



Ripristino di emergenza tramite BlueXP DRaaS

NetApp public and hybrid cloud solutions

NetApp
February 04, 2026

Sommario

| | |
|--|----|
| Ripristino di emergenza tramite BlueXP DRaaS | 1 |
| Panoramica | 1 |
| DR tramite BlueXP DRaaS per datastore NFS | 1 |
| Iniziare | 2 |
| Configurazione BlueXP disaster recovery | 4 |
| Configurazione della replica di archiviazione tra l'array del sito di origine e l'array del sito di destinazione | 6 |
| Come configurarlo per VMware Disaster Recovery | 6 |
| Cosa può fare per te il BlueXP disaster recovery ? | 7 |
| Failover di prova | 15 |
| Operazione di test di failover di pulizia | 17 |
| Migrazione pianificata e failover | 18 |
| Rifasamento | 20 |
| Monitoraggio e dashboard | 21 |
| DR tramite BlueXP DRaaS per datastore VMFS | 22 |
| Iniziare | 23 |
| Configurazione BlueXP disaster recovery | 25 |
| Configurazione della replica di archiviazione tra il sito di origine e quello di destinazione | 27 |
| Come configurarlo per VMware Disaster Recovery | 27 |
| Cosa può fare per te il BlueXP disaster recovery ? | 29 |
| Cosa succede durante un'operazione di failover o di test failover? | 37 |

Ripristino di emergenza tramite BlueXP DRaaS

Panoramica

Il Disaster Recovery è al primo posto nei pensieri di ogni amministratore VMware. Poiché VMware incapsula interi server in una serie di file che costituiscono la macchina virtuale, gli amministratori sfruttano tecniche basate sull'archiviazione a blocchi, come cloni, snapshot e repliche, per proteggere queste VM. Gli array ONTAP offrono una replica integrata per trasferire i dati del volume e, di conseguenza, le macchine virtuali residenti sui LUN del datastore designati, da un sito all'altro. BlueXP DRaaS si integra con vSphere e automatizza l'intero flusso di lavoro per un failover e un failback senza interruzioni in caso di disastro. Combinando la replicazione dello storage con l'automazione intelligente, gli amministratori hanno ora a disposizione un modo gestibile non solo per configurare, automatizzare e testare i piani di disaster recovery, ma anche per eseguirli facilmente in caso di disastro.

La parte più dispendiosa in termini di tempo di un failover DR in un ambiente VMware vSphere è l'esecuzione dei passaggi necessari per inventariare, registrare, riconfigurare e accendere le VM nel sito DR. Una soluzione ideale ha sia un basso RPO (misurato in minuti) sia un basso RTO (misurato in minuti o ore). Un fattore che spesso viene trascurato in una soluzione DR è la capacità di testare la soluzione DR in modo efficiente a intervalli periodici.

Per progettare una soluzione DR, è necessario tenere a mente i seguenti fattori:

- L'obiettivo del tempo di recupero (RTO). L'RTO indica la rapidità con cui un'azienda può riprendersi da un disastro o, più specificamente, il tempo necessario per eseguire il processo di ripristino e rendere nuovamente disponibili i servizi aziendali.
- L'obiettivo del punto di ripristino (RPO). L'RPO indica l'età dei dati recuperati dopo essere stati resi disponibili, in relazione al momento in cui si è verificato il disastro.
- Scalabilità e adattabilità. Questo fattore include la possibilità di aumentare gradualmente le risorse di archiviazione man mano che aumenta la domanda.

Per maggiori informazioni tecniche sulle soluzioni disponibili, consultare:

- ["DR tramite BlueXP DRaaS per datastore NFS"](#)
- ["DR tramite BlueXP DRaaS per datastore VMFS"](#)

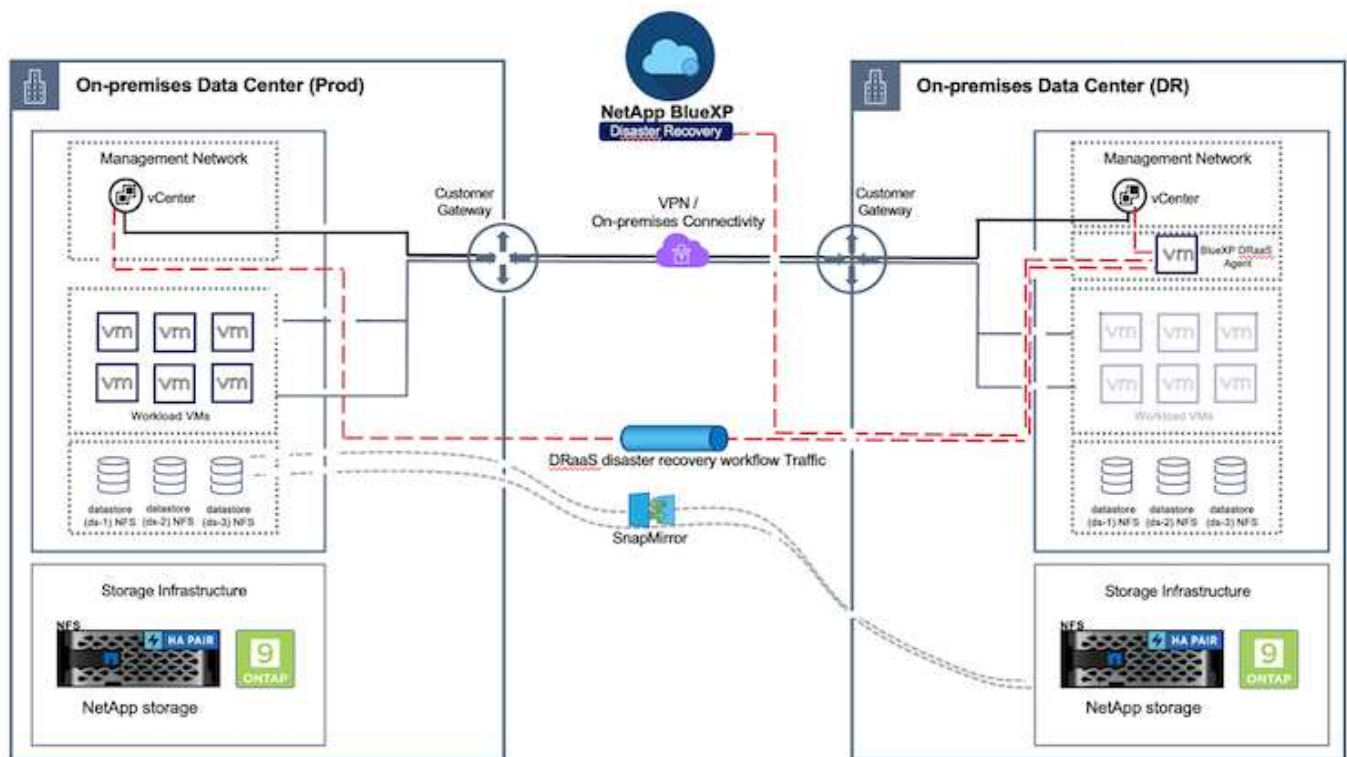
DR tramite BlueXP DRaaS per datastore NFS

L'implementazione del disaster recovery tramite replica a livello di blocco dal sito di produzione al sito di disaster recovery è un metodo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Utilizzando la replica NetApp SnapMirror, i carichi di lavoro VMware in esecuzione su sistemi ONTAP locali con datastore NFS possono essere replicati su un altro sistema di storage ONTAP situato in un data center di ripristino designato in cui è distribuito anche VMware.

Questa sezione del documento descrive la configurazione di BlueXP DRaaS per impostare il disaster recovery per le VM VMware on-premise su un altro sito designato. Come parte di questa configurazione, l'account BlueXP, il connettore BlueXP e gli array ONTAP sono stati aggiunti all'interno dell'area di lavoro BlueXP, necessari per abilitare la comunicazione da VMware vCenter allo storage ONTAP. Inoltre, questo documento spiega nel dettaglio come configurare la replica tra siti e come impostare e testare un piano di ripristino. L'ultima sezione contiene istruzioni su come eseguire un failover completo del sito e su come effettuare il failback quando il sito primario viene ripristinato e acquistato online.

Utilizzando il servizio BlueXP disaster recovery, integrato nella console NetApp BlueXP, le aziende possono individuare facilmente i propri VMware vCenter e storage ONTAP in sede. Le organizzazioni possono quindi creare raggruppamenti di risorse, creare un piano di disaster recovery, associarlo a gruppi di risorse e testare o eseguire failover e failback. SnapMirror fornisce la replicazione dei blocchi a livello di storage per mantenere i due siti aggiornati con modifiche incrementali, con un Recovery Point Objective (RPO) fino a 5 minuti. Inoltre, è possibile simulare procedure di disaster recovery senza compromettere la produzione o incorrere in costi di archiviazione aggiuntivi.

Il BlueXP disaster recovery sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore NFS dall'ultimo snapshot replicato sul sito di disaster recovery. Dopo aver completato il test di disaster recovery, i clienti possono facilmente eliminare l'ambiente di test senza influire sulle risorse di produzione effettivamente replicate. In caso di un failover effettivo, il servizio BlueXP disaster recovery orchestra tutti i passaggi necessari per ripristinare automaticamente le macchine virtuali protette sul sito di disaster recovery designato con pochi clic. Il servizio invertirà anche la relazione SnapMirror con il sito primario per un'operazione di failback, quando necessario. Tutte queste funzionalità hanno un costo molto inferiore rispetto ad altre alternative note.

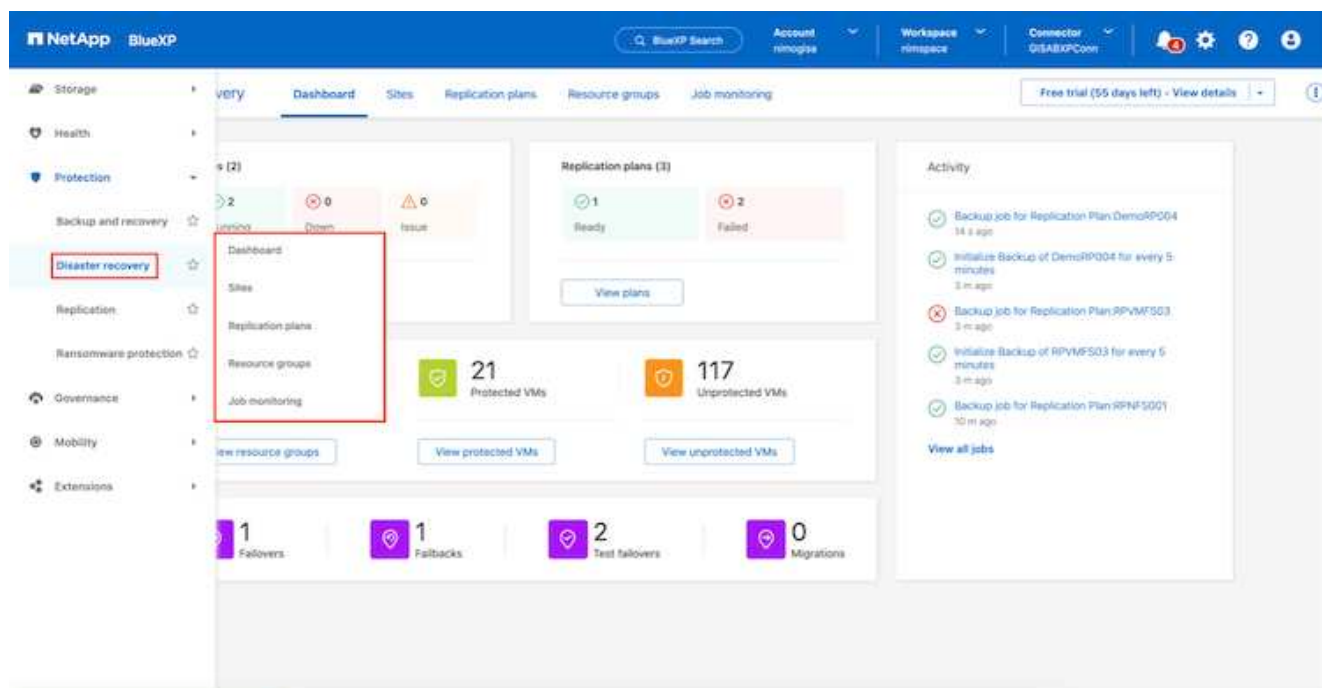


Iniziare

Per iniziare a utilizzare il BlueXP disaster recovery, utilizzare la console BlueXP e quindi accedere al servizio.

1. Accedi a BlueXP.

2. Dal menu di navigazione a sinistra BlueXP , seleziona Protezione > Ripristino di emergenza.
3. Viene visualizzata la Dashboard BlueXP disaster recovery .



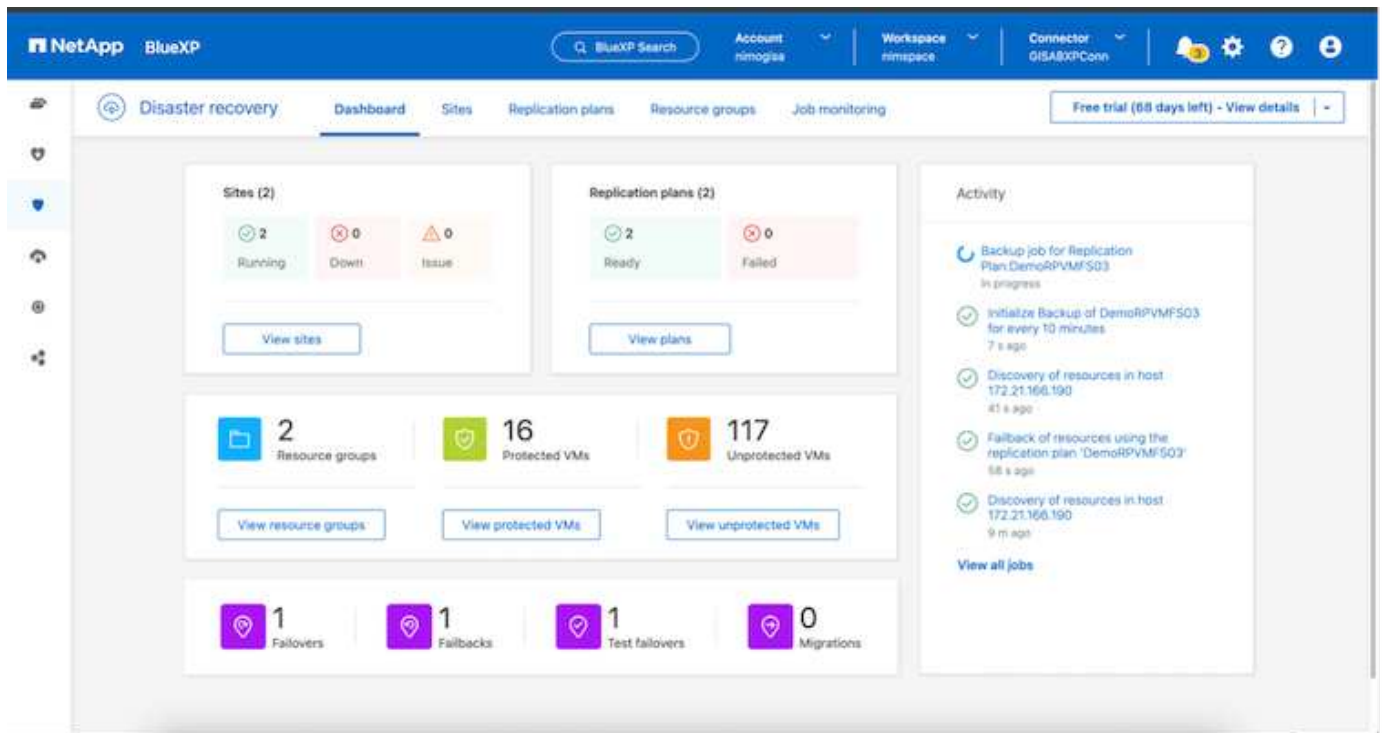
Prima di configurare il piano di disaster recovery, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- BlueXP Connector è configurato in NetApp BlueXP.
- Le istanze del connettore BlueXP dispongono di connettività con i sistemi di archiviazione e vCenter di origine e di destinazione.
- Cluster NetApp Data ONTAP per fornire datastore NFS di storage.
- In BlueXP sono stati aggiunti sistemi di storage NetApp on-premise che ospitano datastore NFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su NFS designati.
- Assicurarsi che l'ambiente disponga di versioni supportate dei server vCenter Server ed ESXi.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere un paio di clic e circa 3-5 minuti.



