



## **NetApp per Azure/AVS**

### **NetApp Solutions**

NetApp  
April 26, 2024

# Sommario

- Multicloud ibrido NetApp con soluzioni VMware ..... 1
  - Protezione dei carichi di lavoro su Azure/AVS ..... 1
  - Migrazione dei carichi di lavoro su Azure/AVS..... 63
  - Disponibilità regionale: Datastore NFS supplementare per ANF ..... 80

# Multicloud ibrido NetApp con soluzioni VMware

## Protezione dei carichi di lavoro su Azure/AVS

### Disaster Recovery con ANF e JetStream

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). Utilizzando il framework VMware VAIO, è possibile replicare i workload VMware on-premise sullo storage Azure Blob e ripristinarli, consentendo una perdita di dati minima o quasi nulla e un RTO quasi nullo.

Il DR Jetstream può essere utilizzato per ripristinare perfettamente i carichi di lavoro replicati da on-premise ad AVS e in particolare a Azure NetApp Files. Consente un disaster recovery conveniente utilizzando risorse minime presso il sito di DR e uno storage cloud conveniente. Jetstream DR automatizza il ripristino degli archivi dati ANF tramite Azure Blob Storage. Jetstream DR ripristina macchine virtuali indipendenti o gruppi di macchine virtuali correlate nell'infrastruttura del sito di ripristino in base alla mappatura di rete e fornisce un ripristino point-in-time per la protezione ransomware.

Il presente documento fornisce informazioni sui principi operativi di DR di JetStream e sui relativi componenti principali.

## Panoramica sull'implementazione della soluzione

1. Installare il software DR JetStream nel data center on-premise.
  - a. Scarica il pacchetto software DR JetStream da Azure Marketplace (ZIP) e implementa il DR MSA (OVA) JetStream nel cluster designato.
  - b. Configurare il cluster con il pacchetto di filtri i/o (installare JetStream VIB).
  - c. Provisioning di Azure Blob (Azure Storage account) nella stessa regione del cluster DR AVS.
  - d. Implementare appliance DRVA e assegnare volumi di log di replica (VMDK da datastore esistente o storage iSCSI condiviso).
  - e. Creare domini protetti (gruppi di macchine virtuali correlate) e assegnare DRVA e Azure Blob Storage/ANF.
  - f. Protezione all'avviamento.
2. Installare il software DR JetStream nel cloud privato Azure VMware Solution.
  - a. Utilizzare il comando Esegui per installare e configurare il DR JetStream.
  - b. Aggiungere lo stesso container Azure Blob e individuare i domini utilizzando l'opzione Scan Domains (domini di scansione).
  - c. Implementare le appliance DRVA richieste.
  - d. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
  - e. Importare domini protetti e configurare ROCvA (Recovery VA) per utilizzare il datastore ANF per il posizionamento delle macchine virtuali.
  - f. Selezionare l'opzione di failover appropriata e avviare la reidratazione continua per domini RTO o macchine virtuali quasi a zero.
3. Durante un evento di emergenza, attivare il failover degli archivi dati Azure NetApp Files nel sito di DR AVS designato.
4. Richiamare il failback sul sito protetto dopo il ripristino del sito protetto. prima di iniziare, assicurarsi che i prerequisiti siano soddisfatti, come indicato in questa sezione "[collegamento](#)". Inoltre, eseguire il Bandwidth Testing Tool (BWT) fornito dal software JetStream per valutare le performance potenziali dello storage Azure Blob e la relativa larghezza di banda di replica se utilizzato con il software DR JetStream. Una volta implementati i prerequisiti, inclusa la connettività, impostare e sottoscrivere JetStream DR per AVS da "[Azure Marketplace](#)". Una volta scaricato il pacchetto software, procedere con la procedura di installazione descritta in precedenza.

Quando si pianifica e si avvia la protezione per un gran numero di macchine virtuali (ad esempio, 100+), utilizzare il Capacity Planning Tool (CPT) di JetStream DR Automation Toolkit. Fornire un elenco di macchine virtuali da proteggere insieme alle preferenze RTO e del gruppo di ripristino, quindi eseguire CPT.

CPT esegue le seguenti funzioni:

- Combinazione di macchine virtuali in domini di protezione in base al proprio RTO.
- Definizione del numero ottimale di DRVA e delle relative risorse.
- Stima della larghezza di banda di replica richiesta.
- Identificazione delle caratteristiche del volume del registro di replica (capacità, larghezza di banda e così via).
- Stima della capacità di storage a oggetti richiesta e molto altro ancora.



Il numero e il contenuto dei domini prescritti dipendono da diverse caratteristiche delle macchine virtuali, come IOPS medi, capacità totale, priorità (che definisce l'ordine di failover), RTO e altre.

### **Installare JetStream DR in Datacenter on-premise**

Il software Jetstream DR è costituito da tre componenti principali: Appliance virtuale Jetstream DR Management Server (MSA), appliance virtuale DR (DRVA) e componenti host (pacchetti di filtro i/o). MSA viene utilizzato per installare e configurare i componenti host sul cluster di calcolo e quindi per amministrare il software DR JetStream. Il seguente elenco fornisce una descrizione dettagliata del processo di installazione:

## Come installare JetStream DR per on-premise

1. Verificare i prerequisiti.
2. Eseguire Capacity Planning Tool per ottenere consigli su risorse e configurazione (facoltativo ma consigliato per le prove proof-of-concept).
3. Implementare l'MSA DR JetStream su un host vSphere nel cluster designato.
4. Avviare MSA utilizzando il nome DNS in un browser.
5. Registrare il server vCenter con MSA.per eseguire l'installazione, attenersi alla seguente procedura dettagliata:
6. Una volta implementato JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR utilizzando vSphere Web Client. Per eseguire questa operazione, accedere a Datacenter > Configure > JetStream DR.



7. Dall'interfaccia DR di JetStream, selezionare il cluster appropriato.



8. Configurare il cluster con il pacchetto di filtri i/O.



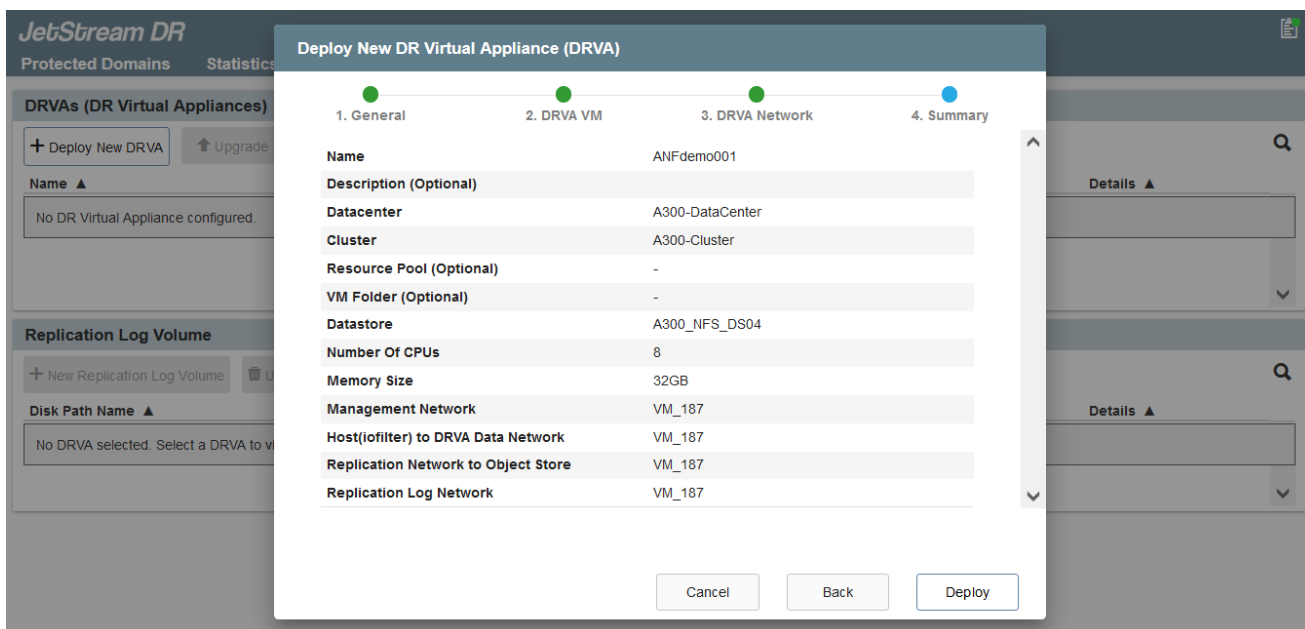
9. Aggiungere Azure Blob Storage situato nel sito di ripristino.

10. Implementare un'appliance virtuale DR (DRVA) dalla scheda Appliances (appliance).



I DRA possono essere creati automaticamente dal CPT, ma per le prove POC consigliamo di configurare ed eseguire manualmente il ciclo di DR (protezione dell'avvio > failover > failback).

JetStream DRVA è un'appliance virtuale che facilita le funzioni chiave nel processo di replica dei dati. Un cluster protetto deve contenere almeno un DRVA e, in genere, un DRVA viene configurato per host. Ogni DRVA può gestire più domini protetti.



In questo esempio, sono stati creati quattro DRVA per 80 macchine virtuali.

1. Creare volumi di log di replica per ogni DRVA utilizzando VMDK dagli archivi dati disponibili o da pool di storage iSCSI condivisi indipendenti.

2. Dalla scheda Protected Domains (domini protetti), creare il numero richiesto di domini protetti utilizzando le informazioni relative al sito Azure Blob Storage, all'istanza DRVA e al registro di replica. Un dominio protetto definisce una macchina virtuale specifica o un insieme di macchine virtuali all'interno del cluster che sono protetti insieme e assegnati a un ordine di priorità per le operazioni di failover/failback.

**JetStream DR**

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: + Create More

**Create Protected Domain**

1. General 2. Primary Site 3. Summary

Protected Domain Name: ANFPD001

Priority Level (Optional): 1

Total estimated data size to be protected: 1000GB

DR Virtual Appliance: ANFdemo001

Compression: Yes

Compression Level: Default

Normal GC Storage Overhead: 50%

Maximum GC Storage Overhead: 300%

Replication Log Storage: /dev/sdb

Replication Log Size: 94.31GB

Metadata Size: 31.56GB

Cancel Back Create

3. Selezionare le macchine virtuali che si desidera proteggere e avviare la protezione delle macchine virtuali del dominio protetto. In questo modo viene avviata la replica dei dati nell'archivio Blob designato.



Verificare che venga utilizzata la stessa modalità di protezione per tutte le macchine virtuali in un dominio protetto.



La modalità Write-Back (VMDK) può offrire performance superiori.

**JetStream DR**

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: ANFPD001

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs | Settings | Alerts

+ Start Protection Stop Protection

☐ VM Name No VM is protected.

**Start Protection**

Protection Mode for selected VMs: Write-Back(VMDK)

<input type="checkbox"/> VM Name	# of Disks...	Protection Mode
<input checked="" type="checkbox"/> AuctionAppA1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionAppB1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionDB1	2	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionLB1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionMSQ1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionNoSQL1	2	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionWebA1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionWebB1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> Client1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> D32DB1	2	Write-Back(VMDK)

Cancel Start Protection



Verificare che i volumi dei log di replica siano posizionati su uno storage dalle performance elevate.



I run book di failover possono essere configurati per raggruppare le macchine virtuali (denominate Recovery Group), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

## **Installare JetStream DR per AVS in un cloud privato Azure VMware Solution utilizzando il comando Run**

Una Best practice per un sito di recovery (AVS) consiste nella creazione anticipata di un cluster pilota a tre nodi. Ciò consente di preconfigurare l'infrastruttura del sito di ripristino, inclusi i seguenti elementi:

- Segmenti di rete di destinazione, firewall, servizi come DHCP e DNS e così via.
- Installazione di JetStream DR per AVS
- Configurazione dei volumi ANF come datastore e inoltre JetStream DR supporta la modalità RTO quasi zero per i domini mission-critical. Per questi domini, lo storage di destinazione deve essere preinstallato. ANF è un tipo di storage consigliato in questo caso.



La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS per soddisfare i requisiti on-premise.

A seconda dei requisiti SLA e RTO, è possibile utilizzare il failover continuo o la normale modalità di failover (standard). Per un RTO vicino allo zero, è necessario avviare una procedura di reidratazione continua presso il sito di ripristino.

## Come installare JetStream DR per AVS in un cloud privato

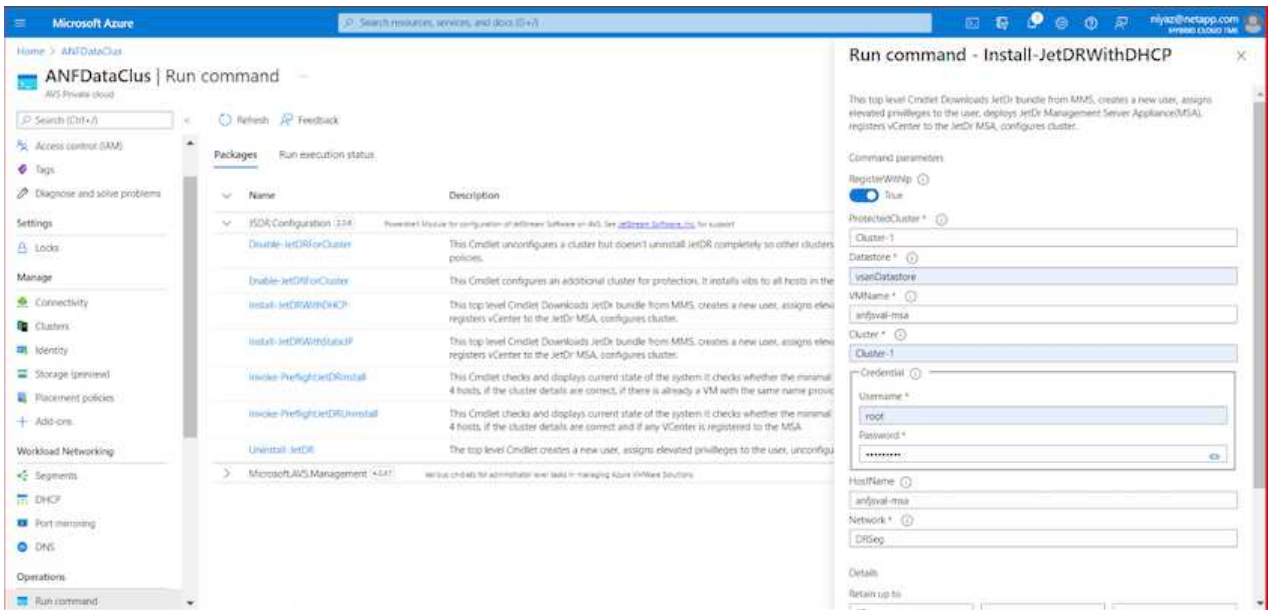
Per installare JetStream DR per AVS su un cloud privato Azure VMware Solution, attenersi alla seguente procedura:

1. Dal portale Azure, accedere alla soluzione Azure VMware Solution, selezionare il cloud privato e selezionare Esegui comando > pacchetti > Configurazione JSDR.



L'utente CloudAdmin predefinito in Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente un'installazione semplificata e automatica del DR JetStream invocando il comando Azure VMware Solution Run per il DR JetStream.

La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente DR JetStream, accedere a SDDC Datacenter > Configura > JetStream DR.

**JetStream DR** Protected Domains Statistics Storage Sites Appliances **Configurations** Task Log

**Site Details** [Alarm Settings](#)

vCenter Server Hostname 172.30.156.2

Management Appliance Hostname anfsval-msa

Software Version 4.0.2.450

Subscription ID - [Configure](#)

Tenant ID / Application ID - [Configure](#)

Application Secret - [Configure](#)

[Configure Cluster](#) [Upgrade](#) [Unconfigure](#) [Resolve Configure Issue](#)

<input type="checkbox"/>	Cluster Name ▲	Datacenter Name ▲	Status ▲	Software Version ▲	Host Details ▲
<input type="checkbox"/>	Cluster-1	SDDC-Datacenter	Ok	4.0.2.132	<a href="#">Details</a>

- Dall'interfaccia DR di JetStream, aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster on-premise come sito di storage, quindi eseguire l'opzione Scan Domains.

**JetStream DR** Protected Domains Statistics Storage Sites Appliances Configurations Task Log

**Available Protected Domain(s) For Import**

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
ANFPD000	Protected Domain Tile0	20	20	<a href="#">Import</a>
ANFPD001	-	20	20	<a href="#">Import</a>
ANFPD002	Protected Domain 02	20	20	<a href="#">Import</a>
ANFPD003	Protected Domain Tile 03	20	20	<a href="#">Import</a>

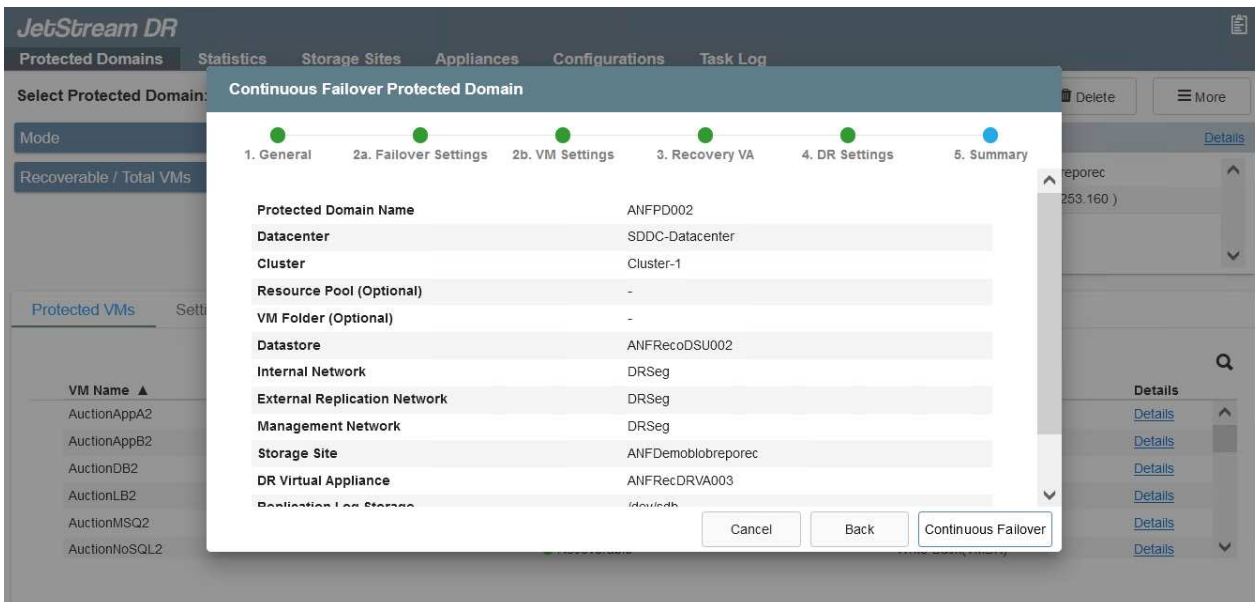
[Close](#)

- Una volta importati i domini protetti, implementare le appliance DRVA. In questo esempio, la reidratazione continua viene avviata manualmente dal sito di ripristino utilizzando l'interfaccia utente DR JetStream.



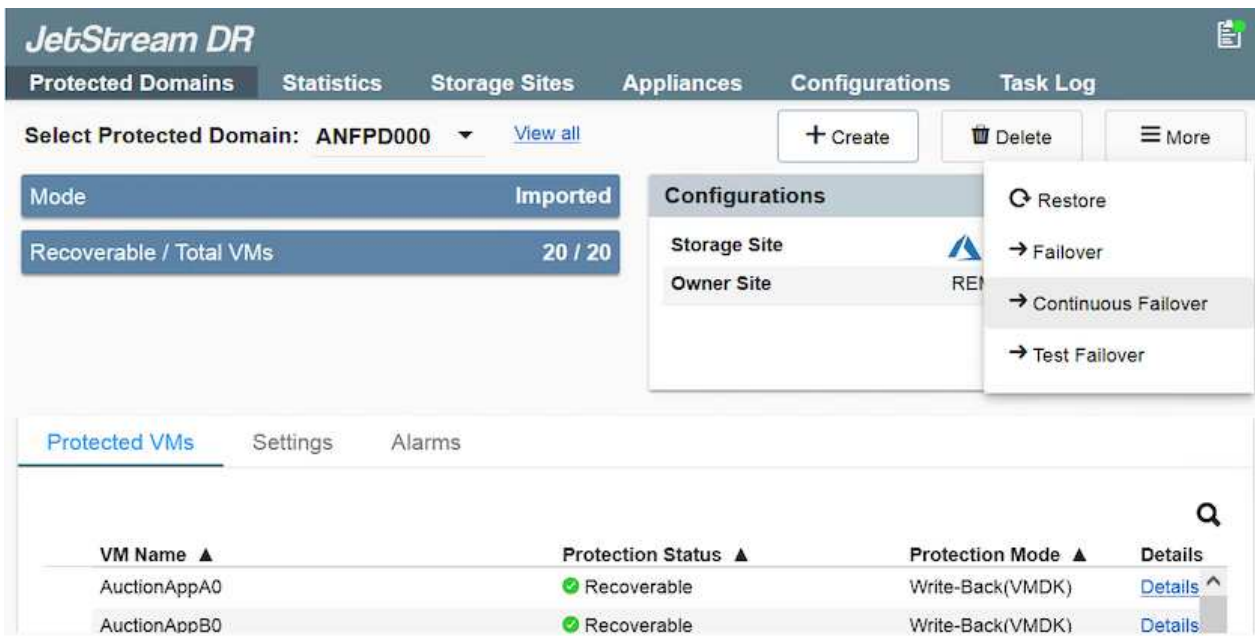
Questi passaggi possono anche essere automatizzati utilizzando i piani creati da CPT.

- Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
- Importare i domini protetti e configurare Recovery VA in modo che utilizzi il datastore ANF per il posizionamento delle macchine virtuali.



Assicurarsi che DHCP sia attivato sul segmento selezionato e che sia disponibile un numero sufficiente di IP. Gli IP dinamici vengono temporaneamente utilizzati durante il ripristino dei domini. Ogni macchina virtuale di ripristino (inclusa la reidratazione continua) richiede un IP dinamico individuale. Una volta completato il ripristino, l'IP viene rilasciato e può essere riutilizzato.

7. Selezionare l'opzione di failover appropriata (failover o failover continuo). In questo esempio, viene selezionata la reidratazione continua (failover continuo).



## Esecuzione di failover/failover

## Come eseguire un failover/failover

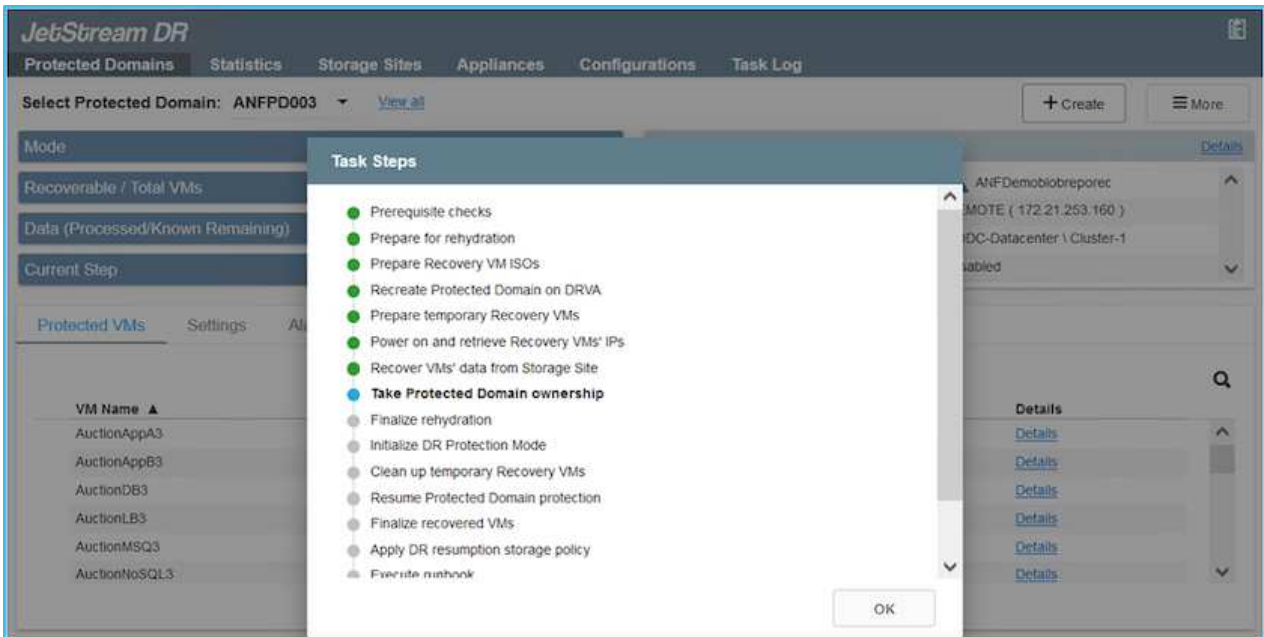
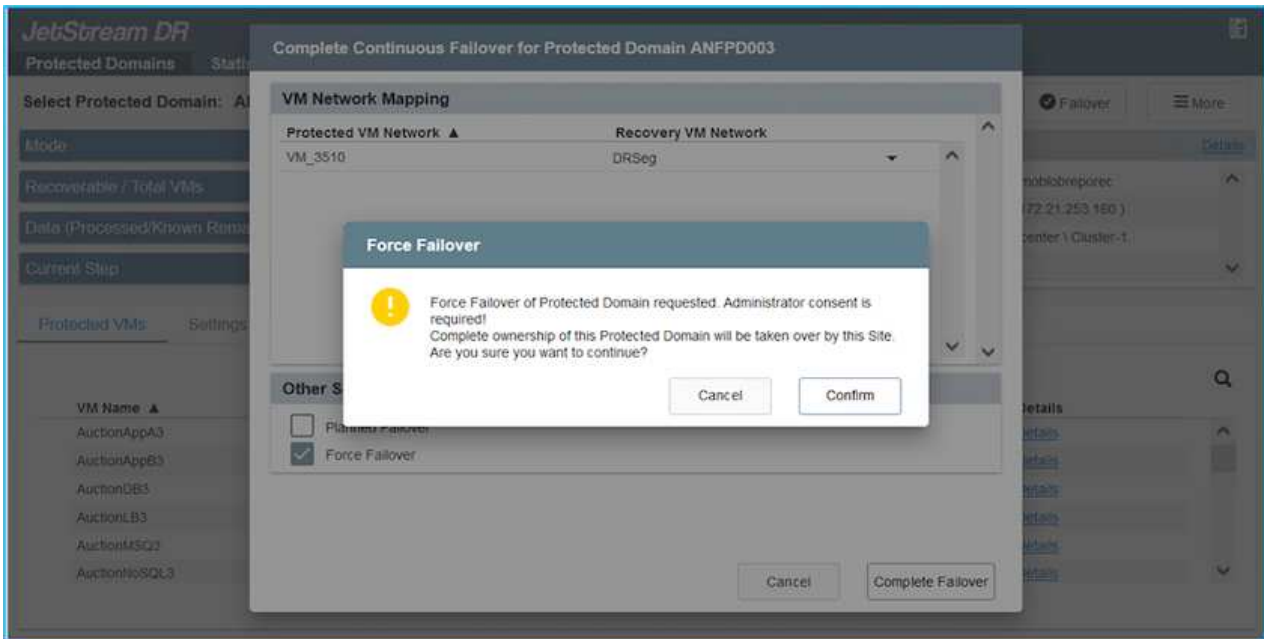
1. In caso di disastro nel cluster protetto dell'ambiente on-premise (errore parziale o completo), attivare il failover.



CPT può essere utilizzato per eseguire il piano di failover per ripristinare le macchine virtuali da Azure Blob Storage nel sito di ripristino del cluster AVS.

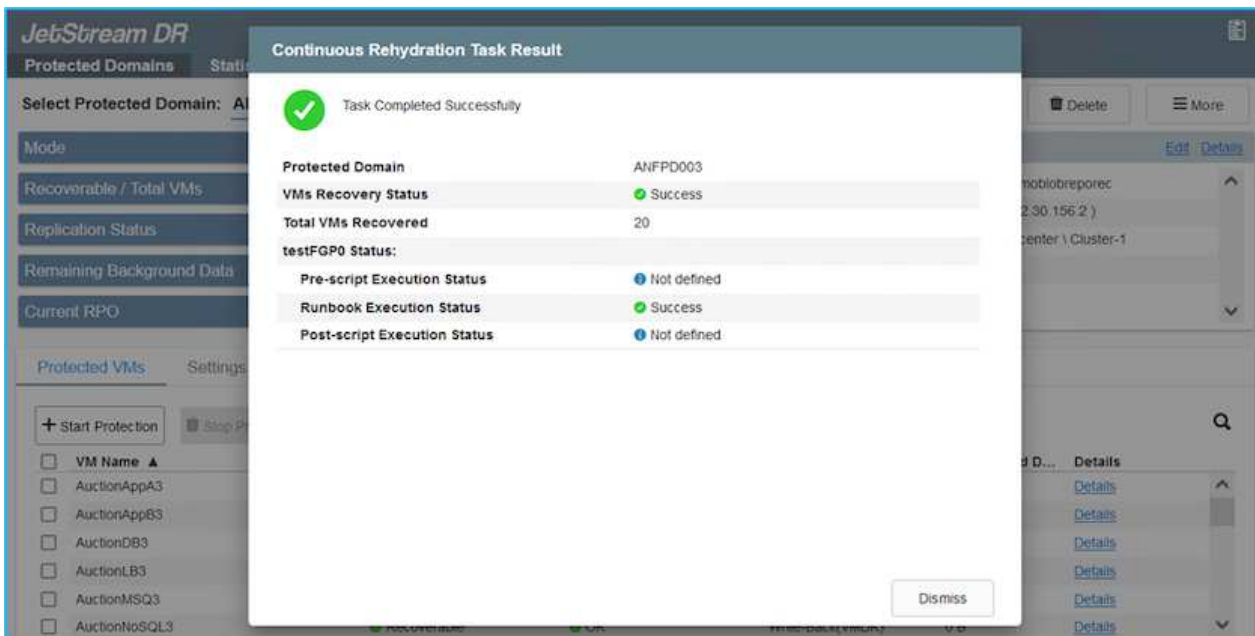


Dopo il failover (per la reidratazione continua o standard) quando le macchine virtuali protette sono state avviate in AVS, la protezione viene automaticamente ripristinata e JetStream DR continua a replicare i propri dati nei container appropriati/originali in Azure Blob Storage.



La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

2. Una volta completata l'attività, accedere alle macchine virtuali ripristinate e il business continua normalmente.



Una volta che il sito primario è stato nuovamente operativo, è possibile eseguire il failback. La protezione delle macchine virtuali viene ripristinata e la coerenza dei dati deve essere verificata.

3. Ripristinare l'ambiente on-premise. A seconda del tipo di incidente, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software DR JetStream.



Nota: Il `recovery_utility_prepare_failback` Lo script fornito nel toolkit di automazione può essere utilizzato per pulire il sito protetto originale di tutte le macchine virtuali obsolete, le informazioni di dominio e così via.

4. Accedere all'ambiente on-premise ripristinato, accedere all'interfaccia utente DR Jetstream e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione failover nell'interfaccia utente.

**JetStream DR**

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: ANFPD003 [View all](#)

Mode: Running in Failover

Active Site: 172.30.156.2

Recoverable / Total VMs: 20 / 20

Configurations

Storage Site: ANFPD003

Owner Site: REMOTE

+ Create | Delete | More

Restore | Resume Continuous Rehydration | Failback

Protected VMs | Settings | Alarms

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
AuctionAppA3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionAppB3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionDB3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionLB3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionMSQ3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
AuctionNoSQL3	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>



Il piano di failback generato da CPT può anche essere utilizzato per avviare il ritorno delle macchine virtuali e dei relativi dati dall'archivio di oggetti all'ambiente VMware originale.



Specificare il ritardo massimo dopo la pausa delle macchine virtuali nel sito di ripristino e il riavvio nel sito protetto. Questo tempo include il completamento della replica dopo l'arresto delle macchine virtuali di failover, il tempo necessario per pulire il sito di recovery e il tempo necessario per ricreare le macchine virtuali in un sito protetto. Il valore consigliato da NetApp è di 10 minuti.

