Disaster recovery BlueXP

NetApp Solutions

NetApp
August 24, 2024

Sommario

Disaster recovery BlueXP

Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM

La strategia di backup 3-2-1 è un metodo di protezione dei dati accettato dal settore, che offre un approccio completo alla protezione dei dati importanti. Questa strategia è affidabile e garantisce che, anche in caso di incidenti imprevisti, vi sia ancora una copia dei dati disponibili.

Autore: Josh Powell - NetApp Solutions Engineering

Panoramica

La strategia si articola in tre regole fondamentali:

1. Conservare almeno tre copie dei dati. In questo modo, anche se una copia viene smarrita o danneggiata, sono ancora disponibili almeno due copie rimanenti.
2. Memorizzare due copie di backup su diversi supporti o dispositivi di archiviazione. La diversificazione dei supporti storage contribuisce a proteggerli da guasti specifici dei dispositivi o dei supporti. Se un dispositivo viene danneggiato o un tipo di supporto si guasta, l'altra copia di backup rimane inalterata.
3. Infine, assicurarsi che almeno una copia di backup sia fuori sede. Lo storage offsite serve come protezione contro i disastri localizzati, come incendi o inondazioni, che potrebbero rendere le copie on-site inutilizzabili.

Questo documento di soluzione descrive una soluzione di backup 3-2-1 che utilizza il plug-in SnapCenter per VMware vSphere (SCV) per creare backup primari e secondari delle nostre macchine virtuali on-premise e backup e recovery BlueXP per le macchine virtuali per effettuare il backup di una copia dei nostri dati su cloud storage o StorageGRID.

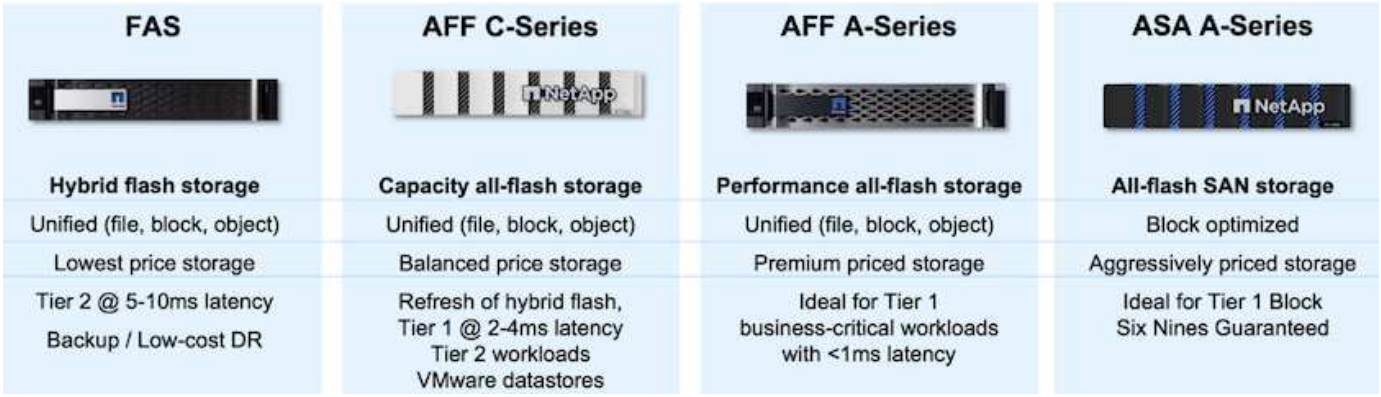
Casi di utilizzo

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup e ripristino di macchine virtuali e datastore on-premise utilizzando il plug-in SnapCenter per VMware vSphere.
- Backup e ripristino di macchine virtuali e datastore on-premise, in hosting su cluster ONTAP e backup su storage a oggetti utilizzando backup e recovery di BlueXP per le macchine virtuali.

Storage NetApp ONTAP

ONTAP è la soluzione di storage leader del settore di NetApp che offre storage unificato con accesso a protocolli SAN o NAS. La strategia di backup 3-2-1 garantisce la protezione dei dati on-premise su più tipi di supporto, mentre NetApp offre piattaforme che vanno da flash ad alta velocità a supporti a costi inferiori.



Per ulteriori informazioni su tutti i prodotti hardware della piattaforma NetApp, consulta l'articolo "Storage NetApp".

Plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter per VMware vSphere è un'offerta di protezione dei dati strettamente integrata con VMware vSphere e consente una facile gestione di backup e ripristini per le macchine virtuali. Come parte di questa soluzione, SnapMirror fornisce un metodo rapido e affidabile per creare una seconda copia di backup immutabile dei dati della macchina virtuale su un cluster di storage ONTAP secondario. Con questa architettura implementata, le operazioni di ripristino delle macchine virtuali possono essere avviate facilmente da posizioni di backup primarie o secondarie.

SCV viene installato come appliance virtuale linux utilizzando un file OVA. Il plug-in ora utilizza un plug-in remoto
architettura. Il plug-in remoto viene eseguito al di fuori del server vCenter e viene ospitato sull'appliance virtuale SCV.

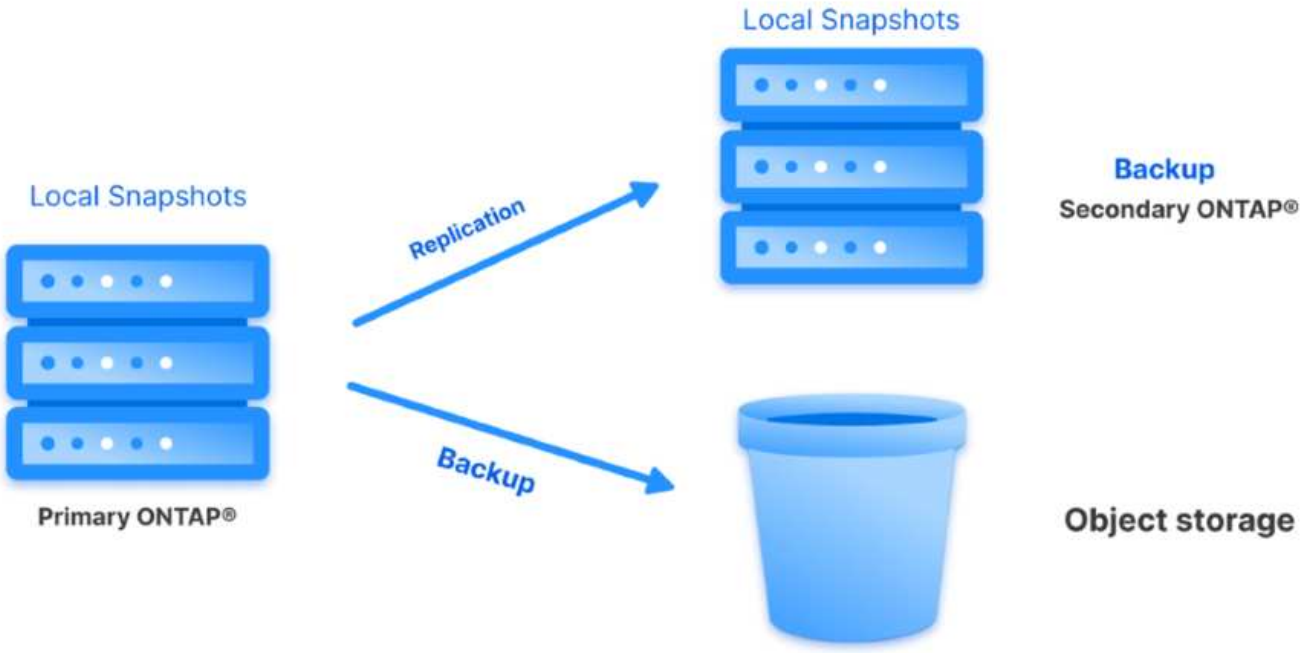
Per informazioni dettagliate sul distributore idraulico, fare riferimento a. "Plug-in SnapCenter per la documentazione di VMware vSphere".

Backup e recovery di BlueXP per le macchine virtuali

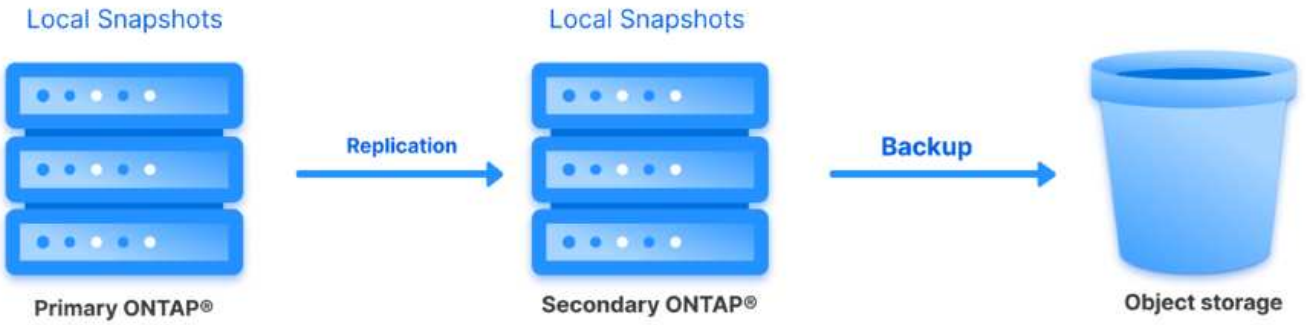
Il backup e recovery di BlueXP è uno strumento basato su cloud per la gestione dei dati che offre un singolo pannello di controllo per un'ampia gamma di operazioni di backup e recovery negli ambienti on-premise e cloud. Parte della suite di backup e recovery BlueXP di NetApp è una funzionalità che si integra con il plug-in SnapCenter per VMware vSphere (on-premise) per estendere una copia dei dati allo storage a oggetti nel cloud. In questo modo viene stabilita una terza copia dei dati fuori sede che provengono dai backup dello storage primario o secondario. Il backup e recovery di BlueXP semplifica la configurazione di policy dello storage che trasferiscono le copie dei dati da una di queste due posizioni on-premise.

La scelta tra backup primari e secondari come origine in BlueXP Backup and Recovery comporterà l'implementazione di una delle due topologie:

Topologia fan-out – quando un backup viene avviato dal plug-in SnapCenter per VMware vSphere, viene immediatamente creata una snapshot locale. SCV avvia quindi un'operazione SnapMirror che replica lo snapshot più recente nel cluster ONTAP secondario. In BlueXP Backup and Recovery, una policy specifica il cluster ONTAP primario come origine di una copia Snapshot dei dati da trasferire nello storage a oggetti nel cloud provider scelto.



Topologia a cascata – la creazione delle copie dei dati primari e secondari mediante SCV è identica alla topologia fan-out menzionata in precedenza. Tuttavia, questa volta viene creata una policy in BlueXP Backup and Recovery che specifica che il backup nello storage a oggetti avrà origine dal cluster ONTAP secondario.



Il backup e recovery di BlueXP può creare copie di backup degli snapshot ONTAP on-premise nello storage AWS Glacier, Azure Blob e GCP Archive.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

Inoltre, puoi utilizzare NetApp StorageGRID come destinazione del backup dello storage a oggetti. Per ulteriori informazioni su StorageGRID, fare riferimento alla "Landing page di StorageGRID".

Panoramica sull'implementazione della soluzione

Questo elenco fornisce i passaggi di alto livello necessari per configurare questa soluzione ed eseguire operazioni di backup e ripristino da SCV e BlueXP - Backup e ripristino:

1. Configurare la relazione SnapMirror tra i cluster ONTAP da utilizzare per le copie di dati primarie e secondarie.
2. Configura il plug-in SnapCenter per VMware vSphere.
   a. Aggiunta di sistemi storage
   b. Creare policy di backup
   c. Creare gruppi di risorse
   d. Eseguire i primi processi di backup
3. Configura backup e recovery di BlueXP per le macchine virtuali
   a. Aggiungi ambiente di lavoro
   b. Scopri le appliance SCV e vCenter
   c. Creare policy di backup
   d. Attivare i backup
4. Ripristinare le macchine virtuali dallo storage primario e secondario utilizzando SCV.
5. Ripristina le macchine virtuali dallo storage a oggetti utilizzando il backup e ripristino di BlueXP.

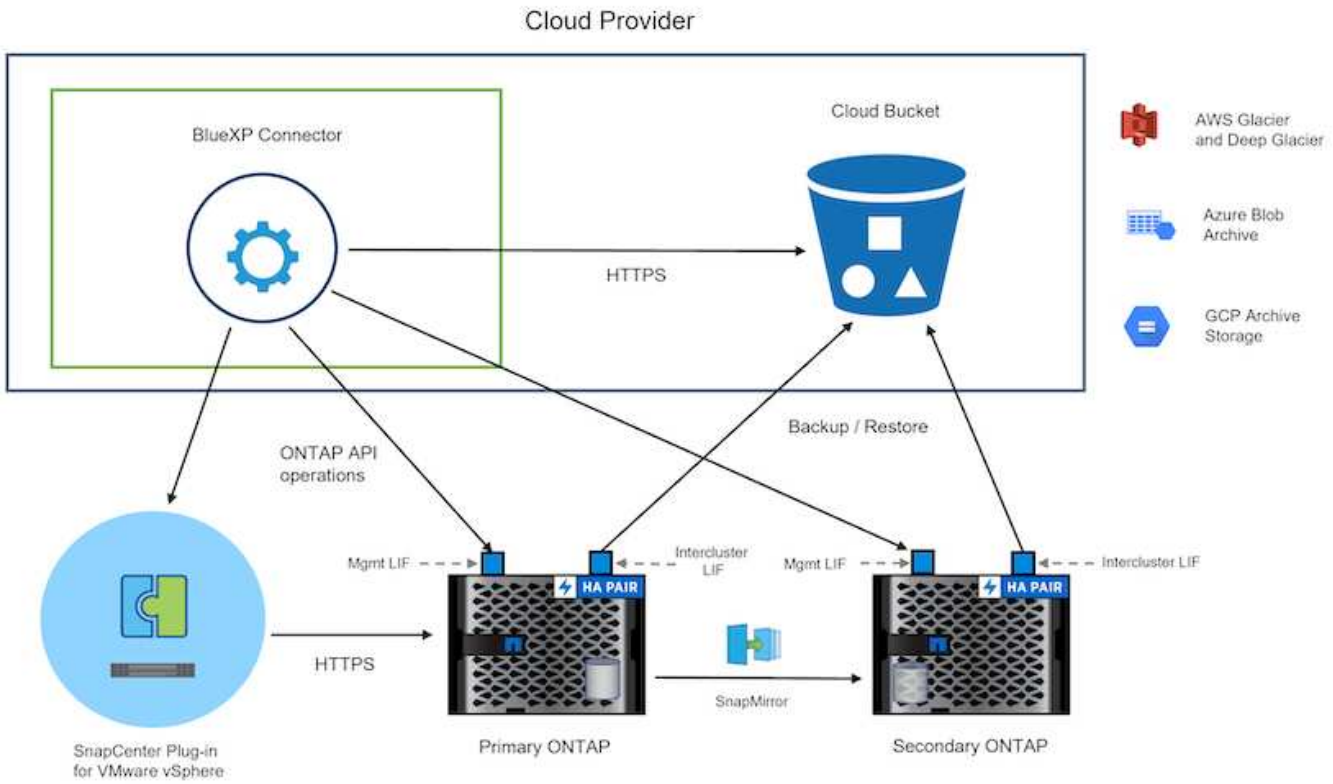
Prerequisiti

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

1. Cluster di storage ONTAP con datastore NFS o VMFS connessi a VMware vSphere. Sono supportati datastore NFS e VMFS. Per questa soluzione sono stati utilizzati datastore NFS.
2. Cluster di storage ONTAP secondario con relazioni SnapMirror stabilite per volumi usati per datastore NFS.
3. Connettore BlueXP installato per il cloud provider utilizzato per i backup dello storage a oggetti.
4. Le macchine virtuali di cui eseguire il backup si trovano su datastore NFS che si trovano sul cluster di storage ONTAP primario.
5. Connettività di rete tra il connettore BlueXP e le interfacce di gestione del cluster di storage ONTAP on-premise.
6. Connettività di rete tra il connettore BlueXP e la macchina virtuale di un'appliance SCV on-premise e tra il connettore BlueXP e vCenter.
7. Connettività di rete tra le LIF ONTAP on-premise e il servizio di storage a oggetti.
8. DNS configurato per l'SVM di gestione su cluster di storage ONTAP primari e secondari. Per ulteriori informazioni, fare riferimento a. "Configurare il DNS per la risoluzione del nome host".

Architettura di alto livello

Il test/convalida di questa soluzione è stato eseguito in un laboratorio che potrebbe corrispondere o meno all'ambiente di implementazione finale.



Implementazione della soluzione

Questa soluzione fornisce istruzioni dettagliate per l'implementazione e la convalida di una soluzione che utilizza il plug-in SnapCenter per VMware vSphere, oltre al backup e al recovery di BlueXP, per eseguire backup e recovery di macchine virtuali Windows e Linux all'interno di un cluster VMware vSphere situato in un data center on-premise. Le macchine virtuali di questo setup sono memorizzate su datastore NFS ospitati da un cluster di storage ONTAP A300. Inoltre, un cluster di storage ONTAP A300 separato funge da destinazione secondaria per i volumi replicati mediante SnapMirror. Inoltre, lo storage a oggetti ospitato su Amazon Web Services e Azure Blob è stato utilizzato come destinazione per una terza copia dei dati.

Ci occuperemo della creazione di relazioni SnapMirror per copie secondarie dei nostri backup gestiti da SCV e della configurazione dei lavori di backup nel backup e ripristino di SCV e BlueXP.

Per informazioni dettagliate sul plug-in SnapCenter per VMware vSphere, consultare la "Plug-in SnapCenter per la documentazione di VMware vSphere".

Per informazioni dettagliate sul backup e recovery di BlueXP, consulta la "Documentazione di backup e ripristino BlueXP".

Stabilire relazioni di SnapMirror tra cluster ONTAP

Il plug-in SnapCenter per VMware vSphere utilizza la tecnologia ONTAP SnapMirror per gestire il trasporto delle copie SnapMirror e/o SnapVault secondarie in un cluster ONTAP secondario.

Le policy di backup dei distributori idraulici possono utilizzare relazioni SnapMirror o SnapVault. La differenza principale consiste nel fatto che quando si utilizza l'opzione SnapMirror, la pianificazione della conservazione configurata per i backup nella policy sarà la stessa nelle posizioni principale e secondaria. SnapVault è progettato per l'archiviazione e, quando si utilizza questa opzione, è possibile stabilire una pianificazione della conservazione separata con la relazione di SnapMirror per le copie Snapshot sul cluster di storage ONTAP secondario.

La configurazione delle relazioni di SnapMirror può essere effettuata in BlueXP, dove molti dei passaggi sono automatizzati, o può essere fatta con System Manager e l'interfaccia a riga di comando di ONTAP. Tutti questi metodi sono discussi di seguito.

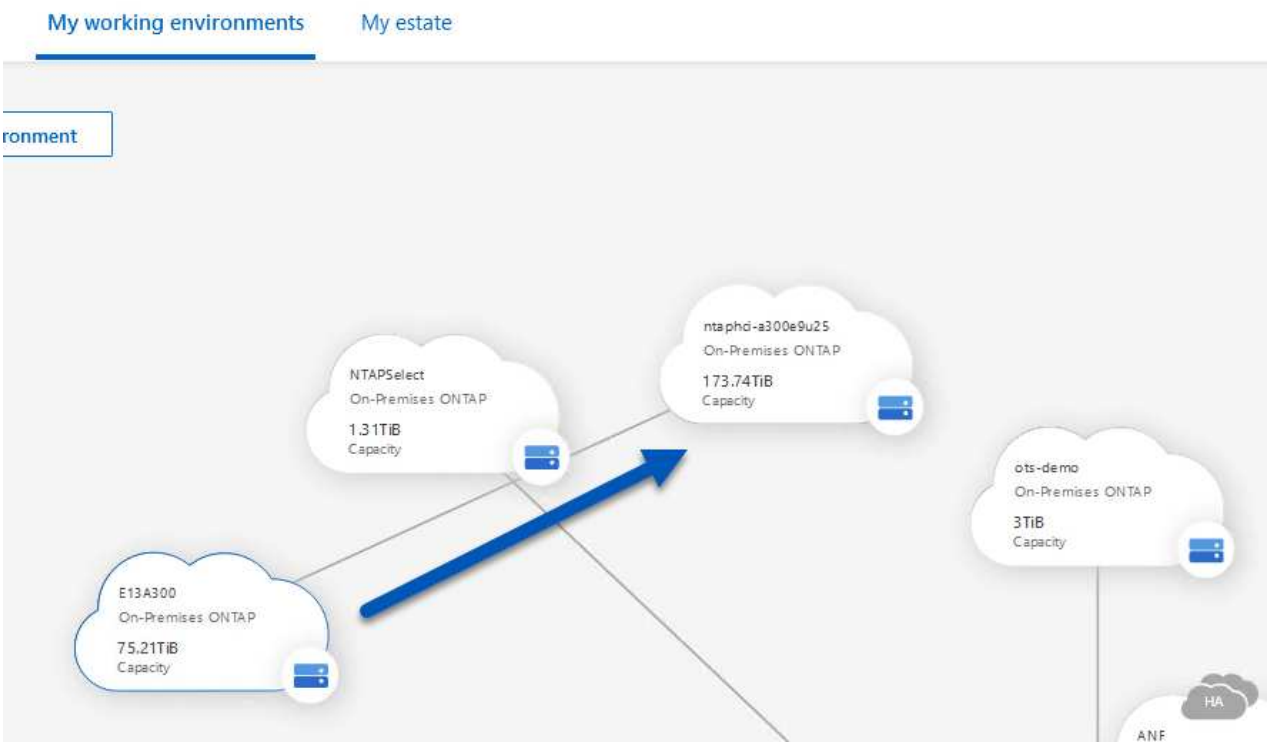
Stabilisci relazioni di SnapMirror con BlueXP

Dalla console web BlueXP devi completare i seguenti passaggi:

Configurazione della replica per sistemi di storage ONTAP primari e secondari

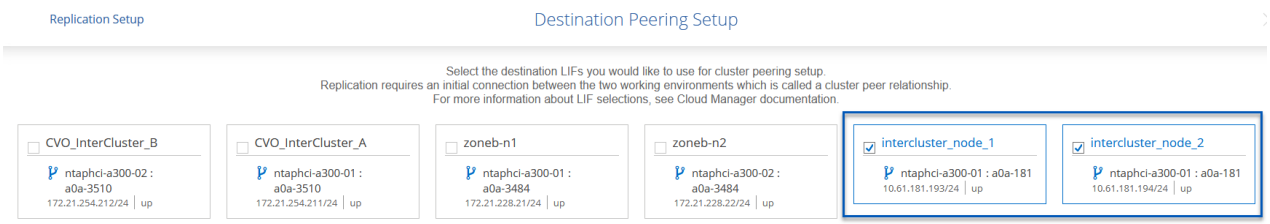
Iniziare accedendo alla console web BlueXP e navigando in Canvas.

1. Trascinare e rilasciare il sistema di storage ONTAP di origine (primario) nel sistema di storage ONTAP di destinazione (secondario).

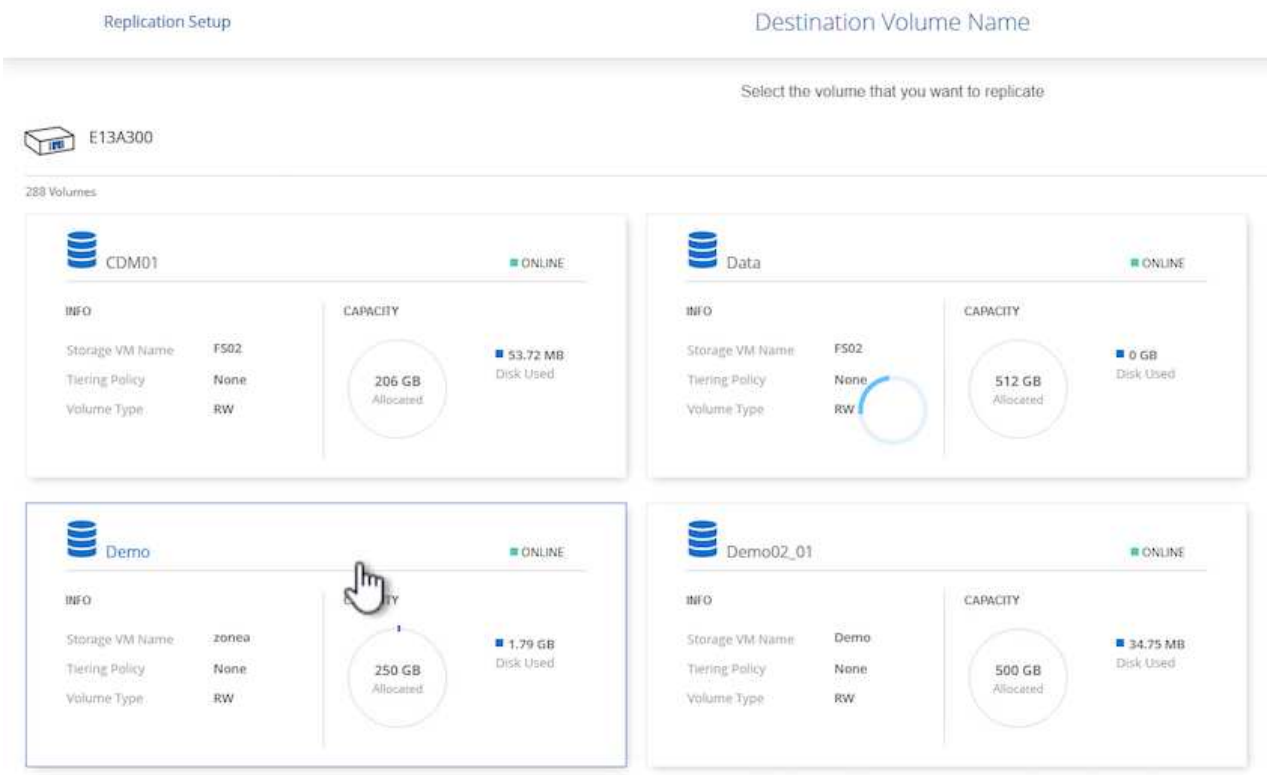


2. Dal menu visualizzato, selezionare **Replica**.

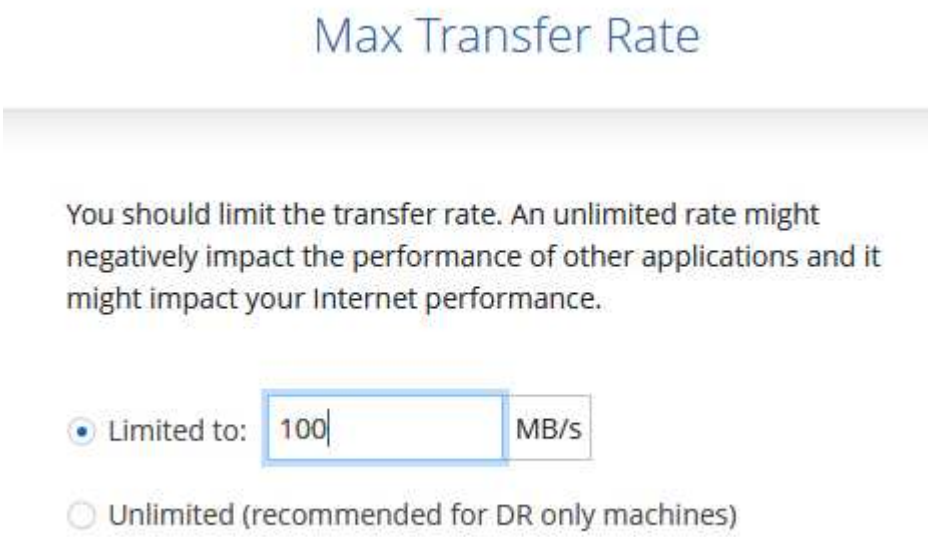
3. Nella pagina **impostazione peering di destinazione**, selezionare le LIF Intercluster di destinazione da utilizzare per la connessione tra sistemi storage.



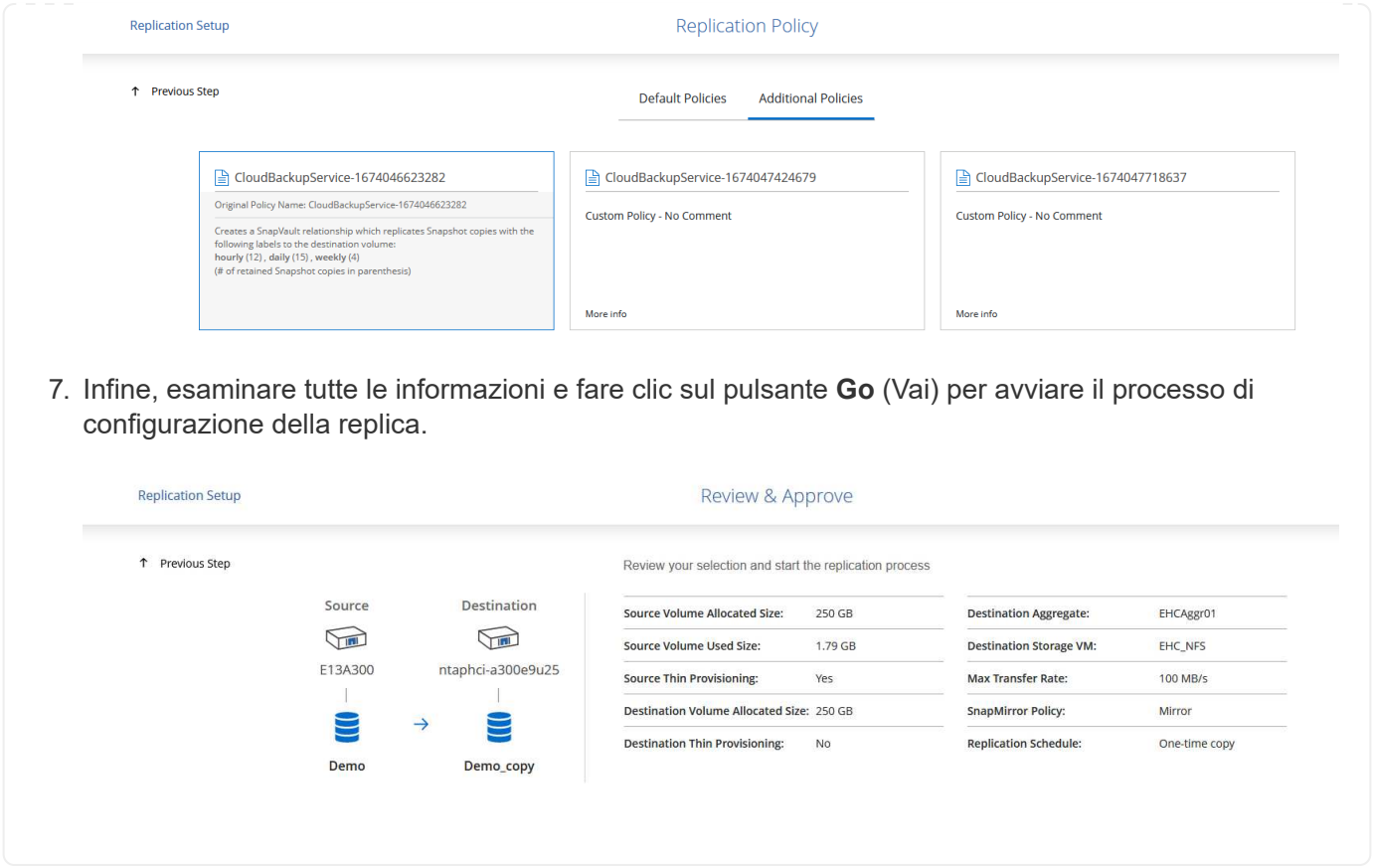
4. Nella pagina **Destination Volume Name** (Nome volume di destinazione), selezionare innanzitutto il volume di origine, quindi compilare il nome del volume di destinazione e selezionare la SVM e l'aggregato di destinazione. Fare clic su **Avanti** per continuare.



5. Scegliere la velocità di trasferimento massima alla quale eseguire la replica.



6. Scegliere il criterio che determinerà il programma di conservazione per i backup secondari. Questo criterio può essere creato in anticipo (vedere il processo manuale riportato di seguito nel passaggio **Crea un criterio di conservazione snapshot**) o può essere modificato in seguito, se lo si desidera.



7. Infine, esaminare tutte le informazioni e fare clic sul pulsante **Go** (Vai) per avviare il processo di configurazione della replica.

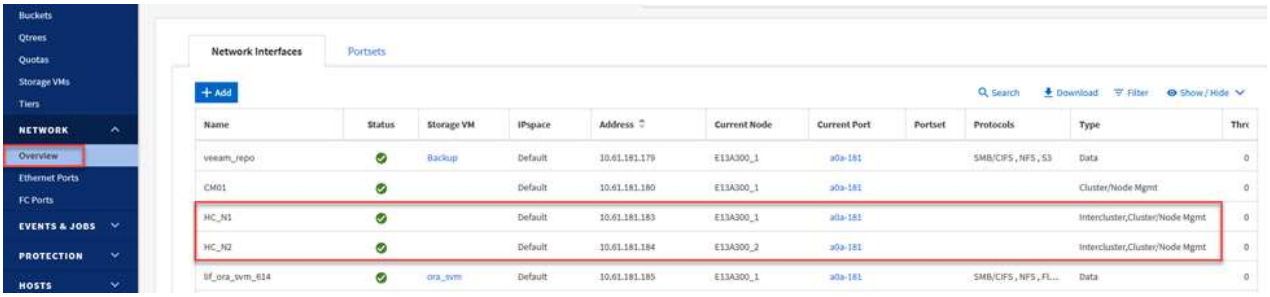
Stabilire relazioni di SnapMirror con System Manager e la CLI di ONTAP

Tutti i passaggi necessari per stabilire le relazioni SnapMirror possono essere eseguiti con System Manager o la CLI di ONTAP. La sezione seguente fornisce informazioni dettagliate su entrambi i metodi:

Registrare le interfacce logiche Intercluster di origine e destinazione

Per i cluster ONTAP di origine e di destinazione, puoi recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

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



2. Per recuperare gli indirizzi IP di Intercluster utilizzando l'interfaccia CLI, eseguire il seguente comando:

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

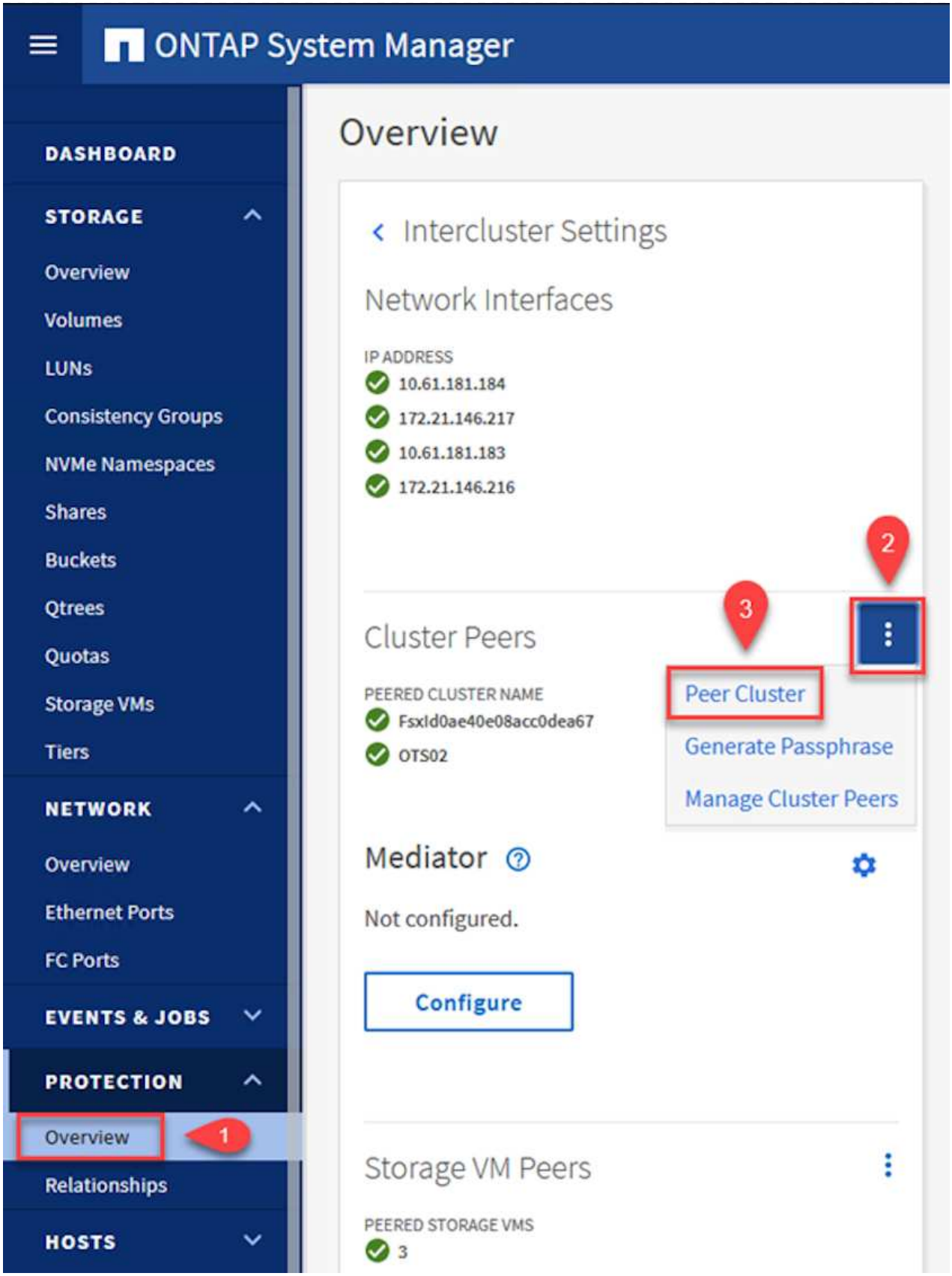
Stabilisci il peering dei cluster tra i cluster ONTAP

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

1. Impostare il peering sul cluster ONTAP di destinazione utilizzando l' `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca da utilizzare in seguito nel cluster di origine per completare il processo di creazione.

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

2. Nel cluster di origine, è possibile stabilire la relazione peer del cluster utilizzando Gestore di sistema di ONTAP o l'interfaccia CLI. Da Gestore di sistema di ONTAP, accedere a protezione > Panoramica e selezionare cluster peer.

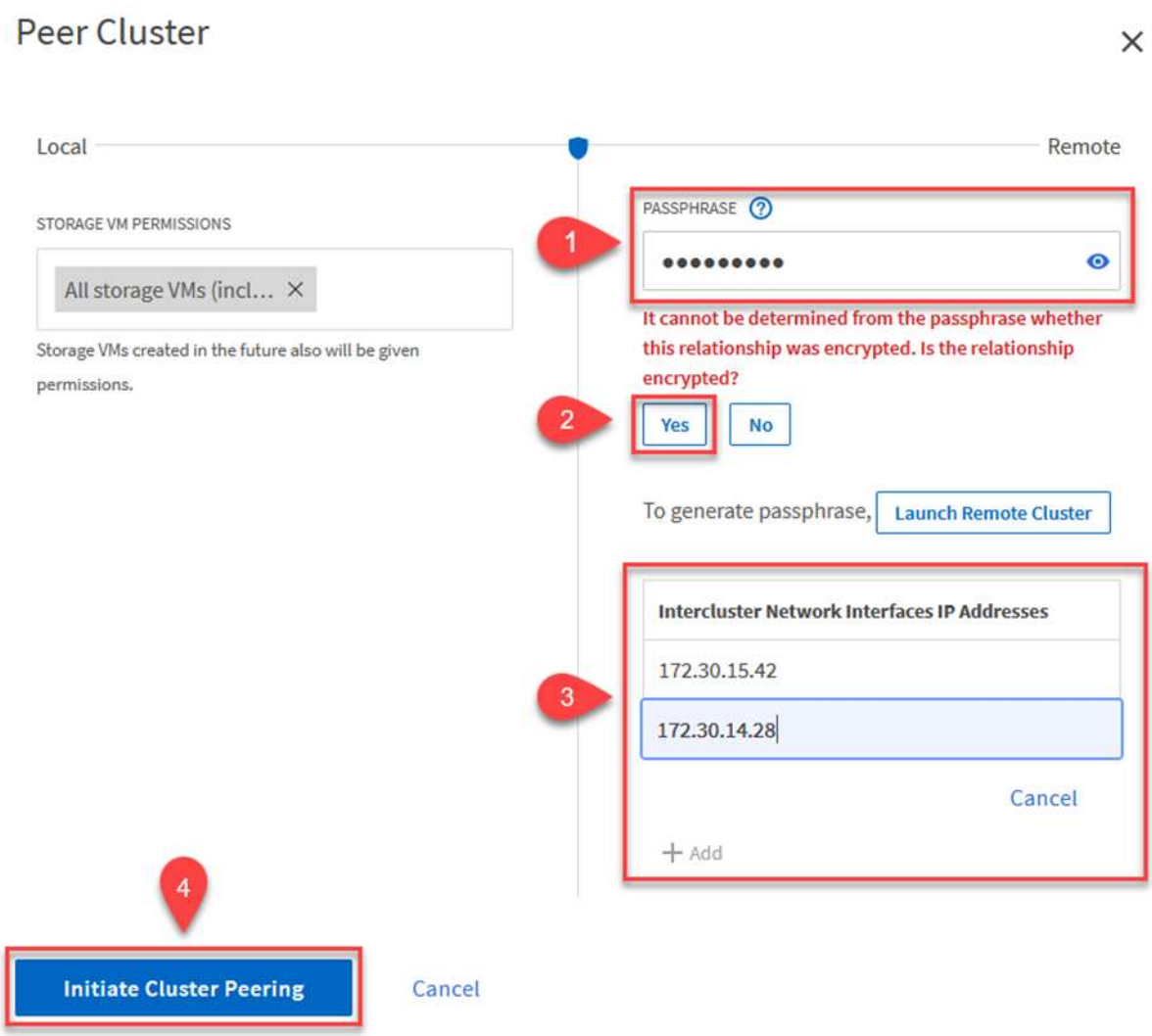


3. Nella finestra di dialogo Peer Cluster, inserire le informazioni richieste:
   a. Immettere la passphrase utilizzata per stabilire la relazione del cluster peer nel cluster ONTAP di destinazione.

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

c. Inserire l'indirizzo IP intercluster LIF del cluster ONTAP di destinazione.

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



4. Verificare lo stato della relazione di peer del cluster dal cluster ONTAP di destinazione con il seguente comando:

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

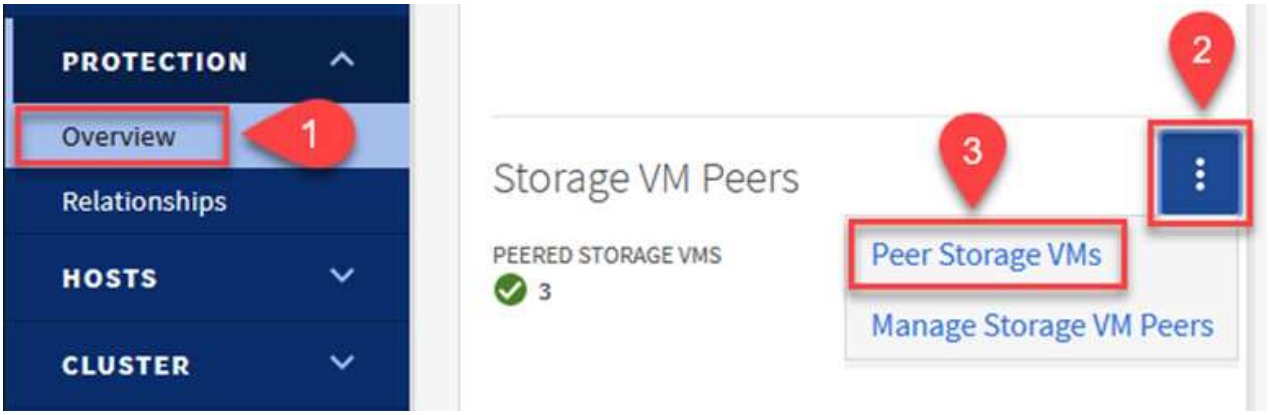
Stabilire una relazione di peering SVM

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

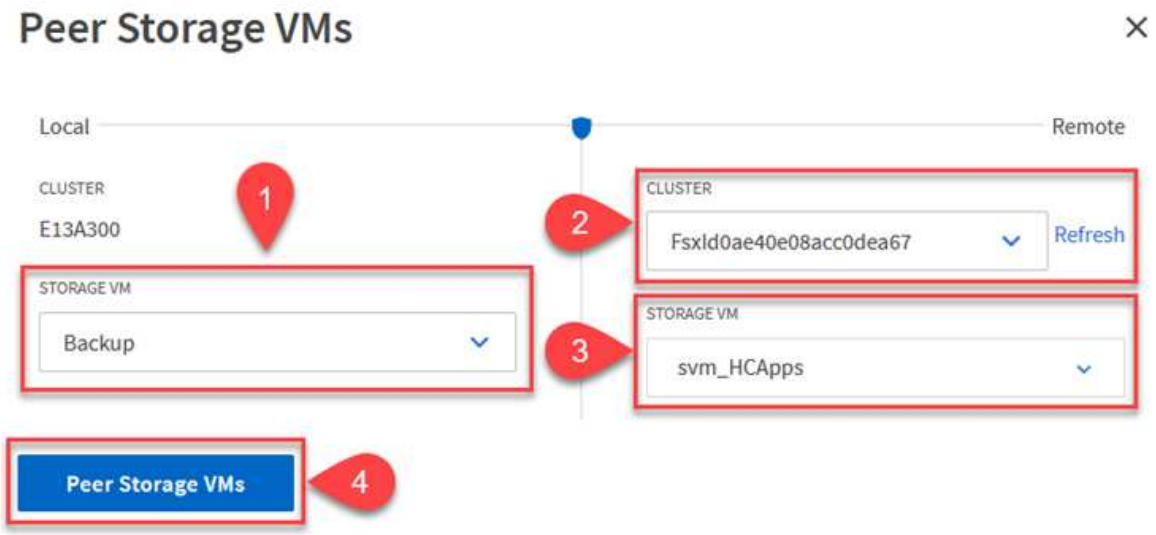
1. Dal cluster ONTAP di destinazione, utilizza il seguente comando dall'interfaccia CLI per creare la relazione peer SVM:

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

2. Dal cluster ONTAP di origine, accettare la relazione di peering con Gestore di sistema ONTAP o CLI.
3. Da Gestore di sistema ONTAP, andare a protezione > Panoramica e selezionare le VM di storage peer in peer di macchine virtuali di storage.