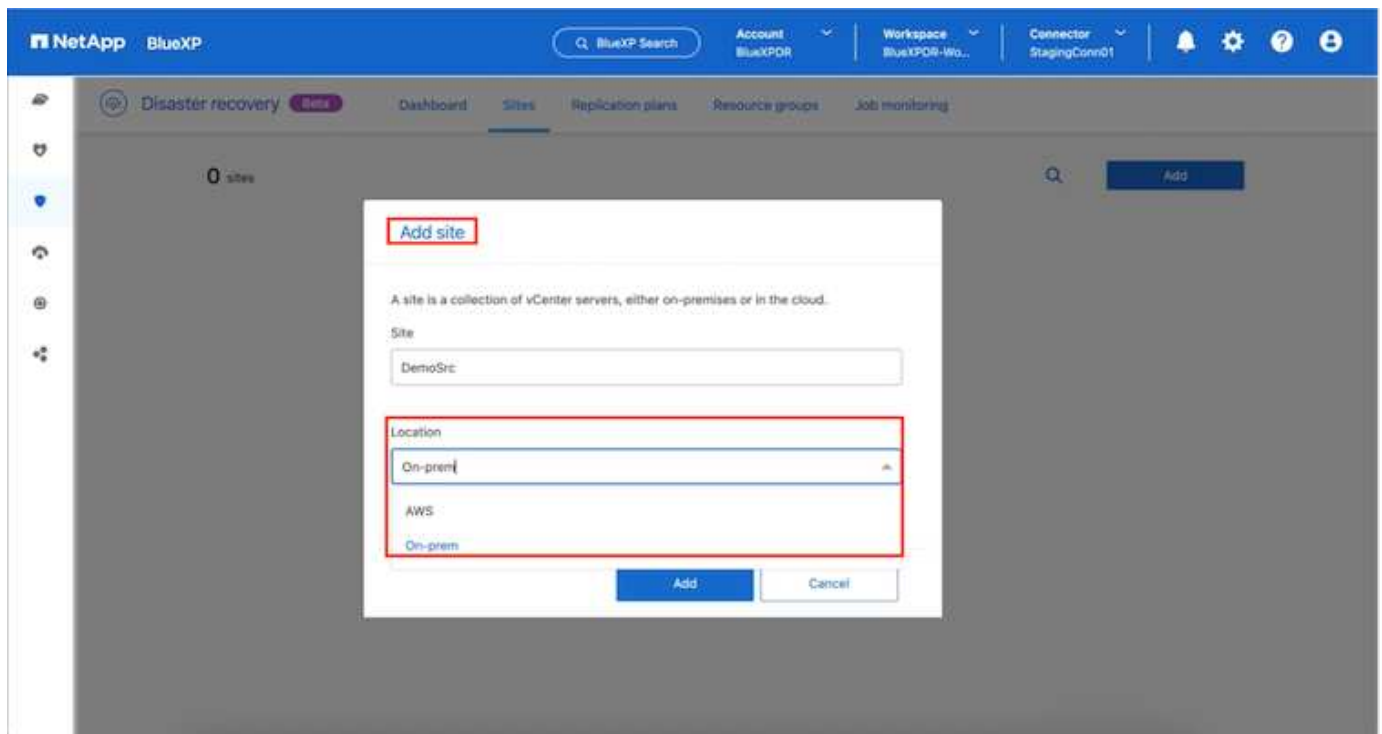
NetApp consiglia di distribuire il connettore BlueXP nel sito di destinazione o in un terzo sito, in modo che il connettore BlueXP possa comunicare tramite la rete con le risorse di origine e di destinazione.



Configurazione BlueXP disaster recovery

Il primo passo per prepararsi al disaster recovery è individuare e aggiungere le risorse di archiviazione e vCenter locali al BlueXP disaster recovery.

Aprire la console BlueXP e selezionare **Protezione > Ripristino di emergenza** dal menu di navigazione a sinistra. Selezionare **Scopri server vCenter** oppure utilizzare il menu in alto, selezionare **Siti > Aggiungi > Aggiungi vCenter**.



Aggiungere le seguenti piattaforme:

- **Fonte.** vCenter locale.

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCConn

Disaster recovery Dashboard **Sites** Replication plans Resource groups Job monitoring

Free trial (55 days left) - View details

2 sites

nimDemoSrc 172.21.166.155 Healthy

nimDemoDe 172.21.166.155 Healthy

Add vCenter server

Enter connection details for the vCenter server that is accessible from the BlueXP Connector.

Site: nimDemoSrc BlueXP Connector: GISABXPCConn

vCenter IP address: 172.21.166.155

vCenter user name: administrator@rnmcdc.local vCenter password: *****

☒ Use self-signed certificates

Add Cancel

- **Destinazione.** VMC SDDC vCenter.

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCConn

Disaster recovery Dashboard **Sites** Replication plans Resource groups Job monitoring

Free trial (55 days left) - View details

2 sites

nimDemoSrc 172.21.166.155 Healthy

nimDemoDe 172.21.166.155 Healthy

Add vCenter server

Enter connection details for the vCenter server that is accessible from the BlueXP Connector.

Site: nimDemoSrc BlueXP Connector: GISABXPCConn

vCenter IP address: 172.21.166.190

vCenter user name: administrator@rnmcdc.local vCenter password: *****

☒ Use self-signed certificates

Add Cancel

Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione 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 che sono stati modificati o aggiunti dall'aggiornamento precedente. SnapMirror può essere facilmente configurato tramite NetApp OnCommand System Manager o ONTAP CLI. BlueXP DRaaS crea anche la relazione SnapMirror a condizione che il cluster e il peering SVM siano configurati in anticipo.

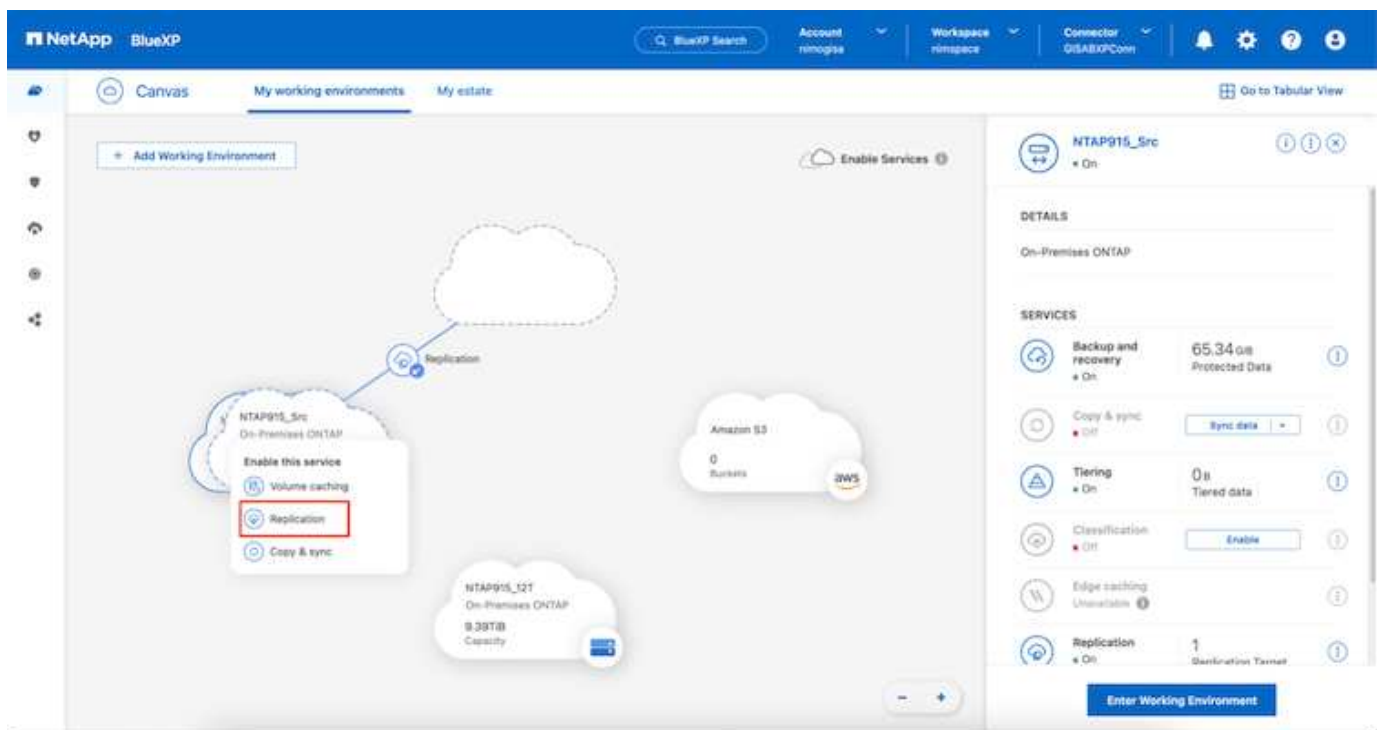
Nei casi in cui lo storage primario non è completamente perso, SnapMirror fornisce un mezzo efficiente per risincronizzare i siti primario e DR. SnapMirror può risincronizzare i due siti, trasferendo solo i dati modificati o nuovi dal sito DR al sito primario, semplicemente invertendo le relazioni SnapMirror. 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 dall'ultima sincronizzazione riuscita della copia Snapshot vengono inviati alla destinazione.



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

Come configurarlo per VMware Disaster Recovery

Il processo per creare una replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è sfruttare BlueXP per configurare la replica SnapMirror, utilizzando un semplice trascinamento del sistema ONTAP di origine nell'ambiente sulla destinazione per avviare la procedura guidata che guida attraverso il resto del processo.



BlueXP DRaaS può anche automatizzare la stessa operazione, a condizione che siano soddisfatti i due criteri seguenti:

- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.



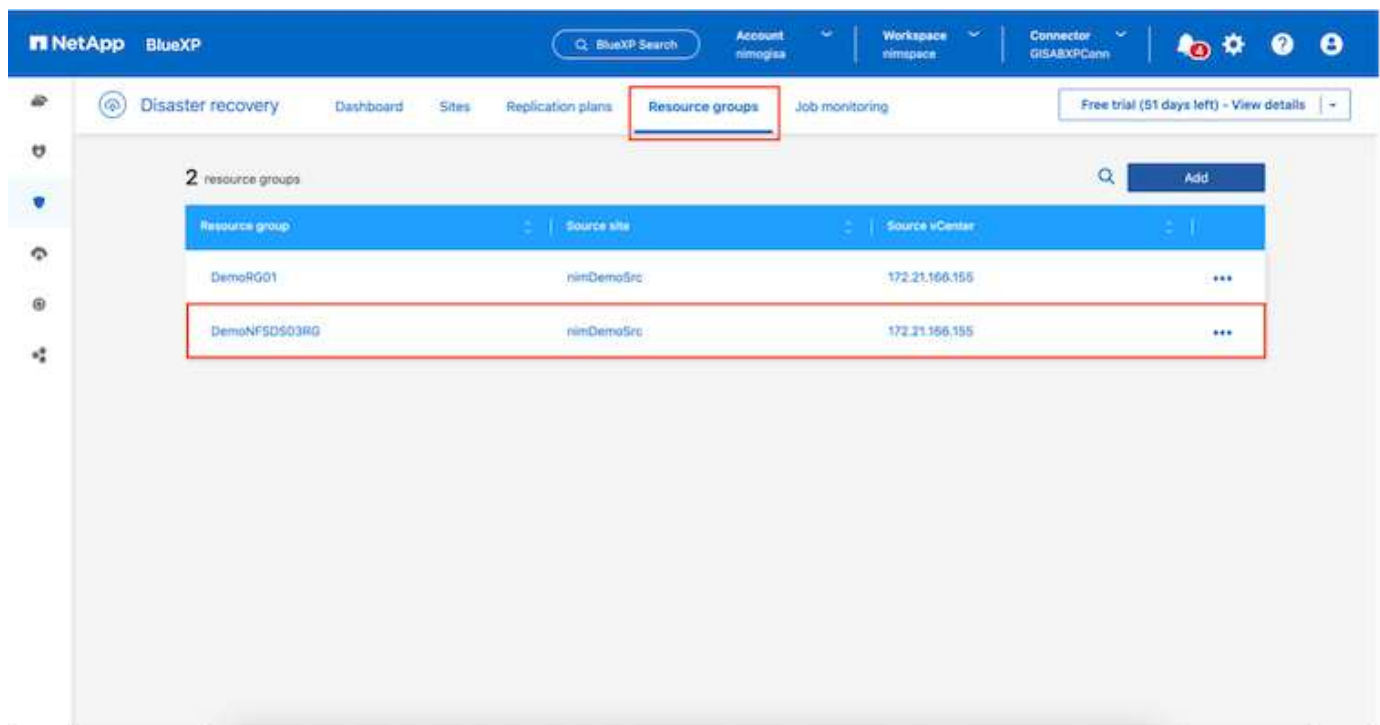
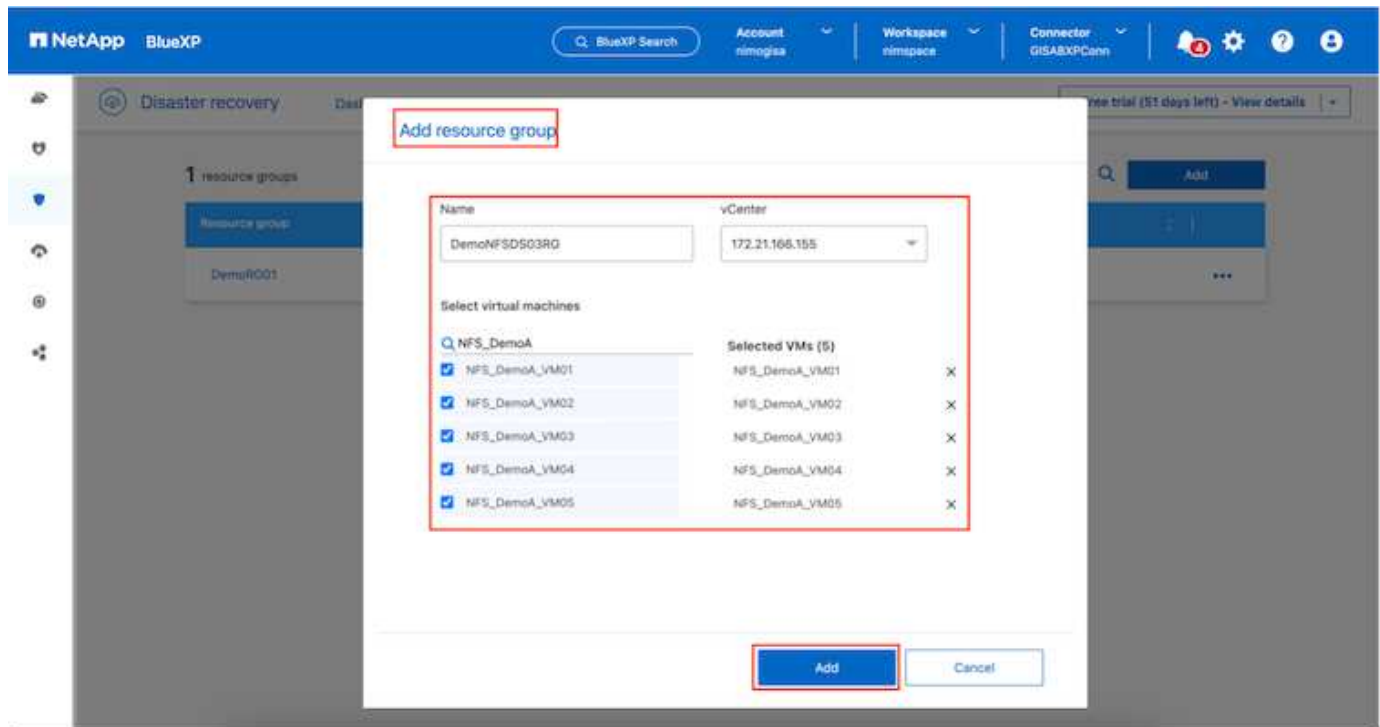
Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS rileva la relazione e continua con il resto delle operazioni del flusso di lavoro.

Cosa può fare per te il BlueXP disaster recovery ?

Dopo aver aggiunto i siti di origine e di destinazione, il BlueXP disaster recovery esegue automaticamente un'analisi approfondita e visualizza le VM insieme ai metadati associati. Il BlueXP disaster recovery rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle VM e li popola.

