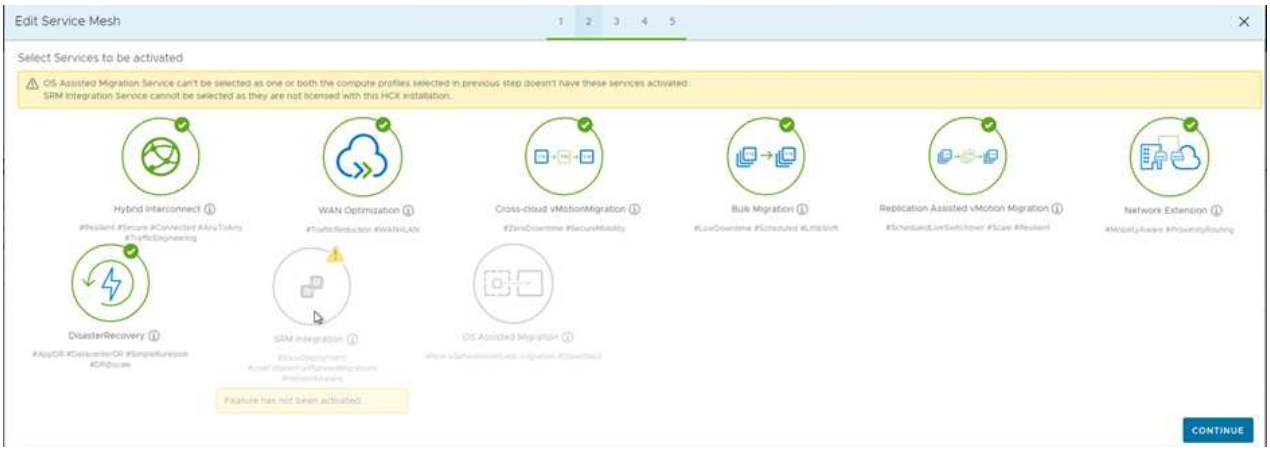


Parte di questo processo prevede l'implementazione di appliance HCX che verranno configurate automaticamente sui siti di origine e di destinazione, creando un fabric di trasporto sicuro.

