Disaster Recovery con CVO e AVS (archiviazione connessa agli ospiti)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

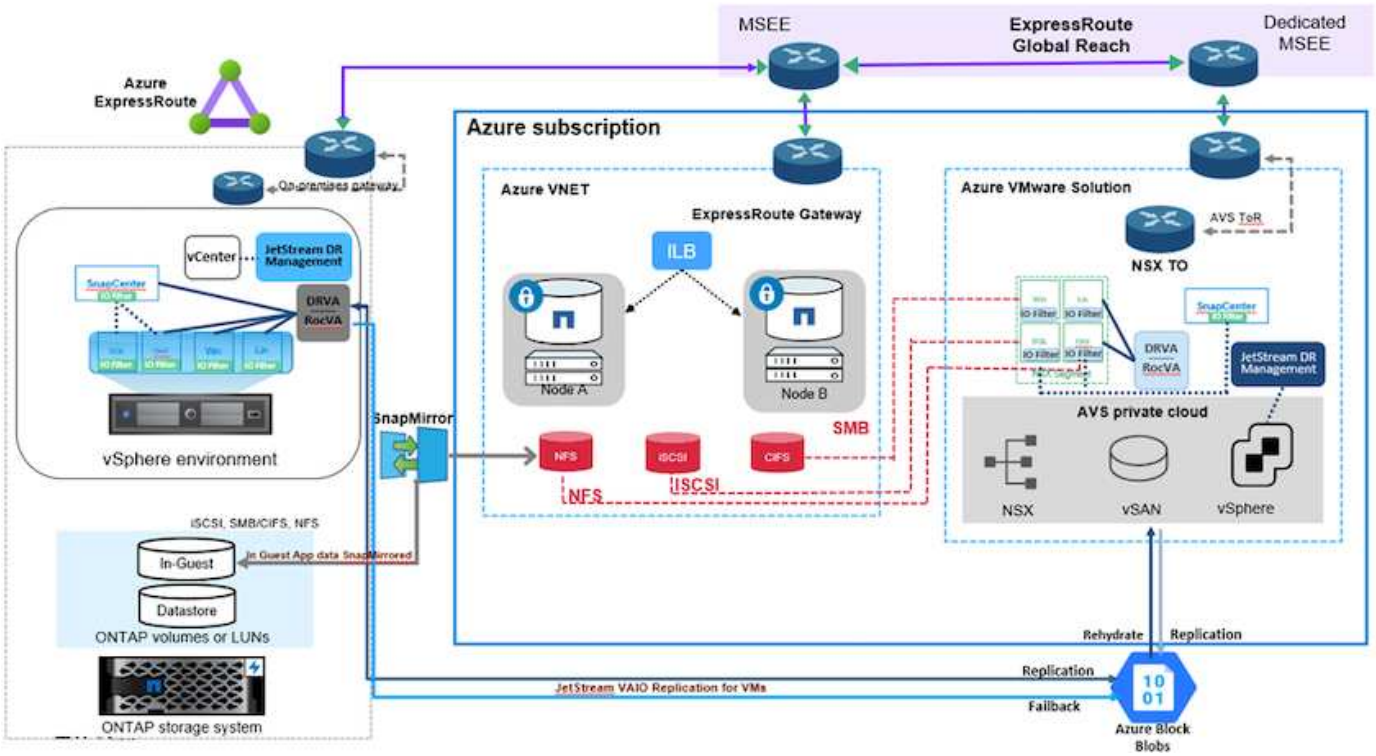
Sommario

Disaster Recovery con CVO e AVS (archiviazione connessa agli ospiti)

Il disaster recovery sul cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati come il ransomware. Con NetApp SnapMirror, i carichi di lavoro VMware locali che utilizzano storage connesso agli ospiti possono essere replicati su NetApp Cloud Volumes ONTAP in esecuzione in Azure.

Panoramica

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
Questo documento fornisce un approccio dettagliato per la configurazione e
l'esecuzione del disaster recovery utilizzando NetApp SnapMirror,
JetStream e Azure VMware Solution (AVS).
```



Ipotesi

Questo documento si concentra sull'archiviazione in-guest per i dati delle applicazioni (nota anche come guest connected) e presuppone che l'ambiente locale utilizzi SnapCenter per backup coerenti con le applicazioni.

> Il presente documento si applica 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 aziendali.

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

> Esistono diverse opzioni per connettere i data center locali ad Azure, il che ci impedisce di descrivere un flusso di lavoro specifico in questo documento. Per il metodo di connettività locale-Azure appropriato, fare riferimento alla documentazione di Azure.

Distribuzione della soluzione DR

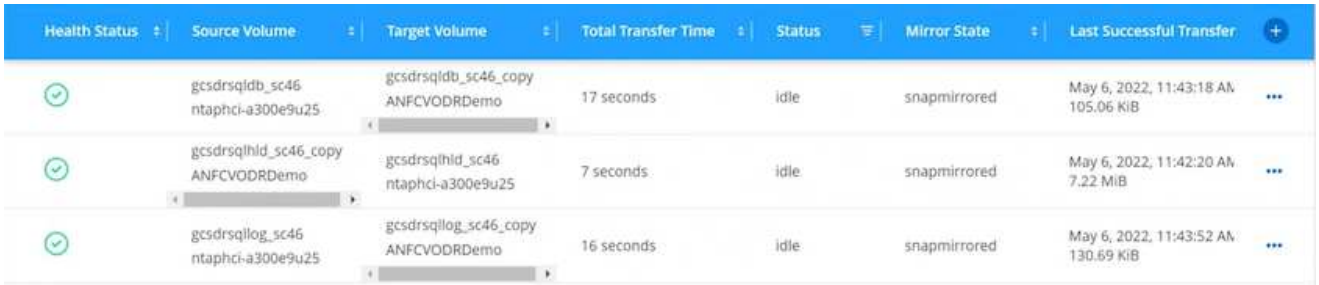
Panoramica sulla distribuzione della soluzione

1. Assicurarsi che i dati dell'applicazione vengano sottoposti a backup tramite SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning Cloud Volumes ONTAP con la dimensione corretta dell'istanza utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
    a. Configurare SnapMirror per i volumi applicativi pertinenti.
    b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti SnapMirror dopo i processi pianificati.
3. Installare il software JetStream DR nel data center locale e avviare la protezione per le macchine virtuali.
4. Installare il software JetStream DR nel cloud privato Azure VMware Solution.
5. Durante un evento di emergenza, interrompere la relazione SnapMirror tramite Cloud Manager e attivare il failover delle macchine virtuali su Azure NetApp Files o sui datastore vSAN nel sito AVS DR designato.
    a. Ricollegare i LUN ISCSI e i mount NFS per le VM dell'applicazione.
6. Richiamare il failback sul sito protetto tramite la risincronizzazione inversa SnapMirror dopo il ripristino del sito primario.

Dettagli di distribuzione

Configurare CVO su Azure e replicare i volumi su CVO

Il primo passaggio consiste nel configurare Cloud Volumes ONTAP su Azure ("Collegamento") e replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze e le conservazioni degli snapshot desiderate.



Configurare gli host AVS e l'accesso ai dati CVO

Due fattori importanti da considerare quando si distribuisce l'SDDC sono le dimensioni del cluster SDDC nella soluzione Azure VMware e per quanto tempo mantenere in servizio l'SDDC. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. L'SDDC può essere composto da un minimo di tre host, fino a diventare un cluster multi-host in una distribuzione su larga scala.

La decisione di implementare un cluster AVS si basa principalmente sui requisiti RPO/RTO. Grazie alla soluzione Azure VMware, l'SDDC può essere predisposto just in time in preparazione per i test o per un evento di emergenza effettivo. Un SDDC distribuito just-in-time consente di risparmiare sui costi di hosting ESXi quando non si è alle prese con un disastro. Tuttavia, questa forma di distribuzione influisce sull'RTO di alcune ore durante il provisioning di SDDC.

L'opzione più comunemente implementata è quella di far funzionare l'SDDC in modalità di funzionamento sempre acceso, con spia luminosa. Questa opzione occupa poco spazio, con tre host sempre disponibili, e velocizza le operazioni di ripristino, fornendo una baseline funzionante per le attività di simulazione e i controlli di conformità, evitando così il rischio di discrepanze operative tra i siti di produzione e di ripristino di emergenza. Il gruppo di spie luminose può essere rapidamente ampliato fino al livello desiderato quando necessario per gestire un evento DR effettivo.

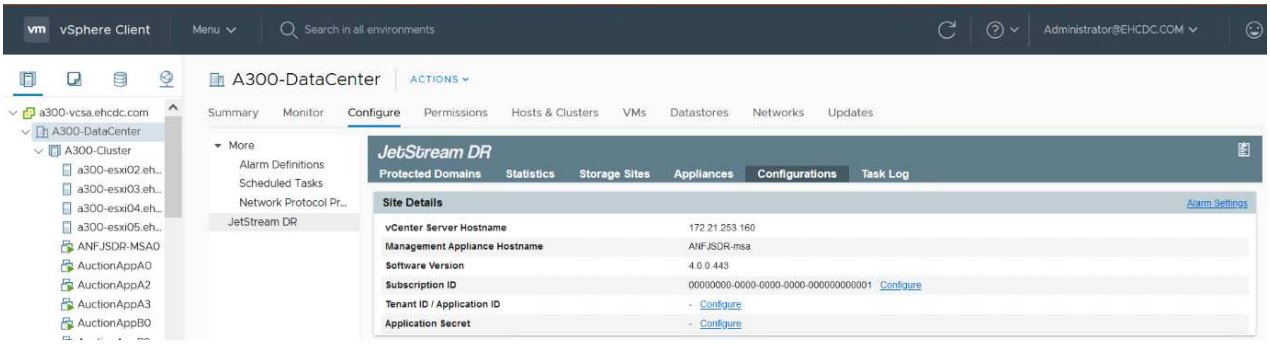
Per configurare AVS SDDC (sia su richiesta che in modalità pilota), vedere"Distribuire e configurare l'ambiente di virtualizzazione su Azure" . Come prerequisito, verificare che le VM guest residenti sugli host AVS siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e AVS, iniziare a configurare Jetstream per automatizzare il ripristino dei carichi di lavoro locali su AVS (VM con VMDK applicativi e VM con storage interno) utilizzando il meccanismo VAIO e sfruttando SnapMirror per le copie dei volumi applicativi su Cloud Volumes ONTAP.

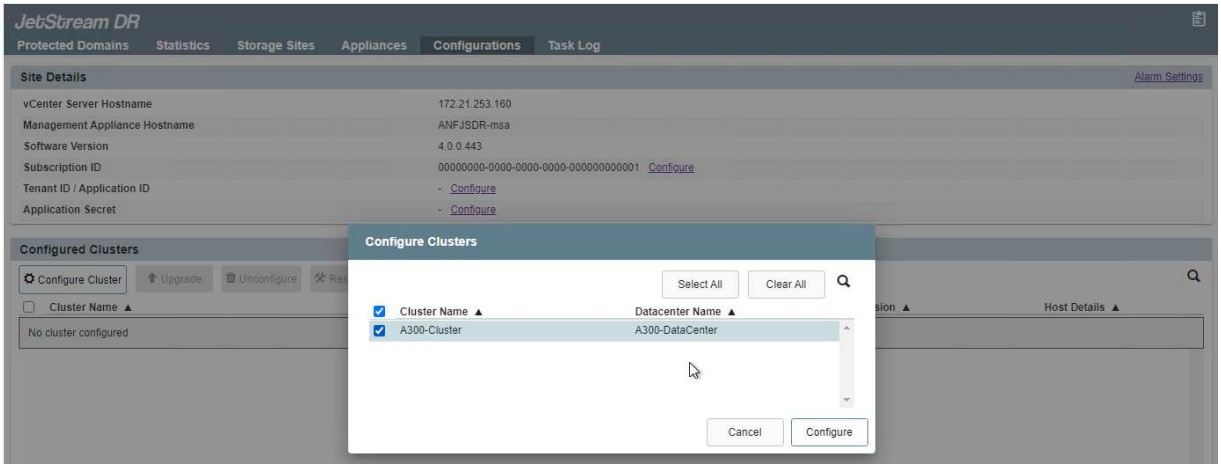
Installa JetStream DR nel data center locale

Il software JetStream DR è costituito da tre componenti principali: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) e componenti host (pacchetti di filtri I/O). L'MSA viene utilizzato per installare e configurare i componenti host sul cluster di elaborazione e quindi per amministrare il software JetStream DR. Il processo di installazione è il seguente:

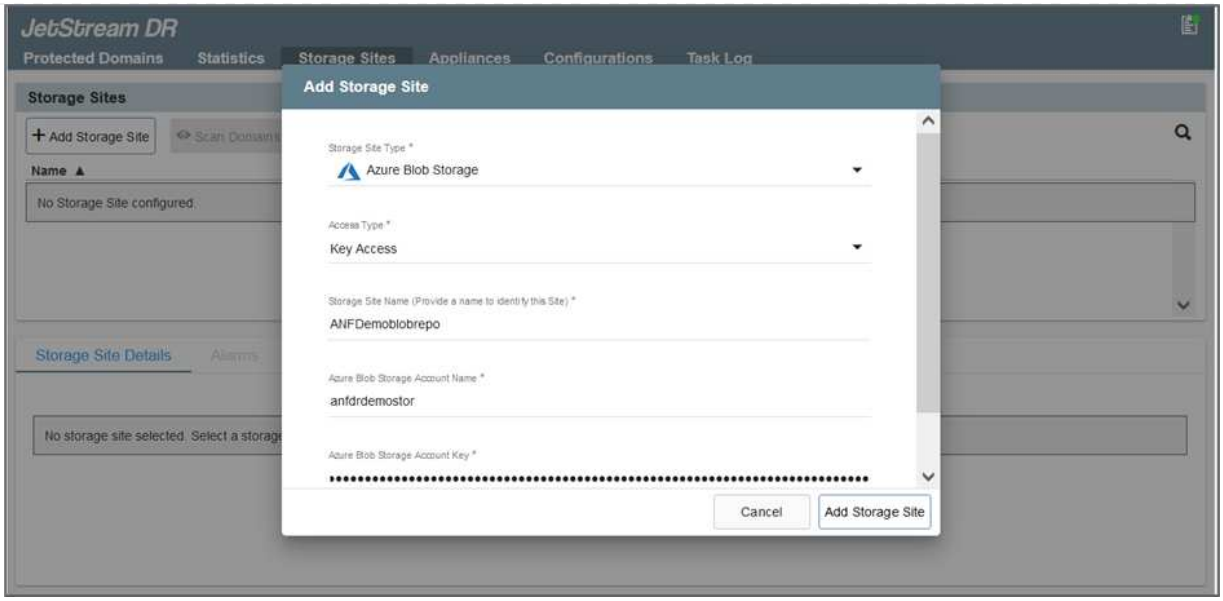
1. Verificare i prerequisiti.
2. Eseguire lo strumento di pianificazione della capacità per ottenere consigli su risorse e configurazioni.
3. Distribuire JetStream DR MSA su ciascun host vSphere nel cluster designato.
4. Avviare l'MSA utilizzando il suo nome DNS in un browser.
5. Registrare il server vCenter con MSA.
6. Dopo aver distribuito JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR con vSphere Web Client. Per farlo, andare su Datacenter > Configura > JetStream DR.