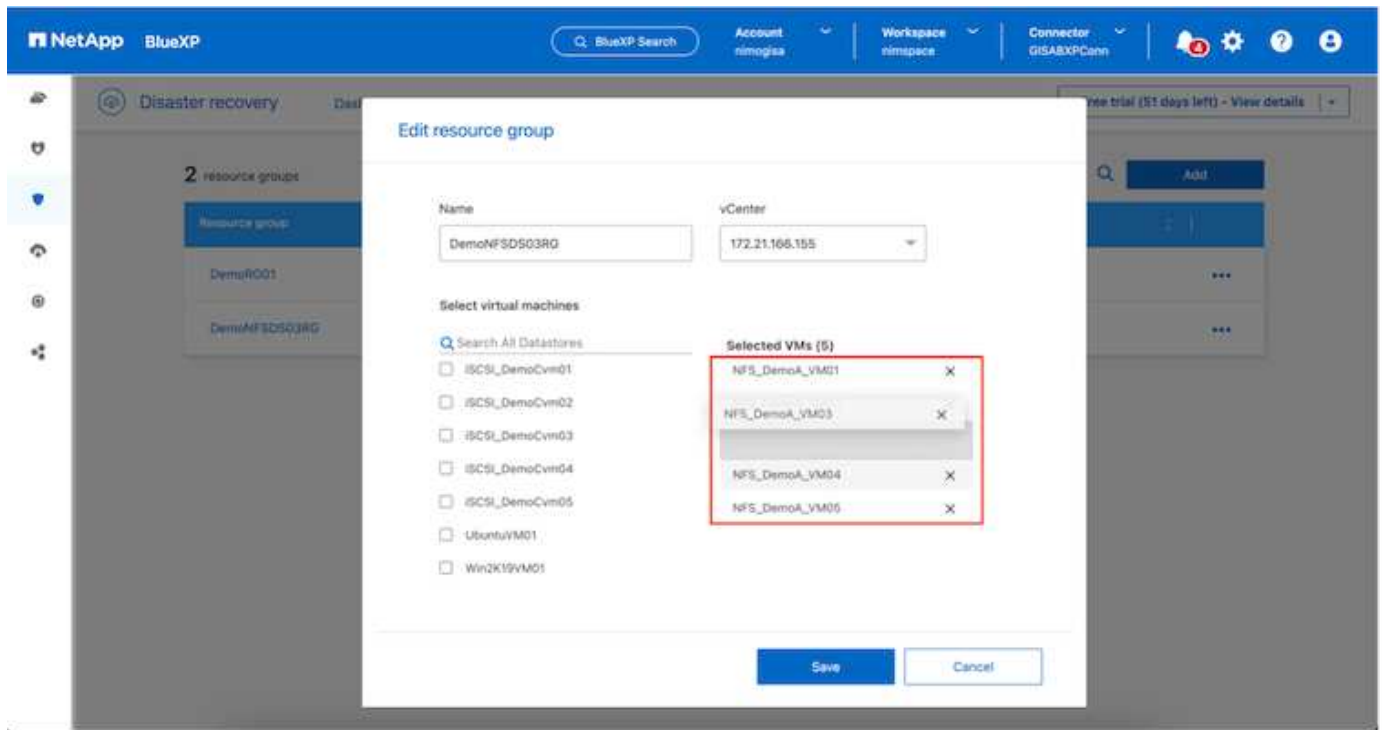
| Site Name | IP Address | Health | VMs | Datastores | Resource groups | Connector |
|-------------|----------------|---------|-----|------------|-----------------|------------|
| nimDemoSrc | 172.21.166.155 | Healthy | 72 | 13 | 1 | GISABXPCnn |
| nimDemoDest | 172.21.166.190 | Healthy | 61 | 3 | 0 | GISABXPCnn |

Dopo aver aggiunto i siti, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse BlueXP disaster recovery consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti al momento del ripristino. Per iniziare a creare gruppi di risorse, vai su **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.

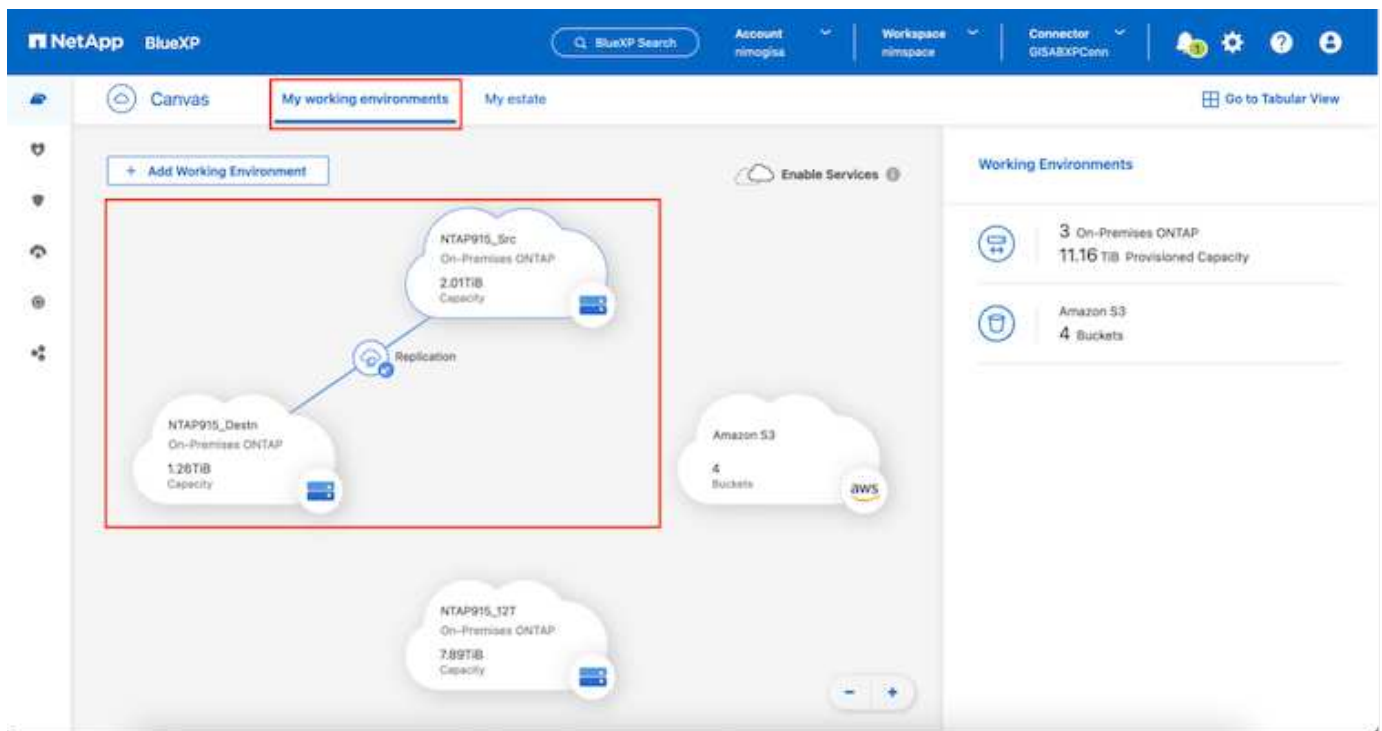


Il gruppo di risorse può essere creato anche durante la creazione di un piano di replica.

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



Una volta creati i gruppi di risorse, il passaggio successivo consiste nel creare il progetto di esecuzione o un piano per ripristinare macchine virtuali e applicazioni in caso di disastro. Come indicato nei prerequisiti, la replica 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.



| Health Status | Source Volume | Target Volume | Total Transfer Time | Status | Mirror State | Last Successful Transfer |
|---------------|-------------------------------|--------------------------------------|---------------------|--------|--------------|----------------------------------|
| | NTAP915_Src | NTAP915_Destn | | | | 2023 Sep |
| ✓ | Demo_TPS_DS01 NTAP915_Src | Demo_TPS_DS01_Copy NTAP915_Destn | 13 seconds | idle | snapmirrored | Aug 5, 2024, 6:15 386.63 MiB |
| ✓ | Src_250_Vol01 NTAP915_Src | Src_250_Vol01_Copy NTAP915_Destn | 4 seconds | idle | snapmirrored | Aug 16, 2024, 12:1 79.23 MiB |
| ✓ | Src_NFS_DS03 NTAP915_Src | Src_NFS_DS03_CP NTAP915_Destn | 12 seconds | idle | snapmirrored | Aug 16, 2024, 12:1 24.64 MiB |
| ✓ | Src_NFS_DS04 NTAP915_Src | Src_NFS_DS04_CP NTAP915_Destn | 3 seconds | idle | snapmirrored | Aug 16, 2024, 12:1 47.38 MiB |
| ✓ | Src_JSCSI_DS04 NTAP915_Src | Src_JSCSI_DS04_copy NTAP915_Destn | 4 seconds | idle | snapmirrored | Aug 16, 2024, 12:1 108.87 MiB |
| ✓ | nimpra NTAP915_Src | nimpra_dest NTAP915_Destn | 2 seconds | idle | snapmirrored | Aug 16, 2024, 12:1 3.48 KiB |

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**.

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.

Add replication plan

1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

Replication plan name
DemoNFSDS03RP

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

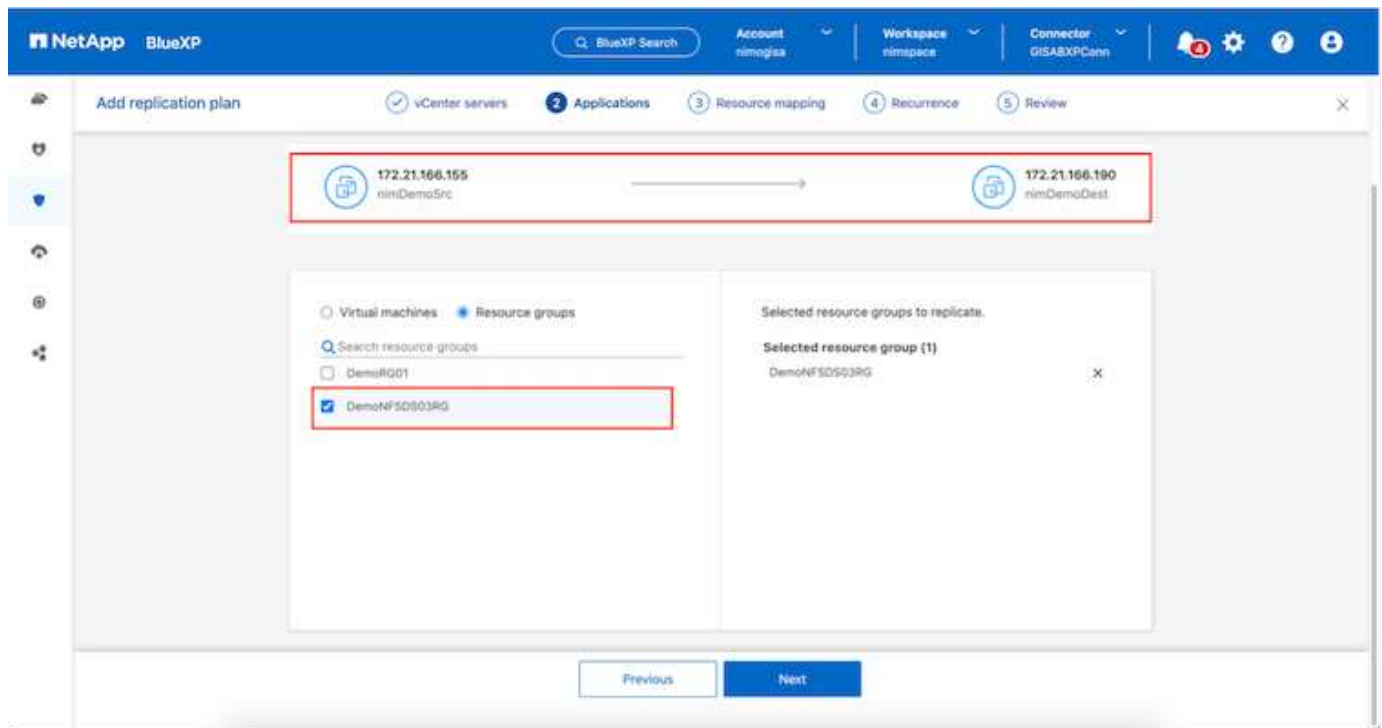
Source vCenter: 172.21.166.155

Target vCenter: 172.21.166.190

Cancel Next

Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono

essere ripristinate le macchine virtuali delle applicazioni.

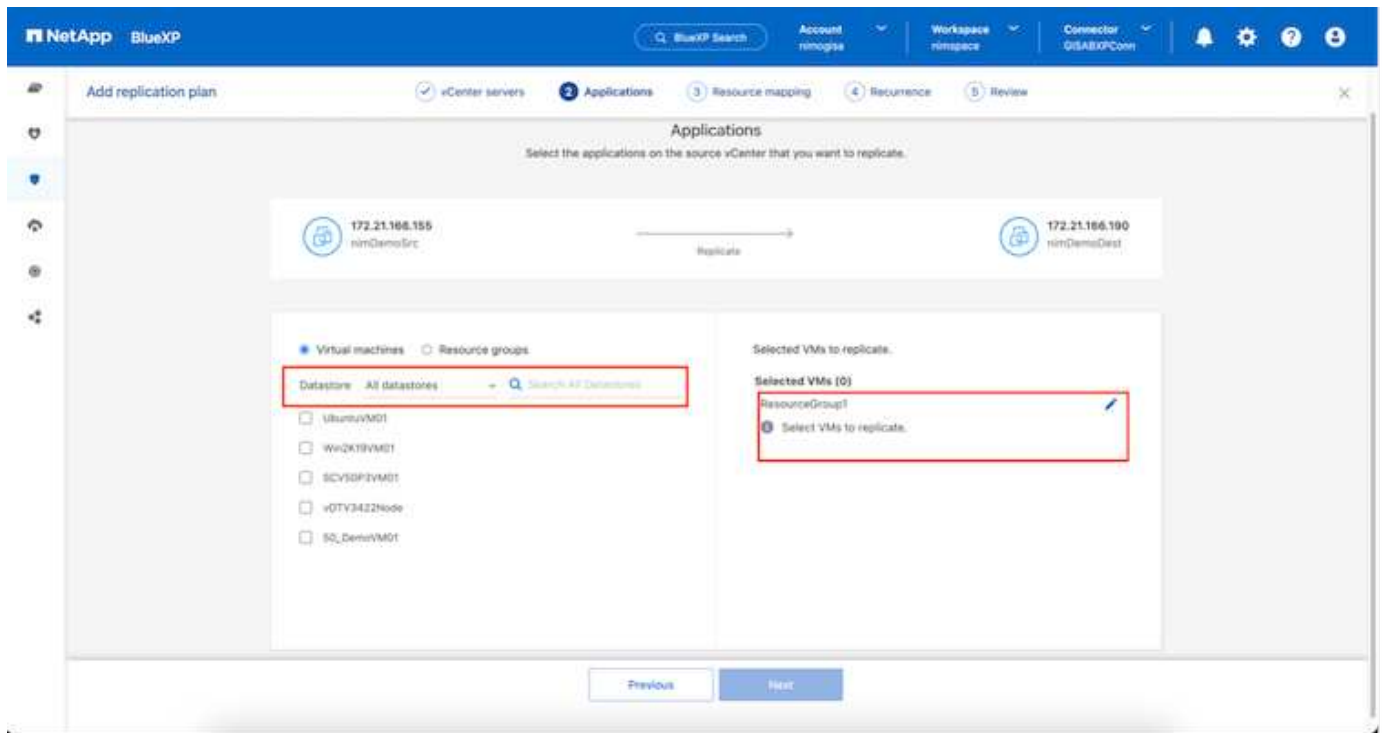


Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.