5. Selezionare i profili di calcolo di origine e remoti e fare clic su Continue (continua).

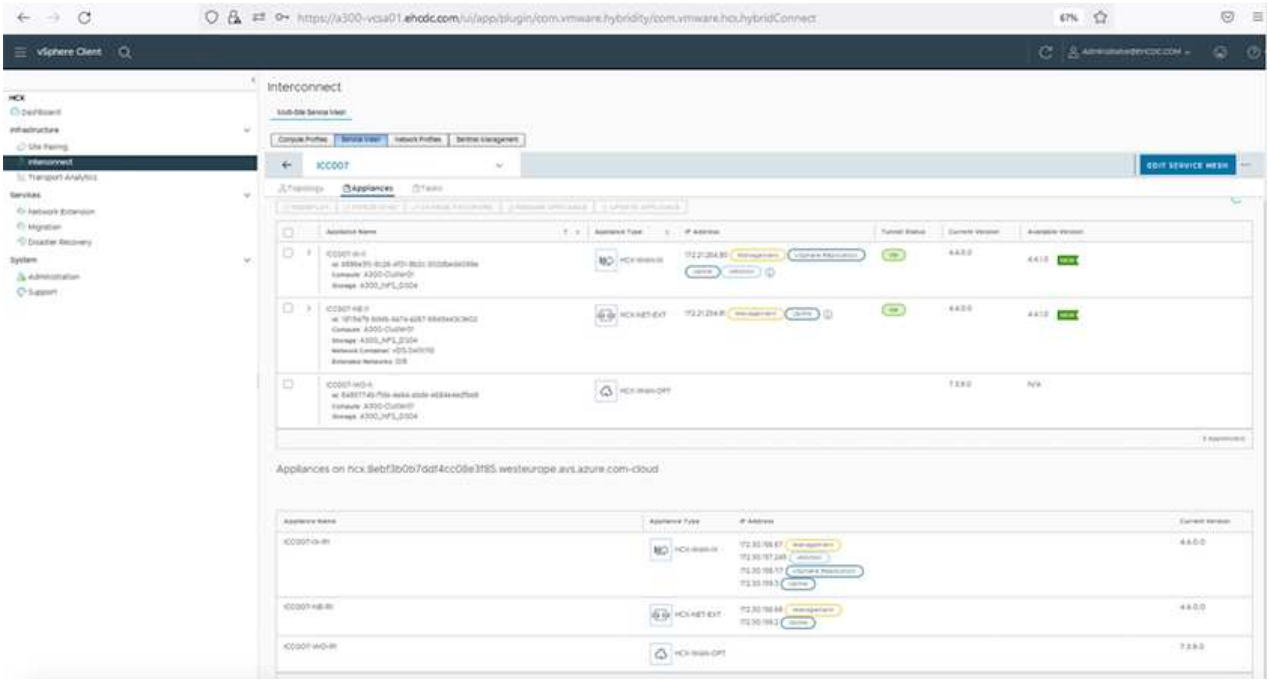


6. Selezionare il servizio da attivare e fare clic su Continue (continua).



Per la migrazione vMotion assistita da replica, l'integrazione SRM e la migrazione assistita dal sistema operativo è richiesta una licenza HCX Enterprise.

7. Creare un nome per la mesh del servizio e fare clic su Finish (fine) per avviare il processo di creazione. Il completamento dell'implementazione richiede circa 30 minuti. Dopo aver configurato la mesh del servizio, sono state create l'infrastruttura virtuale e il networking necessari per migrare le VM dei carichi di lavoro.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

Fase 6: Migrazione dei carichi di lavoro

HCX offre servizi di migrazione bidirezionale tra due o più ambienti distinti, come gli SDDC on-premise e VMC. È possibile migrare i carichi di lavoro delle applicazioni da e verso i siti attivati DA HCX utilizzando una vasta gamma di tecnologie di migrazione, come LA migrazione in blocco HCX, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (disponibile con HCX Enterprise Edition) e HCX OS Assisted Migration (disponibile con HCX Enterprise Edition).

Per ulteriori informazioni sulle tecnologie di migrazione HCX disponibili, consulta "Tipi di migrazione VMware HCX"

L'appliance HCX-IX utilizza il servizio Mobility Agent per eseguire migrazioni vMotion, Cold e Replication Assisted vMotion (RAV).

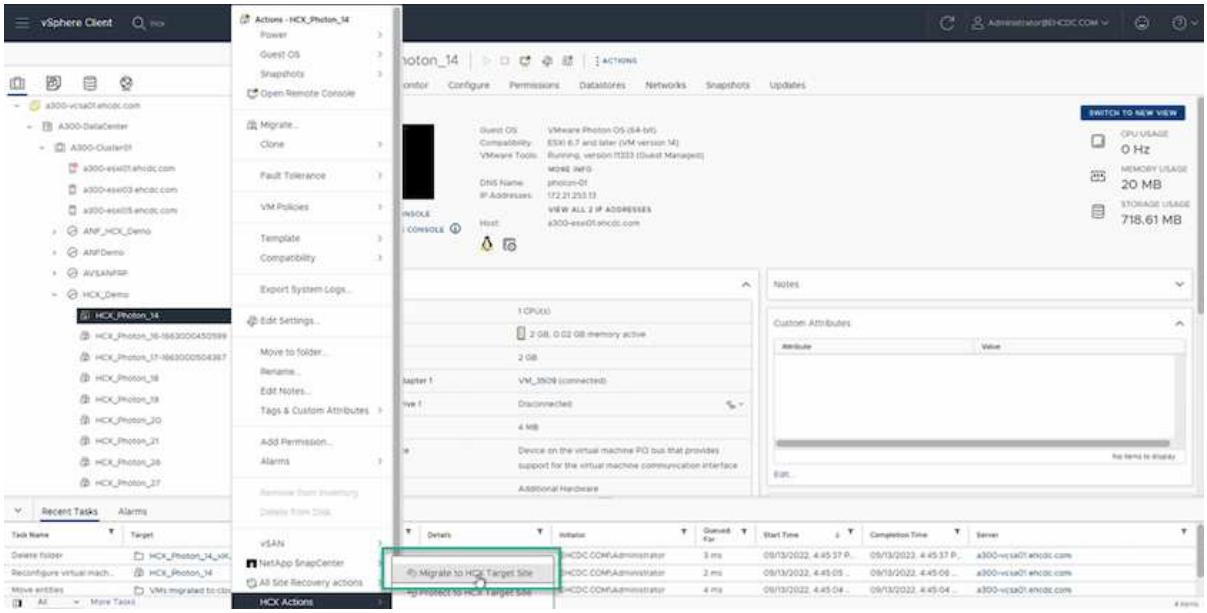
L'appliance HCX-IX aggiunge il servizio Mobility Agent come oggetto host in vCenter Server. Il processore, la memoria, lo storage e le risorse di rete visualizzati su questo oggetto non rappresentano il consumo effettivo dell'hypervisor fisico che ospita l'appliance IX.