7. Dall'interfaccia JetStream DR, completare le seguenti attività:
   a. Configurare il cluster con il pacchetto filtro I/O.

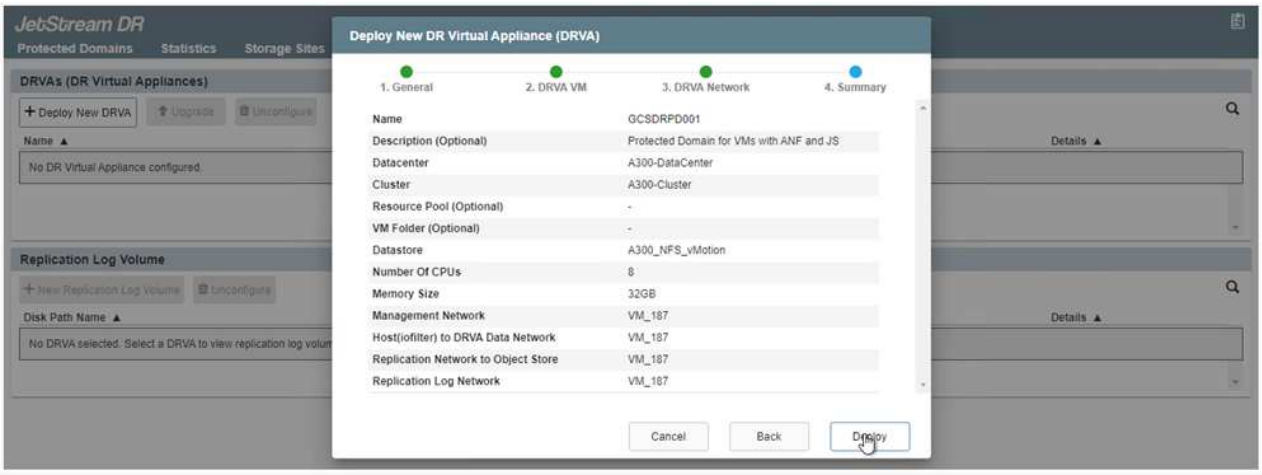


   b. Aggiungere l'archiviazione BLOB di Azure situata nel sito di ripristino.

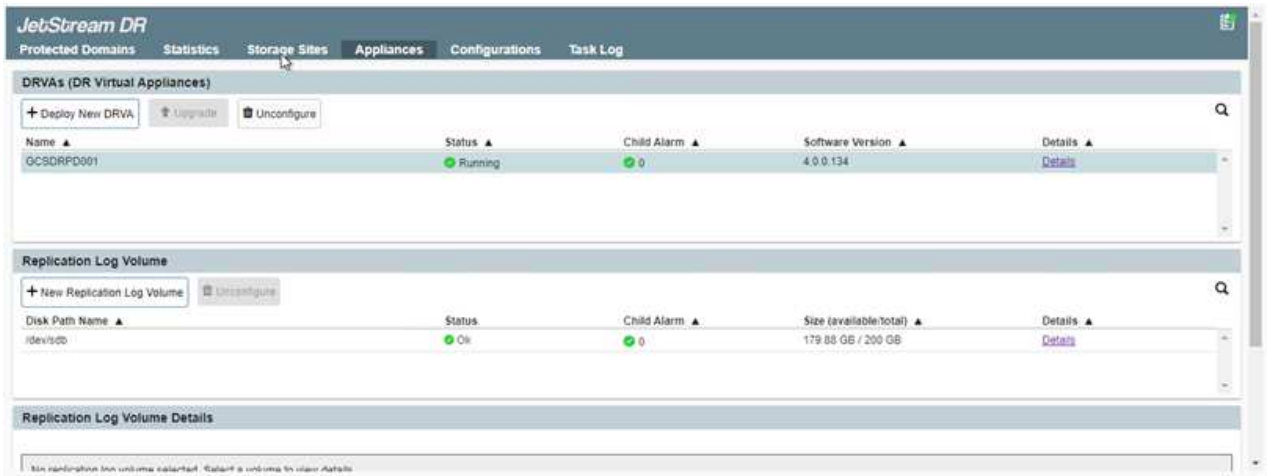


8. Distribuire il numero richiesto di DR Virtual Appliance (DRVA) dalla scheda Appliance.

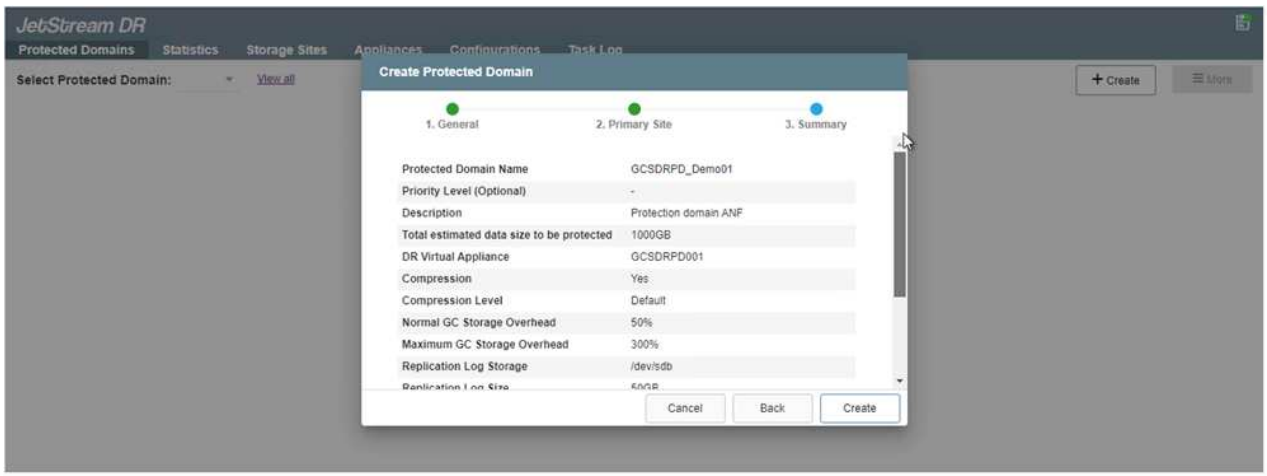
> Utilizzare lo strumento di pianificazione della capacità per stimare il numero di DRVA necessari.

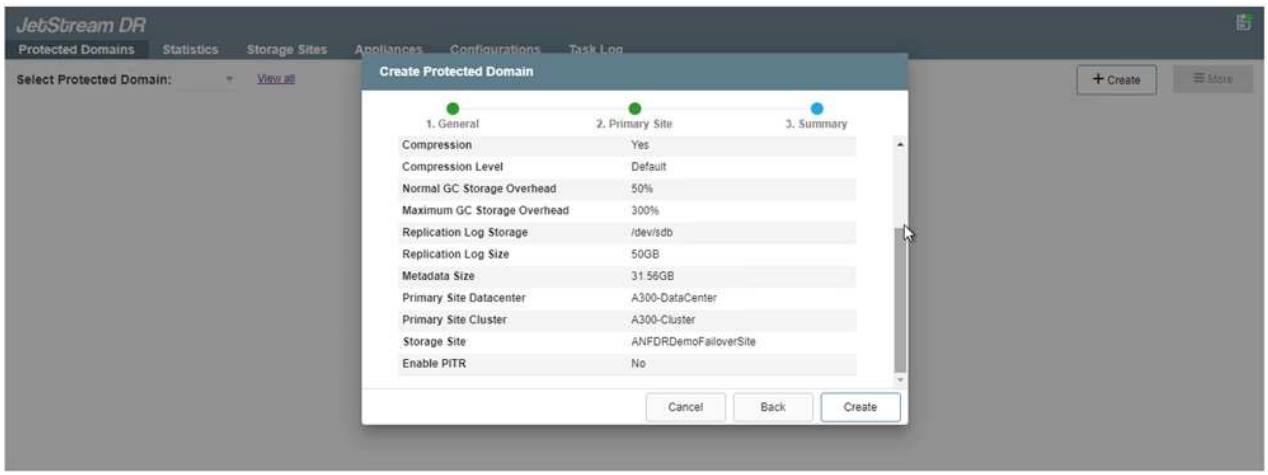


9. Creare volumi di registro di replica per ogni DRVA utilizzando il VMDK dagli archivi dati disponibili o dal pool di archiviazione iSCSI condiviso indipendente.



10. Dalla scheda Domini protetti, creare il numero richiesto di domini protetti utilizzando le informazioni sul sito di Azure Blob Storage, l'istanza DRVA e il registro di replica. Un dominio protetto definisce una VM specifica o un set di VM applicative all'interno del cluster, protette insieme e a cui viene assegnato un ordine di priorità per le operazioni di failover/failback.

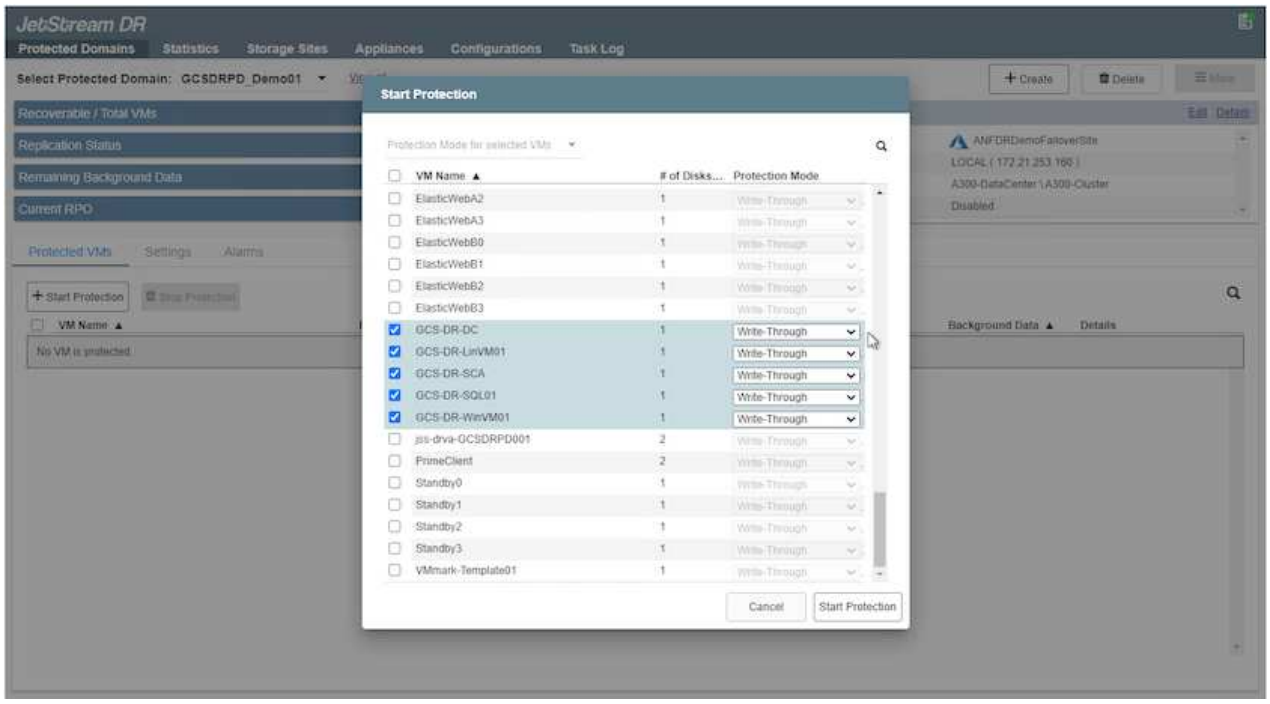




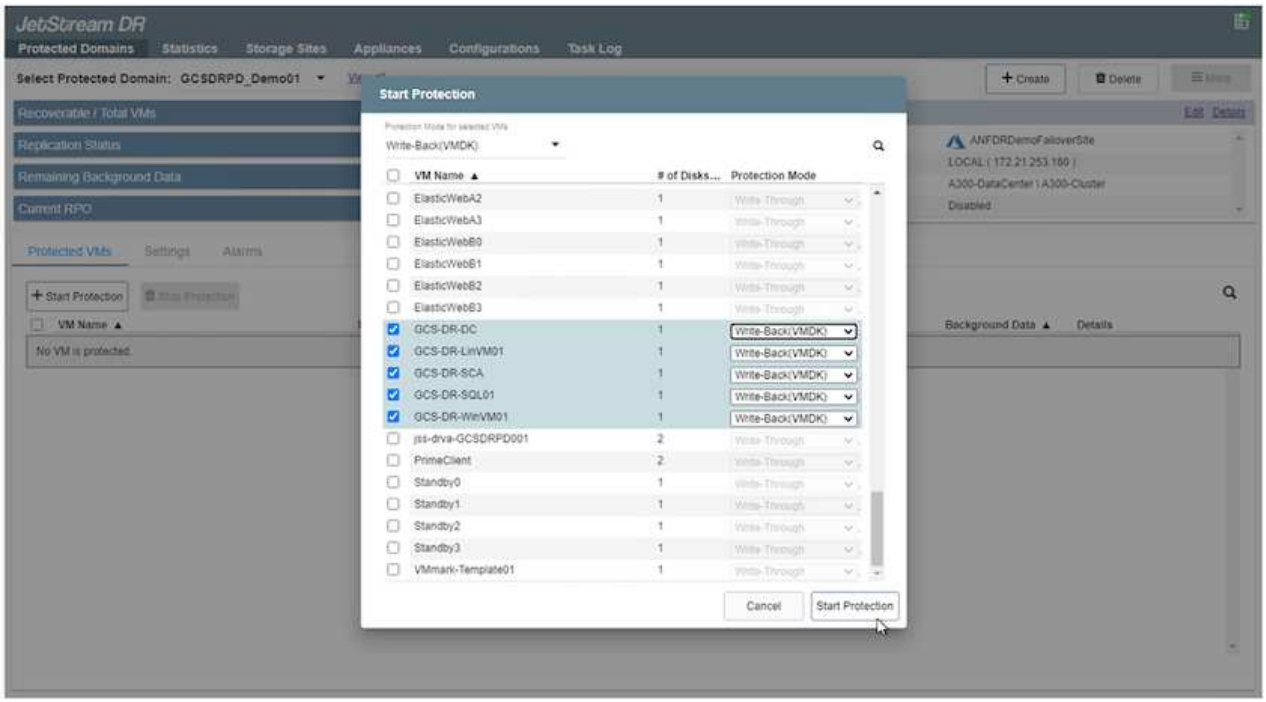
11. Selezionare le VM da proteggere e raggrupparle in gruppi di applicazioni in base alla dipendenza. Le definizioni delle applicazioni consentono di raggruppare set di VM in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e convalide facoltative delle applicazioni che possono essere eseguite al momento del ripristino.