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



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

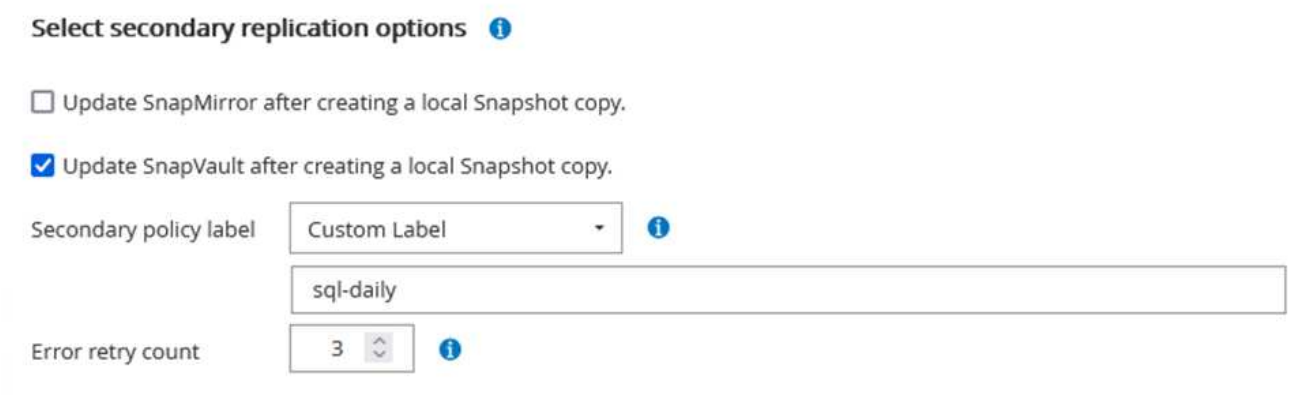
Creare un criterio di conservazione delle snapshot

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

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

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

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



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

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

1. Creare il criterio SnapMirror sul cluster FSX.

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

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

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

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

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

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

Creare volumi di destinazione

Per creare un volume di destinazione su ONTAP che sarà destinatario di copie Snapshot dai volumi di origine, esegui il seguente comando sul cluster ONTAP di destinazione:

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

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

Per creare una relazione di SnapMirror tra un volume di origine e di destinazione, esegui il seguente comando sul cluster ONTAP di destinazione:

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

Inizializzare le relazioni di SnapMirror

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

Per creare un volume, esegui il seguente comando sul cluster ONTAP di destinazione:

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

Configurare il plug-in SnapCenter per VMware vSphere

Una volta installato, è possibile accedere al plug-in SnapCenter per VMware vSphere dall'interfaccia di gestione dell'appliance vCenter Server. SCV gestirà i backup degli archivi dati NFS montati sugli host ESXi e che contengono le macchine virtuali Windows e Linux.

Esaminare "Workflow di data Protection" Sezione della documentazione del distributore idraulico per ulteriori

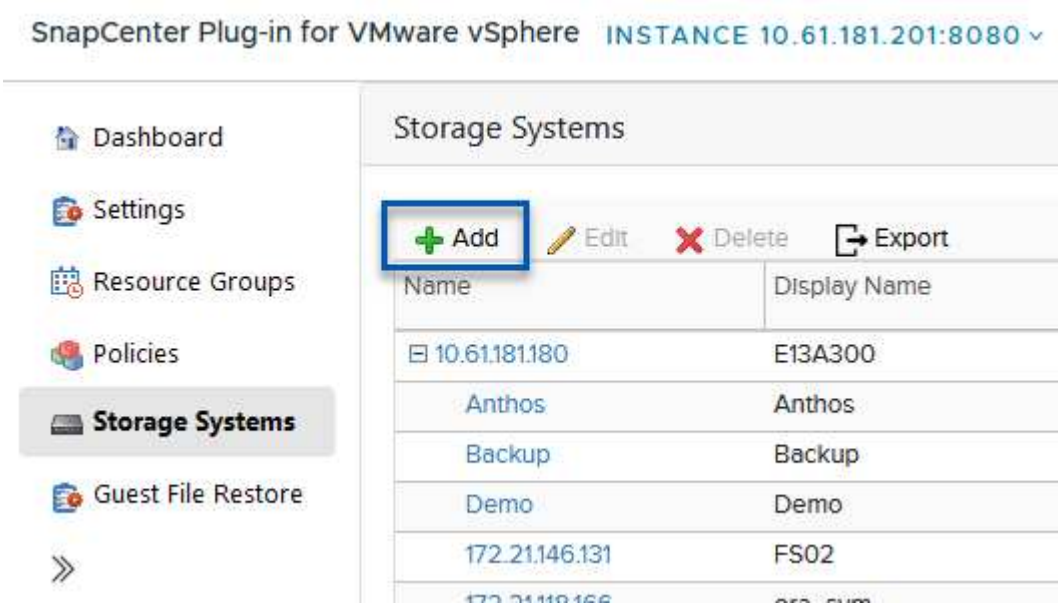
informazioni sulle fasi di configurazione dei backup.

Per configurare backup di macchine virtuali e datastore, è necessario completare i seguenti passaggi dall'interfaccia del plug-in.

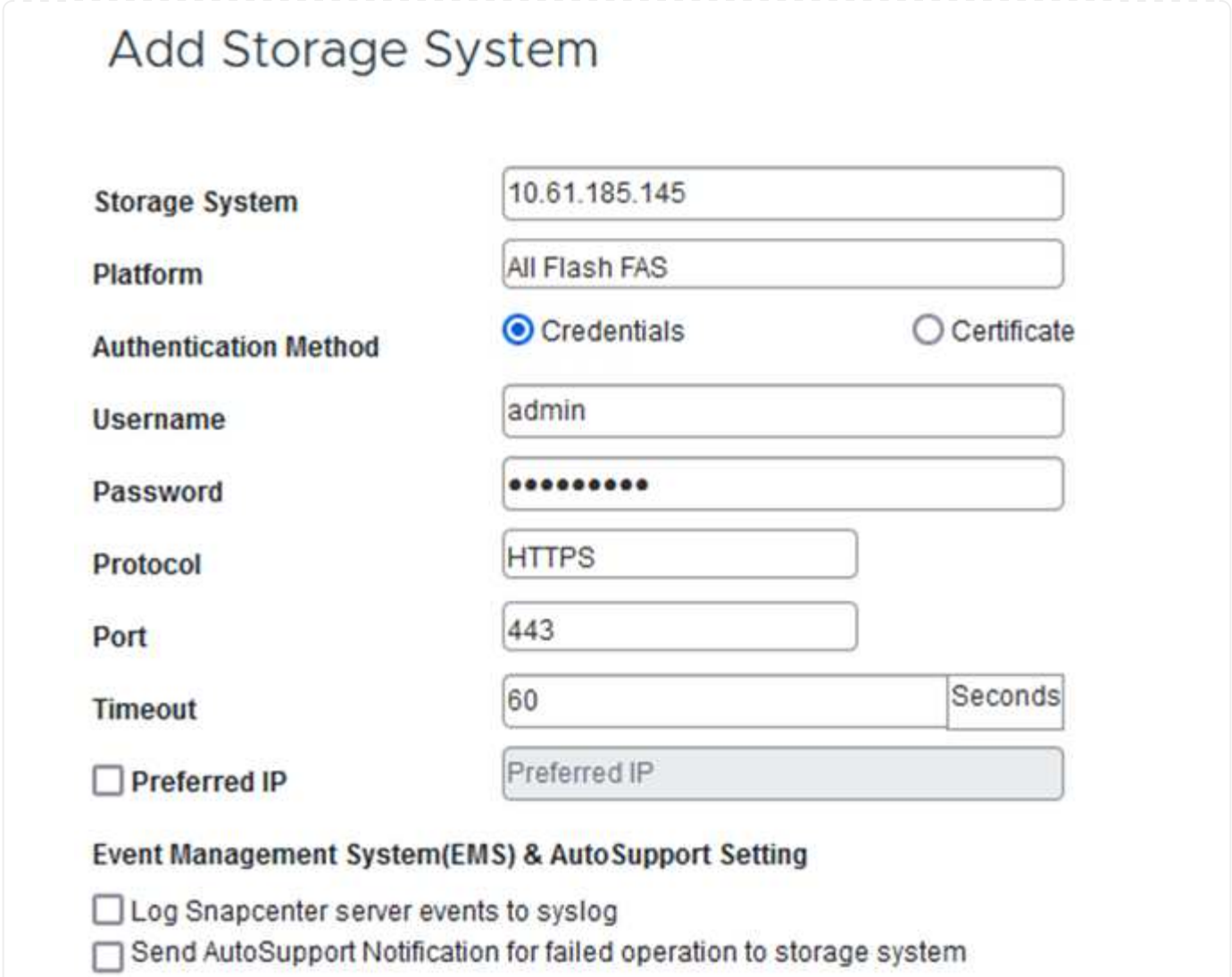
Sistemi storage Discovery ONTAP

Scopri i cluster di storage ONTAP da utilizzare per il backup primario e secondario.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **sistemi di archiviazione** nel menu a sinistra e fare clic sul pulsante **Aggiungi**.



2. Compilare le credenziali e il tipo di piattaforma per il sistema di storage ONTAP primario e fare clic su **Aggiungi**.



3. Ripetere questa procedura per il sistema di storage ONTAP secondario.

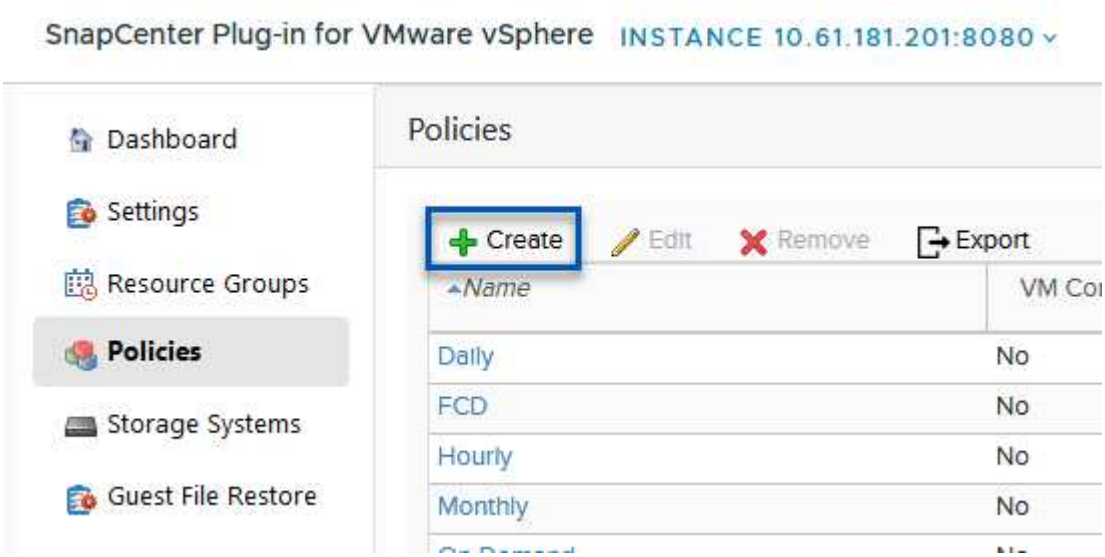
Creare le politiche di backup dei distributori idraulici

I criteri specificano il periodo di conservazione, la frequenza e le opzioni di replica per i backup gestiti da SCV.

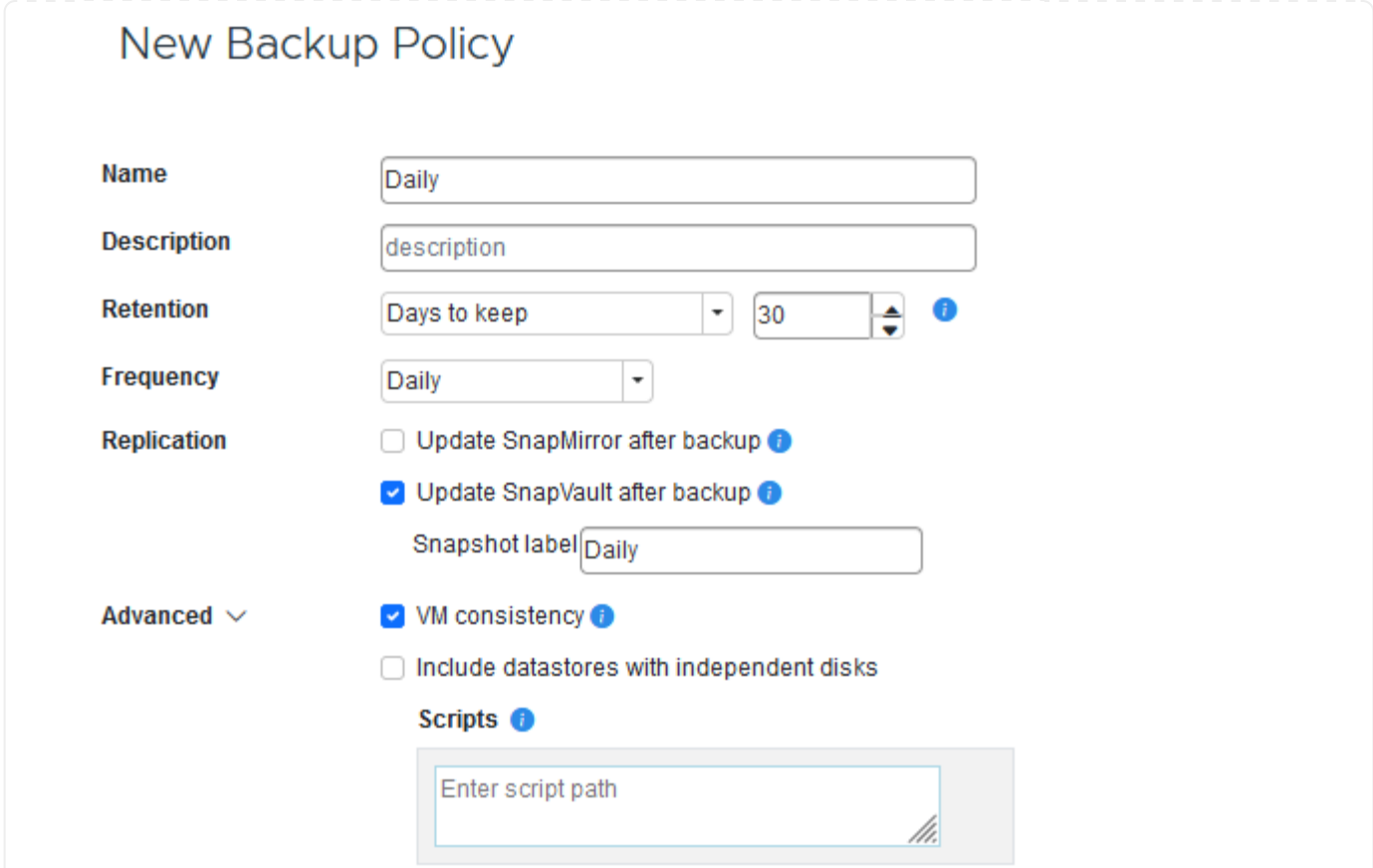
Esaminare "Creare policy di backup per macchine virtuali e datastore" della documentazione per ulteriori informazioni.

Per creare i criteri di backup, attenersi alla seguente procedura:

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **Policies** nel menu a sinistra e fare clic sul pulsante **Create**.



2. Specificare un nome per il criterio, il periodo di conservazione, la frequenza e le opzioni di replica e l'etichetta dello snapshot.



Quando si crea una policy nel plug-in di SnapCenter sono visualizzate le opzioni per SnapMirror e SnapVault. Scegliendo SnapMirror, il programma di conservazione specificato nella policy sarà lo stesso per gli snapshot primari e secondari. Scegliendo SnapVault, il programma di conservazione per la snapshot secondaria si baserà su una pianificazione separata implementata con la relazione di SnapMirror. Questa funzione è utile quando si desiderano periodi di conservazione più lunghi per backup secondari.

Le etichette degli Snapshot sono utili per attuare policy con uno specifico periodo di conservazione per le copie SnapVault replicate nel cluster ONTAP secondario. Quando SCV viene utilizzato con il backup e ripristino di BlueXP, il campo dell'etichetta dell'istantanea deve essere vuoto oppure match l'etichetta specificata nel criterio di backup di BlueXP.

3. Ripetere la procedura per ogni criterio richiesto. Ad esempio, separare i criteri per i backup giornalieri, settimanali e mensili.

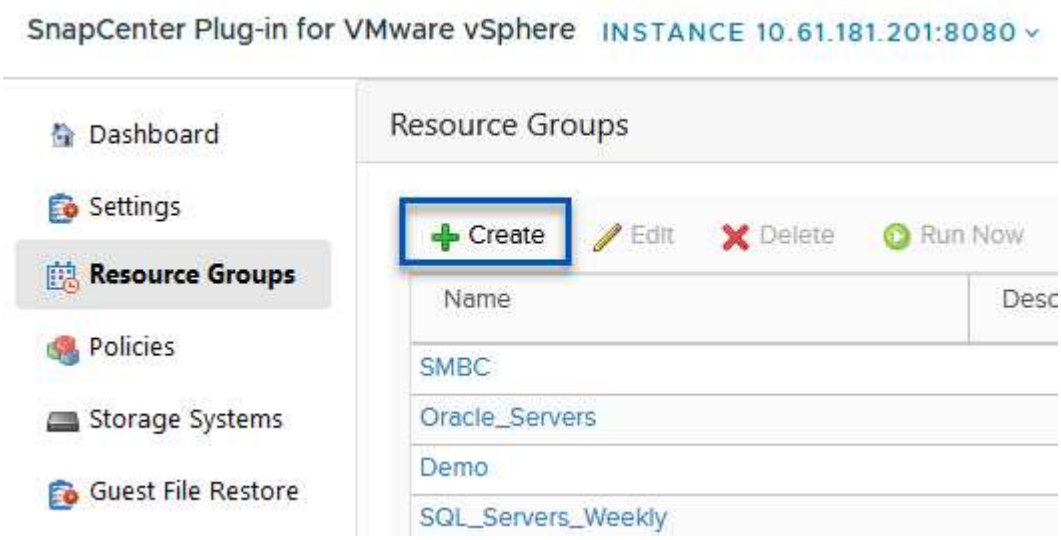
Creare gruppi di risorse

I gruppi di risorse contengono gli archivi dati e le macchine virtuali da includere in un processo di backup, insieme ai criteri e alla pianificazione di backup associati.

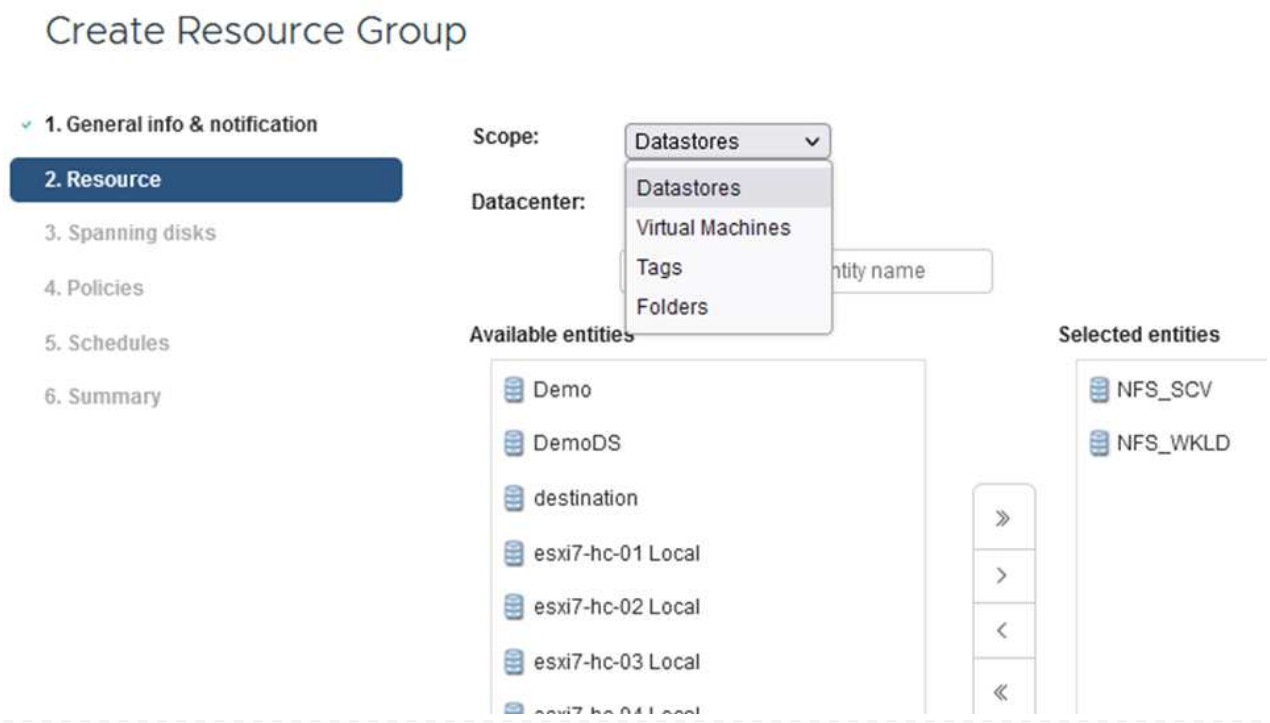
Esaminare "Creare gruppi di risorse" della documentazione per ulteriori informazioni.

Per creare gruppi di risorse, completare i seguenti passaggi.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **gruppi di risorse** nel menu a sinistra e fare clic sul pulsante **Crea**.

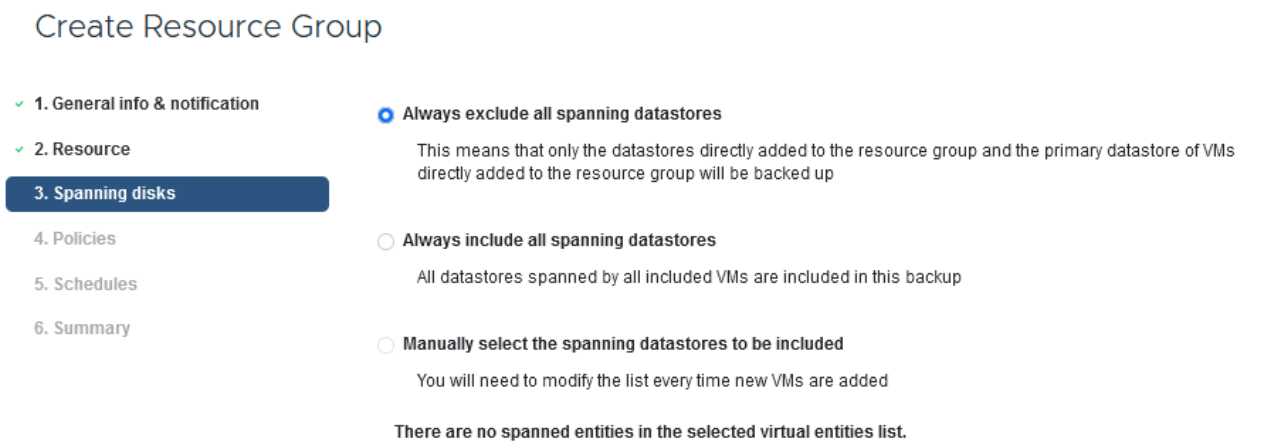


2. Nella procedura guidata Crea gruppo di risorse, immettere un nome e una descrizione per il gruppo, nonché le informazioni necessarie per ricevere le notifiche. Fare clic su **Avanti**
3. Nella pagina successiva selezionare i datastore e le macchine virtuali che si desidera includere nel processo di backup, quindi fare clic su **Avanti**.



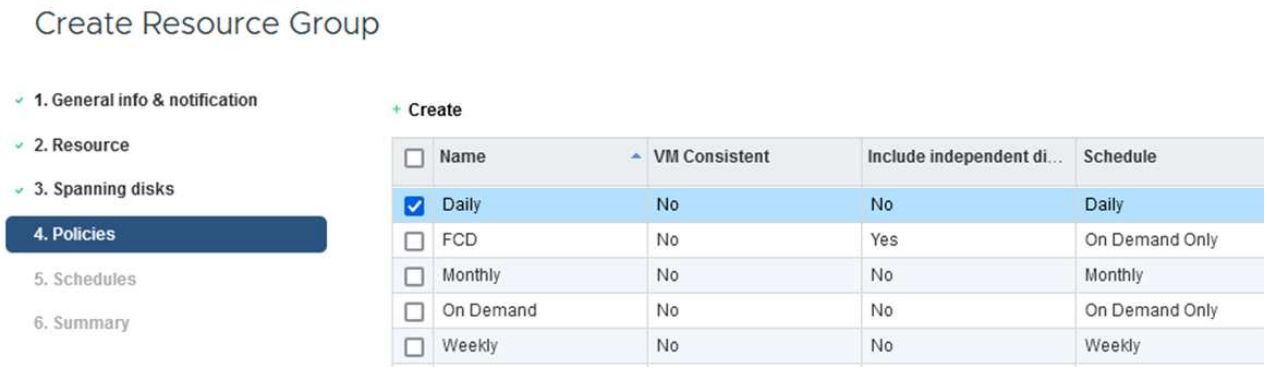
Hai la possibilità di selezionare macchine virtuali specifiche o interi datastore. Indipendentemente dal tipo di scelta effettuata, viene eseguito il backup dell'intero volume (e datastore) poiché il backup è il risultato di una snapshot del volume sottostante. Nella maggior parte dei casi, è più semplice scegliere l'intero datastore. Tuttavia, se si desidera limitare l'elenco delle VM disponibili durante il ripristino, è possibile scegliere solo un sottoinsieme di VM per il backup.

4. Scegli le opzioni per l'estensione dei datastore per le macchine virtuali con VMDK che risiedono in più datastore e fai clic su **Avanti**.



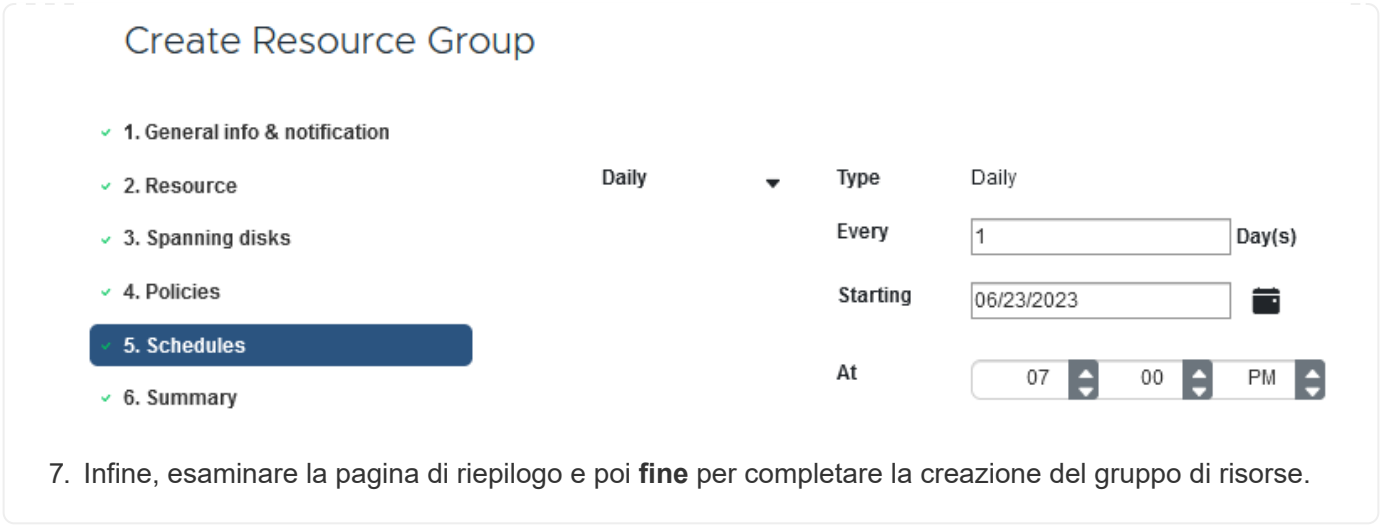
Il backup e recovery di BlueXP non supporta al momento il backup di macchine virtuali con VMDK che coprono più datastore.

5. Nella pagina successiva, selezionare i criteri da associare al gruppo di risorse e fare clic su **Avanti**.



Quando si esegue il backup di snapshot gestite da SCV su storage a oggetti utilizzando il backup e ripristino di BlueXP, ogni gruppo di risorse può essere associato solo a una singola policy.

6. Selezionare una pianificazione che determinerà a quale ora verranno eseguiti i backup. Fare clic su **Avanti**.

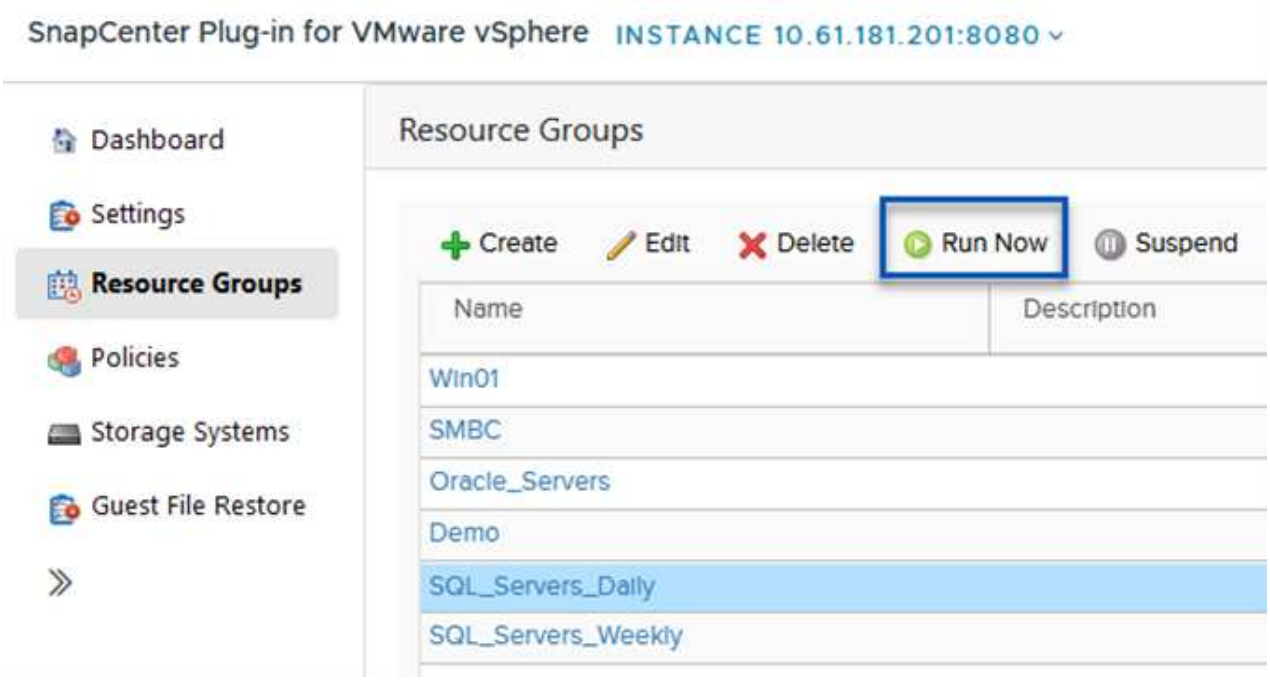


7. Infine, esaminare la pagina di riepilogo e poi **fine** per completare la creazione del gruppo di risorse.

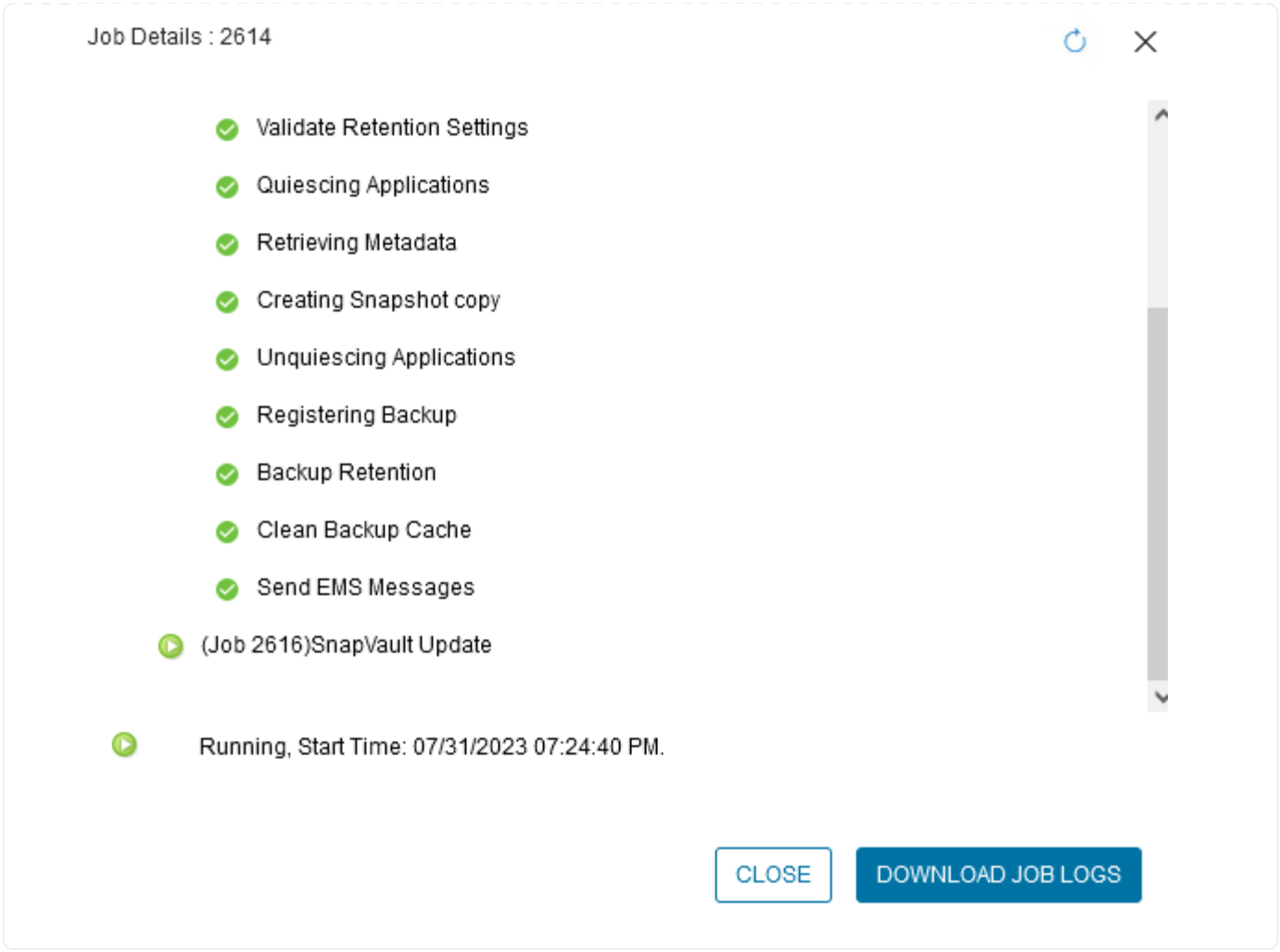
Eseguire un processo di backup

In questa fase finale, eseguire un lavoro di backup e monitorarne l'avanzamento. Almeno un processo di backup deve essere completato correttamente in SCV prima di poter rilevare le risorse dal backup e ripristino di BlueXP.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **gruppi di risorse** nel menu a sinistra.
2. Per avviare un processo di backup, selezionare il gruppo di risorse desiderato e fare clic sul pulsante **Esegui ora**.



3. Per monitorare il processo di backup, accedere a **Dashboard** nel menu a sinistra. In **attività processo recenti** fare clic sul numero ID processo per monitorare l'avanzamento del processo.



Configura i backup sullo storage a oggetti nel backup e recovery di BlueXP

Per consentire a BlueXP di gestire l'infrastruttura dati in modo efficace, richiede la previa installazione di un connettore. Il connettore esegue le azioni necessarie per rilevare le risorse e gestire le operazioni sui dati.

Per ulteriori informazioni sul connettore BlueXP, fare riferimento a. "Scopri di più sui connettori" Nella documentazione BlueXP.

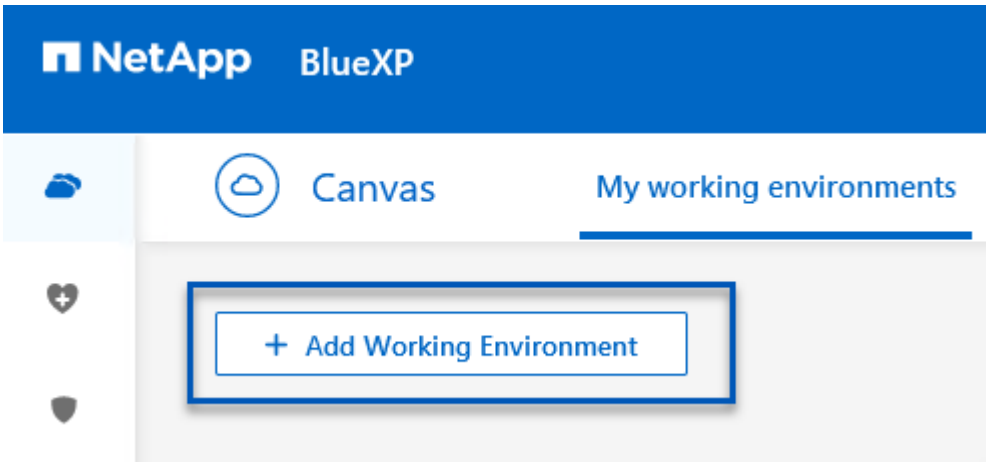
Una volta installato il connettore per il cloud provider utilizzato, una rappresentazione grafica dell'archivio oggetti sarà visibile da Canvas.

Per configurare il backup e ripristino BlueXP sui dati di backup gestiti da SCV on-premise, attenersi alla seguente procedura:

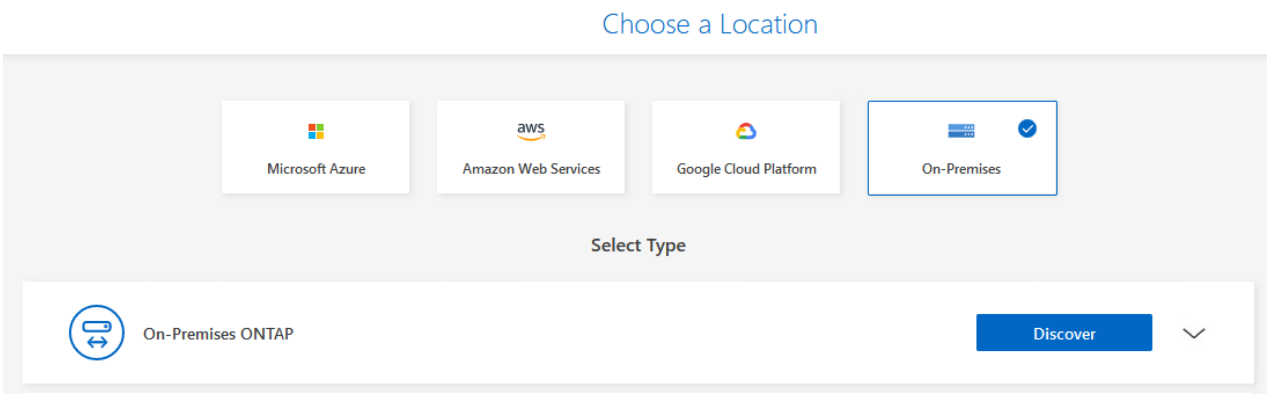
Aggiungere ambienti di lavoro al Canvas

Il primo passo è aggiungere i sistemi storage ONTAP on-premise ad BlueXP

1. Da Canvas selezionare **Aggiungi ambiente di lavoro** per iniziare.



2. Selezionare **on-Premises** (locale) dalla scelta delle località, quindi fare clic sul pulsante **Discover** (rileva).



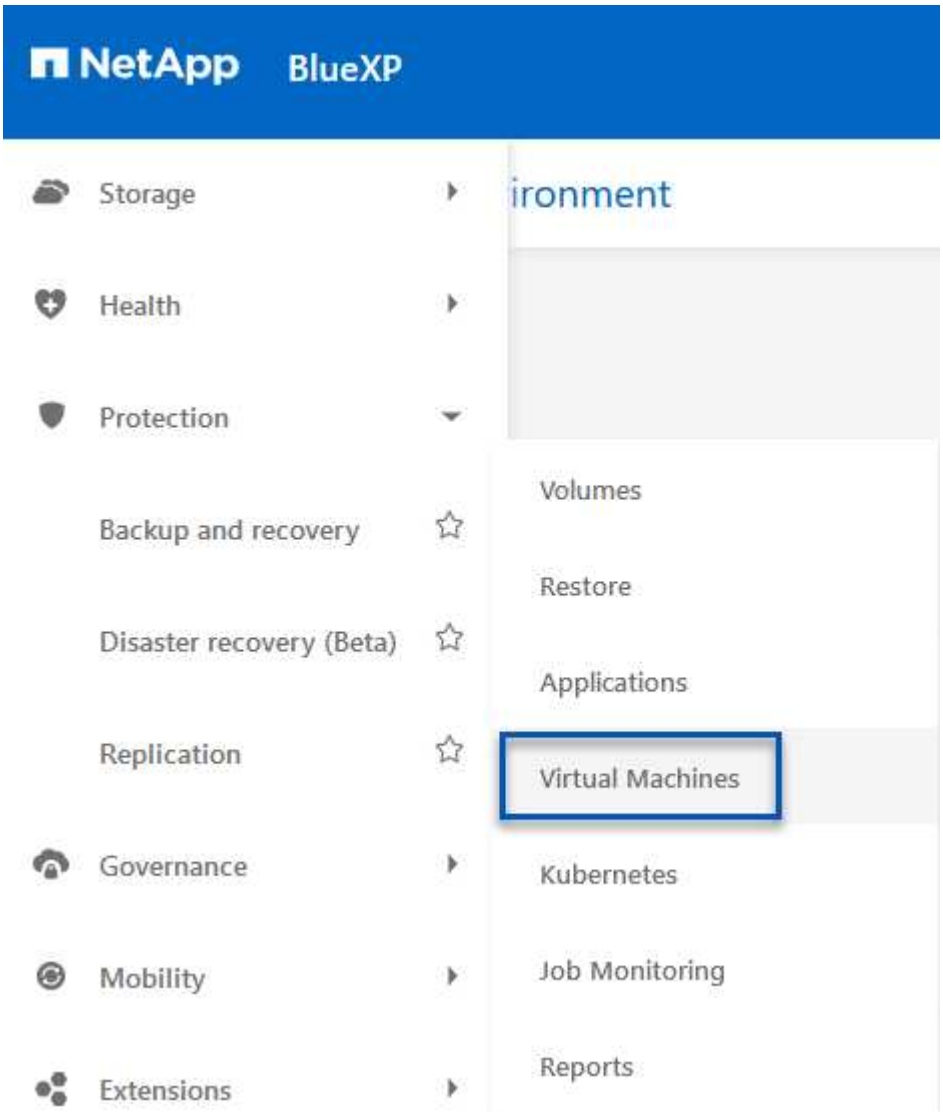
3. Compilare le credenziali per il sistema di archiviazione ONTAP e fare clic sul pulsante **Scopri** per aggiungere l'ambiente di lavoro.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

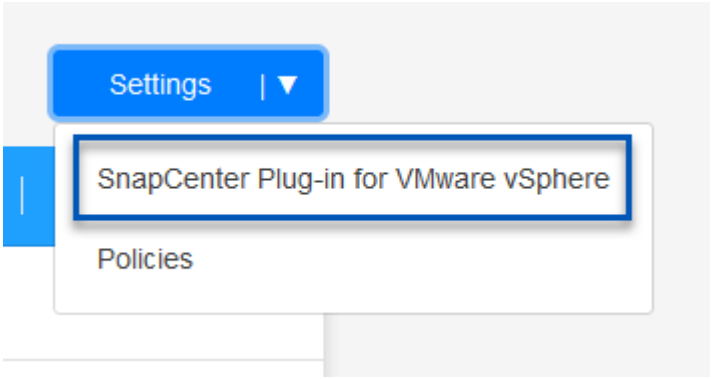
Scopri SCV appliance e vCenter on-premise

Per rilevare il datastore on-premise e le risorse delle macchine virtuali, Aggiungi le informazioni per il broker di dati SCV e le credenziali per l'appliance di gestione vCenter.