VMware HCX vMotion

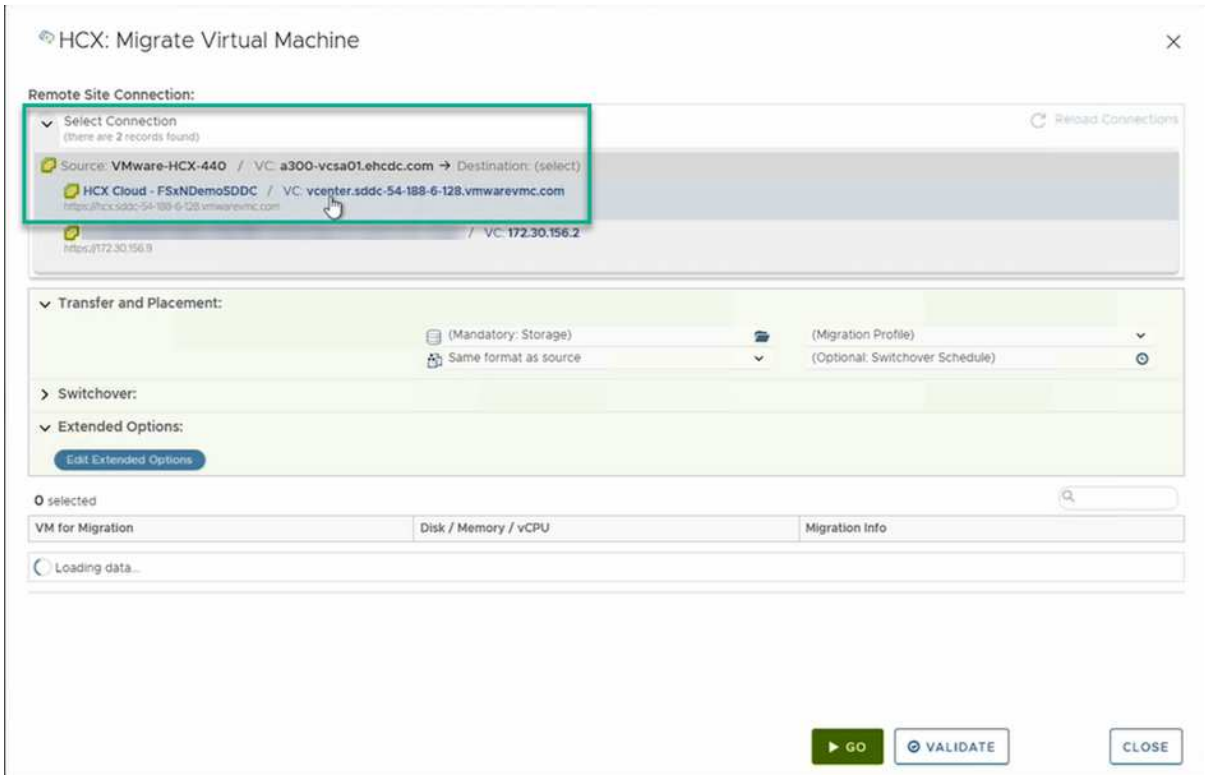
In questa sezione viene descritto il meccanismo vMotion DI HCX. Questa tecnologia di migrazione utilizza il protocollo VMware vMotion per migrare una macchina virtuale a VMC SDDC. L'opzione di migrazione vMotion viene utilizzata per la migrazione dello stato della macchina virtuale di una singola macchina virtuale alla volta. Durante questo metodo di migrazione non si verifica alcuna interruzione del servizio.

Network Extension deve essere installato (per il gruppo di porte a cui è collegata la macchina virtuale) per migrare la macchina virtuale senza dover modificare l'indirizzo IP.