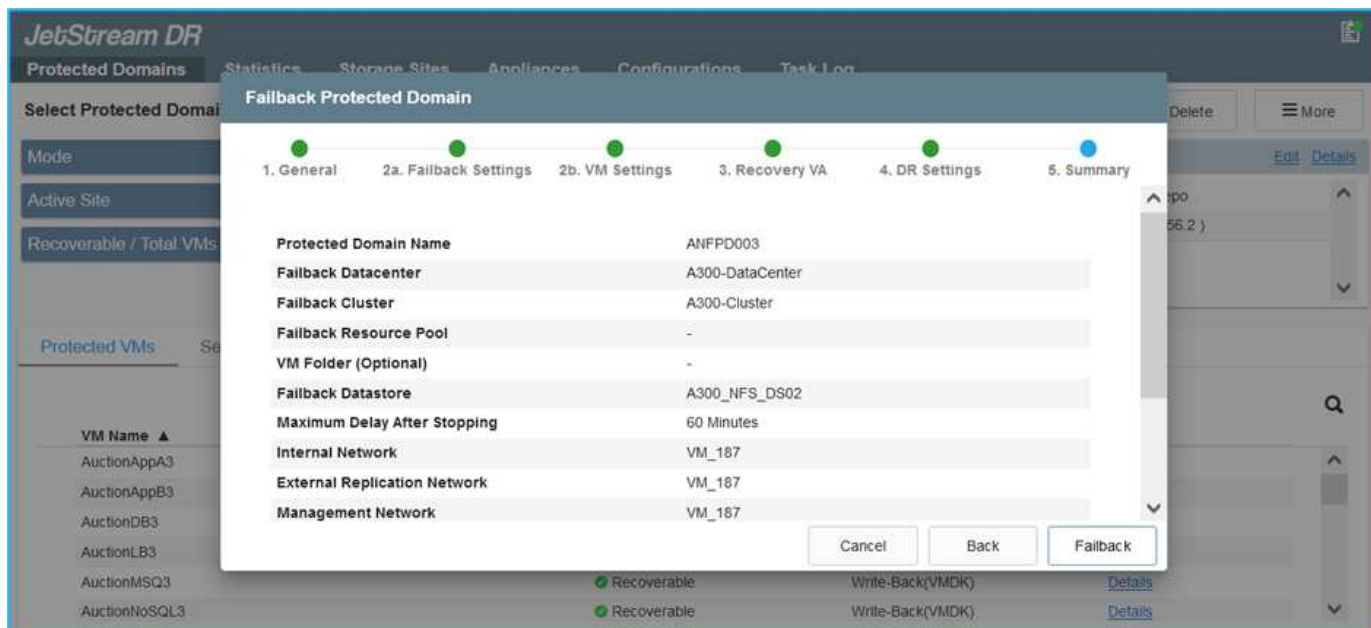
Completare il processo di failback, quindi confermare la ripresa della protezione delle macchine virtuali e la coerenza dei dati.

## Recovery di Ransomware

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, può essere difficile per le organizzazioni IT determinare il punto di ritorno sicuro e, una volta determinato, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi che si verificano nuovamente (dal malware in sospensione o attraverso applicazioni vulnerabili).

Jetstream DR per AVS e gli archivi dati Azure NetApp Files possono risolvere questi problemi consentendo alle organizzazioni di eseguire il ripristino dai punti disponibili nel tempo, in modo che i carichi di lavoro vengano ripristinati in una rete funzionale e isolata, se necessario. Il ripristino consente alle applicazioni di funzionare e comunicare tra loro senza esporre le applicazioni al traffico nord-sud, offrendo così ai team di sicurezza un luogo sicuro per eseguire analisi forensi e altre azioni correttive necessarie.





## Disaster Recovery con CVO e AVS (storage connesso agli ospiti)

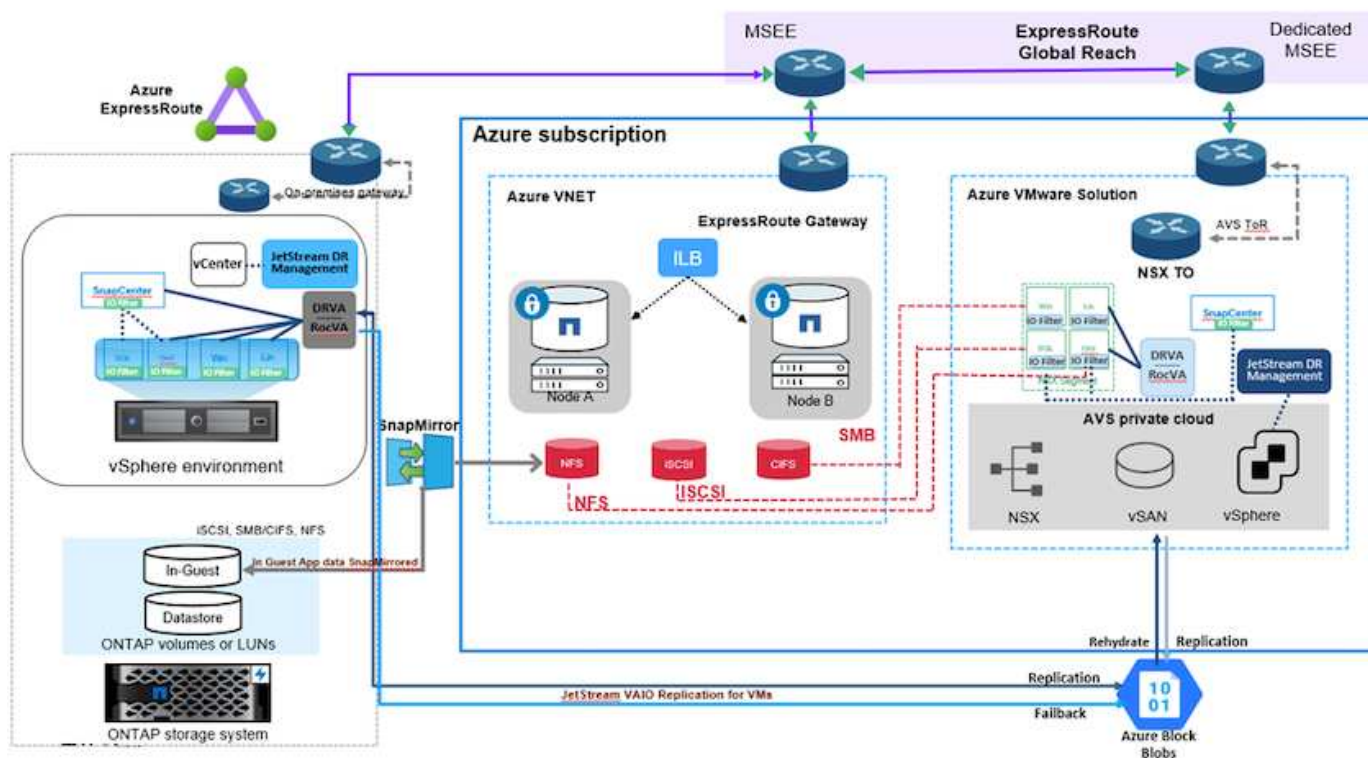
### Panoramica

Autori: Ravi BCB e Niyaz Mohamed, NetApp

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i workload da interruzioni del sito e eventi di corruzione dei dati come ransomware. Con NetApp SnapMirror, è possibile replicare i workload VMware on-premise che utilizzano lo storage connesso con gli ospiti su NetApp Cloud Volumes ONTAP in esecuzione in Azure. Ciò riguarda i dati delle applicazioni, ma le macchine virtuali effettive. Il disaster recovery dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. A tale scopo, SnapMirror e Jetstream possono essere utilizzati per ripristinare perfettamente i carichi di lavoro replicati da on-premise a Cloud Volumes ONTAP utilizzando lo storage vSAN per VM VMDK.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, JetStream e Azure VMware Solution (AVS).





## Presupposti

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



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

Per la connettività tra l'ambiente on-premise e la rete virtuale Azure, utilizzare la portata globale di instradamento espresso o una WAN virtuale con un gateway VPN. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.



Esistono diverse opzioni per connettere i data center on-premise ad Azure, che ci impediscono di delineare un workflow specifico in questo documento. Consultare la documentazione di Azure per il metodo di connettività on-premise-to-Azure appropriato.

## Implementazione della soluzione DR

### Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
  - a. Configurare SnapMirror per i volumi applicativi rilevanti.

- b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
3. Installare il software DR JetStream nel data center on-premise e iniziare la protezione per le macchine virtuali.
4. Installare il software DR JetStream nel cloud privato Azure VMware Solution.
5. Durante un evento di emergenza, interrompere la relazione di SnapMirror utilizzando Cloud Manager e attivare il failover delle macchine virtuali su Azure NetApp Files o su datastore vSAN nel sito di DR AVS designato.
  - a. Ricollegare I LUN ISCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
6. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

## Dettagli sull'implementazione

### Configurare CVO su Azure e replicare i volumi su CVO

Il primo passaggio consiste nella configurazione di Cloud Volumes ONTAP su Azure ("[Collegamento](#)") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritenzioni di snapshot.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	...
	gcsdrsqhld_sc46_copy ANFCVODRDemo	gcsdrsqhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB	...
	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB	...

## Configurare gli host AVS e l'accesso ai dati CVO

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

La decisione di implementare un cluster AVS si basa principalmente sui requisiti RPO/RTO. Con la soluzione VMware Azure, il provisioning SDDC può essere eseguito in tempo, in preparazione di test o di un evento di disastro effettivo. Un SDDC implementato Just in Time consente di risparmiare sui costi degli host ESXi quando non si affronta un disastro. Tuttavia, questa forma di implementazione influisce sull'RTO di alcune ore durante il provisioning di SDDC.

L'opzione implementata più comunemente è l'esecuzione di SDDC in una modalità di funzionamento always-on, con illuminazione pilota. Questa opzione offre un ingombro ridotto di tre host sempre disponibili e accelera le operazioni di recovery fornendo una base di riferimento per le attività di simulazione e i controlli di conformità, evitando così il rischio di deriva operativa tra i siti di produzione e DR. Il cluster pilota-light può essere scalato rapidamente fino al livello desiderato quando necessario per gestire un evento DR effettivo.

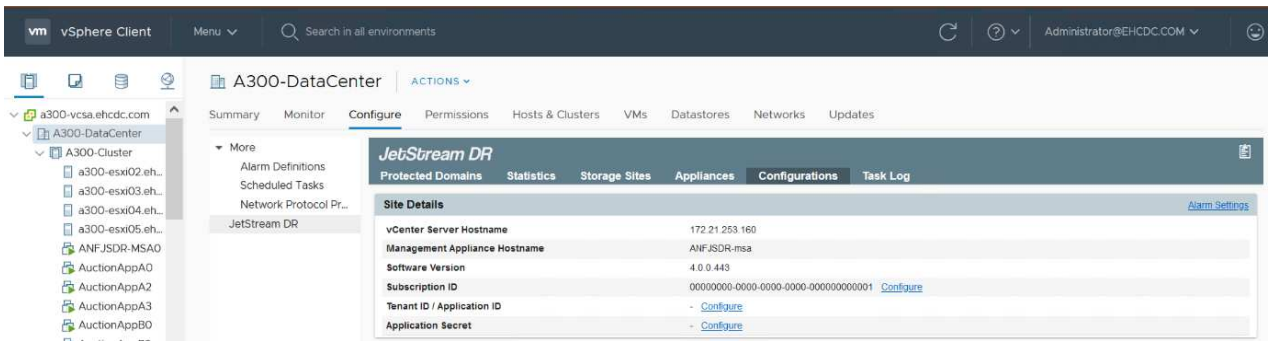
Per configurare AVS SDDC (sia esso on-demand o in modalità pilota-light), vedere ["Implementare e configurare l'ambiente di virtualizzazione su Azure"](#). Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host AVS siano in grado di utilizzare i dati provenienti da Cloud Volumes ONTAP dopo aver stabilito la connettività.

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

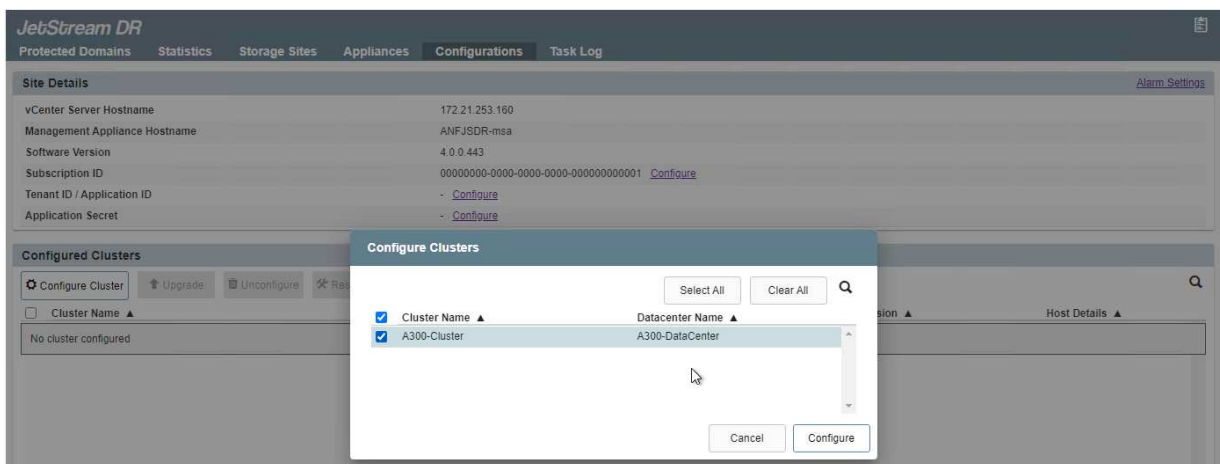
## Installare JetStream DR nel data center on-premise

Il software Jetstream DR è costituito da tre componenti principali: L'appliance virtuale JetStream DR Management Server (MSA), l'appliance virtuale DR (DRVA) e i componenti host (pacchetti di filtri i/o). MSA viene utilizzato per installare e configurare i componenti host sul cluster di calcolo e quindi per amministrare il software DR JetStream. La procedura di installazione è la seguente:

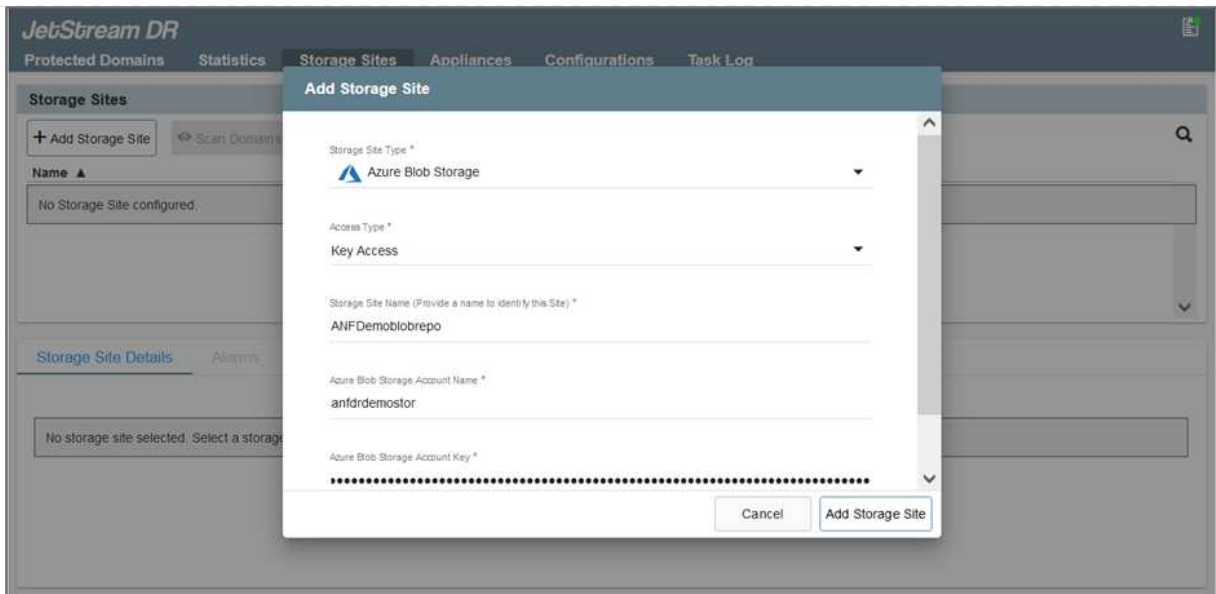
1. Verificare i prerequisiti.
2. Eseguire Capacity Planning Tool per consigli su risorse e configurazione.
3. Distribuire l'MSA DR JetStream su ciascun host vSphere nel cluster designato.
4. Avviare MSA utilizzando il nome DNS in un browser.
5. Registrare il server vCenter con MSA.
6. Una volta implementato JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR con vSphere Web Client. Per eseguire questa operazione, accedere a Datacenter > Configure > JetStream DR.



7. Dall'interfaccia DR JetStream, completare le seguenti attività:
  - a. Configurare il cluster con il pacchetto di filtri i/O.



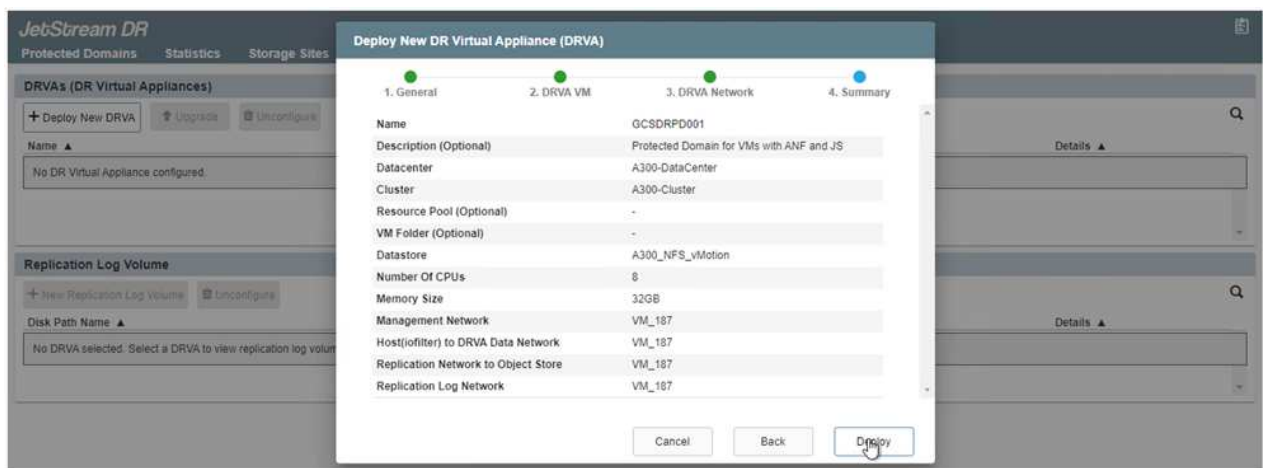
- b. Aggiungere lo storage Azure Blob situato nel sito di ripristino.



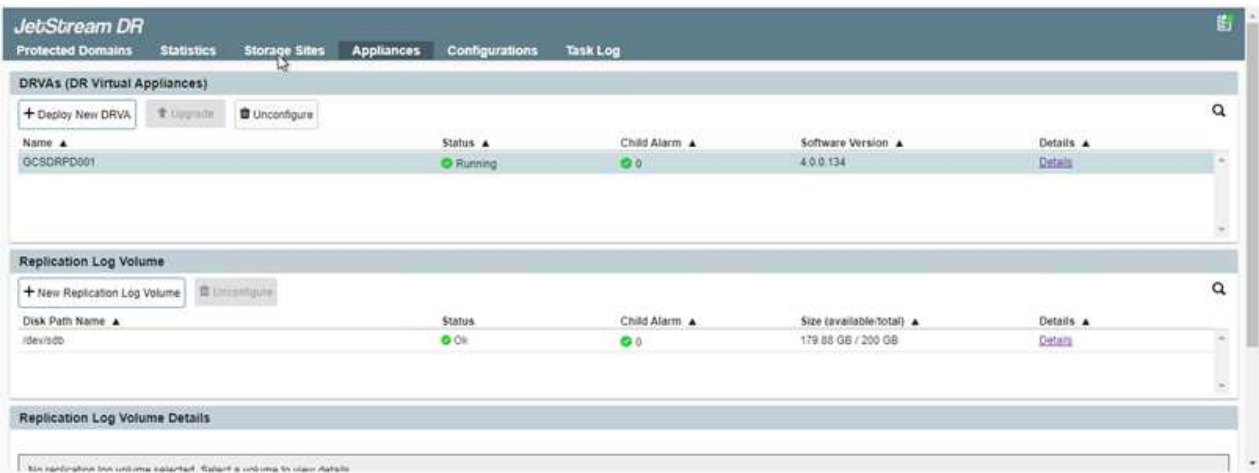
8. Implementare il numero richiesto di DRVA (DR Virtual Appliances) dalla scheda Appliances (appliance).



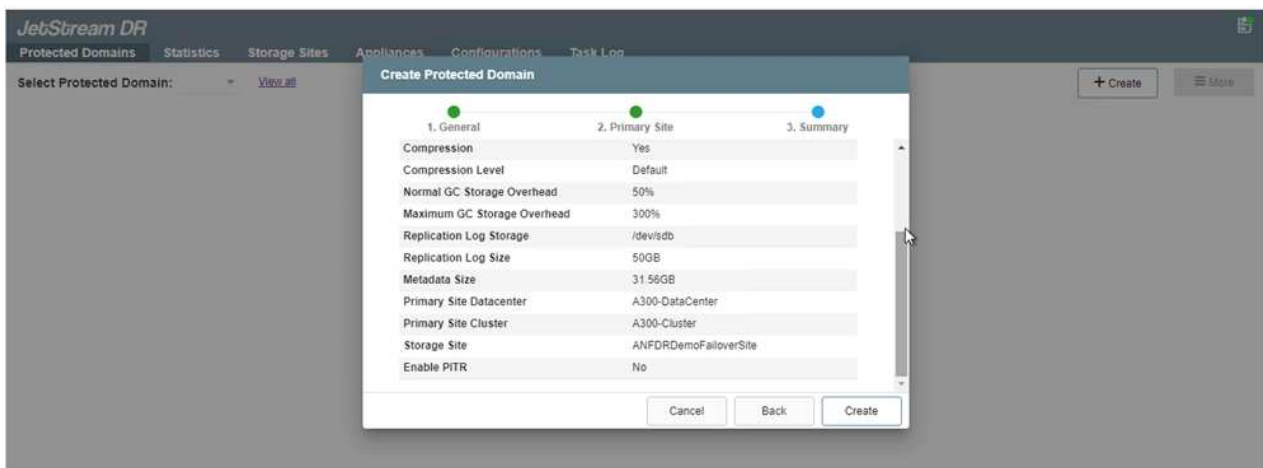
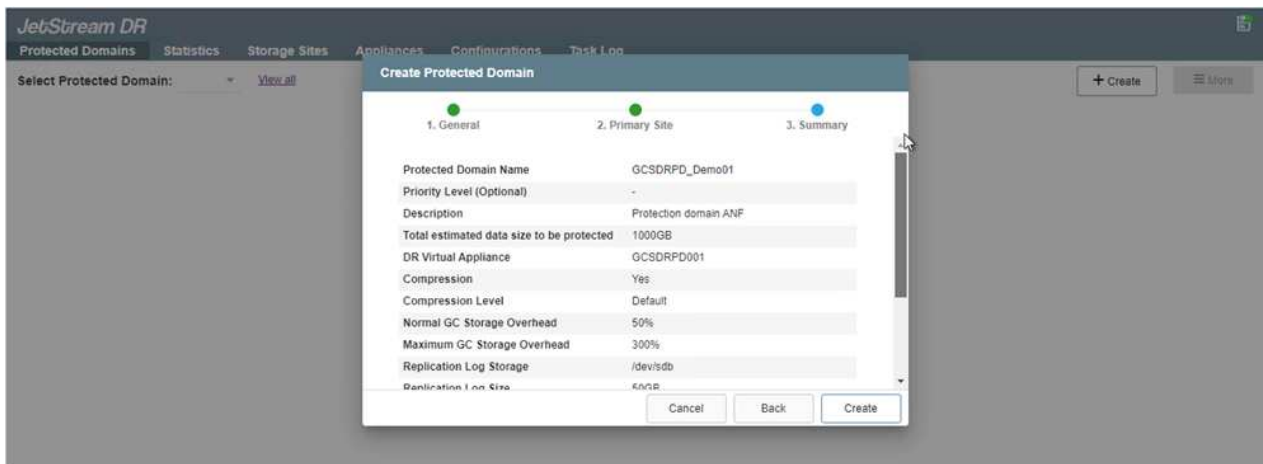
Utilizzare lo strumento di pianificazione della capacità per stimare il numero di DRA richiesti.



9. Creare volumi di log di replica per ogni DRVA utilizzando VMDK dagli archivi dati disponibili o dal pool di storage iSCSI condiviso indipendente.



10. Dalla scheda Protected Domains (domini protetti), creare il numero richiesto di domini protetti utilizzando le informazioni relative al sito Azure Blob Storage, all'istanza DRVA e al registro di replica. Un dominio protetto definisce una macchina virtuale specifica o un insieme di macchine virtuali dell'applicazione all'interno del cluster che sono protetti insieme e assegnati un ordine di priorità per le operazioni di failover/failback.



11. Selezionare le macchine virtuali da proteggere e raggrupparle in gruppi di applicazioni in base alla dipendenza. Le definizioni delle applicazioni consentono di raggruppare set di macchine virtuali 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.

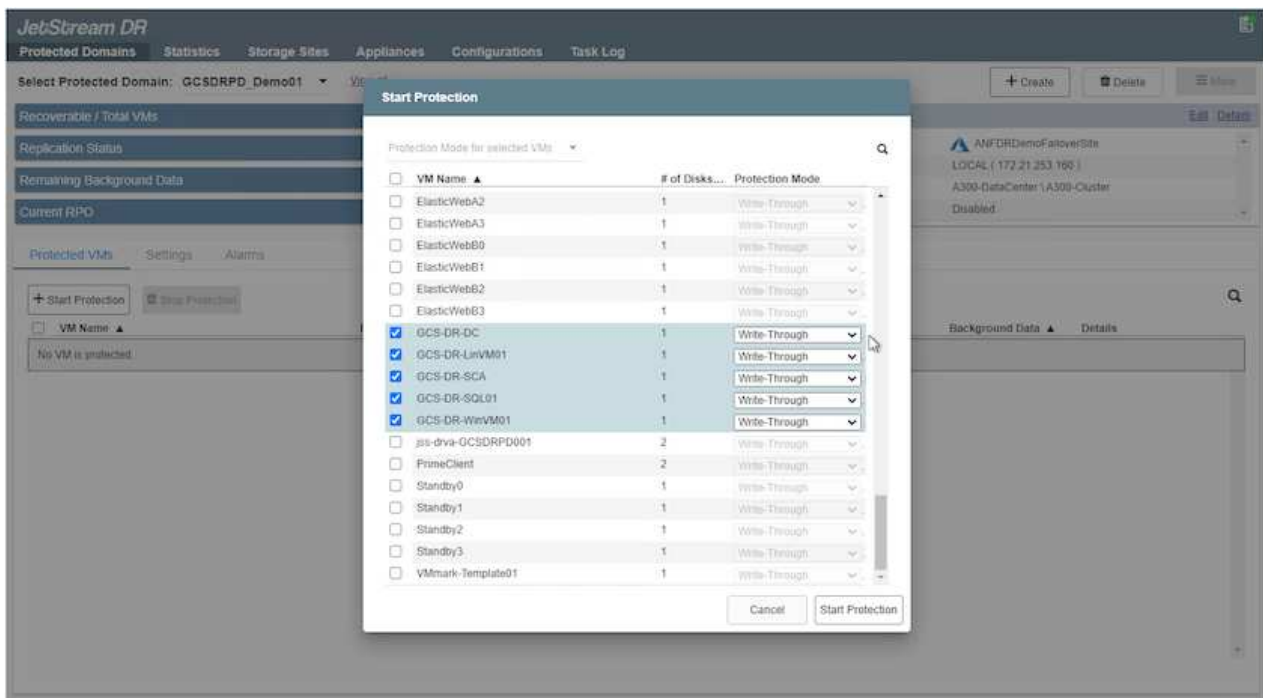




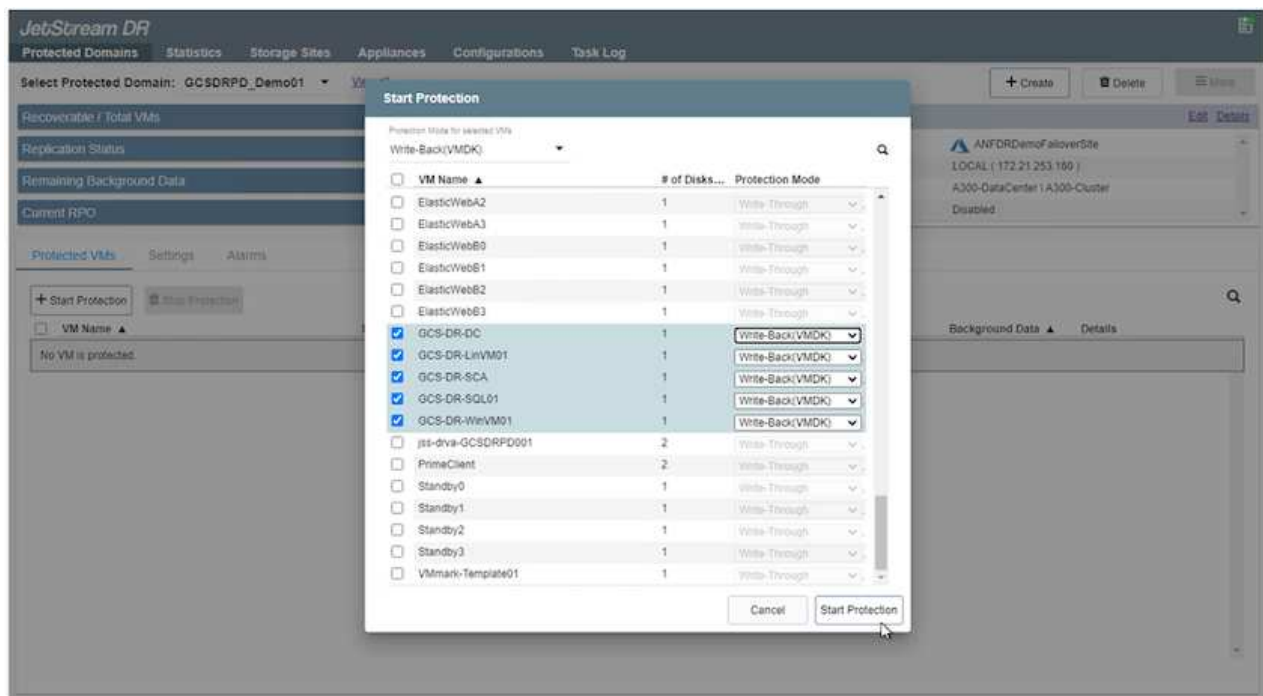
Assicurarsi di utilizzare la stessa modalità di protezione per tutte le macchine virtuali in un dominio protetto.



La modalità Write-Back (VMDK) offre performance superiori.



12. Assicurarsi che i volumi dei log di replica siano posizionati su uno storage dalle performance elevate.



13. Al termine dell'operazione, fare clic su Start Protection (Avvia protezione) per il dominio protetto. In questo modo viene avviata la replica dei dati per le macchine virtuali selezionate nell'archivio Blob designato.

The screenshot shows the JetStream DR interface with the 'Running Tasks' dialog box open. The dialog lists several tasks with their progress percentages: 'Start Protection (GCS-DR-SCA) 50%', 'Start Protection (GCS-DR-Win...) 50%', 'Start Protection (GCS-DR-Lin...) 50%', 'Start Protection (GCS-DR-DC) 50%', 'Start Protection (GCS-DR-SQ...) 50%', and 'Configure VMDK Re... Completed'. A 'Close' button is visible at the bottom of the dialog.

14. Una volta completata la replica, lo stato di protezione della macchina virtuale viene contrassegnato come ripristinabile.