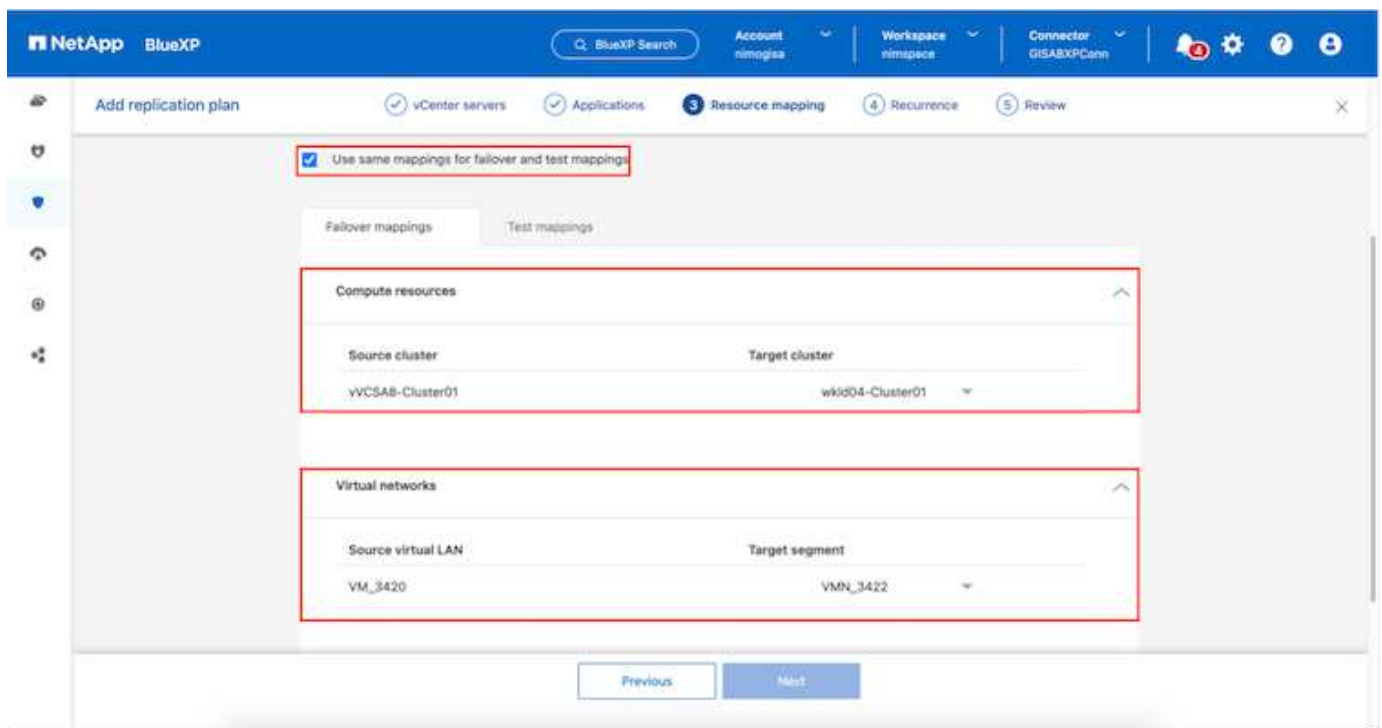


Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Vengono avviati in parallelo due gruppi di risorse.

La schermata seguente mostra l'opzione per filtrare macchine virtuali o datastore specifici in base ai requisiti organizzativi se i gruppi di risorse non sono stati creati in precedenza.



Una volta selezionati i gruppi di risorse, creare i mapping di failover. In questo passaggio, specificare come le risorse dall'ambiente di origine vengono mappate alla destinazione. Ciò include risorse di elaborazione e reti virtuali. Personalizzazione IP, pre- e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento a ["Creare un piano di replicazione"](#).



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

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCnn

Add replication plan vCenter servers Applications **3 Resource mapping** 4 Recurrence 5 Review

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for Same as source

☐ Use the same script for all V Different from source

| Source VM | CPU | RAM | Boot delay (mins between 0 and 10) | Create application consistent replicas |
|----------------|-----|------|------------------------------------|--|
| DemoNFS03R0 | | | | |
| NFS_DemoA_VM01 | 2 | 4 GB | 0 | <input type="checkbox"/> |
| NFS_DemoA_VM02 | 2 | 4 GB | 0 | <input type="checkbox"/> |

Previous Next

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

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCnn

Add replication plan vCenter servers Applications **3 Resource mapping** **4 Recurrence** 5 Review

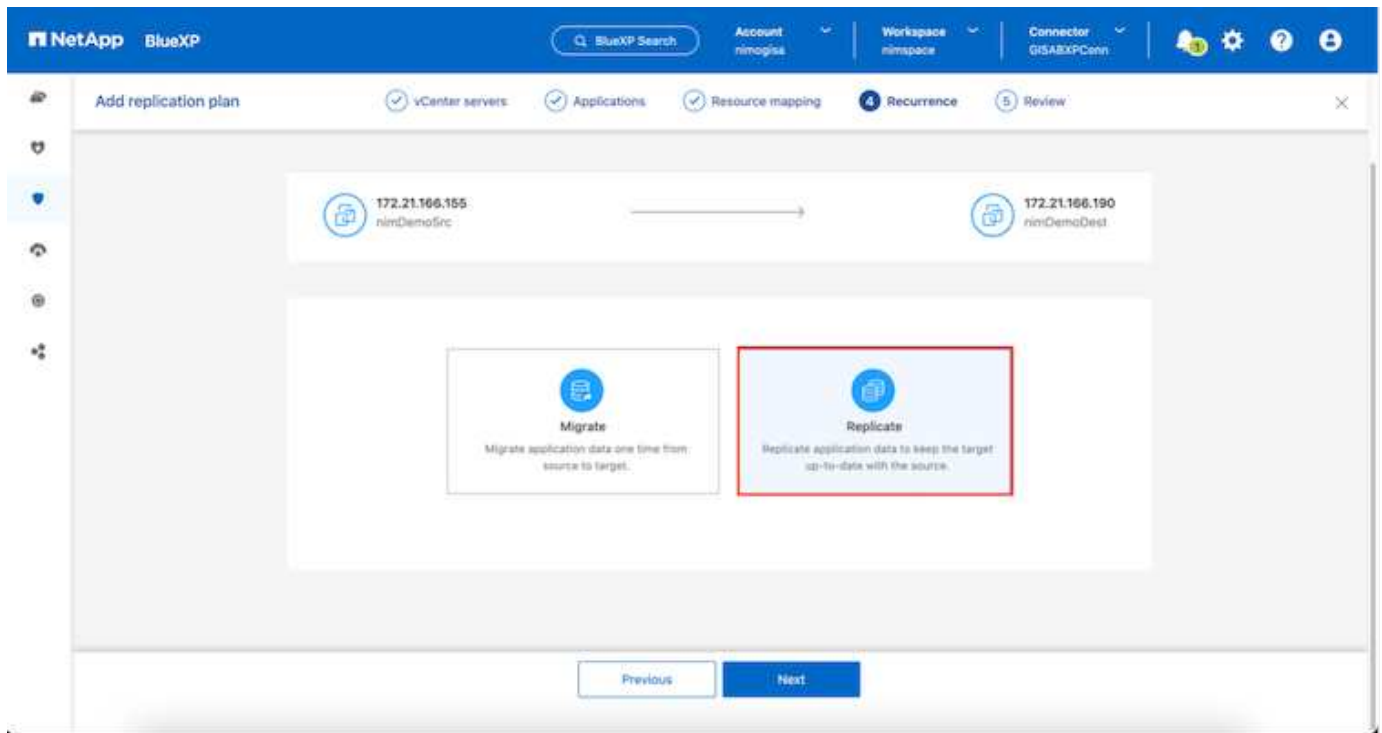
172.21.166.165 nimDemoSrc → 172.21.166.190 nimDemoDest

☒ Use same mappings for failover and test mappings

| Fallover mappings | Test mappings |
|-------------------|---------------|
| Compute resources | Mapped |
| Virtual networks | Mapped |
| Virtual machines | Mapped |

Previous Next

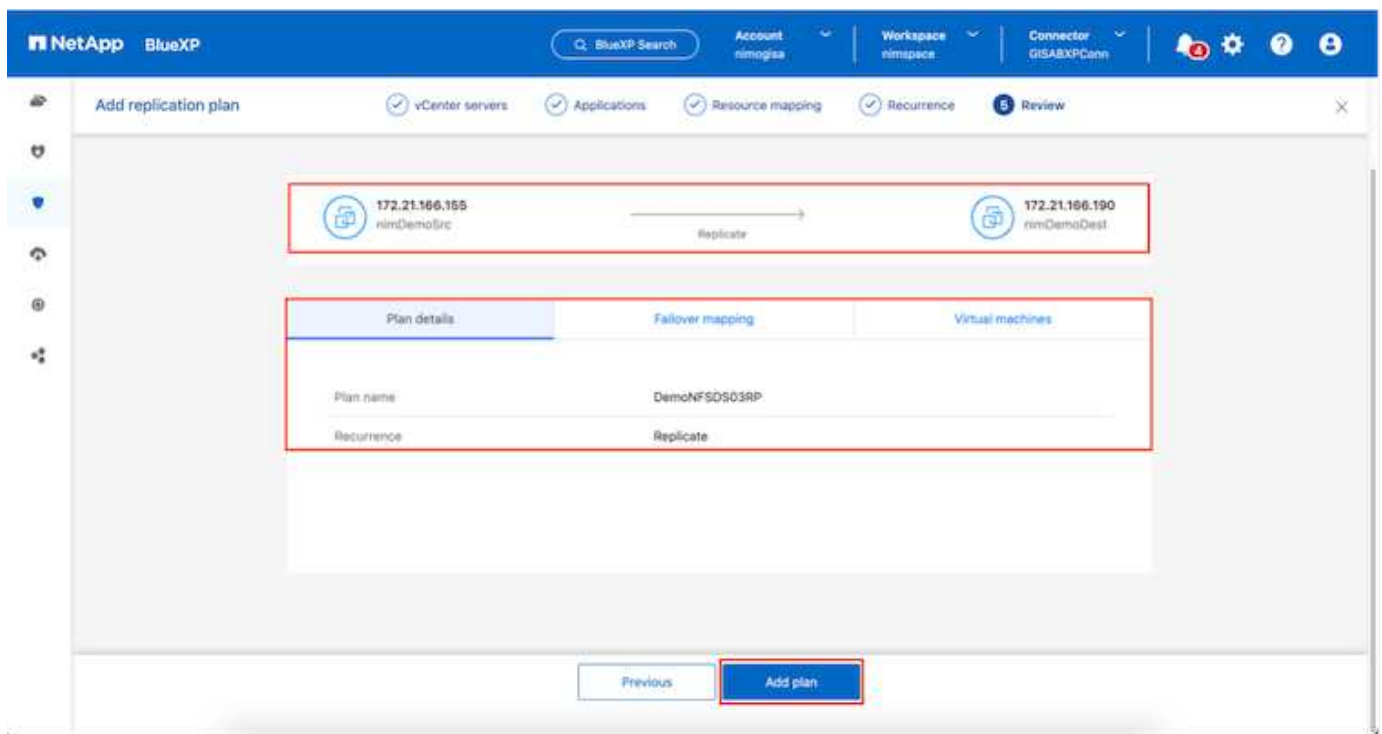
Selezionare il tipo di ricorrenza. In parole semplici, seleziona l'opzione Migra (migrazione una tantum tramite failover) o replica continua ricorrente. In questa procedura dettagliata è selezionata l'opzione Replica.

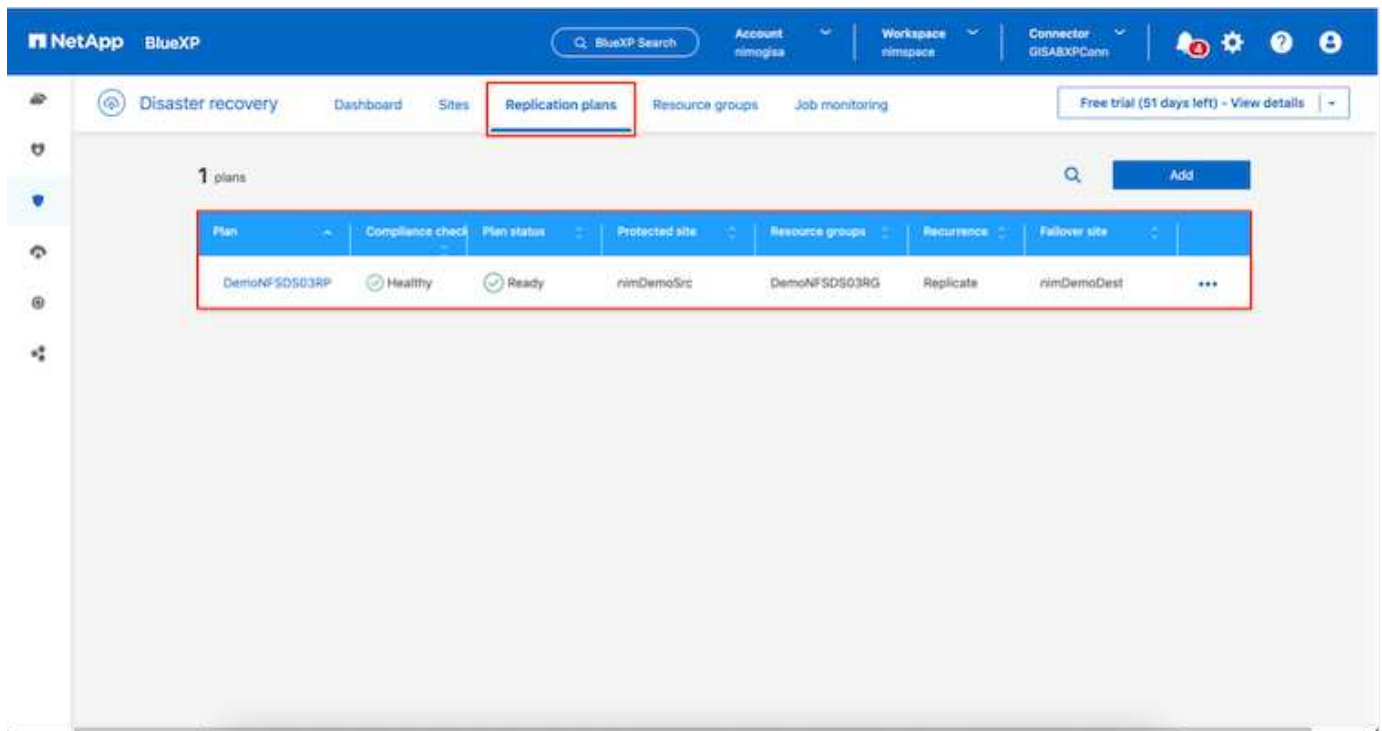


Una volta fatto, rivedi le mappature create e poi clicca su **Aggiungi piano**.



In un piano di replicazione è possibile includere VM di volumi diversi e SVM. A seconda del posizionamento della VM (sia sullo stesso volume o su volumi separati all'interno della stessa SVM, volumi separati su SVM diverse), il BlueXP disaster recovery crea uno snapshot del gruppo di coerenza.