Assicurarsi che venga utilizzata la stessa modalità di protezione per tutte le VM in un dominio protetto.

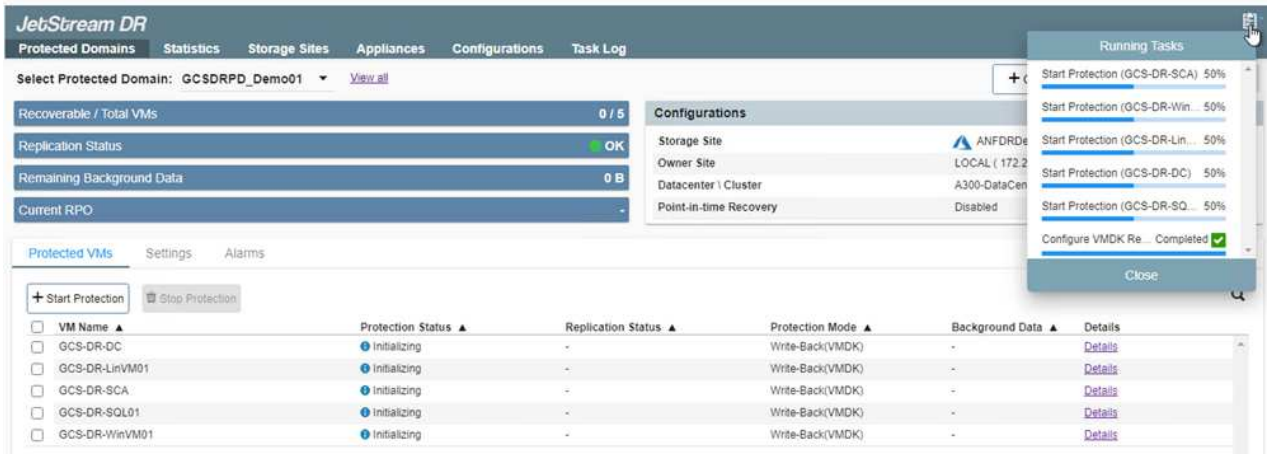
La modalità Write-Back (VMDK) offre prestazioni più elevate.



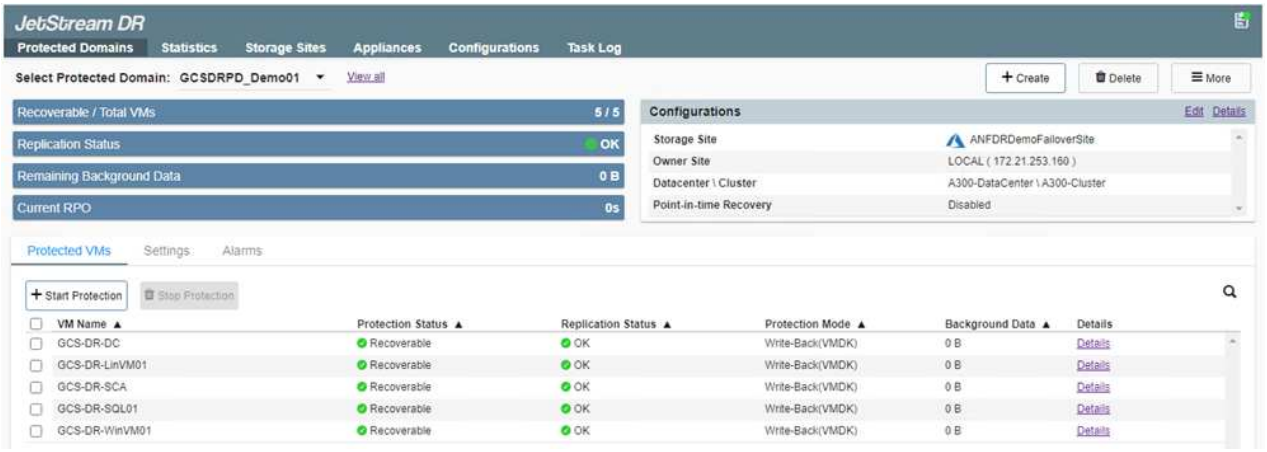
12. Assicurarsi che i volumi del registro di replica siano posizionati su un archivio ad alte prestazioni.



13. Al termine, fare clic su Avvia protezione per il dominio protetto. In questo modo viene avviata la replica dei dati per le VM selezionate nell'archivio BLOB designato.



14. Una volta completata la replica, lo stato di protezione della VM viene contrassegnato come Recuperabile.

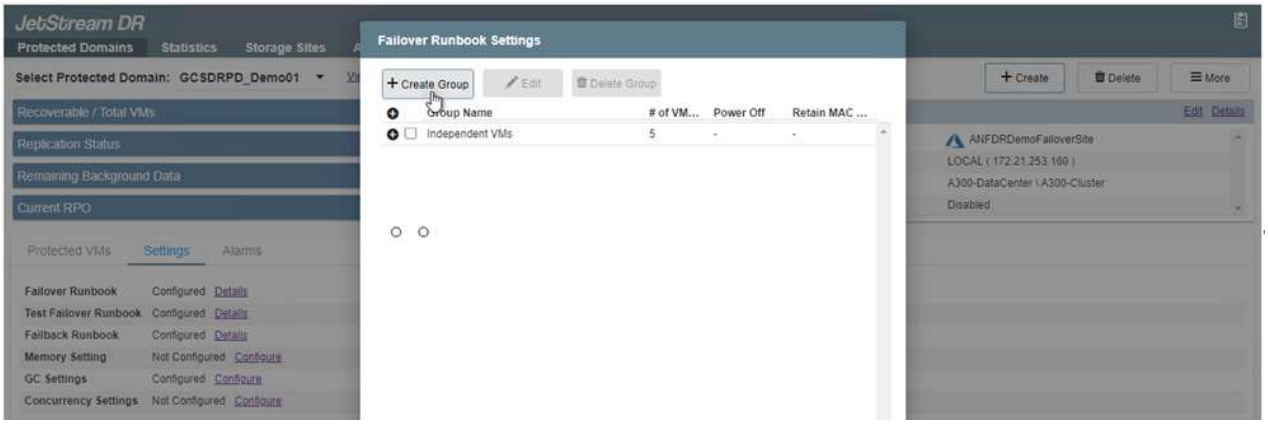


> I runbook di failover possono essere configurati per raggruppare le VM (denominate gruppo di ripristino), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

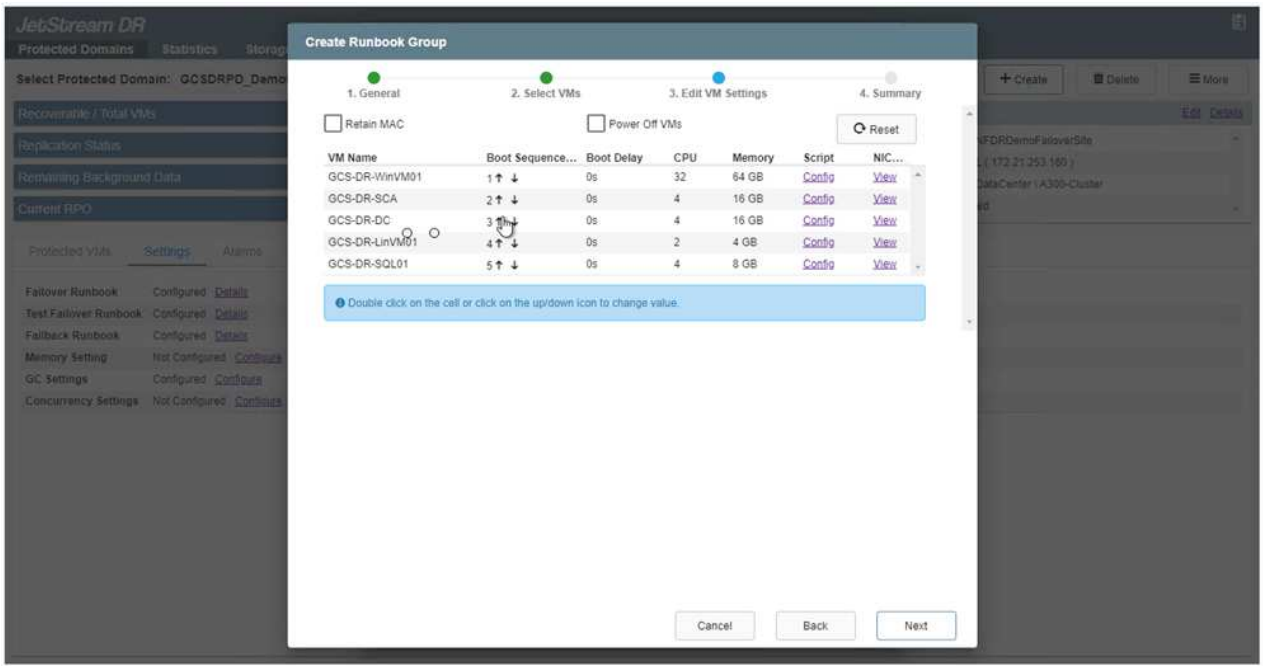
15. Fare clic su Impostazioni e quindi sul collegamento Configura runbook per configurare il gruppo runbook.

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

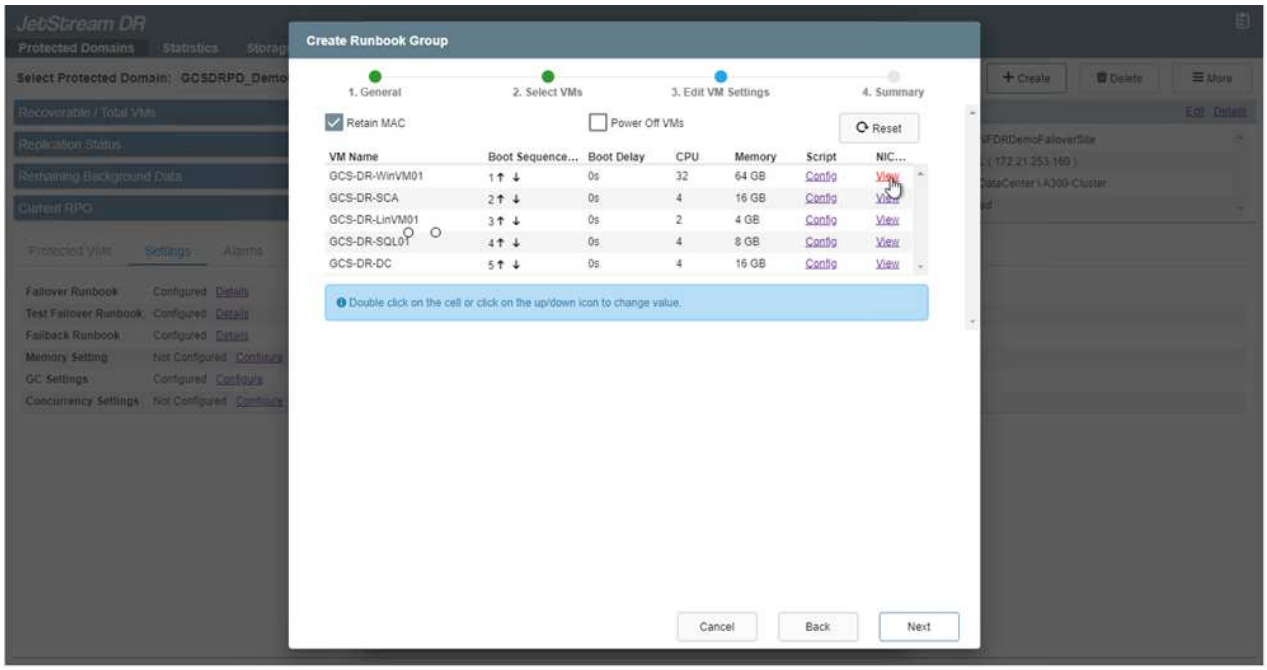
Se necessario, nella parte inferiore dello schermo, è possibile applicare pre-script e post-script personalizzati da eseguire automaticamente prima e dopo l'operazione del gruppo di runbook. Assicurarsi che gli script Runbook risiedano sul server di gestione.