The screenshot shows the JetStream DR interface with the 'Protected VMs' table. The table lists VMs with their protection status, replication status, and protection mode. The status is 'Recoverable' for all listed VMs.

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	<a href="#">Details</a>



Le runbook di failover possono essere configurate per raggruppare le macchine virtuali (denominate gruppo di ripristino), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

15. Fare clic su Impostazioni, quindi sul collegamento Configura runbook per configurare il gruppo runbook.

The screenshot shows the JetStream DR interface with the 'Settings' tab selected. The 'Failover Runbook' is listed as 'Not Configured' with a 'Configure' link. Other settings like 'Test Failover Runbook', 'Fallback Runbook', 'Memory Setting', 'GC Settings', and 'Concurrency Settings' are also listed.

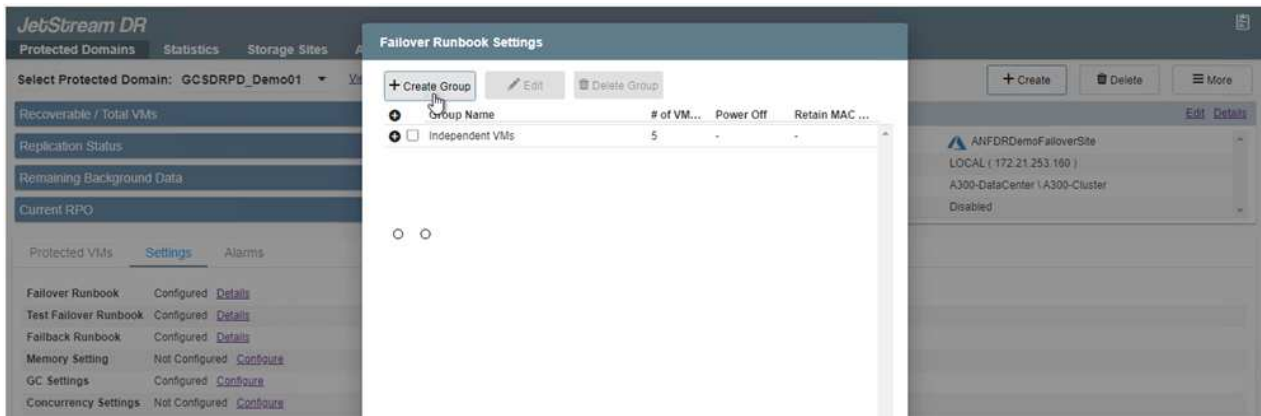
Setting	Status	Action
Failover Runbook	Not Configured	<a href="#">Configure</a>
Test Failover Runbook	Not Configured	<a href="#">Configure</a>
Fallback Runbook	Not Configured	<a href="#">Configure</a>
Memory Setting	Not Configured	<a href="#">Configure</a>
GC Settings	Configured	<a href="#">Configure</a>
Concurrency Settings	Not Configured	<a href="#">Configure</a>

16. Fare clic sul pulsante Create Group (Crea gruppo) per iniziare a creare un nuovo gruppo di runbook.

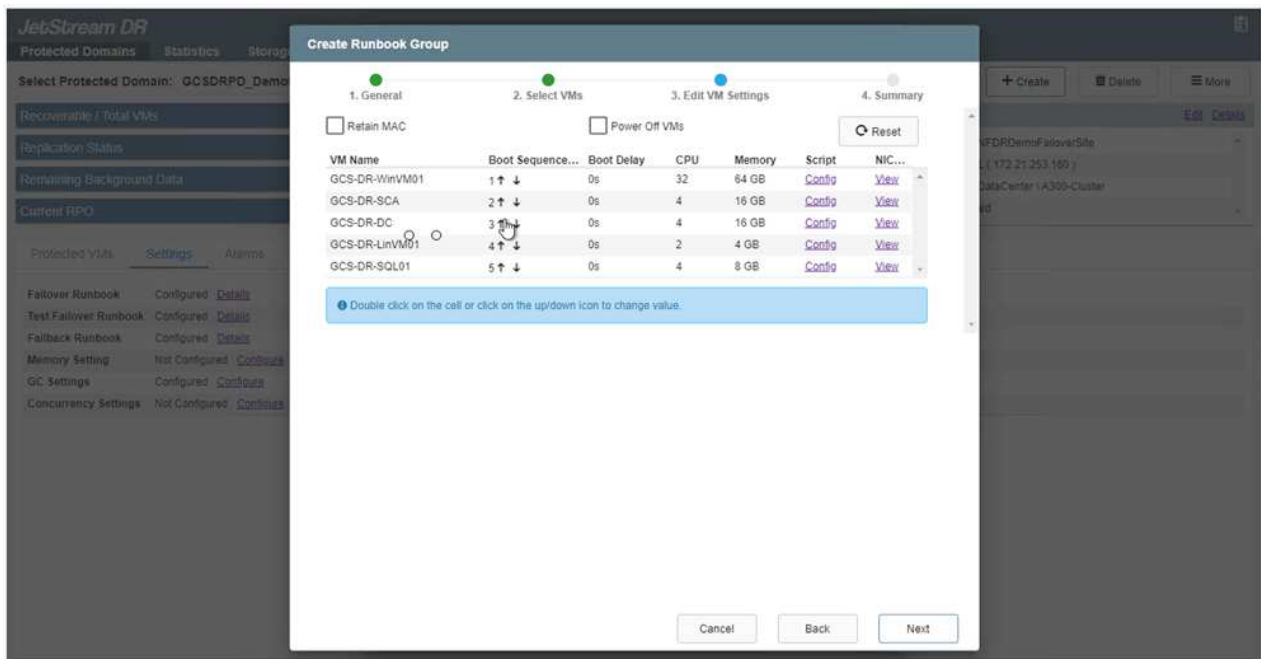




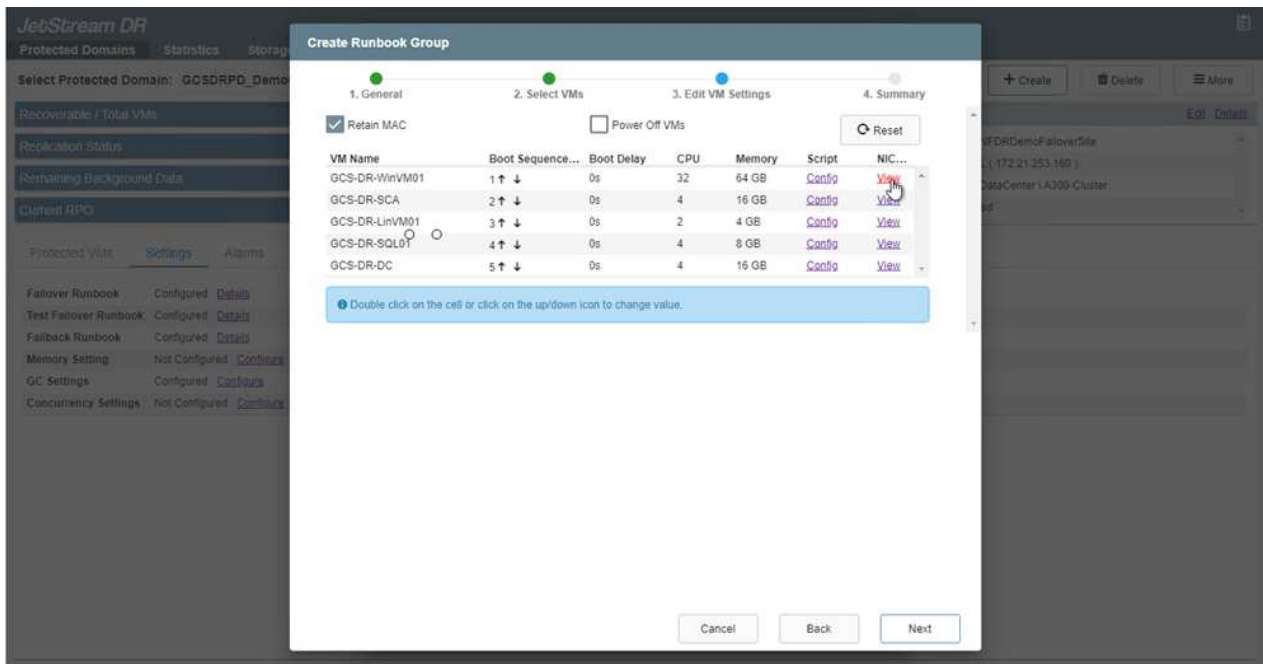
Se necessario, nella parte inferiore della schermata, applicare pre-script e post-script personalizzati da eseguire automaticamente prima e dopo l'operazione del gruppo di runbook. Assicurarsi che gli script Runbook risiedano sul server di gestione.



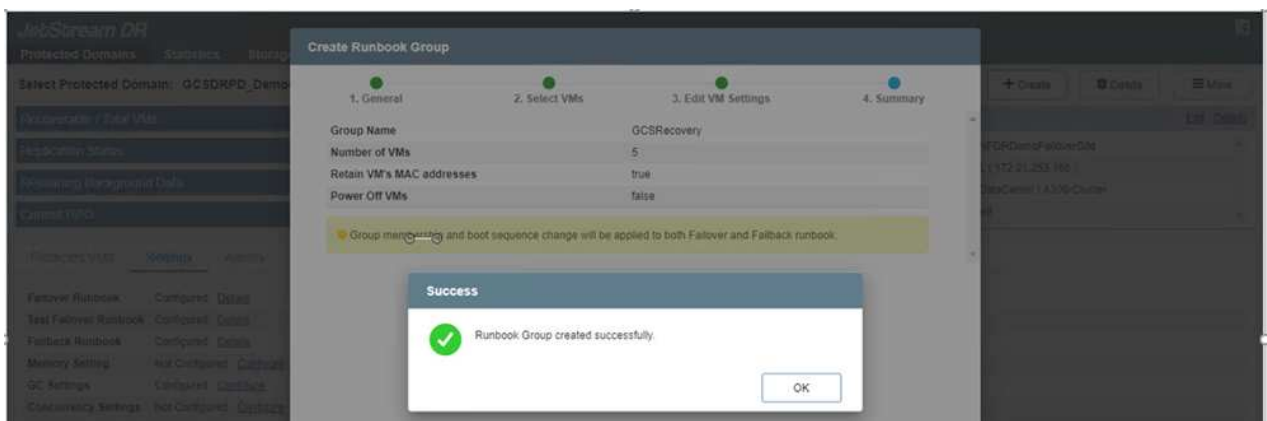
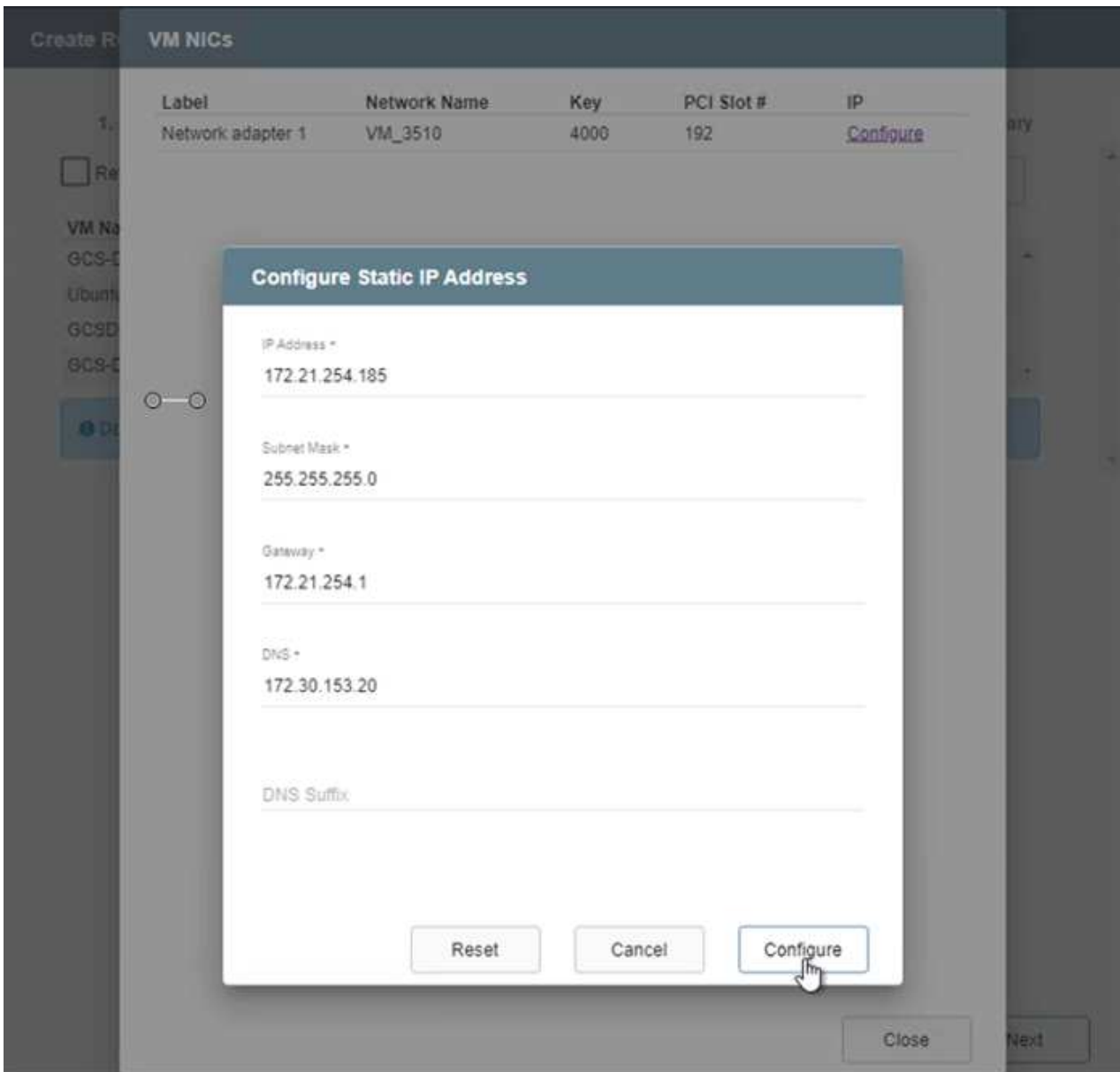
17. Modificare le impostazioni della macchina virtuale secondo necessità. Specificare i parametri per il ripristino delle macchine virtuali, tra cui la sequenza di avvio, il ritardo di avvio (specificato in secondi), il numero di CPU e la quantità di memoria da allocare. Modificare la sequenza di avvio delle macchine virtuali facendo clic sulle frecce verso l'alto o verso il basso. Sono inoltre disponibili opzioni per conservare MAC.



18. Gli indirizzi IP statici possono essere configurati manualmente per le singole macchine virtuali del gruppo. Fare clic sul collegamento NIC View (visualizzazione NIC) di una macchina virtuale per configurare manualmente le impostazioni dell'indirizzo IP.



19. Fare clic sul pulsante Configure (Configura) per salvare le impostazioni NIC per le rispettive macchine virtuali.



Lo stato dei runbook di failover e failback è ora elencato come configurato. I gruppi runbook di failover e failback vengono creati in coppie utilizzando lo stesso gruppo iniziale di macchine virtuali e impostazioni. Se necessario, le impostazioni di qualsiasi gruppo di runbook possono essere personalizzate singolarmente facendo clic sul relativo link Details (Dettagli) e apportando modifiche.

## Installare JetStream DR per AVS nel cloud privato

Una Best practice per un sito di recovery (AVS) consiste nella creazione anticipata di un cluster pilota a tre nodi. Ciò consente di preconfigurare l'infrastruttura del sito di ripristino, tra cui:

- Segmenti di rete di destinazione, firewall, servizi come DHCP e DNS e così via
- Installazione di JetStream DR per AVS
- Configurazione dei volumi ANF come datastore e altro ancora

Jetstream DR supporta una modalità RTO quasi zero per i domini mission-critical. Per questi domini, lo storage di destinazione deve essere preinstallato. ANF è un tipo di storage consigliato in questo caso.



La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS per soddisfare i requisiti on-premise.



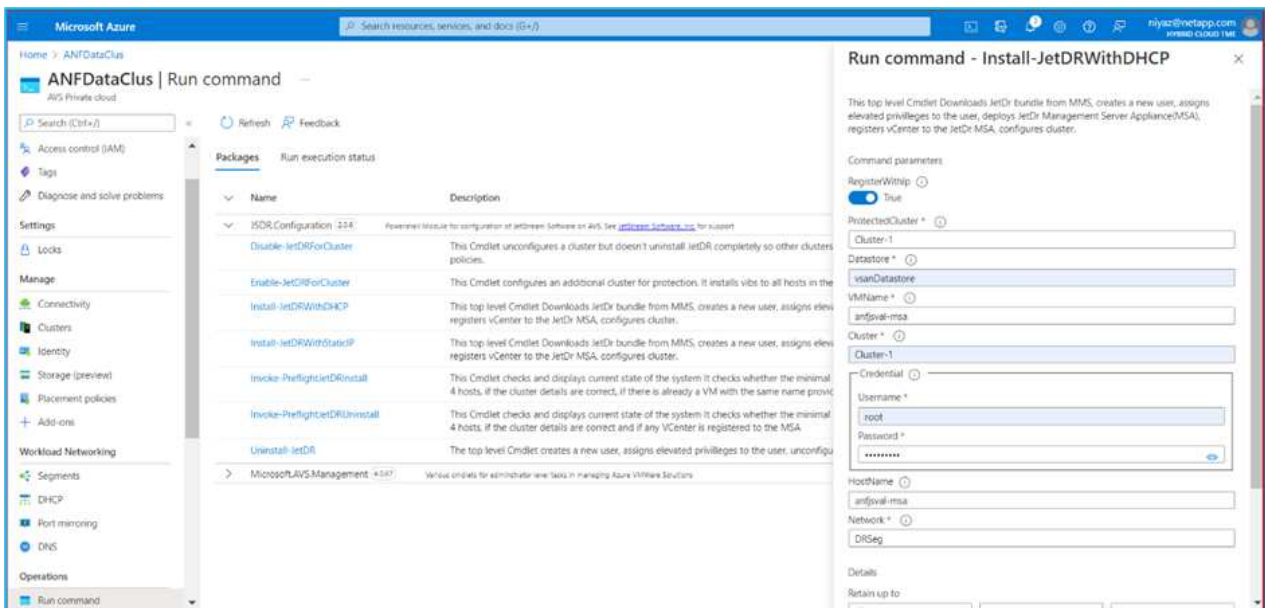
A seconda dei requisiti SLA e RTO, è possibile utilizzare il failover continuo o la normale modalità di failover (standard). Per un RTO vicino allo zero, è necessario avviare una reidratazione continua nel sito di ripristino.

1. Per installare JetStream DR per AVS su un cloud privato Azure VMware Solution, utilizzare il comando Esegui. Dal portale Azure, accedere alla soluzione Azure VMware, selezionare il cloud privato e selezionare Esegui comando > pacchetti > Configurazione JS DR.

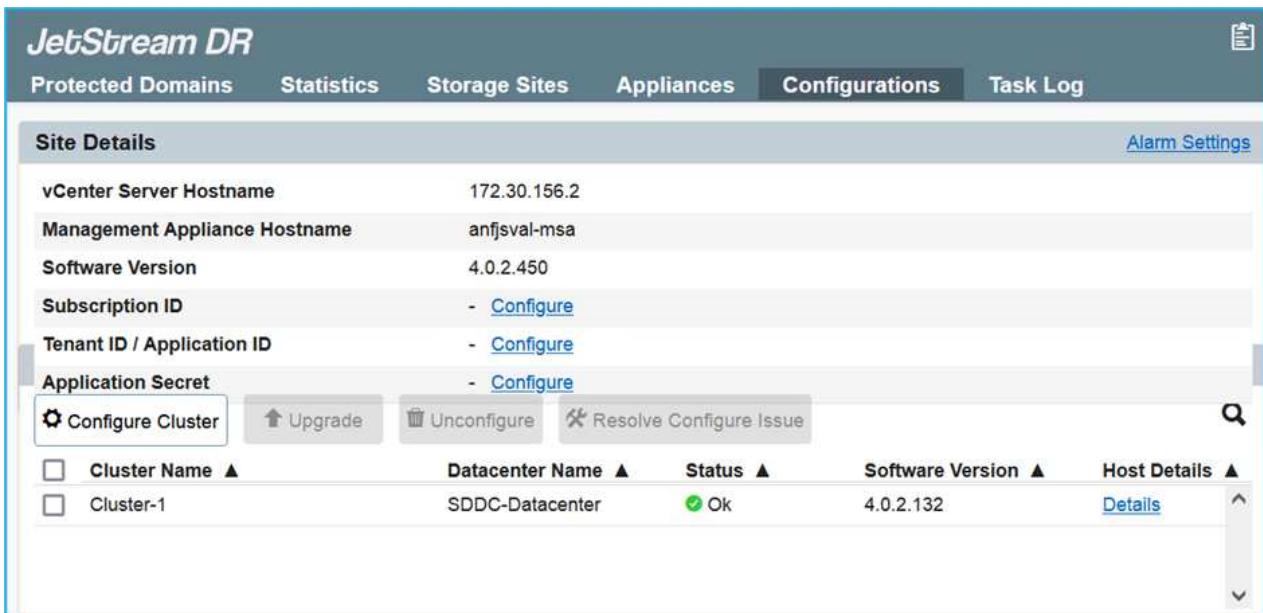


L'utente CloudAdmin predefinito di Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente un'installazione semplificata e automatica del DR JetStream invocando il comando Azure VMware Solution Run per il DR JetStream.

La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente DR JetStream, accedere a SDDC Datacenter > Configure > JetStream DR.



3. Dall'interfaccia DR JetStream, completare le seguenti attività:

- Aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster on-premise come sito di storage, quindi eseguire l'opzione Scan Domains.
- Nella finestra di dialogo a comparsa visualizzata, selezionare il dominio protetto da importare, quindi fare clic sul relativo collegamento Importa.



4. Il dominio viene importato per il ripristino. Accedere alla scheda Protected Domains (domini protetti) e verificare che sia stato selezionato il dominio desiderato oppure scegliere quello desiderato dal menu Select Protected Domain (Seleziona dominio protetto). Viene visualizzato un elenco delle macchine virtuali ripristinabili nel dominio protetto.

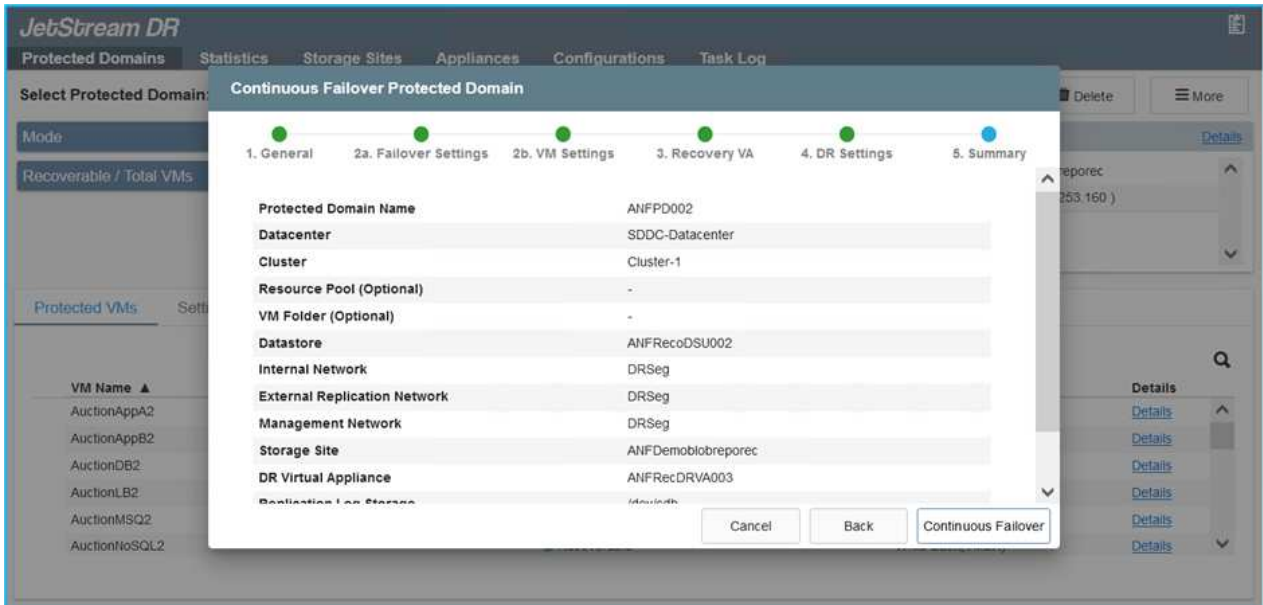


5. Una volta importati i domini protetti, implementare le appliance DRVA.



Questi passaggi possono anche essere automatizzati utilizzando piani creati da CPT.

6. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
7. Importare i domini protetti e configurare il VA di ripristino in modo che utilizzi un datastore ANF per il posizionamento delle macchine virtuali.



Assicurarsi che DHCP sia attivato sul segmento selezionato e che sia disponibile un numero sufficiente di IP. Gli IP dinamici vengono temporaneamente utilizzati durante il ripristino dei domini. Ogni macchina virtuale di ripristino (inclusa la reidratazione continua) richiede un IP dinamico individuale. Una volta completato il ripristino, l'IP viene rilasciato e può essere riutilizzato.

8. Selezionare l'opzione di failover appropriata (failover o failover continuo). In questo esempio, viene selezionata la reidratazione continua (failover continuo).



Anche se le modalità di failover continuo e failover differiscono quando viene eseguita la configurazione, entrambe le modalità di failover vengono configurate utilizzando le stesse procedure. I passaggi di failover vengono configurati ed eseguiti insieme in risposta a un evento di emergenza. È possibile configurare il failover continuo in qualsiasi momento e consentire l'esecuzione in background durante il normale funzionamento del sistema. In seguito a un evento di emergenza, il failover continuo viene completato per trasferire immediatamente la proprietà delle macchine virtuali protette al sito di ripristino (RTO quasi nullo).

**JetStream DR**

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCDRDP\_Demo01 [View all](#)

Mode Imported

Recoverable / Total VMs 5 / 5

Configurations

Storage Site ANFDemoblobrepor

Owner Site REMOTE ( 172.21.253.11)

Restore

Failover

Continuous Failover

Test Failover

Protected VMs Settings Alarms

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

Viene avviato il processo di failover continuo, che può essere monitorato dall'interfaccia utente. Facendo clic sull'icona blu nella sezione Current Step (fase corrente) viene visualizzata una finestra a comparsa che mostra i dettagli della fase corrente del processo di failover.



## Failover e failover

1. In caso di disastro nel cluster protetto dell'ambiente on-premise (errore parziale o completo), è possibile attivare il failover per le macchine virtuali utilizzando Jetstream dopo aver interrotto la relazione SnapMirror per i rispettivi volumi applicativi.

The screenshot displays the 'Replication' section of a management console. At the top, a summary bar shows: 3 Volume Relationships, 4.78 GiB Replicated Capacity, 0 Currently Transferring, 3 Healthy, and 0 Failed. Below this, a table lists three volume relationships, all with a 'snapmirrored' mirror state and an 'idle' status. A context menu is open for the first relationship, showing options like 'Break', 'Reverse Resync', 'Edit Schedule', 'Edit Max Transfer Rate', 'Update', and 'Delete'. The 'Break' option is highlighted. Below the table, a 'Break Relationship' dialog box is shown, asking for confirmation to break the relationship between 'gcsdrsqldb\_sc46' and 'gcsdrsqldb\_sc46\_copy'. The 'Break' button in the dialog is highlighted.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	Information
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	snapmirrored	Break

Break Relationship

Are you sure that you want to break the relationship between "gcsdrsqldb\_sc46" and "gcsdrsqldb\_sc46\_copy"?

Break Cancel



Questo passaggio può essere facilmente automatizzato per facilitare il processo di recovery.

2. Accedere all'interfaccia utente Jetstream su AVS SDDC (lato destinazione) e attivare l'opzione di failover per completare il failover. La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

Nella finestra di dialogo visualizzata al completamento del failover, è possibile specificare l'attività di failover come pianificata o presunta come forzata.



**JetStream DR**

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: **GCSDRPD\_Demo01** [View all](#)

**Mode:** Continuous Rehydration in Progress

**Recoverable / Total VMs:** 4 / 4

**Data (Processed/Known Remaining):** 329.01 GB / 6.19 GB

**Current Step:** Recover VMs' data from Storage Site

**Configurations**

Storage Site	ANFDemo01breporec
Owner Site	REMOTE ( 172.21.253.160 )
Datacenter \ Cluster	SDDC-Datacenter \ Cluster-1
Point-in-time Recovery	Disabled

**Protected VMs** | Settings | Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

### Complete Continuous Failover for Protected Domain

#### VM Network Mapping

Protected VM Network	Recovery VM Network
VM_3510	DRStretchSeg

#### Other Settings

☐ Planned Failover  
☒ Force Failover

Some VM's guest credential are required because of network configuration: [Configure](#)

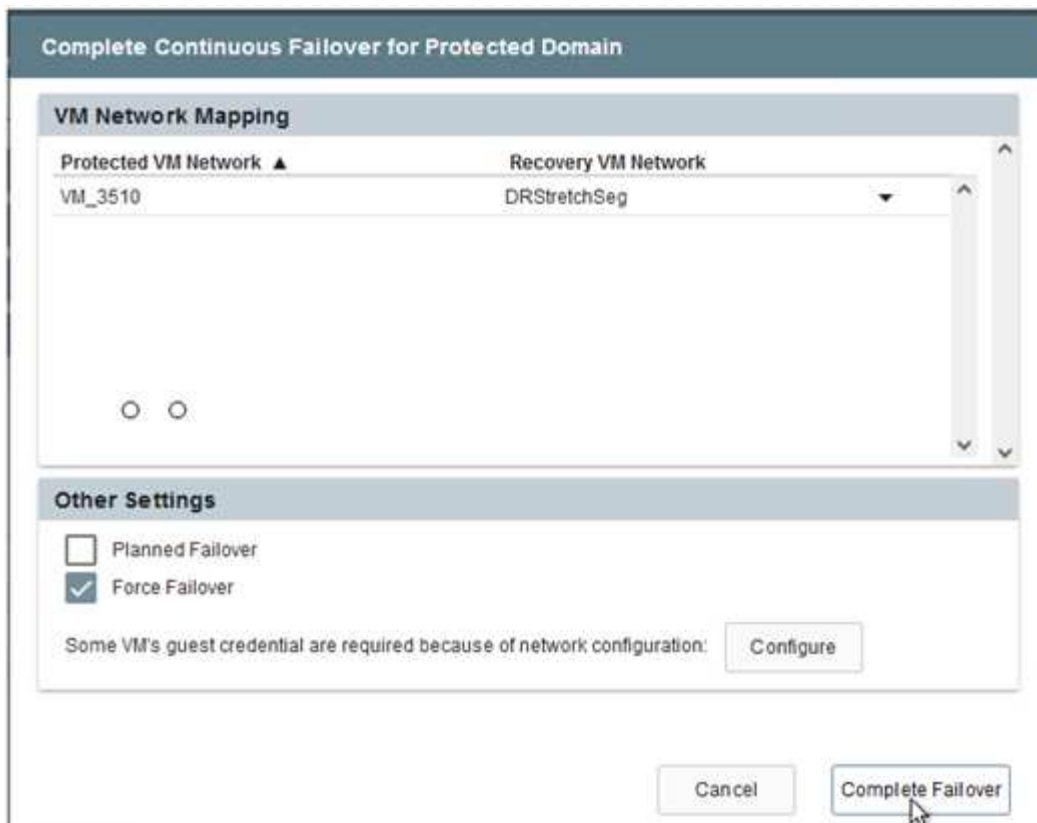
[Cancel](#)
[Complete Failover](#)

Il failover forzato presuppone che il sito primario non sia più accessibile e che la proprietà del dominio protetto debba essere direttamente assunta dal sito di ripristino.

### Force Failover


 Force Failover of Protected Domain requested. Administrator consent is required!  
 Complete ownership of this Protected Domain will be taken over by this Site.  
 Are you sure you want to continue?