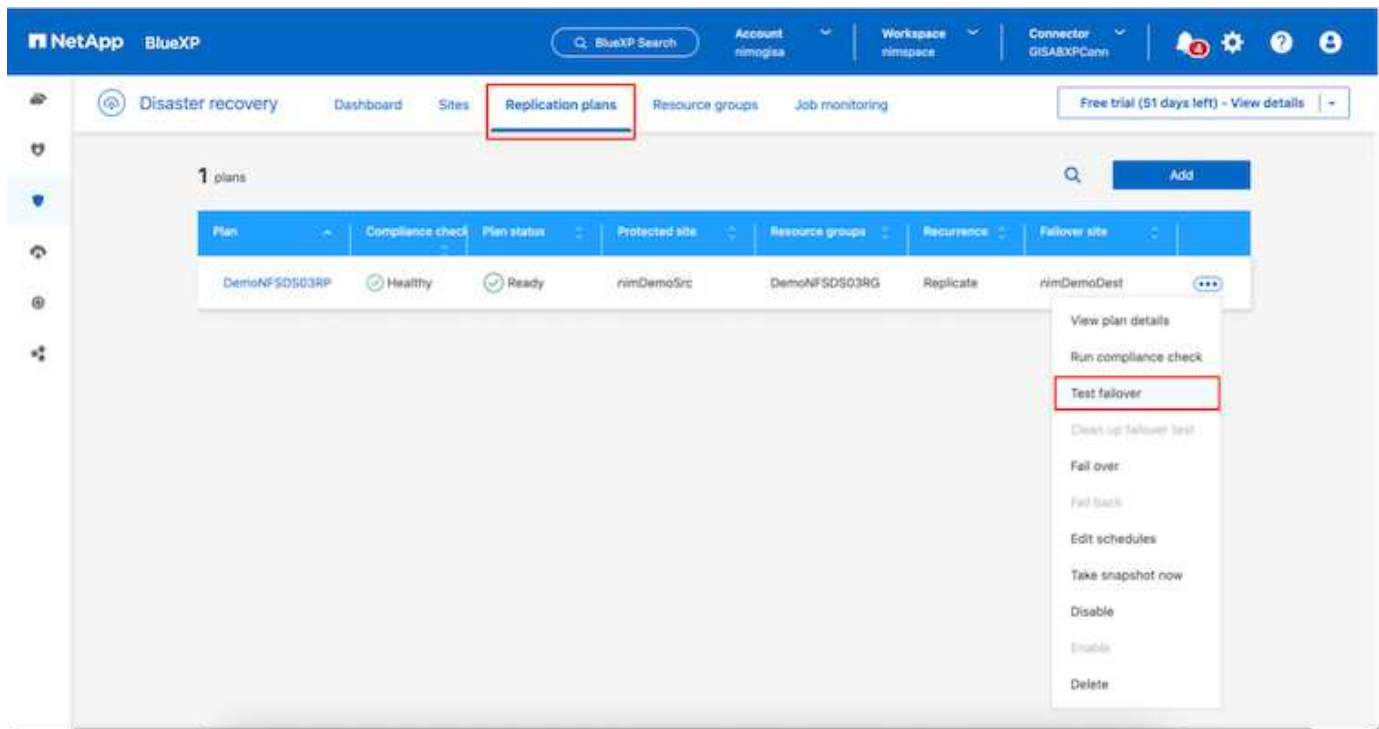


BlueXP DRaaS è costituito dai seguenti flussi di lavoro:

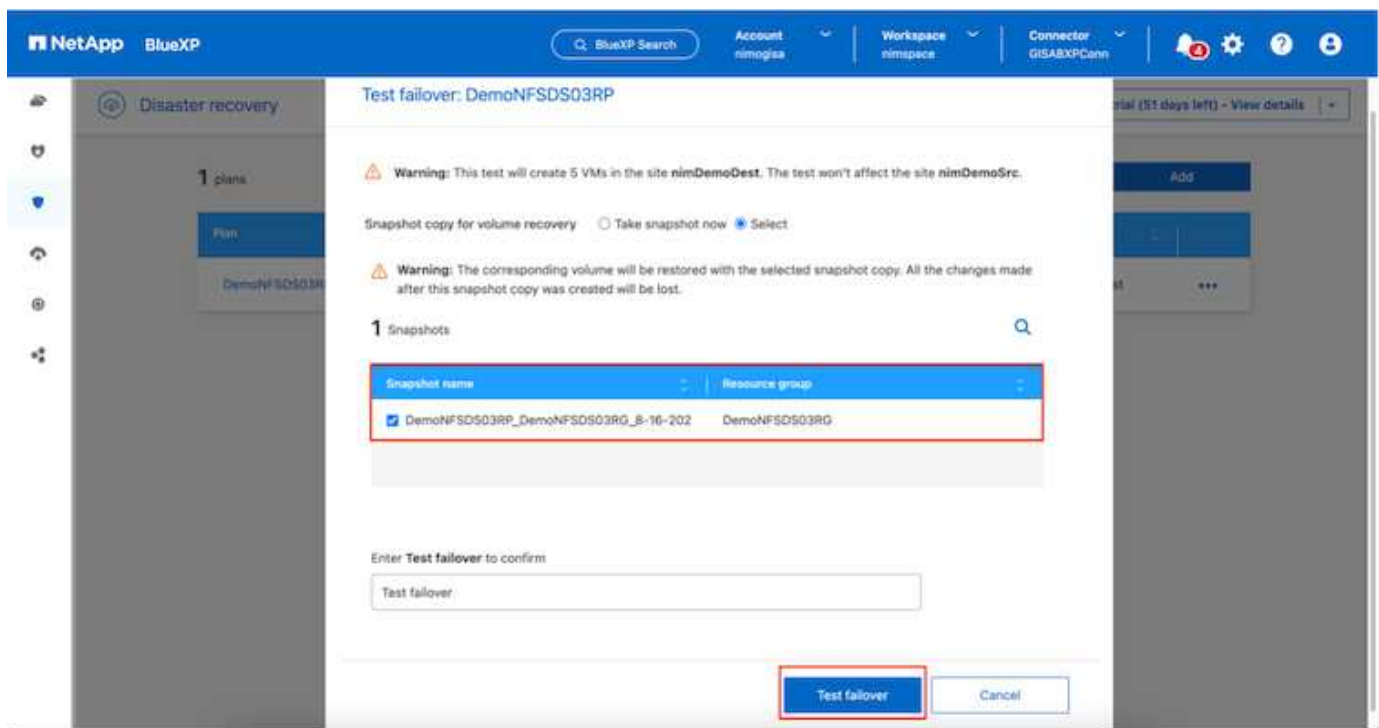
- Failover di test (incluse simulazioni automatiche periodiche)
- Test di failover di pulizia
- Failover
- Rifasamento

Failover di prova

Il failover di test 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.



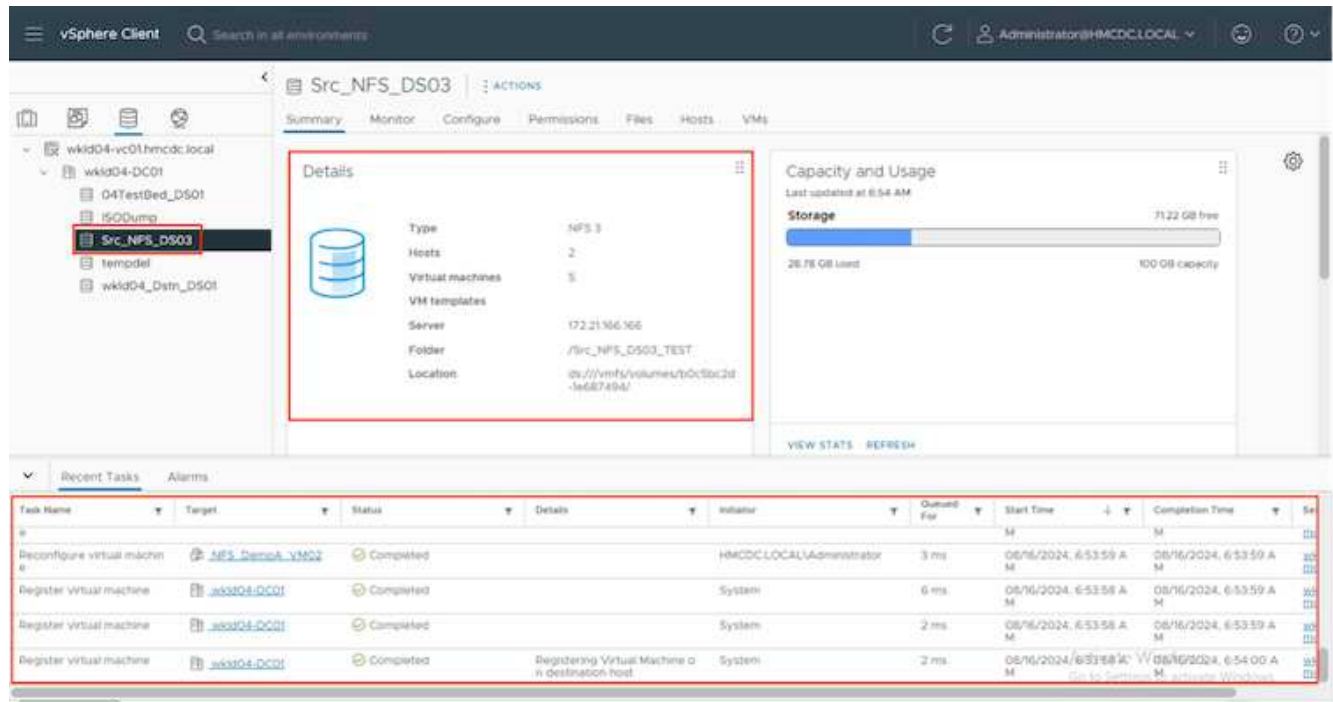
BlueXP DRaaS incorpora la possibilità di selezionare lo snapshot come funzionalità opzionale nell'operazione di failover di test. Questa funzionalità consente all'amministratore VMware di verificare che tutte le modifiche apportate di recente all'ambiente vengano replicate nel sito di destinazione e siano 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 prova, BlueXP DRaaS automatizza le seguenti attività:

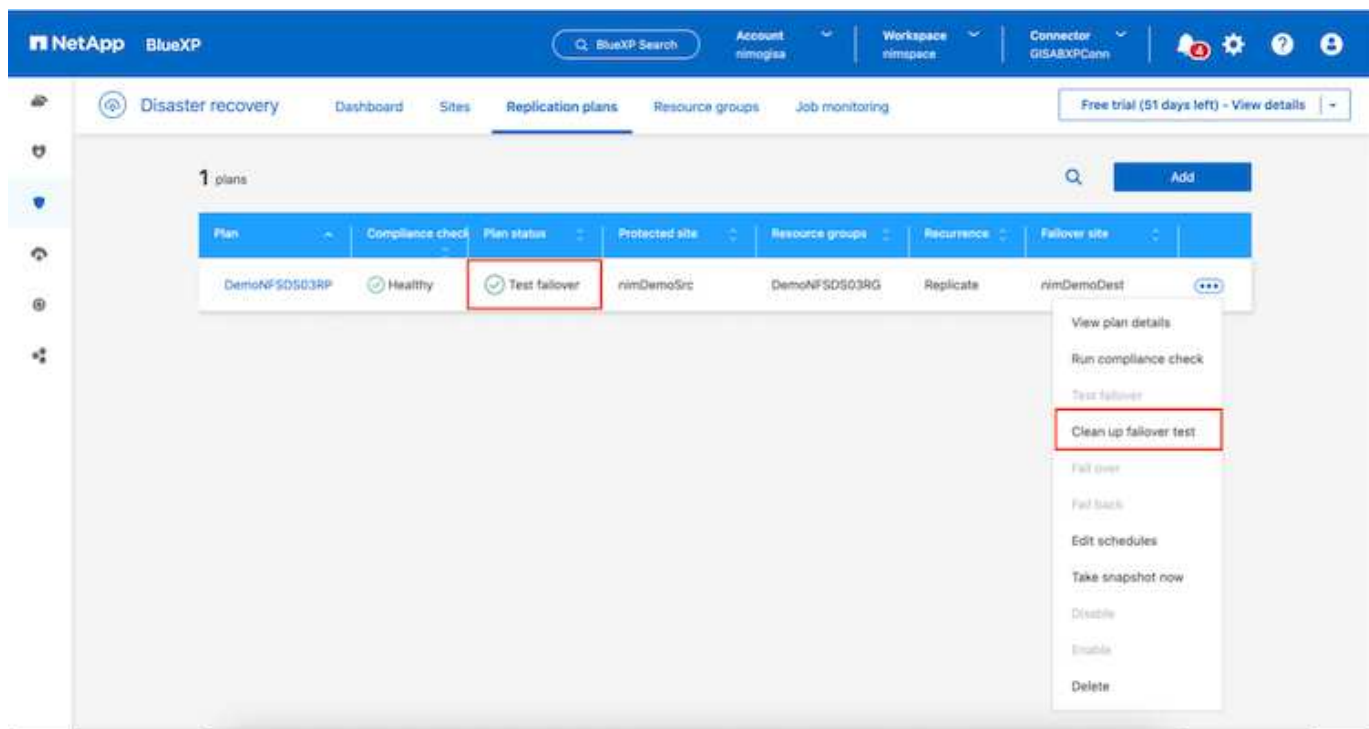
- Attivazione delle relazioni SnapMirror per aggiornare l'archiviazione nel sito di destinazione con tutte le modifiche recenti apportate nel sito di produzione.

- Creazione di volumi NetApp FlexClone dei volumi FlexVol sull'array di archiviazione DR.
- Collegamento dei datastore NFS nei volumi FlexClone agli host ESXi nel sito DR.
- Collegamento degli adattatori di rete della VM alla rete di prova specificata durante la mappatura.
- Riconfigurazione delle impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito DR.
- Esecuzione di tutti i comandi personalizzati memorizzati nel piano di replicazione.
- Accensione delle VM nell'ordine definito nel piano di replica.



Operazione di test di failover di pulizia

L'operazione di test di failover di pulizia avviene dopo il completamento del test del piano di replica e quando l'amministratore VMware risponde al prompt di pulizia.



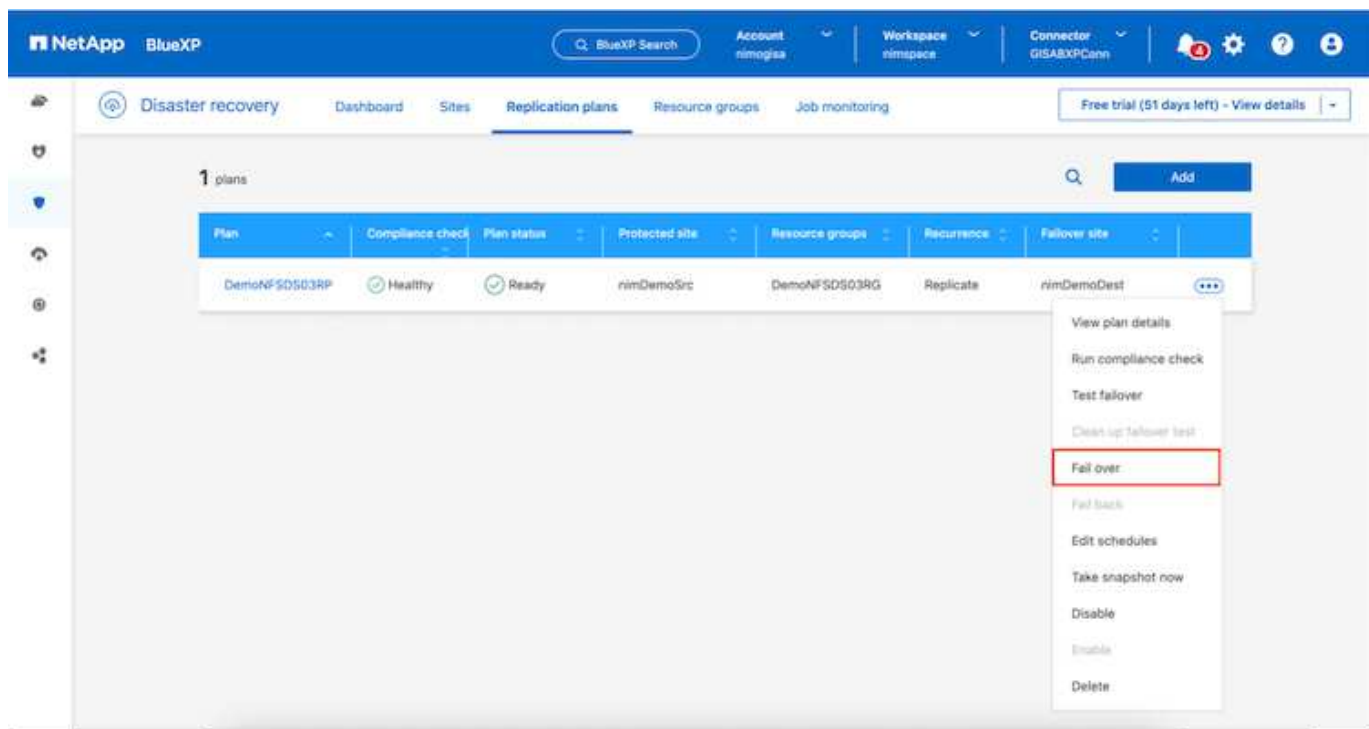
Questa azione reimposterà le macchine virtuali (VM) e lo stato del piano di replica allo stato pronto.

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

1. Spegne ogni VM recuperata nella copia FlexClone utilizzata per il test.
2. Elimina il volume FlexClone utilizzato per presentare le VM recuperate durante il test.