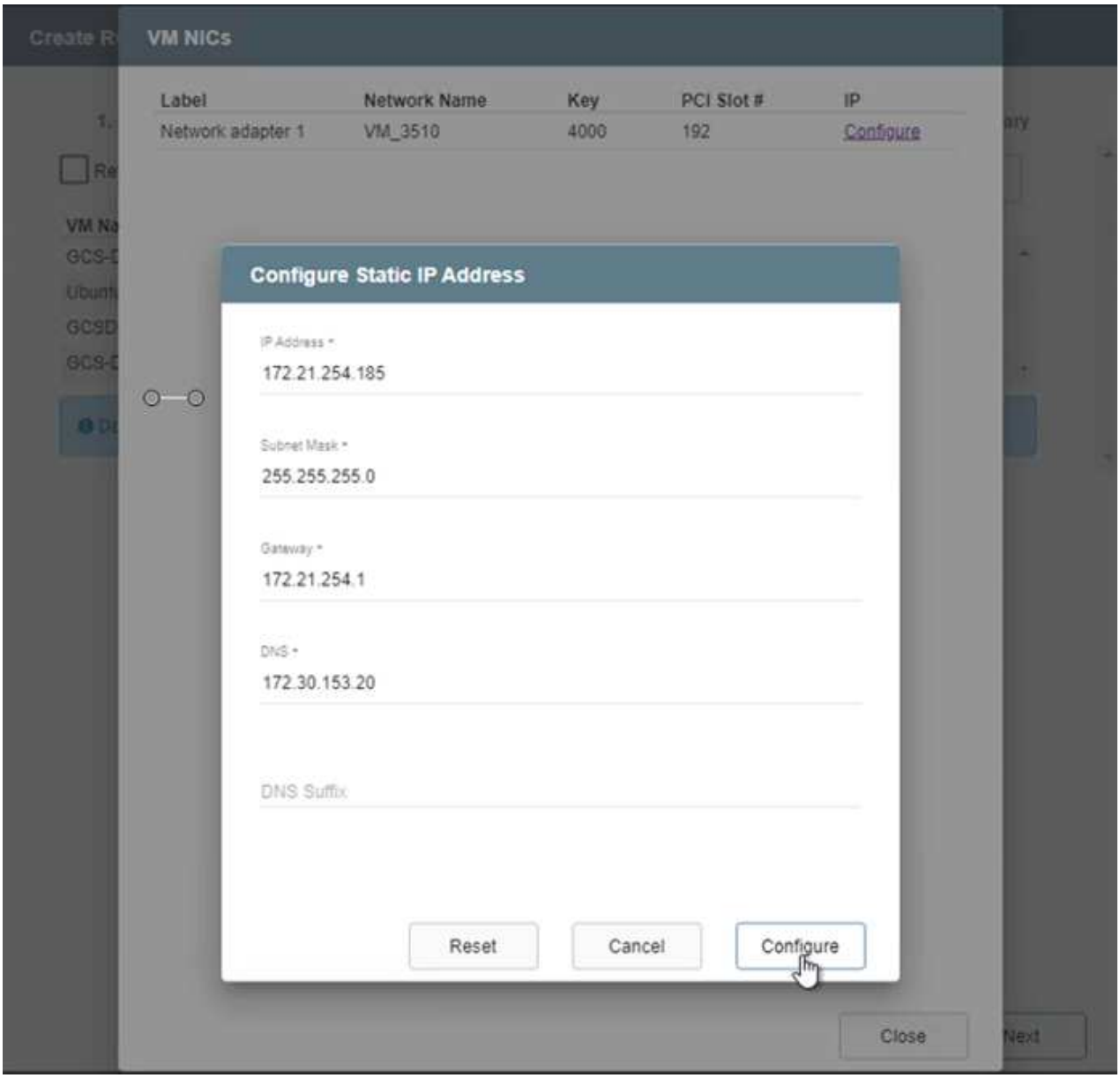
17. Modificare le impostazioni della VM secondo necessità. Specificare i parametri per il ripristino delle VM, tra cui la sequenza di avvio, il ritardo di avvio (specificato in secondi), il numero di CPU e la quantità di memoria da allocare. Modificare la sequenza di avvio delle VM facendo clic sulle frecce su o giù. Sono disponibili anche opzioni per conservare MAC.

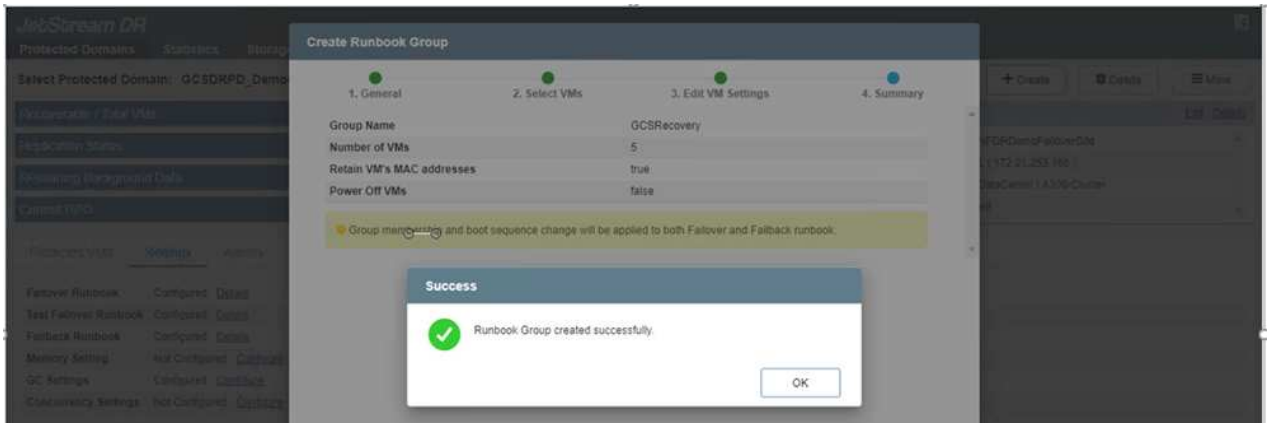


18. Gli indirizzi IP statici possono essere configurati manualmente per le singole VM del gruppo. Fare clic sul collegamento Visualizzazione NIC di una VM per configurare manualmente le impostazioni del suo indirizzo IP.



19. Fare clic sul pulsante Configura per salvare le impostazioni NIC per le rispettive VM.





Lo stato dei runbook di failover e failback è ora elencato come Configurato. I gruppi di runbook di failover e failback vengono creati in coppia utilizzando lo stesso gruppo iniziale di VM e impostazioni. Se necessario, è possibile personalizzare singolarmente le impostazioni di qualsiasi gruppo di runbook facendo clic sul rispettivo collegamento Dettagli e apportando le modifiche.

Installa JetStream DR per AVS nel cloud privato

Una buona pratica per un sito di ripristino (AVS) è quella di creare in anticipo un cluster di luci 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 altro ancora

JetStream DR supporta una modalità RTO prossima allo zero per i domini mission-critical. Per questi domini, lo storage di destinazione dovrebbe essere preinstallato. In questo caso, l'ANF è il tipo di archiviazione consigliato.

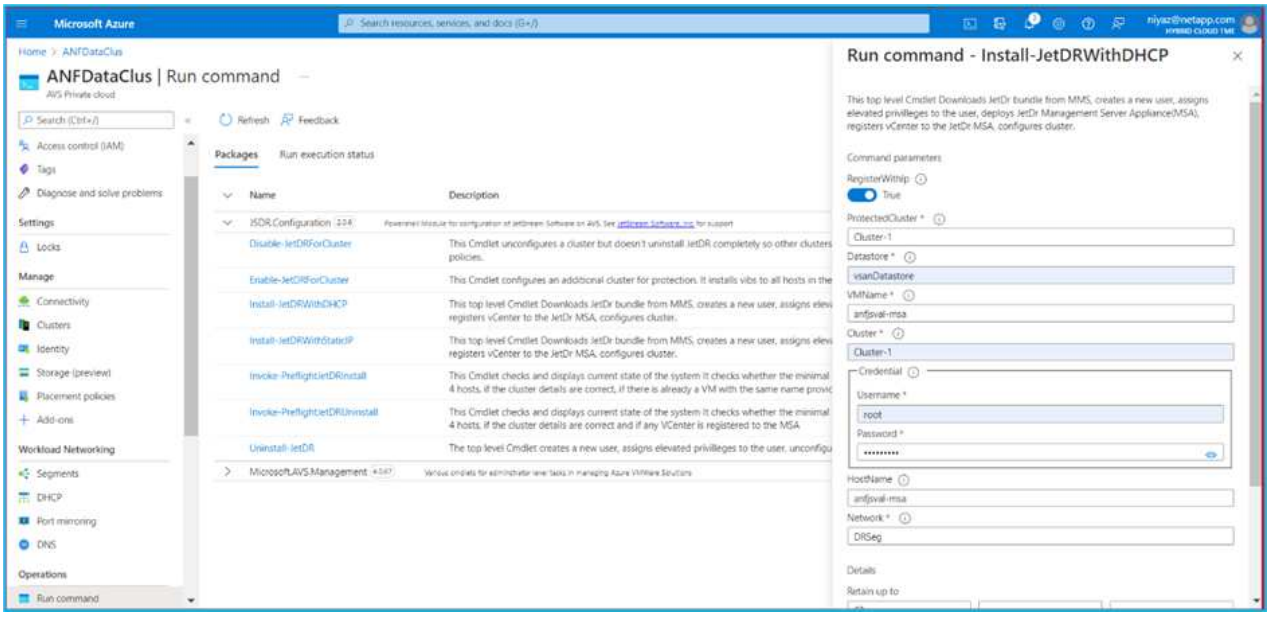
La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS in modo da soddisfare i requisiti locali.

A seconda dei requisiti SLA e RTO, è possibile utilizzare la modalità failover continuo o failover regolare (standard). Per un RTO prossimo allo zero, è necessario iniziare la reidratazione continua nel sito di recupero.

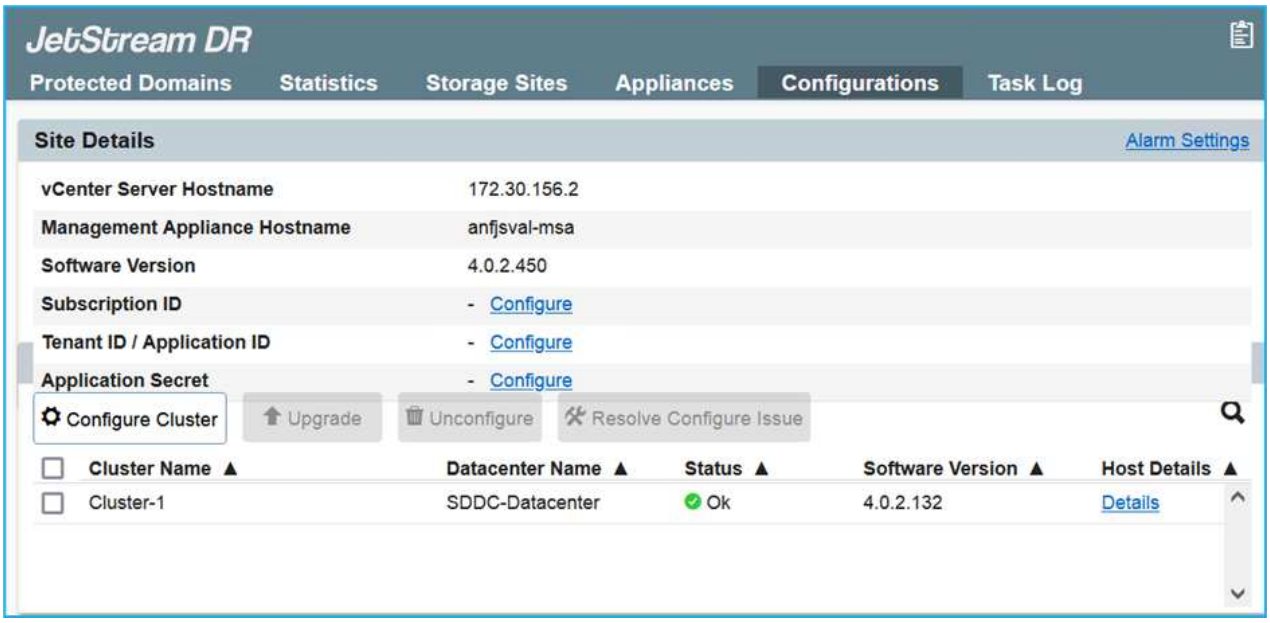
1. Per installare JetStream DR per AVS su un cloud privato di Azure VMware Solution, utilizzare il comando Esegui. Dal portale di Azure, vai alla soluzione Azure VMware, seleziona il cloud privato e seleziona Esegui comando > Pacchetti > JSDR.Configuration.

   L'utente CloudAdmin predefinito della soluzione Azure VMware non dispone di privilegi sufficienti per installare JetStream DR per AVS. La soluzione Azure VMware consente l'installazione semplificata e automatizzata di JetStream DR richiamando il comando Esegui della soluzione Azure VMware per JetStream DR.

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

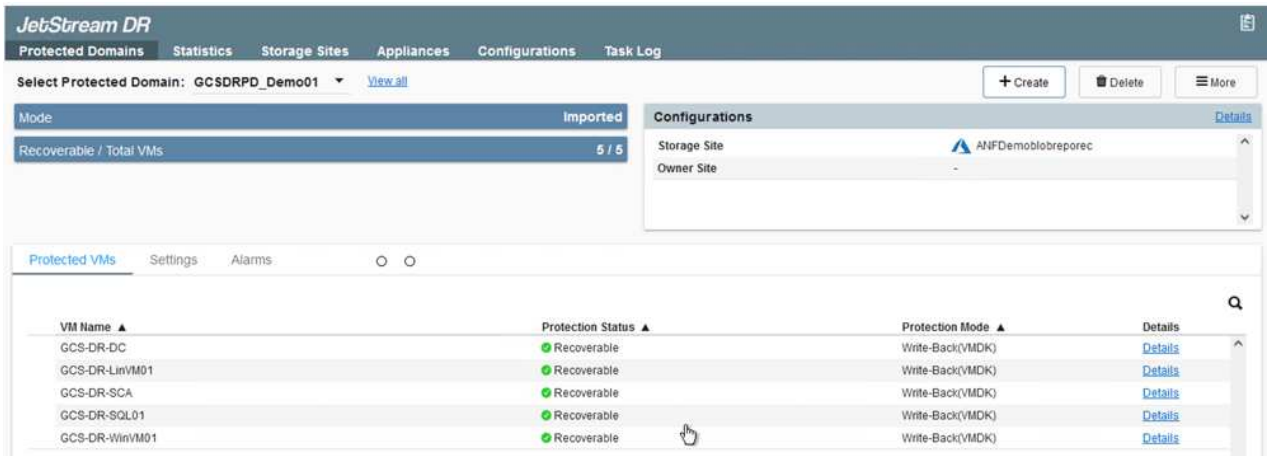


2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente di JetStream DR, andare su SDDC Datacenter > Configura > JetStream DR.



3. Dall'interfaccia JetStream DR, completare le seguenti attività:
   a. Aggiungere l'account di Azure Blob Storage utilizzato per proteggere il cluster locale come sito di archiviazione, quindi eseguire l'opzione Scansiona domini.
   b. Nella finestra di dialogo pop-up che appare, seleziona il dominio protetto da importare e poi clicca sul relativo link Importa.