[Cancel](#)
[Confirm](#)



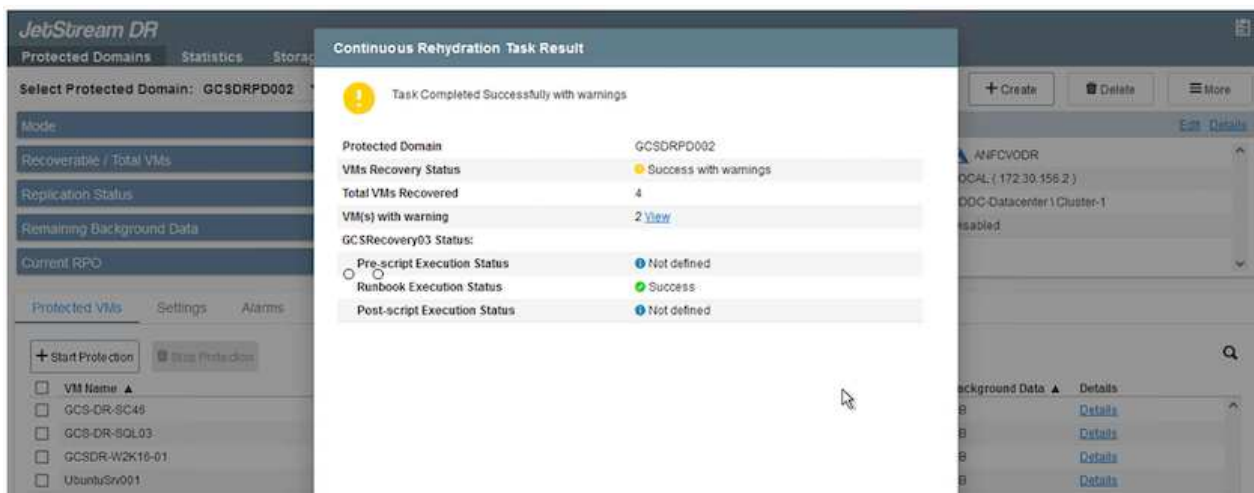
3. Una volta completato il failover continuo, viene visualizzato un messaggio che conferma il completamento dell'attività. Al termine dell'attività, accedere alle macchine virtuali ripristinate per configurare le sessioni iSCSI o NFS.



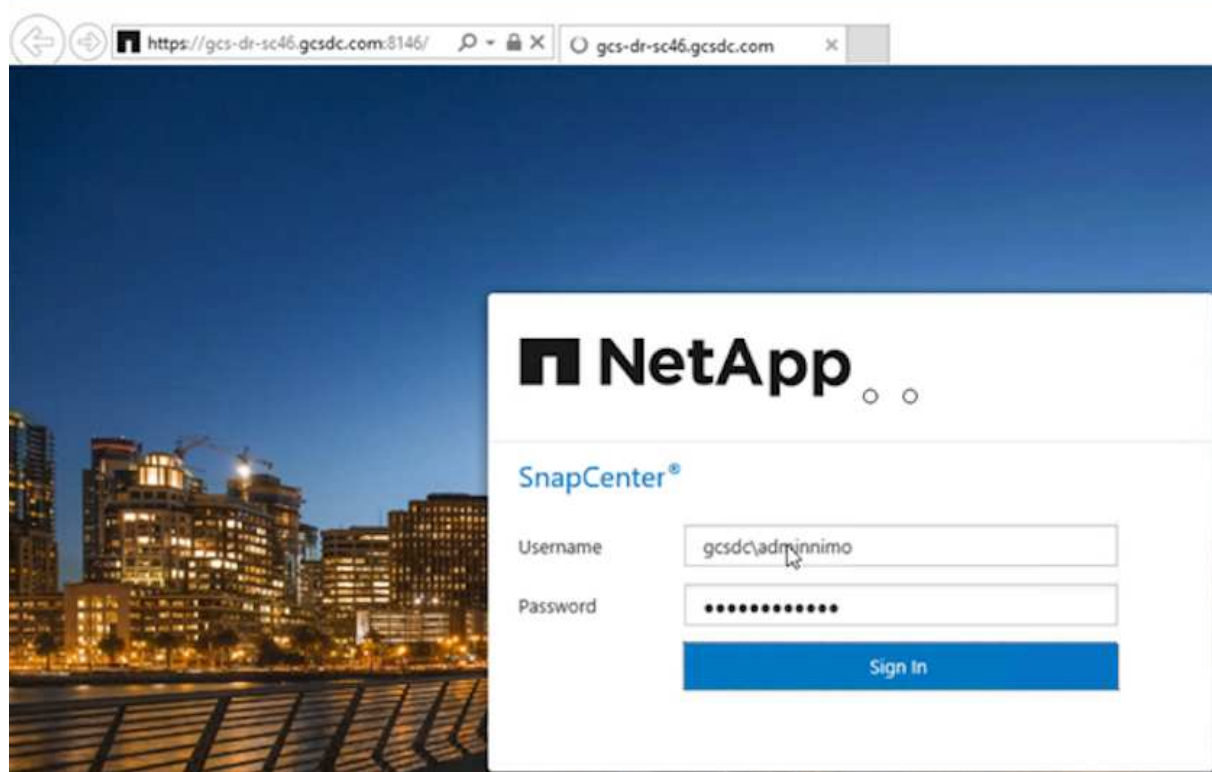
La modalità di failover diventa in esecuzione in failover e lo stato della macchina virtuale è ripristinabile. Tutte le macchine virtuali del dominio protetto sono ora in esecuzione nel sito di ripristino nello stato specificato dalle impostazioni del runbook di failover.



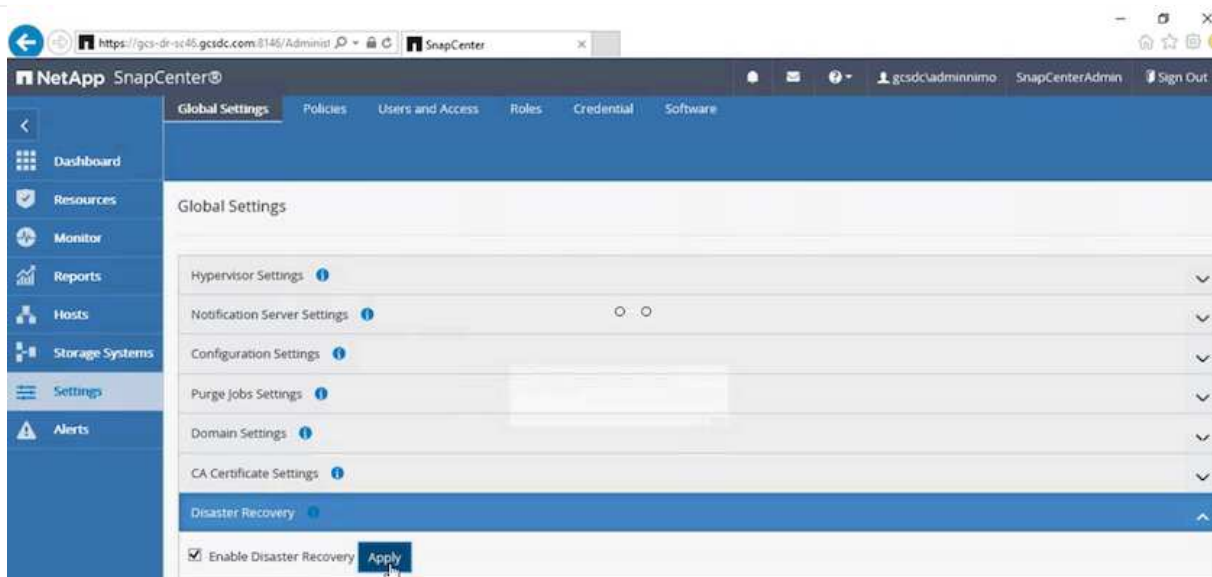
Per verificare la configurazione e l'infrastruttura di failover, è possibile utilizzare JetStream DR in modalità test (opzione Test failover) per osservare il ripristino delle macchine virtuali e dei relativi dati dall'archivio di oggetti in un ambiente di test recovery. Quando una procedura di failover viene eseguita in modalità test, il suo funzionamento assomiglia a un processo di failover effettivo.



4. Una volta ripristinate le macchine virtuali, utilizzare il disaster recovery dello storage per lo storage in-guest. Per dimostrare questo processo, in questo esempio viene utilizzato SQL Server.
5. Accedere alla macchina virtuale SnapCenter recuperata su AVS SDDC e attivare la modalità DR.
  - a. Accedere all'interfaccia utente di SnapCenter utilizzando il browserN.



- b. Nella pagina Settings (Impostazioni), accedere a Settings (Impostazioni) > Global Settings (Impostazioni globali) > Disaster Recovery (Ripristino di emergenza).
- c. Selezionare Enable Disaster Recovery (attiva ripristino di emergenza).
- d. Fare clic su Applica.

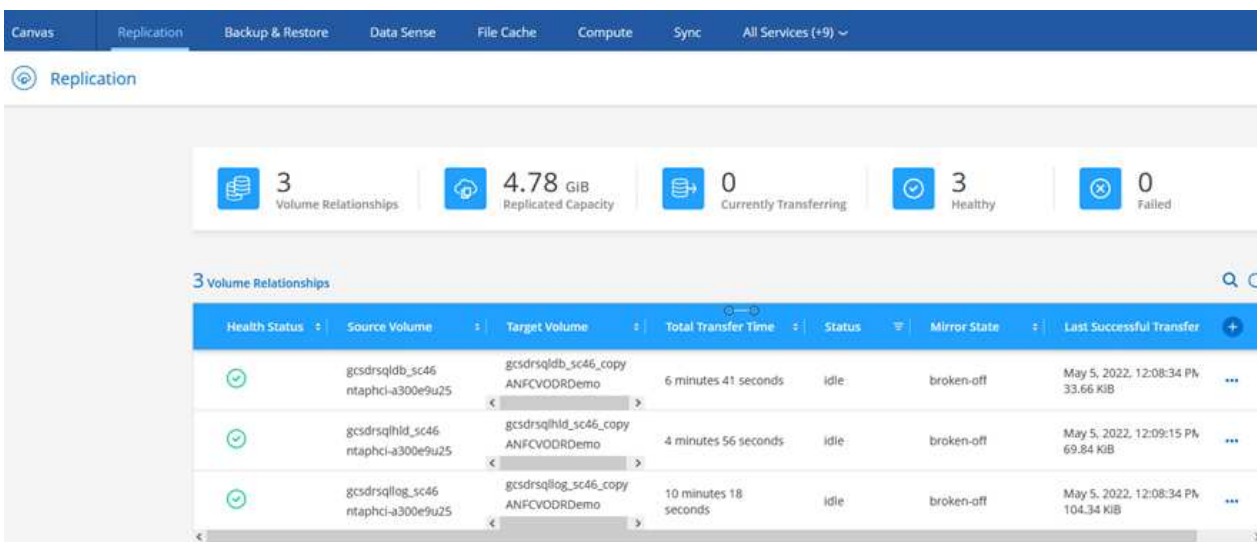


e. Verificare che il processo DR sia attivato facendo clic su Monitor > Jobs (Monitor > processi).

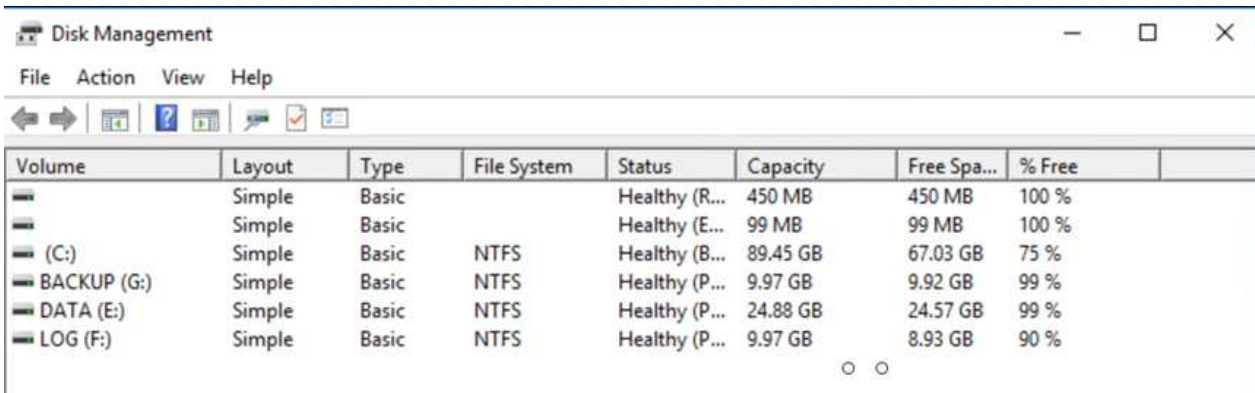


Per il disaster recovery dello storage è necessario utilizzare NetApp SnapCenter 4.6 o versione successiva. Per le versioni precedenti, è necessario utilizzare snapshot coerenti con l'applicazione (replicati utilizzando SnapMirror) e eseguire il ripristino manuale nel caso in cui i backup precedenti debbano essere ripristinati nel sito di disaster recovery.

6. Verificare che la relazione di SnapMirror non sia più stabilita.



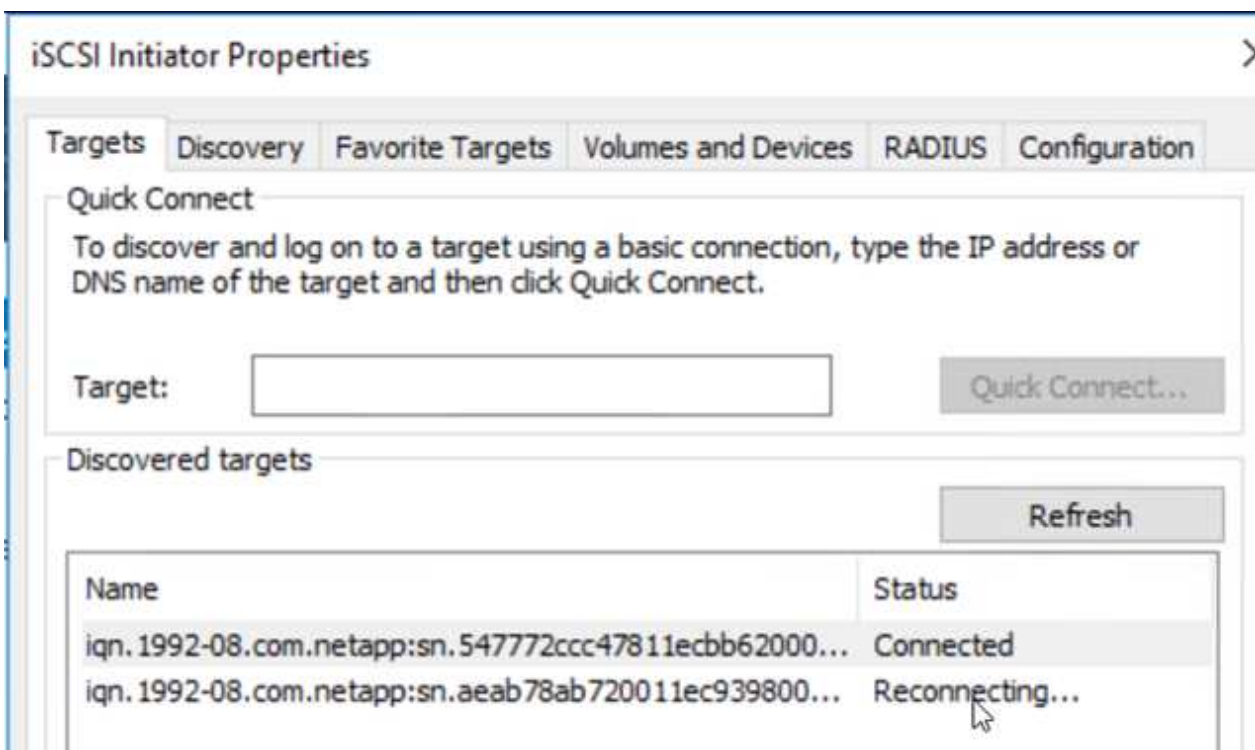
7. Collegare il LUN da Cloud Volumes ONTAP alla macchina virtuale SQL guest recuperata con le stesse lettere di unità.



Disk Management window showing a list of volumes. The table below represents the data shown in the screenshot.

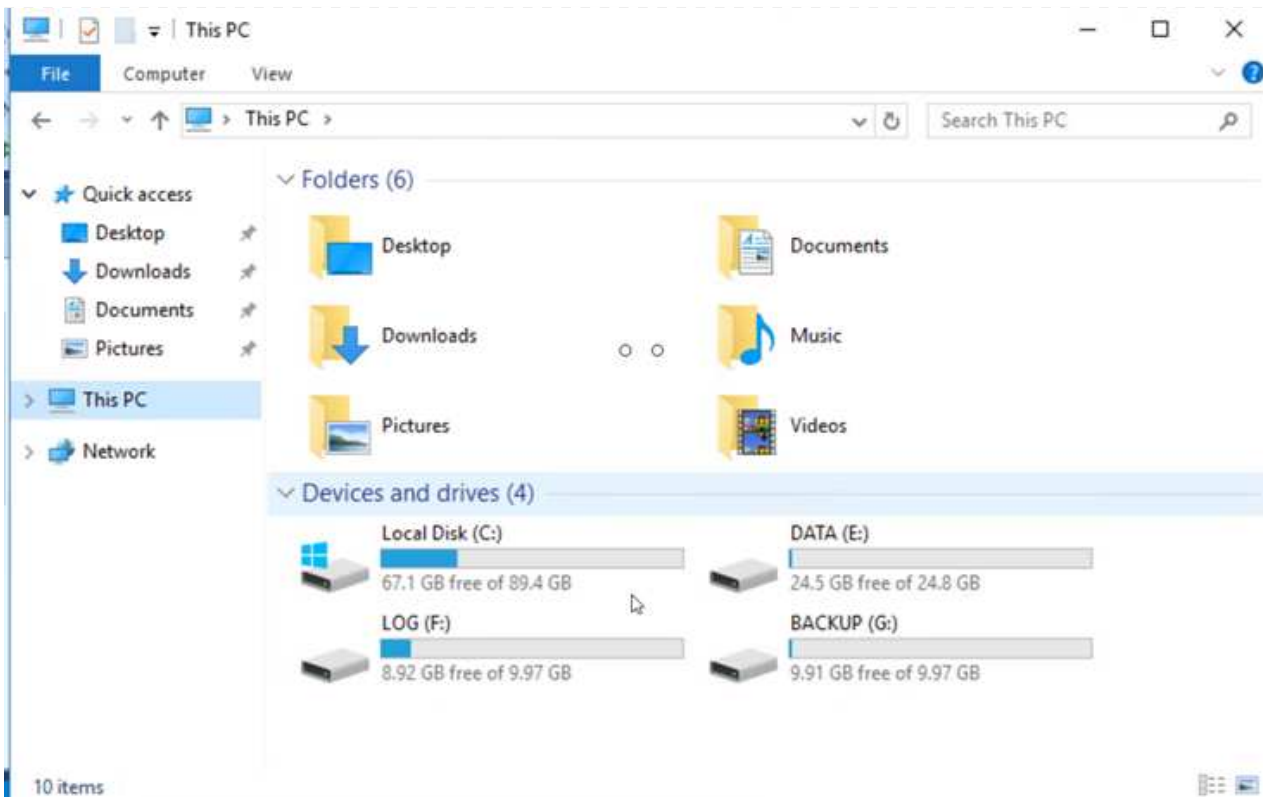
Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
...	Simple	Basic		Healthy (R...	450 MB	450 MB	100 %
...	Simple	Basic		Healthy (E...	99 MB	99 MB	100 %
(C:)	Simple	Basic	NTFS	Healthy (B...	89.45 GB	67.03 GB	75 %
BACKUP (G:)	Simple	Basic	NTFS	Healthy (P...	9.97 GB	9.92 GB	99 %
DATA (E:)	Simple	Basic	NTFS	Healthy (P...	24.88 GB	24.57 GB	99 %
LOG (F:)	Simple	Basic	NTFS	Healthy (P...	9.97 GB	8.93 GB	90 %

8. Aprire iSCSI Initiator, cancellare la sessione disconnessa precedente e aggiungere la nuova destinazione insieme al multipath per i volumi Cloud Volumes ONTAP replicati.

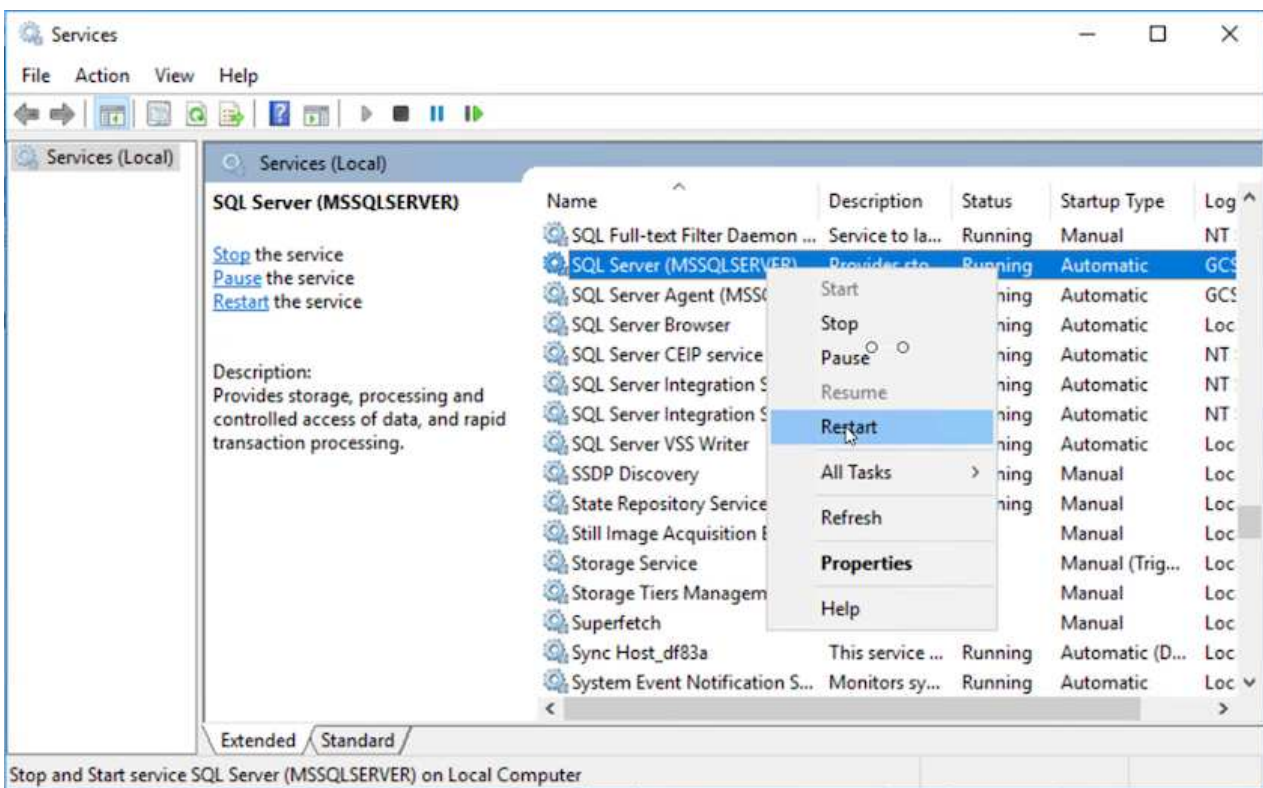


9. Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.

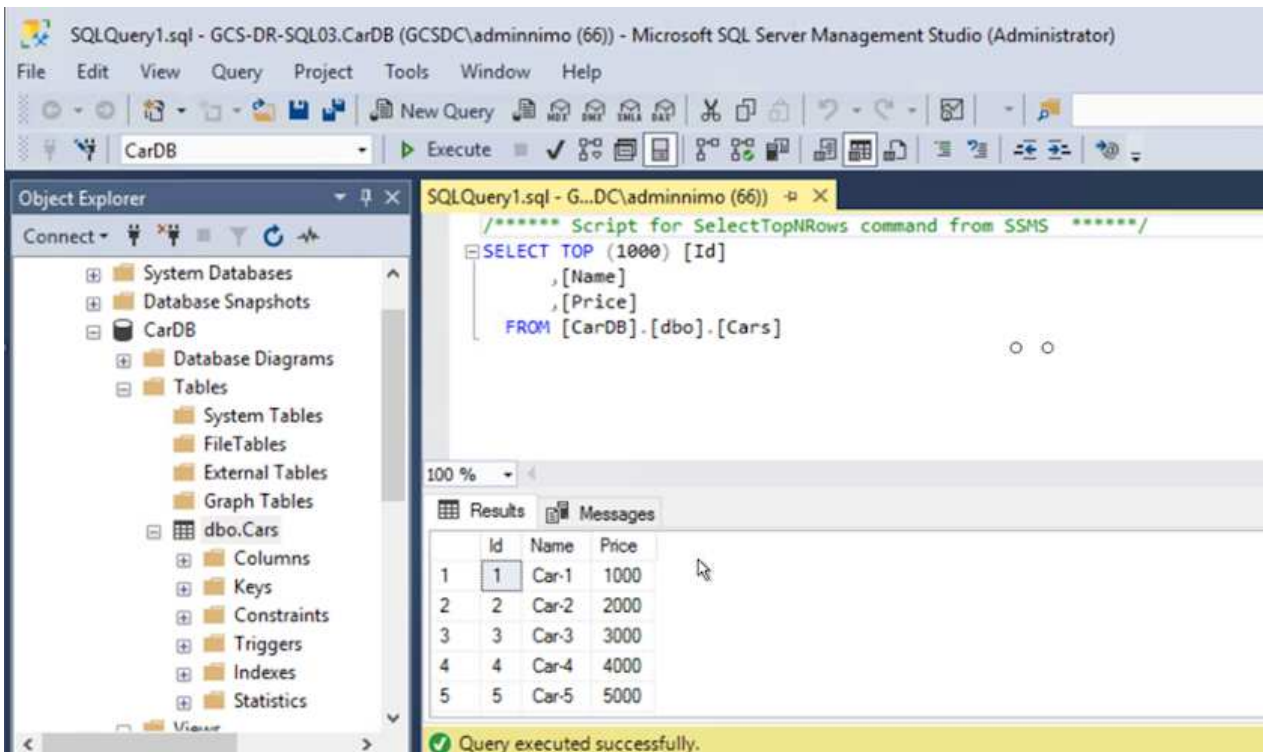




10. Riavviare il servizio del server MSSQL.



11. Assicurarsi che le risorse SQL siano nuovamente in linea.



Nel caso di NFS, collegare i volumi utilizzando il comando mount e aggiornare /etc/fstab voci.

A questo punto, è possibile eseguire le operazioni e continuare normalmente il business.



Sull'estremità NSX-T, è possibile creare un gateway Tier-1 dedicato separato per simulare scenari di failover. Ciò garantisce che tutti i carichi di lavoro possano comunicare tra loro, ma che nessun traffico possa essere instradato all'interno o all'esterno dell'ambiente, in modo che qualsiasi attività di triage, contenimento o protezione avanzata possa essere eseguita senza rischi di contaminazione incrociata. Questa operazione non rientra nell'ambito del presente documento, ma può essere facilmente eseguita per simulare l'isolamento.

Una volta che il sito primario è stato nuovamente operativo, è possibile eseguire il failback. La protezione delle macchine virtuali viene ripristinata da Jetstream e la relazione SnapMirror deve essere invertita.

1. Ripristinare l'ambiente on-premise. A seconda del tipo di incidente, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software DR JetStream.
2. Accedere all'ambiente on-premise ripristinato, accedere all'interfaccia utente DR Jetstream e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione failover nell'interfaccia utente.



Il piano di failback generato da CPT può anche essere utilizzato per avviare il ritorno delle macchine virtuali e dei relativi dati dall'archivio di oggetti all'ambiente VMware originale.

**JetStream DR**

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD\_Demo01 [View all](#)

Mode: Running in Failover

Active Site: 172.30.156.2

Recoverable / Total VMs: 4 / 4

Configurations

Storage Site: ANFCVODR

Owner Site: REMOTE (172.30.156.2)

Actions: + Create, Delete, More

More Actions: Restore, Resume Continuous Rehydration, Failback

Protected VMs | Settings | Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>



Specificare il ritardo massimo dopo la pausa delle macchine virtuali nel sito di ripristino e il riavvio nel sito protetto. Il tempo necessario per completare questo processo include il completamento della replica dopo l'arresto delle macchine virtuali di failover, il tempo necessario per pulire il sito di ripristino e il tempo necessario per ricreare le macchine virtuali nel sito protetto. NetApp consiglia 10 minuti.

**Failback Protected Domain**

1. General | 2a. Failback Settings | 2b. VM Settings | 3. Recovery VA | 4. DR Settings | 5. Summary

Failback Datacenter: A300-DataCenter

Failback Cluster: A300-Cluster

Failback Resource Pool: -

VM Folder (Optional): -

Failback Datastore: A300\_NFS\_vMotion

Maximum Delay After Stopping: 10 Minutes

Internal Network: VM\_187

External Replication Network: VM\_187

Management Network: VM\_187

Storage Site: ANFCVODR

DR Virtual Appliance: GCSDRVA002

Replication Local Storage: /dev/sdb

Buttons: Cancel, Back, Failback

3. Completare il processo di failback e confermare la ripresa della protezione delle macchine virtuali e la coerenza dei dati.



**JetStream DR**

Protected Domains | Statistics | Storage S...

Select Protected Domain: **GCSDRPD002**

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs | Settings | Alarms

**Failback Task Result**

Task Completed Successfully

Protected Domain: GCSDRPD002

VMs Recovery Status: Success

Total VMs Recovered: 4

GCSDRecovery03 Status:

Pre-script Execution Status: Not defined

Runbook Execution Status: Success

Post-script Execution Status: Not defined

- Una volta ripristinate le macchine virtuali, scollegare lo storage secondario dall'host e connettersi allo storage primario.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	

Information

Resync

Reverse Resync

Edit Schedule

Edit Max Transfer Rate

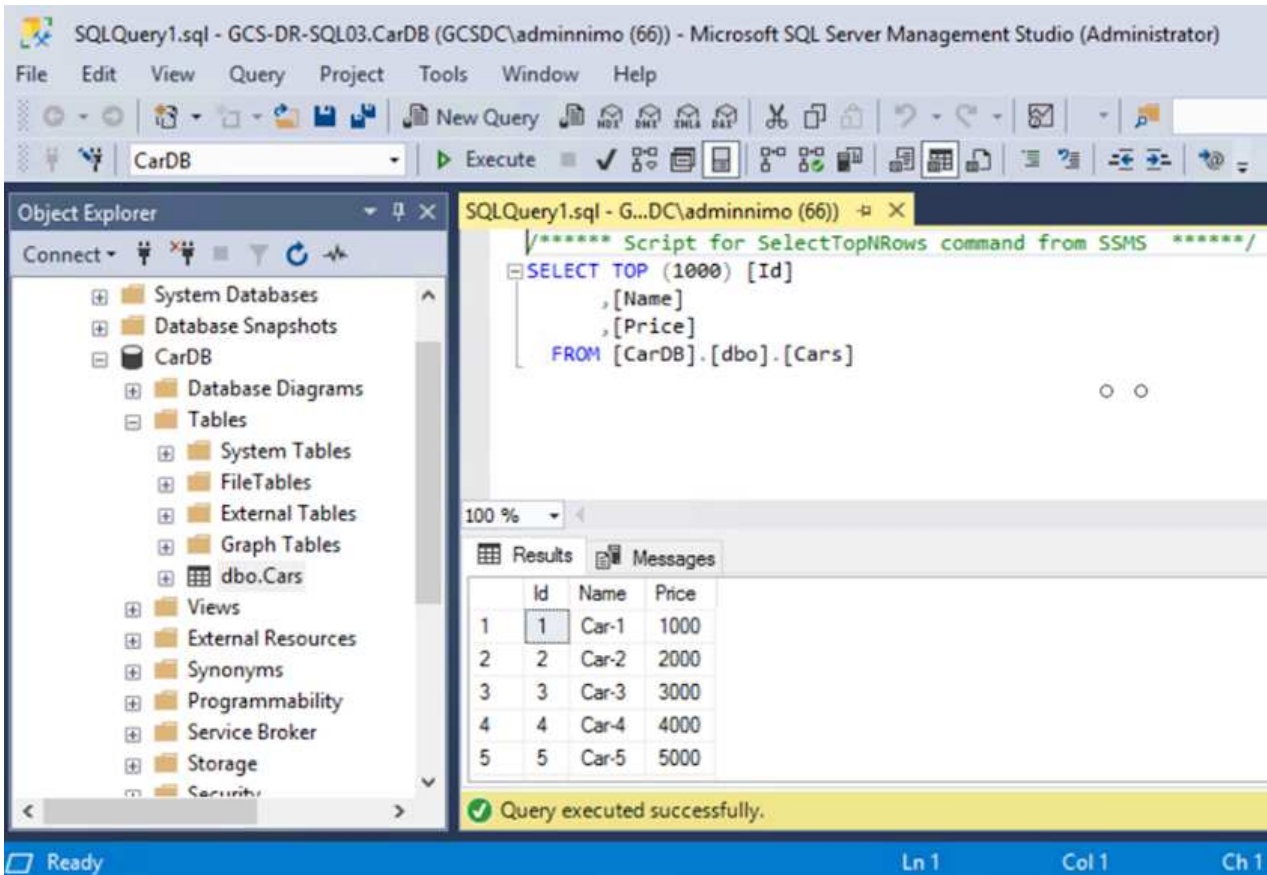
Delete

3 Volume Relationships | 6.54 GiB Replicated Capacity | 0 Currently Transferring | 3 Healthy | 0 Failed

3 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6, 2022, 11:03:00 AM 5.73 MiB
✓	gcsdrsqhld_sc46_copy ANFCVODRDemo	gcsdrsqhld_sc46 ntaphci-a300e9u25	1 minute 46 seconds	idle	snapmirrored	May 6, 2022, 11:01:39 AM 800.76 MiB
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	51 seconds	idle	snapmirrored	May 6, 2022, 11:03:15 AM 785.8 MiB

- Riavviare il servizio del server MSSQL.
- Verificare che le risorse SQL siano nuovamente in linea.