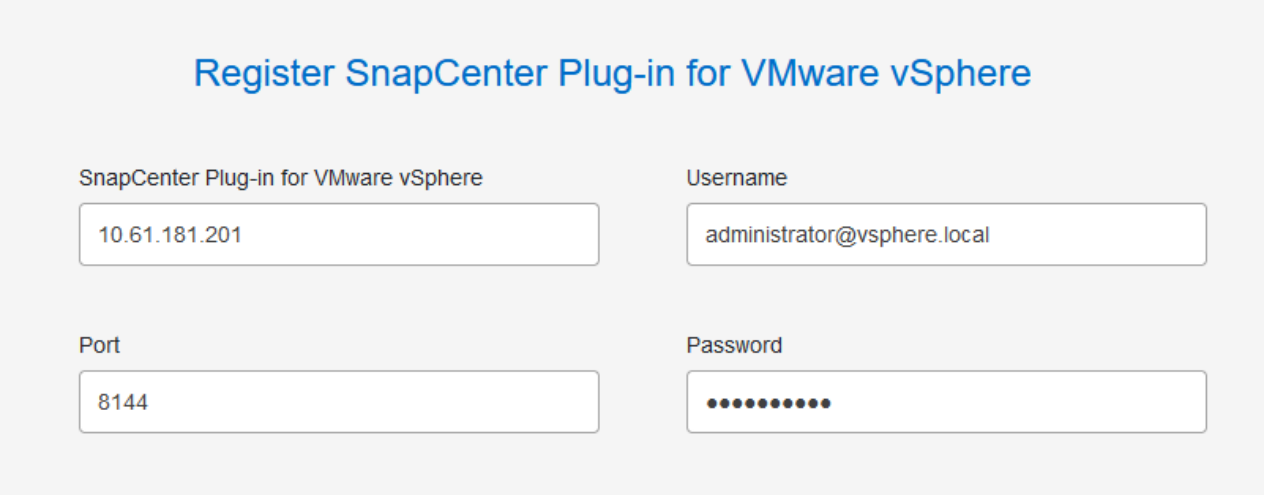
1. Dal menu a sinistra di BlueXP, selezionare **protezione > Backup e ripristino > macchine virtuali**



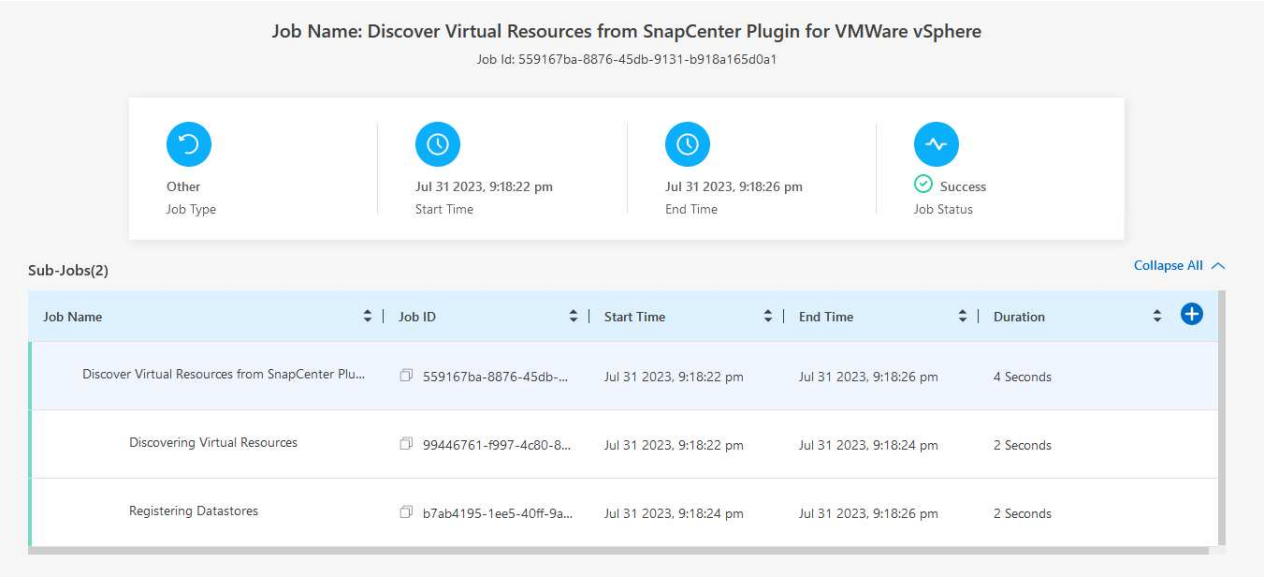
2. Dalla schermata principale macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare **Plug-in SnapCenter per VMware vSphere**.



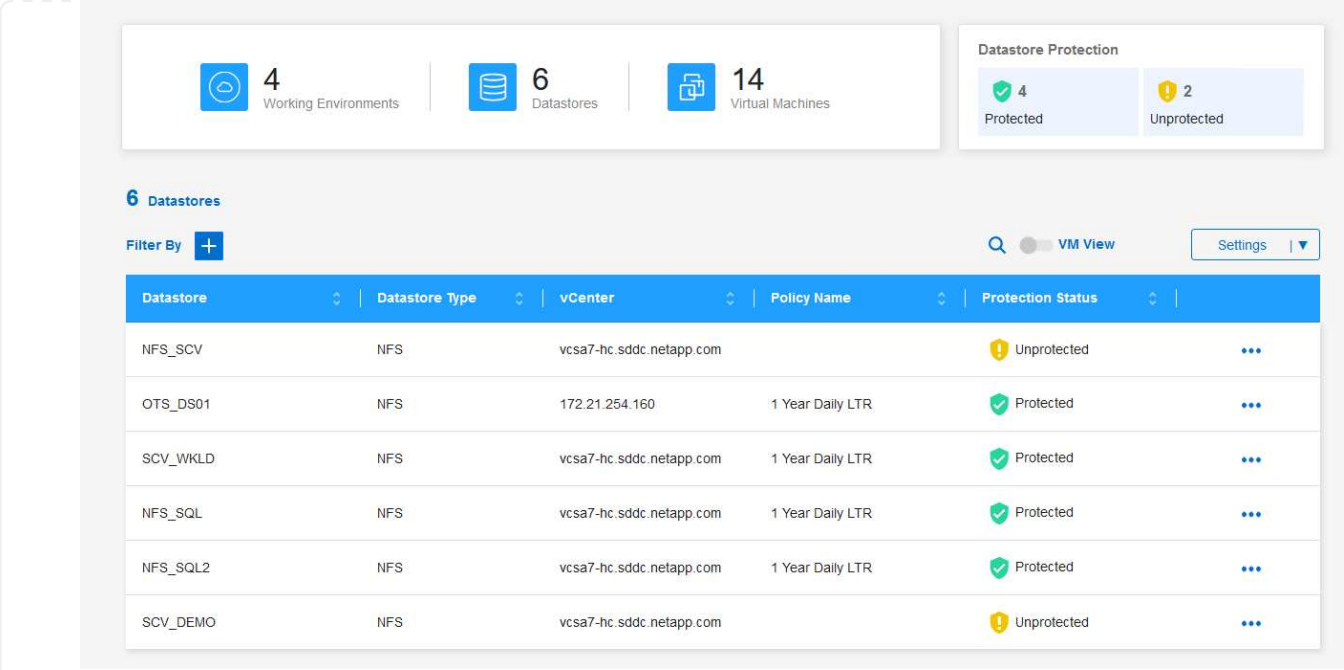
3. Fare clic sul pulsante **Registra**, quindi immettere l'indirizzo IP e il numero di porta per l'appliance plug-in SnapCenter e il nome utente e la password per l'appliance di gestione vCenter. Fare clic sul pulsante **Registra** per avviare il processo di ricerca.



4. È possibile monitorare l'avanzamento dei lavori dalla scheda monitoraggio processi.



5. Una volta completato il rilevamento, sarà possibile visualizzare i datastore e le macchine virtuali in tutti gli apparecchi SCV rilevati.

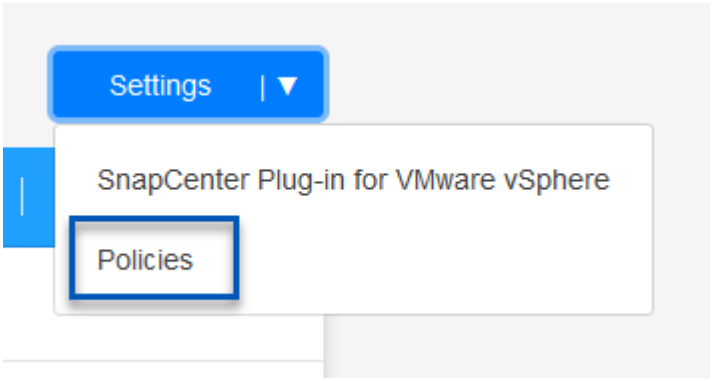

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV NFS vcsa7-hc.sddc.netapp.com Unprotected
OTS_DS01 NFS 172.21.254.160 1 Year Daily LTR Protected
SCV_WKLD NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
NFS_SQL NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
NFS_SQL2 NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
SCV_DEMO NFS vcsa7-hc.sddc.netapp.com Unprotected

Crea policy di backup BlueXP

Nel backup e recovery di BlueXP per le macchine virtuali, crea policy per specificare il periodo di conservazione, l'origine di backup e la policy di archiviazione.

Per ulteriori informazioni sulla creazione dei criteri, consultare "Creare una policy per il backup dei datastore".

1. Dalla pagina principale di backup e ripristino di BlueXP per le macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare **Criteri**.



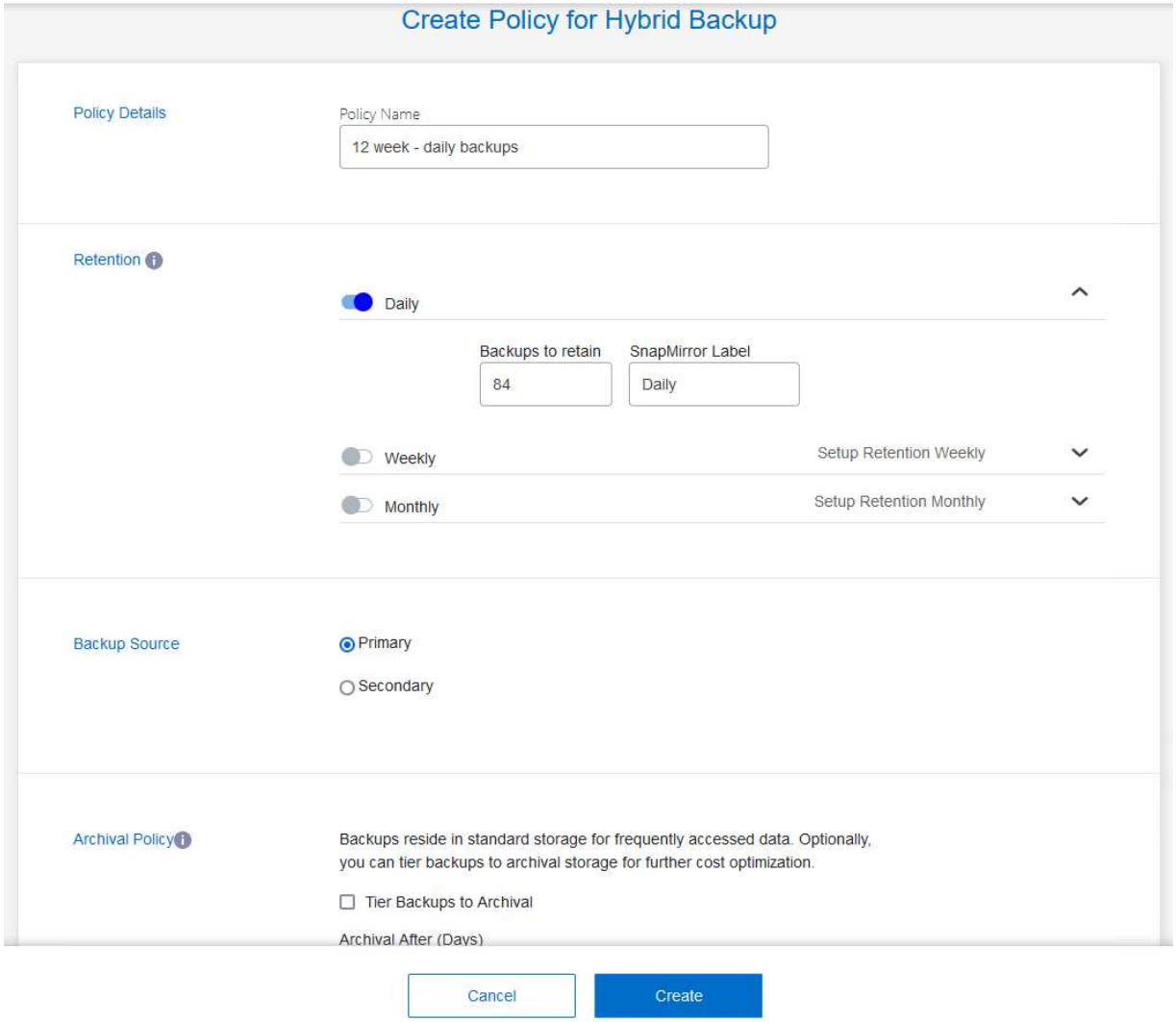
2. Fare clic su **Crea criterio** per accedere alla finestra **Crea criterio per il backup ibrido**.

   a. Aggiungere un nome per il criterio

   b. Selezionare il periodo di conservazione desiderato

   c. Seleziona se i backup devono provenire dal sistema di storage ONTAP on-premise primario o secondario

   d. In alternativa, è possibile specificare, dopo il periodo di tempo, il tiering dei backup nello storage di archivio, ottenendo ulteriori risparmi sui costi.



L'etichetta SnapMirror immessa qui viene utilizzata per identificare i backup da applicare anche la policy. Il nome dell'etichetta deve corrispondere al nome dell'etichetta nella politica SCV in loco corrispondente.

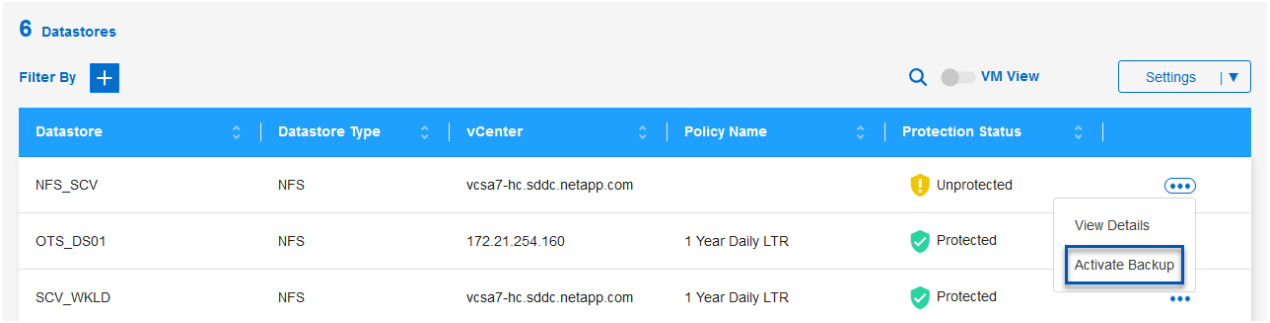
3. Fare clic su **Crea** per completare la creazione del criterio.

Effettuare il backup dei datastore su Amazon Web Services

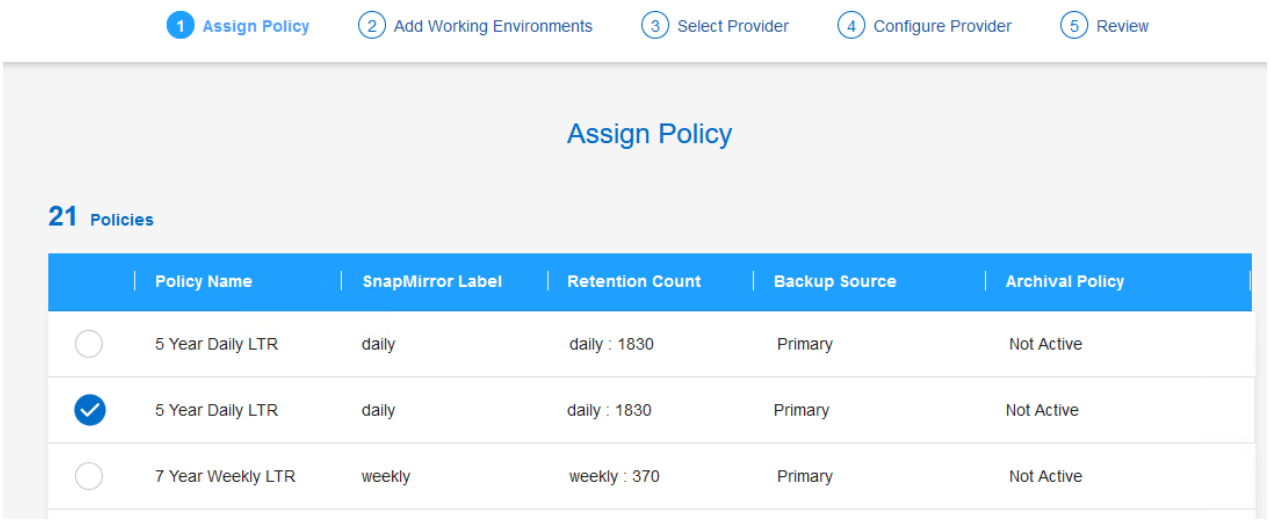
L'ultima fase consiste nell'attivare la data Protection per i singoli datastore e le macchine virtuali. Segue una descrizione della modalità di attivazione dei backup in AWS.

Per ulteriori informazioni, fare riferimento a. "Eseguire il backup dei datastore su Amazon Web Services".

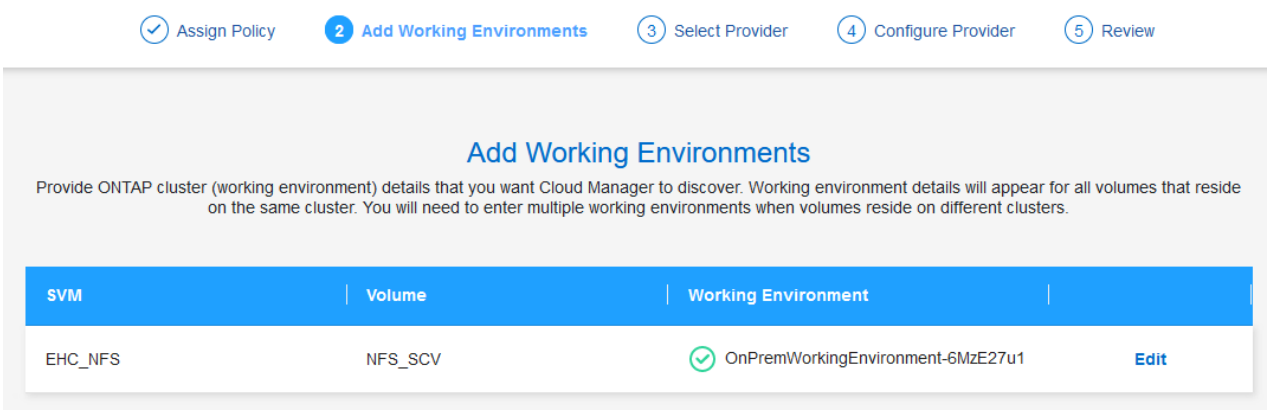
1. Dalla pagina principale di backup e recovery di BlueXP per le macchine virtuali, accedi al menu a discesa delle impostazioni per il datastore da sottoporre a backup e seleziona **attiva backup**.



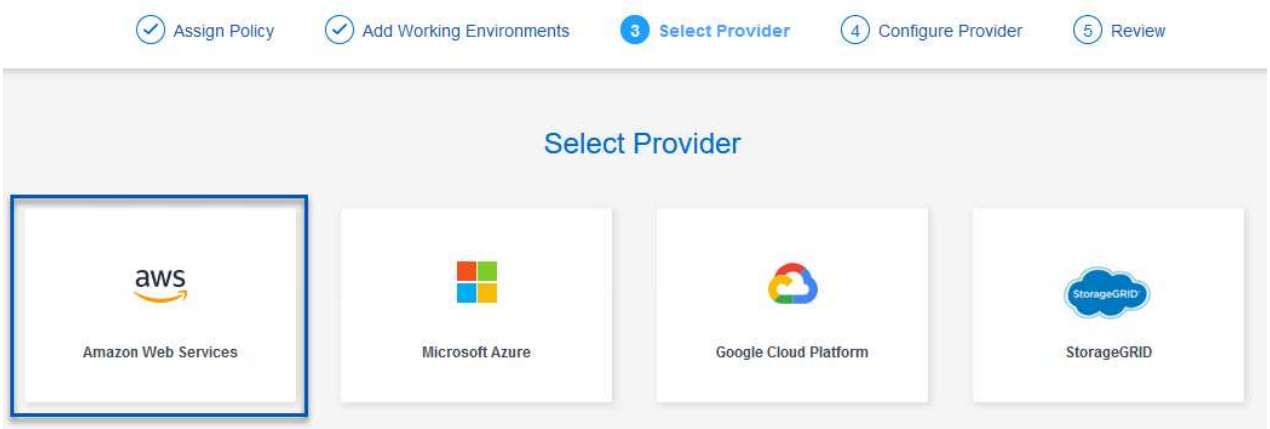
2. Assegnare il criterio da utilizzare per l'operazione di protezione dei dati e fare clic su **Avanti**.



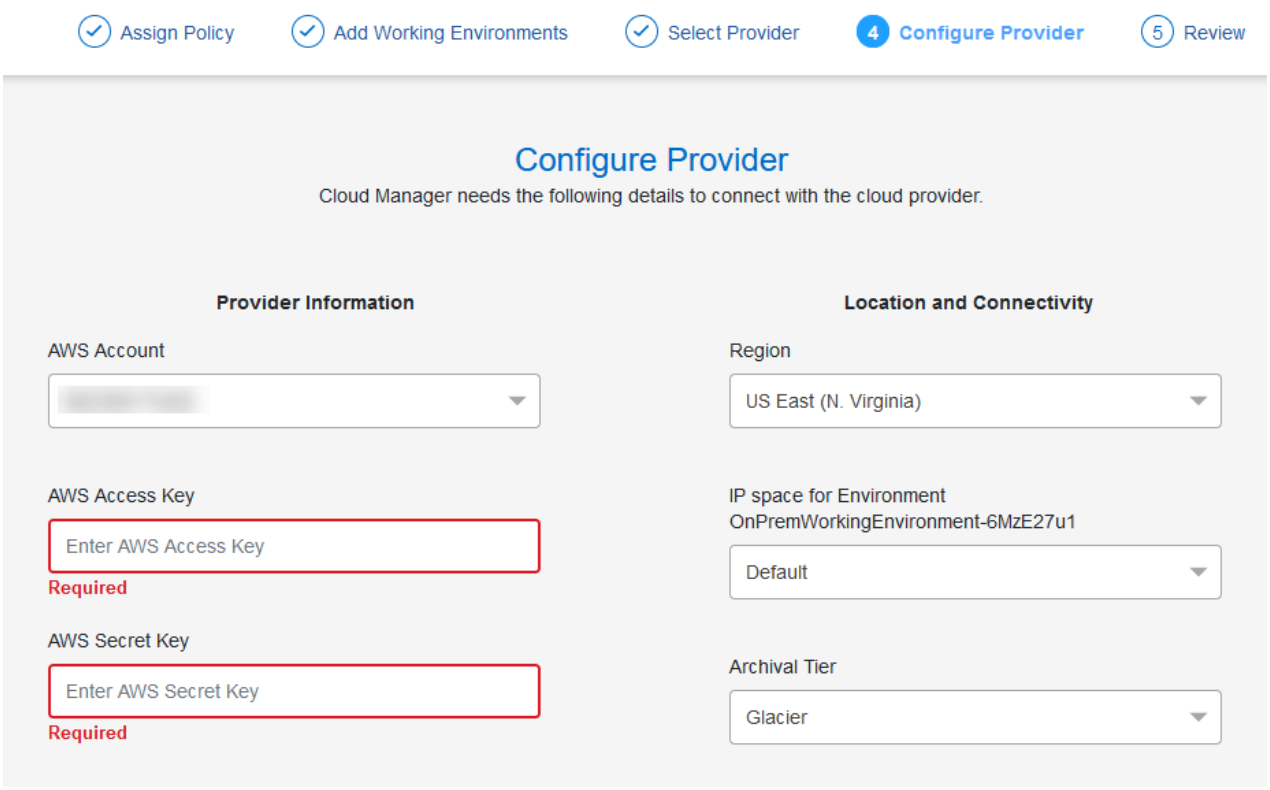
3. Nella pagina **Aggiungi ambienti di lavoro**, il datastore e l'ambiente di lavoro con un segno di spunta dovrebbero apparire se l'ambiente di lavoro è stato precedentemente rilevato. Se l'ambiente di lavoro non è stato rilevato in precedenza, è possibile aggiungerlo qui. Fare clic su **Avanti** per continuare.



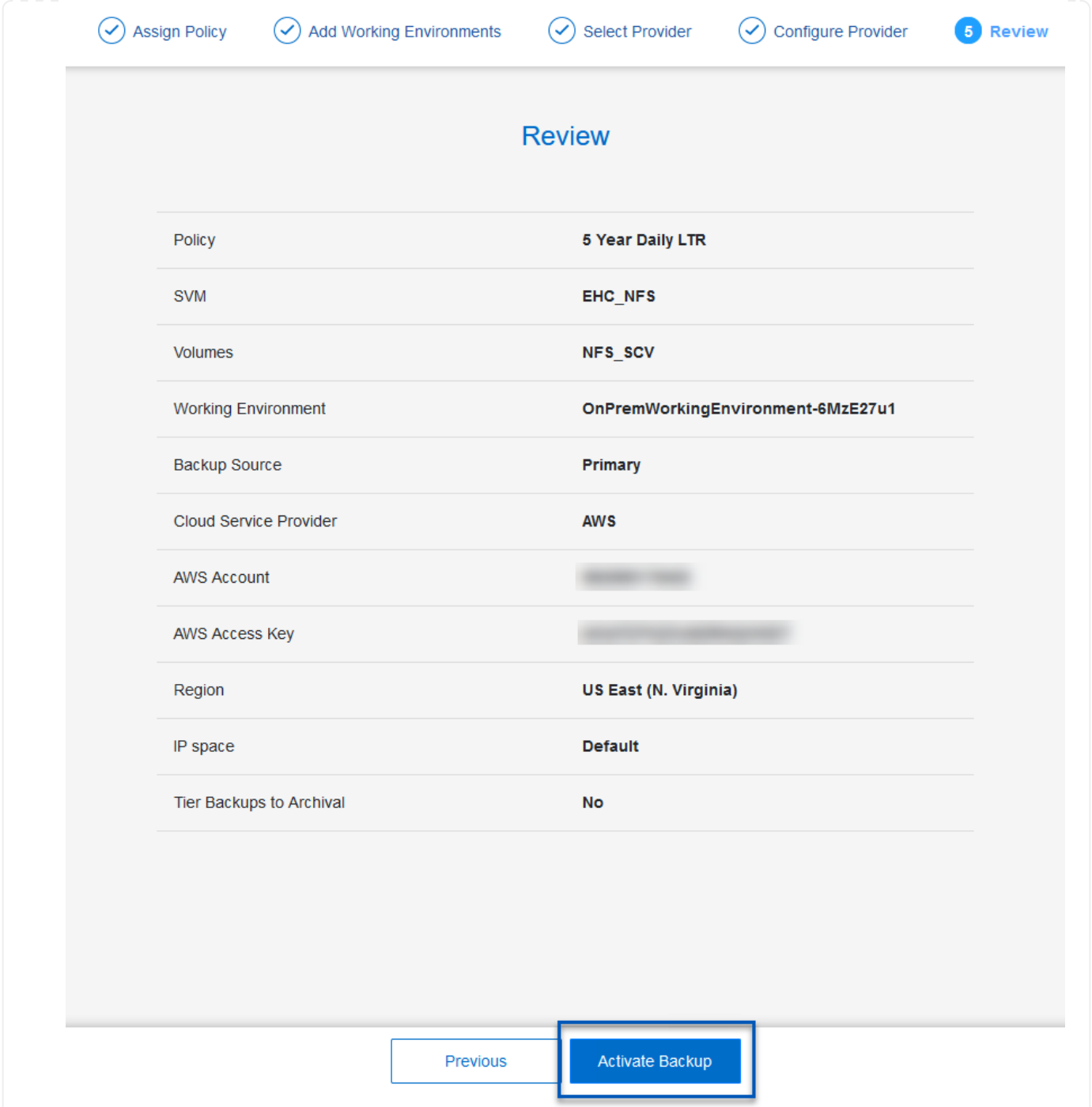
4. Nella pagina **Select Provider** (Seleziona fornitore), fare clic su AWS, quindi sul pulsante **Next** (Avanti) per continuare.



5. Compila le informazioni sulle credenziali specifiche del provider per AWS, inclusi la chiave di accesso AWS e la chiave segreta, la regione e il Tier di archivio da utilizzare. Inoltre, seleziona lo spazio IP ONTAP per il sistema storage ONTAP on-premise. Fare clic su **Avanti**.



6. Infine, esaminare i dettagli del processo di backup e fare clic sul pulsante **attiva backup** per avviare la protezione dei dati del datastore.



A questo punto il trasferimento dei dati potrebbe non iniziare immediatamente. Il backup e recovery di BlueXP analizza ogni ora le snapshot in sospeso e le trasferisce nello storage a oggetti.

Ripristino delle macchine virtuali in caso di perdita di dati

Garantire la protezione dei dati è solo un aspetto della protezione dati completa. Un aspetto altrettanto cruciale è la possibilità di ripristinare tempestivamente i dati da qualsiasi posizione in caso di perdita di dati o attacco ransomware. Questa funzionalità è fondamentale per mantenere operative di business perfette e soddisfare i recovery point objective.

NetApp offre una strategia 3-2-1 altamente adattabile, che offre un controllo customizzato sulle pianificazioni della conservazione nelle posizioni di storage primario, secondario e a oggetti. Questa strategia offre la flessibilità necessaria per personalizzare gli approcci di protezione dei dati in base a esigenze specifiche.

Questa sezione offre una panoramica del processo di ripristino dei dati dal plug-in SnapCenter per VMware vSphere e da backup e recovery BlueXP per le macchine virtuali.

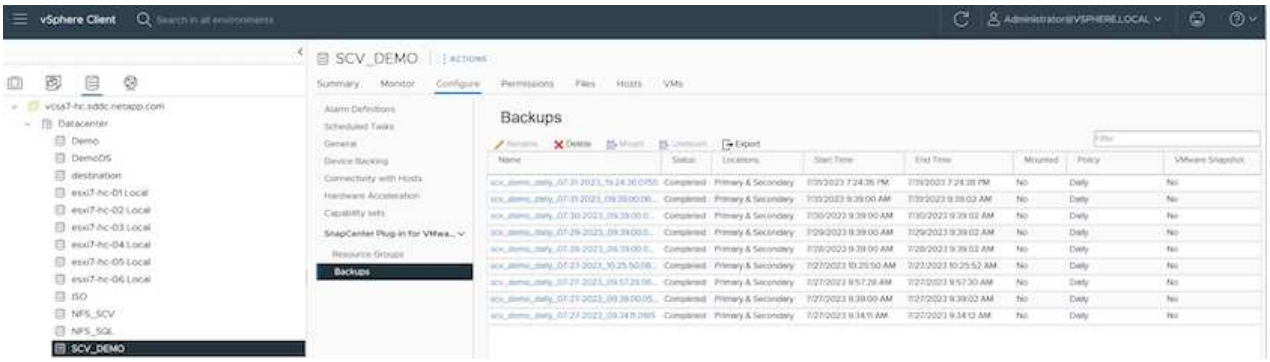
Ripristino di macchine virtuali dal plug-in SnapCenter per VMware vSphere

Per questa soluzione, le macchine virtuali sono state ripristinate in posizioni originali e alternative. Non tutti gli aspetti delle capacità di ripristino dei dati dei distributori idraulici saranno trattati in questa soluzione. Per informazioni dettagliate su tutto ciò che il distributore idraulico ha da offrire, fare riferimento alla "Ripristinare le macchine virtuali dai backup" nella documentazione del prodotto.

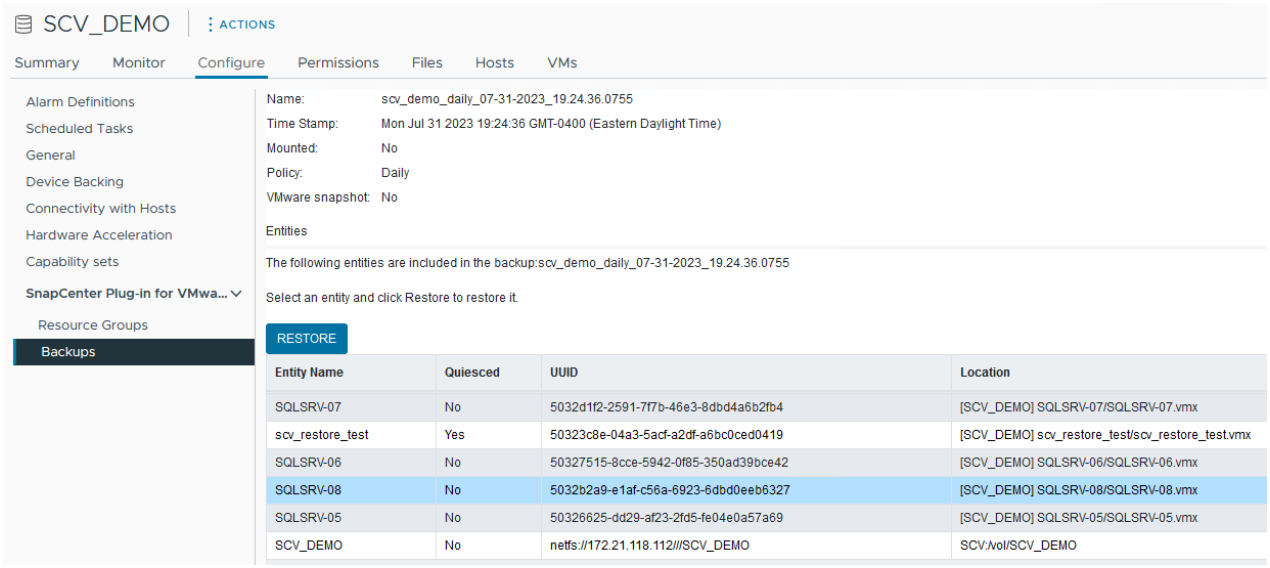
Ripristinare le macchine virtuali dal distributore idraulico

Completare i seguenti passaggi per ripristinare un ripristino di una macchina virtuale dallo storage primario o secondario.

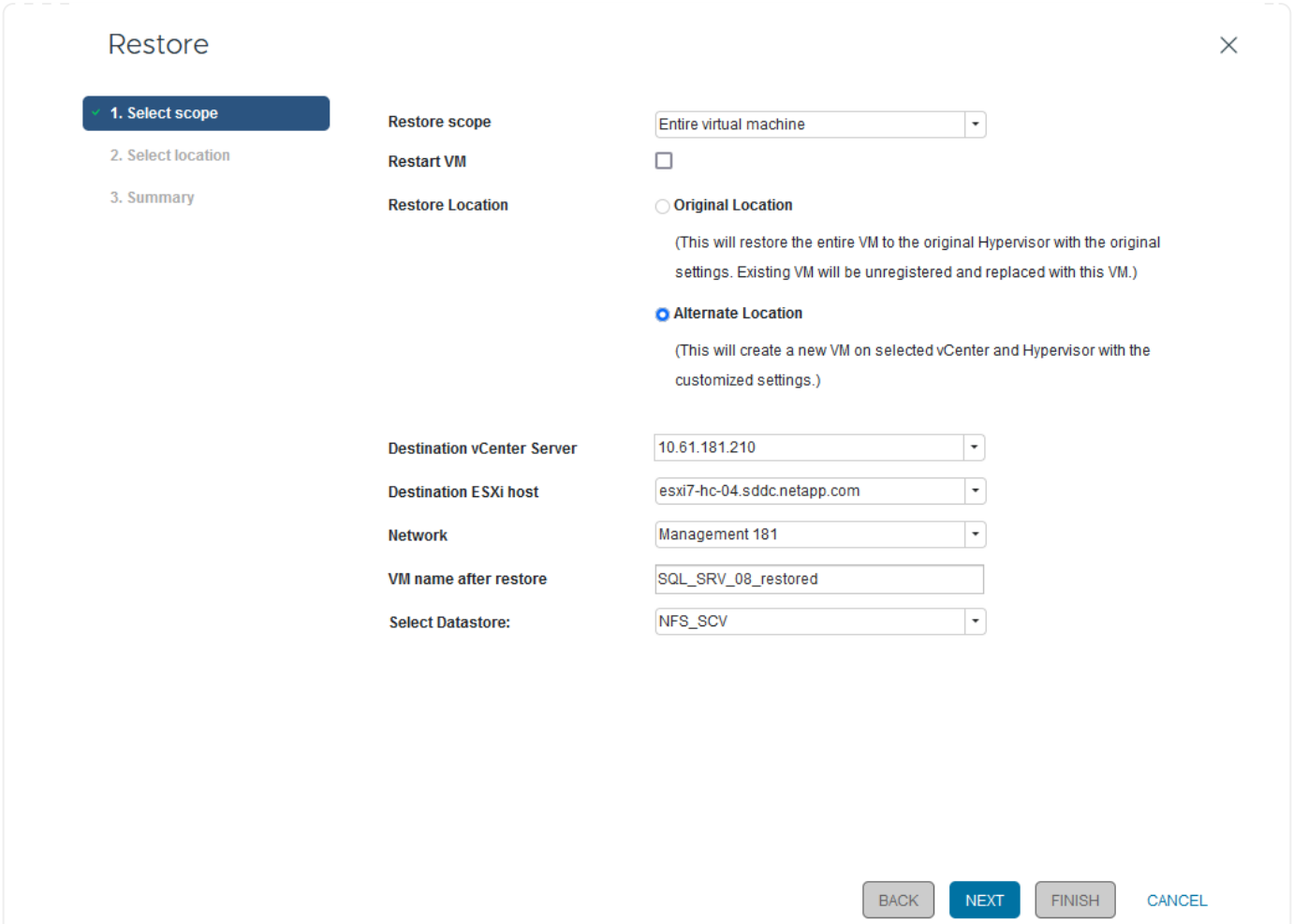
1. Dal client vCenter, accedere a **inventario > archiviazione** e fare clic sul datastore che contiene le macchine virtuali che si desidera ripristinare.
2. Dalla scheda **Configure** fare clic su **backups** per accedere all'elenco dei backup disponibili.



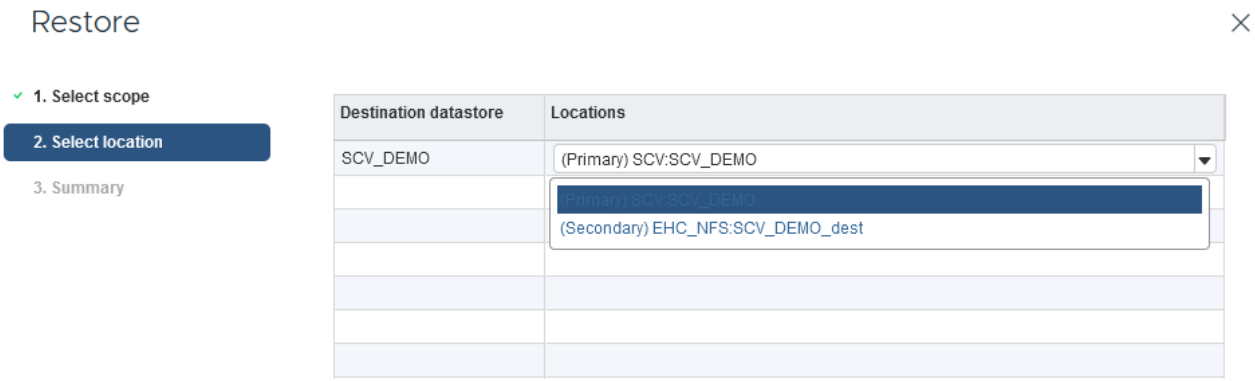
3. Fare clic su un backup per accedere all'elenco delle VM, quindi selezionare una VM da ripristinare. Fare clic su **Ripristina**.



4. Dalla procedura guidata di ripristino, selezionare per ripristinare l'intera macchina virtuale o un VMDK specifico. Seleziona per eseguire l'installazione nella posizione originale o in una posizione alternativa, fornisci il nome della macchina virtuale dopo il ripristino e il datastore di destinazione. Fare clic su **Avanti**.



5. Scegli di eseguire il backup dalla posizione dello storage primario o secondario.



6. Infine, esaminare un riepilogo del processo di backup e fare clic su fine per avviare il processo di ripristino.

Ripristino di macchine virtuali dal backup e recovery di BlueXP per le macchine virtuali

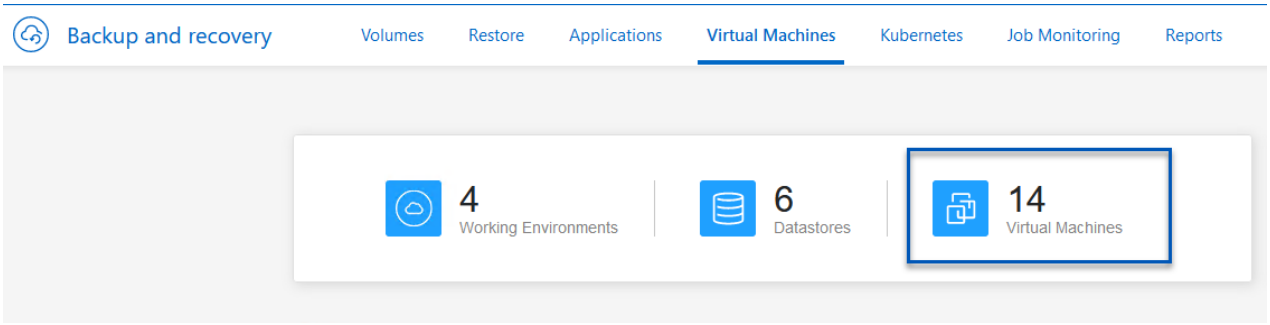
Il backup e recovery di BlueXP per le macchine virtuali consente di ripristinare le macchine virtuali nella loro posizione originale. È possibile accedere alle funzioni di ripristino dalla console web BlueXP.

Per ulteriori informazioni, fare riferimento a. "Ripristinare i dati delle macchine virtuali dal cloud".

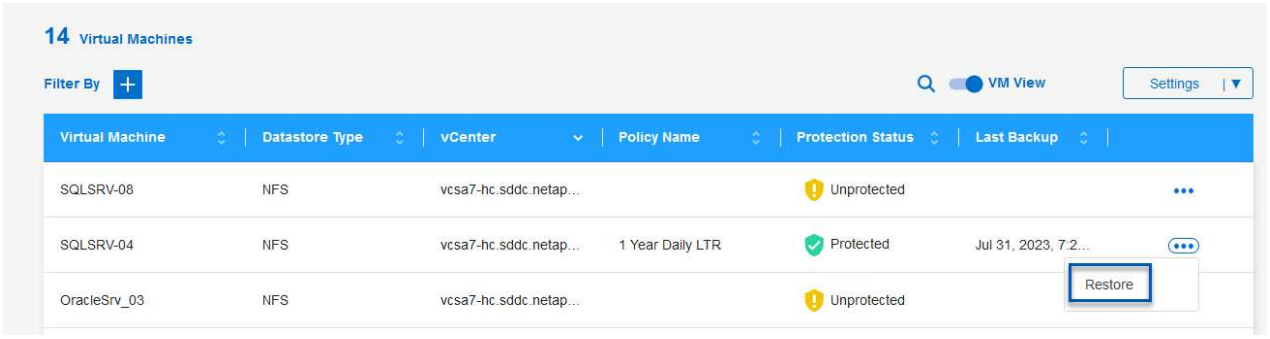
Ripristina le macchine virtuali dal backup e recovery di BlueXP

Per ripristinare una macchina virtuale dal backup e recovery di BlueXP, completa i seguenti passaggi.

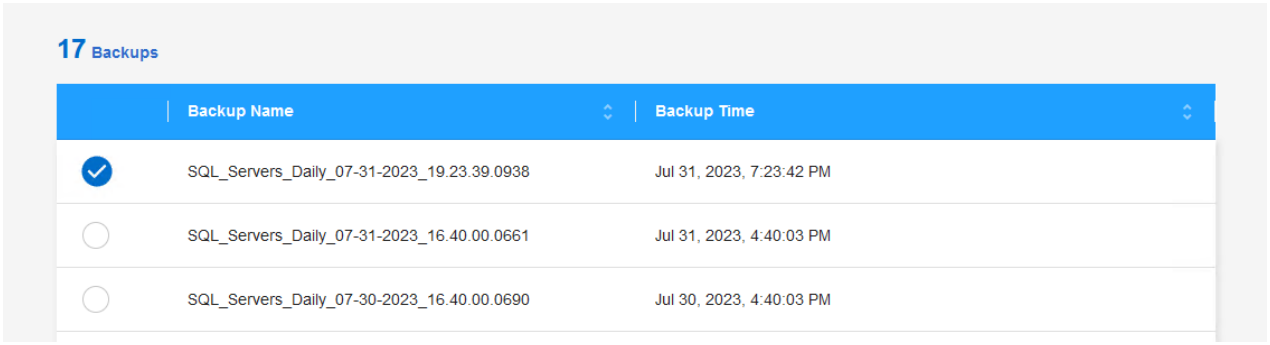
1. Accedere a **protezione > Backup e ripristino > macchine virtuali** e fare clic su macchine virtuali per visualizzare l'elenco delle macchine virtuali disponibili per il ripristino.



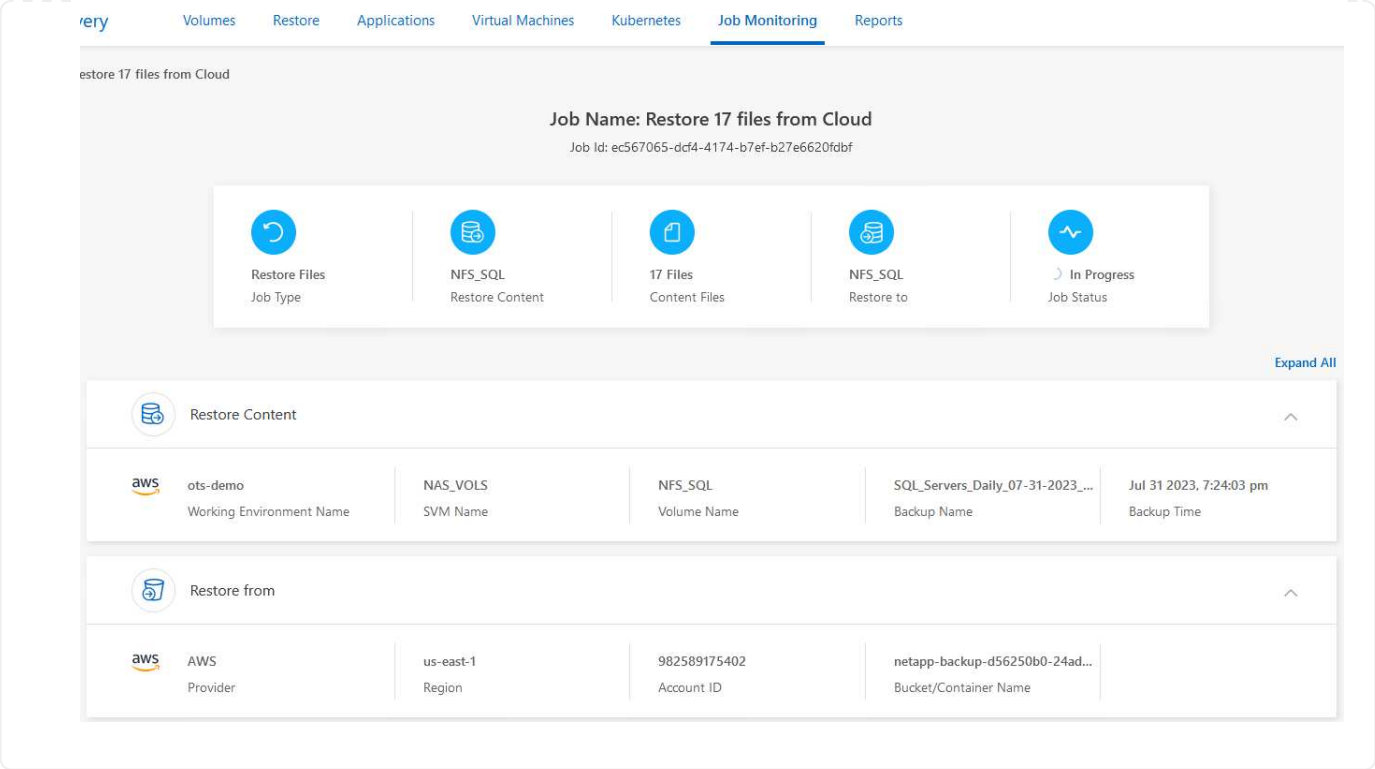
2. Accedere al menu a discesa delle impostazioni per la VM da ripristinare e selezionare



3. Selezionare il backup da cui eseguire il ripristino e fare clic su **Avanti**.



4. Esaminare un riepilogo del processo di backup e fare clic su **Ripristina** per avviare il processo di ripristino.
5. Monitorare l'avanzamento del processo di ripristino dalla scheda **monitoraggio processo**.