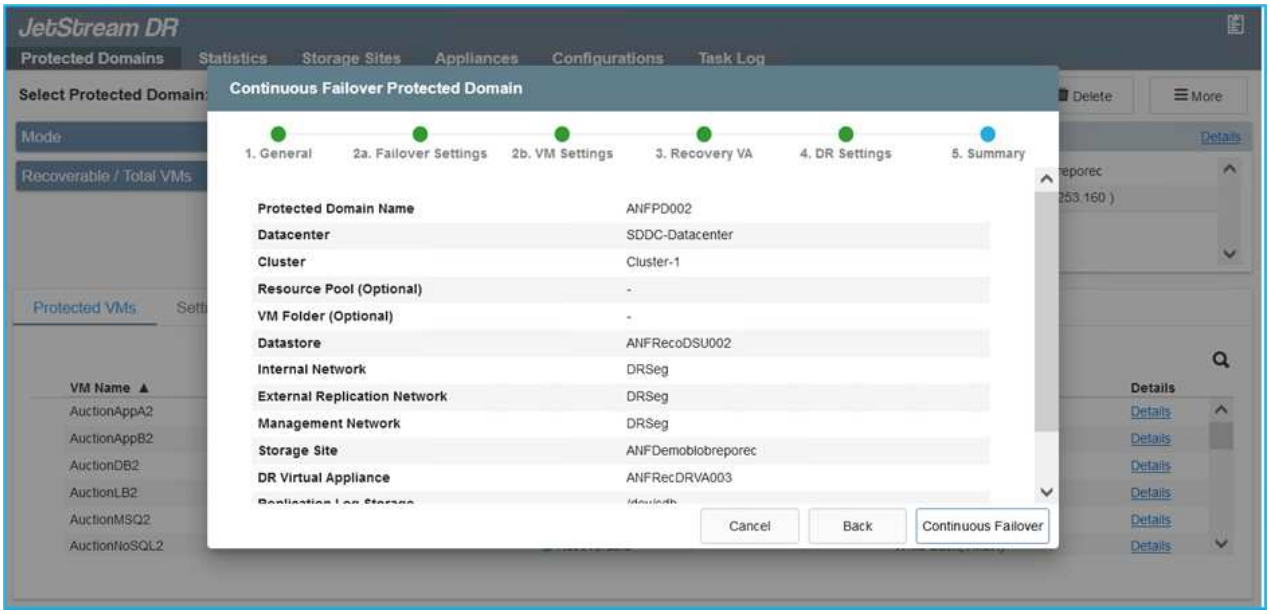
4. Il dominio viene importato per il ripristino. Vai alla scheda Domini protetti e verifica che sia stato selezionato il dominio desiderato oppure scegli quello desiderato dal menu Seleziona dominio protetto. Viene visualizzato un elenco delle VM recuperabili nel dominio protetto.



5. Dopo aver importato i domini protetti, distribuire gli appliance DRVA.

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

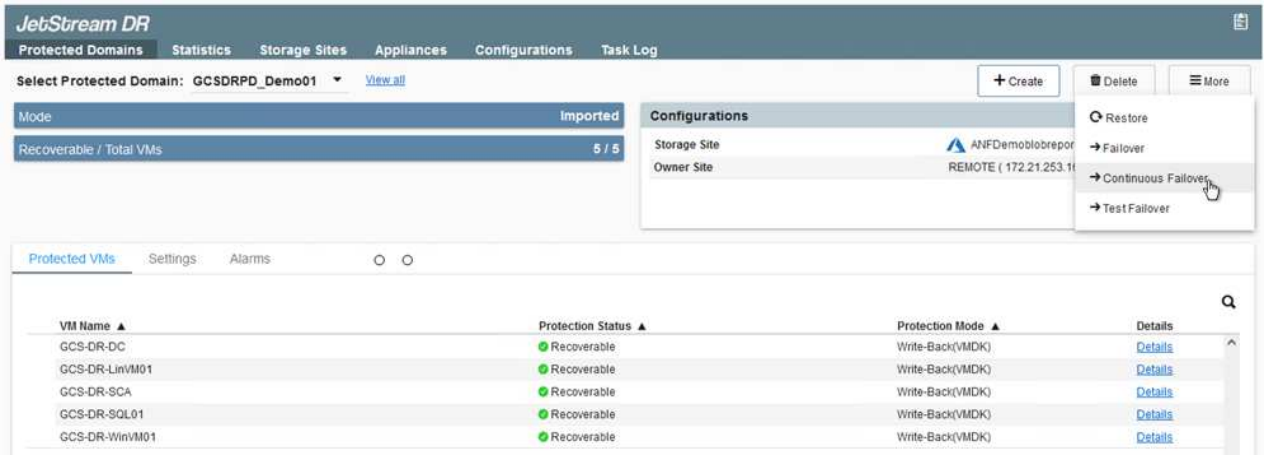
6. Creare volumi di log di replicazione utilizzando i datastore vSAN o ANF disponibili.
7. Importare i domini protetti e configurare il VA di ripristino per utilizzare un datastore ANF per i posizionamenti delle VM.



Assicurarsi che DHCP sia abilitato sul segmento selezionato e che siano disponibili sufficienti IP. Gli IP dinamici vengono utilizzati temporaneamente mentre i domini sono in fase di ripristino. Ogni VM in fase 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 continuo o failover). In questo esempio è stata selezionata la reidratazione continua (failover continuo).

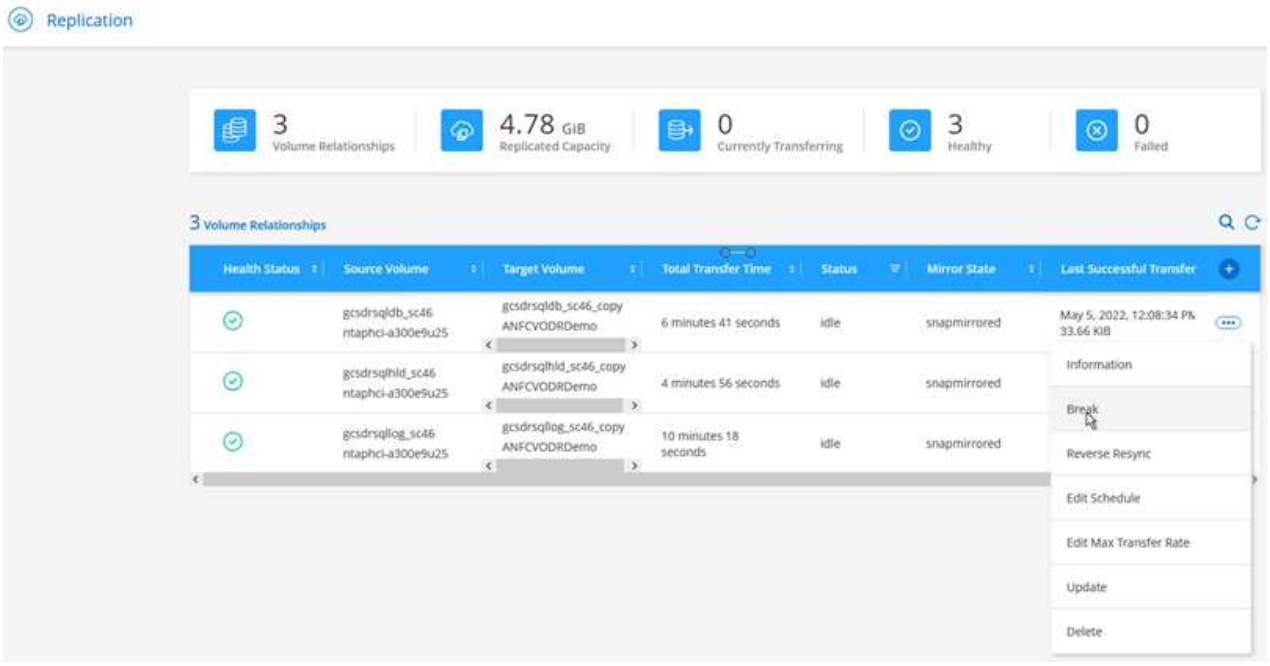
Sebbene il failover continuo e le modalità di failover differiscano nel momento in cui viene eseguita la configurazione, entrambe le modalità di failover vengono configurate utilizzando gli stessi passaggi. I passaggi di failover vengono configurati ed eseguiti insieme in risposta a un evento disastroso. Il failover continuo può essere configurato in qualsiasi momento e quindi consentito in esecuzione in background durante il normale funzionamento del sistema. Dopo che si è verificato un evento disastroso, viene completato il failover continuo per trasferire immediatamente la proprietà delle VM protette al sito di ripristino (RTO prossimo allo zero).

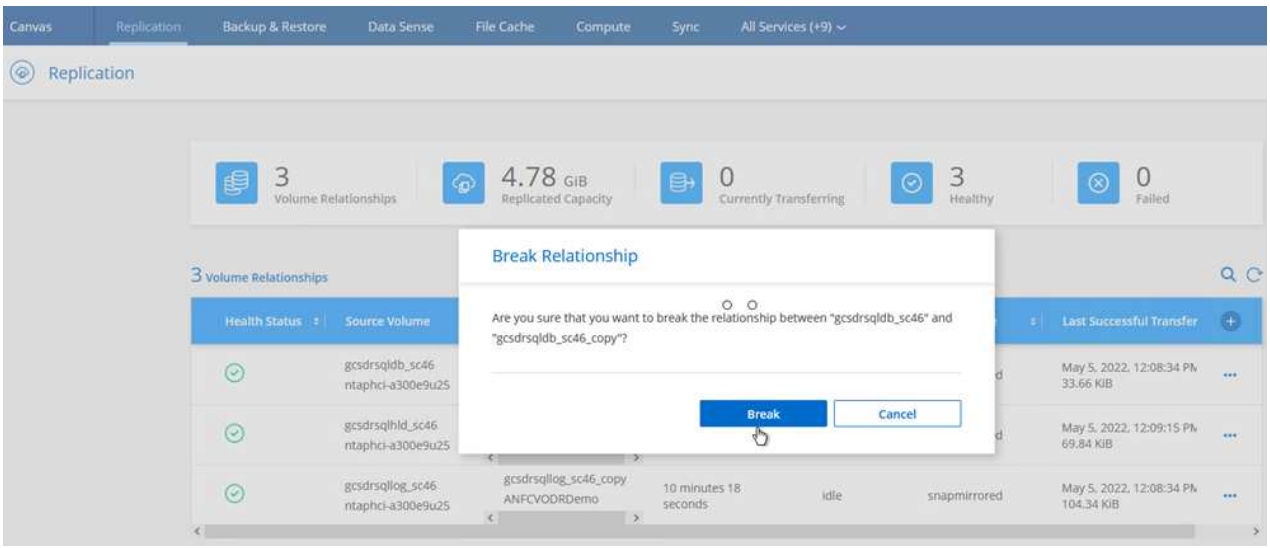


Viene avviato il processo di failover continuo, il cui avanzamento può essere monitorato dall'interfaccia utente. Facendo clic sull'icona blu nella sezione Fase corrente viene visualizzata una finestra pop-up che mostra i dettagli della fase corrente del processo di failover.

Failover e Failback

1. Dopo che si è verificato un disastro nel cluster protetto dell'ambiente on-premise (guasto parziale o completo), è possibile attivare il failover per le VM che utilizzano Jetstream dopo aver interrotto la relazione SnapMirror per i rispettivi volumi applicativi.

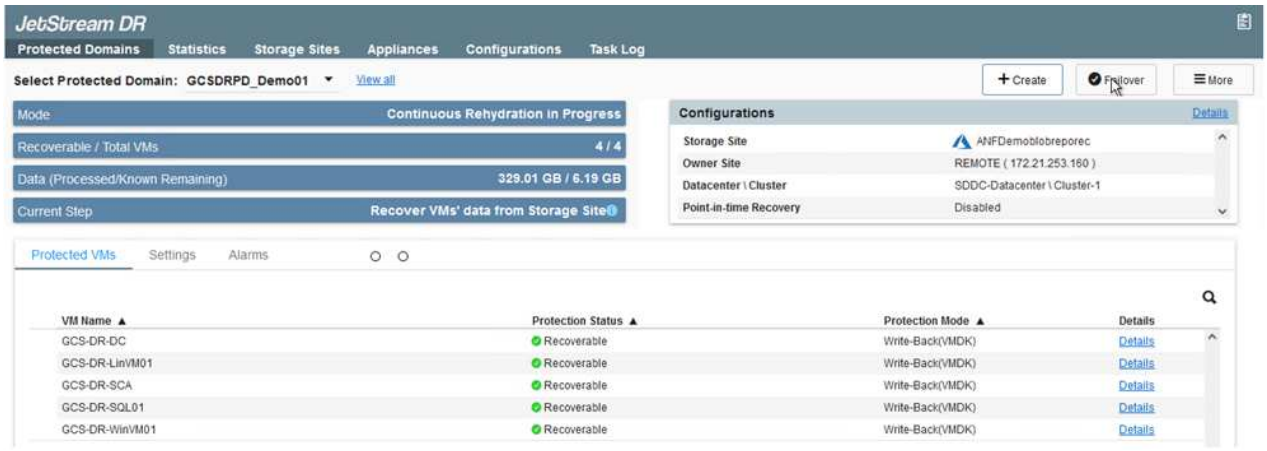


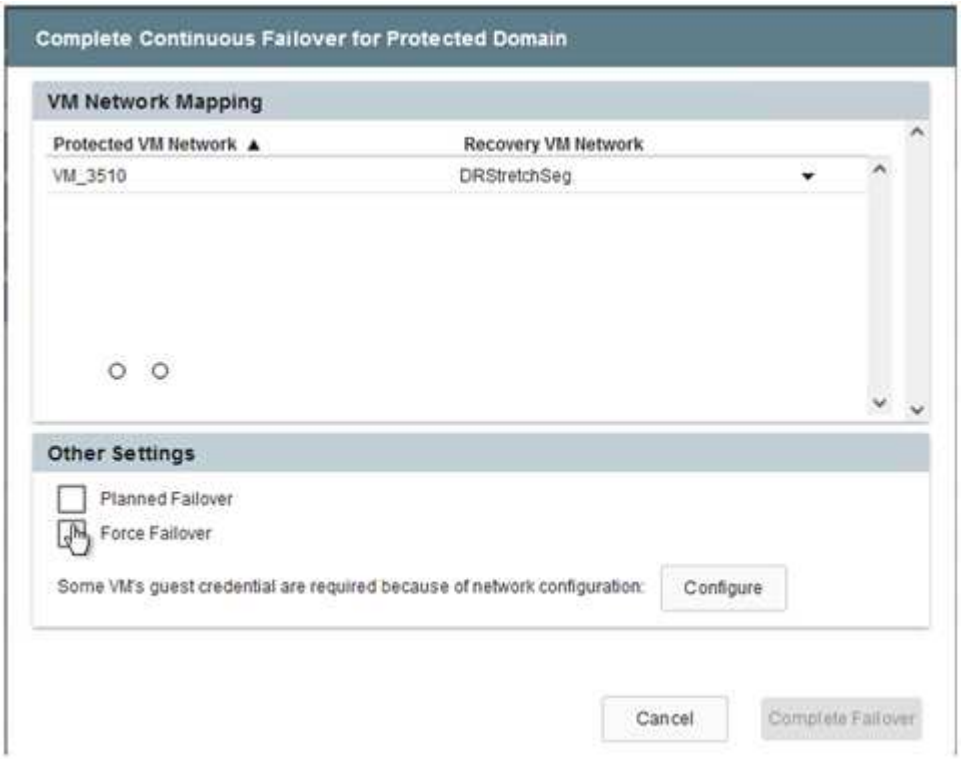


Questo passaggio può essere facilmente automatizzato per facilitare il processo di recupero.