Per eseguire il failback allo storage primario, assicurarsi che la direzione della relazione rimanga la stessa di prima del failover eseguendo un'operazione di risincronizzazione inversa.



Per mantenere i ruoli dello storage primario e secondario dopo l'operazione di risincronizzazione inversa, eseguire nuovamente l'operazione di risincronizzazione inversa.

Questo processo è applicabile ad altre applicazioni come Oracle, ad altri tipi di database simili e ad altre applicazioni che utilizzano lo storage connesso al guest.

Come sempre, verifica le fasi necessarie per il ripristino dei carichi di lavoro critici prima di portarli in produzione.

## Vantaggi di questa soluzione

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

- Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- L'ottimizzazione della CPU e della RAM può contribuire a ridurre i costi del cloud consentendo il ripristino di cluster di calcolo più piccoli.

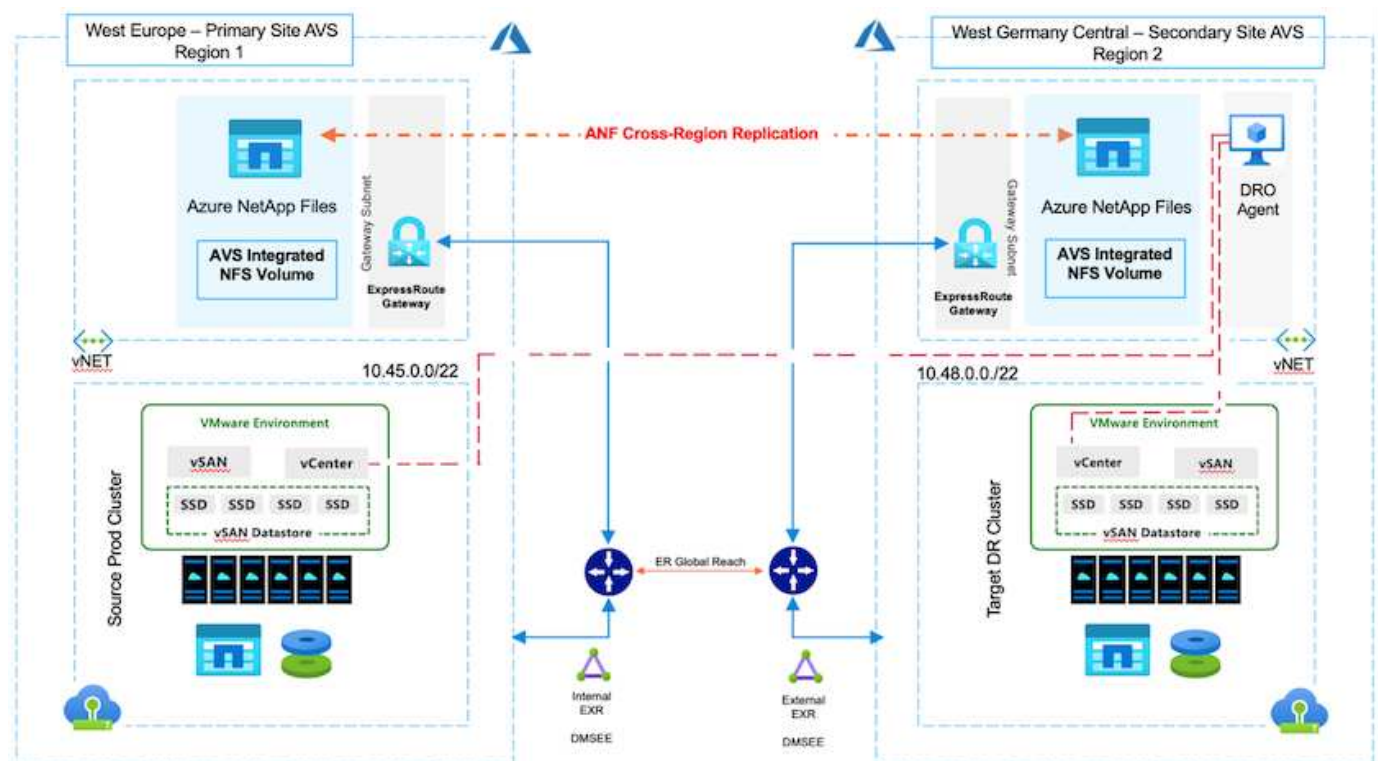
## TR-4955: Disaster recovery con Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

Autore: Niyaz Mohamed, NetApp Solutions Engineering

### Panoramica

Il disaster recovery che utilizza la replica a livello di blocco tra regioni all'interno del 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 replica dei volumi Azure NetApp Files (ANF) cross-region, i carichi di lavoro VMware eseguiti su un sito SDDC Azure VMware Solution (AVS) utilizzando i volumi Azure NetApp Files come datastore NFS sul sito AVS primario possono essere replicati in un sito AVS secondario designato nella regione di recupero di destinazione.

Disaster Recovery Orchestrator (DRO) (una soluzione basata su script con un'interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da un SDDC AVS a un altro. DRO automatizza il recovery interrompendo il peering delle repliche e montando il volume di destinazione come datastore, attraverso la registrazione delle macchine virtuali in AVS, sulle mappature di rete direttamente su NSX-T (incluso con tutti i cloud privati AVS).



### Prerequisiti e raccomandazioni generali

- Verificare di aver attivato la replica tra regioni creando il peering delle repliche. Vedere ["Creare la replica di un volume per Azure NetApp Files"](#).

- È necessario configurare ExpressRoute Global Reach tra i cloud privati Azure VMware Solution di origine e di destinazione.
- È necessario disporre di un service principal in grado di accedere alle risorse.
- È supportata la seguente topologia: Dal sito AVS primario al sito AVS secondario.
- Configurare **"replica"** pianifica ciascun volume in modo appropriato in base alle esigenze aziendali e al tasso di cambiamento dei dati.



Non sono supportate topologie a cascata e fan-in e fan-out.

## Per iniziare

### Implementare la soluzione VMware Azure

Il **"Soluzione VMware Azure"** (AVS) è un servizio di cloud ibrido che fornisce SDDC VMware completamente funzionali all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione di prima parte completamente gestita e supportata da Microsoft e verificata da VMware che utilizza l'infrastruttura Azure. Pertanto, i clienti ottengono VMware ESXi per la virtualizzazione del calcolo, vSAN per lo storage iperconvergente e NSX per il networking e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture di data center leader di settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure native. Una combinazione di SDDC e Azure NetApp Files per la soluzione VMware Azure offre le migliori performance con una latenza di rete minima.

Per configurare un cloud privato AVS su Azure, seguire la procedura descritta in questa sezione **"collegamento"** Per la documentazione NetApp e in questo **"collegamento"** Per la documentazione Microsoft. Un ambiente pilota con configurazione minima può essere utilizzato per scopi di DR. Questa configurazione contiene solo i componenti principali per supportare le applicazioni critiche e può scalare e generare più host per sostenere la maggior parte del carico in caso di failover.



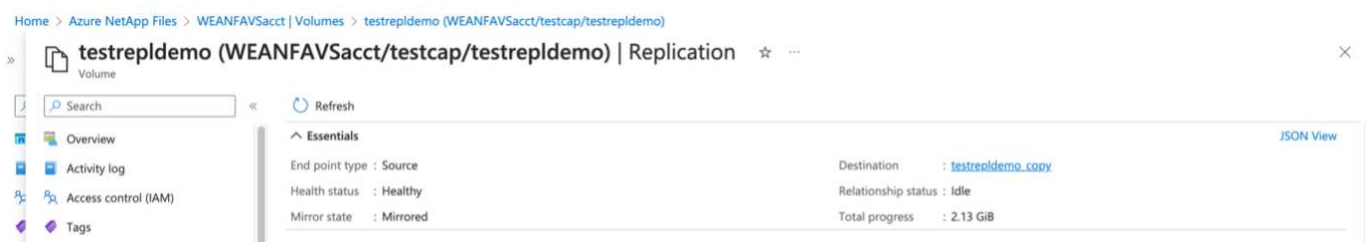
Nella versione iniziale, DRO supporta un cluster SDDC AVS esistente. La creazione di SDDC on-demand sarà disponibile in una release imminente.

### Provisioning e configurazione di Azure NetApp Files

**"Azure NetApp Files"** è un servizio di file storage misurato di livello enterprise dalle performance elevate. Seguire la procedura descritta in questa sezione **"collegamento"** Eseguire il provisioning e la configurazione di Azure NetApp Files come datastore NFS per ottimizzare le implementazioni di cloud privato AVS.

### Creazione di replica di volumi per i volumi datastore basati su file di Azure NetApp

Il primo passaggio consiste nell'impostare la replica cross-region per i volumi del datastore desiderati dal sito primario AVS al sito secondario AVS con le frequenze e le retention appropriate.



Seguire la procedura descritta in questa sezione **"collegamento"** per impostare la replica tra regioni creando il peering delle repliche. Il livello di servizio per il pool di capacità di destinazione può corrispondere a quello del

pool di capacità di origine. Tuttavia, per questo caso di utilizzo specifico, è possibile selezionare il livello di servizio standard, quindi ["modificare il livello di servizio"](#) In caso di disastro reale o di simulazioni di DR.



Una relazione di replica tra regioni è un prerequisito e deve essere creata in anticipo.

## Installazione DRO

Per iniziare a utilizzare DRO, utilizzare il sistema operativo Ubuntu sulla macchina virtuale Azure designata e assicurarsi di soddisfare i prerequisiti. Quindi installare il pacchetto.

### Prerequisiti:

- Service Principal in grado di accedere alle risorse.
- Assicurarsi che esista una connettività appropriata alle istanze SDDC e Azure NetApp Files di origine e destinazione.
- Se si utilizzano i nomi DNS, la risoluzione DNS deve essere effettiva. In caso contrario, utilizzare gli indirizzi IP per vCenter.

### Requisiti del sistema operativo:

- Ubuntu Focal 20.04 (LTS) i seguenti pacchetti devono essere installati sulla macchina virtuale dell'agente designata:
- Docker
- Docker - compose
- JqChange `docker.sock` a questa nuova autorizzazione: `sudo chmod 666 /var/run/docker.sock`.



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

I passaggi sono i seguenti:

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

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



L'agente deve essere installato nell'area del sito AVS secondario o nell'area del sito AVS primario in un AZ separato da SDDC.

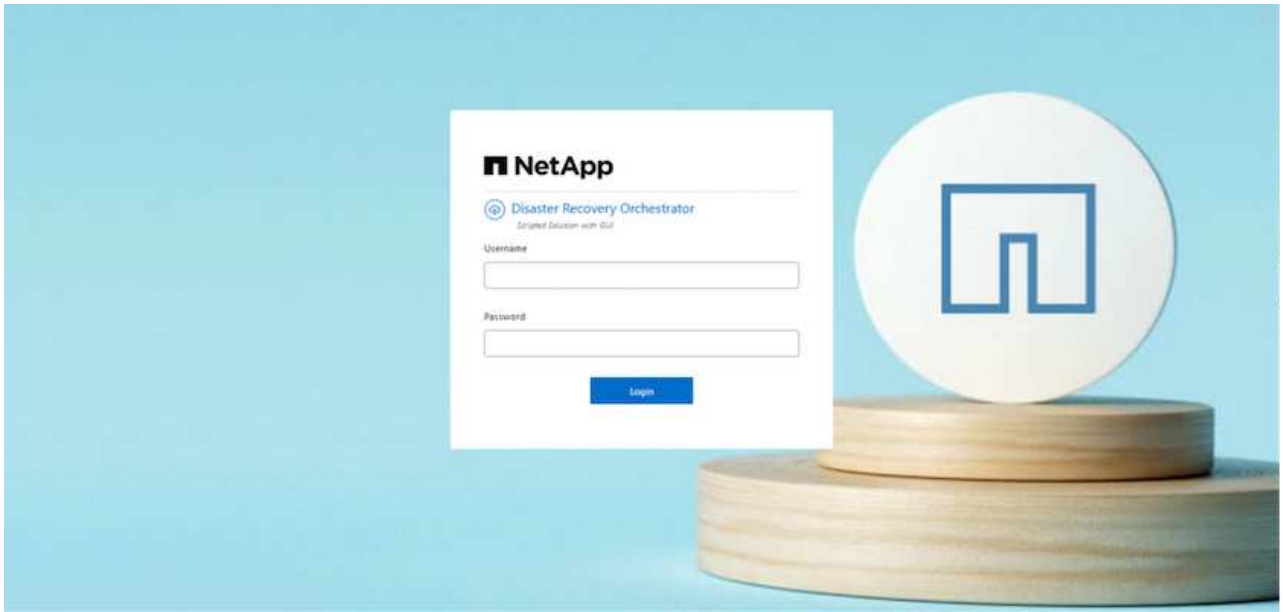
2. Decomprimere il pacchetto, eseguire lo script di implementazione e immettere l'IP host (ad esempio, 10.10.10.10).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Accedere all'interfaccia utente utilizzando le seguenti credenziali:

- Nome utente: admin

- Password: admin



## Configurazione DRO

Dopo aver configurato correttamente Azure NetApp Files e AVS, è possibile iniziare a configurare DRO per automatizzare il ripristino dei workload dal sito AVS primario al sito AVS secondario. NetApp consiglia di implementare l'agente DRO nel sito AVS secondario e di configurare la connessione del gateway ExpressRoute in modo che l'agente DRO possa comunicare tramite la rete con i componenti AVS e Azure NetApp Files appropriati.

Il primo passaggio consiste nell'aggiungere credenziali. DRO richiede l'autorizzazione per scoprire Azure NetApp Files e la soluzione VMware Azure. È possibile concedere le autorizzazioni richieste a un account Azure creando e configurando un'applicazione Azure Active Directory (ad) e ottenendo le credenziali Azure necessarie a DRO. È necessario associare l'entità del servizio all'abbonamento Azure e assegnargli un ruolo personalizzato con le autorizzazioni necessarie pertinenti. Quando si aggiungono ambienti di origine e di destinazione, viene richiesto di selezionare le credenziali associate all'entità del servizio. È necessario aggiungere queste credenziali a DRO prima di fare clic su Add New Site (Aggiungi nuovo sito).

Per eseguire questa operazione, attenersi alla seguente procedura:

1. Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti (/admin/admin). La password può essere reimpostata dopo il primo accesso utilizzando l'opzione Change Password (Modifica password).
2. Nella parte superiore destra della console DRO, fare clic sull'icona **Impostazioni** e selezionare **credenziali**.
3. Fare clic su Add New Credential (Aggiungi nuova credenziale) e seguire la procedura guidata.
4. Per definire le credenziali, immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
  - Nome della credenziale
  - ID tenant
  - ID client



- Segreto del client
- ID abbonamento

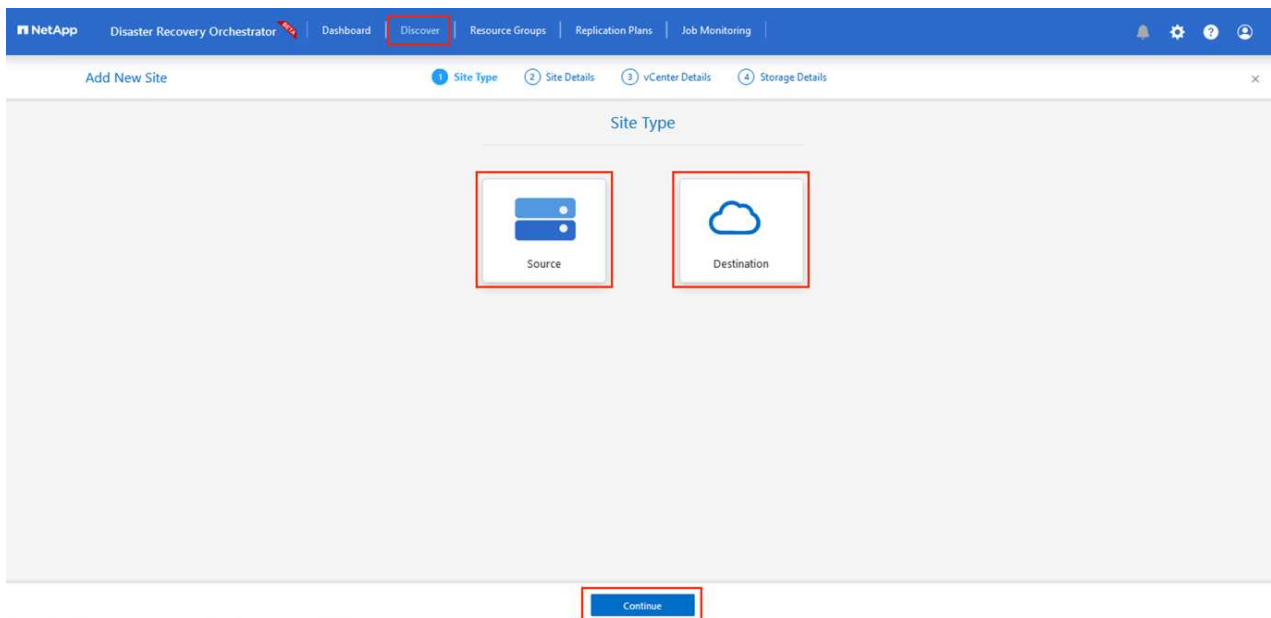
Queste informazioni dovrebbero essere state acquisite al momento della creazione dell'applicazione ad.

5. Confermare i dettagli relativi alle nuove credenziali e fare clic su Add Credential (Aggiungi credenziale).

The screenshot shows the 'Add New Credential' interface in the NetApp Disaster Recovery Orchestrator. The top navigation bar includes 'NetApp', 'Disaster Recovery Orchestrator', and several menu items: 'Dashboard', 'Discover', 'Resource Groups', 'Replication Plans', and 'Job Monitoring'. On the right side of the navigation bar, there are icons for a bell, a gear (highlighted with a red box), a question mark, and a user profile. Below the navigation bar, the page title is 'Add New Credential' and the sub-header is '1 Credentials Details'. The main content area is titled 'Enter Credentials Details' and contains five input fields, each with a red highlight: 'Credential Name', 'Tenant Id', 'Client Id', 'Client Secret', and 'Subscription Id'. At the bottom of the form is a blue button labeled 'Add Credential'.

Dopo aver aggiunto le credenziali, è il momento di individuare e aggiungere i siti AVS primari e secondari (sia vCenter che l'account storage Azure NetApp Files) a DRO. Per aggiungere il sito di origine e di destinazione, attenersi alla seguente procedura:

6. Accedere alla scheda **Discover**.
7. Fare clic su **Aggiungi nuovo sito**.
8. Aggiungere il seguente sito AVS primario (indicato come **origine** nella console).
  - VCenter SDDC
  - Account storage Azure NetApp Files
9. Aggiungere il seguente sito AVS secondario (indicato come **destinazione** nella console).
  - VCenter SDDC
  - Account storage Azure NetApp Files

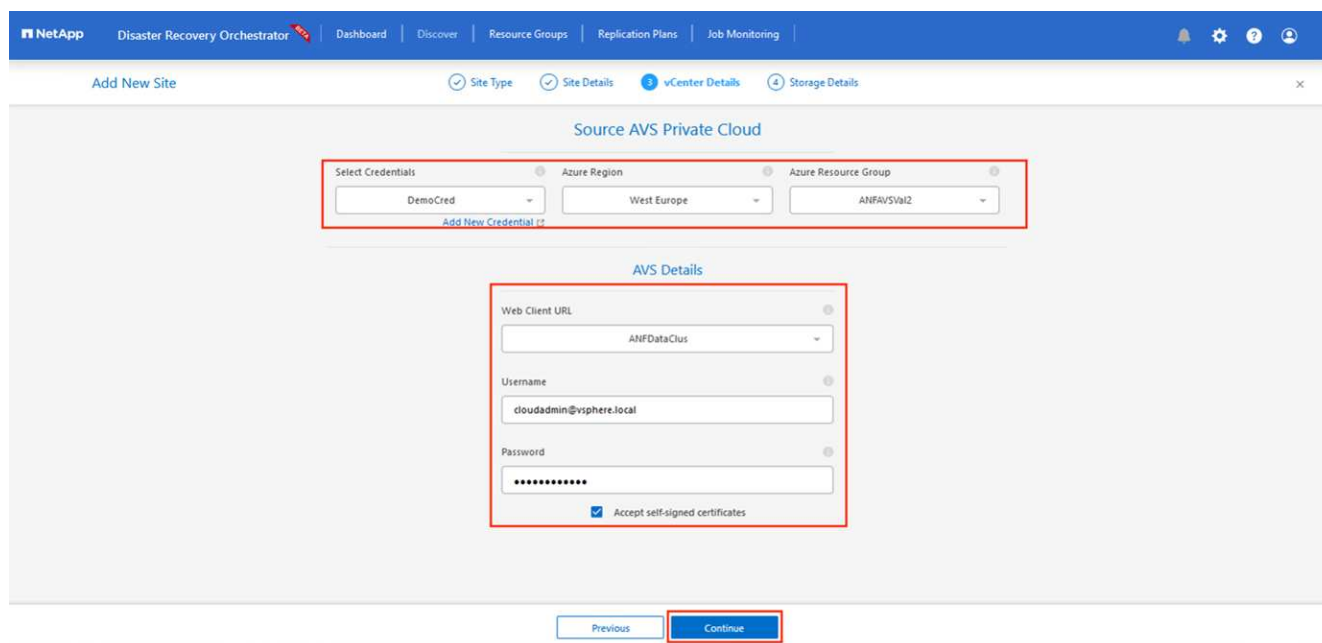


10. Aggiungere i dettagli del sito facendo clic su **Source (origine)**, immettendo un nome descrittivo del sito e selezionando il connettore. Quindi fare clic su **continua**.



A scopo dimostrativo, l'aggiunta di un sito di origine viene trattata in questo documento.

11. Aggiorna i dettagli di vCenter. A tale scopo, selezionare le credenziali, l'area Azure e il gruppo di risorse dal menu a discesa per l'AVS SDDC primario.
12. IL DRO elenca tutti gli SDDC disponibili all'interno della regione. Selezionare l'URL del cloud privato designato dal menu a discesa.
13. Inserire il `cloudadmin@vsphere.local` credenziali dell'utente. È possibile accedervi dal portale Azure. Seguire la procedura indicata in questo ["collegamento"](#). Al termine, fare clic su **Continue** (continua).



14. Selezionare i dettagli dell'archiviazione di origine (ANF) selezionando il gruppo Azure Resource e l'account NetApp.



## 15. Fare clic su **Create Site** (Crea sito).

Site Name	Site Type	Location	vCenter	Storage	VM List	Discovery Status
DemoDest	Destination	Cloud	1	1		https://10.75.0.2/ Success
DemoSRC	Source	Cloud	1	1	<a href="#">View VM List</a>	https://172.30.156.2/ Success

Una volta aggiunto, DRO esegue il rilevamento automatico e visualizza le macchine virtuali con repliche tra regioni corrispondenti dal sito di origine al sito di destinazione. DRO rileva automaticamente le reti e i segmenti utilizzati dalle macchine virtuali e li popola.

VM Name	VM Status	VM State	DataStore	CPU	Memory (MB)
HCBench_2.6.1	Not Protected	Powered On	vsanDatastore	8	8192
hci-fio-datastore-13984-0-1	Not Protected	Powered Off	HCBench_2.6.1	32	65536
ICCA005-WD-R1	Not Protected	Powered On	vsanDatastore	8	14336
ICCA005-FIE-R1	Not Protected	Powered On	vsanDatastore	8	3072
ICCA005-IX-R1	Not Protected	Powered On	vsanDatastore	8	3072
HCK_Demo_05	Not Protected	Powered Off	Demo002	1	2048
hci-nim-datastore-13984-0-1	Not Protected	Powered Off	HCBench_2.6.1	24	49152

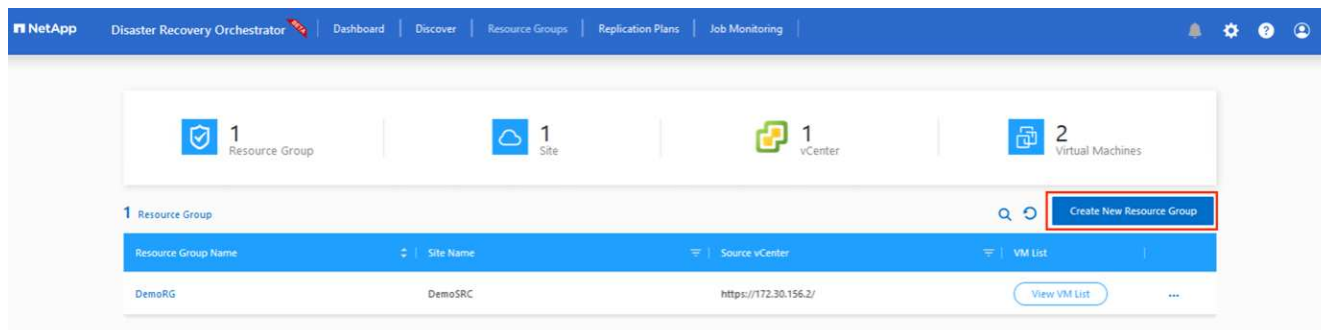
Il passaggio successivo consiste nel raggruppare le macchine virtuali richieste nei rispettivi gruppi funzionali come gruppi di risorse.

### Raggruppamenti di risorse

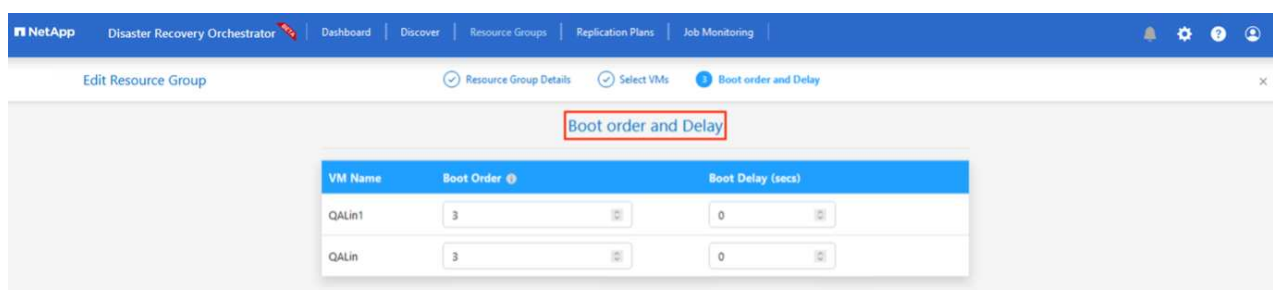
Una volta aggiunte le piattaforme, raggruppare le macchine virtuali che si desidera ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di macchine virtuali dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali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

Per iniziare a creare gruppi di risorse, fare clic sulla voce di menu **Crea nuovo gruppo di risorse**.

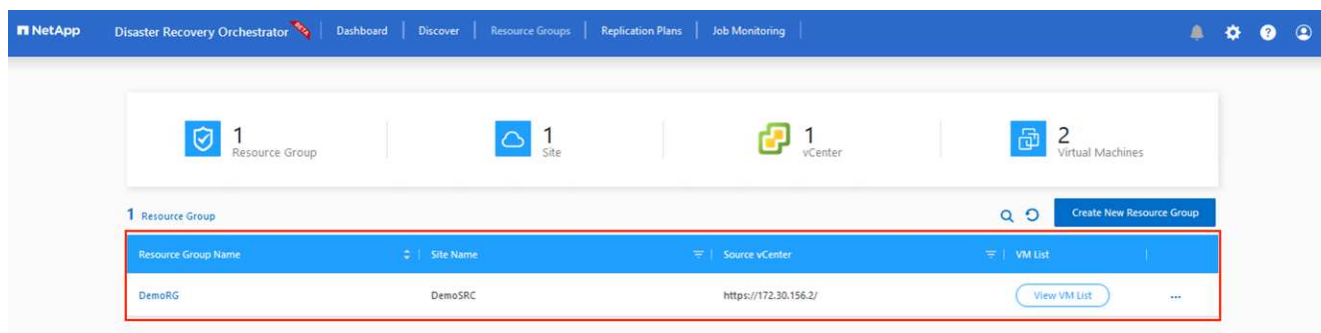
1. Accedere a **Resource Groups** e fare clic su **Create New Resource Group** (Crea nuovo gruppo di risorse).