Conclusione

La strategia di backup 3-2-1, se implementata con il plug-in SnapCenter per backup e recovery di VMware vSphere e BlueXP per le macchine virtuali, offre una soluzione solida, affidabile e conveniente per la protezione dei dati. Questa strategia non solo garantisce ridondanza e accessibilità dei dati, ma offre anche la flessibilità di ripristinare i dati da qualsiasi posizione e da sistemi storage ONTAP on-premise e dallo storage a oggetti basato sul cloud.

Il caso di utilizzo presentato in questa documentazione si concentra sulle tecnologie comprovate di data Protection che evidenziano l'integrazione tra NetApp, VMware e i cloud provider leader. Il plug-in SnapCenter per VMware vSphere offre un'integrazione perfetta con VMware vSphere, consentendo una gestione efficiente e centralizzata delle operazioni di protezione dei dati. Questa integrazione semplifica i processi di backup e recovery per le macchine virtuali, consentendo operazioni di pianificazione, monitoraggio e ripristino flessibili all'interno dell'ecosistema VMware. Il backup e recovery di BlueXP per le macchine virtuali fornisce quello (1) in 3-2-1, fornendo backup sicuri e a corto di aria dei dati delle macchine virtuali sullo storage a oggetti basato sul cloud. L'interfaccia intuitiva e il flusso di lavoro logico offrono una piattaforma sicura per l'archiviazione a lungo termine dei dati critici.

Ulteriori informazioni

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

- "Plug-in SnapCenter per la documentazione di VMware vSphere"
- "Documentazione BlueXP"

Dr con BlueXP DRaas

Panoramica

Il disaster recovery è la priorità per ogni amministratore VMware. Poiché VMware incapsula interi server in una serie di file che costituiscono la macchina virtuale, gli amministratori possono sfruttare tecniche basate sullo storage a blocchi quali cloni, snapshot e repliche per proteggere queste macchine virtuali. Gli array ONTAP offrono una replica integrata per trasferire i dati dei volumi, e quindi le macchine virtuali che risiedono nelle LUN del datastore designate, da un sito all'altro. BlueXP DRaaS si integra con vSphere e automatizza l'intero flusso di lavoro per un failover e un failback perfetti in caso di emergenza. Combinando la replica dello storage con l'automazione intelligente, gli amministratori hanno ora a disposizione un metodo gestibile non solo per configurare, automatizzare e testare i piani di disaster recovery, ma anche per eseguirli facilmente in caso di emergenza.

La maggior parte delle parti che richiedono molto tempo di un failover del disaster recovery in un ambiente VMware vSphere è l'esecuzione dei passaggi necessari per inventariare, registrare, riconfigurare e accendere le macchine virtuali nel sito di disaster recovery. Una soluzione ideale presenta un RPO basso (misurato in minuti) e un RTO basso (misurato in minuti-ore). Un fattore spesso trascurato in una soluzione di DR è la possibilità di testare in modo efficiente la soluzione DR su un intervallo periodico.

Per progettare una soluzione di DR, tenere presente i seguenti fattori:

- L'obiettivo RTO (Recovery Time Objective). L'RTO rappresenta la velocità con cui un'azienda può eseguire il ripristino da un evento disastroso o, in particolare, il tempo necessario per eseguire il processo di ripristino e rendere nuovamente disponibili i servizi aziendali.
- L'obiettivo RPO (Recovery Point Objective). L'RPO indica la data di nascita dei dati recuperati dopo che sono stati resi disponibili, in relazione al tempo in cui si è verificato il disastro.
- Scalabilità e adattabilità. Questo fattore include la possibilità di aumentare le risorse di storage in maniera incrementale con l'aumentare della domanda.

Per ulteriori informazioni tecniche sulle soluzioni disponibili, vedere:

- "Dr utilizzando BlueXP DRaaS per datastore NFS"
- "Dr utilizzando BlueXP DRaaS per archivi dati VMFS"

Dr utilizzando BlueXP DRaaS per datastore NFS

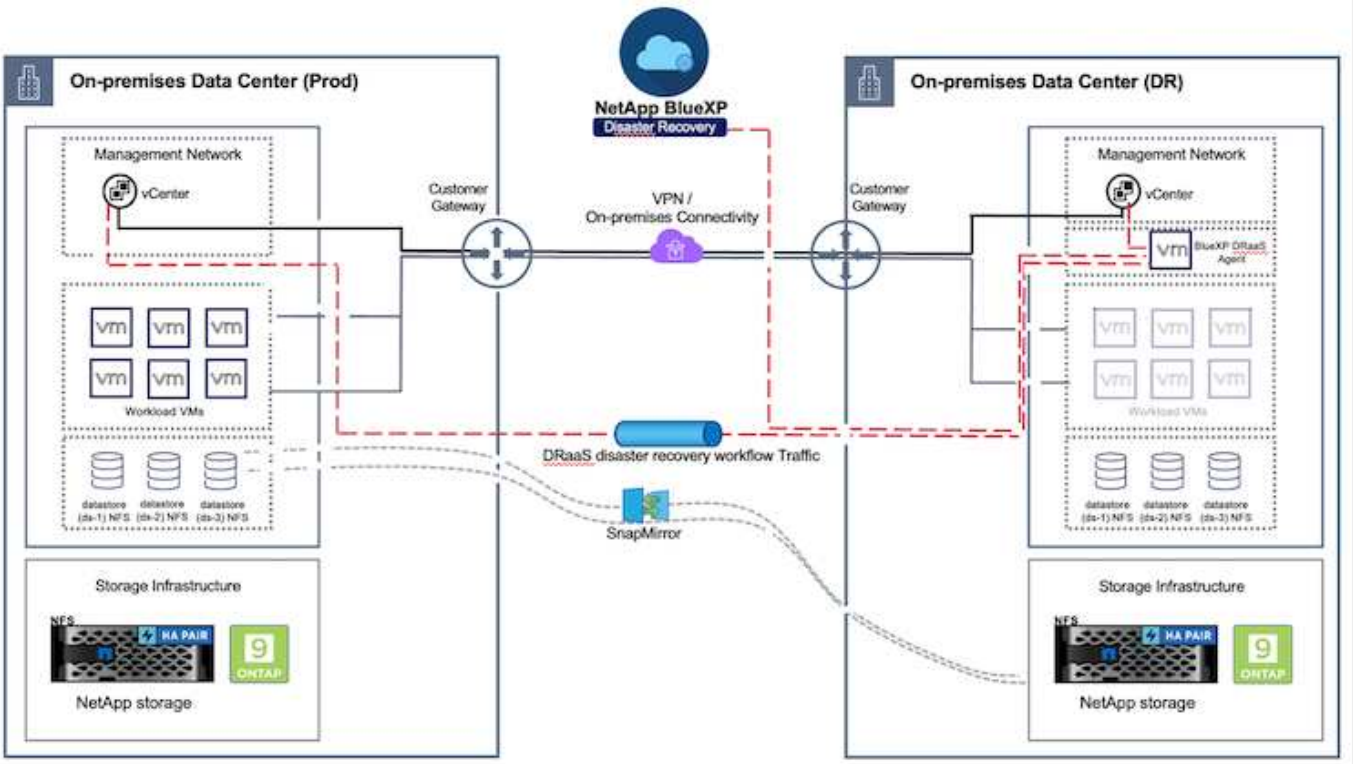
L'implementazione del disaster recovery attraverso la replica a livello di blocco dal sito di produzione al sito di disaster recovery è un metodo resiliente e conveniente per proteggere i carichi di lavoro da black-out del sito e eventi di corruzione dei dati, come gli attacchi ransomware. Utilizzando la replica di NetApp SnapMirror, è possibile replicare i carichi di lavoro VMware in esecuzione su sistemi ONTAP on-premise con datastore NFS in un altro sistema storage ONTAP situato in un data center di recovery designato in cui viene anche implementata VMware.

Questa sezione del documento descrive la configurazione di BlueXP DRaaS per l'impostazione del disaster recovery per VM VMware on-premise in un altro sito designato. Durante questa configurazione, l'account BlueXP , BlueXP Connector, gli array ONTAP aggiunti nell'area di lavoro BlueXP , necessaria per consentire la comunicazione da VMware vCenter allo storage ONTAP. Inoltre, in questo documento viene descritto come

configurare la replica tra siti e come impostare e verificare un piano di ripristino. L'ultima sezione contiene istruzioni per l'esecuzione di un failover completo del sito e per il failback quando il sito primario viene recuperato e acquistato online.

Utilizzando il servizio di disaster recovery BlueXP , integrato nella console NetApp BlueXP , le aziende possono facilmente scoprire i propri VMware vCenter e lo storage ONTAP on-premise. Le organizzazioni possono quindi creare raggruppamenti di risorse, creare un piano di disaster recovery, associarlo a gruppi di risorse e verificare o eseguire failover e failback. SnapMirror offre una replica a blocchi a livello di storage per mantenere aggiornati i due siti con modifiche incrementali, con un conseguente recovery point objective (RPO) fino a 5 minuti. Inoltre, è possibile simulare le procedure di disaster recovery senza influire sulla produzione o sostenere costi di storage aggiuntivi.

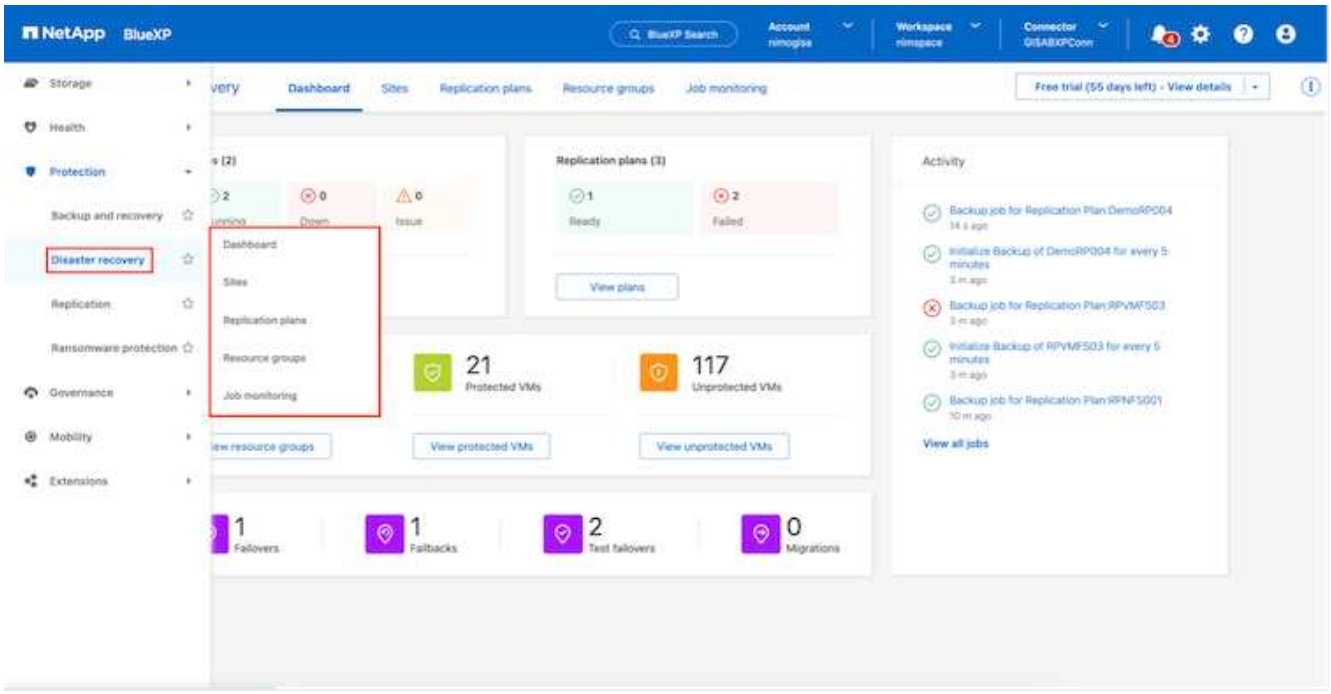
Il disaster recovery di BlueXP sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore NFS dall'ultima snapshot replicata nel sito di disaster recovery. Dopo aver completato il test di disaster recovery, i clienti possono eliminare facilmente l'ambiente di test senza influire sulle reali risorse di produzione replicate. In caso di failover effettivo, il servizio di disaster recovery BlueXP orchestra tutti i passaggi necessari per attivare automaticamente le macchine virtuali protette sul sito di disaster recovery designato, con pochi clic. Il servizio inverte inoltre la relazione SnapMirror al sito primario e replicherà eventuali modifiche da quello secondario a quello primario per un'operazione di failback, se necessario. Tutte queste funzionalità sono caratterizzate da un costo nettamente inferiore rispetto ad altre note alternative.



Per iniziare

Per iniziare con il disaster recovery di BlueXP , usa la console BlueXP e accedi al servizio.

1. Accedere a BlueXP.
2. Dal sistema di navigazione BlueXP sinistro, selezionare protezione > Disaster Recovery.
3. Viene visualizzata la dashboard di disaster recovery di BlueXP .

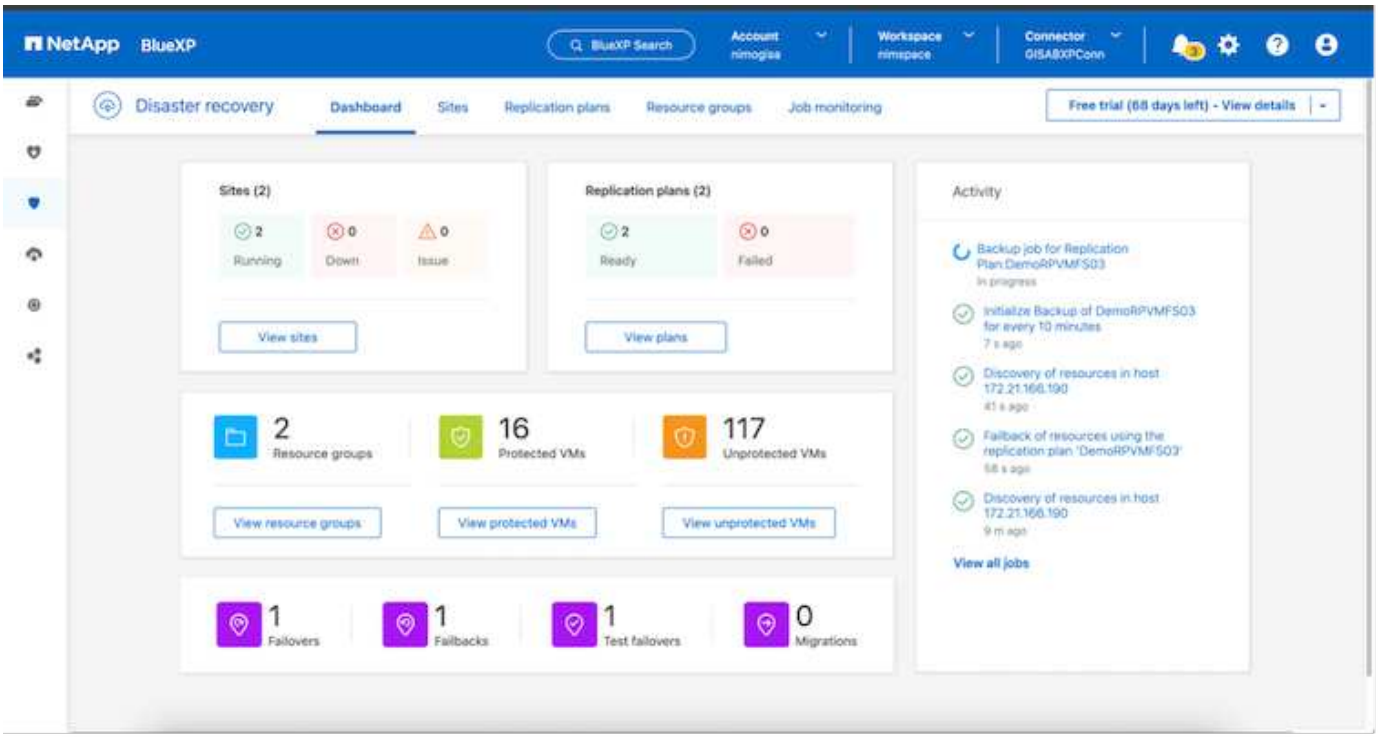


Prima di configurare il piano di disaster recovery, verificare che siano soddisfatti i seguenti prerequisiti:

- BlueXP Connector è impostato in NetApp BlueXP .
- L'istanza di BlueXP Connector dispone di connettività ai sistemi storage e vCenter di origine e destinazione.
- Cluster NetApp Data ONTAP per fornire datastore NFS di storage.
- I sistemi storage NetApp on-premise che ospitano datastore NFS per VMware sono aggiunti in BlueXP .
- Quando si utilizzano nomi DNS, la risoluzione DNS deve essere attiva. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi del datastore designati basati su NFS.
- Assicurarsi che l'ambiente disponga di versioni supportate dei server vCenter Server e ESXi.

Una volta stabilita la connettività tra i siti di origine e di destinazione, procedere con la procedura di configurazione, che richiede un paio di clic e richiede da 3 a 5 minuti circa.

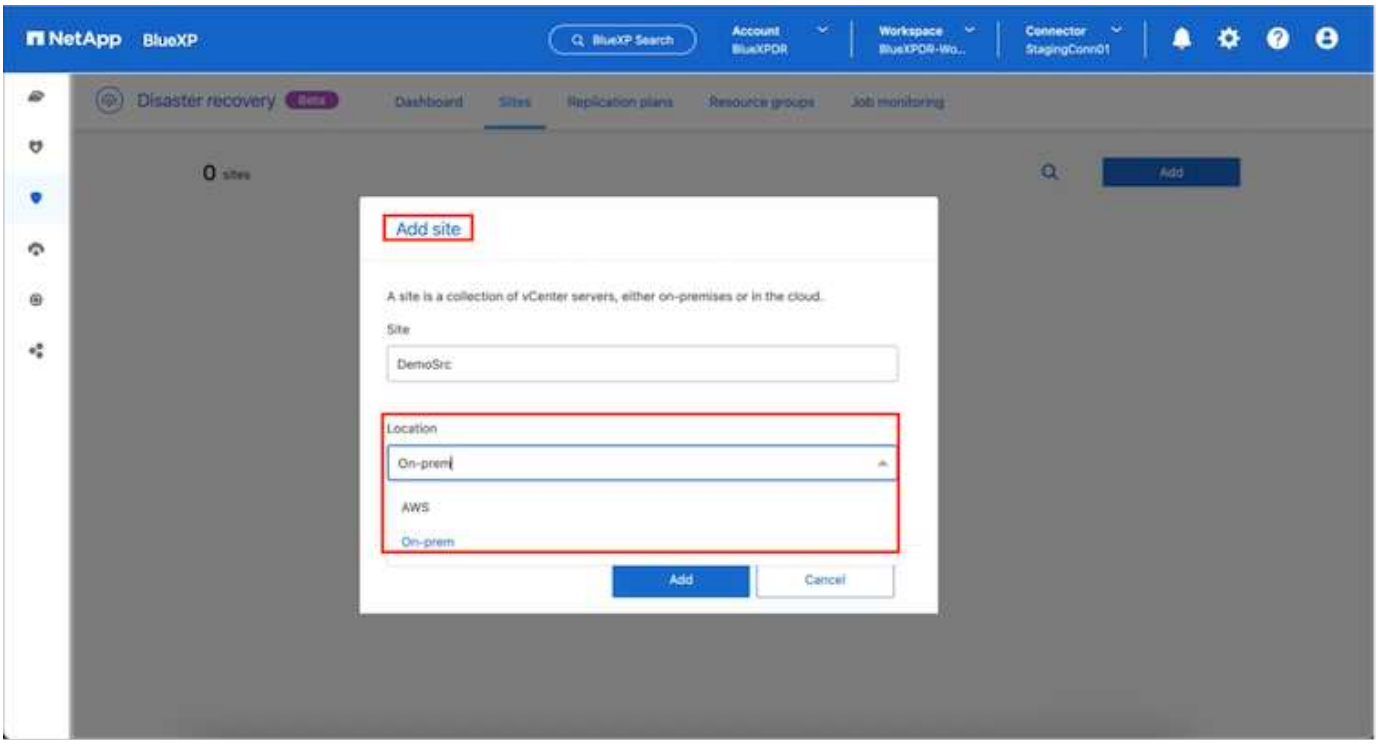
NetApp consiglia di implementare BlueXP Connector nel sito di destinazione o in un terzo sito, in modo che BlueXP Connector possa comunicare attraverso la rete con le risorse di origine e di destinazione.



Configurazione del disaster recovery BlueXP

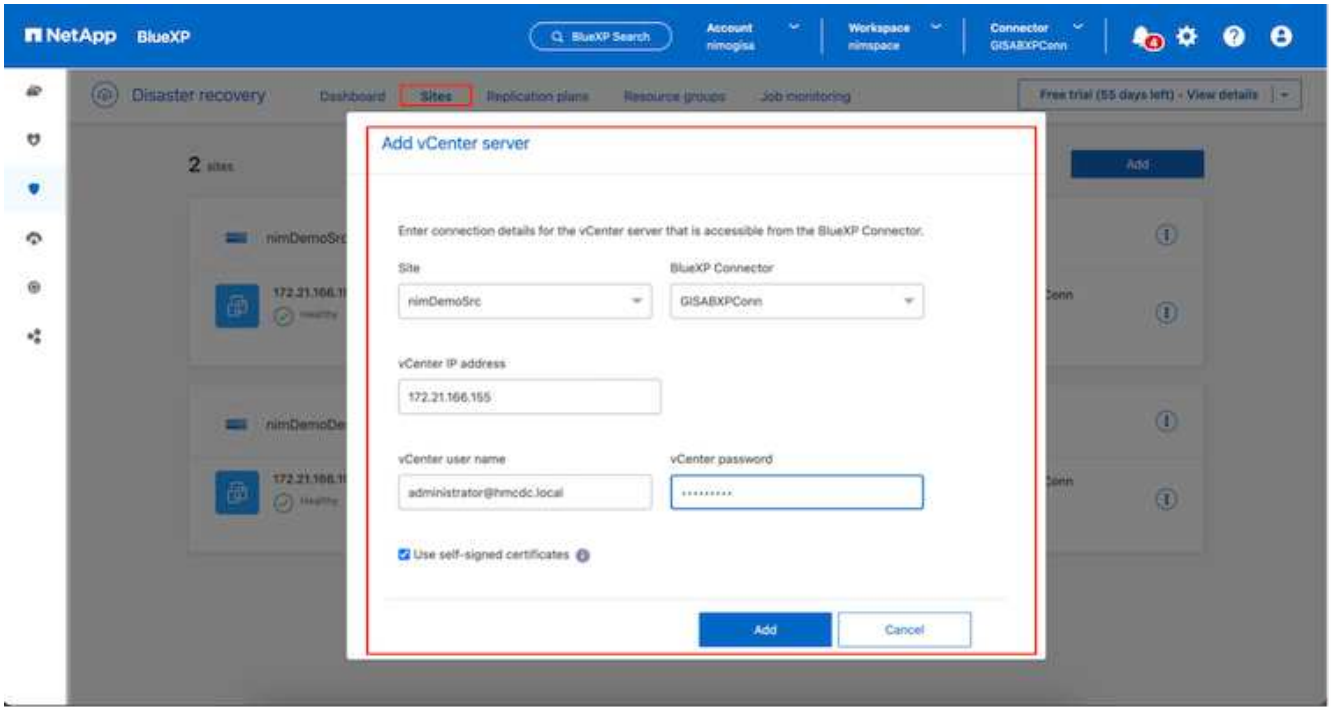
Il primo passo per prepararsi al disaster recovery è il rilevamento e l'aggiunta delle risorse di storage e vCenter on-premise al disaster recovery di BlueXP .

Aprire la console BlueXP e selezionare **protezione > Ripristino di emergenza** dal menu di navigazione sinistro. Selezionare **Scopri i server vCenter** o utilizzare il menu principale, selezionare **Siti > Aggiungi > Aggiungi vCenter**.

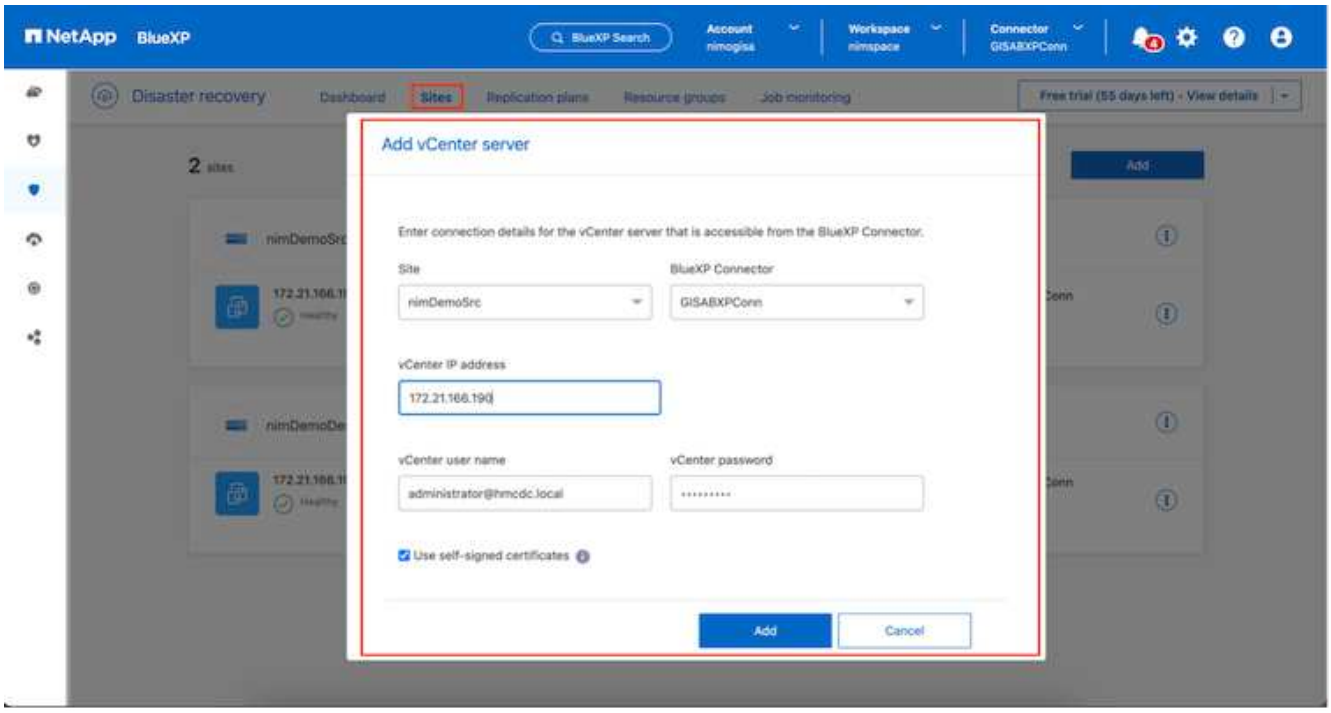


Aggiungere le seguenti piattaforme:

- **Fonte**. VCenter on-premise.



- **Destinazione**. VCenter SDDC di VMC.



Una volta aggiunti i vCenter, viene attivato il rilevamento automatico.

Configurazione della replica dello storage tra l'array del sito di origine e l'array del sito di destinazione

SnapMirror fornisce la replica dei dati in un ambiente NetApp. Basata sulla tecnologia NetApp Snapshot®, la replica SnapMirror è estremamente efficiente perché replica solo i blocchi modificati o aggiunti dall'aggiornamento precedente. SnapMirror può essere facilmente configurato utilizzando Gestione di sistema

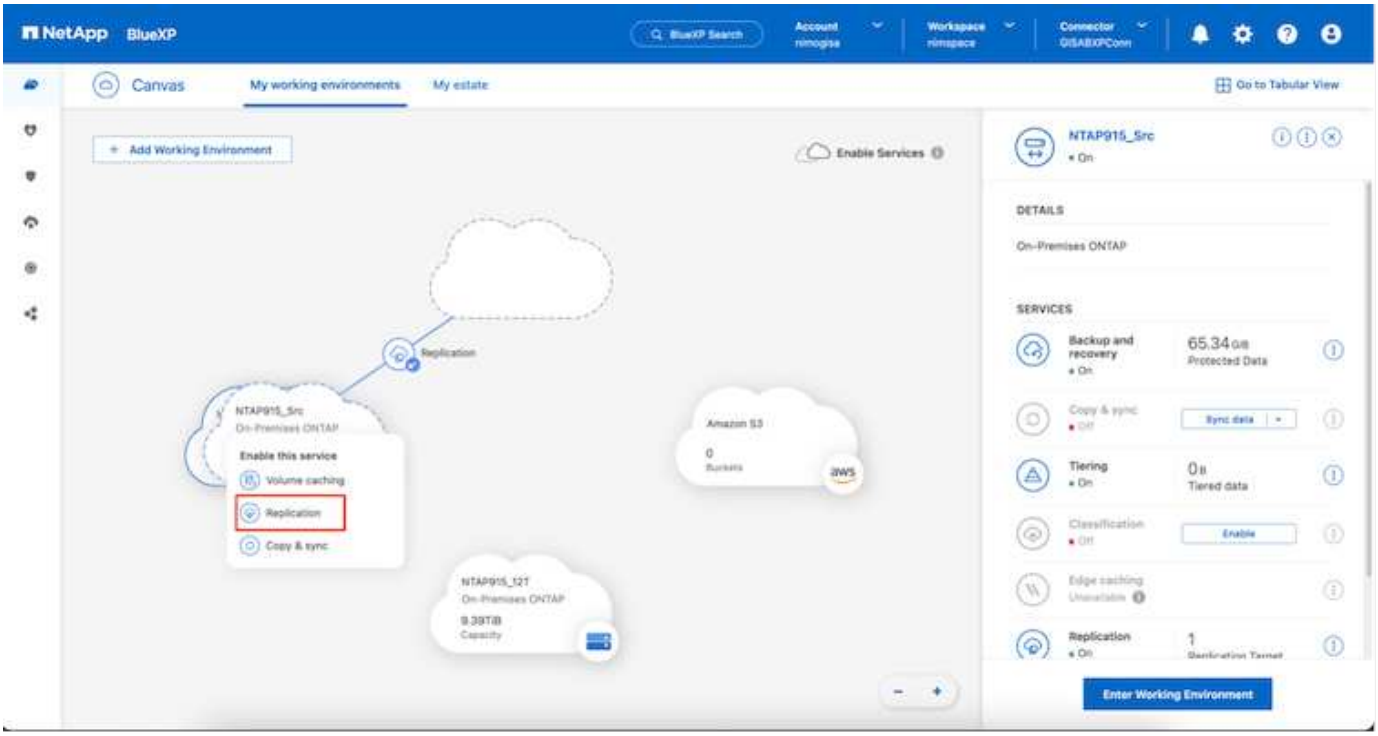
di NetApp OnCommand® o la CLI di ONTAP. Inoltre, BlueXP DRaaS crea il cluster fornito di relazione SnapMirror e il peering della SVM è configurato in anticipo.

Per i casi in cui lo storage primario non viene completamente perso, SnapMirror fornisce un metodo efficiente per la risincronizzazione dei siti primario e di DR. SnapMirror può risincronizzare i due siti, trasferendo solo i dati modificati o nuovi al sito primario dal sito di DR, semplicemente invertendo le relazioni di SnapMirror. Ciò significa che i piani di replica in BlueXP DRaaS possono essere risincronizzati in entrambe le direzioni dopo un failover, senza dover ricopiare l'intero volume. Se una relazione viene risincronizzata nella direzione inversa, solo i nuovi dati scritti dopo l'ultima sincronizzazione riuscita della copia Snapshot vengono inviati nuovamente alla destinazione.

Se la relazione di SnapMirror è già configurata per il volume tramite CLI o System Manager, BlueXP DRaaS raccoglie la relazione e continua con il resto delle operazioni del workflow.

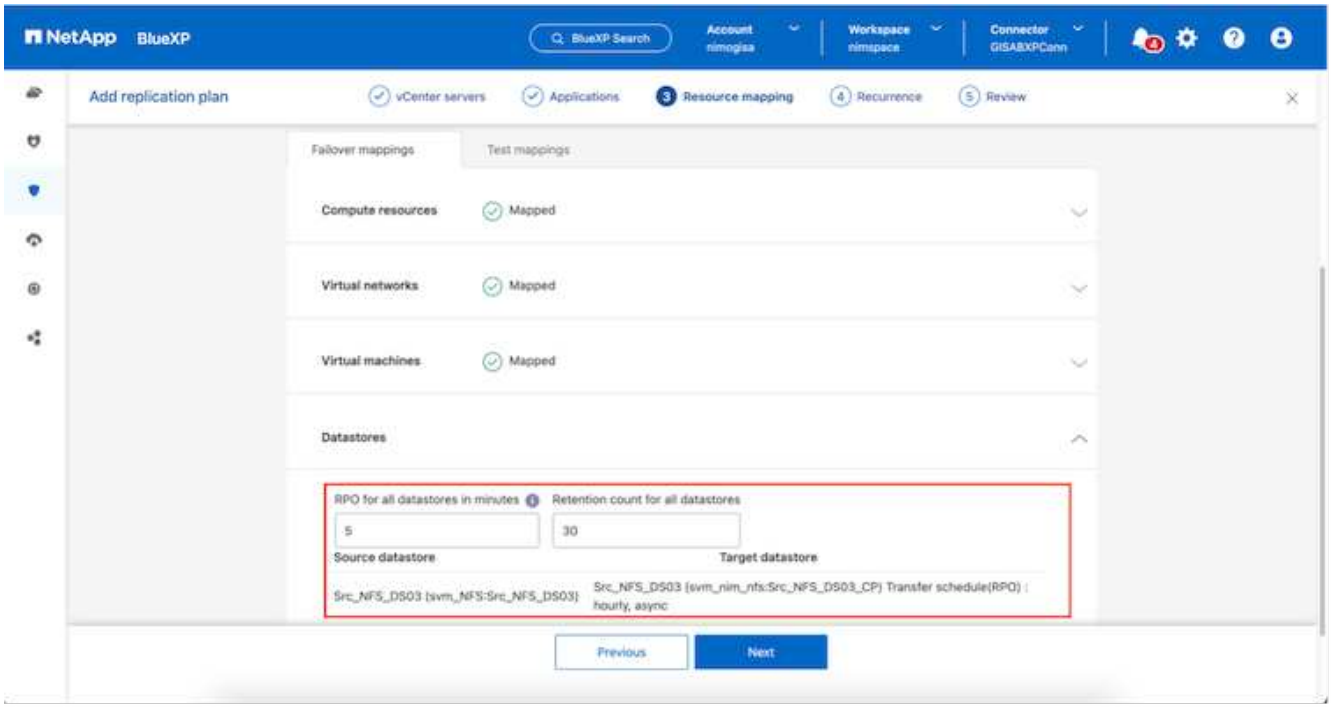
Come configurarlo per il Disaster Recovery VMware

Il processo di creazione della replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice consiste nell'utilizzare BlueXP per configurare la replica SnapMirror utilizzando il semplice drag & drop del sistema ONTAP di origine nell'ambiente sulla destinazione per attivare la procedura guidata che guida per il resto del processo.



BlueXP DRaaS può automatizzare anche lo stesso, purché vengano soddisfatti i due criteri seguenti:

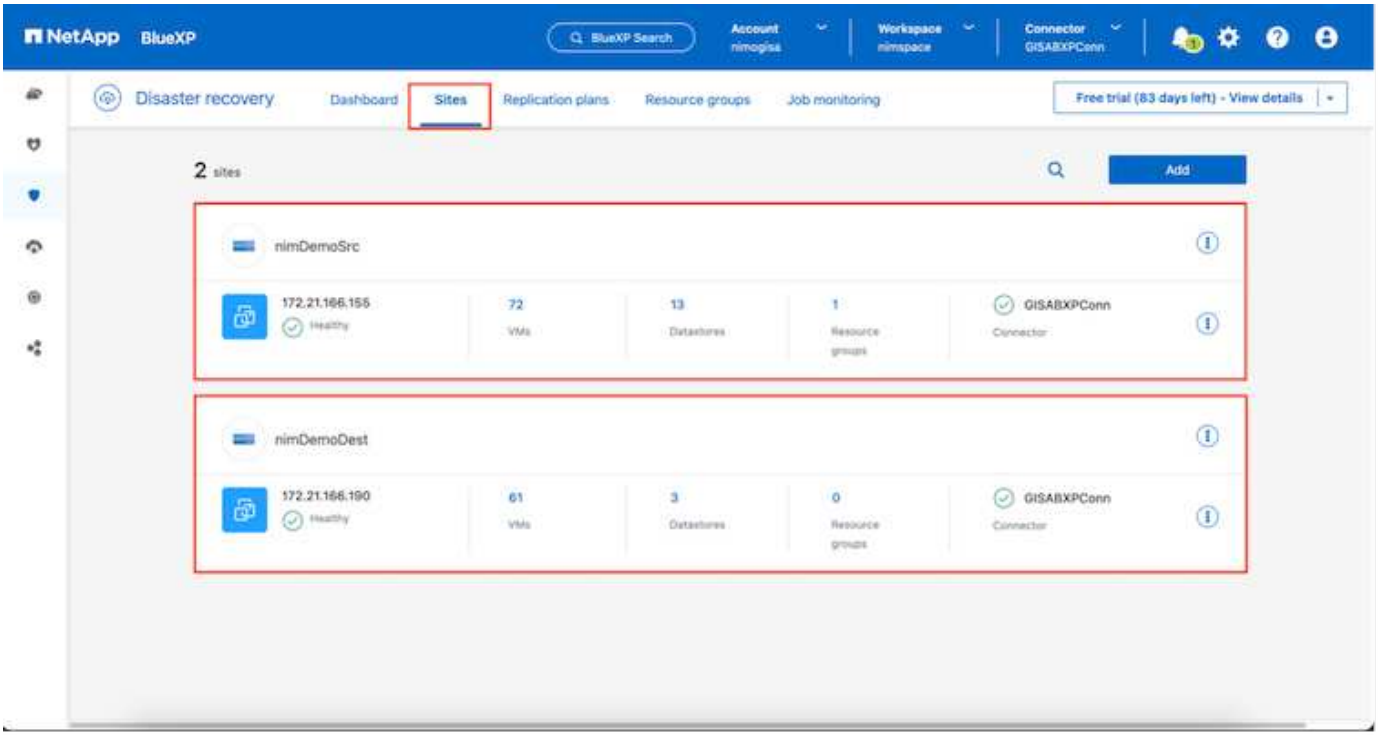
- I cluster di origine e di destinazione hanno una relazione peer.
- La SVM di origine e la SVM di destinazione hanno una relazione di tipo peer.



Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS raccoglie la relazione e continua con il resto delle operazioni del workflow.

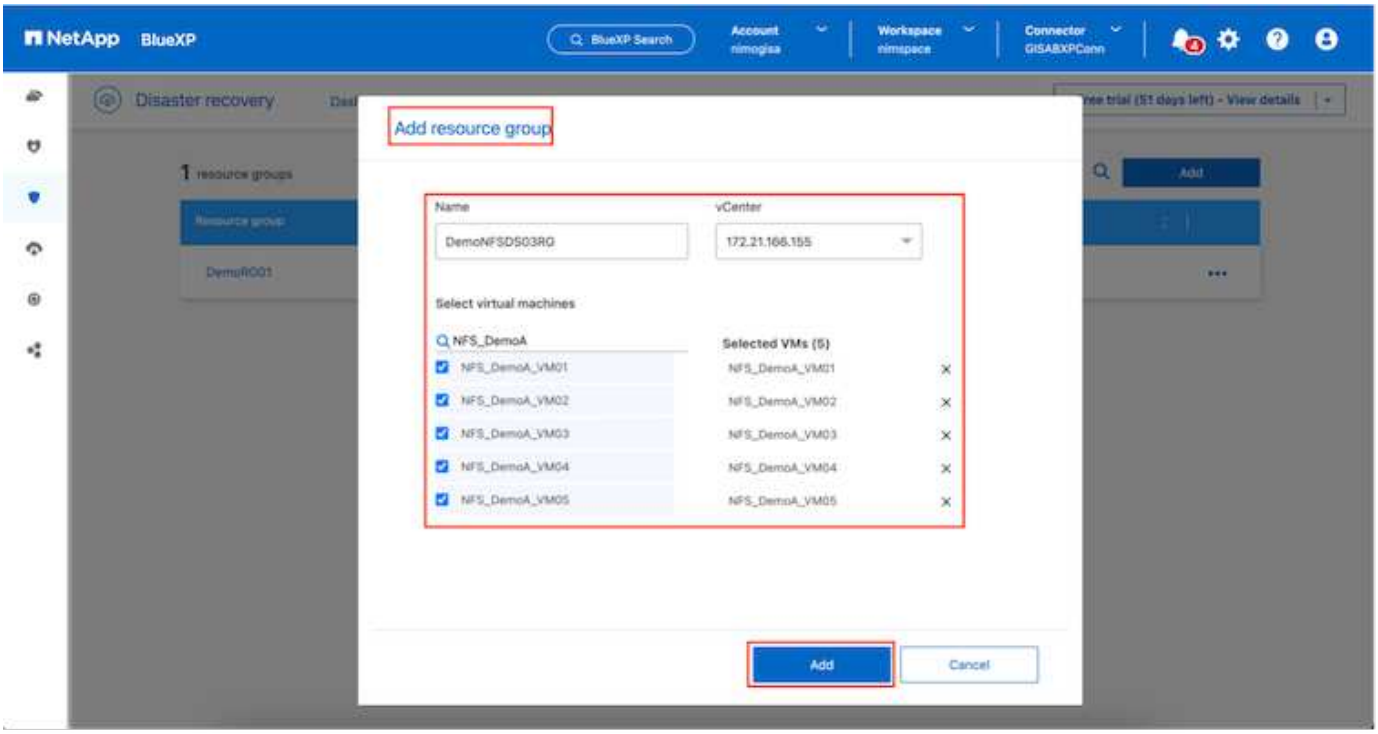
In che modo il disaster recovery di BlueXP può aiutarti?

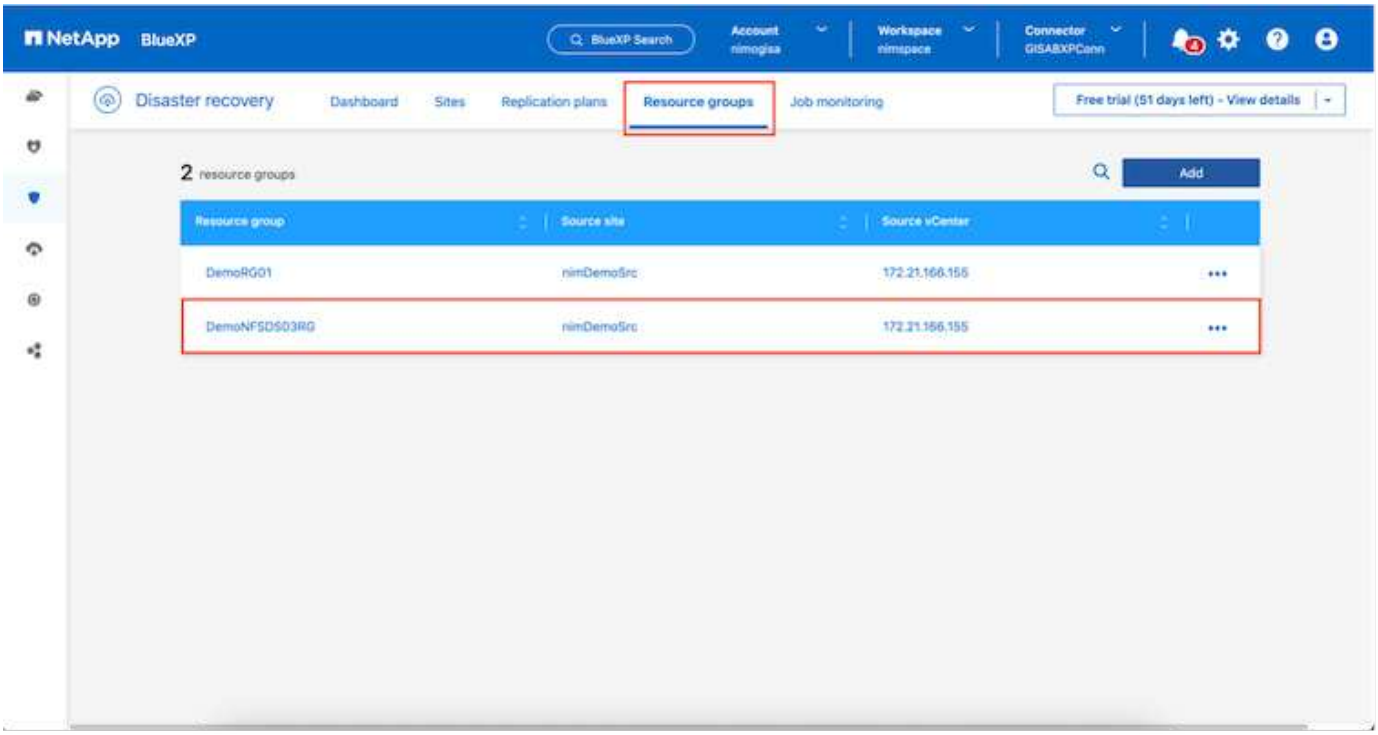
Una volta aggiunti i siti di origine e destinazione, il disaster recovery di BlueXP esegue il rilevamento automatico dei dati approfonditi e visualizza le macchine virtuali con i metadati associati. Il disaster recovery di BlueXP rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle macchine virtuali e le compila.