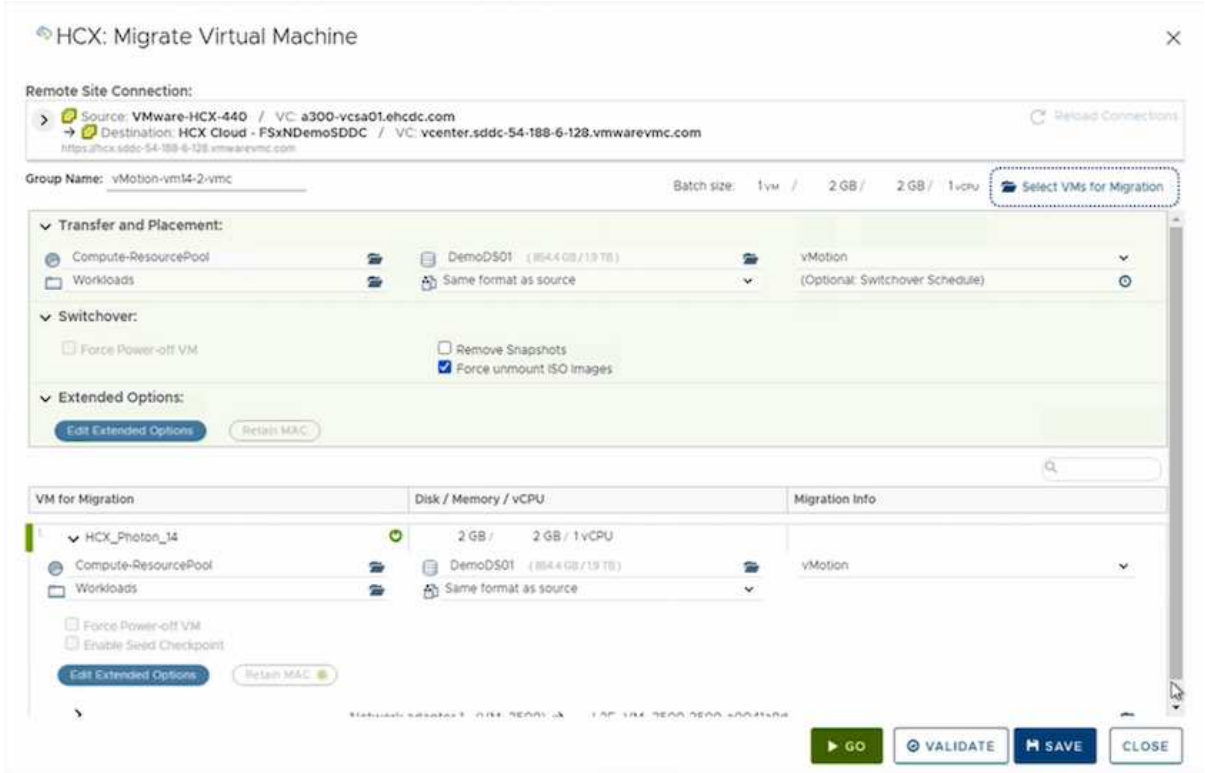
1. Dal client vSphere on-premise, accedere a Inventory (inventario), fare clic con il pulsante destro del mouse sulla macchina virtuale da migrare e selezionare HCX Actions (azioni HCX) > Migrate to HCX Target Site (Migra al sito di destinazione HCX).