2. In New Resource Group (nuovo gruppo di risorse), selezionare il sito di origine dal menu a discesa e fare clic su **Create** (Crea).
3. Fornire i dettagli del gruppo di risorse e fare clic su **continua**.
4. Selezionare le macchine virtuali appropriate utilizzando l'opzione di ricerca.
5. Selezionare **Boot Order** (Ordine di avvio) e **Boot Delay** (sec) per tutte le macchine virtuali selezionate. Impostare l'ordine della sequenza di accensione selezionando ciascuna macchina virtuale e impostando la relativa priorità. Il valore predefinito per tutte le macchine virtuali è 3. Le opzioni sono le seguenti:
  - La prima macchina virtuale ad accenderlo
  - Predefinito
  - L'ultima macchina virtuale ad accenderlo



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



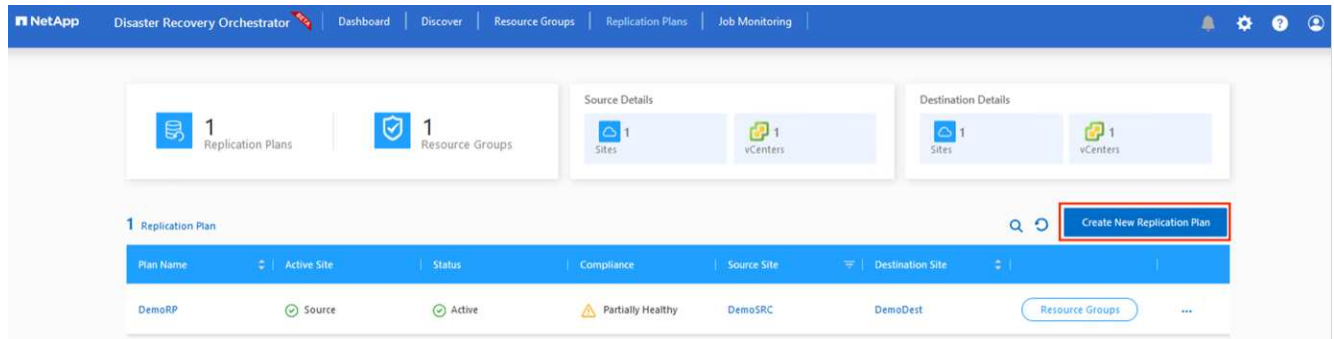
## Piani di replica

È necessario disporre 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, scegliere i gruppi di risorse da includere in questo piano e includere anche il raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, Tier-1, Tier-2 e così via). I piani sono spesso chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda Replication Plan (piano di replica) e fare clic su **New**

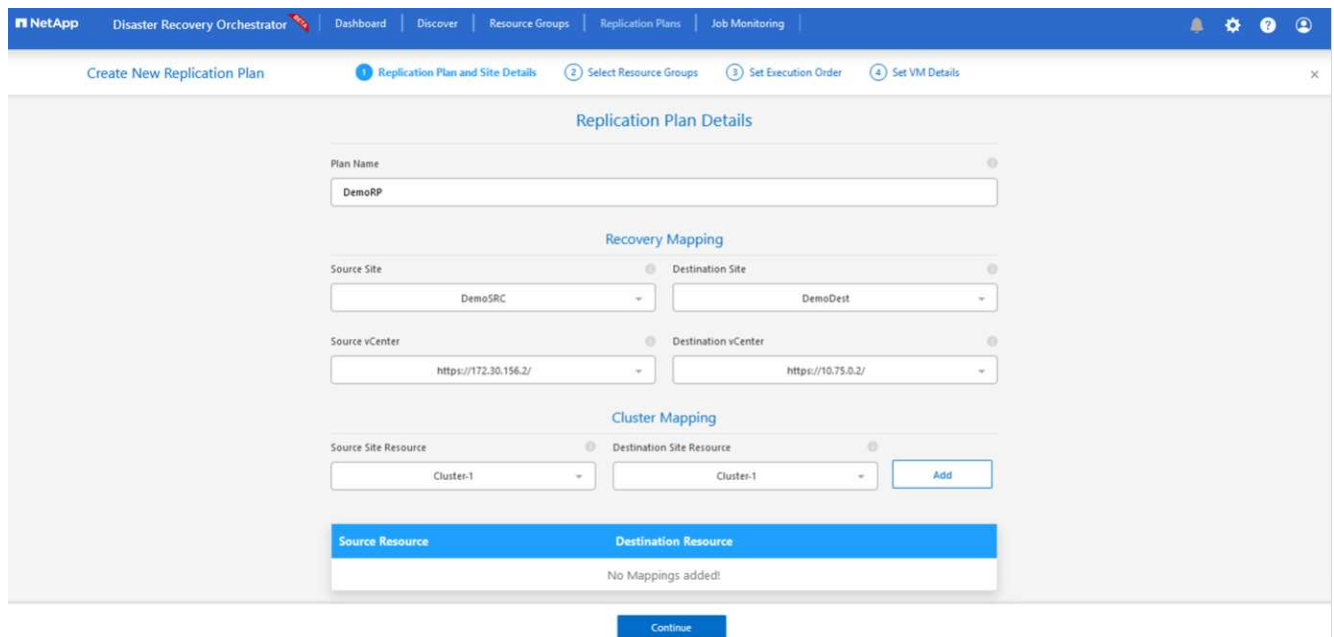
## Replication Plan (nuovo piano di replica).

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

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



2. In **New Replication Plan**, fornire un nome per il piano e aggiungere i mapping di ripristino selezionando Source Site (Sito di origine), Associated vCenter (vCenter associato), Destination Site (Sito di destinazione) e Associated vCenter (vCenter associato).



3. Una volta completata la mappatura di ripristino, selezionare **Cluster Mapping** (mappatura cluster).

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

### Replication Plan Details

Plan Name: DemoRP

#### Recovery Mapping

Source Site: DemoSRC | Destination Site: DemoDest

Source vCenter: https://172.30.156.2/ | Destination vCenter: https://10.75.0.2/

#### Cluster Mapping

No more Source/Destination cluster resources available for mapping

Source Resource	Destination Resource	
Cluster-1	Cluster-1	Delete

Continue

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, impostare la mappatura di rete sul segmento appropriato. I segmenti devono essere già sottoposti a provisioning sul cluster AVS secondario e, per mappare le macchine virtuali su di essi, selezionare il segmento appropriato.
7. I mapping degli archivi dati vengono selezionati automaticamente in base alla selezione delle macchine virtuali.



La replica cross-region (CRR) è a livello di volume. Pertanto, tutte le macchine virtuali che risiedono sul rispettivo volume vengono replicate nella destinazione CRR. Assicurarsi di selezionare tutte le macchine virtuali che fanno parte del datastore, in quanto vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

### Replication Plan Details

#### Select Execution Order

Resource Group Name	Execution Order
DemoRG	3

#### Network Mapping

No more Source/Destination network resources available for mapping

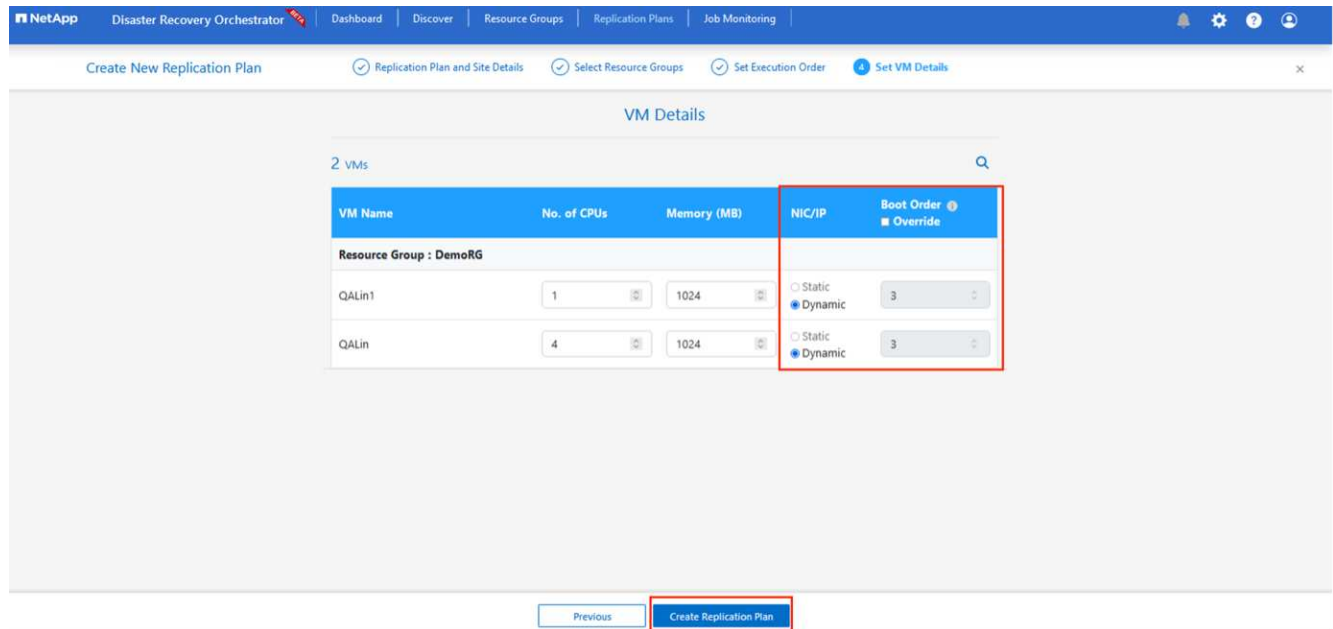
Source Resource	Destination Resource	
SepSeg	SegDR	Delete

#### DataStore Mapping

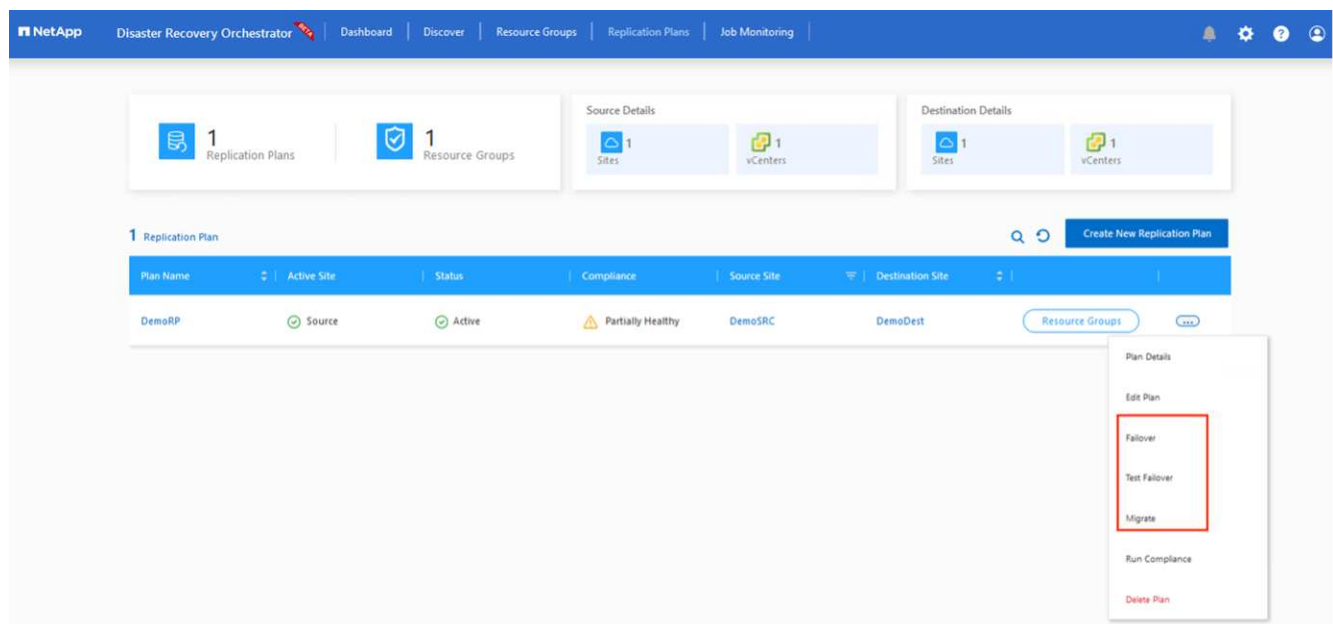
Source DataStore	Destination Volume
TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrc01copy

Previous | Continue

8. In VM details (Dettagli VM), è possibile ridimensionare i parametri della CPU e della RAM delle macchine virtuali. Questo può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o quando si eseguono test di DR senza dover eseguire il provisioning di un'infrastruttura fisica VMware uno a uno. Inoltre, modificare l'ordine di avvio e il ritardo di avvio (sec) 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 ciò che è stato selezionato 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.

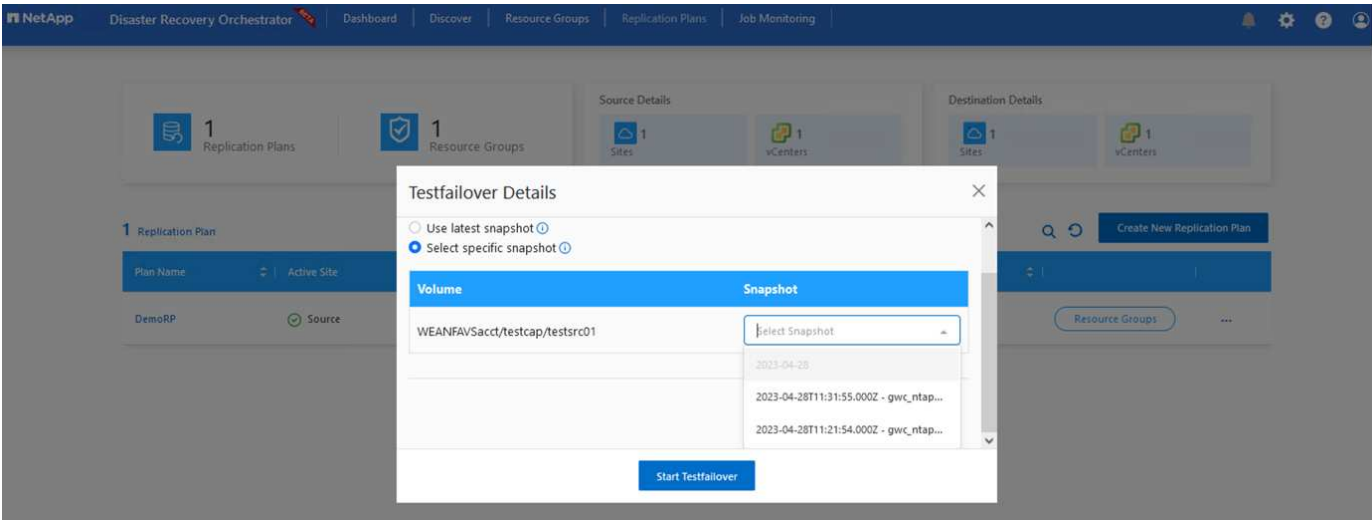


9. Fare clic su **Create Replication Plan** (Crea piano di replica). Una volta creato il piano di replica, è possibile eseguire il failover, il failover di test o le opzioni di migrazione in base ai requisiti.

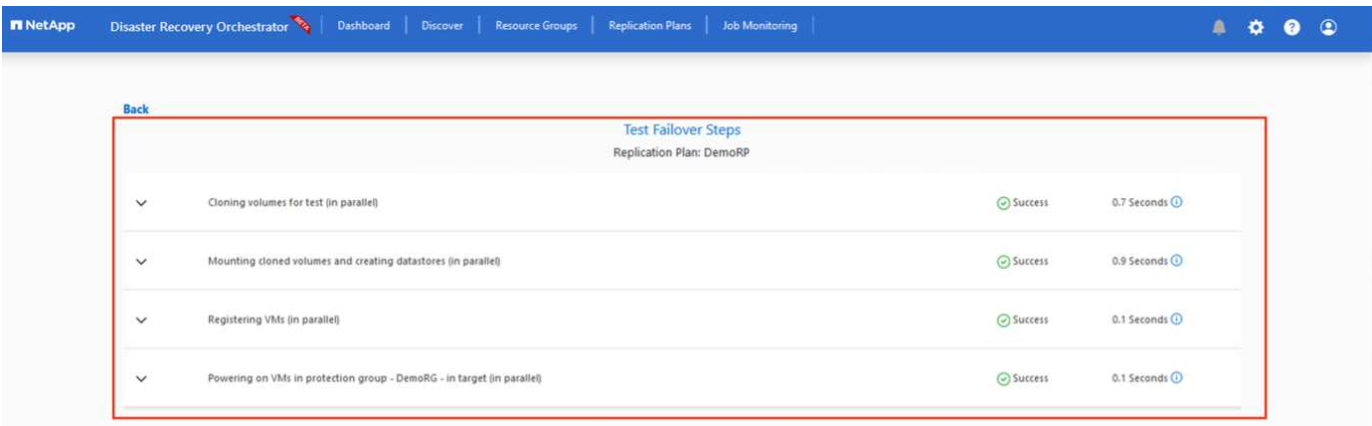


Durante le opzioni di failover e test di failover, viene utilizzato lo snapshot più recente oppure è possibile selezionare uno snapshot specifico da uno snapshot point-in-time. L'opzione point-in-time può essere molto

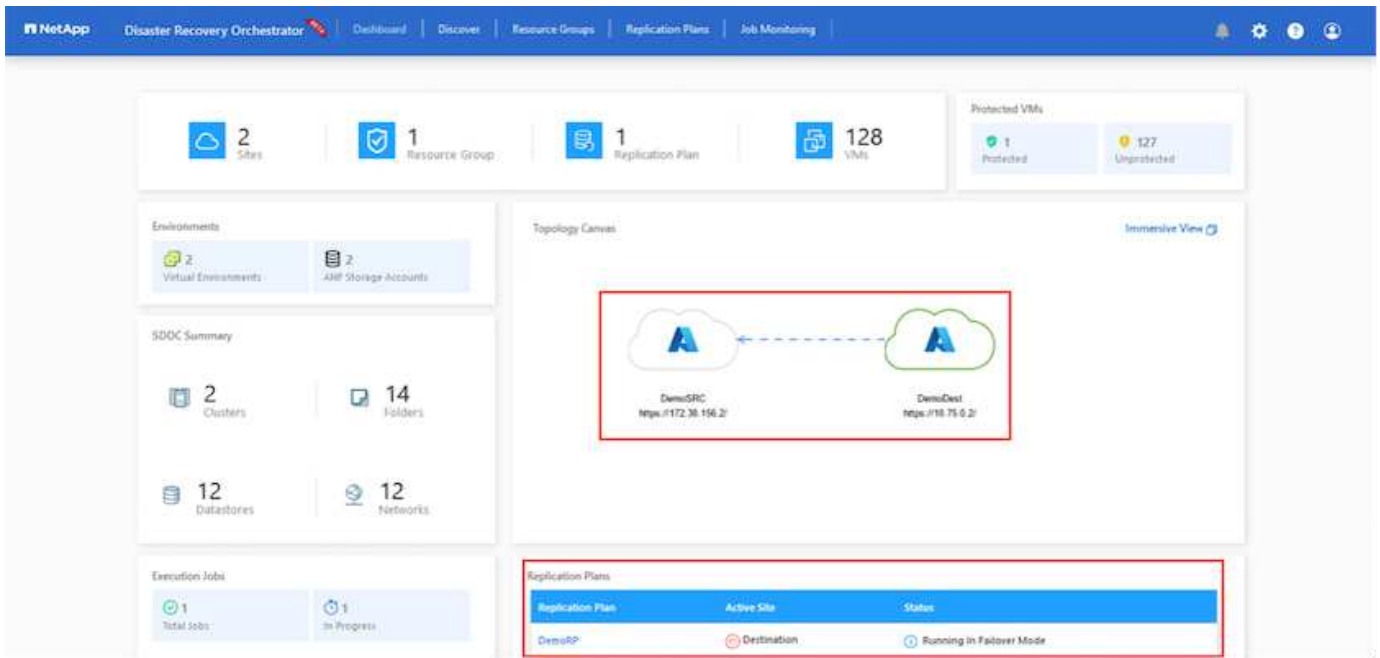
vantaggiosa se si sta affrontando un evento di corruzione come ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i tempi di rilevazione disponibili.



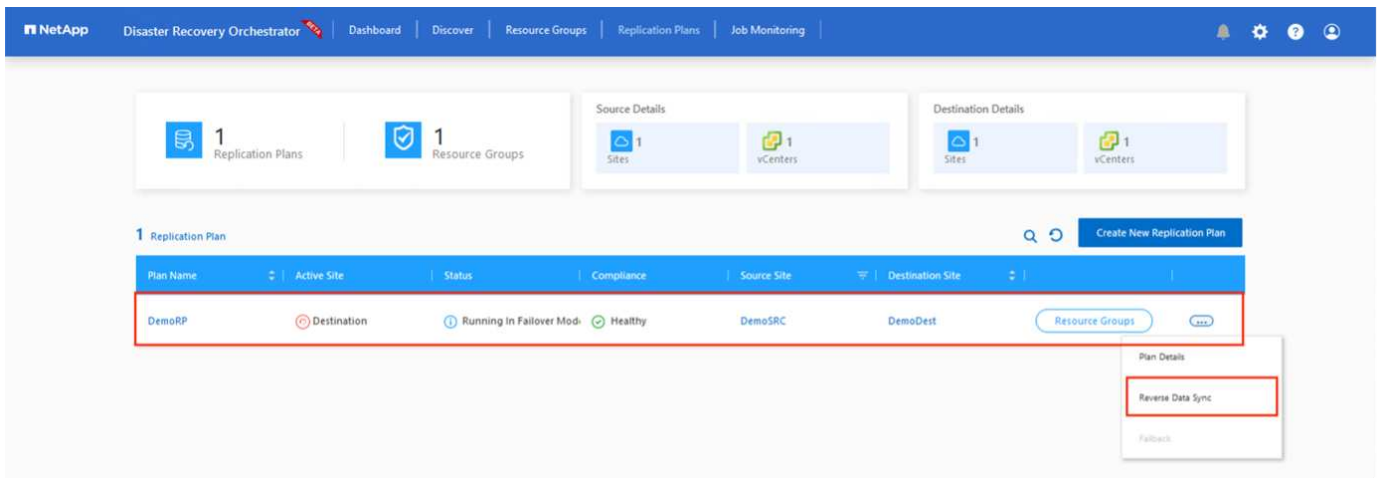
Per attivare il failover o verificare il failover con la configurazione specificata nel piano di replica, fare clic su **failover** o **Test failover**. È possibile monitorare il piano di replica nel menu delle attività.



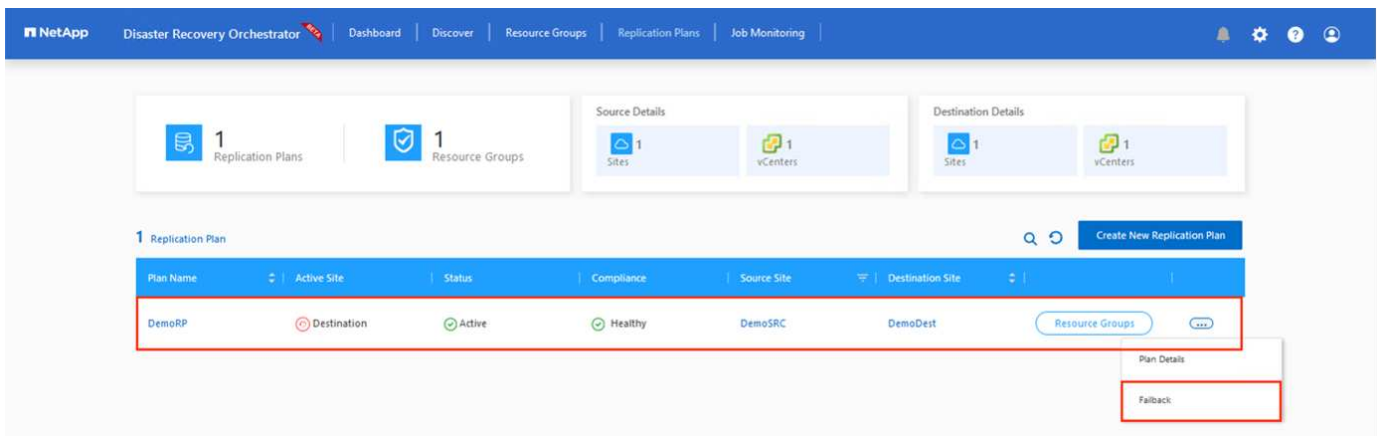
Dopo l'attivazione del failover, gli elementi ripristinati possono essere visualizzati nel sito secondario AVS SDDC vCenter (VM, reti e datastore). Per impostazione predefinita, le macchine virtuali vengono ripristinate nella cartella workload.



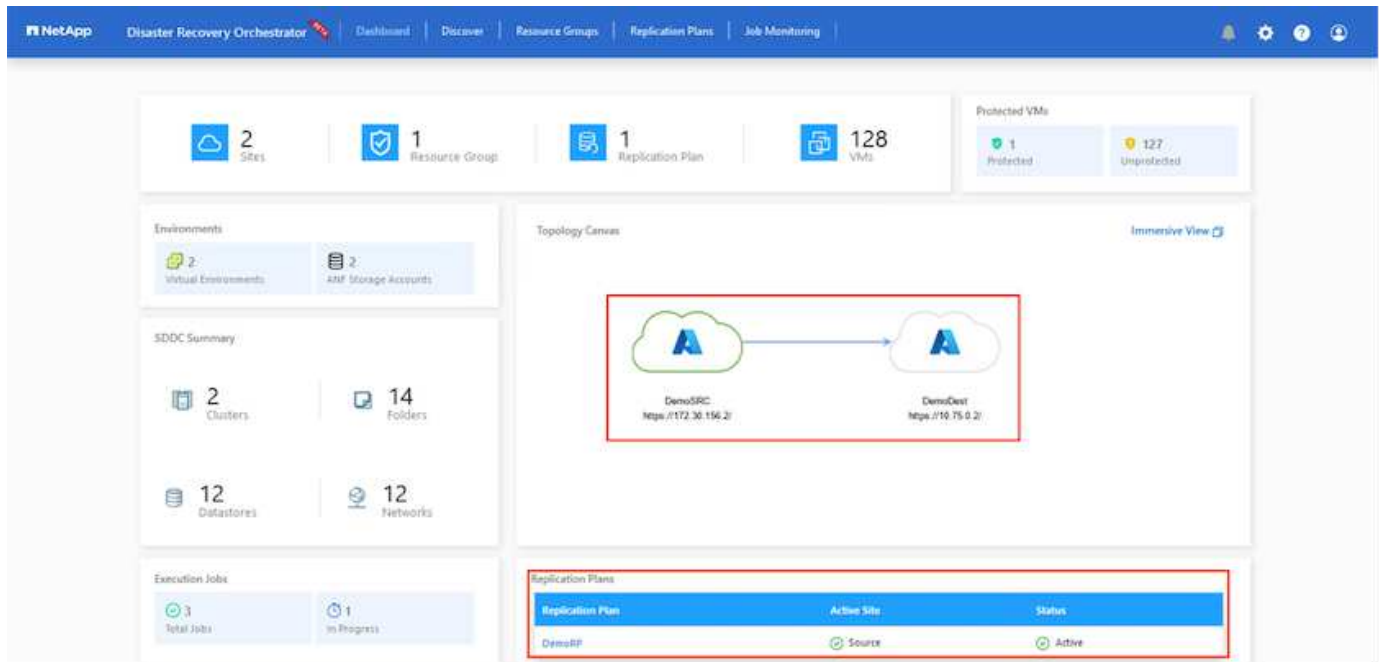
Il failback può essere attivato a livello di piano di replica. In caso di failover di test, l'opzione di strappo può essere utilizzata per eseguire il rollback delle modifiche e rimuovere il volume appena creato. I fallback relativi al failover sono un processo in due fasi. Selezionare il piano di replica e selezionare **Reverse Data Sync**.



Al termine di questa fase, attivare il failback per tornare al sito AVS primario.







Dal portale Azure, possiamo vedere che lo stato di salute della replica è stato interrotto per i volumi appropriati che sono stati mappati al sito secondario AVS SDDC come volumi di lettura/scrittura. Durante il failover di test, DRO non esegue il mapping del volume di destinazione o di replica. Al contrario, crea un nuovo volume dello snapshot di replica cross-region richiesto ed espone il volume come datastore, che consuma ulteriore capacità fisica dal pool di capacità e garantisce che il volume di origine non venga modificato. In particolare, i processi di replica possono continuare durante i test di DR o i flussi di lavoro di triage. Inoltre, questo processo garantisce che il ripristino possa essere ripulito senza il rischio che la replica venga distrutta in caso di errori o di ripristino di dati corrotti.

### 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, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi che si verificano (ad esempio, da malware in sospensione o attraverso applicazioni vulnerabili).

DRO risolve questi problemi consentendo alle organizzazioni di eseguire il ripristino da qualsiasi point-in-time disponibile. I carichi di lavoro vengono quindi ripristinati in reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro, ma non siano esposte al traffico nord-sud. Questo processo offre ai team di sicurezza un luogo sicuro per condurre indagini legali e identificare eventuali malware nascosti o inattivi.

### Conclusione

La soluzione di disaster recovery Azure NetApp Files e Azure offre i seguenti vantaggi:

- Sfrutta una replica Azure NetApp Files cross-region efficiente e resiliente.
- Ripristino a qualsiasi point-in-time disponibile con la conservazione degli snapshot.
- Automatizzare completamente tutte le fasi necessarie per ripristinare da centinaia a migliaia di macchine virtuali dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- Il recupero del workload sfrutta il processo "Create new volumes from the most recent snapshot" (Crea nuovi volumi dalle snapshot più recenti), che non manipola il volume replicato.

- Evitare qualsiasi rischio di corruzione dei dati sui volumi o sugli snapshot.
- Evita le interruzioni della replica durante i flussi di lavoro dei test di DR.
- Sfrutta i dati di DR e le risorse di calcolo del cloud per i flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- L'ottimizzazione della CPU e della RAM può contribuire a ridurre i costi del cloud consentendo il ripristino a cluster di calcolo più piccoli.

#### Dove trovare ulteriori informazioni

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

- Creare la replica di un volume per Azure NetApp Files

["https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"](https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering)

- Replica cross-region di volumi Azure NetApp Files

["https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"](https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives)

- "Soluzione VMware Azure"

["https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"](https://learn.microsoft.com/en-us/azure/azure-vmware/introduction)

- Implementare e configurare l'ambiente di virtualizzazione su Azure

["https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"](https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html)

- Implementare e configurare Azure VMware Solution

<https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal>

## Utilizzo di Veeam Replication e datastore Azure NetApp Files per il disaster recovery nella soluzione Azure VMware

Autore: Niyaz Mohamed - Ingegneria di soluzioni di NetApp

### Panoramica

I datastore Azure NetApp Files (ANF) separano lo storage dal calcolo e liberano la flessibilità necessaria a qualsiasi organizzazione per portare i propri workload nel cloud. Offre ai clienti un'infrastruttura storage flessibile e dalle performance elevate, che scala in modo indipendente dalle risorse di calcolo. Le dimensioni del datastore di Azure NetApp Files semplificano e ottimizzano l'implementazione insieme alla soluzione Azure VMware (AVS) come sito di disaster recovery per gli ambienti VMware on-premise.

I datastore NFS basati su volume Azure NetApp Files (ANF) possono essere utilizzati per replicare i dati on-premise utilizzando qualsiasi soluzione di terze parti validata che offre funzionalità di replica delle VM. Aggiungendo datastore Azure NetApp Files, potrai ottimizzare i costi dell'implementazione rispetto a una soluzione SDDC Azure VMware con un'enorme quantità di host ESXi per ospitare lo storage. Questo approccio è chiamato "quadro spie pilota". Un cluster di spie pilota è una configurazione host AVS minima (3 nodi AVS) insieme alla capacità del datastore Azure NetApp Files.

L'obiettivo è mantenere un'infrastruttura a basso costo con tutti i componenti principali per gestire il failover. Un cluster di spie pilota può scalare in orizzontale e fornire più host AVS se si verifica un failover. Inoltre, una volta completato il failover e ripristinate le normali operazioni, il cluster di spie può scalare di nuovo alla modalità operativa a basso costo.

## Finalità del presente documento

Questo articolo descrive come utilizzare il datastore Azure NetApp Files con Veeam Backup e la replica per configurare il disaster recovery per le VM VMware on-premise su (AVS) utilizzando la funzionalità software di replica Veeam VM.

Veeam Backup & Replication è un'applicazione di backup e replica per ambienti virtuali. Quando le macchine virtuali vengono replicate, Veeam Backup & Replication viene replicato da AVS, il software crea una copia esatta delle VM nel formato VMware vSphere nativo sul cluster SDDC AVS di destinazione. Veeam Backup & Replication manterrà la copia sincronizzata con la VM originale. La replica offre il miglior recovery time objective (RTO) essendo presente una copia montata di una macchina virtuale nel sito di DR in uno stato ready-to-start.

Questo meccanismo di replica garantisce che i carichi di lavoro possano avviarsi rapidamente in un AVS 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, zero blocchi di dati, file swap e "file OS guest di macchine virtuali esclusi". Il software comprime anche il traffico di replica. Per evitare che i processi di replica consumino l'intera larghezza di banda della rete, è possibile utilizzare 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 uno dei suoi punti di ripristino noti. Ciò abilita recovery dal ransomware o test isolati, se necessario. 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. ["Implementa la soluzione Azure VMware \(AVS\)"](#) cloud privato e ["Collegare i datastore Azure NetApp Files"](#) Agli host della soluzione Azure VMware.

Un ambiente pilota configurato con una configurazione minima può essere utilizzato per scopi di DR. In caso di incidente, è possibile eseguire il failover delle macchine virtuali su questo cluster e aggiungere nodi.

3. Impostare il processo 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 AVS e ANF**

1. Assicurarsi che la VM di backup di Veeam Backup & Replication sia connessa all'origine e ai cluster SDDC AVS di destinazione.
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 Azure NetApp Files 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/durante la replica, Veeam Backup & Replication richiede a VMware vSphere la creazione di una snapshot delle VM. Lo snapshot della VM è la copia point-in-time di una VM che include dischi virtuali, stato del sistema, configurazione e metadati. 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. Fare clic con il pulsante destro del mouse sul nodo processi e selezionare processo di replica > macchina virtuale.
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 Azure ha limitato la larghezza di banda.
  - \*Selezionare la casella di controllo Network remapping (per i siti AVS SDDC con reti diverse) se i segmenti della soluzione Azure VMware SDDC non corrispondono a quelli delle reti dei siti in sede.
  - Se lo schema di indirizzamento IP nel sito di produzione locale differisce dallo schema nel sito AVS di destinazione, selezionare la casella di controllo Replica re-IP (per siti DR con schema di indirizzamento IP diverso).