Una volta aggiunti i siti, è possibile raggruppare le macchine virtuali in gruppi di risorse. I gruppi di risorse per il

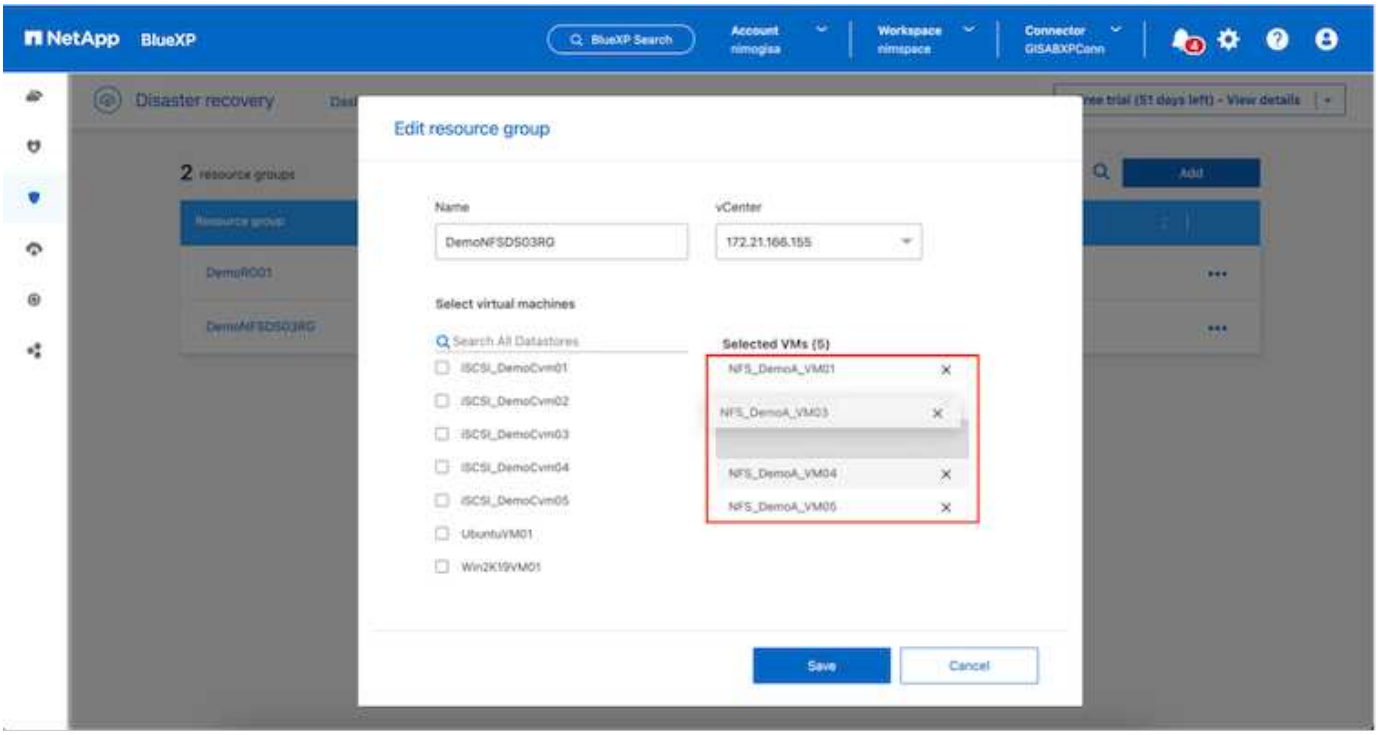
disaster recovery di BlueXP consentono di raggruppare una serie di macchine virtuali dipendenti in gruppi logici che contengono gli ordini di avvio e i ritardi di avvio che possono essere eseguiti al momento del ripristino. Per iniziare a creare gruppi di risorse, accedere a **gruppi di risorse** e fare clic su **Crea nuovo gruppo di risorse**.



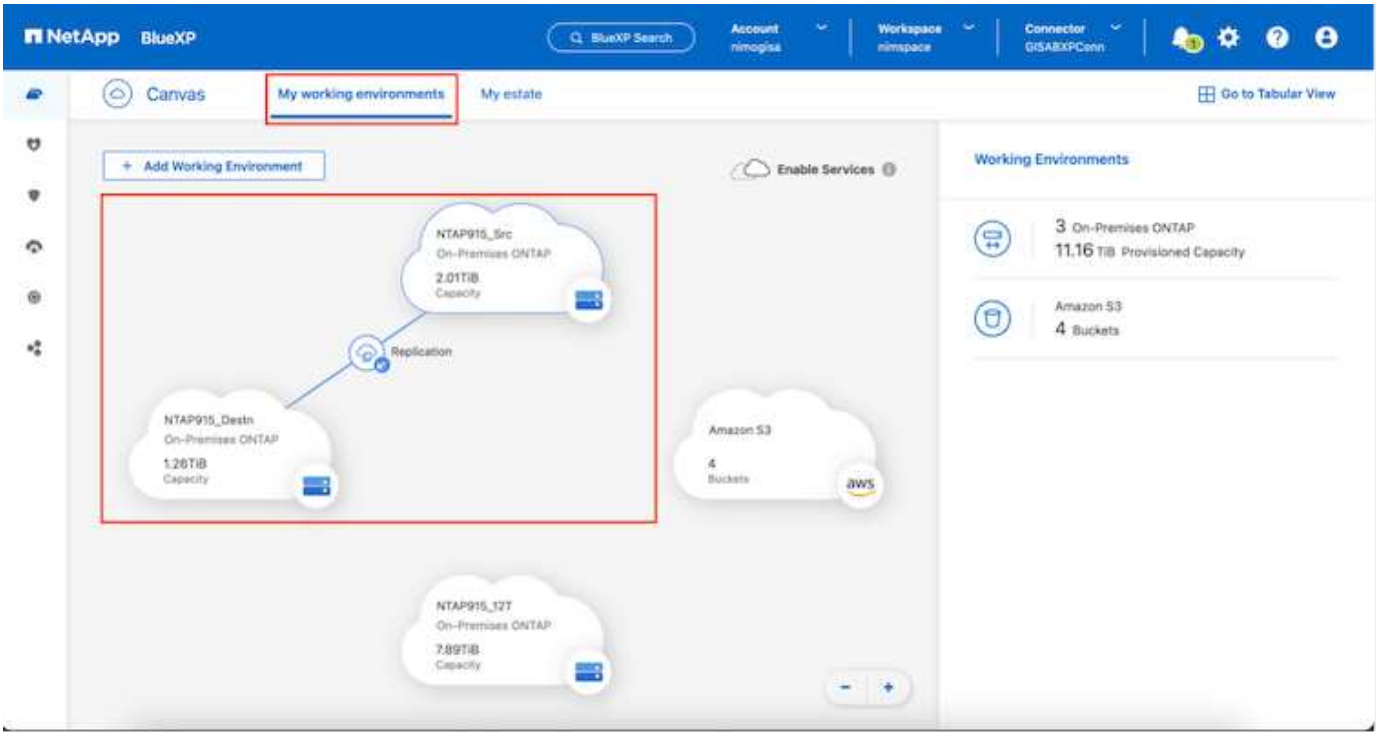


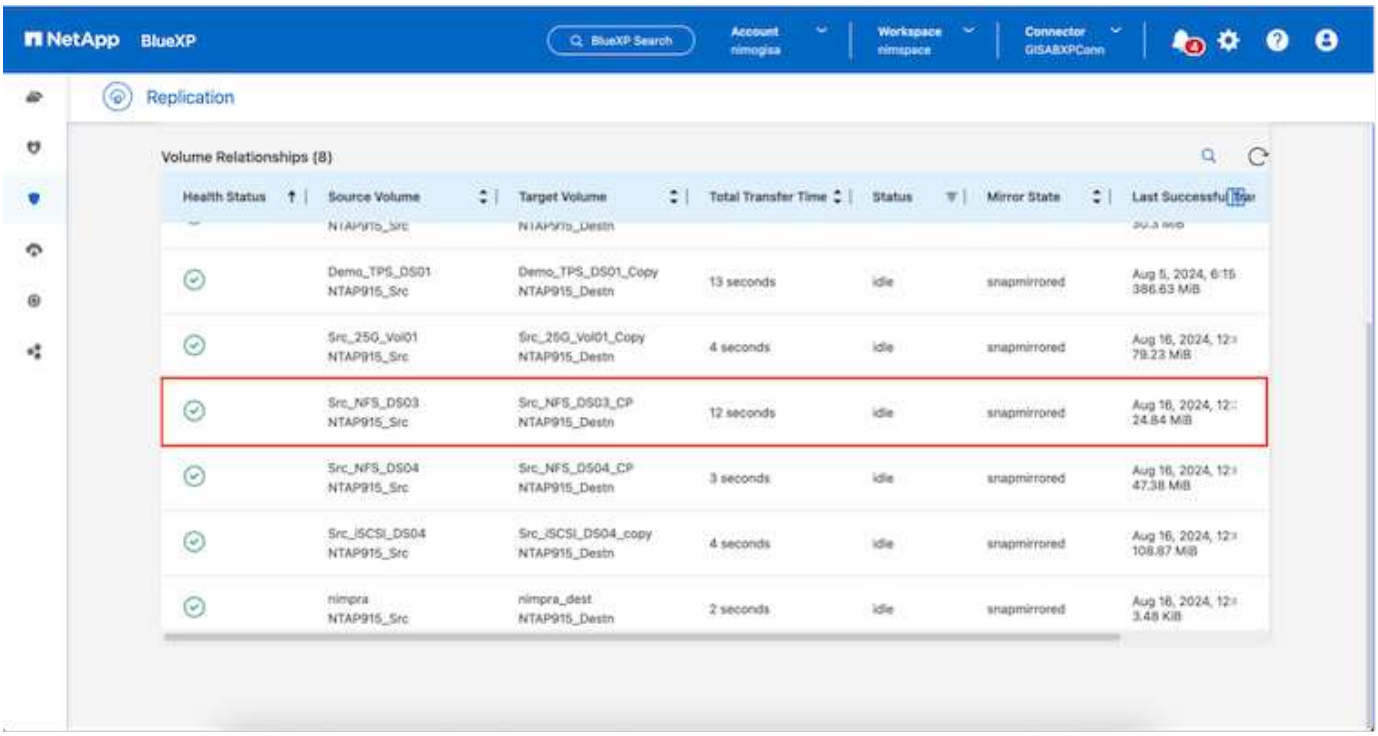
Il gruppo di risorse può anche essere creato durante la creazione di un piano di replica.

L'ordine di avvio delle VM può essere definito o modificato durante la creazione dei gruppi di risorse utilizzando un semplice meccanismo di trascinamento.



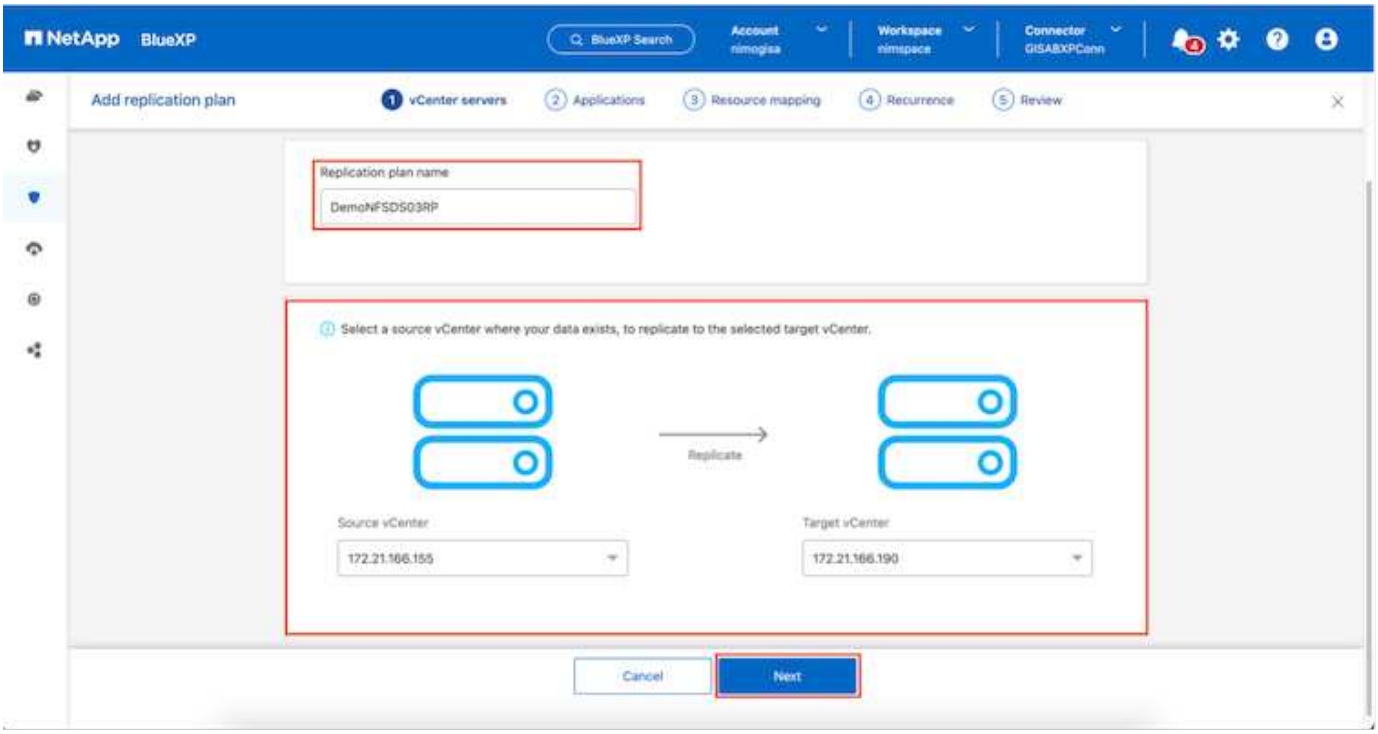
Una volta creati i gruppi di risorse, il passo successivo è creare il piano di esecuzione o un piano per il ripristino di macchine e applicazioni virtuali in caso di emergenza. Come menzionato nei prerequisiti, la replica di SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.





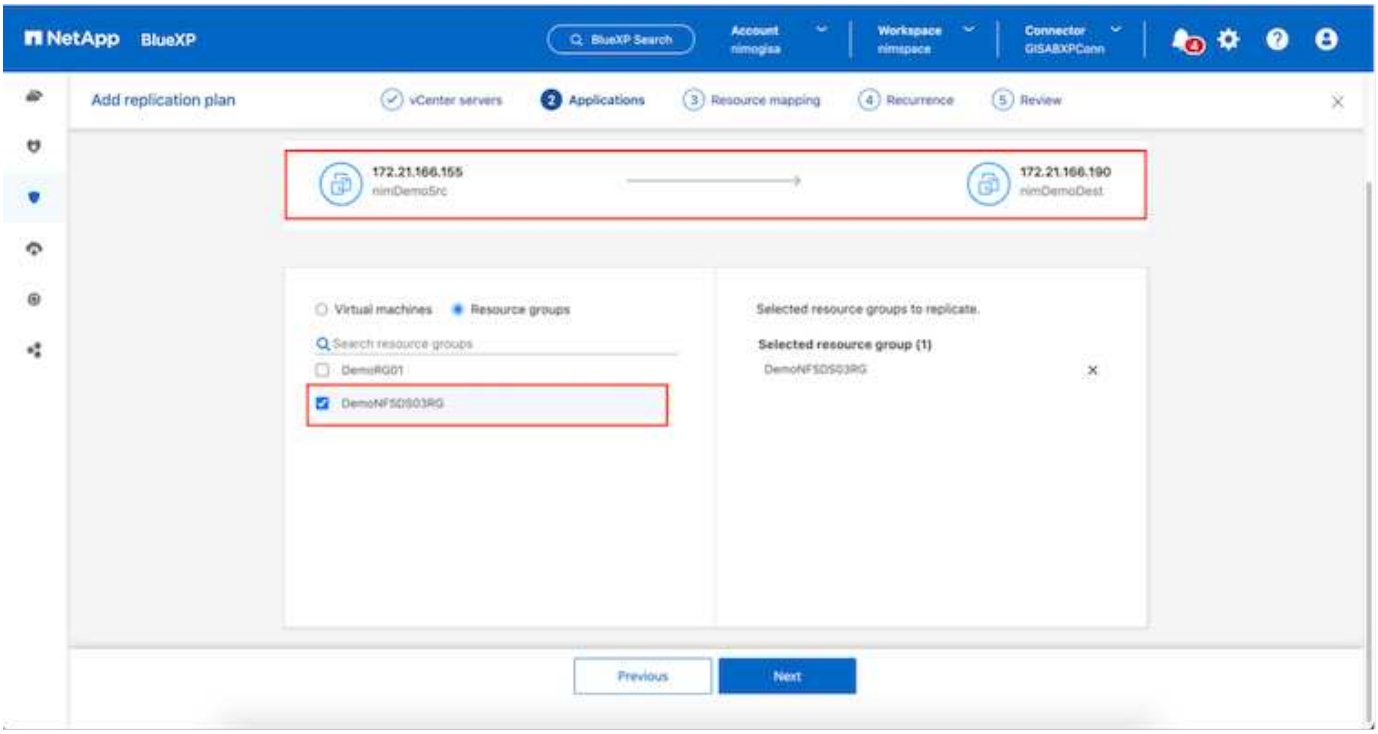
Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **piano di replica** e fare clic su **Aggiungi piano**.

Innanzitutto, selezionare vCenter di origine, quindi il vCenter di destinazione.



Il passaggio successivo consiste nel selezionare i gruppi di risorse esistenti. Se non vengono creati gruppi di risorse, la procedura guidata consente di raggruppare le macchine virtuali richieste (in pratica creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò consente inoltre di definire la sequenza operativa di

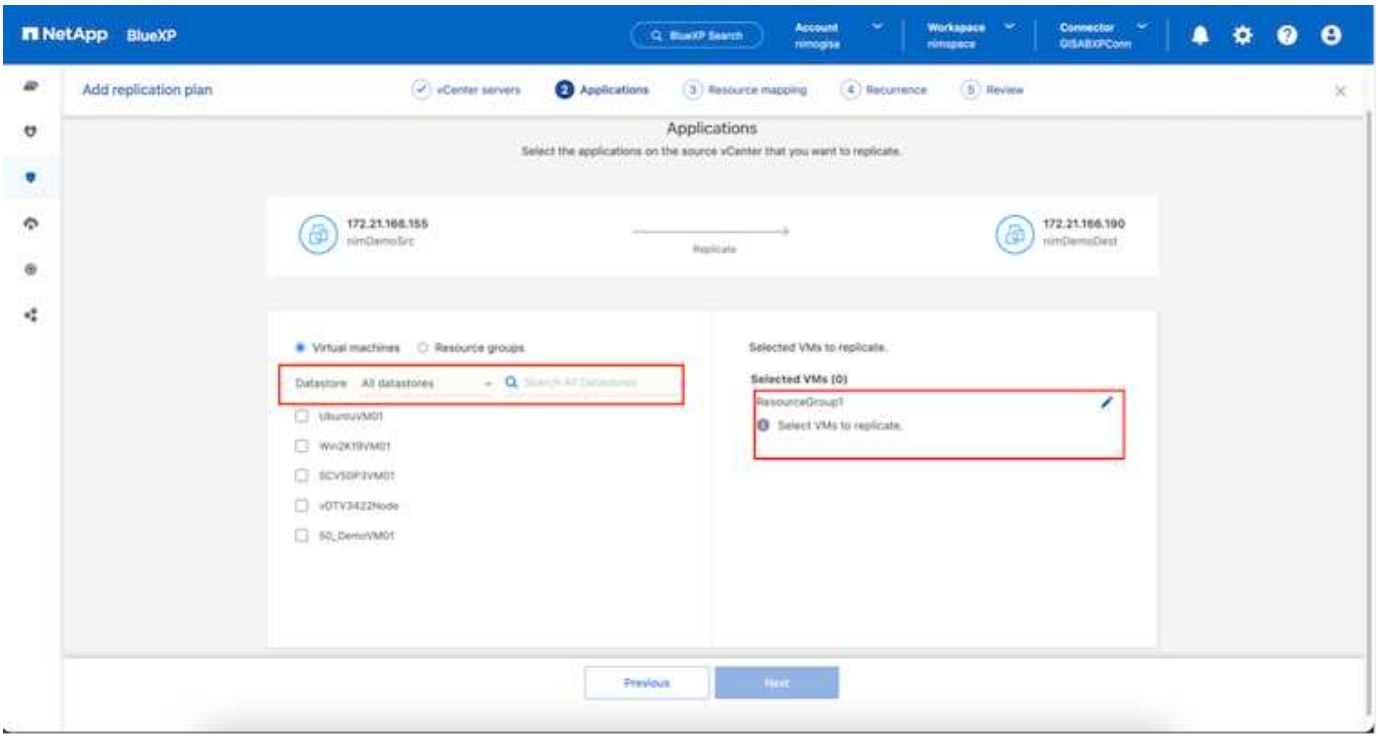
ripristino delle macchine virtuali delle applicazioni.



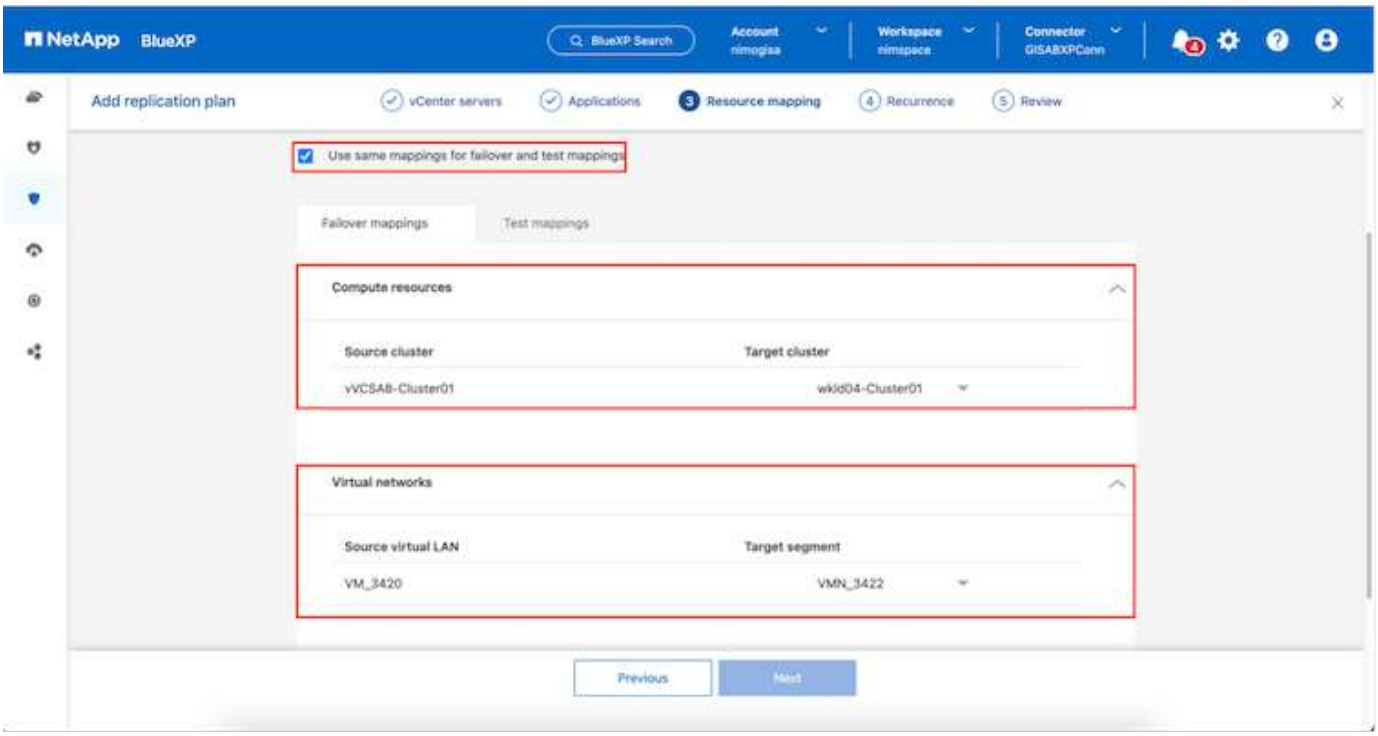
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine di accensione delle macchine virtuali durante il processo di ripristino.

Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Due gruppi di risorse vengono avviati in parallelo.

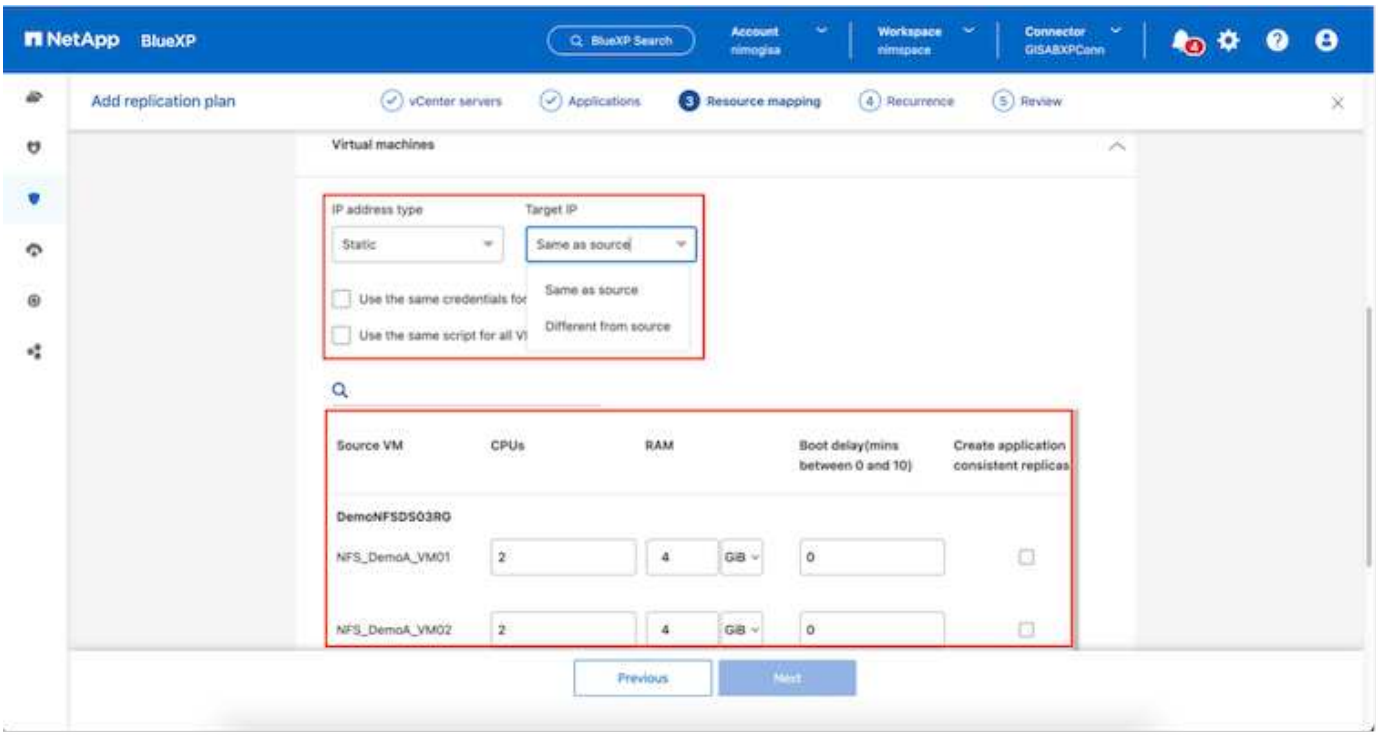
Lo screenshot seguente mostra la possibilità di filtrare le macchine virtuali o gli archivi dati specifici in base ai requisiti organizzativi se i gruppi di risorse non vengono creati in precedenza.



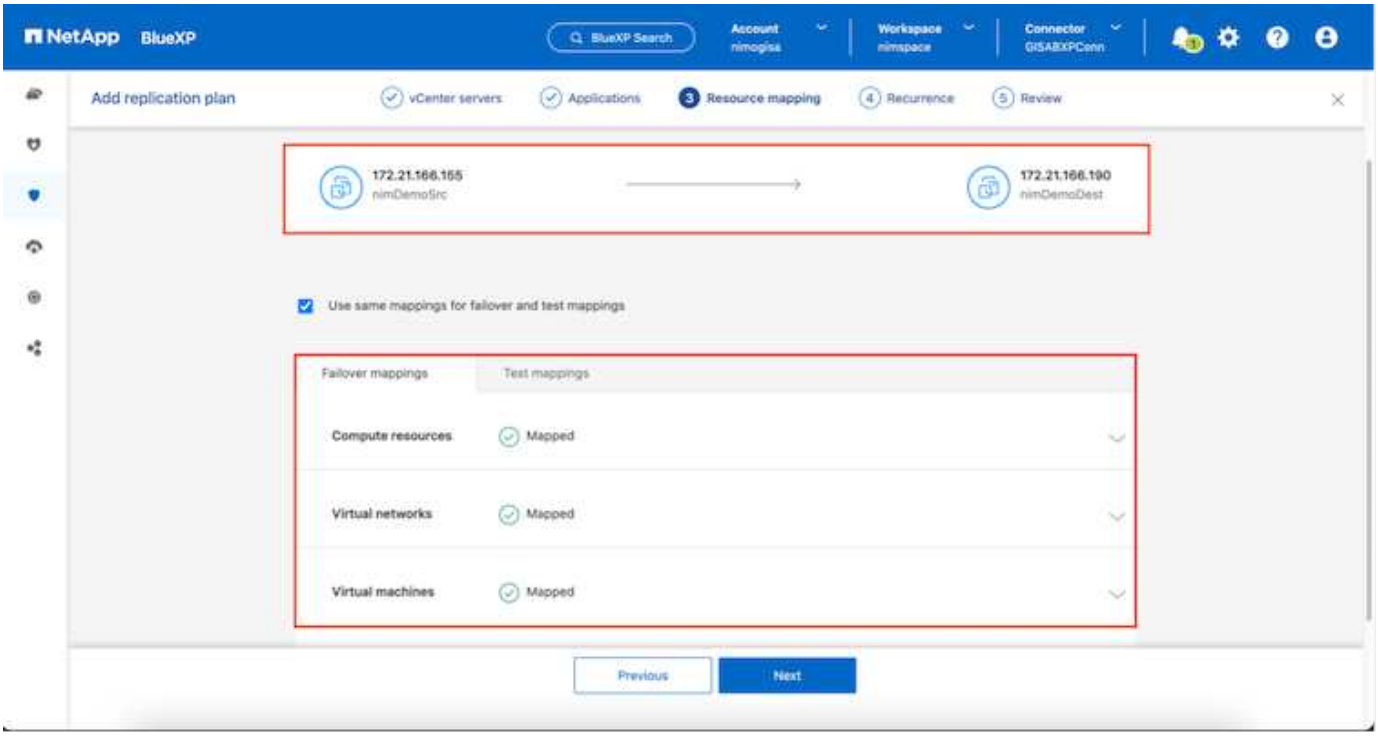
Una volta selezionati i gruppi di risorse, creare le mappature di failover. In questo passaggio, specificare il modo in cui le risorse dell'ambiente di origine vengono mappate alla destinazione. Sono incluse le risorse di elaborazione e le reti virtuali. Personalizzazione IP, pre e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento alla "Creare un piano di replica".



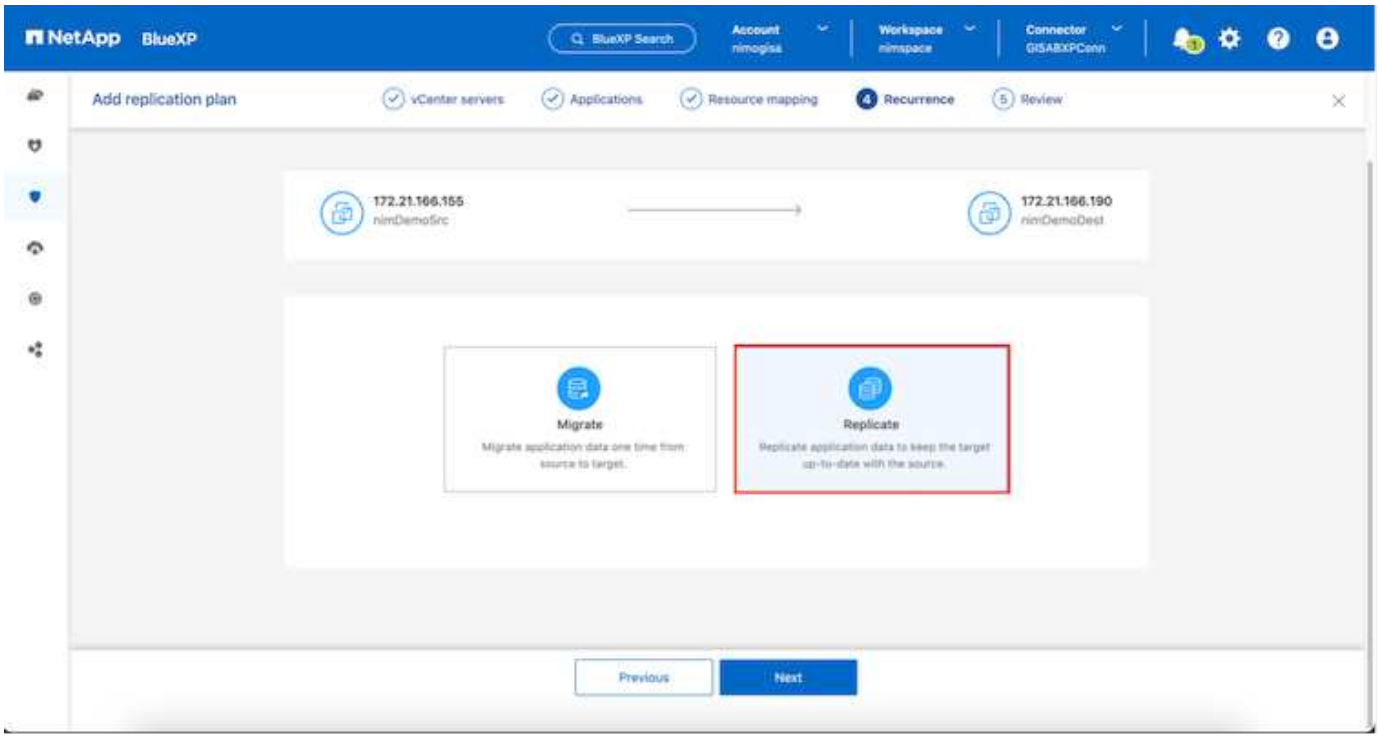
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per impostare mappature diverse per l'ambiente di test, selezionare l'opzione Test mapping (Test mapping) dopo aver deselezionato la casella di controllo come illustrato di seguito:



Una volta completata la mappatura delle risorse, fare clic su Avanti.

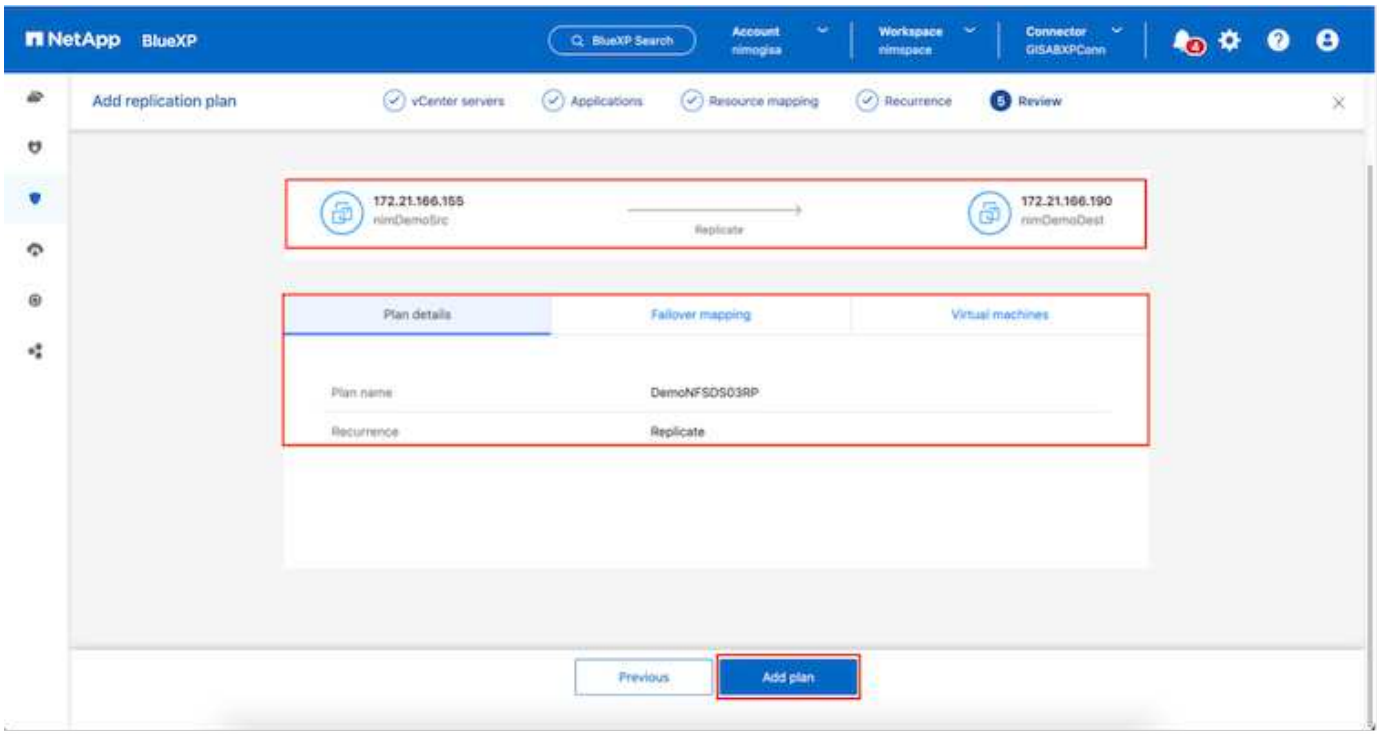


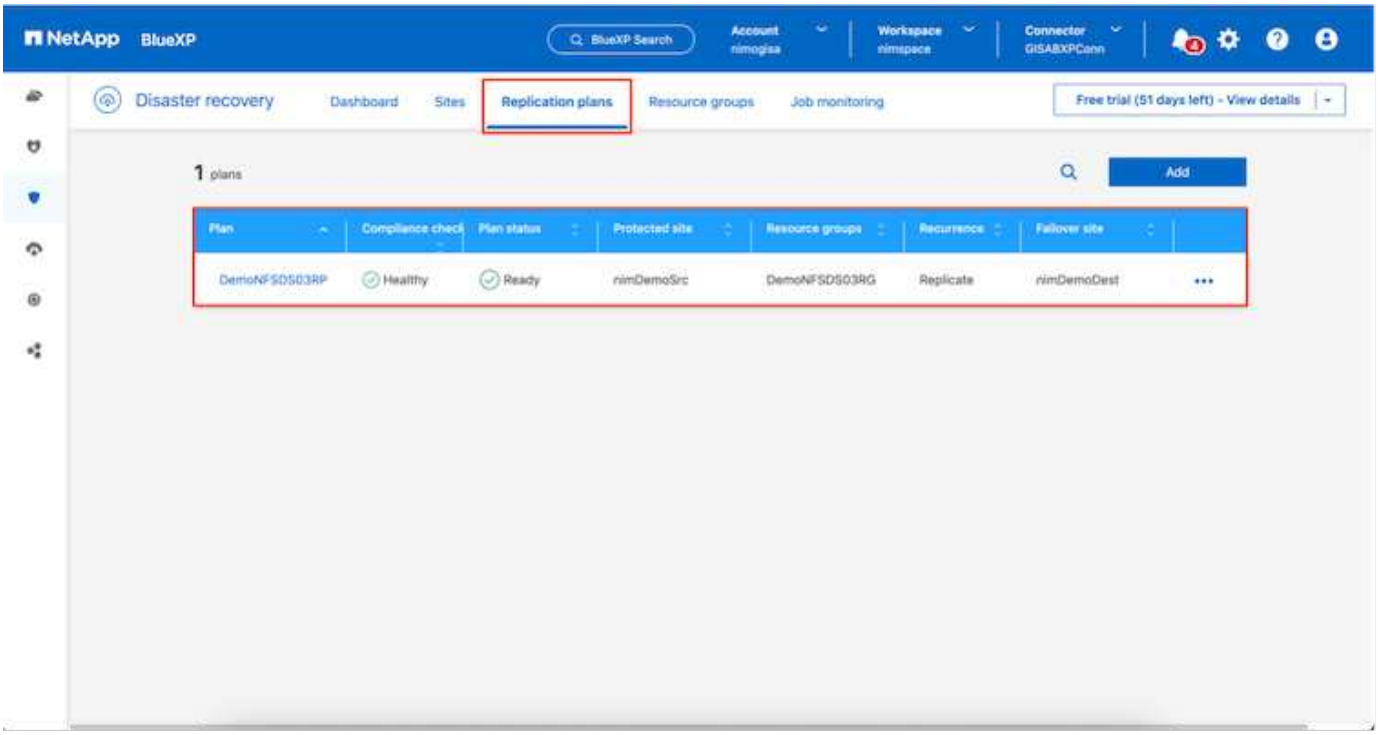
Selezionare il tipo di ricorrenza. In poche parole, selezionare l'opzione Migrate (migrazione una tantum tramite failover) o Replica continua ricorrente. In questa procedura dettagliata, l'opzione Replica è selezionata.



Al termine, rivedere le mappature create e fare clic su **Aggiungi piano**.

È possibile includere in un piano di replica macchine virtuali di volumi e SVM diversi. In base al posizionamento delle macchine virtuali (che si tratti dello stesso volume o di un volume separato all'interno della stessa SVM, di volumi separati su SVM diverse), il disaster recovery di BlueXP crea una snapshot del gruppo di coerenza.



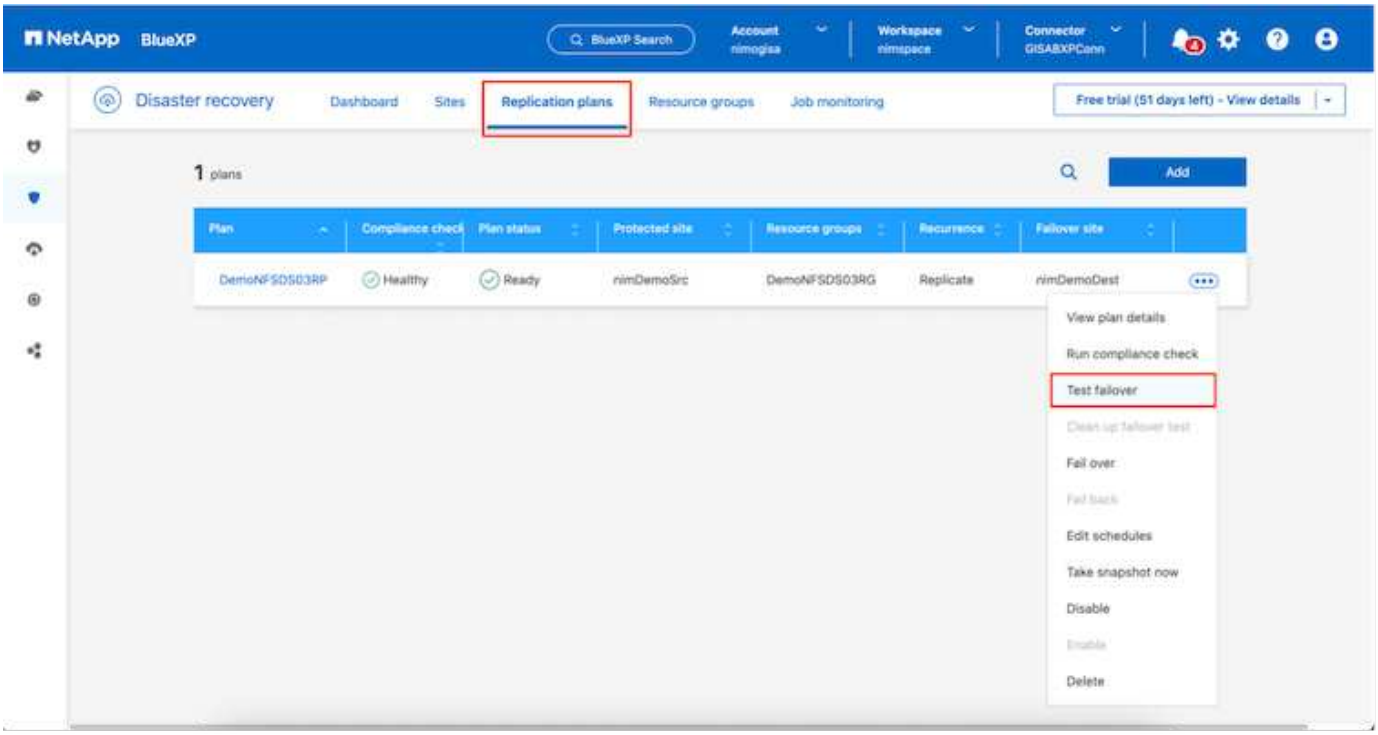


BlueXP DRaaS è costituito dai seguenti flussi di lavoro:

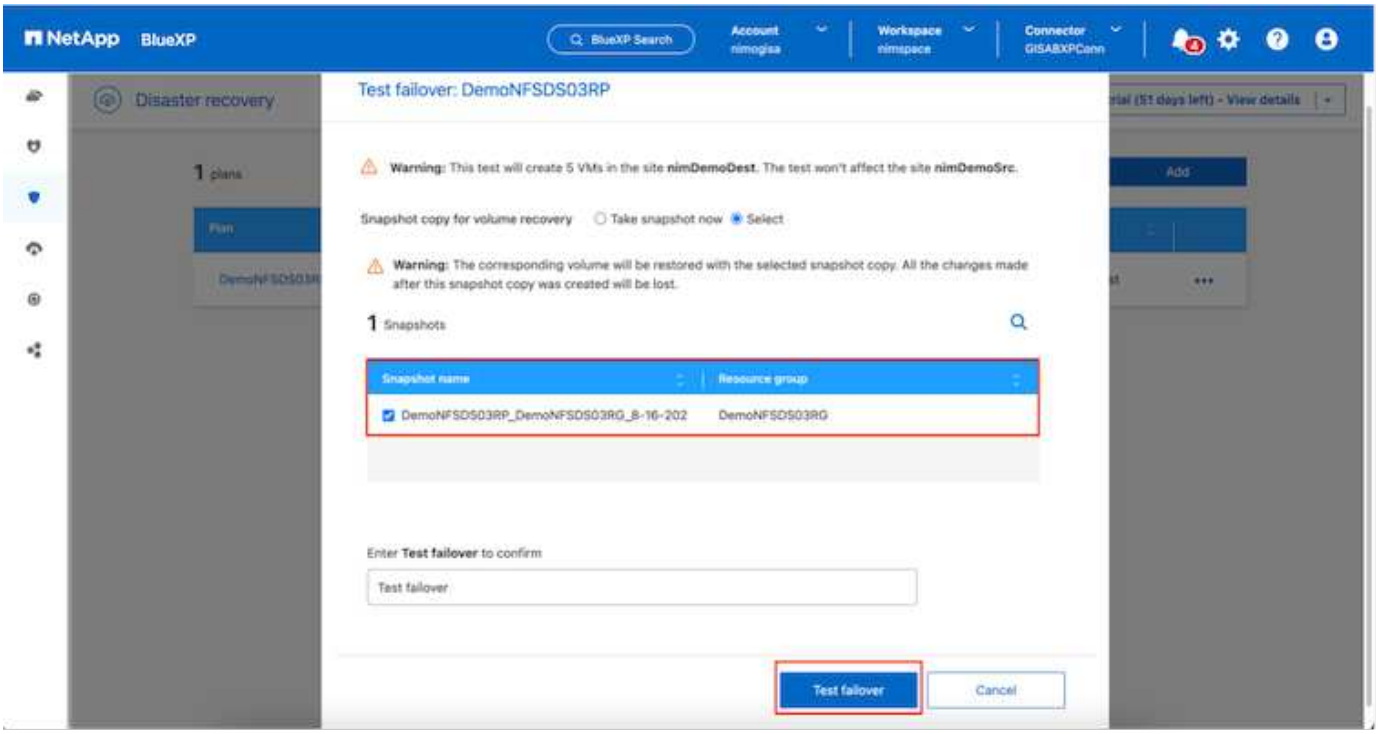
- Failover di test (incluse simulazioni periodiche automatizzate)
- Test di failover di cleanup
- Failover
- Failback

Test del failover

Il test di failover in BlueXP DRaaS è una procedura operativa che consente agli amministratori VMware di convalidare completamente i propri piani di ripristino senza interrompere gli ambienti di produzione.