2. Nella procedura guidata Migrate Virtual Machine, selezionare Remote Site Connection (SDDC VMC di destinazione).



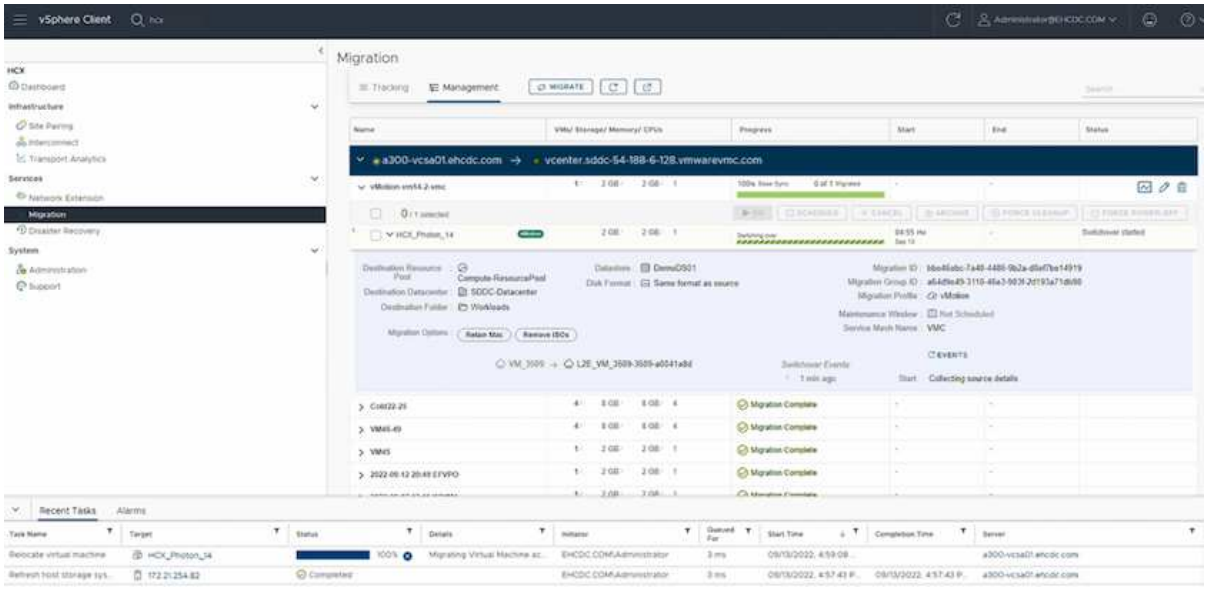
3. Aggiungere un nome di gruppo e, in Transfer and Placement (trasferimento e posizionamento), aggiornare i campi obbligatori (Cluster, Storage e Destination Network), quindi fare clic su Validate (convalida).



4. Al termine dei controlli di convalida, fare clic su Go (Vai) per avviare la migrazione.

Il trasferimento vMotion acquisisce la memoria attiva della macchina virtuale, il suo stato di esecuzione, il suo indirizzo IP e il suo indirizzo MAC. Per ulteriori informazioni sui requisiti e sulle limitazioni di HCX vMotion, vedere "Informazioni su VMware HCX vMotion e Cold Migration".

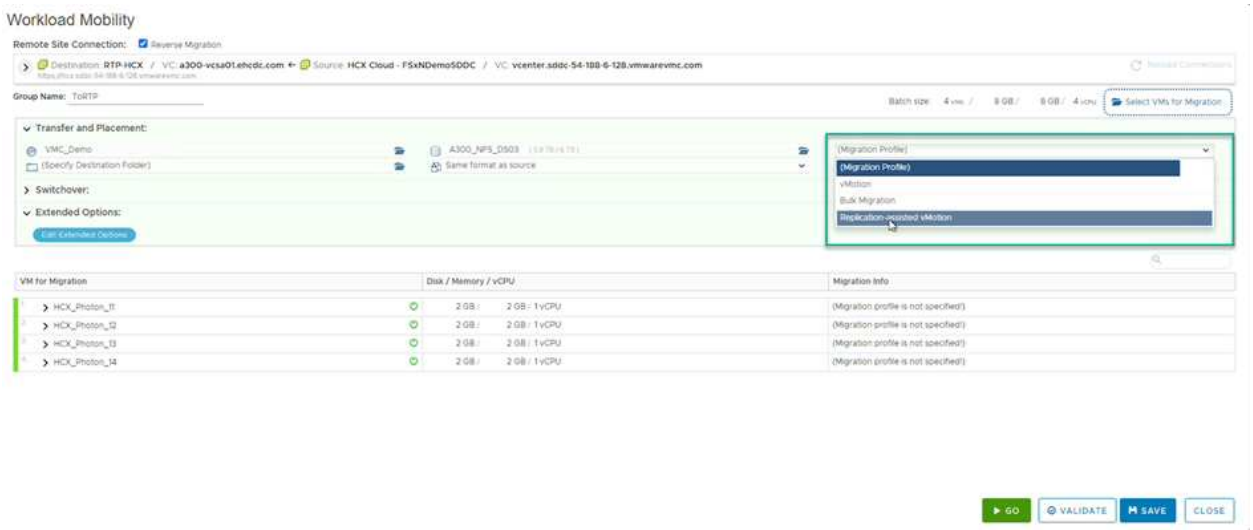
5. È possibile monitorare l'avanzamento e il completamento di vMotion dalla dashboard HCX > Migration (HCX > migrazione).