4. Selezionare le VM da replicare nel datastore Azure NetApp Files collegato a un SDDC della soluzione Azure VMware 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 posizionato facilmente nel datastore Azure NetApp Files, in modo che sia possibile ripristinare le macchine virtuali e espandere il cluster per soddisfare i requisiti di CPU/mem. 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 cluster/host SDDC della soluzione Azure VMware e il pool di risorse, la cartella VM e il datastore FSX per le repliche delle 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 AVS SDDC di destinazione.



Per ulteriori informazioni sulla replica Veeam, fare riferimento ["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 chiamata **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. Fare clic con il pulsante destro del mouse sul nodo repliche e selezionare piani di failover > piano di failover > VMware vSphere.



2. Fornire quindi un nome e una descrizione del 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.



Assicurarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante il failover.

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 **\*Avvia**. 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 cluster/host SDDC di Azure VMware Solution (AVS) di destinazione.

□

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, consultare ["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 **Annulla 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 Azure NetApp Files consente a Veeam o a qualsiasi tool validato di terze parti di fornire una soluzione di DR a basso costo sfruttando i cluster leggeri pilota, anziché standar in un cluster grande solo per le repliche delle VM. Ciò fornisce un modo efficace per gestire un piano di disaster recovery personalizzato e su misura e riutilizzare i prodotti di backup esistenti in sede per il disaster recovery, consentendo il disaster recovery basato sul cloud in uscita dai data center di DR on-premise. È possibile eseguire il failover facendo clic su un pulsante in caso di emergenza o eseguendo il failover automatico in caso

di emergenza.

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

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278>

## Migrazione dei carichi di lavoro su Azure/AVS

### TR-4940: Migrazione dei carichi di lavoro al datastore Azure NetApp Files con VMware HCX - Guida rapida

Autore: NetApp Solutions Engineering

#### **Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore Azure NetApp Files e soluzione VMware Azure**

Uno dei casi di utilizzo più comuni per la soluzione VMware Azure e il datastore Azure NetApp Files è la migrazione dei carichi di lavoro VMware. VMware HCX è un'opzione preferita e offre vari meccanismi di migrazione per spostare macchine virtuali (VM) on-premise e i relativi dati negli archivi dati Azure NetApp Files.

VMware HCX è principalmente una piattaforma di migrazione progettata per semplificare la migrazione delle applicazioni, il ribilanciamento dei carichi di lavoro e persino la business continuity tra i cloud. È incluso come parte di Azure VMware Solution Private Cloud e offre diversi modi per migrare i workload e può essere utilizzato per le operazioni di disaster recovery (DR).

Questo documento fornisce istruzioni dettagliate per il provisioning del datastore Azure NetApp Files, seguito dal download, dall'implementazione e dalla configurazione di VMware HCX, inclusi tutti i componenti principali in sede e il lato soluzione VMware Azure, tra cui interconnessione, estensione di rete e ottimizzazione WAN per l'abilitazione di vari meccanismi di migrazione delle macchine virtuali.



VMware HCX funziona con qualsiasi tipo di datastore poiché la migrazione è a livello di VM. Pertanto, questo documento è valido per i clienti NetApp esistenti e non, che intendono implementare la soluzione Azure NetApp Files con Azure VMware per un'implementazione cloud VMware conveniente.

## Passaggi di alto livello

Questo elenco fornisce i passaggi di alto livello necessari per installare e configurare HCX Cloud Manager sul lato cloud di Azure e installare HCX Connector on-premise:

1. Installare HCX attraverso il portale Azure.
2. Scaricare e implementare IL programma di installazione DI HCX Connector Open Virtualization Appliance (OVA) nel server VMware vCenter on-premise.
3. Attivare HCX con la chiave di licenza.
4. Associare il connettore VMware HCX on-premise con Azure VMware Solution 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 evitare il re-IP durante le migrazioni.
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, consulta questa sezione ["collegamento"](#). Una volta soddisfatti i prerequisiti, inclusa la connettività, configurare e attivare HCX generando la chiave di licenza dal portale Azure VMware Solution. Una volta scaricato il programma di installazione di OVA, procedere con la procedura di installazione come descritto di seguito.

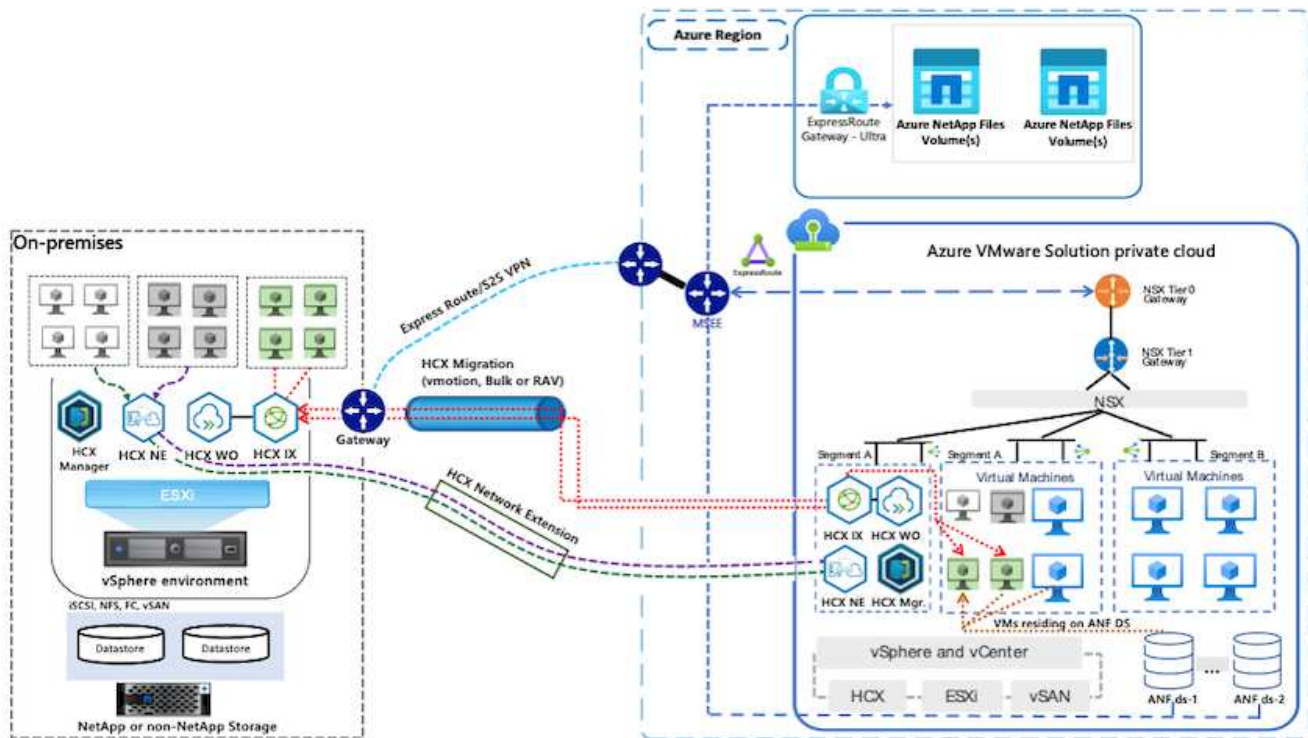


HCX Advanced è l'opzione predefinita e VMware HCX Enterprise Edition è disponibile anche attraverso un ticket di supporto e supportato senza costi aggiuntivi.

- Utilizza un data center software-defined (SDDC) esistente per la soluzione Azure VMware o crea un cloud privato utilizzando questo ["Link NetApp"](#) o questo ["Collegamento Microsoft"](#).
- La migrazione delle macchine virtuali e dei dati associati dal data center abilitato VMware vSphere on-premise richiede la connettività di rete dal data center all'ambiente SDDC. Prima di migrare i carichi di lavoro, ["Configurare una connessione VPN sito-sito o di accesso globale Express Route"](#) tra l'ambiente on-premise e il rispettivo cloud privato.
- Il percorso di rete dall'ambiente VMware vCenter Server on-premise al cloud privato Azure VMware Solution deve supportare la migrazione delle macchine virtuali utilizzando vMotion.
- 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. Nel cloud privato, il routing sulla rete vMotion è configurato per impostazione predefinita.
- Il volume NFS di Azure NetApp Files deve essere montato come datastore nella soluzione VMware di Azure. Seguire i passaggi descritti in questa sezione ["collegamento"](#) Per collegare datastore Azure NetApp Files agli host delle soluzioni VMware Azure.

## 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, che consente la connettività on-premise con Azure VMware Solution.



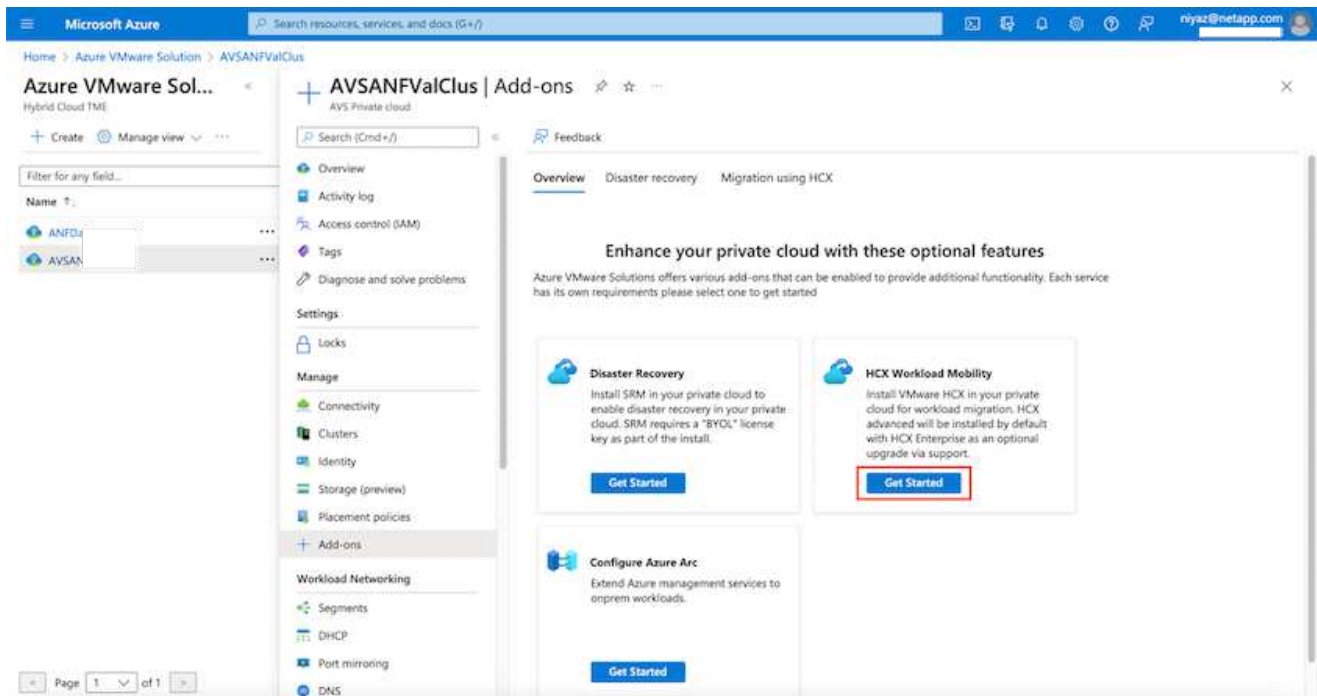
## Implementazione della soluzione

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

## Fase 1: Installare HCX attraverso Azure Portal utilizzando l'opzione Add-ons

Per eseguire l'installazione, attenersi alla seguente procedura:

1. Accedi al portale Azure e accedi al cloud privato Azure VMware Solution.
2. Selezionare il cloud privato appropriato e accedere ai componenti aggiuntivi. Per eseguire questa operazione, accedere a **Gestisci > componenti aggiuntivi**.
3. Nella sezione HCX workload Mobility, fare clic su **Get Started** (inizia subito).



1. Selezionare l'opzione **Accetto i termini e le condizioni** e fare clic su **attiva e implementa**.



L'implementazione predefinita è HCX Advanced. Aprire una richiesta di supporto per attivare l'edizione Enterprise.



L'implementazione richiede da 25 a 30 minuti circa.

Microsoft Azure

Search resources, services, and docs (G+/f)

Home > Azure VMware Solution > AVSANFValClus

### Azure VMware Sol...

Hybrid Cloud TME

+ Create Manage view ...

Filter for any field...

Name ↑

- ANFD
- AVSA

AVSANFValClus | Add-ons

Search (Ctrl+F)

Feedback

Overview Disaster recovery **Migration using HCX**

HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. [Learn more.](#)

☒ I agree with terms and conditions.  
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.

HCX plan ⓘ HCX Advanced

**Enable and deploy**

Settings

- Locks

Manage

- Connectivity
- Clusters
- Identity
- Storage (preview)
- Placement policies

+ Add-ons

Workload Networking

- Segments
- DHCP
- Port mirroring
- DNS

Page 1 of 1



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

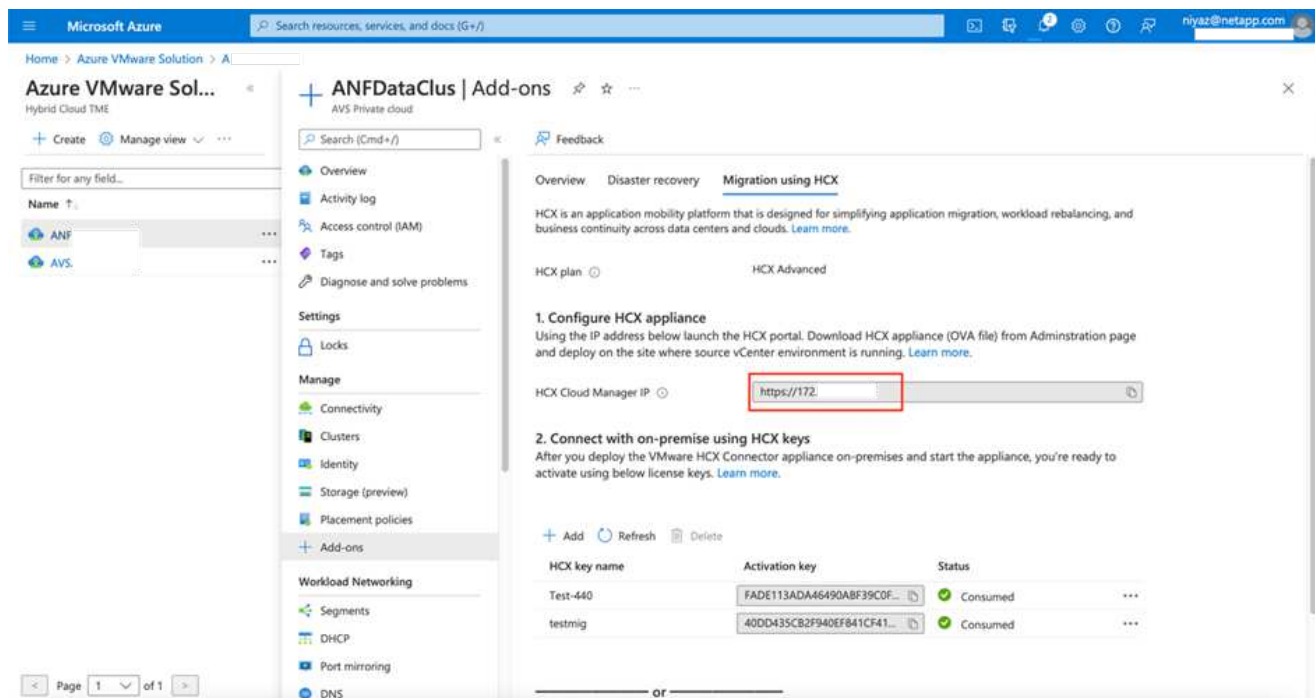
Affinché il connettore on-premise si connetta a HCX Manager in Azure VMware Solution, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente on-premise.

Per scaricare e installare HCX Connector nel server vCenter on-premise, attenersi alla seguente procedura:

1. Dal portale Azure, accedere alla soluzione VMware Azure, selezionare il cloud privato, quindi selezionare **Gestisci > componenti aggiuntivi > migrazione** utilizzando HCX e copiare IL portale HCX Cloud Manager per scaricare il file OVA.



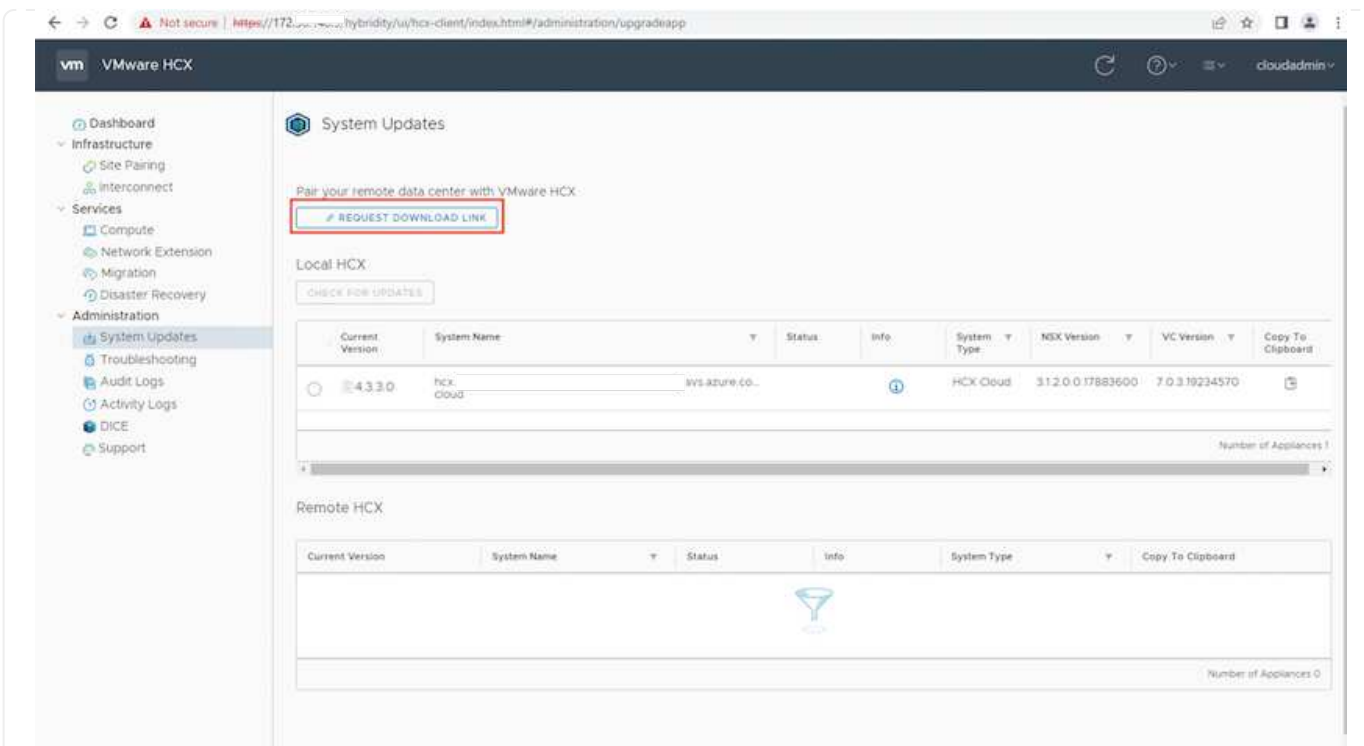
Utilizzare le credenziali utente predefinite di CloudAdmin per accedere al portale HCX.



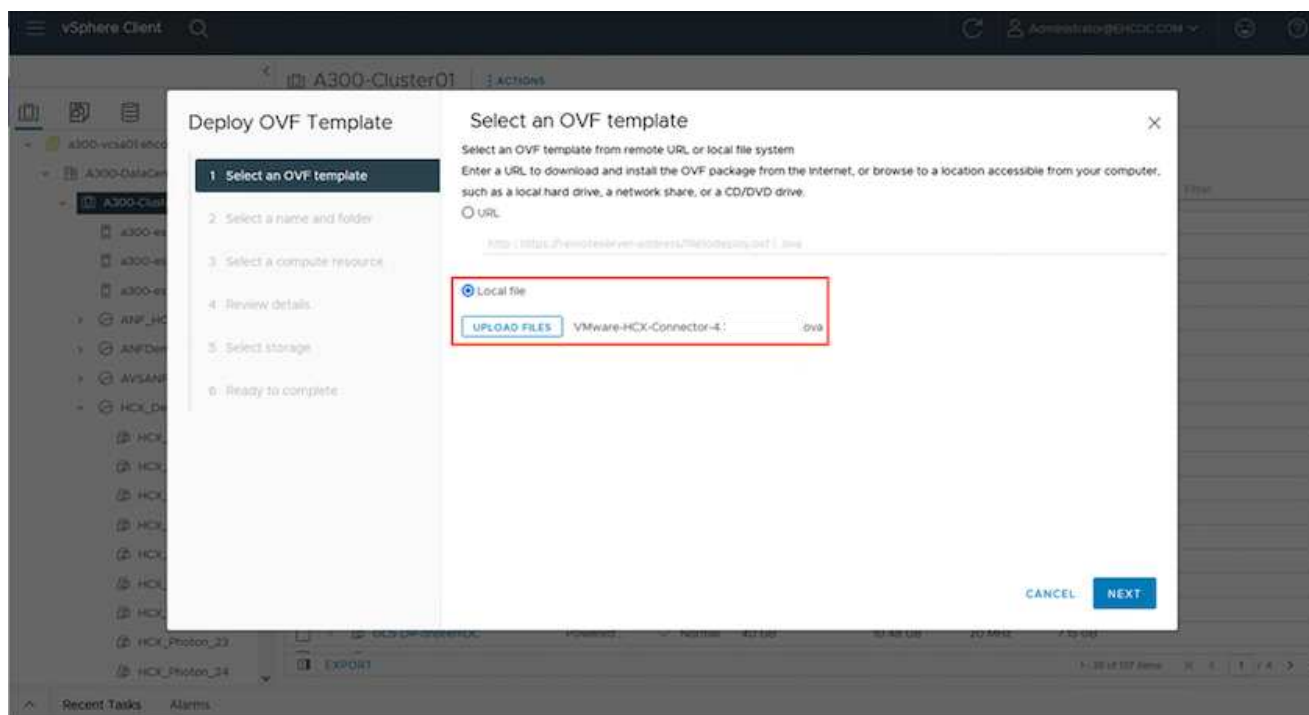
1. Dopo aver effettuato l'accesso al portale HCX con [cloudadmin@vsphere.local](mailto:cloudadmin@vsphere.local) utilizzando il jumphost, accedere a **Administration > System Updates** e fare clic su **Request Download link**.



Scaricare o copiare il collegamento a OVA e incollarlo in un browser per avviare il processo di download del file OVA di VMware HCX Connector da implementare sul server vCenter on-premise.



1. Una volta scaricato l'OVA, implementarlo nell'ambiente VMware vSphere on-premise utilizzando l'opzione **Deploy OVF Template**.



1. Inserire tutte le informazioni richieste per l'implementazione di OVA, fare clic su **Avanti**, quindi fare clic su **fine** per implementare l'OVA di VMware HCX Connector.



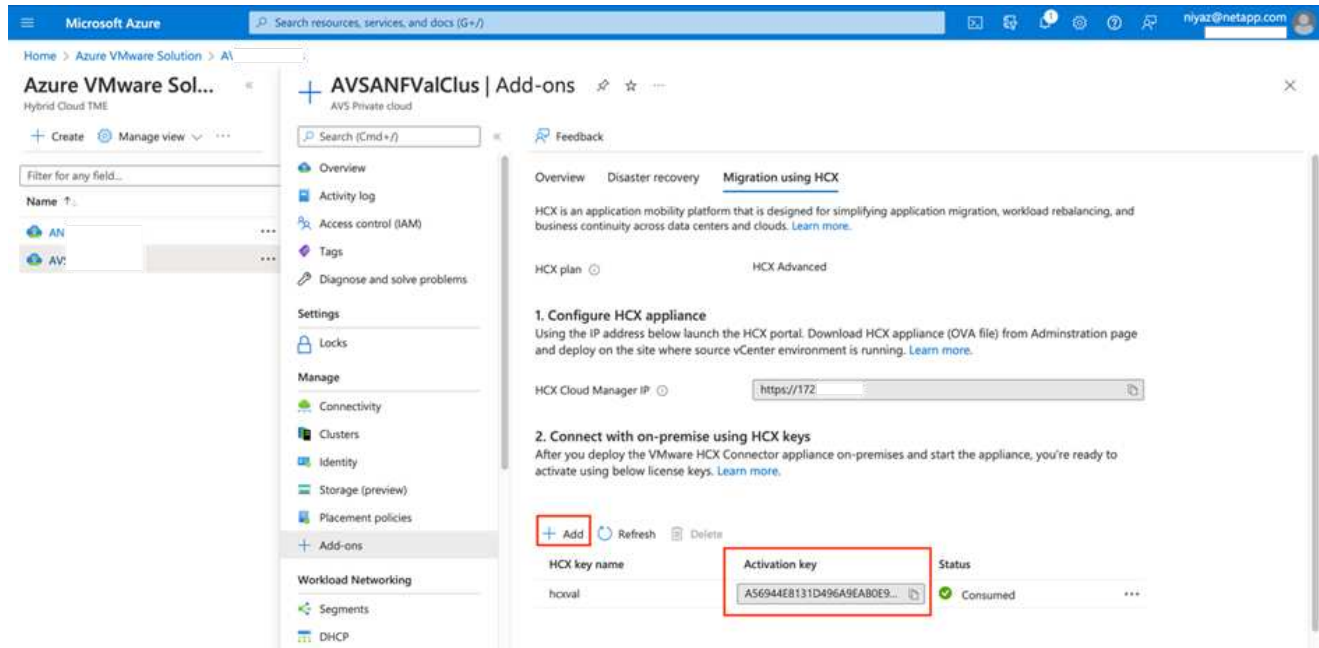
Accendere l'appliance virtuale manualmente.

Per istruzioni dettagliate, consultare ["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 dal portale Azure VMware Solution e attivarla in VMware HCX Manager.

1. Dal portale Azure, accedere alla soluzione VMware Azure, selezionare il cloud privato e selezionare **Gestisci > componenti aggiuntivi > migrazione con HCX**.
2. In **Connect with on-premise using HCX keys** (connessione con chiavi HCX on-premise), fare clic su **Add** (Aggiungi) e copiare la chiave di attivazione.



Per ciascun connettore HCX on-premise implementato è necessaria una chiave separata.

1. Accedere a VMware HCX Manager on-premise all'indirizzo "<https://hcxmanagerIP:9443>" utilizzando le credenziali di amministratore.



Utilizzare la password definita durante l'implementazione di OVA.

1. Nella licenza, inserire la chiave copiata dal passaggio 3 e fare clic su **Activate** (attiva).



Il connettore HCX on-premise deve disporre di accesso a Internet.

1. In **posizione del data center**, fornire la posizione più vicina per l'installazione di VMware HCX Manager on-premise. Fare clic su **continua**.
2. In **Nome sistema**, aggiornare il nome e fare clic su **continua**.
3. Fare clic su **Sì, continua**.
4. In **Connect your vCenter**, fornire il nome di dominio completo (FQDN) o l'indirizzo IP di vCenter Server e le credenziali appropriate, quindi fare clic su **Continue** (continua).



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

1. In **Configure SSO/PSC** (Configura SSO/PSC\*), fornire l'indirizzo FQDN o IP del Platform Services Controller e fare clic su **Continue** (continua).

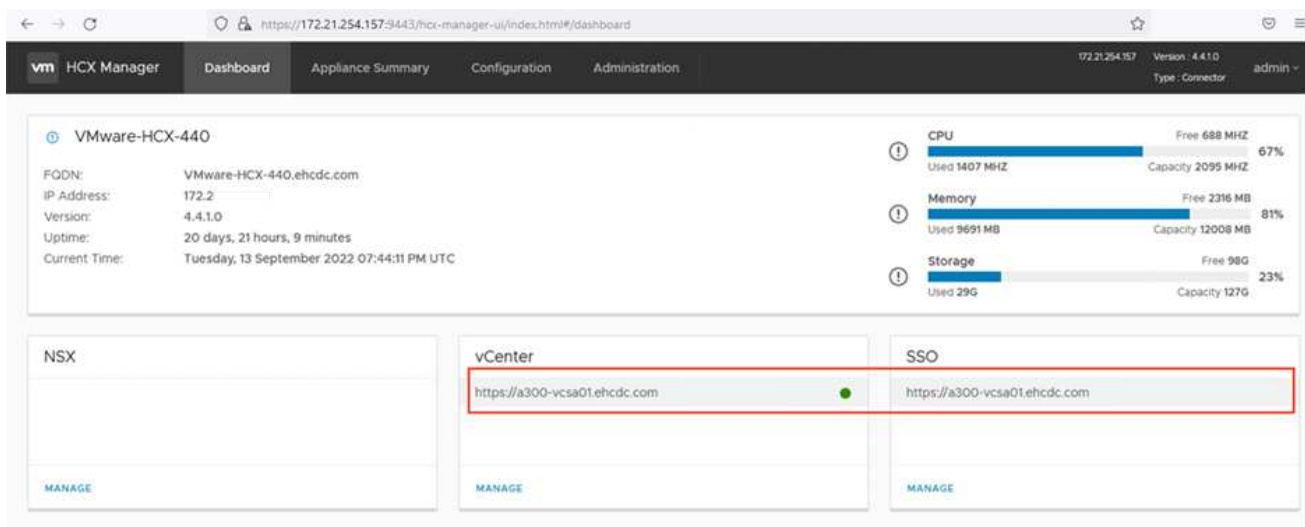


Immettere l'indirizzo IP o il nome FQDN di VMware vCenter Server.

1. Verificare che le informazioni immesse siano corrette e fare clic su **Restart** (Riavvia).
2. Dopo il riavvio dei servizi, vCenter Server viene visualizzato in verde nella pagina visualizzata. VCenter Server e SSO devono disporre dei parametri di configurazione appropriati, che devono essere gli stessi della pagina precedente.



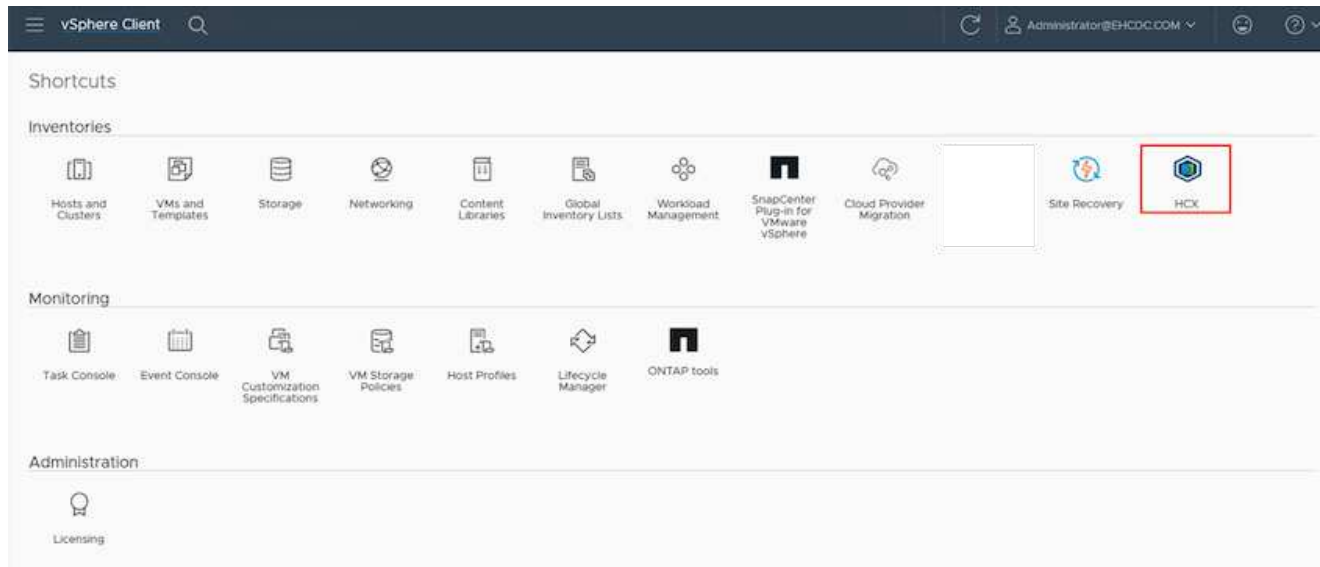
Questo processo richiede circa 10 - 20 minuti e l'aggiunta del plug-in al server vCenter.