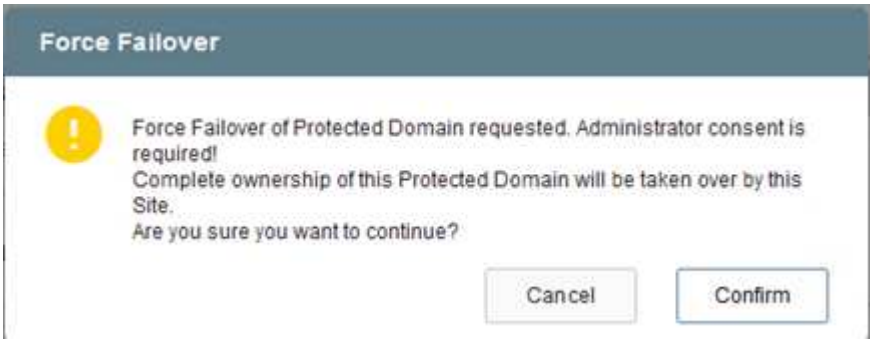
2. Accedere all'interfaccia utente di Jetstream su AVS SDDC (lato destinazione) e attivare l'opzione di failover per completare il failover. La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

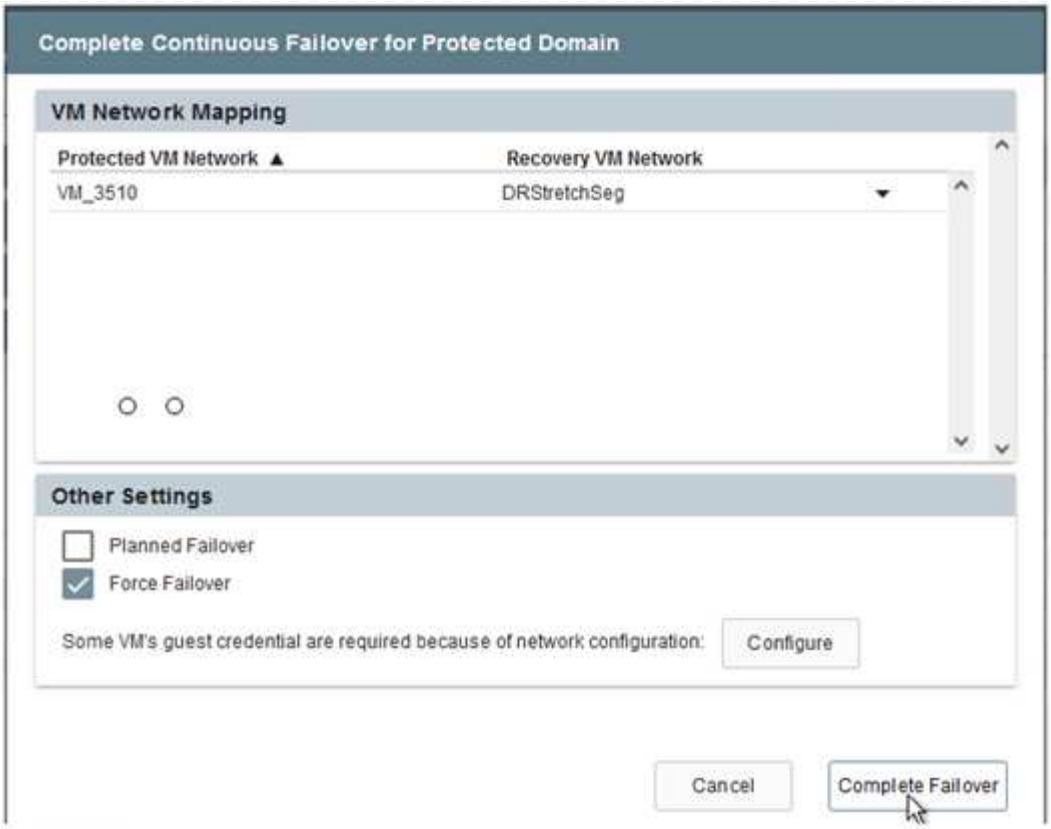
   Nella finestra di dialogo che appare al termine del failover, è possibile specificare l'attività di failover come pianificata o come forzata.





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



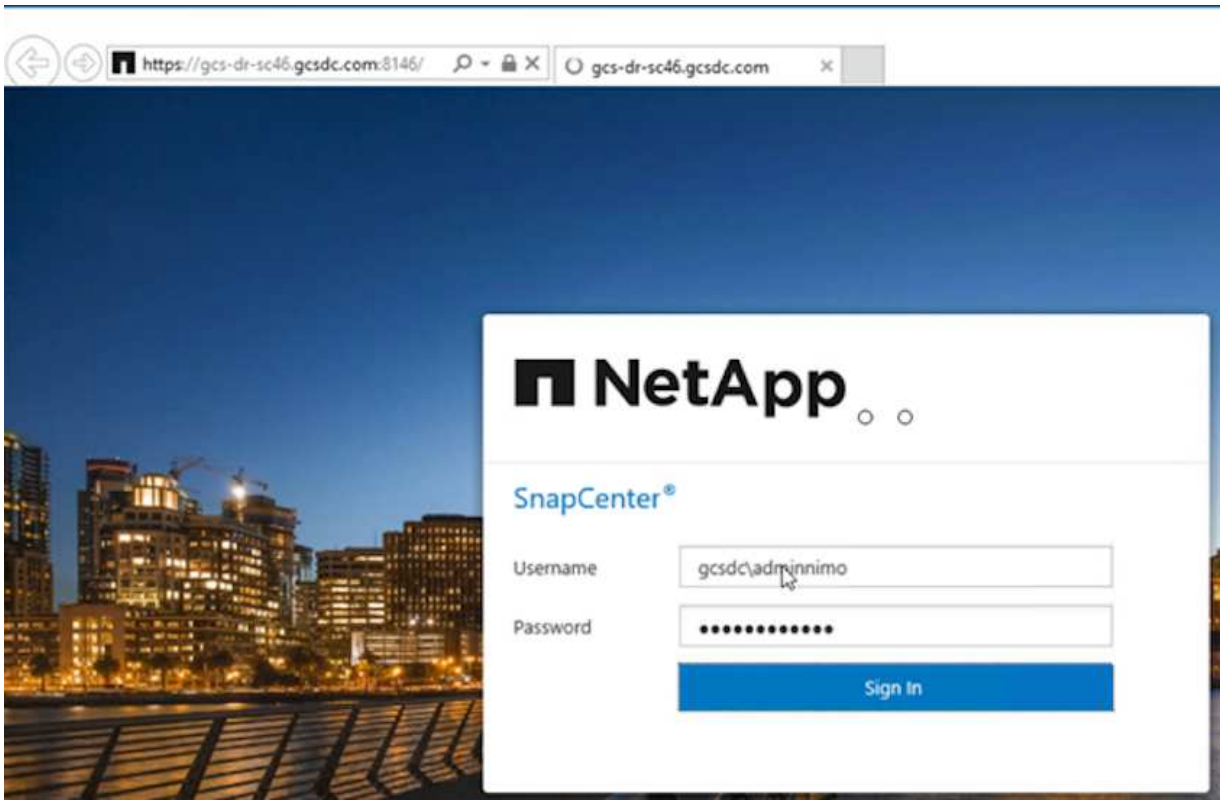


3. Una volta completato il failover continuo, viene visualizzato un messaggio che conferma il completamento dell'attività. Una volta completata l'attività, accedere alle VM ripristinate per configurare le sessioni ISCSI o NFS.

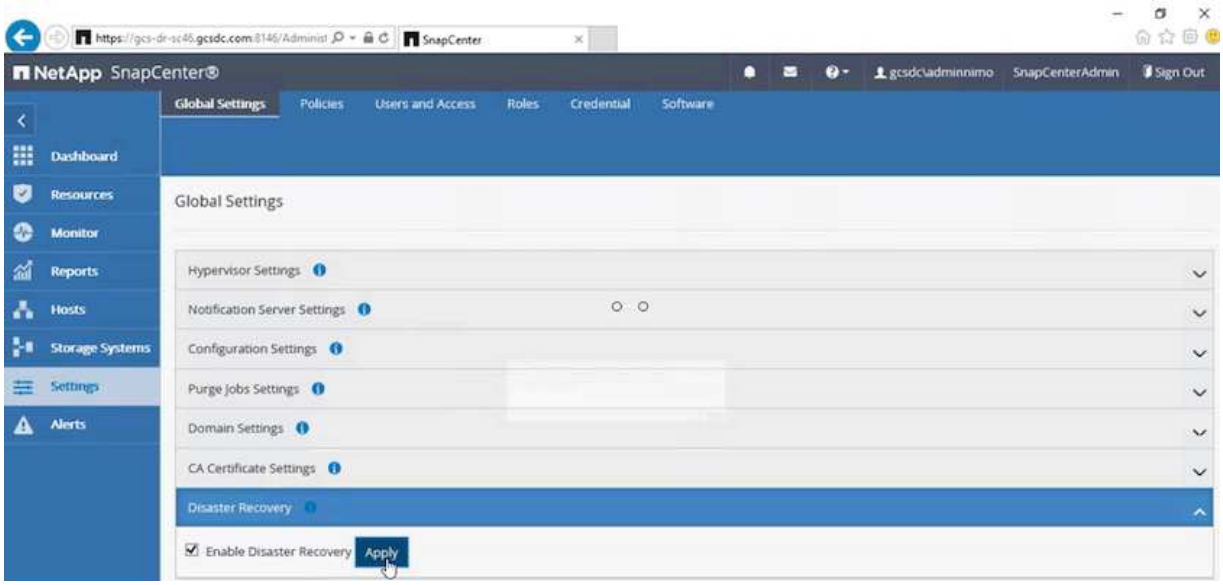
La modalità di failover cambia in In esecuzione in failover e lo stato della VM è Recuperabile. Tutte le VM del dominio protetto sono ora in esecuzione nel sito di ripristino nello stato specificato dalle impostazioni del runbook di failover.

Per verificare la configurazione e l'infrastruttura del failover, JetStream DR può essere utilizzato in modalità di test (opzione Test Failover) per osservare il ripristino delle macchine virtuali e dei relativi dati dall'archivio oggetti in un ambiente di ripristino di test. Quando una procedura di failover viene eseguita in modalità test, il suo funzionamento è simile a un vero e proprio processo di failover.

4. Dopo aver ripristinato le macchine virtuali, utilizzare il ripristino di emergenza dell'archiviazione per l'archiviazione in-guest. Per dimostrare questo processo, in questo esempio viene utilizzato SQL Server.
5. Accedere alla VM SnapCenter recuperata su AVS SDDC e abilitare la modalità DR.
   a. Accedi all'interfaccia utente SnapCenter tramite il browserN.



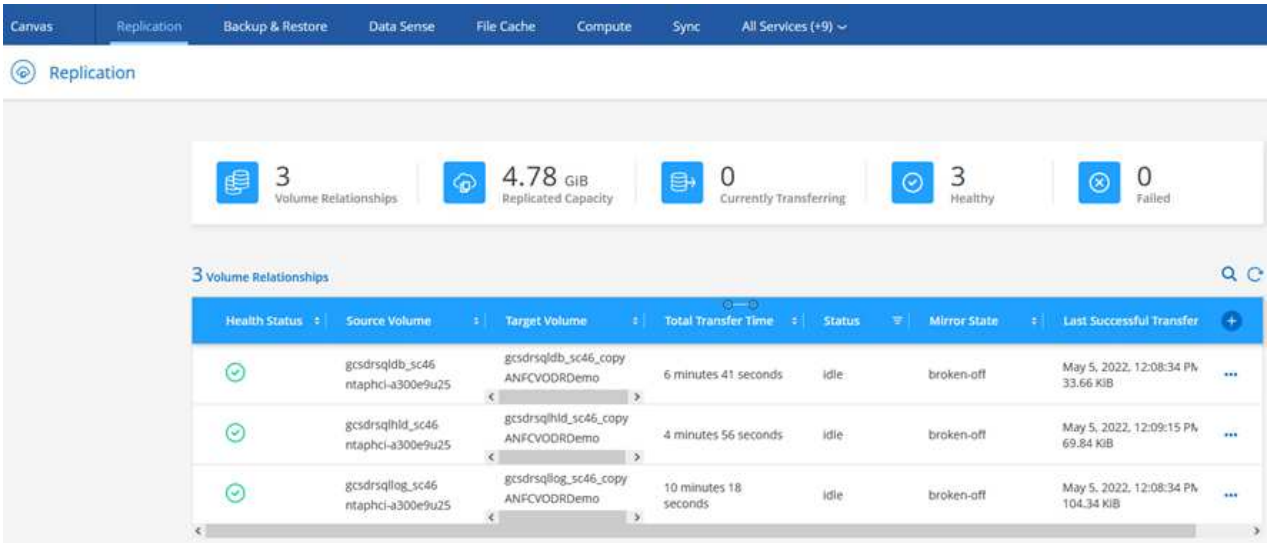
   b. Nella pagina Impostazioni, vai su Impostazioni > Impostazioni globali > Ripristino di emergenza.
   c. Selezionare Abilita ripristino di emergenza.
   d. Fare clic su Applica.



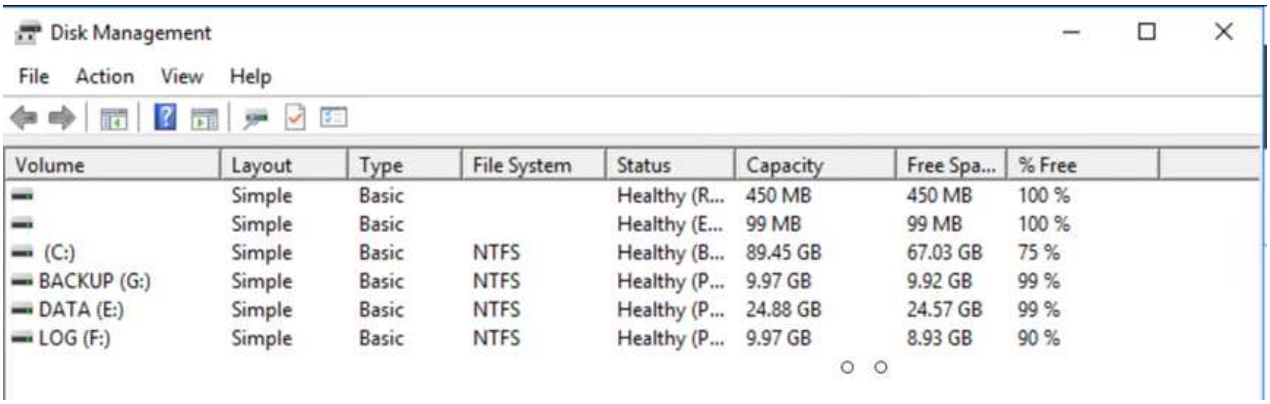
e. Verificare se il processo DR è abilitato facendo clic su Monitor > Processi.