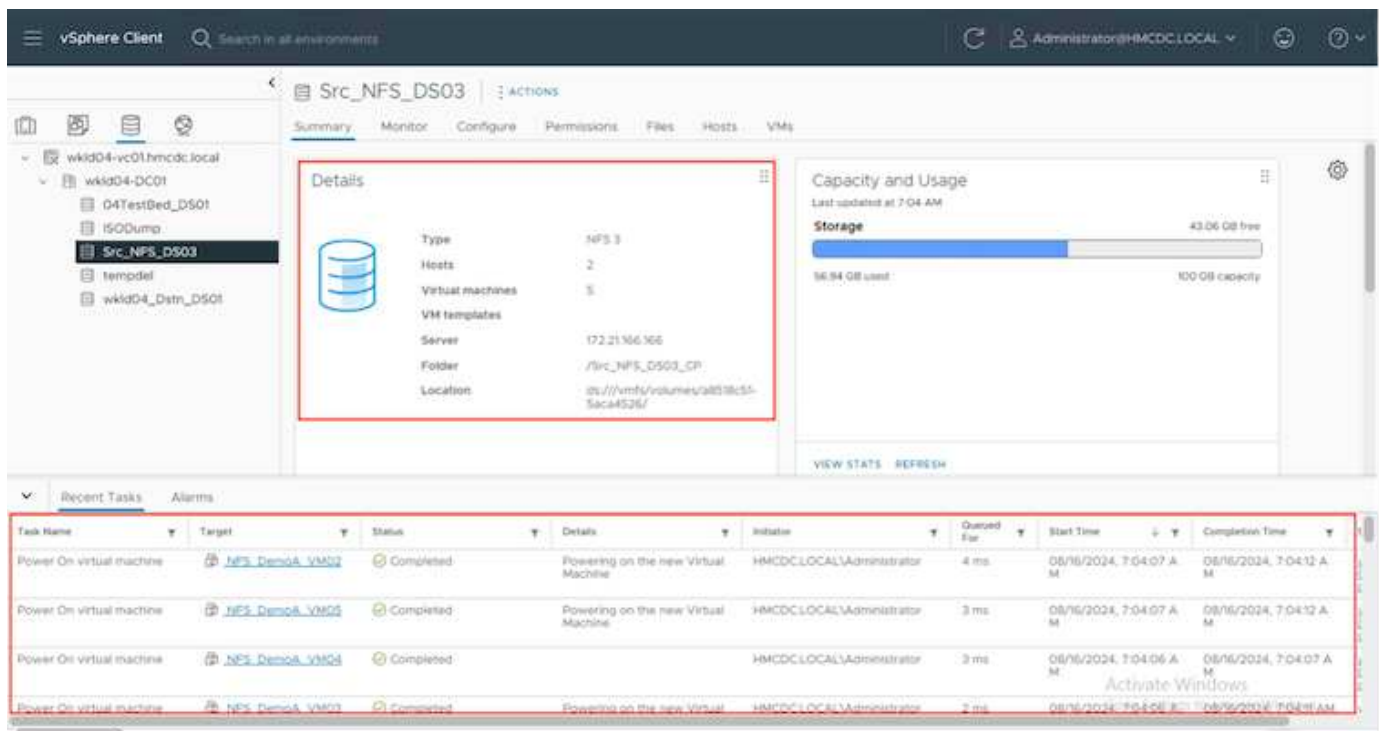
Migrazione pianificata e failover

BlueXP DRaaS dispone di due metodi per eseguire un failover reale: migrazione pianificata e failover. Il primo metodo, la migrazione pianificata, incorpora l'arresto delle VM e la sincronizzazione della replicazione dello storage nel processo per ripristinare o spostare efficacemente le VM 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 VM vengono ripristinate nel sito di destinazione dall'ultimo intervallo di replicazione dell'archiviazione che è stato possibile completare. A seconda dell'RPO progettato nella soluzione, è possibile che si verifichi una certa perdita di dati nello scenario DR.



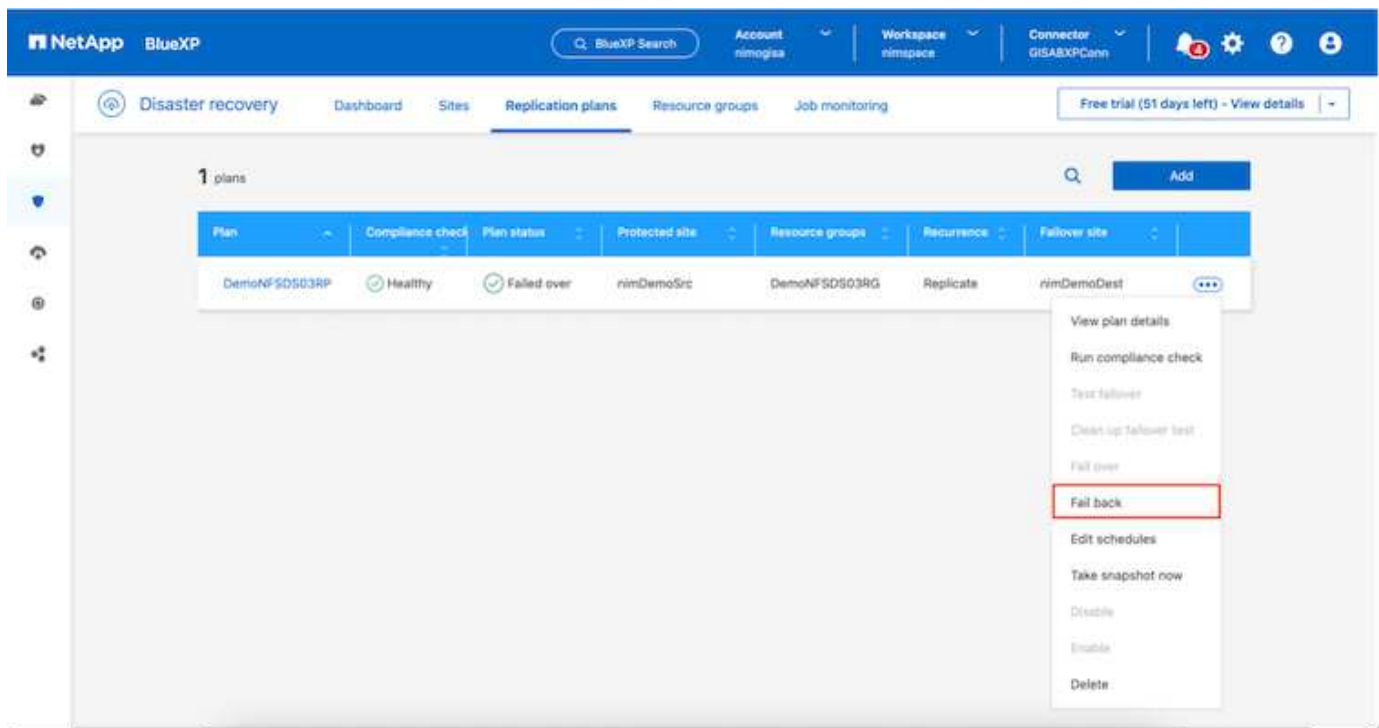
Quando l'amministratore VMware esegue un'operazione di failover, BlueXP DRaaS automatizza le seguenti attività:

- Interrompere ed eseguire il failover delle relazioni NetApp SnapMirror .
- Collegare i datastore NFS replicati agli host ESXi nel sito DR.
- Collegare gli adattatori di rete della VM 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 memorizzati nel piano di replicazione.
- Accendere le VM nell'ordine definito nel piano di replica.



Rifasamento

Un failback è una procedura facoltativa 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 a ripristinare i servizi sul sito di origine.

NOTA: BlueXP DRaaS replica (risincronizza) tutte le modifiche sulla macchina virtuale di origine prima di invertire la direzione della replica. Questo processo inizia da una relazione che ha completato il failover verso

una destinazione e prevede i seguenti passaggi:

- Spegner e annullare la registrazione delle macchine virtuali e dei volumi sul sito di destinazione.
- Interrompere la relazione SnapMirror sulla sorgente originale per renderla di lettura/scrittura.
- Risincronizzare la relazione SnapMirror per invertire la replica.
- Montare il volume sulla sorgente, accendere e registrare le macchine virtuali di origine.

Per maggiori dettagli sull'accesso e la configurazione di BlueXP DRaaS, vedere ["Scopri di più su BlueXP Disaster Recovery per VMware"](#).

Monitoraggio e dashboard

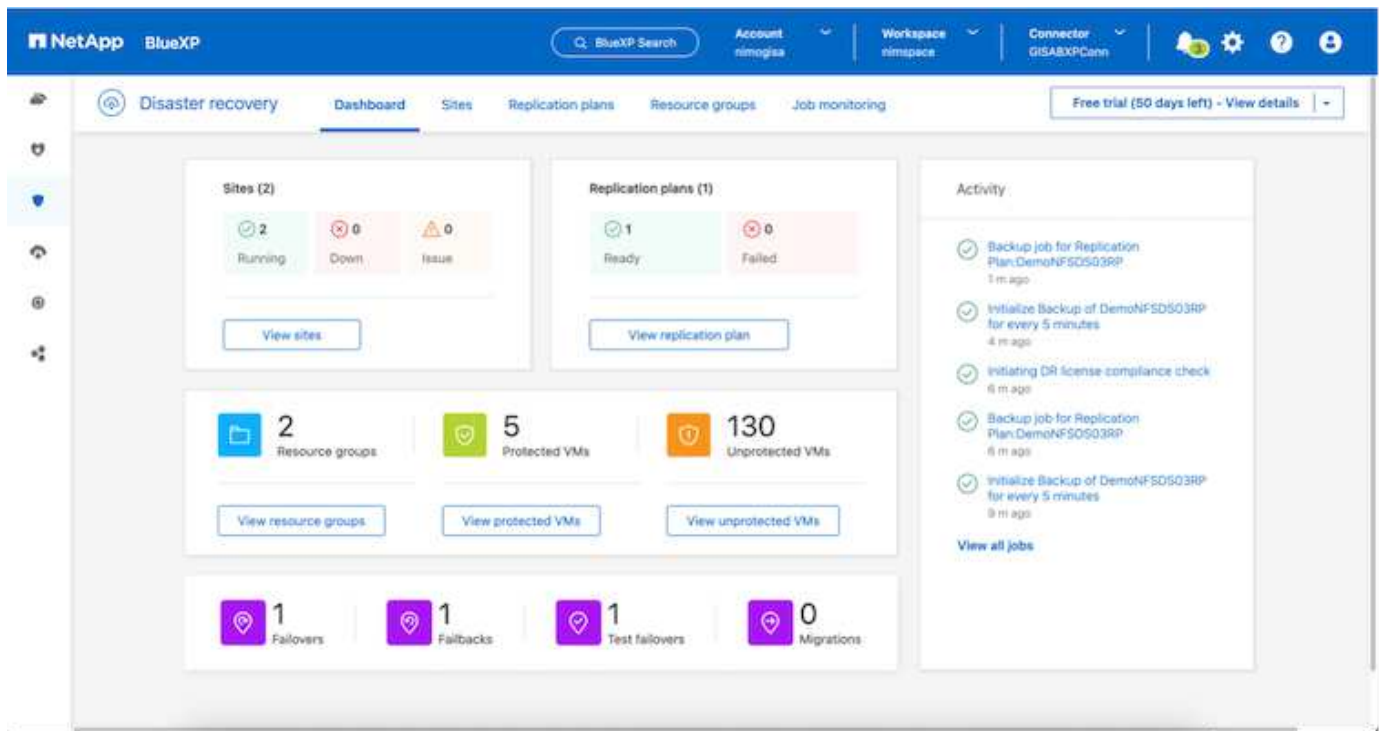
Da BlueXP o dalla CLI ONTAP è possibile monitorare lo stato di integrità della replica per i volumi del datastore appropriati, mentre lo stato di un failover o di un failover di prova può essere monitorato tramite Job Monitoring.

| ID | Status | Workload | Name | Start time | End time |
|--------------------|-----------|------------|---|---------------------|---------------------|
| d923e507-b2c2-401 | In pro... | Backup | Backup job for Replication Plan: DemoNF... | 08/16/2024, 04:5... | - |
| 3549cc9c-aa4e-45e | Succe... | Backup | Initialize Backup of DemoNFSDS03RP for... | 08/16/2024, 04:5... | 08/16/2024, 04:5... |
| 5cb01bcc-9ea5-4afl | Succe... | Backup | Backup job for Replication Plan: DemoNF... | 08/16/2024, 04:4... | 08/16/2024, 04:5... |
| a2f225d9-b7be-4c2f | Succe... | Backup | Initialize Backup of DemoNFSDS03RP for... | 08/16/2024, 04:4... | 08/16/2024, 04:4... |
| 2f8b44d4-4be2-46f | Succe... | Compliance | Compliance check for Replication Plan: D... | 08/16/2024, 04:4... | 08/16/2024, 04:4... |
| 398bc6a3-ata8-45d | Succe... | Compliance | Initialize Compliance of DemoNFSDS03RP... | 08/16/2024, 04:4... | 08/16/2024, 04:4... |
| 97f0bed8-6f77-459f | Succe... | Backup | Backup job for Replication Plan: DemoNF... | 08/16/2024, 04:4... | 08/16/2024, 04:4... |
| bffc015e-ca3a-409d | Succe... | Backup | Initialize Backup of DemoNFSDS03RP for... | 08/16/2024, 04:4... | 08/16/2024, 04:4... |
| cde759a8-ebef-498b | Succe... | Backup | Backup job for Replication Plan: DemoNF... | 08/16/2024, 04:3... | 08/16/2024, 04:4... |
| a414daba-9630-4c5 | Succe... | Backup | Initialize Backup of DemoNFSDS03RP for... | 08/16/2024, 04:3... | 08/16/2024, 04:3... |



Se un lavoro è in corso o in coda e si desidera interromperlo, è disponibile un'opzione per annullarlo.

Grazie alla dashboard BlueXP disaster recovery, puoi valutare con sicurezza lo stato dei siti di disaster recovery e dei piani di replica. Ciò consente agli amministratori di identificare rapidamente siti e piani integri, disconnessi o degradati.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, sentiti libero di seguire il video dettagliato o di utilizzare il ["simulatore di soluzioni"](#).

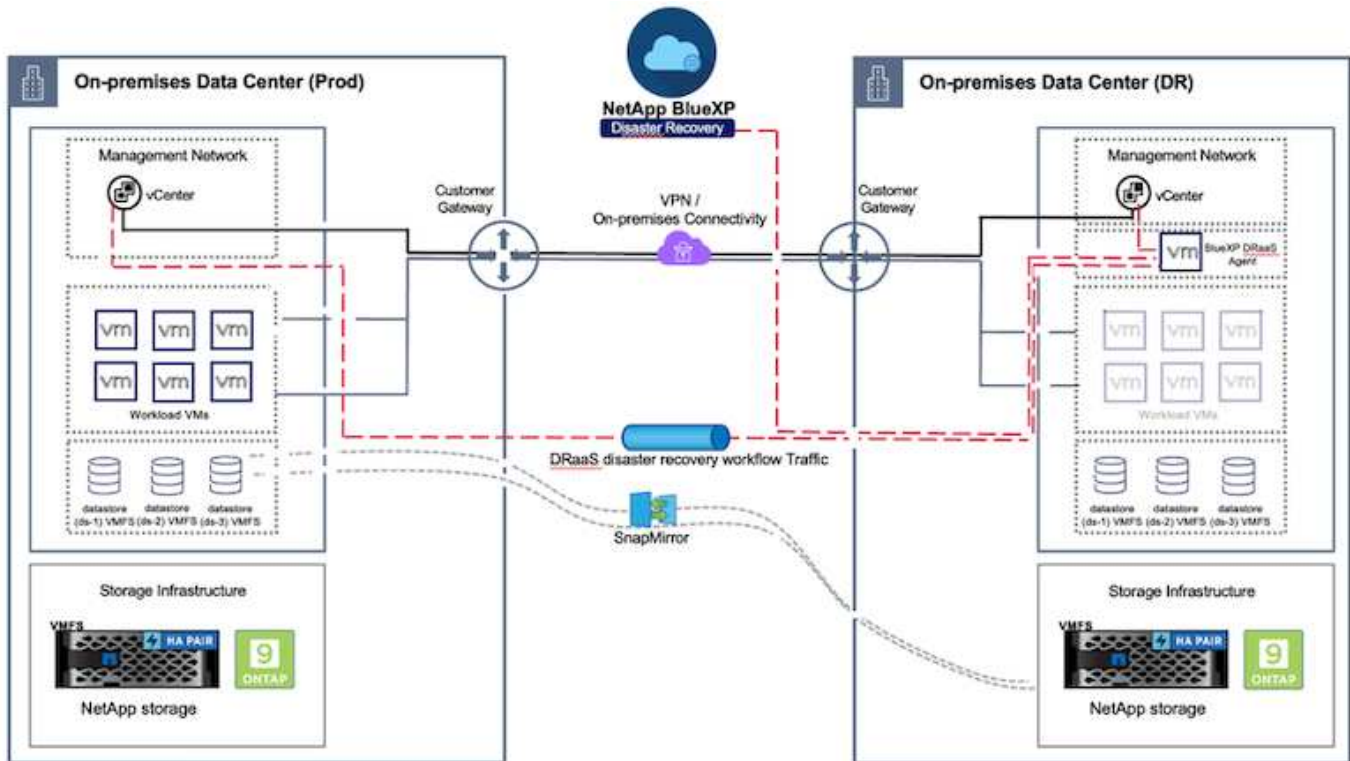
DR tramite BlueXP DRaaS per datastore VMFS

Il disaster recovery mediante replica a livello di blocco dal sito di produzione al sito di disaster recovery è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Con la replica NetApp SnapMirror, i carichi di lavoro VMware in esecuzione su sistemi ONTAP locali che utilizzano datastore VMFS possono essere replicati su un altro sistema di storage ONTAP in un data center di ripristino designato in cui risiede VMware.