## Fase 4: Associazione on-premise di VMware HCX Connector con Azure VMware Solution HCX Cloud Manager

Dopo aver installato HCX Connector sia in sede che in Azure VMware Solution, configurare VMware HCX Connector on-premise per Azure VMware Solution Private Cloud aggiungendo l'accoppiamento. Per configurare l'associazione del sito, attenersi alla seguente procedura:

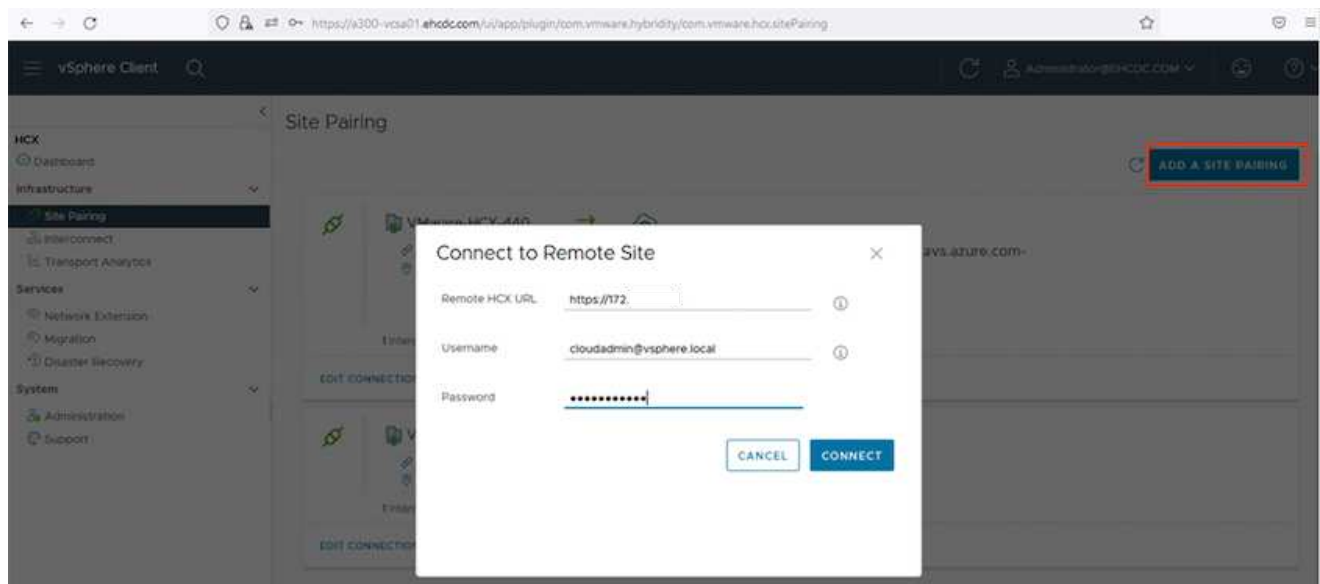
1. Per creare una coppia di siti tra l'ambiente vCenter on-premise e Azure VMware Solution SDDC, accedere a vCenter Server on-premise e al nuovo plug-in HCX vSphere Web Client.



1. In Infrastructure (infrastruttura), fare clic su **Add a Site Pairing** (Aggiungi associazione sito).



Immettere l'URL o l'indirizzo IP di Azure VMware Solution HCX Cloud Manager e le credenziali per il ruolo CloudAdmin per l'accesso al cloud privato.

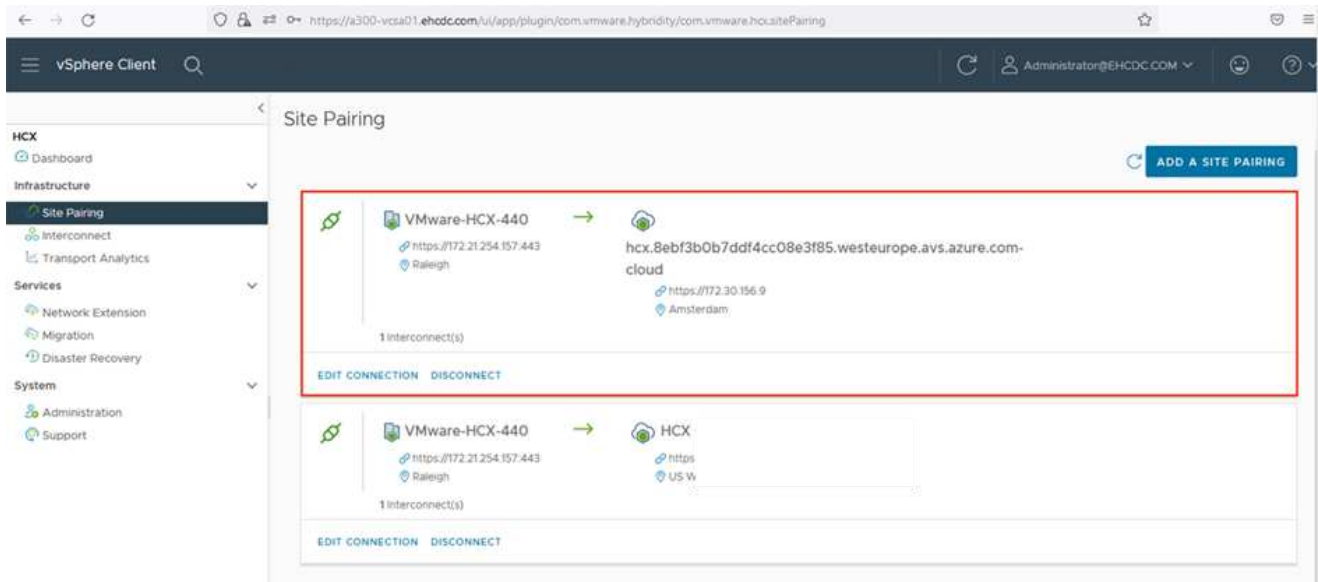


1. Fare clic su **Connect** (Connetti).



Il connettore VMware HCX deve essere in grado di instradare all'indirizzo IP DI HCX Cloud Manager tramite la porta 443.

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



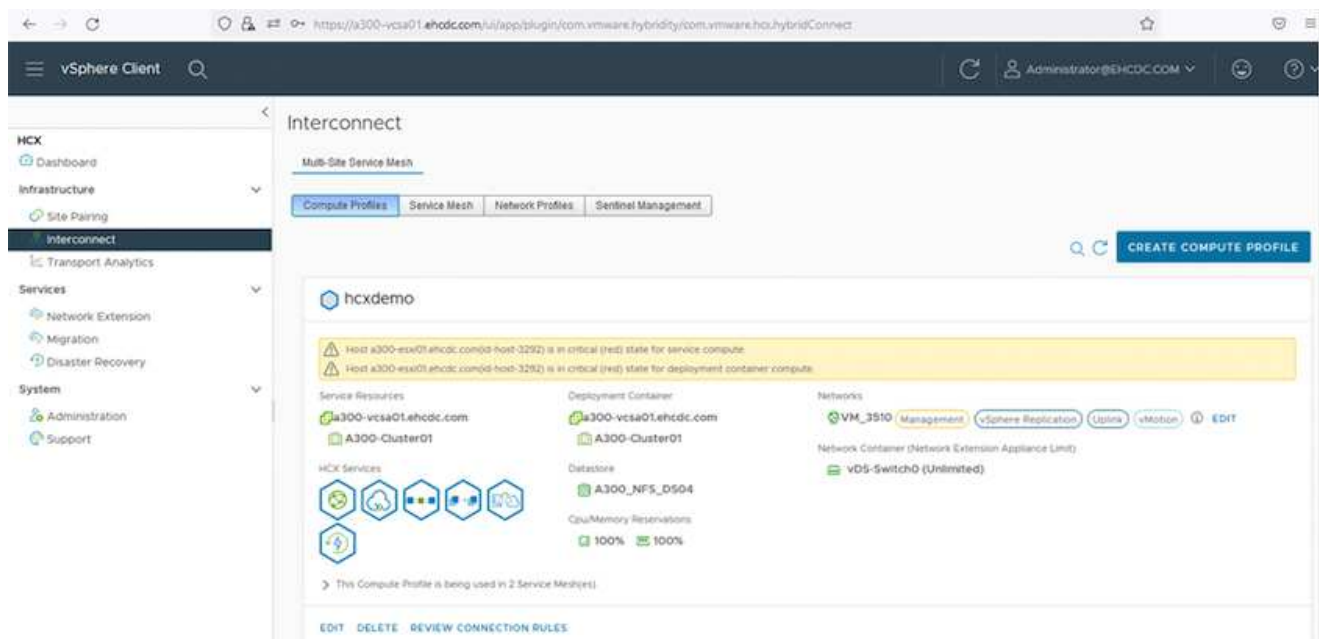
## Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

L'appliance di servizio VMware HCX Interconnect offre funzionalità di replica e migrazione basata su vMotion su Internet e connessioni private al sito di destinazione. L'interconnessione offre crittografia, progettazione del traffico e mobilità delle macchine virtuali. Per creare un'appliance di servizio Interconnect, attenersi alla seguente procedura:

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



I profili di calcolo definiscono i parametri di implementazione, incluse le appliance implementate e la parte del data center VMware accessibile al servizio HCX.



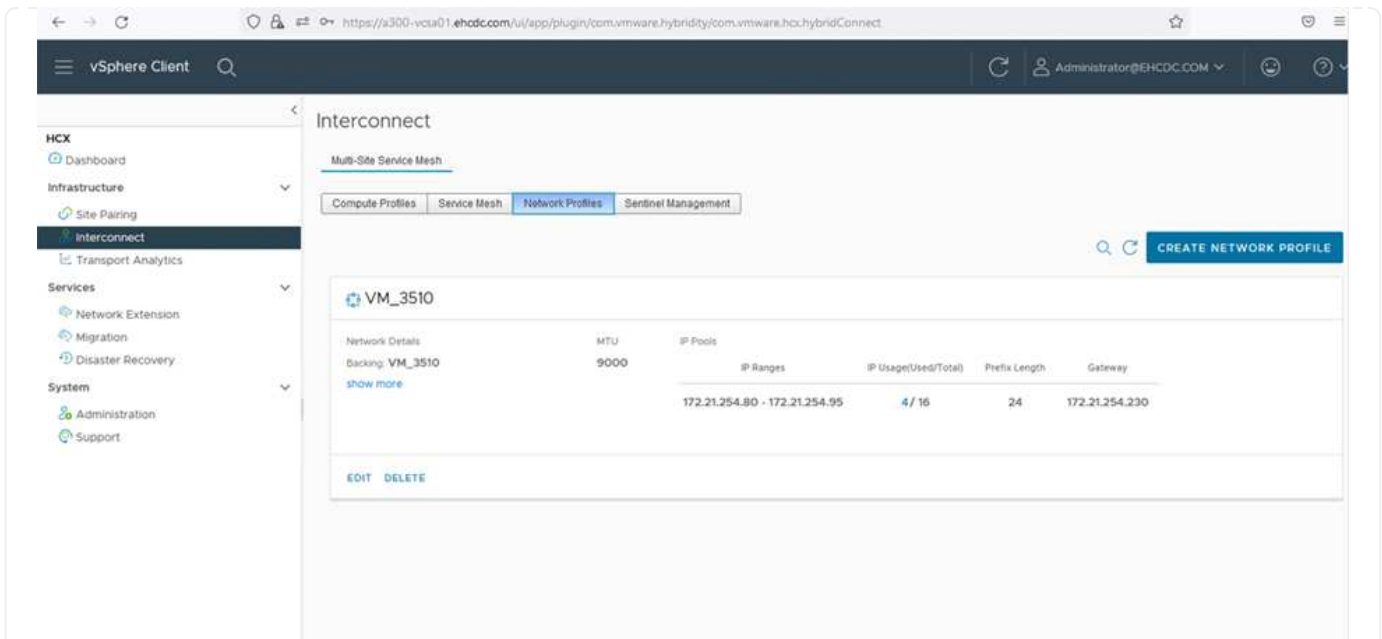
1. Una volta creato il profilo di calcolo, creare i profili di rete selezionando **Multi-Site Service Mesh > Network Profiles > Create Network Profile** (Mesh servizio multi-sito > profili di rete > Crea profilo di rete).

Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati DA HCX per le proprie appliance virtuali.



Questa operazione richiede due o più indirizzi IP. Questi indirizzi IP vengono assegnati dalla rete di gestione alle appliance di interconnessione.

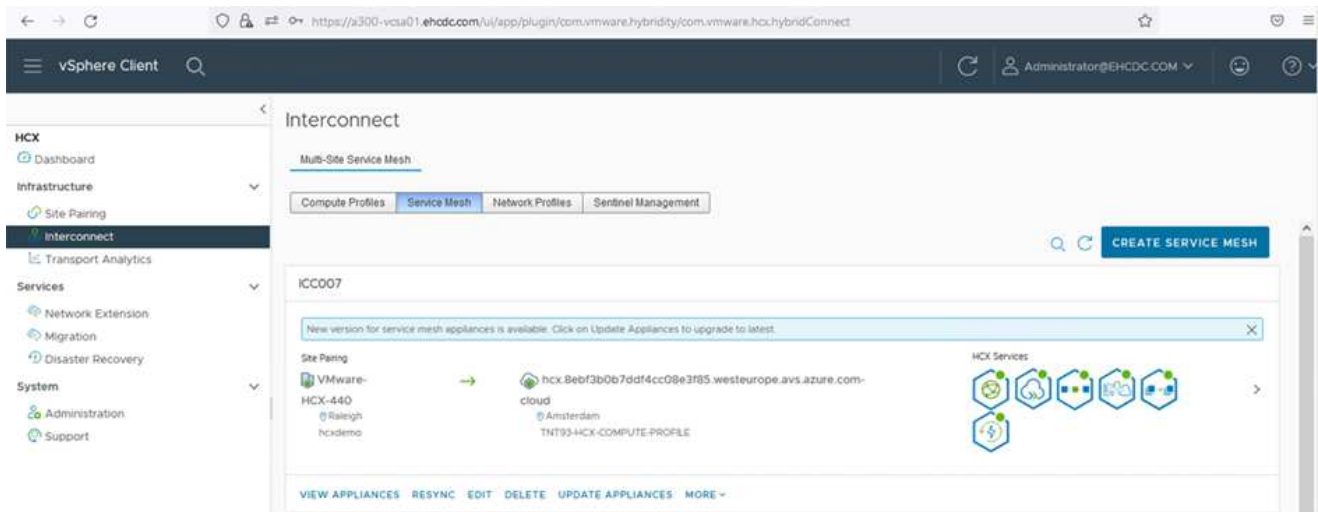




1. A questo punto, i profili di calcolo e di rete sono stati creati correttamente.
2. Creare la mesh del servizio selezionando la scheda **Mesh del servizio** all'interno dell'opzione **Interconnect** e selezionando i siti SDDC on-premise e Azure.
3. Service Mesh specifica una coppia di profili di rete e di calcolo locale e remoto.



Nell'ambito di questo processo, le appliance HCX vengono implementate e configurate automaticamente sui siti di origine e di destinazione per creare un fabric di trasporto sicuro.



1. Questa è la fase finale della configurazione. Il completamento dell'implementazione richiede circa 30 minuti. Una volta configurata la mesh del servizio, l'ambiente è pronto con i tunnel IPsec creati correttamente per migrare le macchine virtuali del carico di lavoro.



## Fase 6: Migrazione dei carichi di lavoro

I carichi di lavoro possono essere migrati bidirezionalmente tra gli SDDC on-premise e Azure utilizzando varie tecnologie di migrazione VMware HCX. Le VM possono essere spostate da e verso le entità attivate da VMware HCX utilizzando diverse 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).

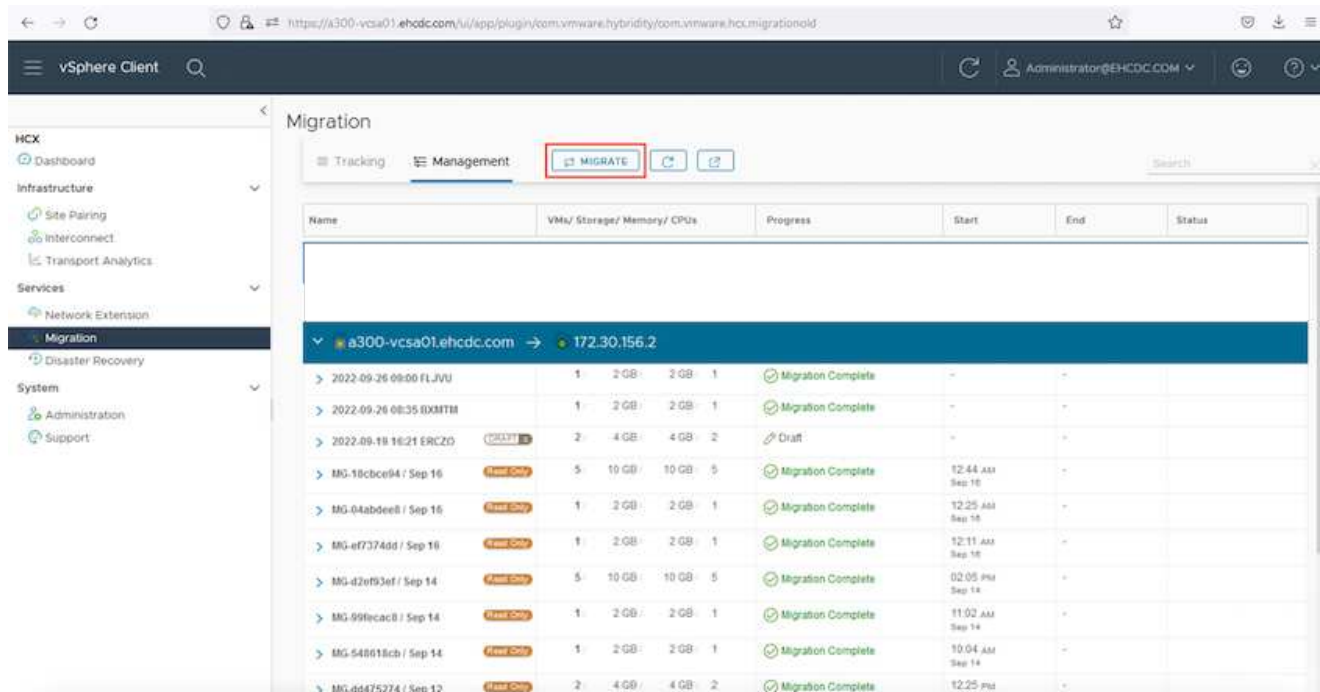
Per ulteriori informazioni sui vari meccanismi di migrazione HCX, vedere ["Tipi di migrazione VMware HCX"](#).

### Migrazione in massa

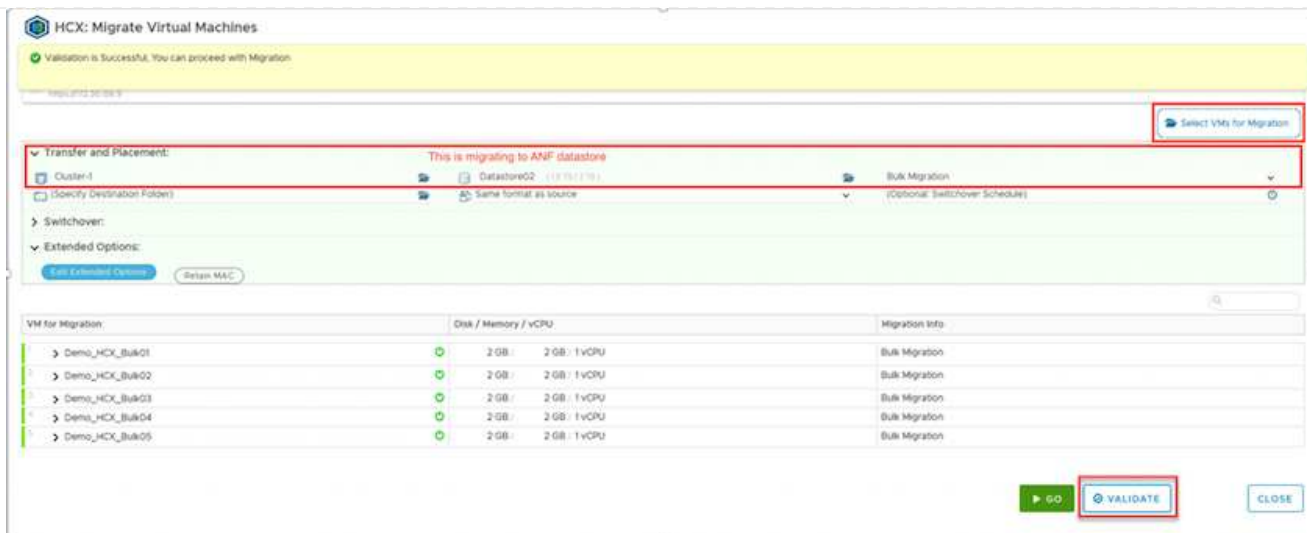
In questa sezione viene descritto in dettaglio il meccanismo di migrazione in blocco. Durante una migrazione in blocco, LA funzionalità di migrazione in blocco di HCX utilizza vSphere Replication per migrare i file disco ricreando la macchina virtuale sull'istanza di destinazione di vSphere HCX.

Per avviare migrazioni di macchine virtuali in blocco, attenersi alla seguente procedura:

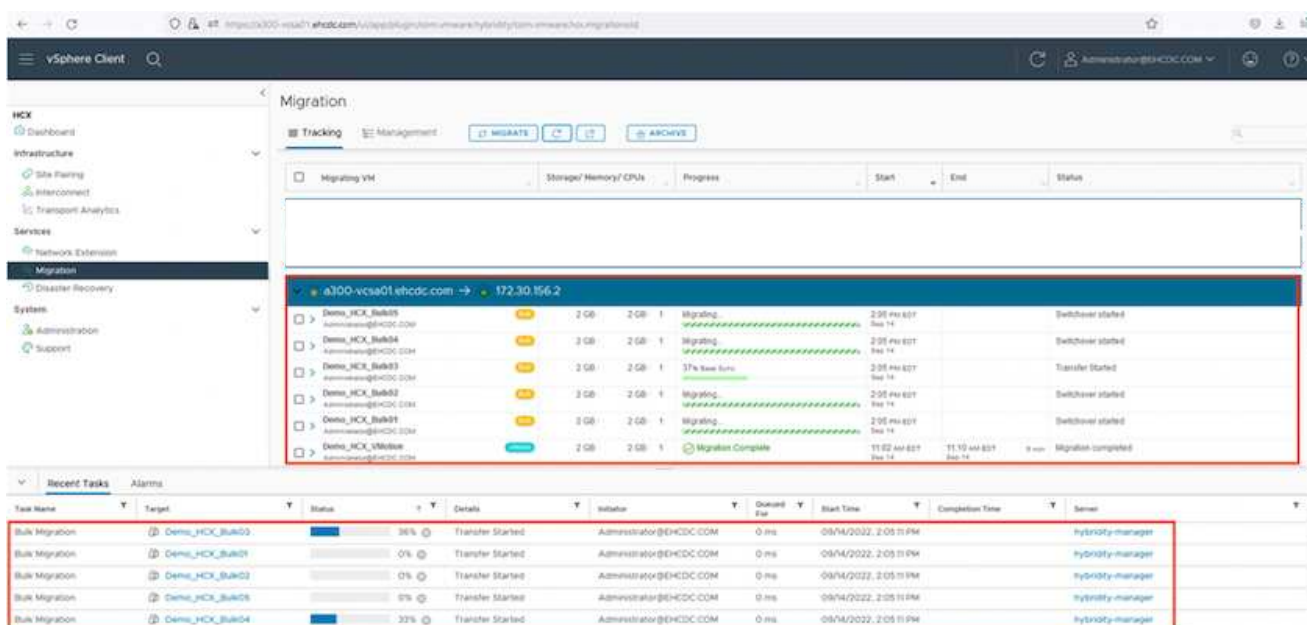
1. Accedere alla scheda **Migrate** in **servizi > migrazione**.



1. Nella sezione **connessione sito remoto**, selezionare la connessione del sito remoto e selezionare l'origine e la destinazione. In questo esempio, la destinazione è Azure VMware Solution SDDC HCX endpoint.
2. Fare clic su **Select VM for Migration** (Seleziona VM per la migrazione). Questo fornisce un elenco di tutte le macchine virtuali on-premise. Selezionare le macchine virtuali in base all'espressione match:value e fare clic su **Add** (Aggiungi).
3. Nella sezione **Transfer and Placement** (trasferimento e posizionamento), aggiornare i campi obbligatori (**Cluster**, **Storage**, **Destination** e **Network**), incluso il profilo di migrazione, quindi fare clic su **Validate** (convalida).

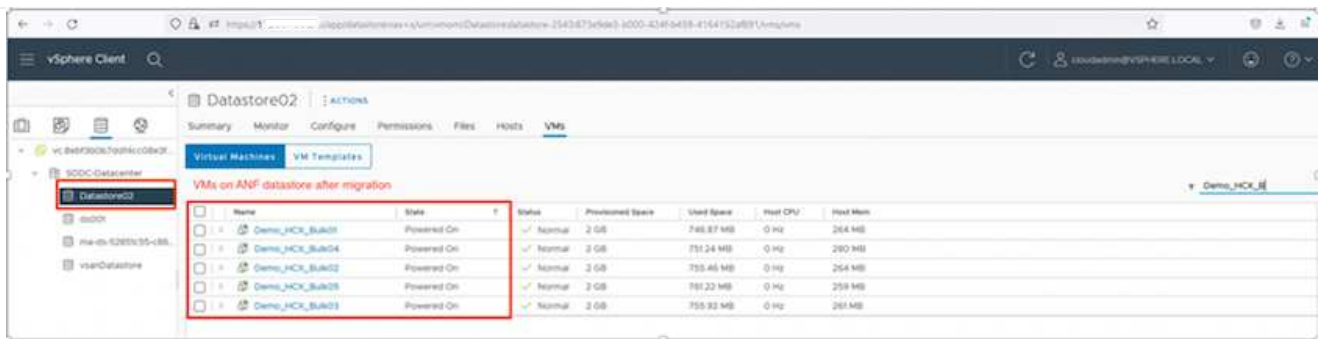


1. Al termine dei controlli di convalida, fare clic su **Go** per avviare la migrazione.



Durante questa migrazione, viene creato un disco segnaposto nel datastore Azure NetApp Files specificato all'interno del vCenter di destinazione per consentire la replica dei dati del disco VM di origine nei dischi segnaposto. L'HBR viene attivato per una sincronizzazione completa con la destinazione e, una volta completata la linea di base, viene eseguita una sincronizzazione incrementale in base al ciclo RPO (Recovery Point Objective). Una volta completata la sincronizzazione completa/incrementale, lo switchover viene attivato automaticamente, a meno che non venga impostata una pianificazione specifica.

1. Una volta completata la migrazione, validare la stessa accedendo al vCenter SDDC di destinazione.

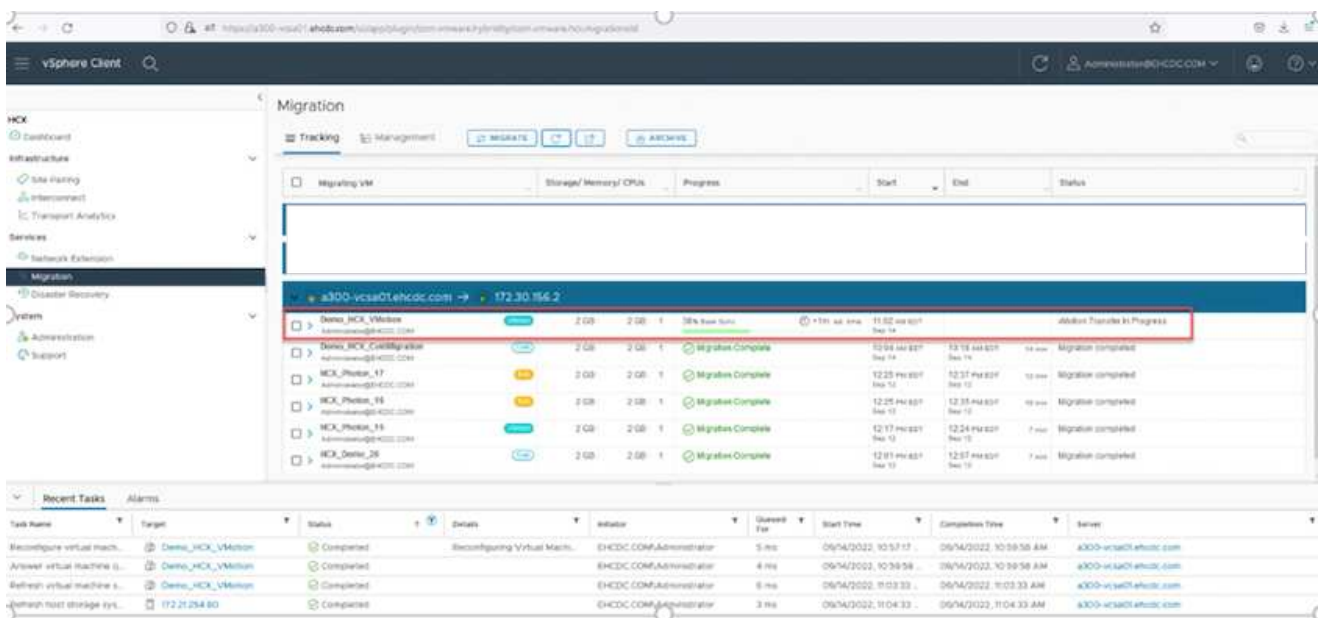


Per ulteriori e dettagliate informazioni sulle varie opzioni di migrazione e su come migrare i carichi di lavoro da una soluzione VMware on-premise a Azure utilizzando HCX, vedere ["Guida utente di VMware HCX"](#).

Per ulteriori informazioni su questo processo, guarda il seguente video:

[Migrazione dei carichi di lavoro con HCX](#)

Ecco una schermata dell'opzione HCX vMotion.



Per ulteriori informazioni su questo processo, guarda il seguente video:

[HCX vMotion](#)



Assicurarsi che sia disponibile una larghezza di banda sufficiente per gestire la migrazione.



Il datastore ANF di destinazione deve disporre di spazio sufficiente per gestire la migrazione.

## Conclusione

Sia che tu stia prendendo come riferimento il cloud all-cloud o ibrido e i dati che risiedono su storage di

qualsiasi tipo/vendor in on-premise, Azure NetApp Files e HCX offrono eccellenti opzioni per implementare e migrare i carichi di lavoro delle applicazioni, riducendo al contempo il TCO rendendo i requisiti dei dati perfetti a livello applicativo. Qualunque sia il caso d'utilizzo, scegli la soluzione VMware Azure insieme a Azure NetApp Files per una rapida realizzazione dei vantaggi 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 VMware vSphere Replication, VMware vMotion o persino la copia del file di rete (NFC).

## Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Azure NetApp Files come datastore su Azure VMware Solution SDDC.
- È possibile migrare facilmente i dati da un datastore on-premise a un datastore Azure NetApp Files.
- È possibile espandere e ridurre facilmente il datastore Azure NetApp Files 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 della soluzione VMware Azure

["https://docs.microsoft.com/en-us/azure/azure-vmware/"](https://docs.microsoft.com/en-us/azure/azure-vmware/)

- Documentazione Azure NetApp Files

["https://docs.microsoft.com/en-us/azure/azure-netapp-files/"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/)

- Guida utente di VMware HCX

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

La disponibilità di datastore NFS supplementari su Azure / AVS è definita da Microsoft. Innanzitutto, è necessario determinare se AVS e ANF sono disponibili in una regione specifica. Quindi, è necessario determinare se il datastore NFS supplementare ANF è supportato in quella regione.

- Verificare la disponibilità di AVS e ANF ["qui"](#).
- Verificare la disponibilità del datastore NFS supplementare ANF ["qui"](#).

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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