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

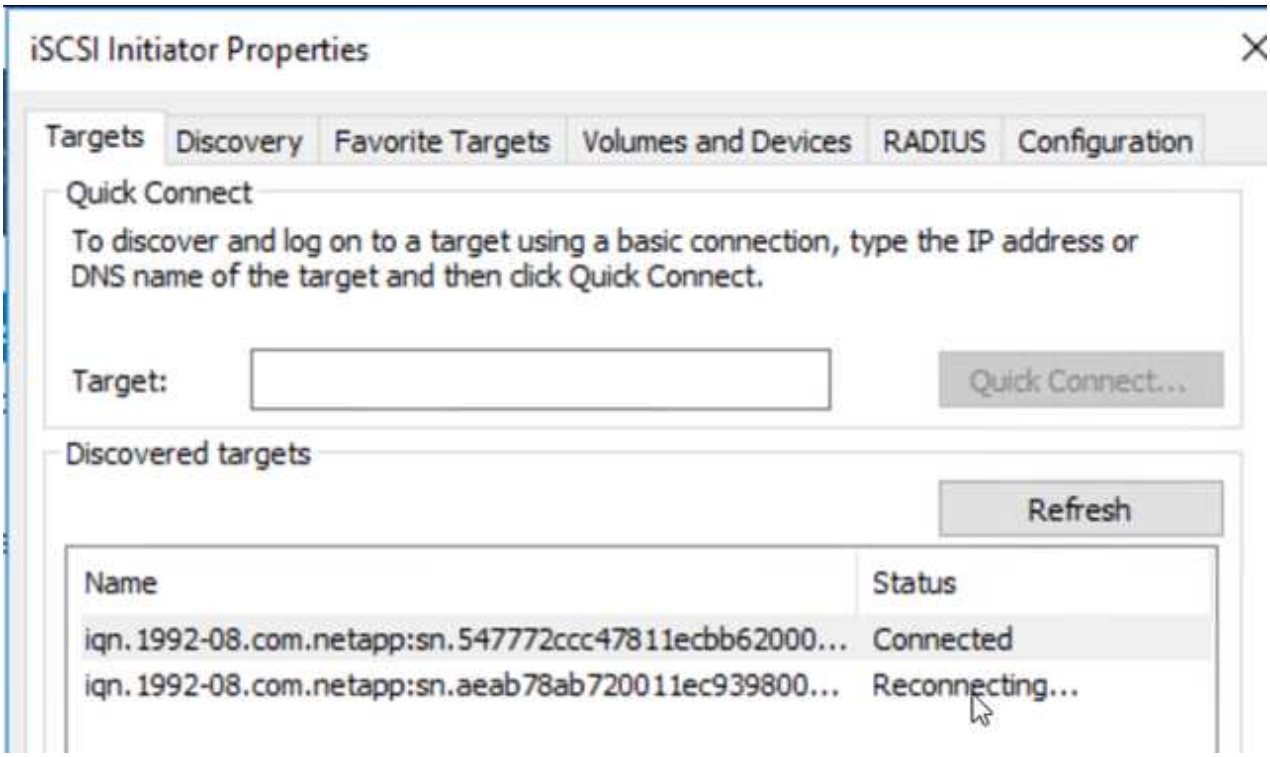
6. Assicurarsi che la relazione SnapMirror sia interrotta.



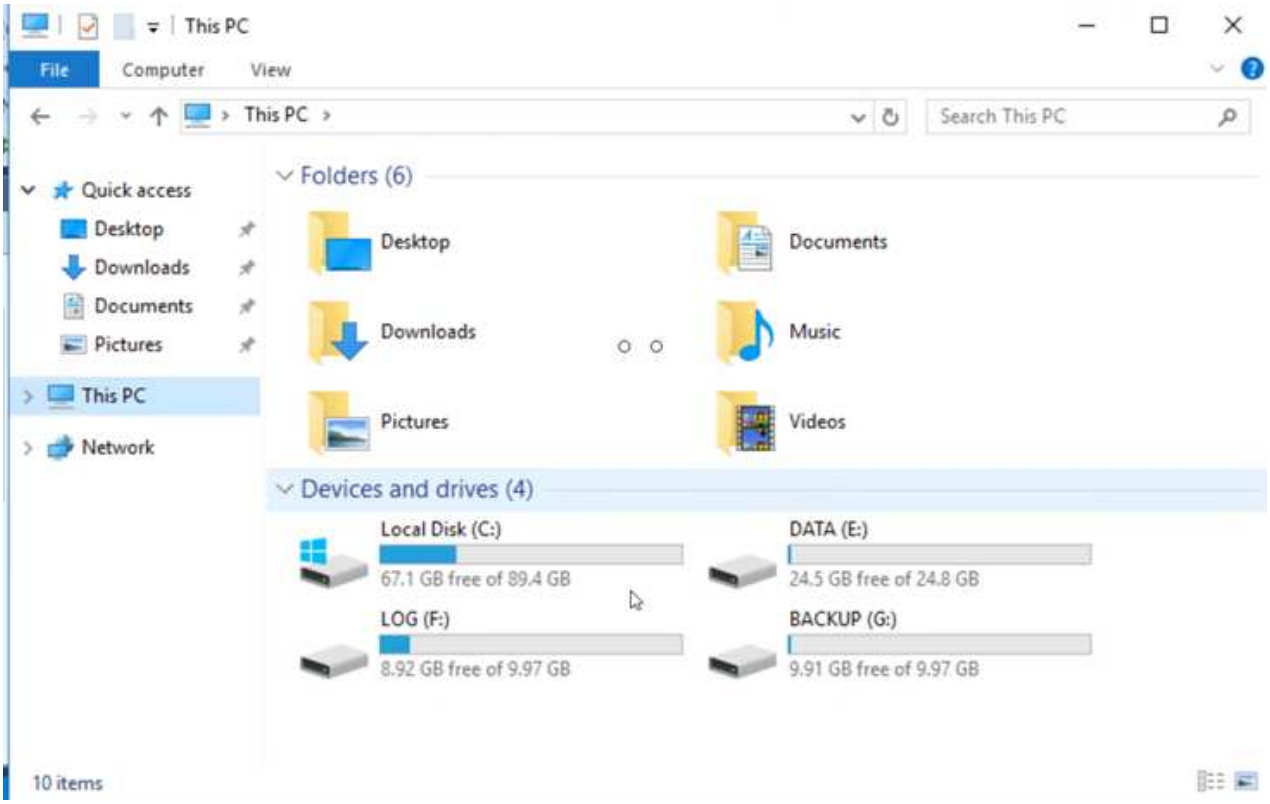
7. Collegare la LUN da Cloud Volumes ONTAP alla VM guest SQL ripristinata con le stesse lettere di unità.



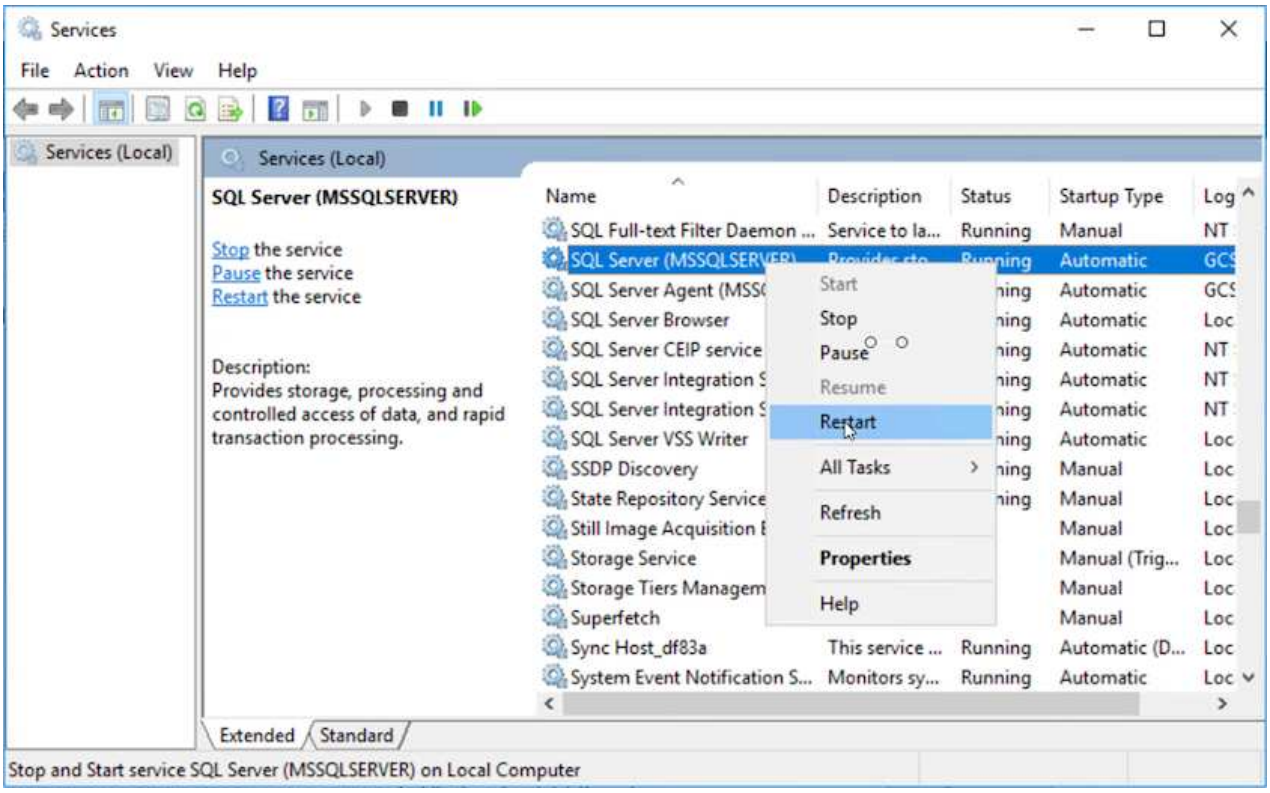
8. Aprire iSCSI Initiator, cancellare la sessione disconnessa precedente e aggiungere la nuova destinazione insieme al multipath per i volumi Cloud Volumes ONTAP replicati.



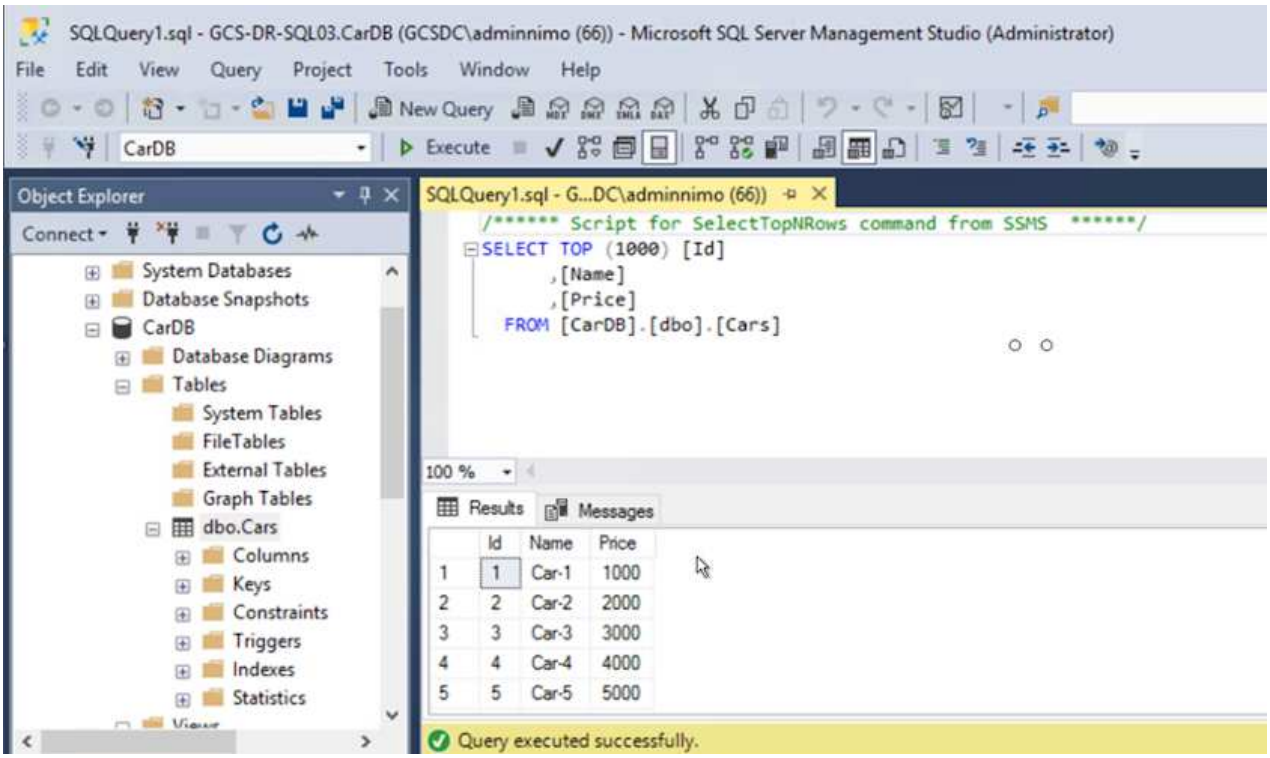
9. Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.



10. Riavviare il servizio del server MSSQL.



11. Assicurarsi che le risorse SQL siano di nuovo online.



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

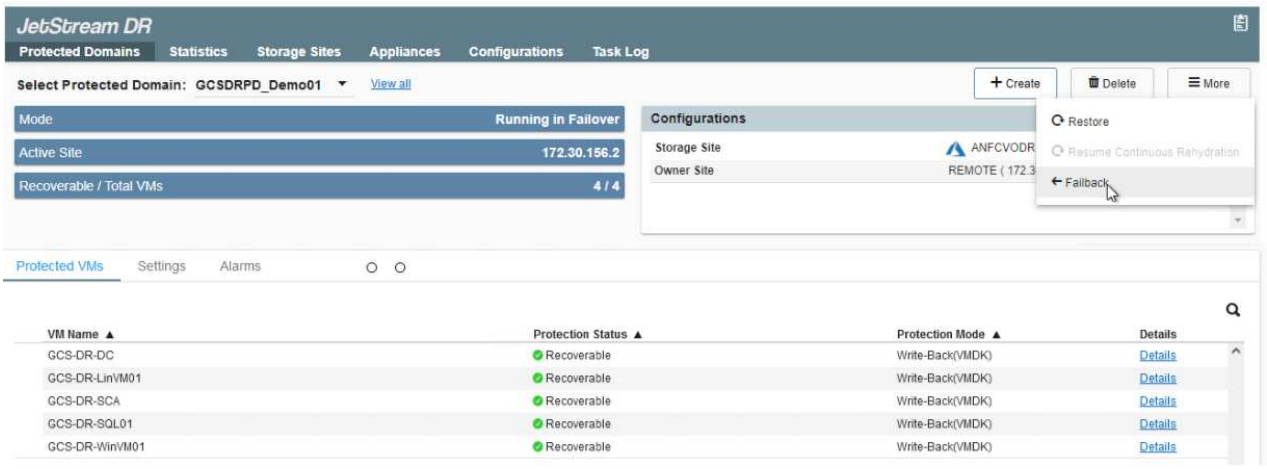
A questo punto, le operazioni possono riprendere e gli affari continuano normalmente.