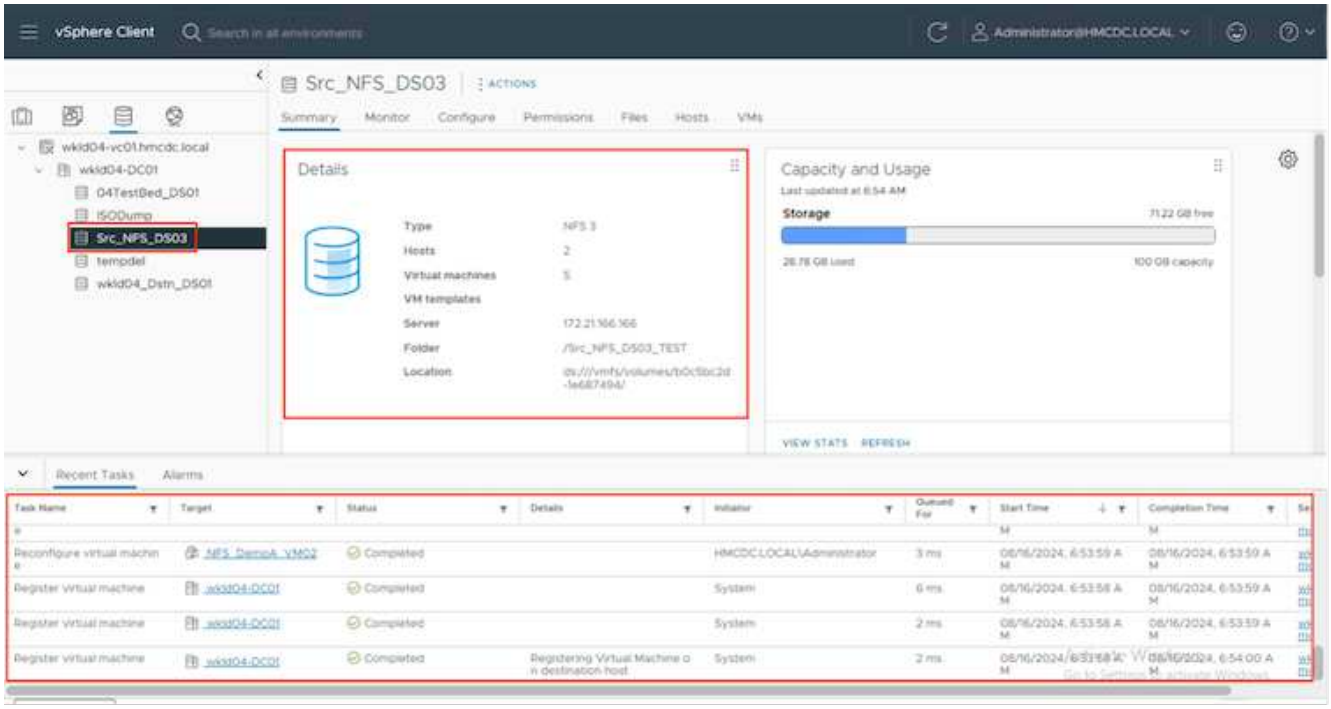
BlueXP DRaaS incorpora la capacità di selezionare lo snapshot come funzionalità opzionale nell'operazione di test failover. Questa funzionalità consente all'amministratore VMware di verificare che eventuali modifiche apportate di recente nell'ambiente vengano replicate nel sito di destinazione e quindi presenti durante il test. Tali modifiche includono patch al sistema operativo guest della VM



Quando l'amministratore VMware esegue un'operazione di failover di test, BlueXP DRaaS automatizza le seguenti attività:

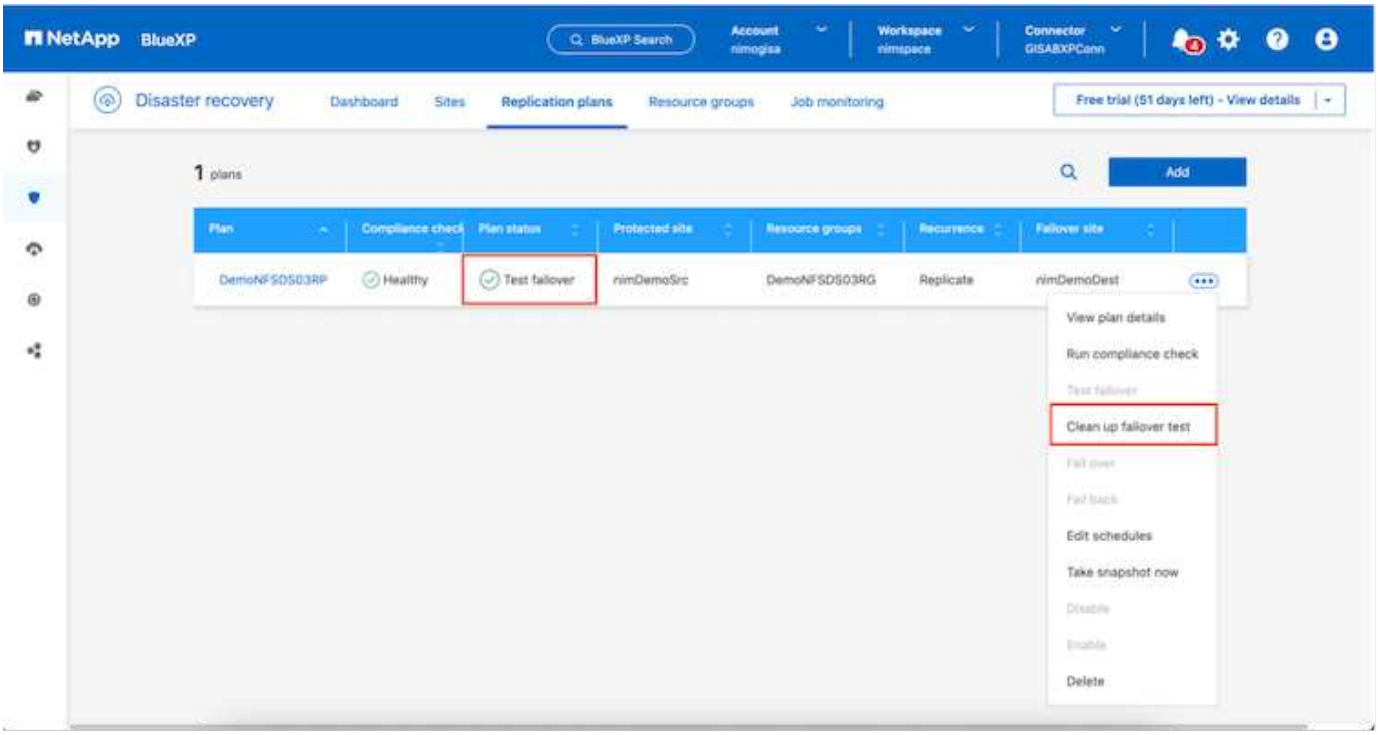
- Attivazione di relazioni SnapMirror per aggiornare lo storage nel sito di destinazione con eventuali modifiche recenti apportate nel sito di produzione.

- Creazione di volumi NetApp FlexClone dei volumi FlexVol sullo storage array di DR.
- Connessione dei datastore NFS nei volumi FlexClone agli host ESXi nel sito di DR.
- Collegamento degli adattatori di rete della macchina virtuale alla rete di test specificata durante la mappatura.
- Riconfigurazione delle impostazioni di rete del sistema operativo guest della VM in base a quanto definito per la rete nel sito DR.
- Eseguire tutti i comandi personalizzati memorizzati nel piano di replica.
- Accensione delle macchine virtuali nell'ordine definito nel piano di replica.



Pulizia dell'operazione del test di failover

L'operazione di verifica del failover di cleanup si verifica dopo che il test del piano di replica è stato completato e l'amministratore VMware risponde al prompt di cleanup.



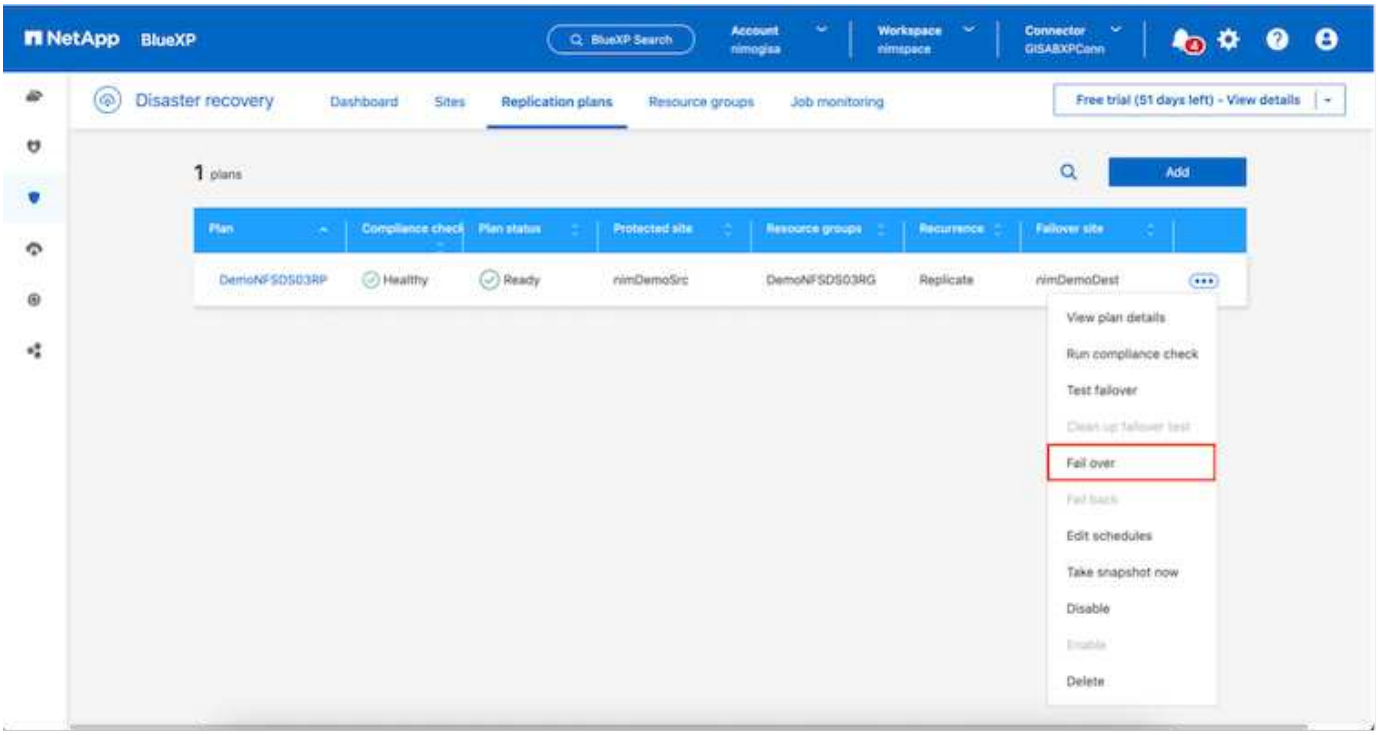
Questa azione ripristina le macchine virtuali (VM) e lo stato del piano di replica allo stato pronto.

Quando l'amministratore VMware esegue un'operazione di ripristino, BlueXP DRaaS completa il seguente processo:

1. Ogni macchina virtuale recuperata nella copia FlexClone utilizzata per il test viene spenta.
2. Elimina il volume FlexClone utilizzato per presentare le macchine virtuali recuperate durante il test.

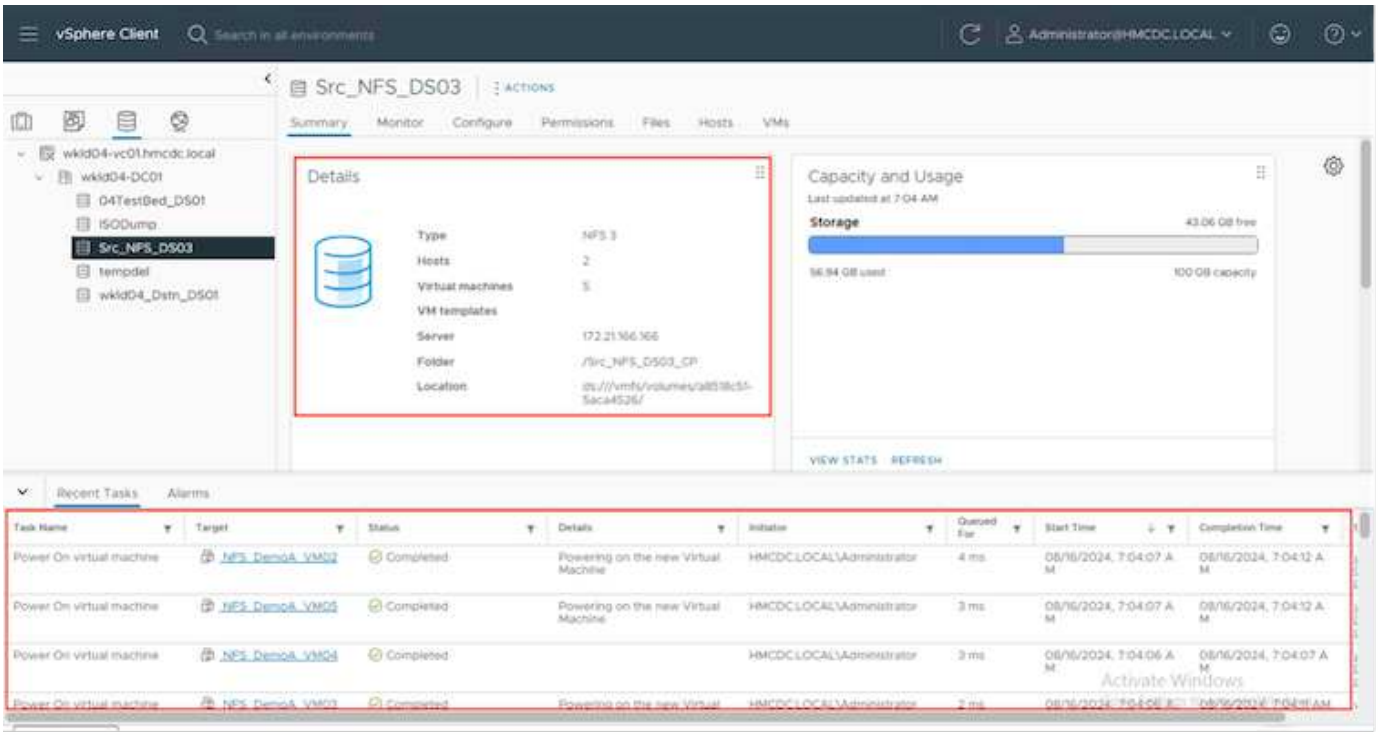
Migrazione pianificata e failover

BlueXP DRaaS offre due metodi per eseguire un vero failover: Migrazione pianificata e failover. Il primo metodo, la migrazione pianificata, comprende l'arresto delle macchine virtuali e la sincronizzazione della replica dello storage nel processo per ripristinare o spostare in modo efficace le macchine virtuali nel sito di destinazione. La migrazione pianificata richiede l'accesso al sito di origine. Il secondo metodo, il failover, è un failover pianificato/non pianificato in cui le macchine virtuali vengono ripristinate nel sito di destinazione dall'ultimo intervallo di replica dello storage in grado di essere completate. A seconda dell'RPO progettato nella soluzione, è prevista una certa quantità di perdita di dati nello scenario di DR.



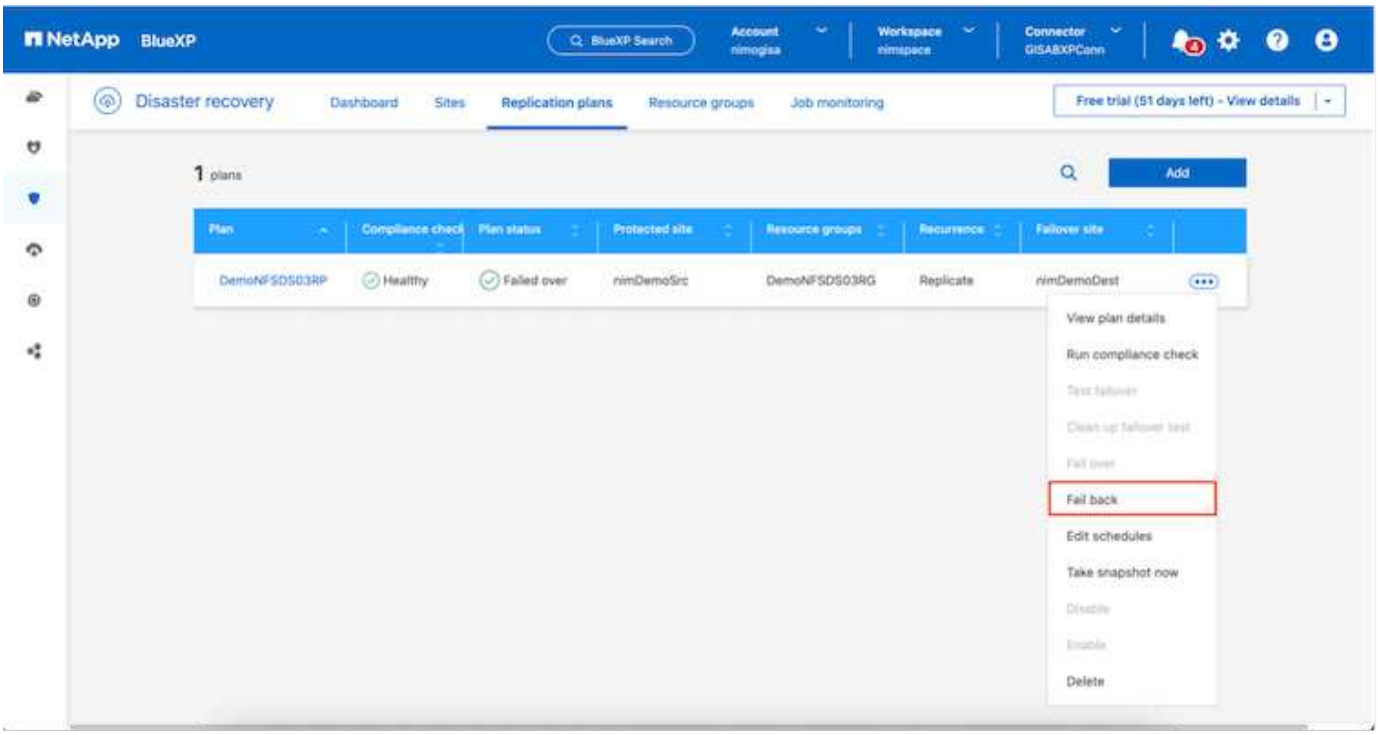
Quando l'amministratore VMware esegue un'operazione di failover, BlueXP DRaaS automatizza le seguenti attività:

- Interrompere e failover le relazioni NetApp SnapMirror.
- Collegare i datastore NFS replicati agli host ESXi nel sito di DR.
- Collegare gli adattatori di rete della macchina virtuale alla rete del sito di destinazione appropriata.
- Riconfigurare le impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito di destinazione.
- Eseguire eventuali comandi personalizzati (se presenti) memorizzati nel piano di replica.
- Accendere le macchine virtuali nell'ordine definito nel piano di replica.



Failback

Un failback è una procedura opzionale che ripristina la configurazione originale dei siti di origine e di destinazione dopo un ripristino.



Gli amministratori VMware possono configurare ed eseguire una procedura di failback quando sono pronti per ripristinare i servizi nel sito di origine.

NOTA: BlueXP DRaaS replica (resyncs) qualsiasi modifica alla macchina virtuale di origine prima di invertire la direzione di replica. Questo processo inizia da una relazione che ha completato il failover a una destinazione

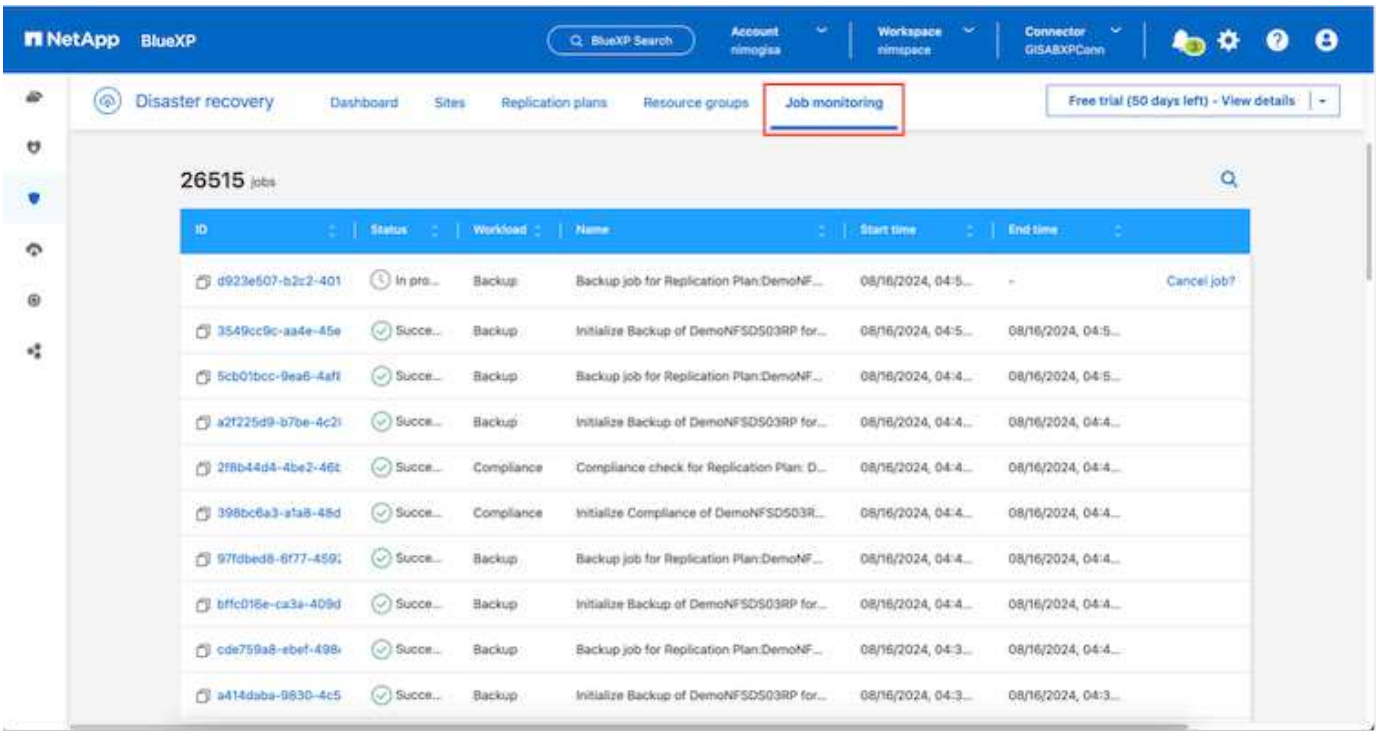
e prevede i seguenti passaggi:

- Spegnere e annullare la registrazione delle macchine virtuali e dei volumi sul sito di destinazione vengono dismontati.
- Interrompere la relazione SnapMirror sull'origine è interrotta per renderla di lettura/scrittura.
- Risincronizzazione della relazione di SnapMirror per invertire la replica.
- Montare il volume sulla sorgente, accendere e registrare le macchine virtuali di origine.

Per ulteriori informazioni sull'accesso e la configurazione di BlueXP DRaaS, vedere "Ulteriori informazioni su Disaster Recovery BlueXP per VMware".

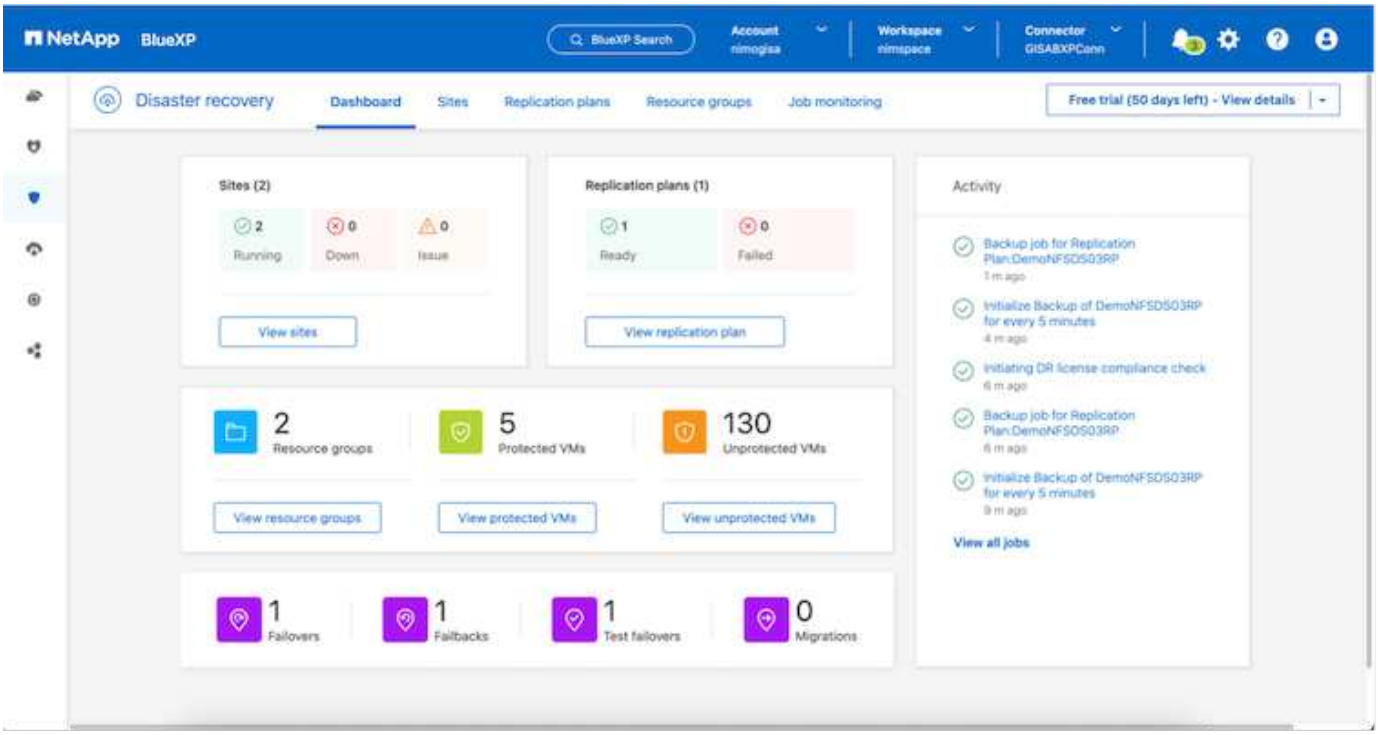
Monitoring e dashboard

Da BlueXP o dalla CLI di ONTAP, puoi monitorare lo stato di salute della replica per i volumi del datastore appropriati e lo stato di un failover o di un failover di test può essere monitorato tramite il monitoraggio dei processi.



Se un lavoro è attualmente in corso o in coda e si desidera interromperlo, è possibile annullarlo.

Grazie alla dashboard di disaster recovery di BlueXP , puoi valutare in modo sicuro lo stato dei siti di disaster recovery e dei piani di replica. Ciò consente agli amministratori di identificare rapidamente siti e piani sani, scollegati o degradati.



Ciò fornisce una soluzione potente per gestire un piano di disaster recovery personalizzato e personalizzato. Il failover può essere eseguito come failover pianificato o failover con un clic su un pulsante in caso di disastro e si decide di attivare il sito di DR.

Per ulteriori informazioni su questo processo, è possibile seguire il video dettagliato della procedura dettagliata o utilizzare la "simulatore di soluzione".

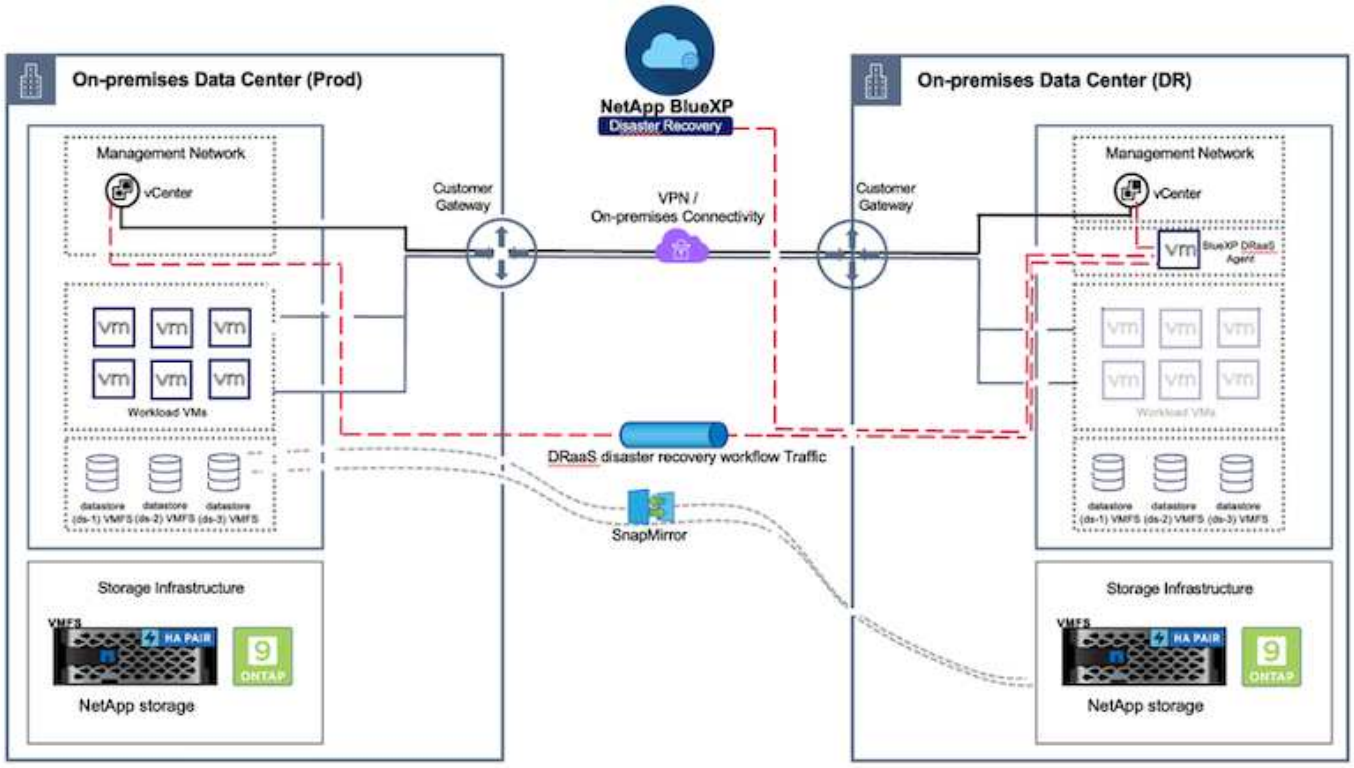
Dr utilizzando BlueXP DRaaS per archivi dati VMFS

Il disaster recovery che utilizza la replica a livello di blocco dal sito di produzione al sito di disaster recovery è un modo resiliente e conveniente di proteggere i carichi di lavoro dai fuori servizio del sito e dagli eventi di corruzione dei dati, come gli attacchi ransomware. Con la replica di NetApp SnapMirror, i carichi di lavoro VMware in esecuzione sui sistemi ONTAP on-premise che utilizzano un datastore VMFS possono essere replicati in un altro sistema storage ONTAP in un data center di recovery designato dove risiede VMware

Questa sezione del documento descrive la configurazione di BlueXP DRaaS per l'impostazione del disaster recovery per VM VMware on-premise in un altro sito designato. Durante questa configurazione, l'account BlueXP , BlueXP Connector, gli array ONTAP aggiunti nell'area di lavoro BlueXP , necessaria per consentire la comunicazione da VMware vCenter allo storage ONTAP. Inoltre, in questo documento viene descritto come configurare la replica tra siti e come impostare e verificare un piano di ripristino. L'ultima sezione contiene istruzioni per l'esecuzione di un failover completo del sito e per il failback quando il sito primario viene recuperato e acquistato online.

Grazie al servizio di disaster recovery BlueXP , integrato nella console NetApp BlueXP , i clienti possono rilevare i propri VMware vCenter on-premise e lo storage ONTAP, creare raggruppamenti di risorse, creare un piano di disaster recovery, associarlo a gruppi di risorse e verificare o eseguire failover e failback. SnapMirror offre una replica dei blocchi a livello di storage per mantenere aggiornati i due siti con modifiche incrementali, con un RPO fino a 5 minuti. È anche possibile simulare procedure di DR come esercizio normale senza alcun impatto sulla produzione e sui datastore replicati o senza incorrere in costi di storage aggiuntivi. Il disaster recovery di BlueXP sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di

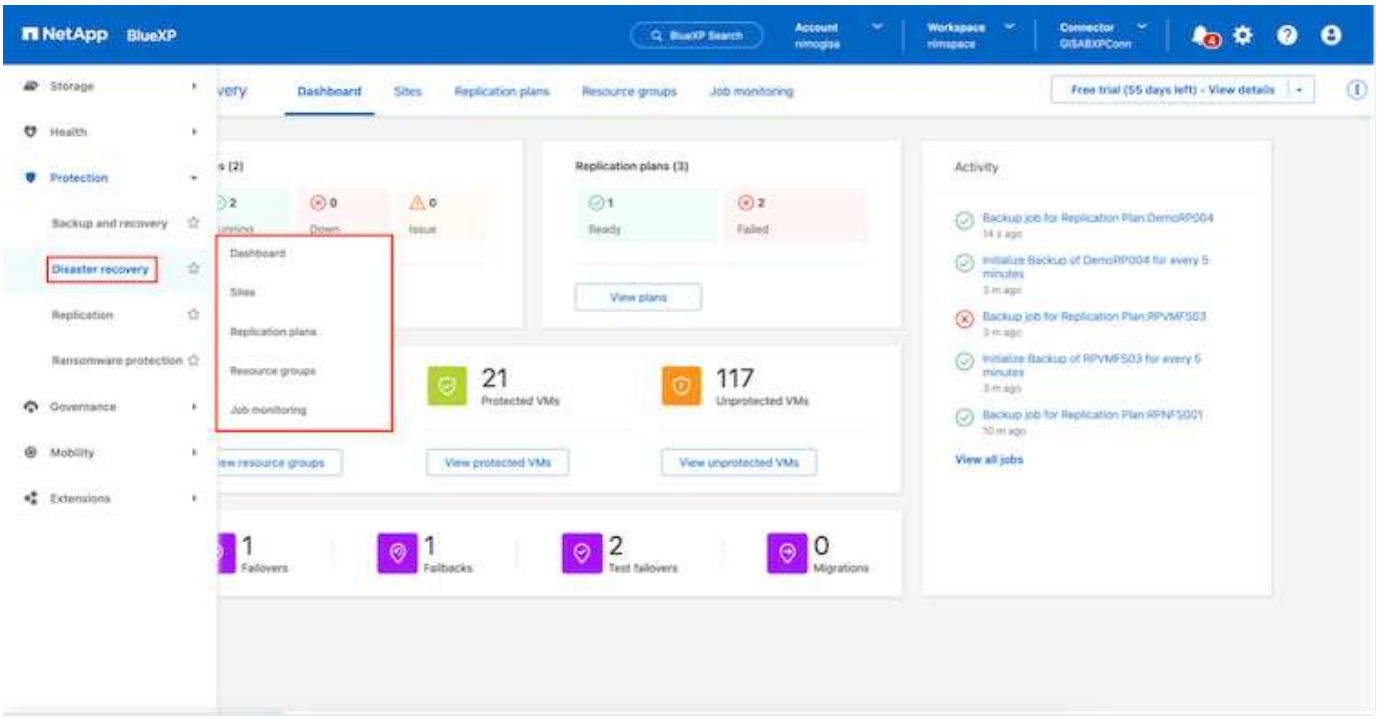
spazio del datastore VMFS dall'ultima snapshot replicata nel sito di disaster recovery. Una volta completato il test di DR, i clienti possono semplicemente eliminare l'ambiente di test senza alcun impatto sulle risorse di produzione effettivamente replicate. In caso di necessità (pianificata o meno) di un failover effettivo, con pochi clic, il servizio di disaster recovery BlueXP orchestrerà tutti i passaggi necessari per attivare automaticamente le macchine virtuali protette sul sito di disaster recovery designato. Il servizio inverte inoltre la relazione SnapMirror al sito primario e replicherà eventuali modifiche da secondario a primario per un'operazione di failback, se necessario. Tutto questo può essere ottenuto con una frazione di costo rispetto ad altre alternative ben note.



Per iniziare

Per iniziare con il disaster recovery di BlueXP , usa la console BlueXP e accedi al servizio.

1. Accedere a BlueXP.
2. Dal sistema di navigazione BlueXP sinistro, selezionare protezione > Disaster Recovery.
3. Viene visualizzata la dashboard di disaster recovery di BlueXP .

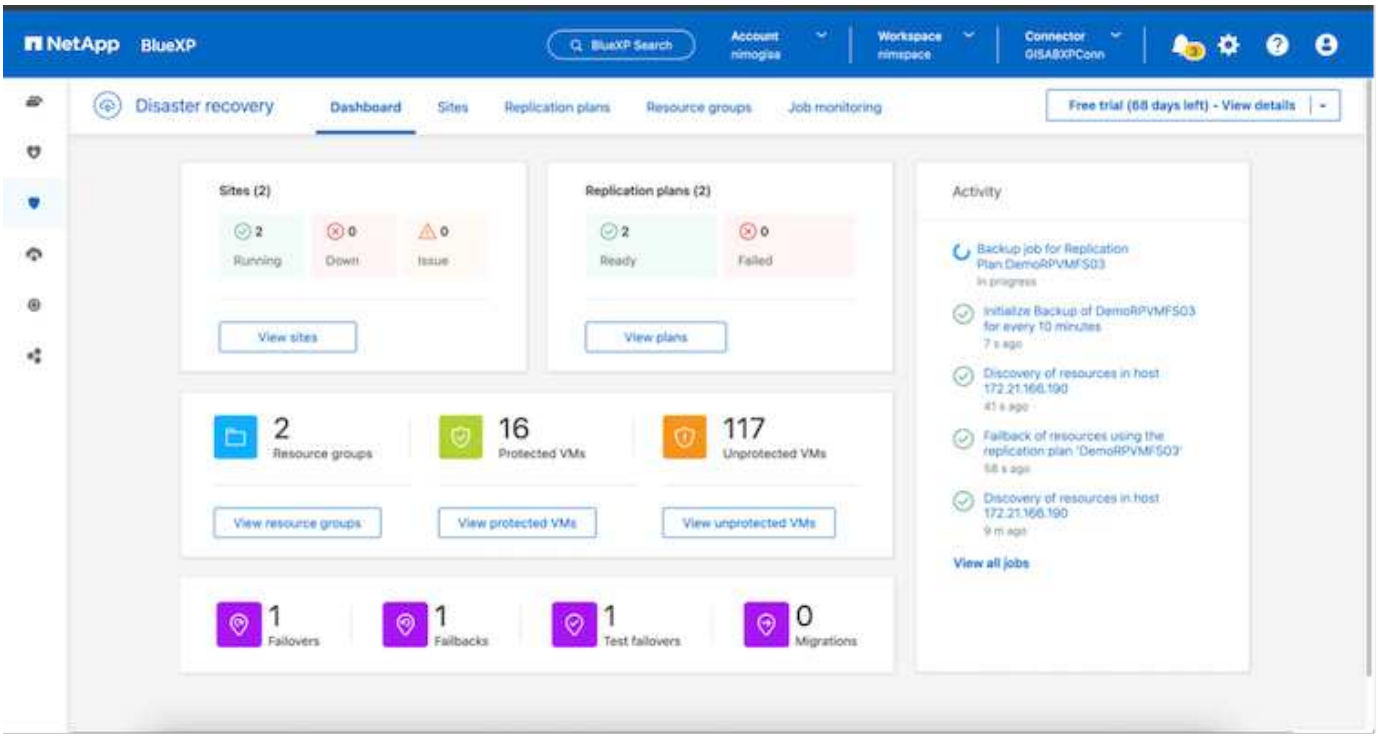


Prima di configurare il piano di disaster recovery, verificare che siano soddisfatti i seguenti prerequisiti:

- BlueXP Connector è impostato in NetApp BlueXP . Il connettore deve essere implementato nel VPC AWS.
- L'istanza di BlueXP Connector dispone di connettività ai sistemi storage e vCenter di origine e destinazione.
- I sistemi di storage NetApp on-premise che ospitano datastore VMFS per VMware vengono aggiunti in BlueXP .
- Quando si utilizzano nomi DNS, la risoluzione DNS deve essere attiva. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi del datastore designati basati su VMFS.

Una volta stabilita la connettività tra i siti di origine e di destinazione, procedere con la procedura di configurazione, che dovrebbe richiedere da 3 a 5 minuti.

NetApp consiglia di installare BlueXP Connector nel sito di disaster recovery o in un terzo sito, in modo che BlueXP Connector possa comunicare attraverso la rete con le risorse di origine e destinazione in caso di black-out reali o disastri naturali.

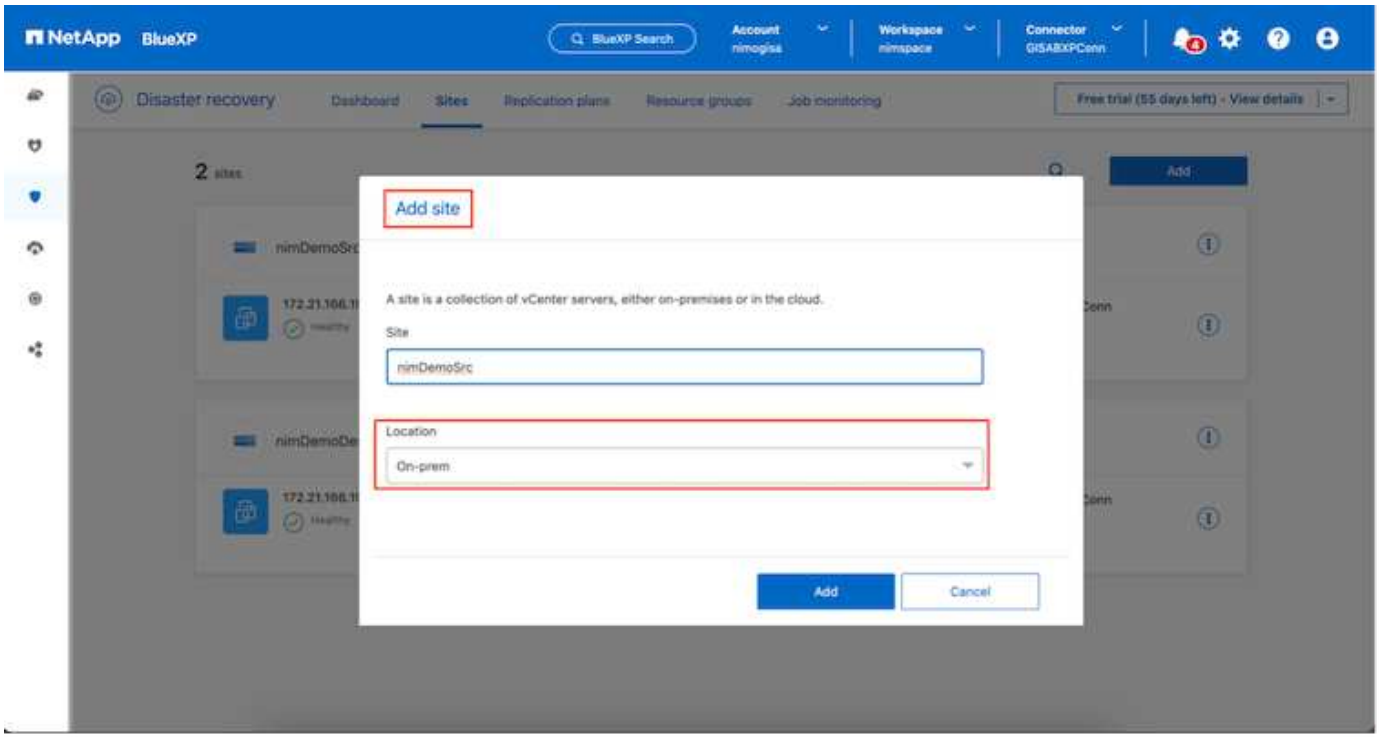


Durante la scrittura di questo documento, il supporto per datastore VMFS da on-premise a on-premise è in anteprima tecnologica. La funzionalità è supportata con datastore VMFS basati su protocollo FC e ISCSI.