Questa sezione del documento descrive la configurazione di BlueXP DRaaS per impostare il disaster recovery per le VM VMware on-premise su un altro sito designato. Come parte di questa configurazione, l'account BlueXP, il connettore BlueXP e gli array ONTAP sono stati aggiunti all'interno dell'area di lavoro BlueXP, necessari per abilitare la comunicazione da VMware vCenter allo storage ONTAP. Inoltre, questo documento spiega nel dettaglio come configurare la replica tra siti e come impostare e testare un piano di ripristino. L'ultima sezione contiene istruzioni su come eseguire un failover completo del sito e su come effettuare il failback quando il sito primario viene ripristinato e acquistato online.

Utilizzando il servizio BlueXP disaster recovery, integrato nella console NetApp BlueXP, i clienti possono scoprire i propri VMware vCenter on-premise insieme allo storage ONTAP, creare raggruppamenti di risorse, creare un piano di disaster recovery, associarlo a gruppi di risorse e testare o eseguire failover e failback. SnapMirror fornisce la replicazione a blocchi a livello di storage per mantenere i due siti aggiornati con modifiche incrementali, con un RPO fino a 5 minuti. È anche possibile simulare le procedure DR come un'esercitazione regolare senza influire sulla produzione e sui datastore replicati o incorrere in costi di

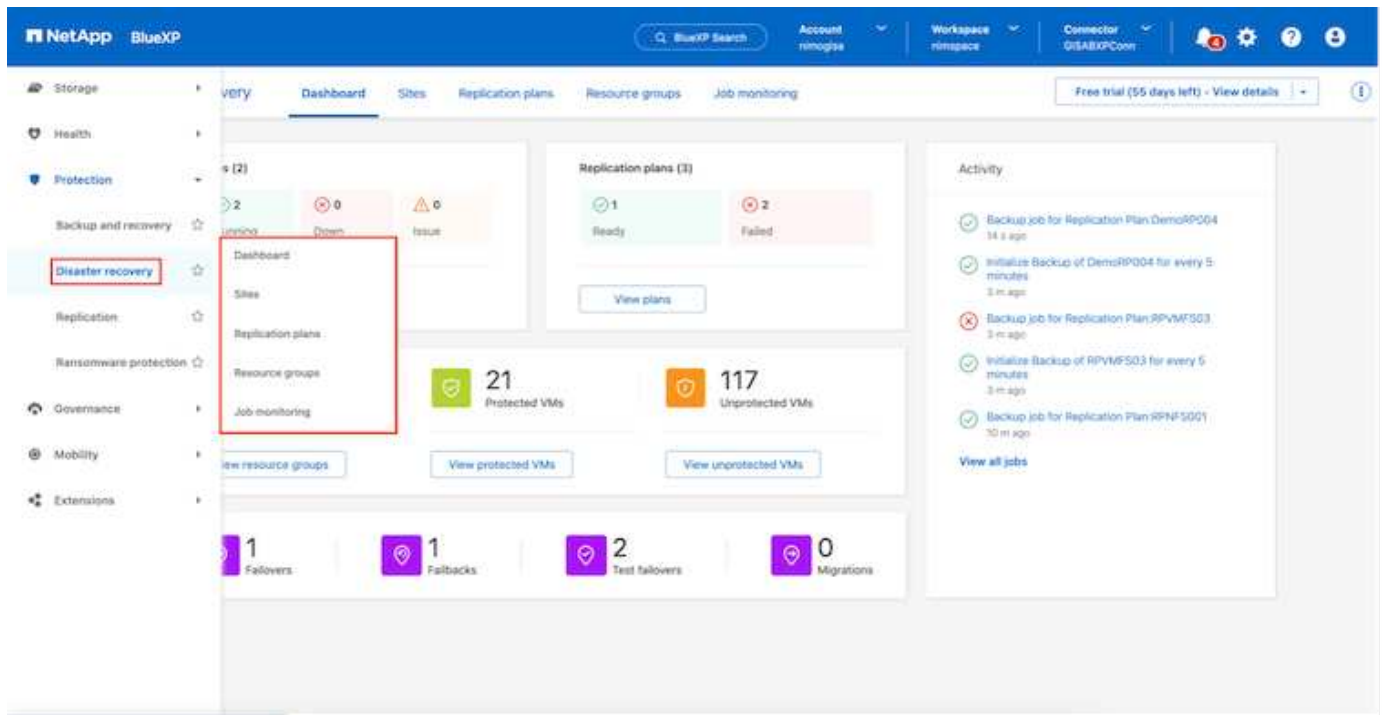
archiviazione aggiuntivi. Il BlueXP disaster recovery sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore VMFS dall'ultimo snapshot replicato sul sito DR. Una volta completato il test DR, i clienti possono semplicemente eliminare l'ambiente di test, sempre senza alcun impatto sulle risorse di produzione effettivamente replicate. Quando si verifica la necessità (pianificata o meno) di un failover effettivo, con pochi clic il servizio BlueXP disaster recovery organizzerà tutti i passaggi necessari per ripristinare automaticamente le macchine virtuali protette sul sito di disaster recovery designato. Il servizio invertirà anche la relazione SnapMirror con il sito primario e replicherà eventuali modifiche dal secondario al primario per un'operazione di failback, quando necessario. Tutto ciò può essere ottenuto con una frazione del costo rispetto ad altre alternative note.



Iniziare

Per iniziare a utilizzare il BlueXP disaster recovery, utilizzare la console BlueXP e quindi accedere al servizio.

1. Accedi a BlueXP.
2. Dal menu di navigazione a sinistra BlueXP , seleziona Protezione > Ripristino di emergenza.
3. Viene visualizzata la Dashboard BlueXP disaster recovery .



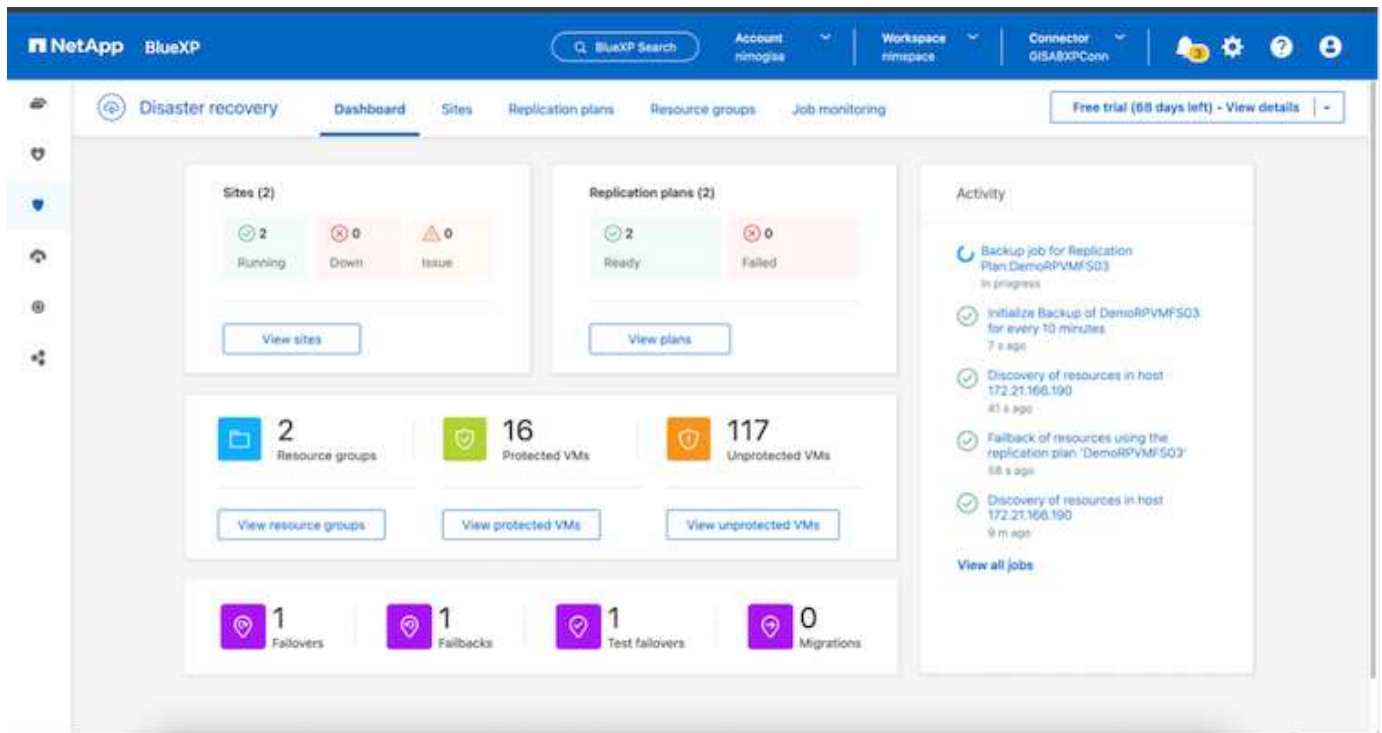
Prima di configurare il piano di disaster recovery, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- BlueXP Connector è configurato in NetApp BlueXP. Il connettore deve essere distribuito in AWS VPC.
- Le istanze del connettore BlueXP dispongono di connettività con i sistemi di archiviazione e vCenter di origine e di destinazione.
- In BlueXP sono stati aggiunti sistemi di storage NetApp on-premise che ospitano datastore VMFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su VMFS designati.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere dai 3 ai 5 minuti.



NetApp consiglia di distribuire il connettore BlueXP nel sito di disaster recovery o in un terzo sito, in modo che il connettore BlueXP possa comunicare tramite la rete con le risorse di origine e di destinazione durante interruzioni reali o calamità naturali.



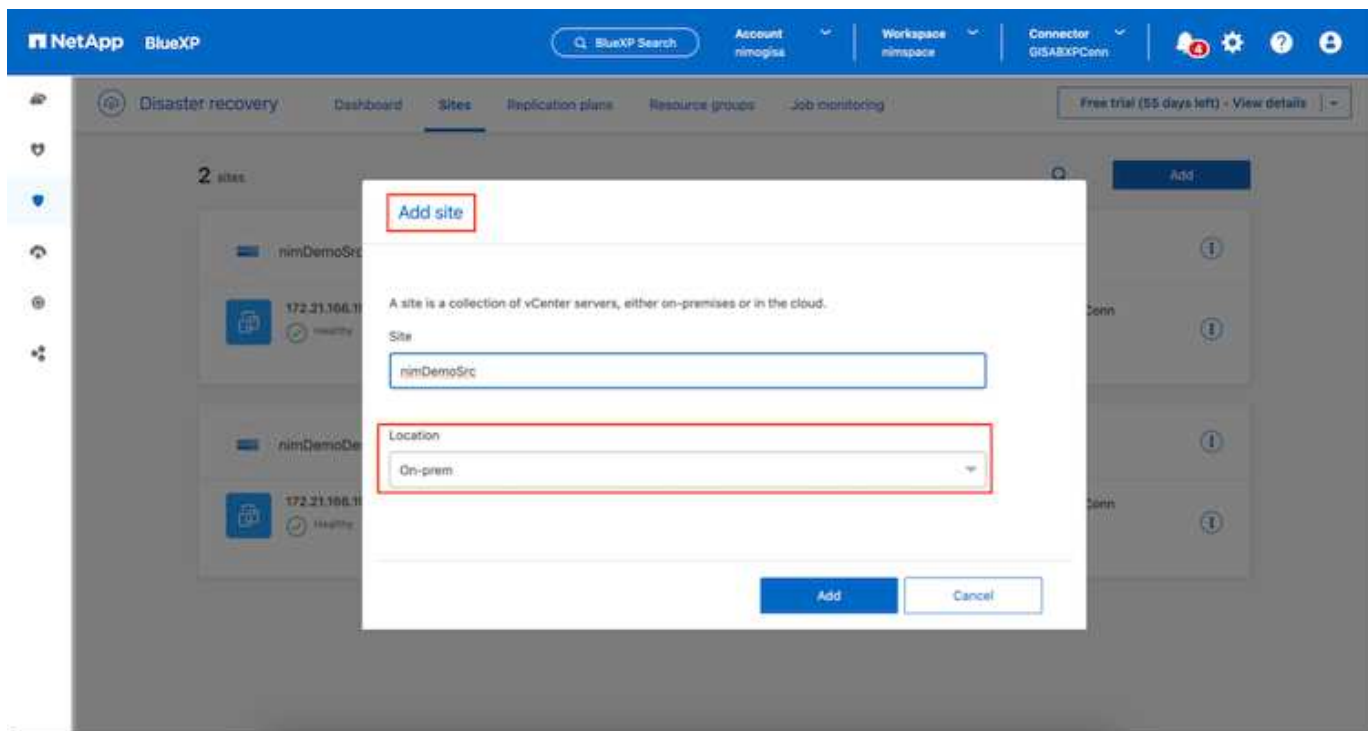
Al momento della stesura di questo documento, il supporto per i datastore VMFS da locale a locale è in fase di anteprima tecnologica. Questa funzionalità è supportata sia con i datastore VMFS basati sul protocollo FC che ISCSI.

Configurazione BlueXP disaster recovery

Il primo passo per prepararsi al disaster recovery è individuare e aggiungere le risorse di archiviazione e vCenter locali al BlueXP disaster recovery.

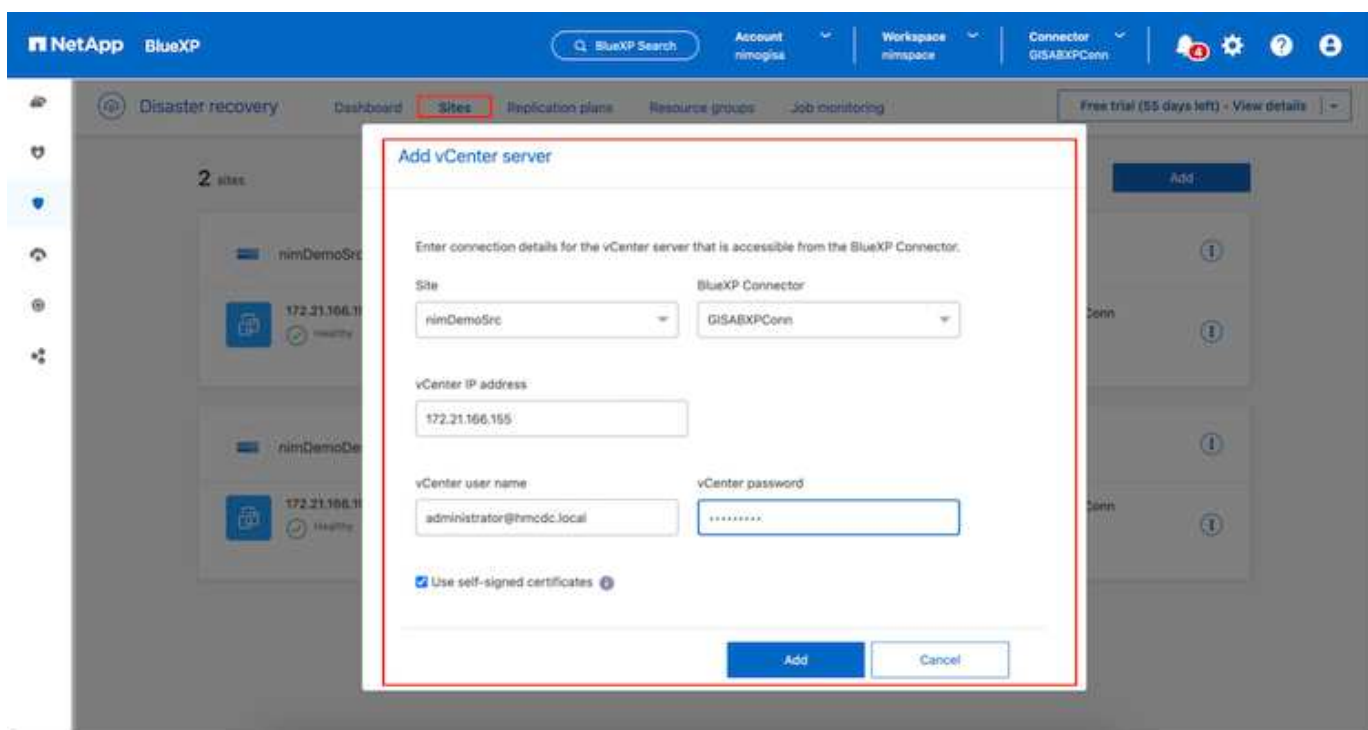


Assicurarsi che i sistemi di archiviazione ONTAP siano aggiunti all'ambiente di lavoro all'interno della tela. Aprire la console BlueXP e selezionare **Protezione > Ripristino di emergenza** dal menu di navigazione a sinistra. Selezionare **Scopri server vCenter** oppure utilizzare il menu in alto, selezionare **Siti > Aggiungi > Aggiungi vCenter**.