Sul lato NSX-T, è possibile creare un gateway di livello 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 entrare o uscire dall'ambiente, in modo che qualsiasi attività di triage, contenimento o rafforzamento possa essere eseguita senza il rischio di contaminazione incrociata. Questa operazione esula dallo scopo del presente documento, ma può essere facilmente eseguita per simulare l'isolamento.

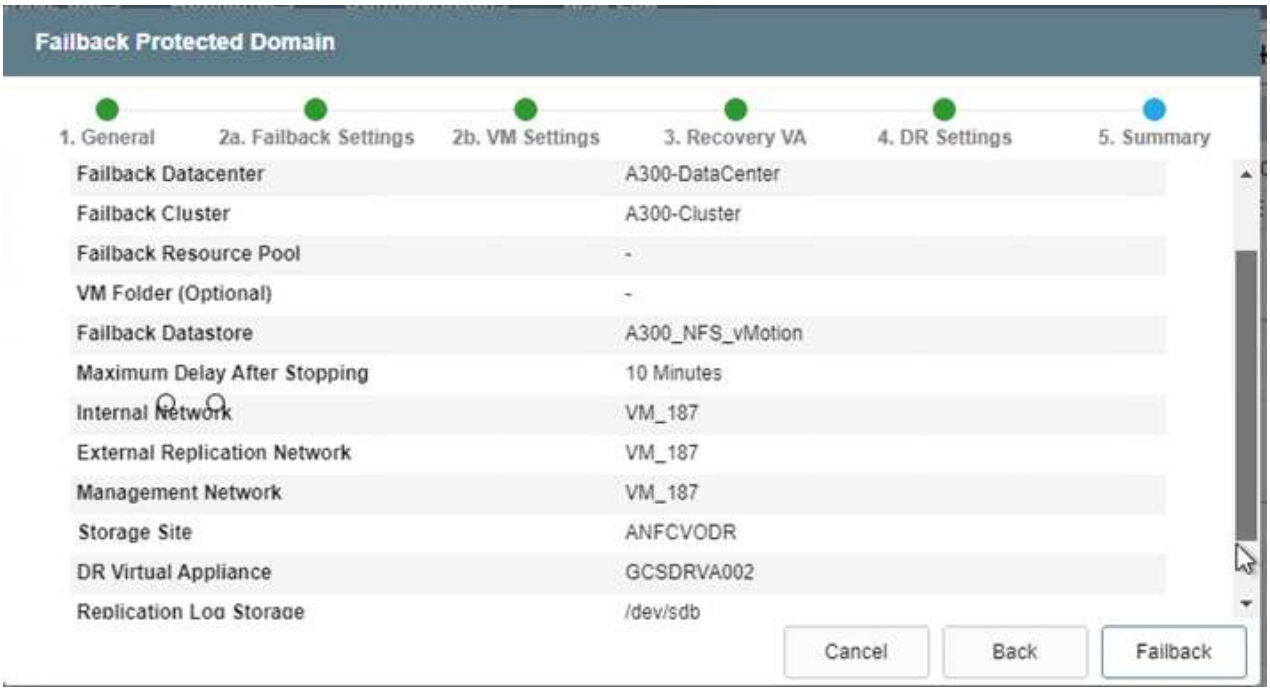
Una volta che il sito primario è di nuovo attivo e funzionante, è possibile eseguire il failback. La protezione della VM viene ripristinata da Jetstream e la relazione SnapMirror deve essere invertita.

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

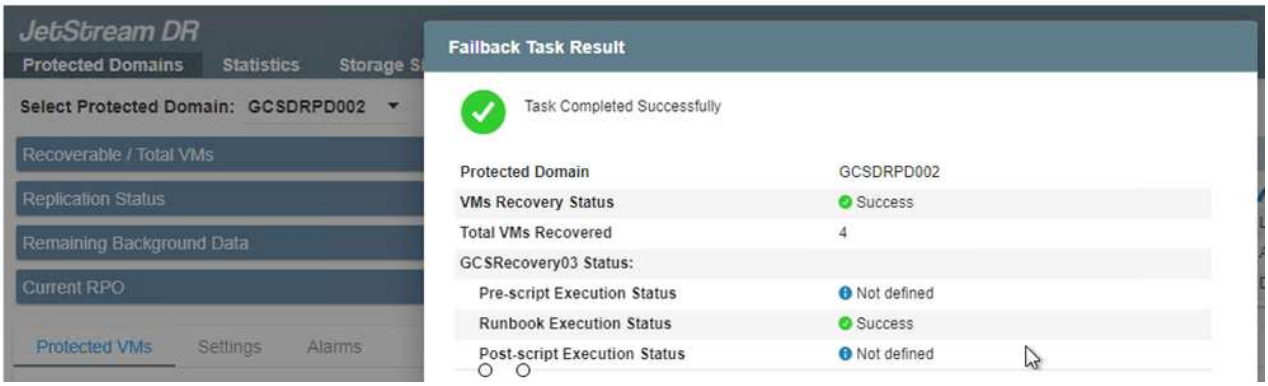
Il piano di failback generato da CPT può essere utilizzato anche per avviare il ritorno delle VM e dei relativi dati dall'archivio oggetti all'ambiente VMware originale.



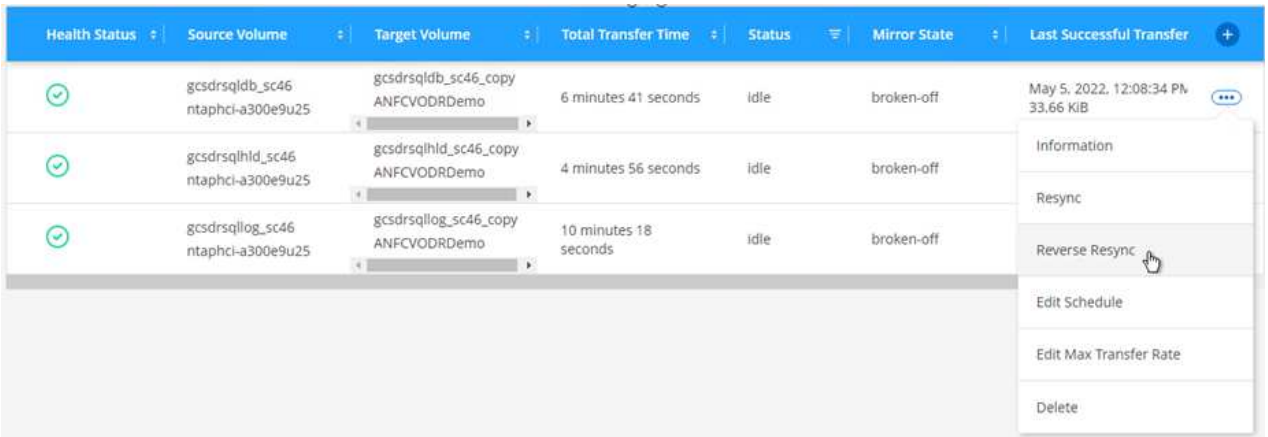
Specificare il ritardo massimo dopo la sospensione delle VM nel sito di ripristino e il loro riavvio nel sito protetto. Il tempo necessario per completare questo processo include il completamento della replica dopo l'arresto delle VM di failover, il tempo necessario per pulire il sito di ripristino e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

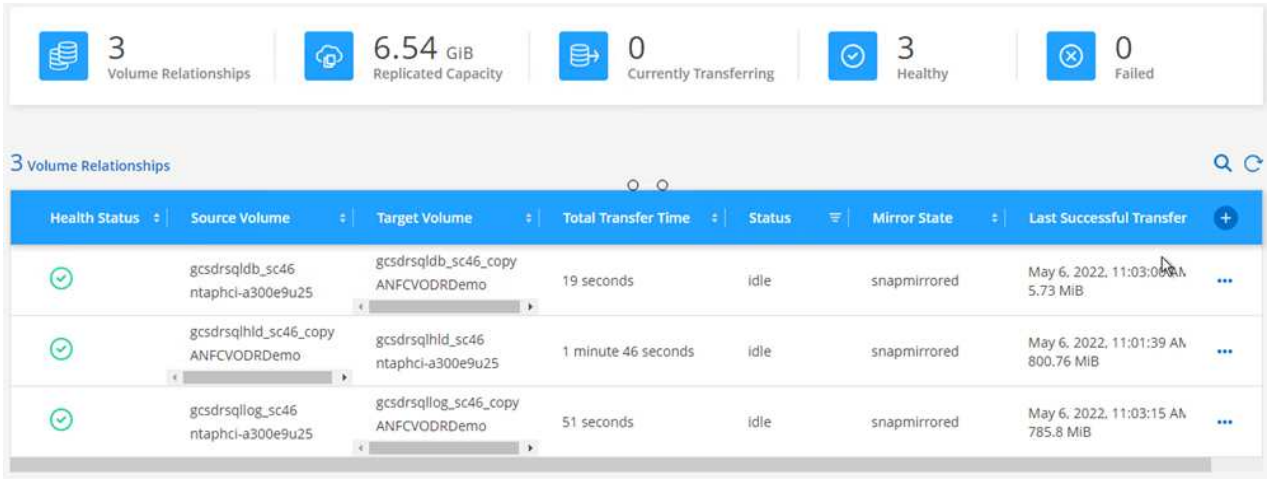


3. Completare il processo di failback e quindi confermare la ripresa della protezione della VM e la coerenza dei dati.

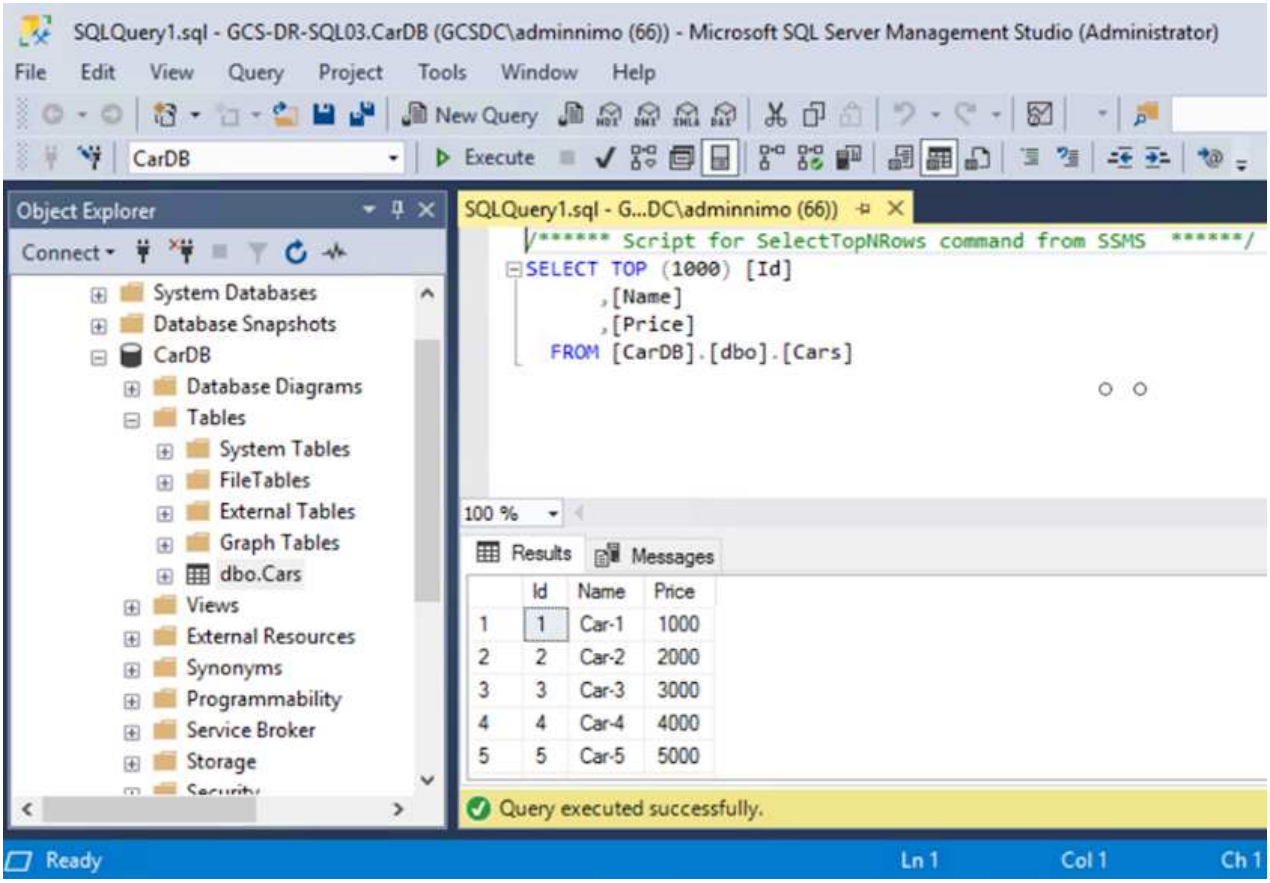


4. Dopo aver ripristinato le VM, scollegare lo storage secondario dall'host e connettersi allo storage primario.





5. Riavviare il servizio del server MSSQL.
6. Verificare che le risorse SQL siano di nuovo online.



Per eseguire il failback sullo 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 di 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, database simili e qualsiasi altra applicazione che utilizzi l'archiviazione connessa agli ospiti.

Come sempre, testare i passaggi necessari per il ripristino dei carichi di lavoro critici prima di trasferirli in produzione.

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Ripristina qualsiasi punto disponibile nel tempo con la conservazione degli snapshot ONTAP .
- È disponibile l'automazione completa per tutti i passaggi necessari al ripristino di centinaia o migliaia di VM, a partire dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- SnapCenter utilizza meccanismi di clonazione che non modificano il volume replicato.
  - In questo modo si evita il rischio di danneggiamento dei dati per volumi e snapshot.
  - Evita interruzioni della replicazione durante i flussi di lavoro dei test DR.
  - Sfrutta i dati DR per flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e aggiornamenti e test di correzione.
- L'ottimizzazione di CPU e RAM può contribuire a ridurre i costi del cloud consentendo il ripristino su cluster di elaborazione più piccoli.

Informazioni sul copyright

Informazioni sul marchio commerciale