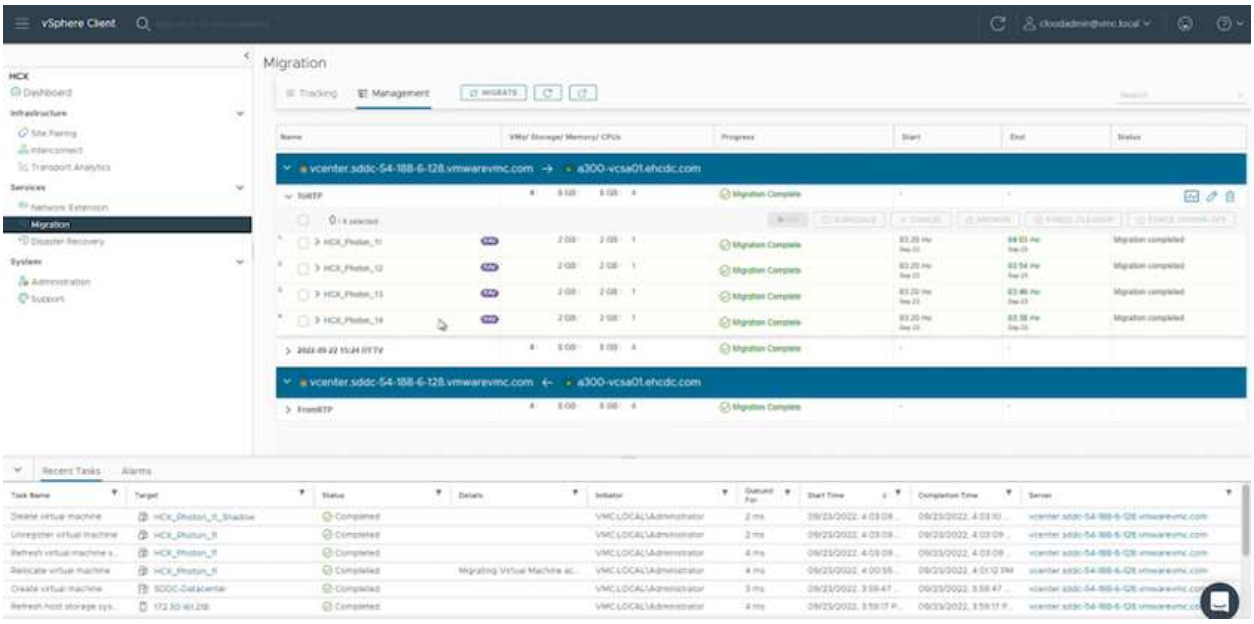
VMotion VMware Replication Assisted

Come si può notare dalla documentazione VMware, VMware HCX Replication Assisted vMotion (RAV) combina i vantaggi della migrazione in blocco e di vMotion. La migrazione in blocco utilizza la replica vSphere per migrare più macchine virtuali in parallelo: La macchina virtuale viene riavviata durante lo switchover. HCX vMotion esegue la migrazione senza downtime, ma viene eseguita in maniera seriale una macchina virtuale alla volta in un gruppo di replica. RAV replica la macchina virtuale in parallelo e la mantiene sincronizzata fino alla finestra di switchover. Durante il processo di switchover, effettua la migrazione di una macchina virtuale alla volta senza downtime per la macchina virtuale.

La seguente schermata mostra il profilo di migrazione come Replication Assisted vMotion.



La durata della replica potrebbe essere maggiore rispetto al vMotion di un numero ridotto di macchine virtuali. Con RAV, sincronizzare solo i delta e includere i contenuti della memoria. Di seguito viene riportata una schermata dello stato della migrazione, che mostra come l'ora di inizio della migrazione sia la stessa e l'ora di fine sia diversa per ciascuna macchina virtuale.



Per ulteriori informazioni sulle opzioni di migrazione HCX e su come migrare i carichi di lavoro da on-premise a VMware Cloud su AWS utilizzando HCX, consulta la "Guida utente di VMware HCX".