Configurazione del disaster recovery BlueXP

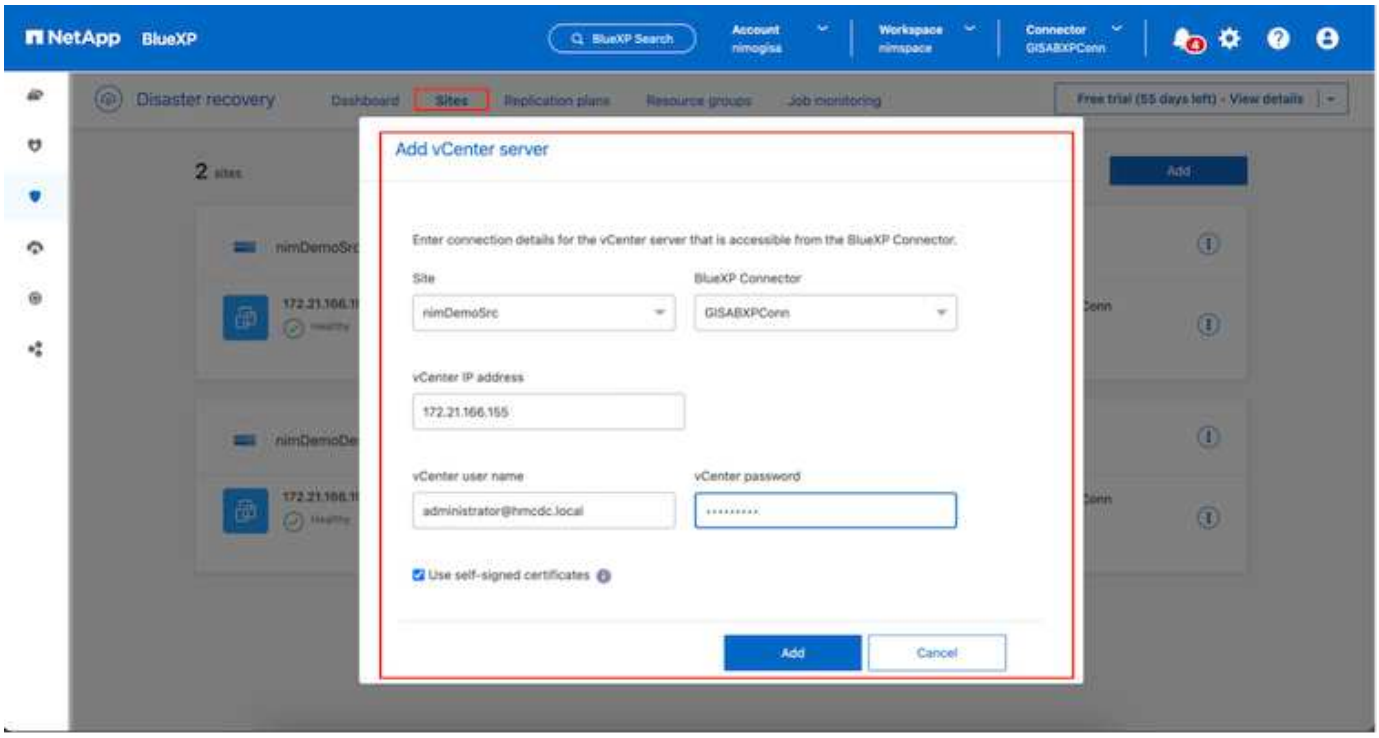
Il primo passo per prepararsi al disaster recovery è il rilevamento e l'aggiunta delle risorse di storage e vCenter on-premise al disaster recovery di BlueXP .

Verifica che i sistemi storage ONTAP vengano aggiunti all'ambiente di lavoro all'interno del Canvas. Aprire la console BlueXP e selezionare **protezione > Ripristino di emergenza** dal menu di navigazione sinistro. Selezionare **Scopri i server vCenter** o utilizzare il menu principale, selezionare **Siti > Aggiungi > Aggiungi vCenter**.

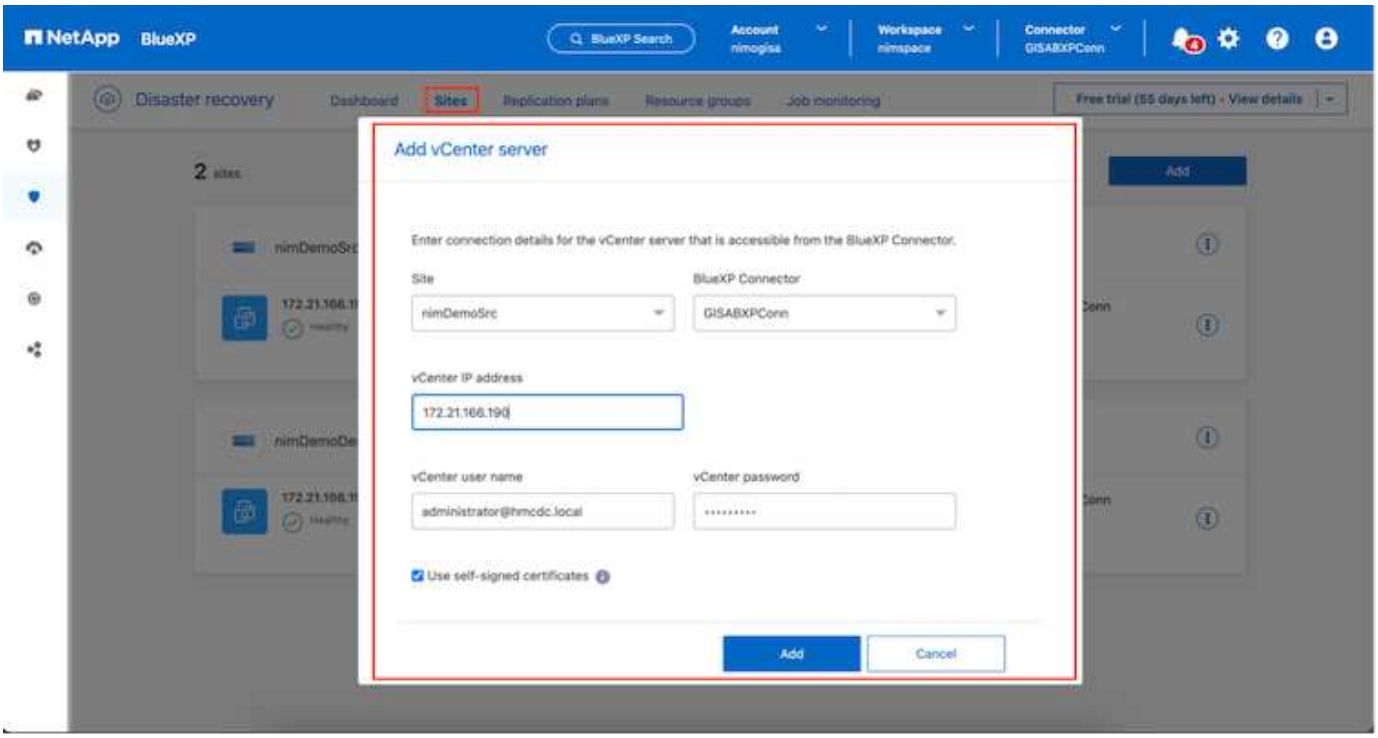


Aggiungere le seguenti piattaforme:

- **Fonte**. VCenter on-premise.



- **Destinazione**. VCenter SDDC di VMC.



Una volta aggiunti i vCenter, viene attivato il rilevamento automatico.

Configurazione della replica dello storage tra il sito di origine e quello di destinazione

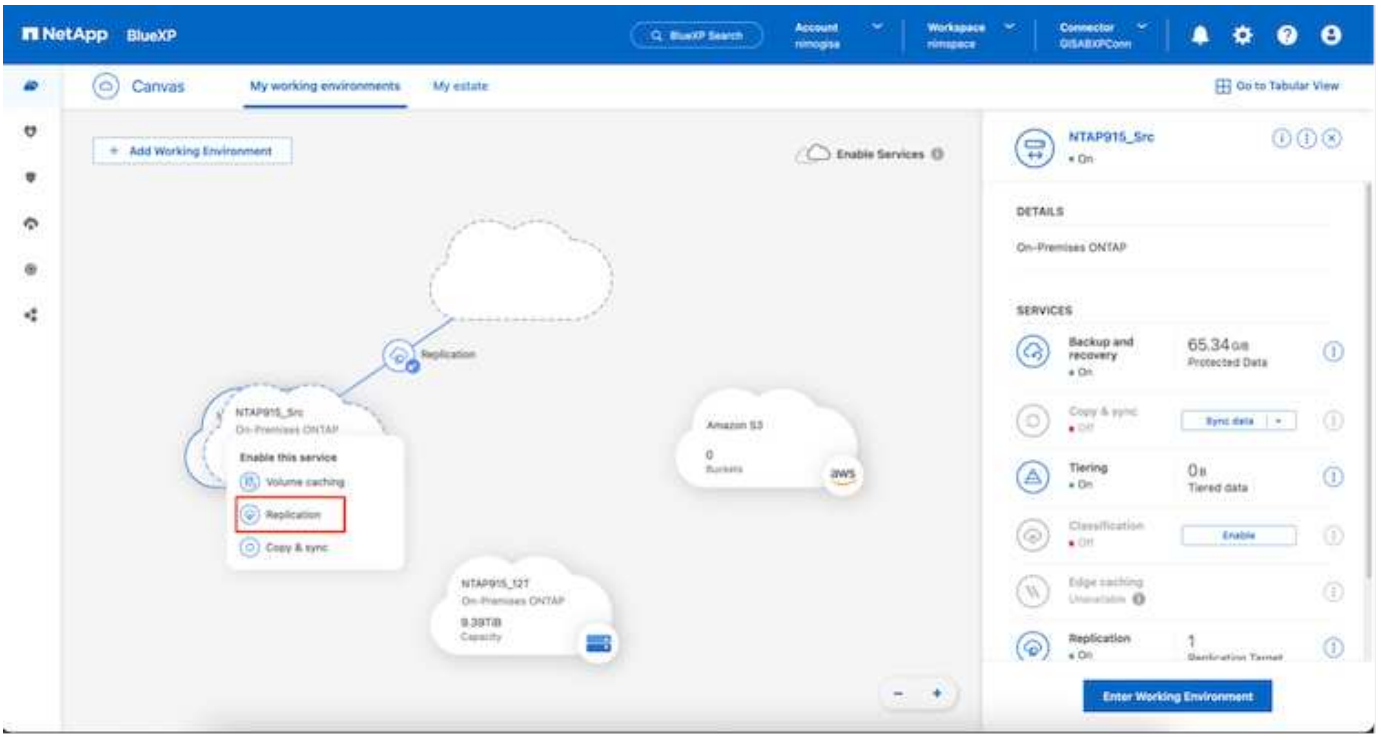
SnapMirror utilizza le snapshot ONTAP per gestire il trasferimento dei dati da una posizione all'altra. Inizialmente, una copia completa basata su uno snapshot del volume di origine viene copiata nella destinazione per eseguire una sincronizzazione di base. Quando si verificano modifiche ai dati nell'origine, viene creato un nuovo snapshot e confrontato con quello di base. I blocchi modificati vengono quindi replicati nella destinazione, con lo snapshot più recente che diventa la base corrente o lo snapshot comune più recente. Ciò consente di ripetere il processo e di inviare aggiornamenti incrementali alla destinazione.

Una volta stabilita una relazione SnapMirror, il volume di destinazione è in stato di sola lettura online e pertanto è ancora accessibile. SnapMirror funziona con blocchi fisici di storage, piuttosto che a un file o a un altro livello logico. Ciò significa che il volume di destinazione è una replica identica dell'origine, inclusi snapshot, impostazioni del volume, ecc. se il volume di origine utilizza funzionalità di efficienza dello spazio ONTAP, come compressione e deduplica dei dati, il volume replicato conserverà queste ottimizzazioni.

L'interruzione della relazione di SnapMirror rende scrivibile il volume di destinazione e di solito viene utilizzato per eseguire un failover quando si utilizza SnapMirror per sincronizzare i dati in un ambiente di DR. SnapMirror è abbastanza sofisticato da consentire la risincronizzazione efficiente dei dati modificati nel sito di failover nel sistema primario, nel caso in cui successivamente tornino online e quindi il ristabilimento della relazione SnapMirror originale.

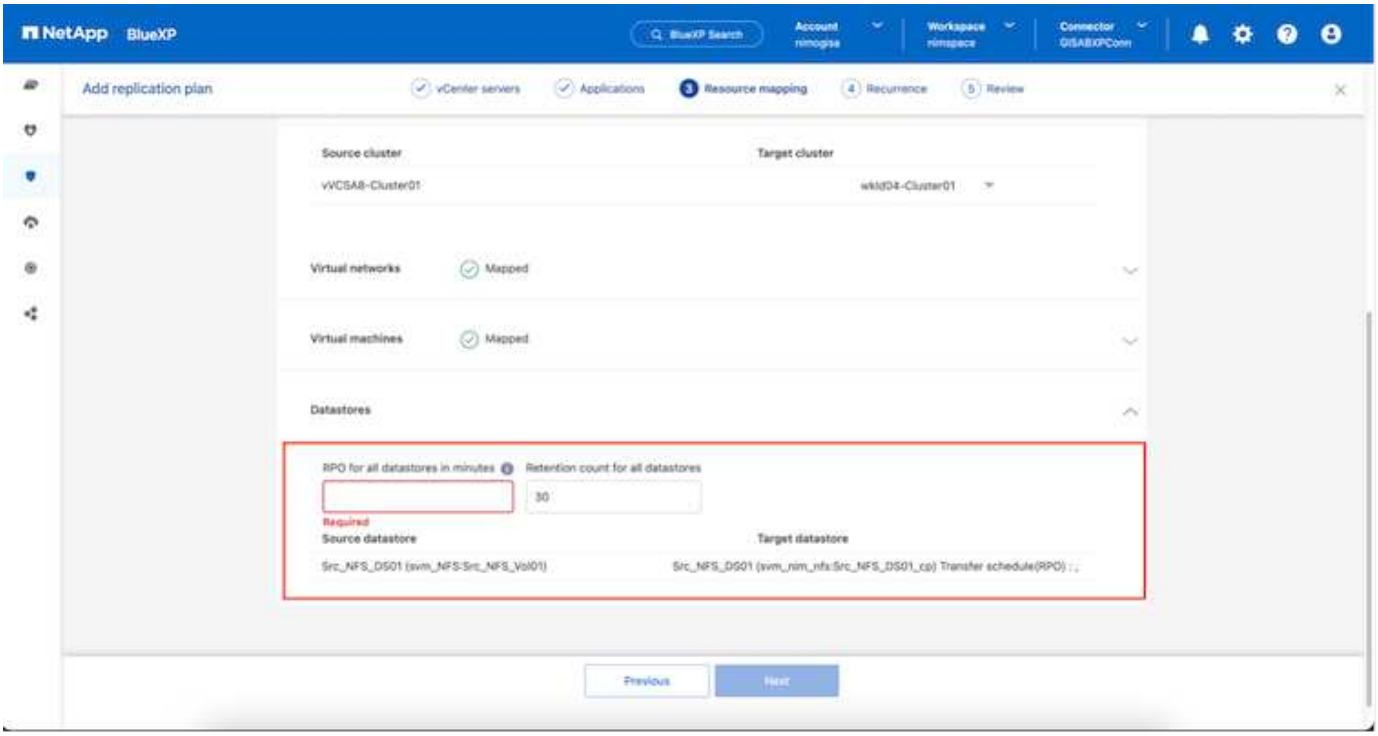
Come configurarlo per il Disaster Recovery VMware

Il processo di creazione della replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice consiste nell'utilizzare BlueXP per configurare la replica SnapMirror utilizzando il semplice drag & drop del sistema ONTAP di origine nell'ambiente sulla destinazione per attivare la procedura guidata che guida per il resto del processo.



BlueXP DRaaS può automatizzare anche lo stesso, purché vengano soddisfatti i due criteri seguenti:

- I cluster di origine e di destinazione hanno una relazione peer.
- La SVM di origine e la SVM di destinazione hanno una relazione di tipo peer.

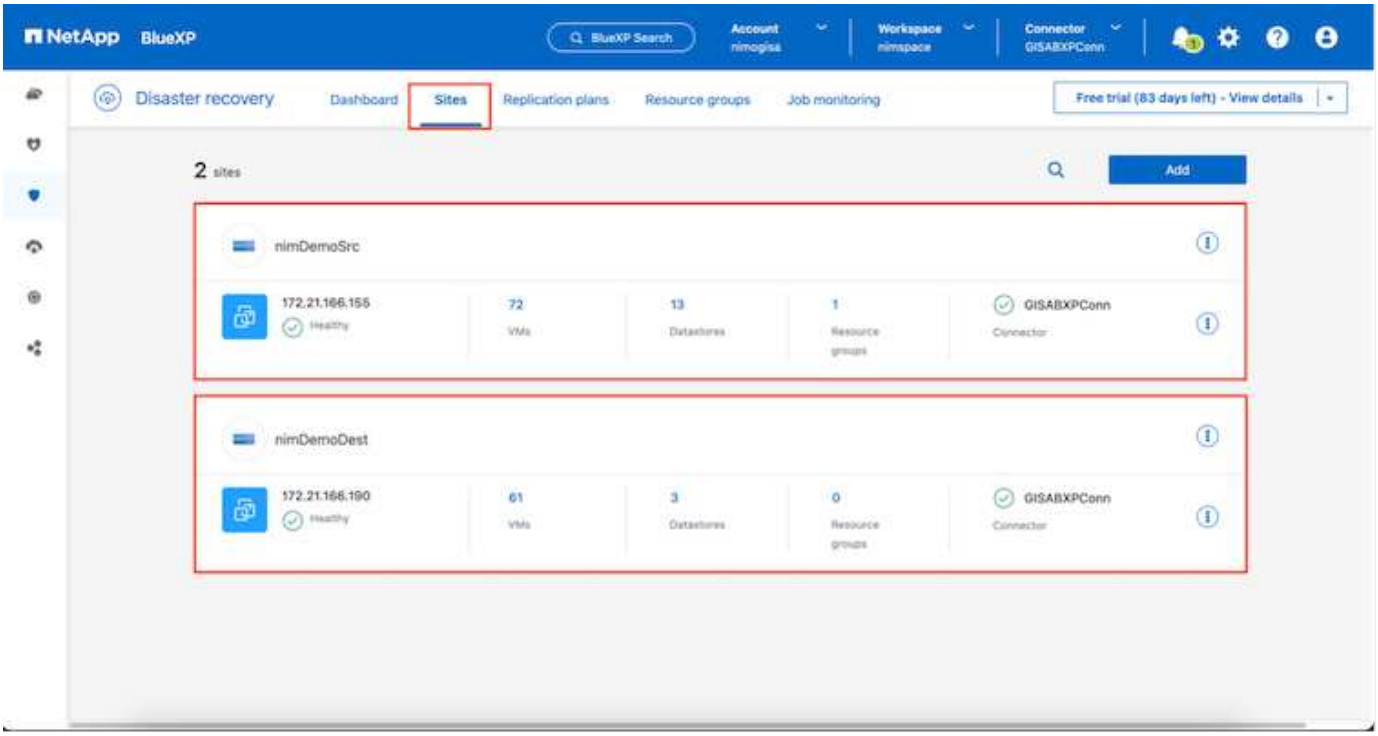


Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS raccoglie la relazione e continua con il resto delle operazioni del workflow.

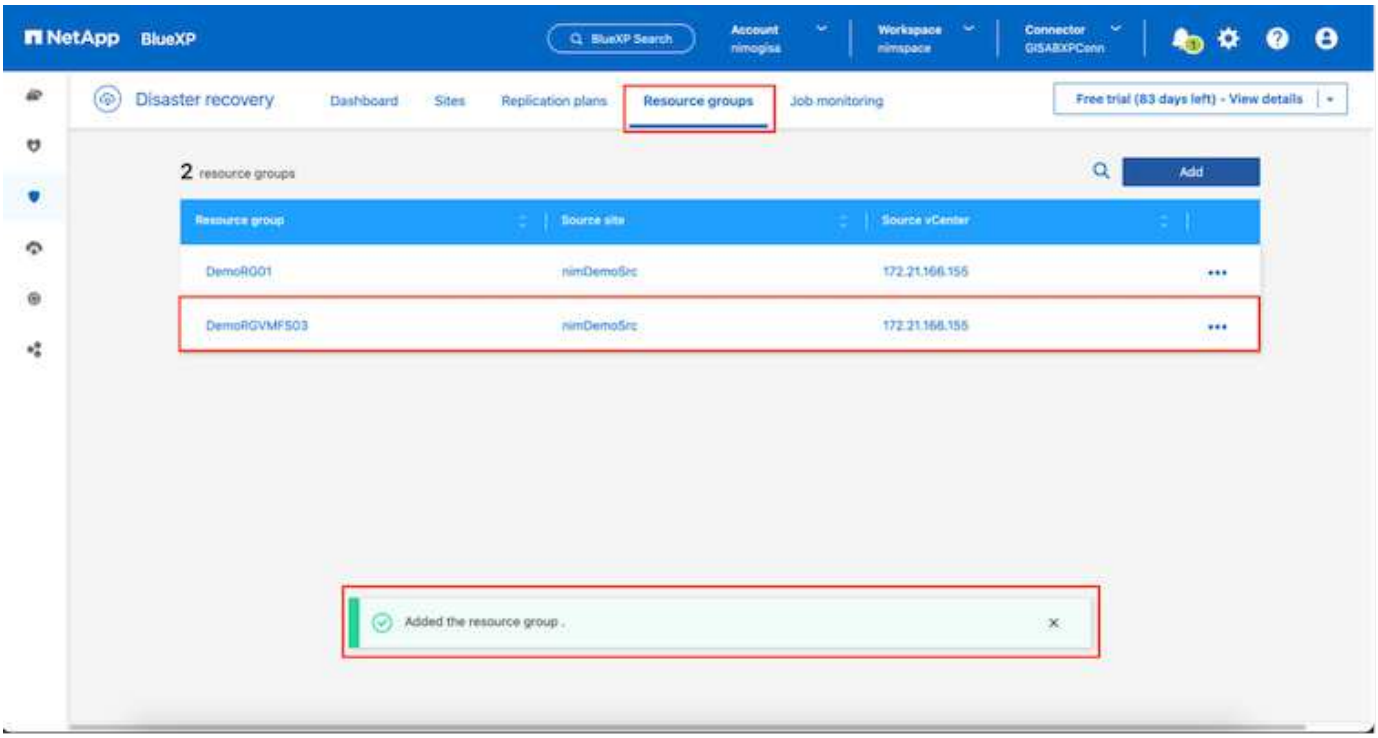
A parte gli approcci sopra indicati, è possibile creare la replica di SnapMirror anche tramite l'interfaccia a riga di comando di ONTAP o System Manager. Indipendentemente dall'approccio utilizzato per sincronizzare i dati utilizzando SnapMirror, BlueXP DRaaS orchestra il workflow per operazioni di disaster recovery perfette ed efficienti.

In che modo il disaster recovery di BlueXP può aiutarti?

Una volta aggiunti i siti di origine e destinazione, il disaster recovery di BlueXP esegue il rilevamento automatico dei dati approfonditi e visualizza le macchine virtuali con i metadati associati. Il disaster recovery di BlueXP rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle macchine virtuali e le compila.

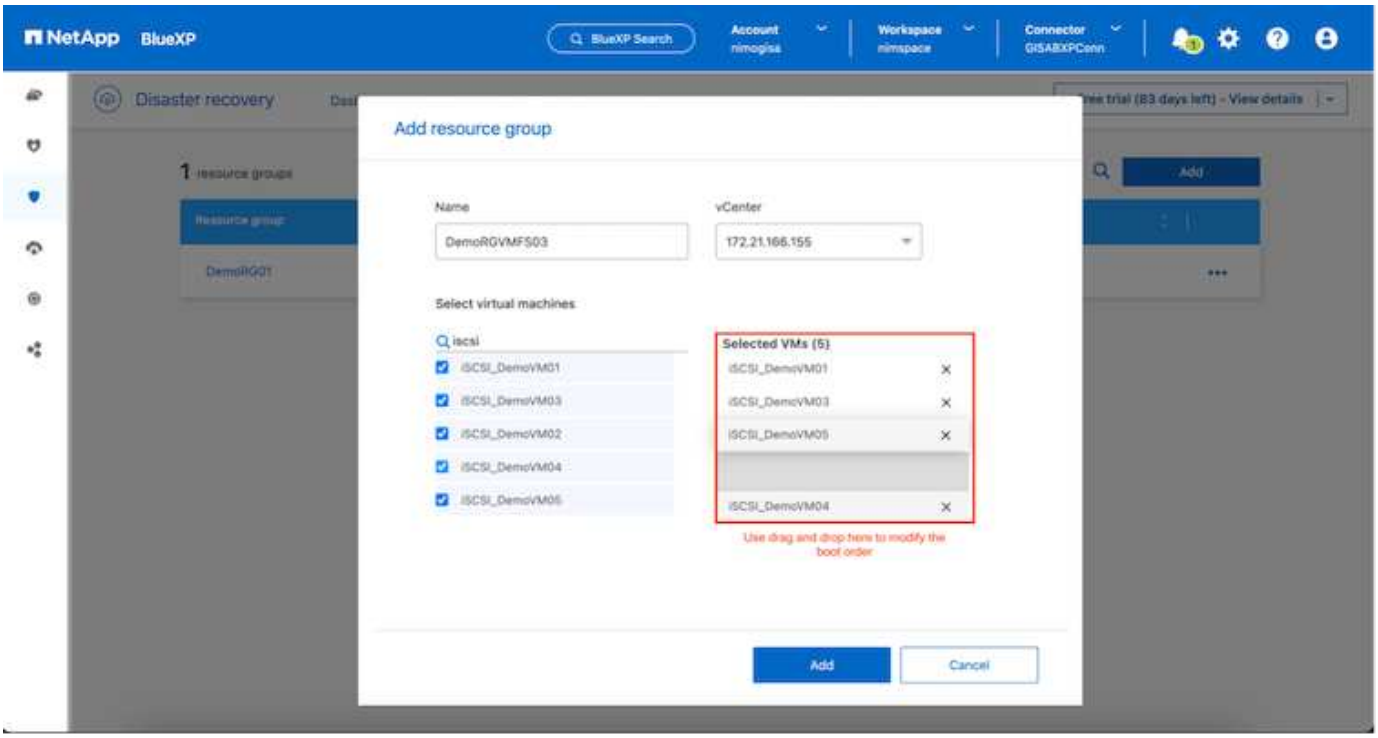


Una volta aggiunti i siti, è possibile raggruppare le macchine virtuali in gruppi di risorse. I gruppi di risorse per il disaster recovery di BlueXP consentono di raggruppare una serie di macchine virtuali dipendenti in gruppi logici che contengono gli ordini di avvio e i ritardi di avvio che possono essere eseguiti al momento del ripristino. Per iniziare a creare gruppi di risorse, accedere a **gruppi di risorse** e fare clic su **Crea nuovo gruppo di risorse**.

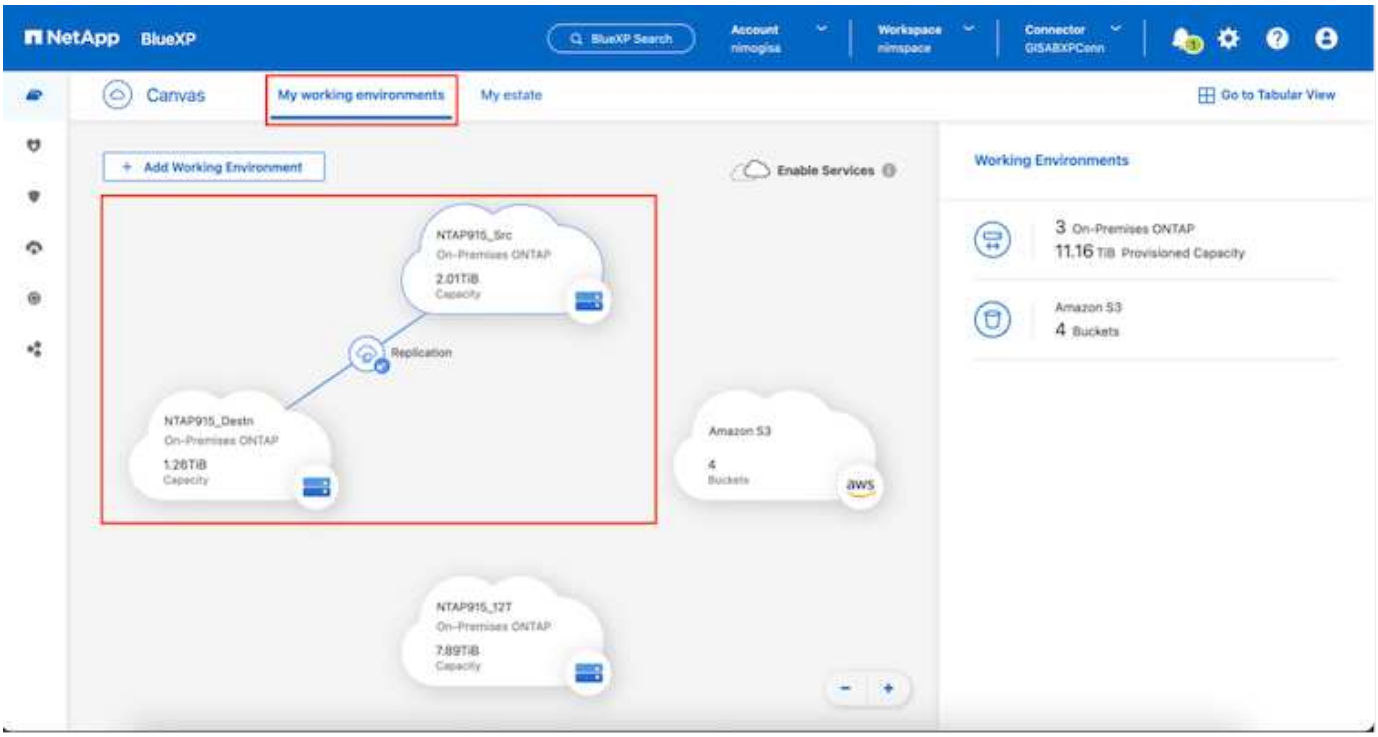


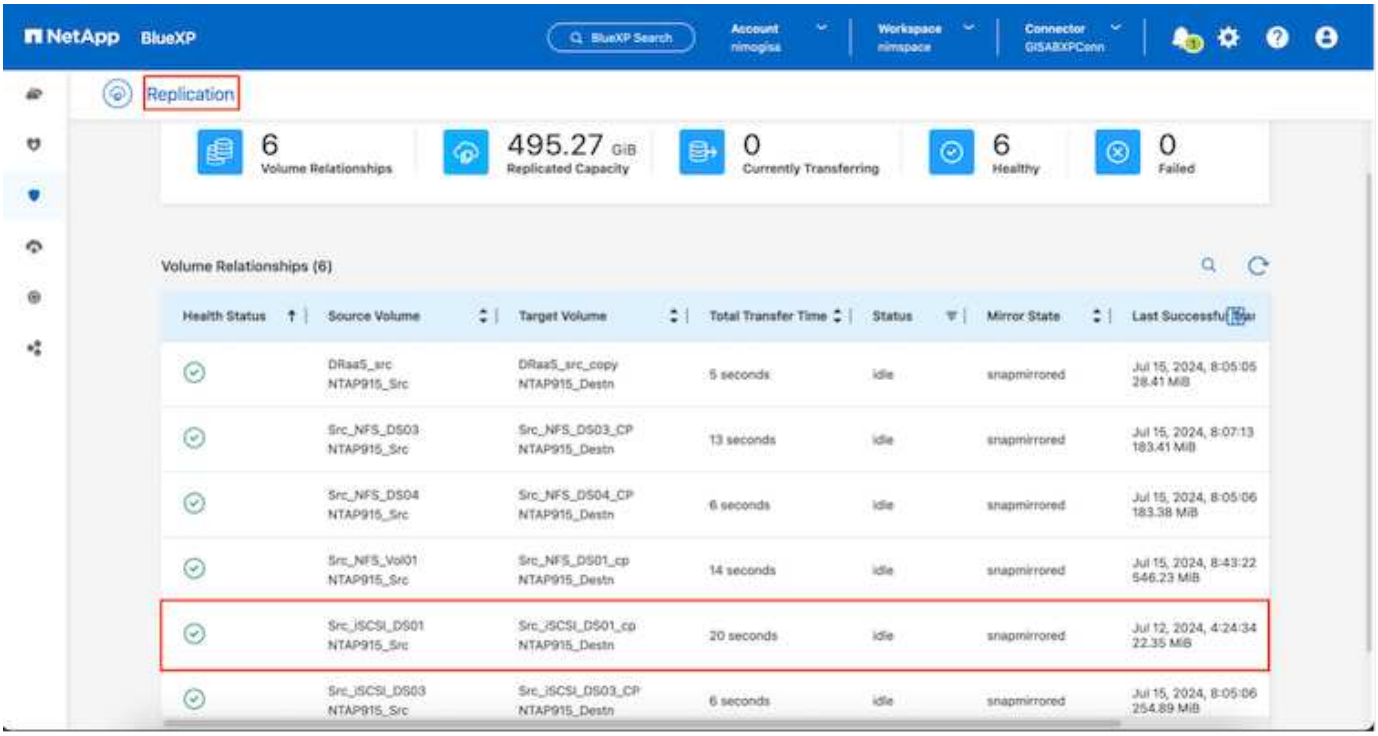
Il gruppo di risorse può anche essere creato durante la creazione di un piano di replica.

L'ordine di avvio delle VM può essere definito o modificato durante la creazione dei gruppi di risorse utilizzando un semplice meccanismo di trascinamento.



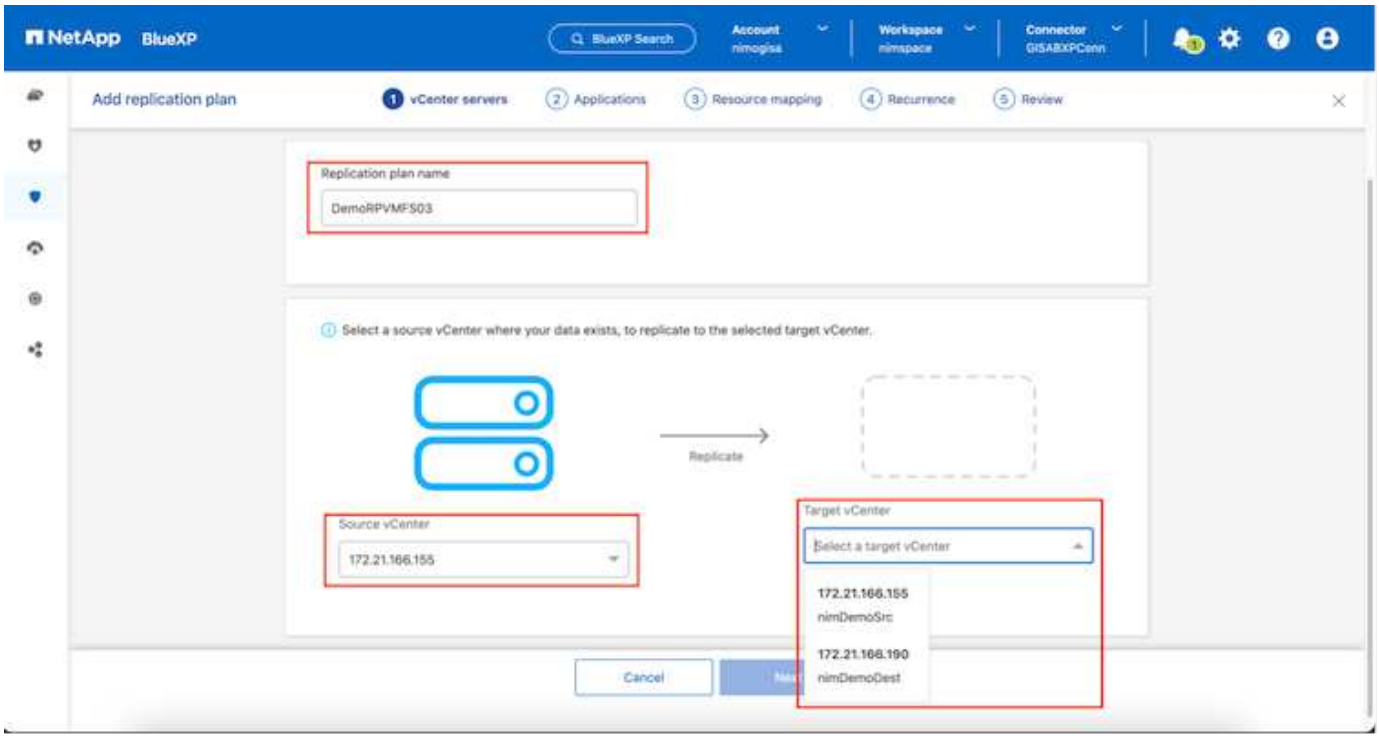
Una volta creati i gruppi di risorse, il passo successivo è creare il piano di esecuzione o un piano per il ripristino di macchine e applicazioni virtuali in caso di emergenza. Come menzionato nei prerequisiti, la replica di SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.



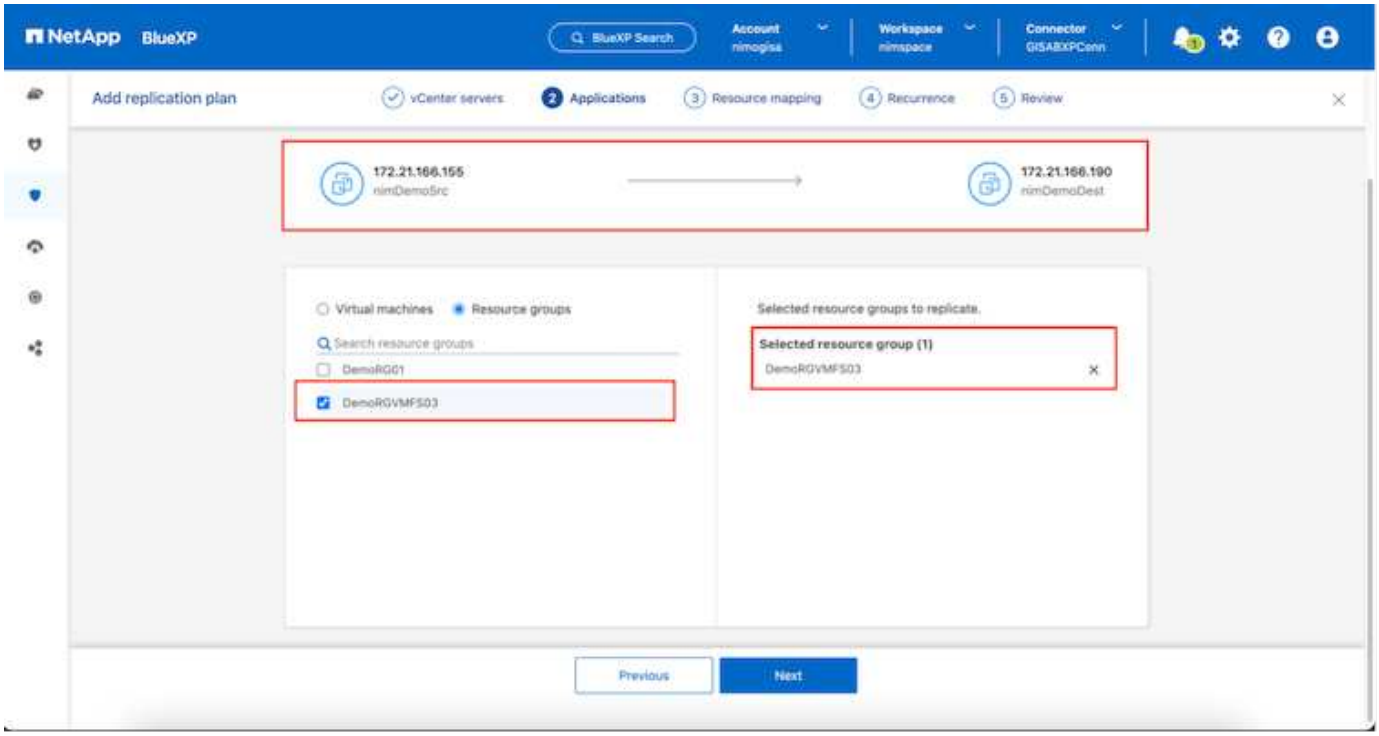


Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **piano di replica** e fare clic su **Aggiungi piano**.

Innanzitutto, selezionare vCenter di origine, quindi il vCenter di destinazione.



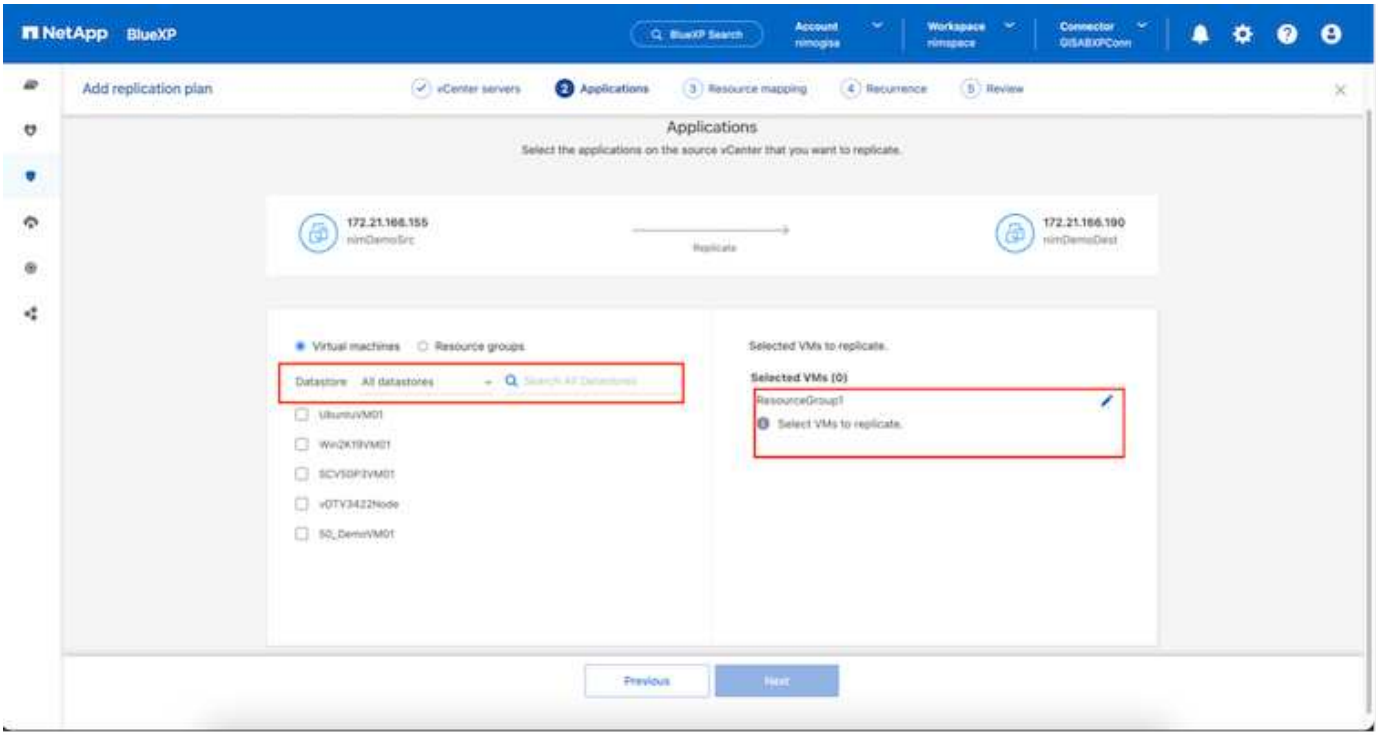
Il passaggio successivo consiste nel selezionare i gruppi di risorse esistenti. Se non vengono creati gruppi di risorse, la procedura guidata consente di raggruppare le macchine virtuali richieste (in pratica creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò consente inoltre di definire la sequenza operativa di ripristino delle macchine virtuali delle applicazioni.



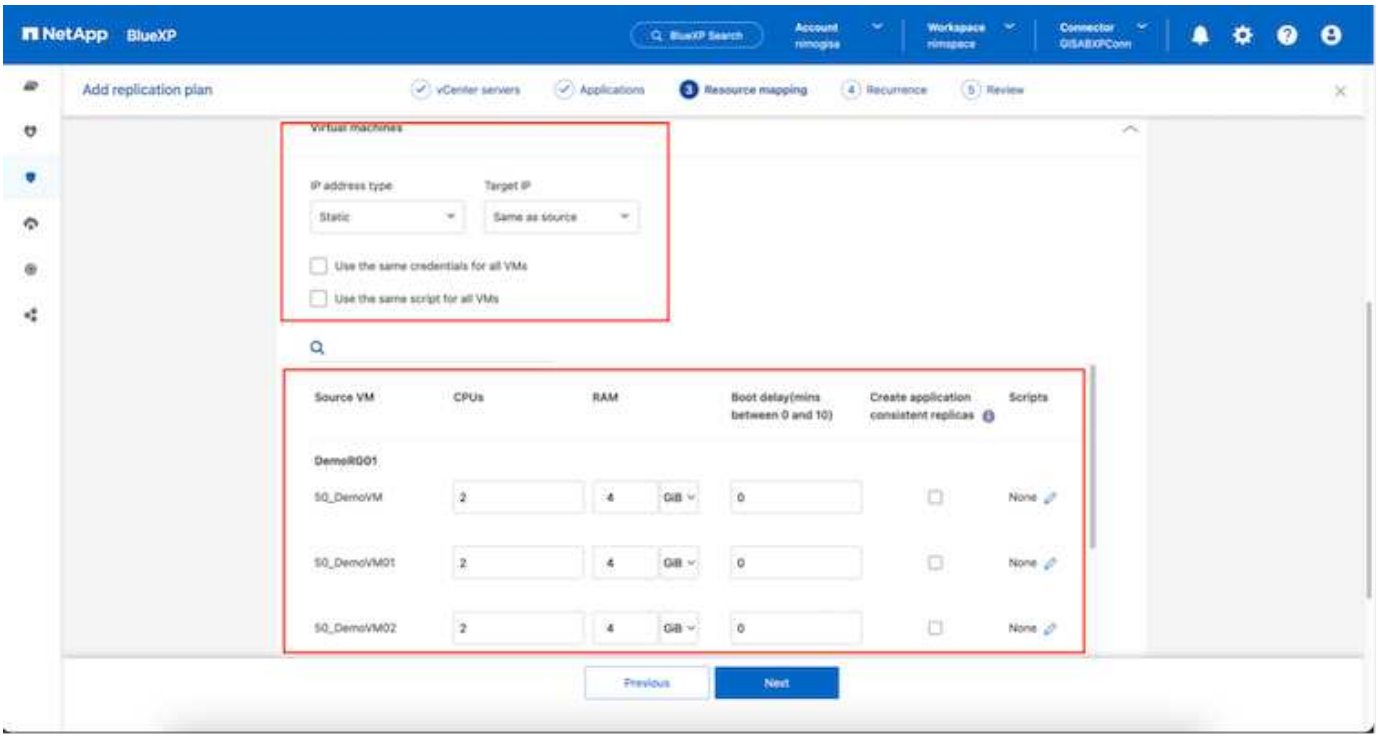
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine di accensione delle macchine virtuali durante il processo di ripristino.

Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Due gruppi di risorse vengono avviati in parallelo.

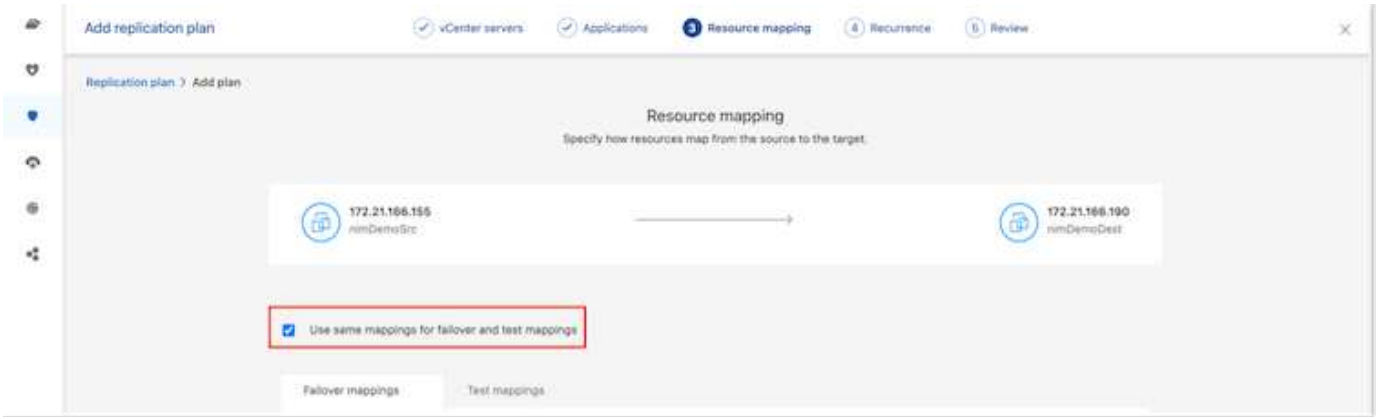
Lo screenshot seguente mostra la possibilità di filtrare le macchine virtuali o gli archivi dati specifici in base ai requisiti organizzativi se i gruppi di risorse non vengono creati in precedenza.



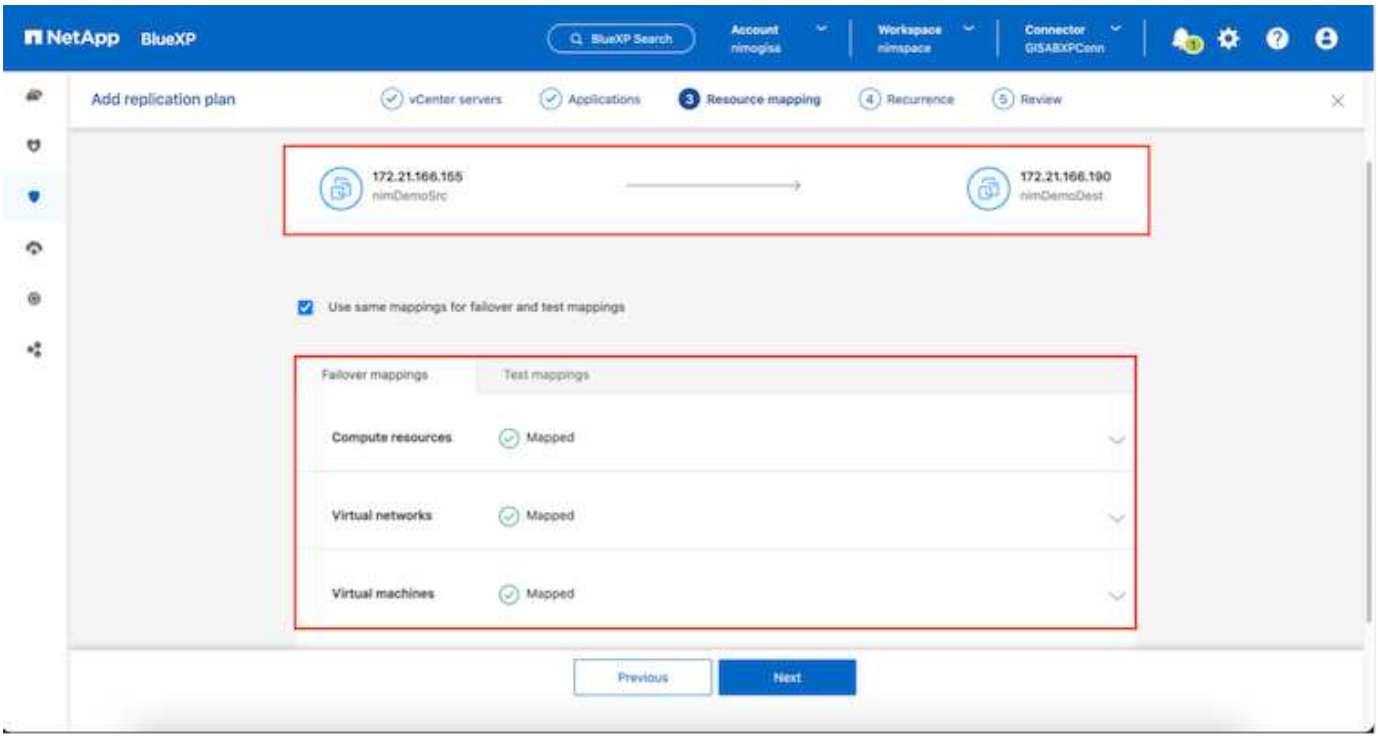
Una volta selezionati i gruppi di risorse, creare le mappature di failover. In questo passaggio, specificare il modo in cui le risorse dell'ambiente di origine vengono mappate alla destinazione. Sono incluse le risorse di elaborazione e le reti virtuali. Personalizzazione IP, pre e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento alla "Creare un piano di replica".



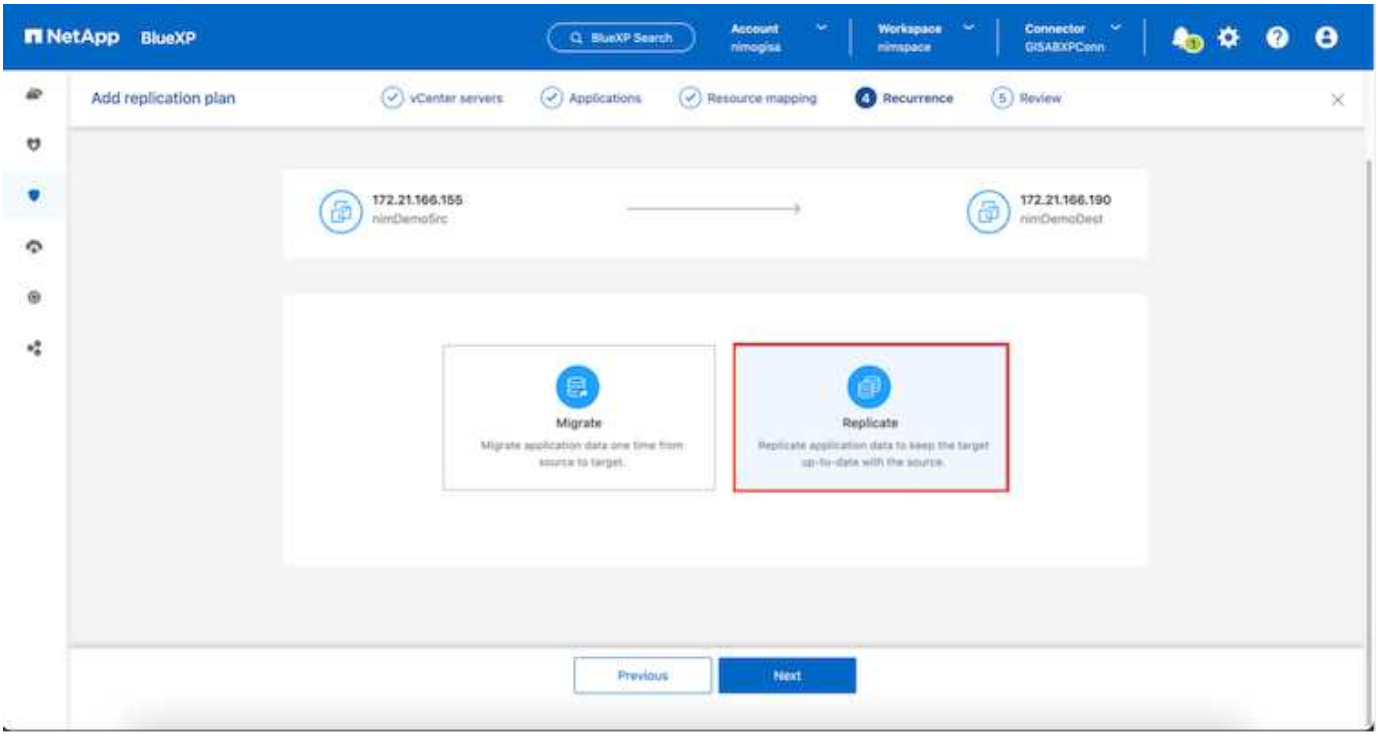
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per applicare mappature diverse per l'ambiente di test, selezionare l'opzione Test mapping (Test mapping) dopo aver deselezionato la casella di controllo come illustrato di seguito:



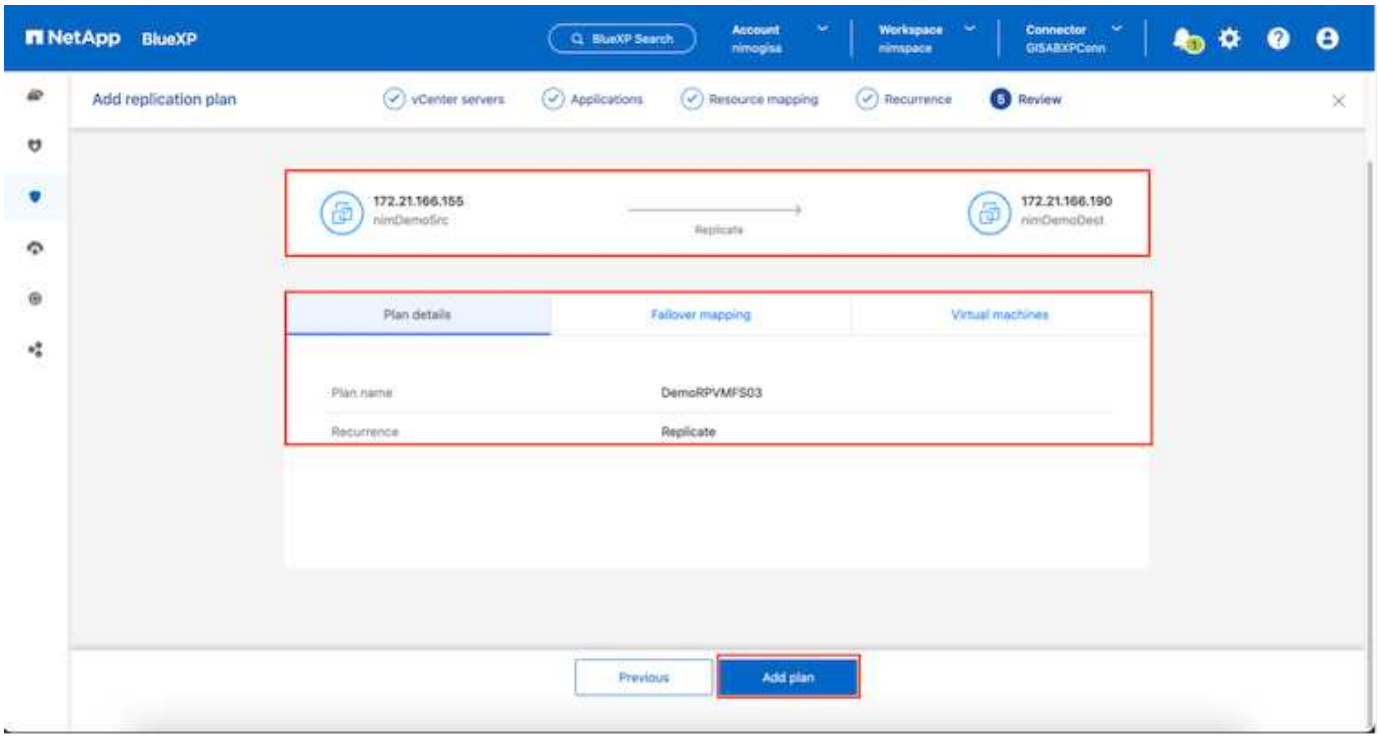
Una volta completata la mappatura delle risorse, fare clic su Avanti.

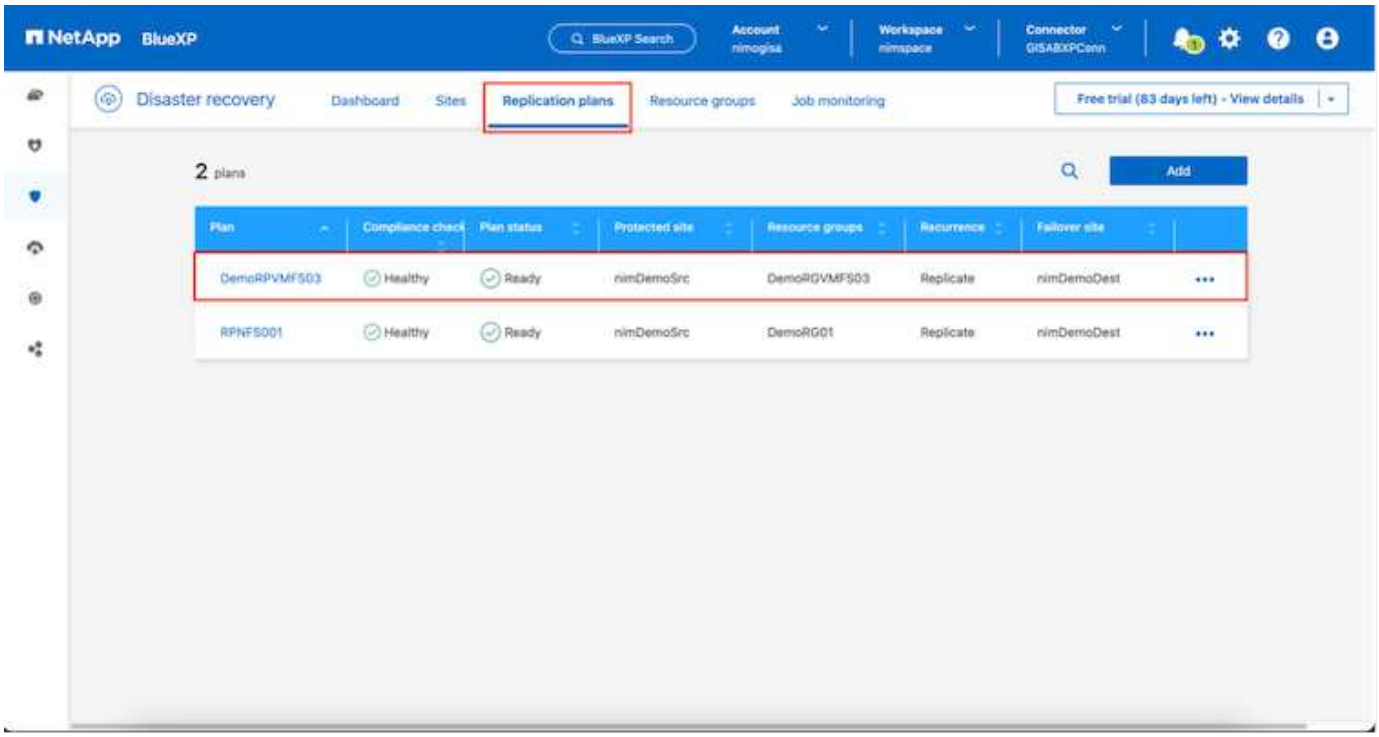


Selezionare il tipo di ricorrenza. In poche parole, selezionare l'opzione Migrate (migrazione una tantum tramite failover) o Replica continua ricorrente. In questa procedura dettagliata, l'opzione Replica è selezionata.

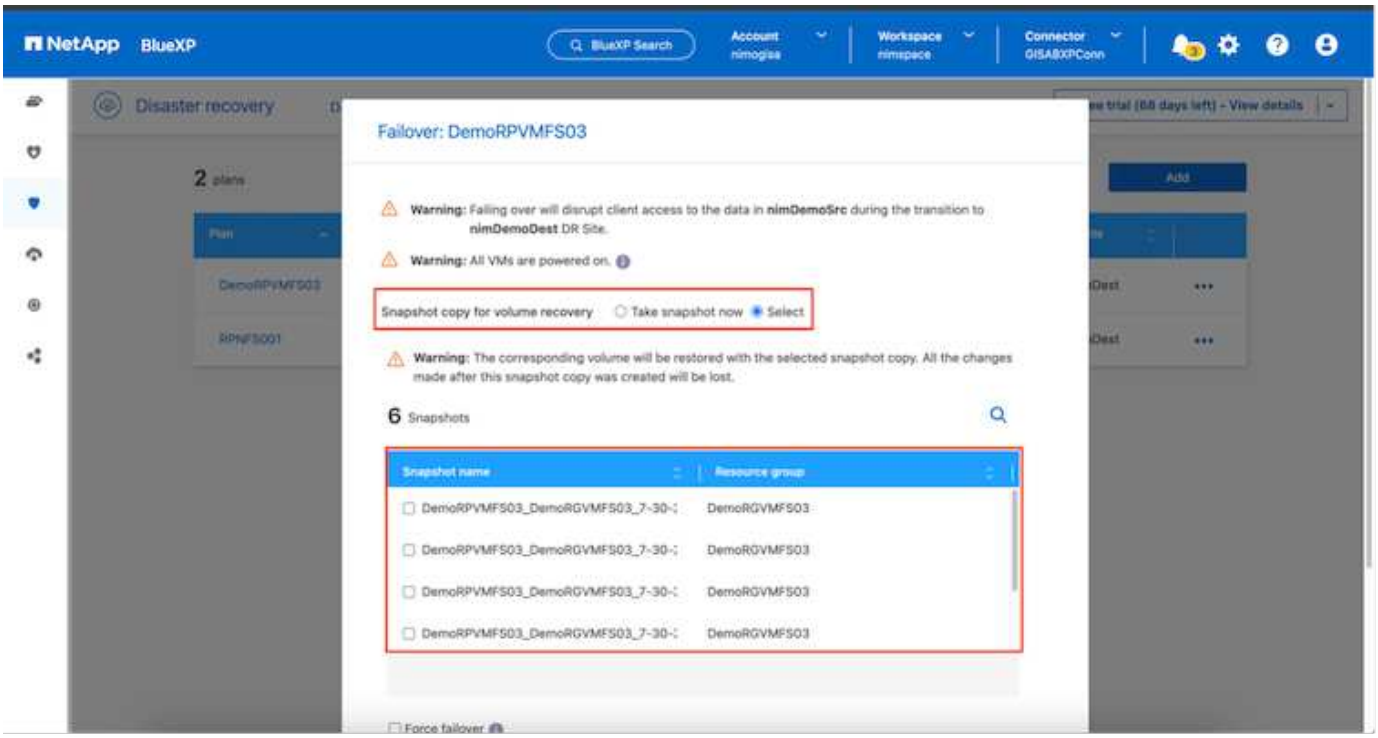


Al termine, rivedere le mappature create e fare clic su Aggiungi piano.

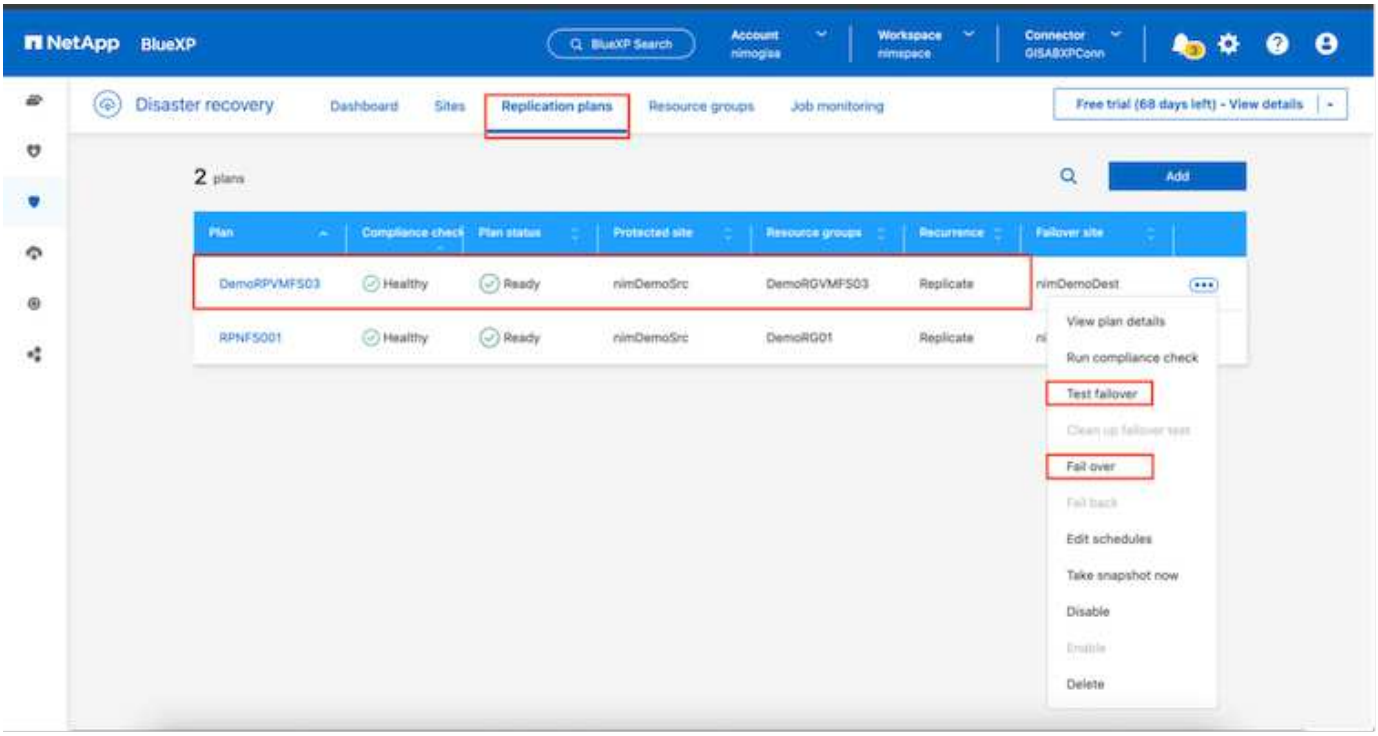




Una volta creato il piano di replica, è possibile eseguire il failover in base ai requisiti selezionando l'opzione failover, test-failover o migrazione. Il disaster recovery di BlueXP garantisce che il processo di replica venga eseguito in base al piano ogni 30 minuti. Durante le opzioni di failover e test-failover, è possibile utilizzare la copia Snapshot SnapMirror più recente oppure selezionare una copia Snapshot specifica da una copia Snapshot point-in-time (per la politica di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile in caso di danneggiamento come il ransomware, dove le repliche più recenti sono già compromesse o crittografate. Il disaster recovery di BlueXP mostra tutti i punti di recovery disponibili.



Per attivare il failover o testare il failover con la configurazione specificata nel piano di replica, fare clic su **failover** o **Test failover**.

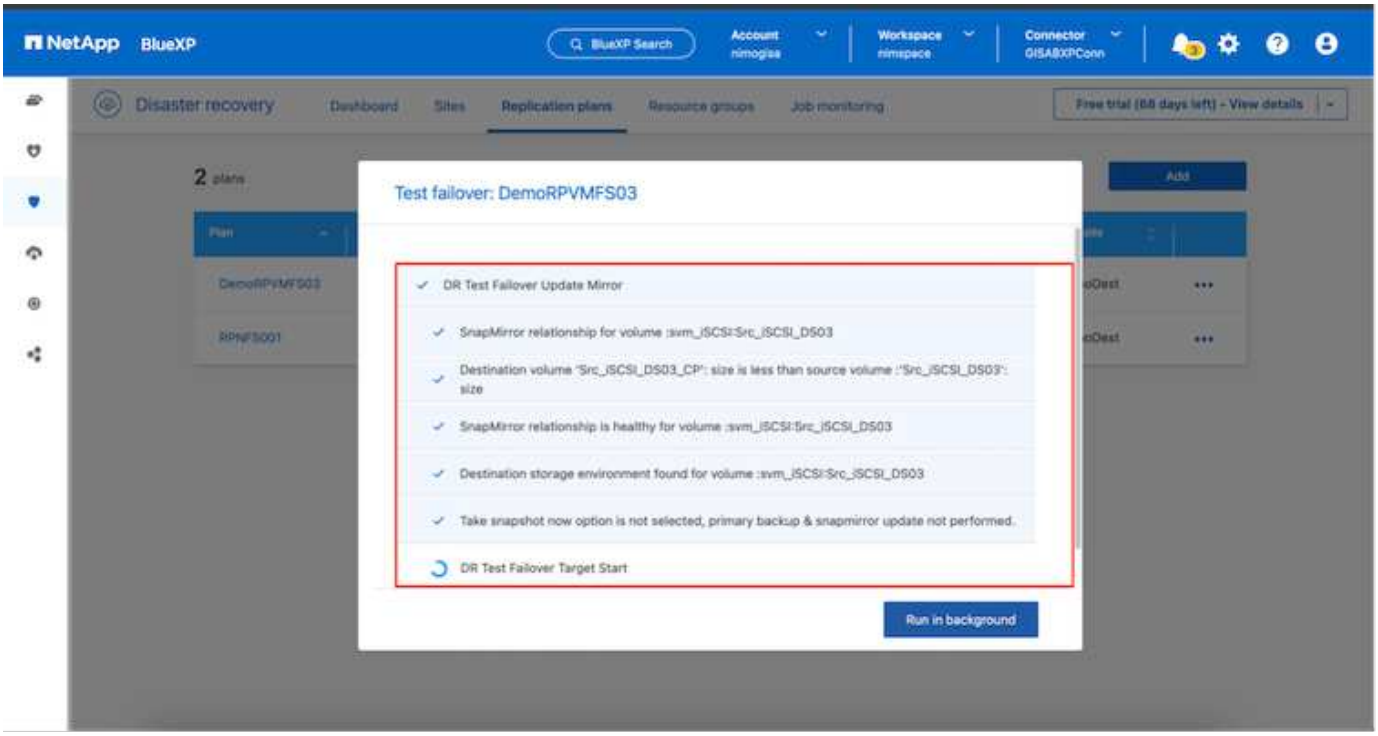


Cosa accade durante un'operazione di failover o di verifica del failover?

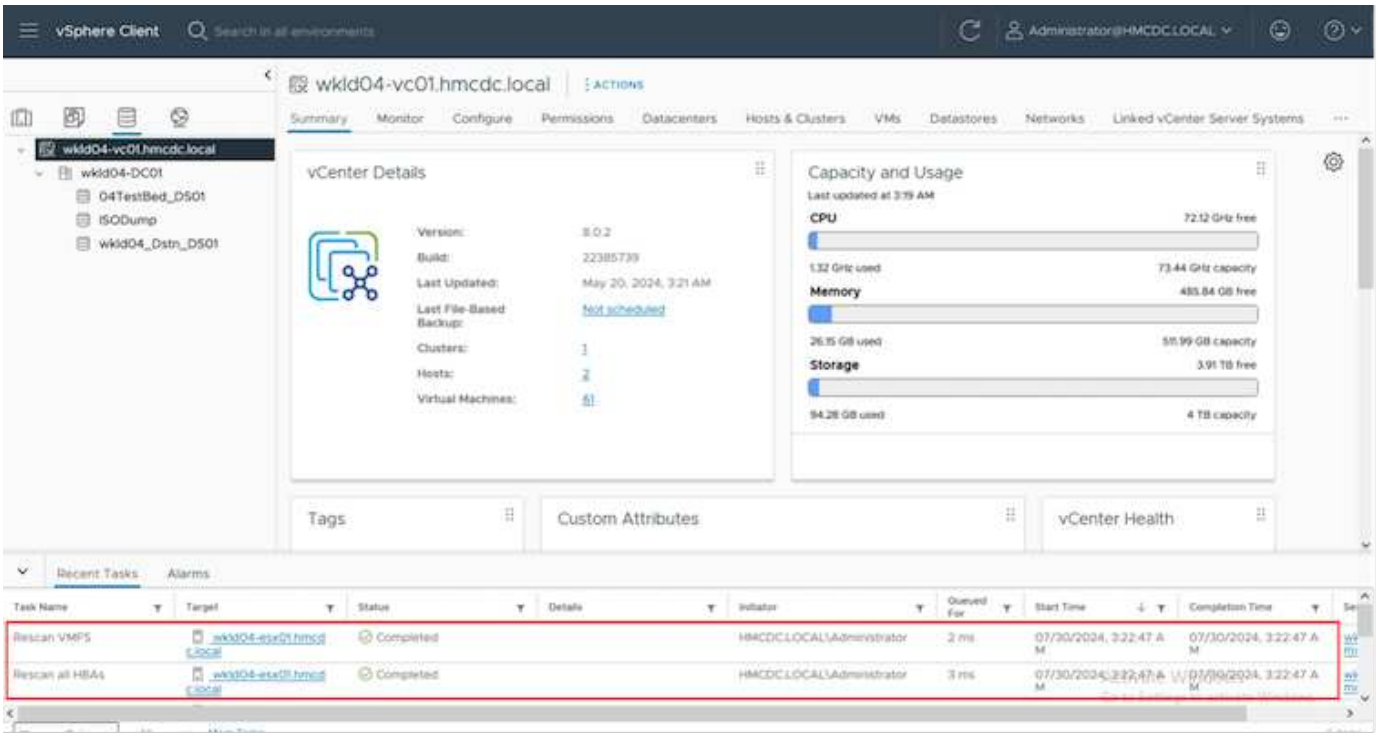
Durante un'operazione di failover di test, il disaster recovery di BlueXP crea un volume FlexClone sul sistema storage ONTAP di destinazione utilizzando l'ultima copia Snapshot o una snapshot selezionata del volume di destinazione.

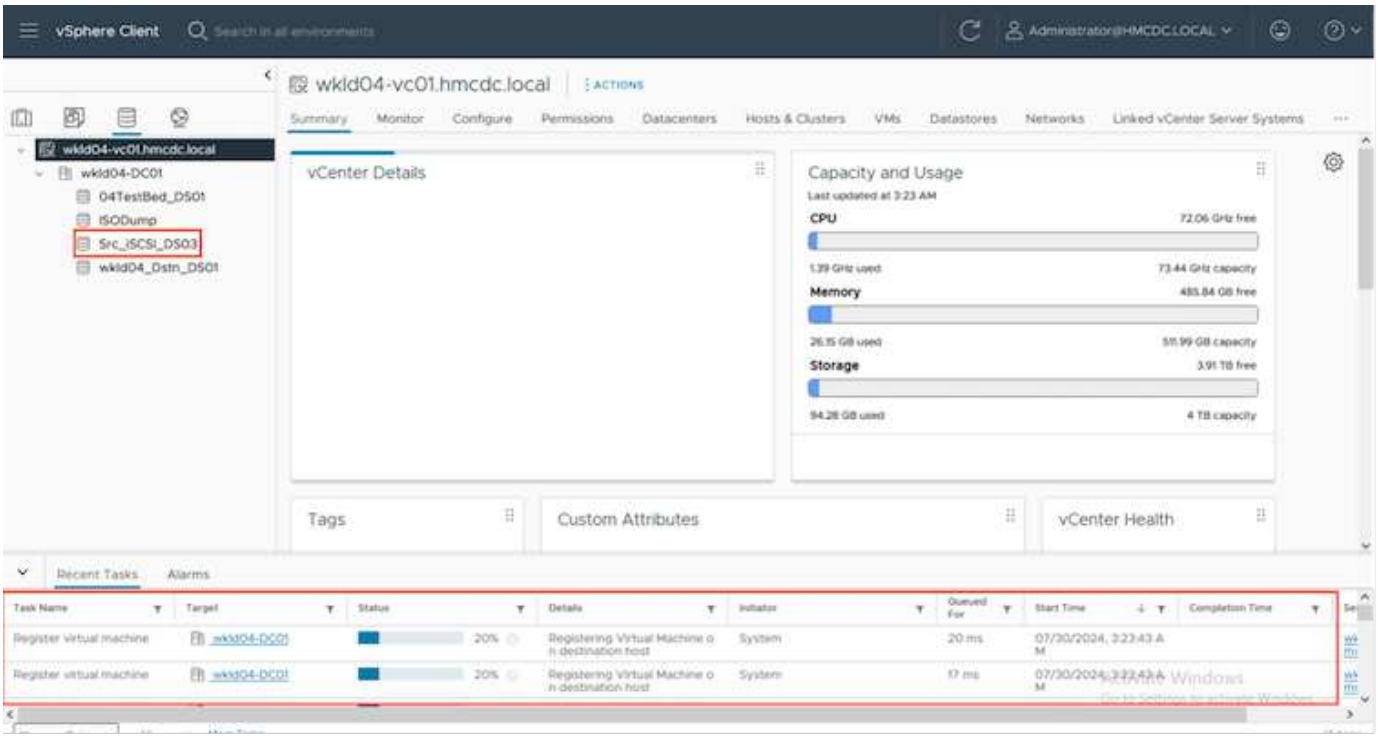
Un'operazione di test failover crea un volume clonato sul sistema di storage ONTAP di destinazione.

L'esecuzione di un'operazione di ripristino di prova non influisce sulla replica di SnapMirror.



Durante il processo, il disaster recovery di BlueXP non esegue la mappatura del volume di destinazione originale. Ma crea un nuovo volume FlexClone dalla snapshot selezionata e un datastore temporaneo di supporto del volume FlexClone viene mappato agli host ESXi.

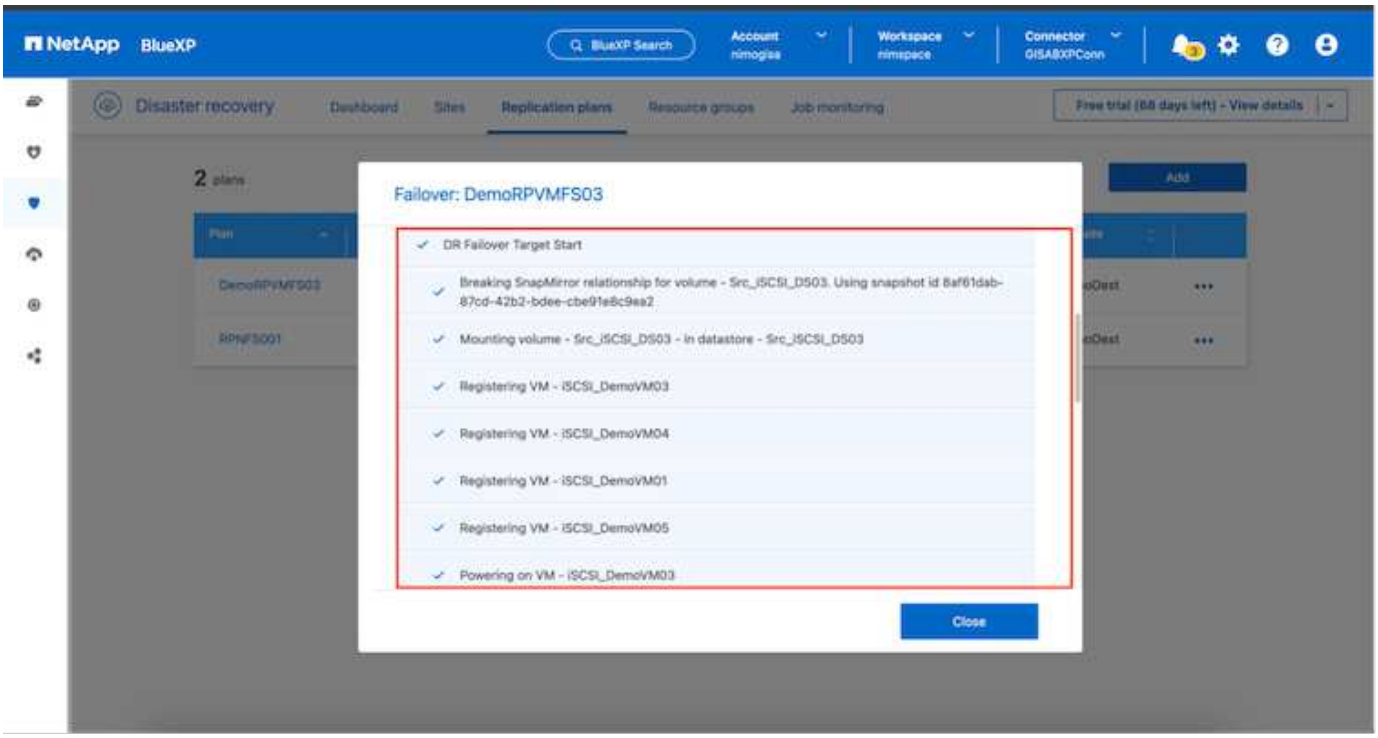




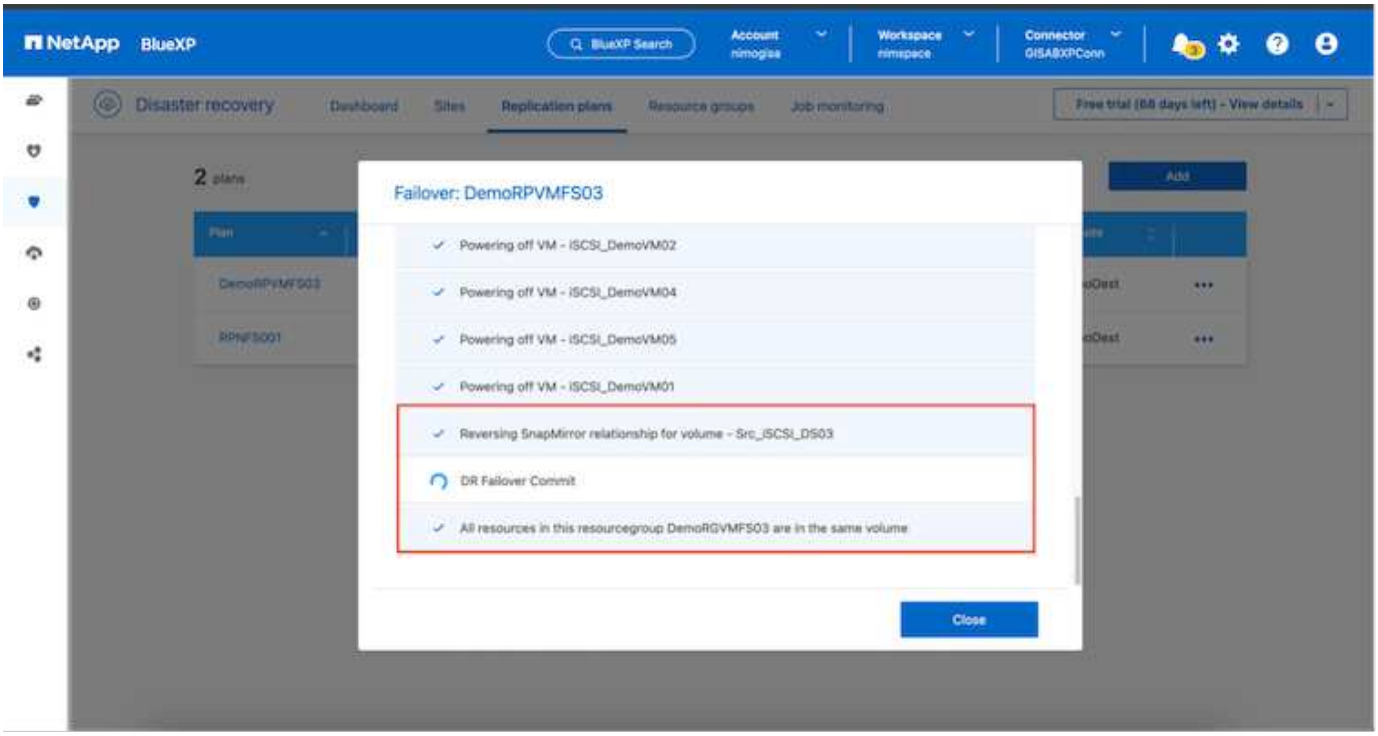
Al termine dell'operazione di failover di test, l'operazione di cleanup può essere attivata utilizzando **"Clean Up failover test"**. Durante questa operazione, il ripristino di emergenza BlueXP distrugge il volume FlexClone utilizzato nell'operazione.

In caso di eventi di emergenza reali, il disaster recovery di BlueXP esegue le seguenti operazioni:

1. Interrompe la relazione SnapMirror tra i siti.
2. Monta il volume del datastore VMFS dopo la firma per l'uso immediato.
3. Registrare le VM
4. Accendere le VM

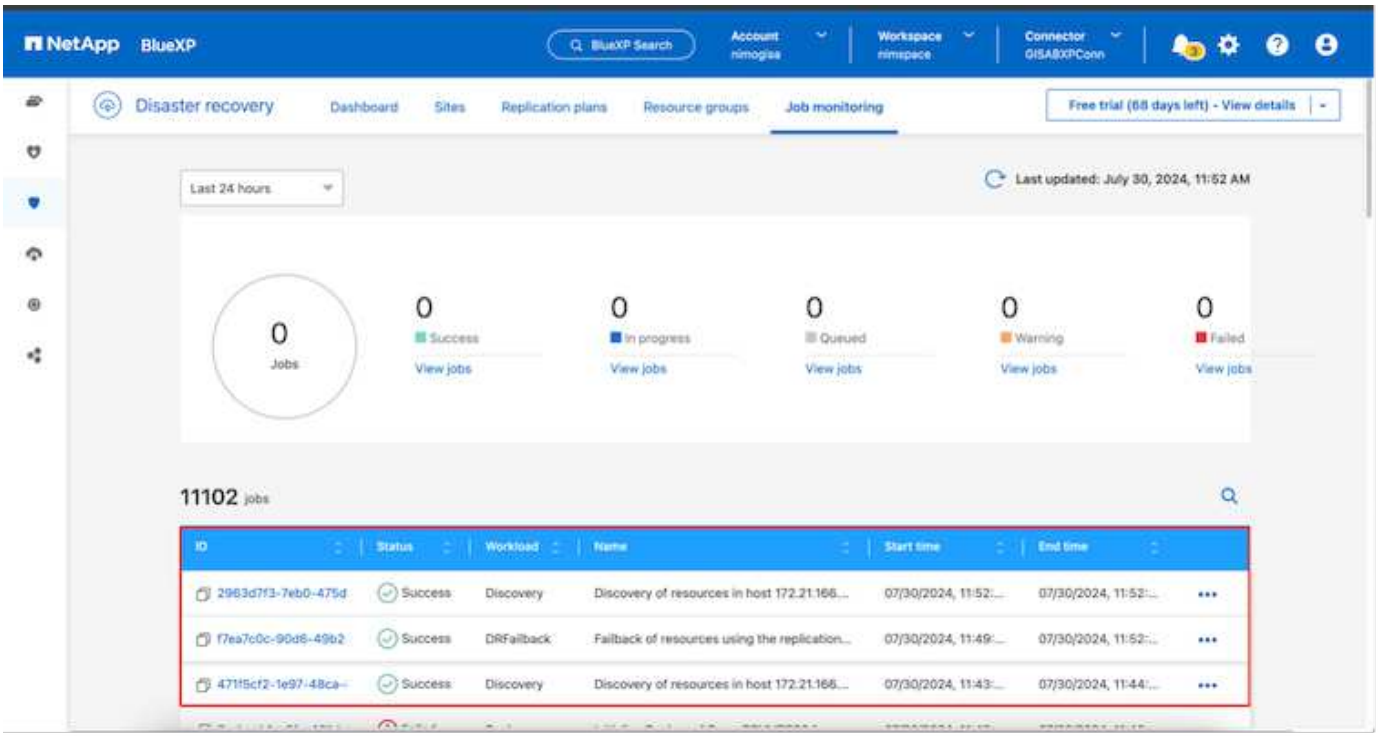


Una volta che il sito primario è in funzione, BlueXP Disaster Recovery abilita la risincronizzazione inversa di SnapMirror e abilita il failback, che può essere eseguito nuovamente con un semplice clic.



E se si sceglie l'opzione di migrazione, viene considerata come un evento di failover pianificato. In questo caso, viene attivata un'ulteriore operazione che consiste nell'arrestare le macchine virtuali nel sito di origine. Il resto dei passaggi rimane lo stesso dell'evento di failover.

Da BlueXP o dalla CLI di ONTAP, puoi monitorare lo stato di salute della replica per i volumi del datastore appropriati e lo stato di un failover o di un failover di test può essere monitorato tramite il monitoraggio dei processi.



Ciò fornisce una soluzione potente per gestire un piano di disaster recovery personalizzato e personalizzato. Il failover può essere eseguito come failover pianificato o failover con un clic su un pulsante in caso di disastro e si decide di attivare il sito di DR.

Per ulteriori informazioni su questo processo, è possibile seguire il video dettagliato della procedura dettagliata o utilizzare la "simulatore di soluzione".

Informazioni sul copyright

Informazioni sul marchio commerciale