VMware HCX vMotion richiede un throughput di 100 Mbps o superiore.

Il datastore VMC FSX di destinazione per ONTAP deve disporre di spazio sufficiente per consentire la migrazione.

Conclusione

Sia che tu stia prendendo di mira il cloud all-cloud o ibrido e i dati che risiedono su storage di qualsiasi tipo/vendor in on-premise, Amazon FSX per NetApp ONTAP insieme A HCX offrono opzioni eccellenti per implementare e migrare i carichi di lavoro riducendo al contempo il TCO rendendo i requisiti dei dati perfetti per il livello applicativo. Qualunque sia il caso d'utilizzo, scegli VMC insieme a FSX per il datastore ONTAP per una rapida realizzazione dei benefici del cloud, un'infrastruttura coerente e operazioni su cloud multipli e on-premise, portabilità bidirezionale dei carichi di lavoro e capacità e performance di livello Enterprise. Si tratta degli stessi processi e procedure familiari utilizzati per connettere lo storage e migrare le macchine virtuali utilizzando la replica VMware vSphere, VMware vMotion o persino la copia NFC.

Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Amazon FSX ONTAP come datastore con VMC SDDC.
- È possibile migrare facilmente i dati da qualsiasi data center on-premise a VMC in esecuzione con FSX per datastore ONTAP
- È possibile espandere e ridurre facilmente il datastore FSX ONTAP per soddisfare i requisiti di capacità e performance durante l'attività di migrazione.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, fare riferimento ai seguenti collegamenti Web:

- Documentazione di VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Documentazione di Amazon FSX per NetApp ONTAP

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  Guida utente di VMware HCX

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Disponibilità regionale: Datastore NFS supplementare per VMC

Scopri di più sul supporto regionale globale per AWS, VMC ed FSX ONTAP.

L'archivio dati NFS sarà disponibile nelle aree in cui sono disponibili entrambi i servizi (VMC ed FSX ONTAP).

La disponibilità di datastore NFS supplementari su AWS / VMC è definita da Amazon. Innanzitutto, è necessario determinare se VMC e FSxN sono disponibili in una regione specifica. Quindi, è necessario determinare se il datastore NFS supplementare FSxN è supportato in quella regione.

- Verificare la disponibilità di VMC "qui".
- La guida ai prezzi di Amazon offre informazioni su dove è disponibile FSxN (FSX ONTAP). Queste informazioni sono disponibili "qui".
- La disponibilità del datastore NFS supplementare FSxN per VMC sarà presto disponibile.

Mentre le informazioni sono ancora in fase di rilascio, il seguente grafico identifica il supporto corrente per VMC, FSxN e FSxN come datastore NFS supplementare.

Americhe

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
US East (Virginia del Nord)	Sì	Sì	Sì
USA Est (Ohio)	Sì	Sì	Sì
US West (California settentrionale)	Sì	No	No
STATI UNITI occidentali (Oregon)	Sì	Sì	Sì
GovCloud (ovest degli Stati Uniti)	Sì	Sì	Sì
Canada (centrale)	Sì	Sì	Sì
Sud America (San Paolo)	Sì	Sì	Sì

Ultimo aggiornamento: 2 giugno 2022.

EMEA

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
Europa (Irlanda)	Sì	Sì	Sì
Europa (Londra)	Sì	Sì	Sì
Europa (Francoforte)	Sì	Sì	Sì
Europa (Parigi)	Sì	Sì	Sì
Europa (Milano)	Sì	Sì	Sì
Europa (Stoccolma)	Sì	Sì	Sì

Ultimo aggiornamento: 2 giugno 2022.

Asia Pacifico

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
Asia Pacifico (Sydney)	Sì	Sì	Sì
Asia Pacifico (Tokyo)	Sì	Sì	Sì
Asia Pacifico (Osaka)	Sì	No	No
Asia Pacifico (Singapore)	Sì	Sì	Sì
Asia Pacifico (Seul)	Sì	Sì	Sì
Asia Pacifico (Mumbai)	Sì	Sì	Sì

Asia Pacifico (Giacarta)	No	No	No
Asia Pacifico (Hong Kong)	Sì	Sì	Sì

Ultimo aggiornamento: 28 settembre 2022.