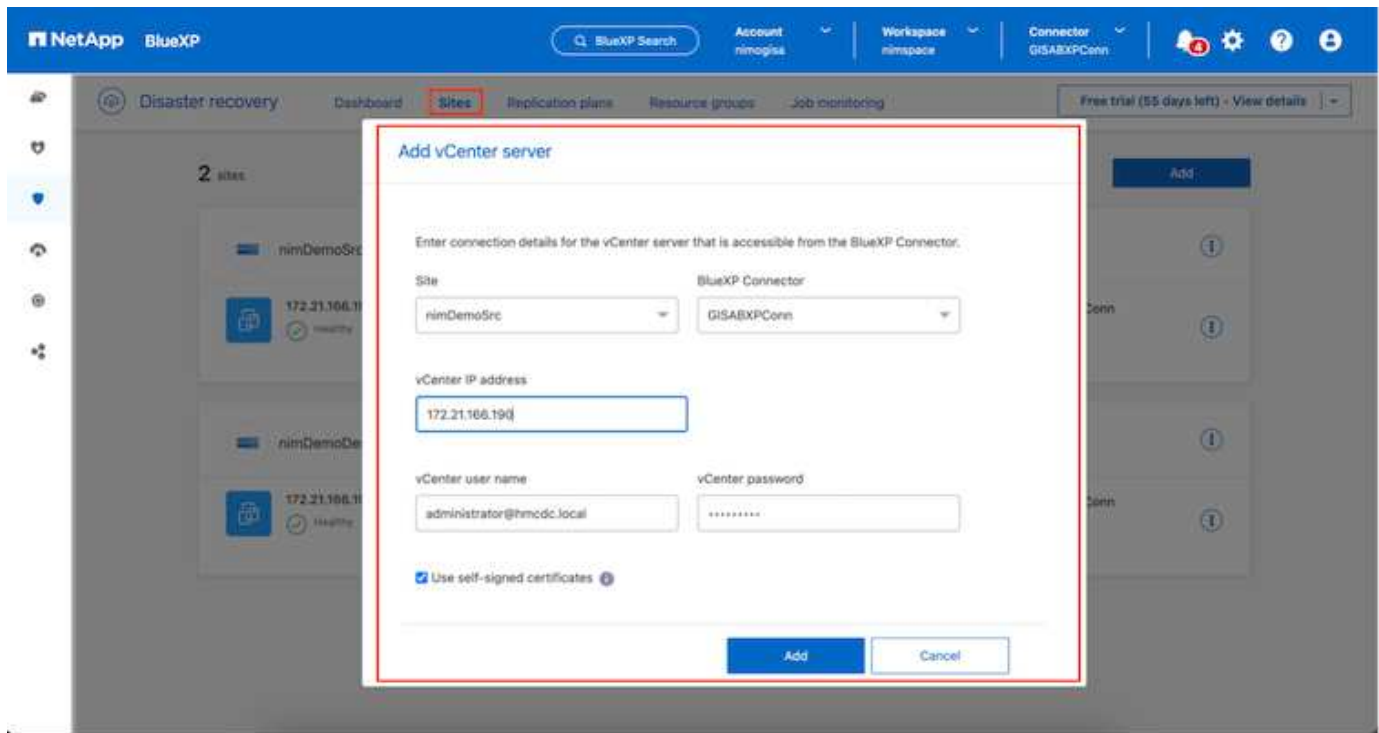


Aggiungere le seguenti piattaforme:

- **Fonte.** vCenter locale.



- **Destinazione.** VMC SDDC vCenter.



Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione tra il sito di origine e quello di destinazione

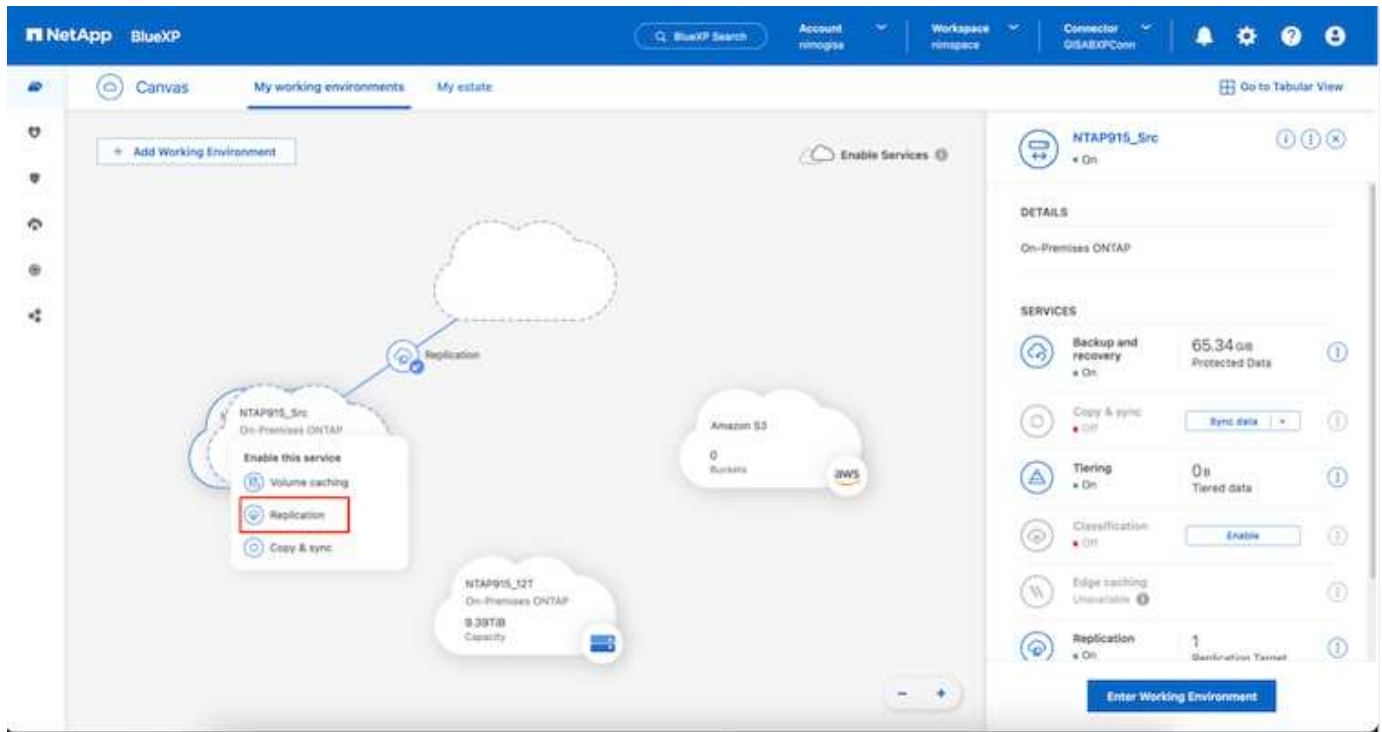
SnapMirror utilizza gli snapshot ONTAP per gestire il trasferimento dei dati da una posizione all'altra. Inizialmente, una copia completa basata su uno snapshot del volume di origine viene copiata sulla destinazione per eseguire una sincronizzazione di base. Quando si verificano modifiche ai dati all'origine, viene creato un nuovo snapshot e confrontato con lo snapshot di base. I blocchi che risultano modificati vengono quindi replicati nella destinazione, con lo snapshot più recente che diventa la baseline 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 uno stato di sola lettura online e quindi è ancora accessibile. SnapMirror funziona con blocchi fisici di archiviazione, anziché a livello di file o altro livello logico. Ciò significa che il volume di destinazione è una replica identica del volume di origine, inclusi snapshot, impostazioni del volume, ecc. Se il volume di origine utilizza funzionalità di efficienza dello spazio ONTAP, come la compressione dei dati e la deduplicazione dei dati, il volume replicato manterrà queste ottimizzazioni.

L'interruzione della relazione SnapMirror rende il volume di destinazione scrivibile e in genere viene utilizzato per eseguire un failover quando SnapMirror viene utilizzato per sincronizzare i dati in un ambiente DR. SnapMirror è sufficientemente sofisticato da consentire la risincronizzazione efficiente dei dati modificati nel sito di failover con il sistema primario, qualora questo dovesse tornare online in seguito, e quindi consentire il ripristino della relazione SnapMirror originale.

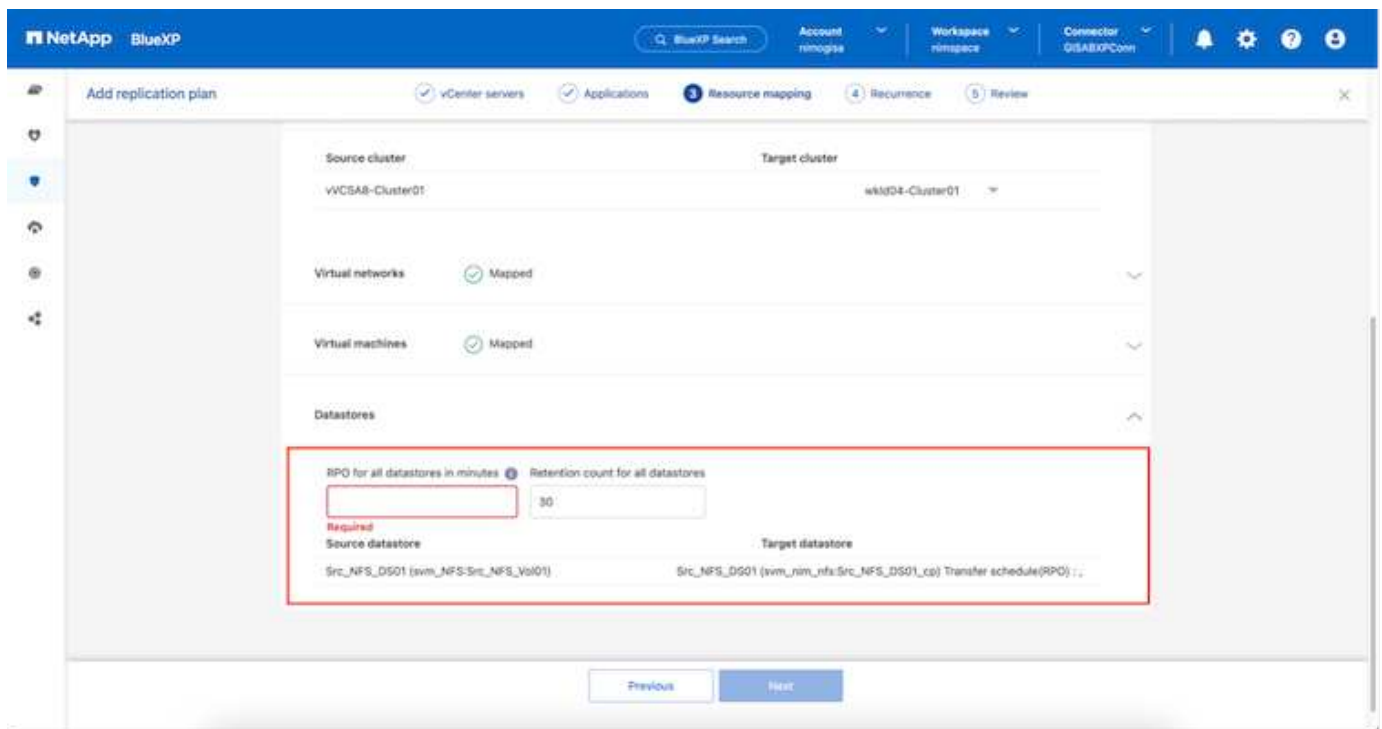
Come configurarlo per VMware Disaster Recovery

Il processo per creare una replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è sfruttare BlueXP per configurare la replica SnapMirror, utilizzando un semplice trascinamento del sistema ONTAP di origine nell'ambiente sulla destinazione per avviare la procedura guidata che guida attraverso il resto del processo.



BlueXP DRaaS può anche automatizzare la stessa operazione, a condizione che siano soddisfatti i due criteri seguenti:

- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.



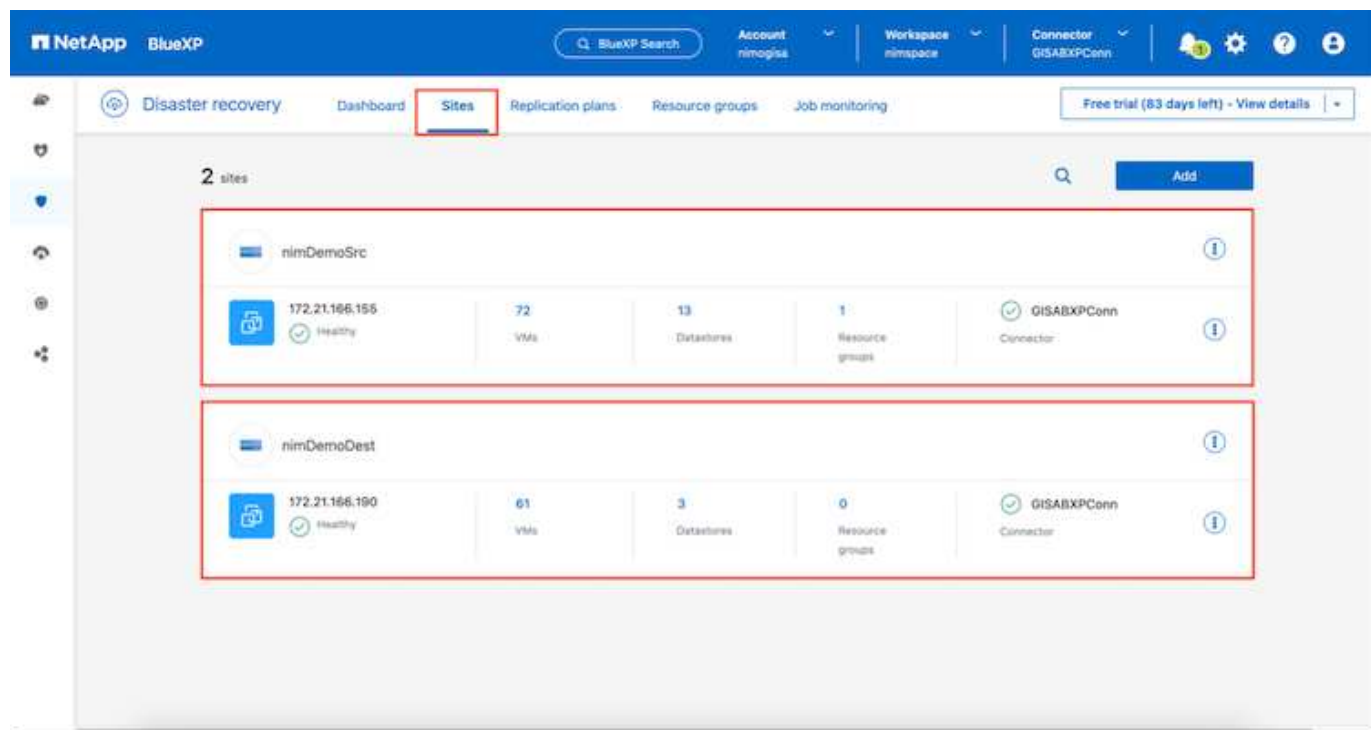
Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS rileva la relazione e continua con il resto delle operazioni del flusso di lavoro.



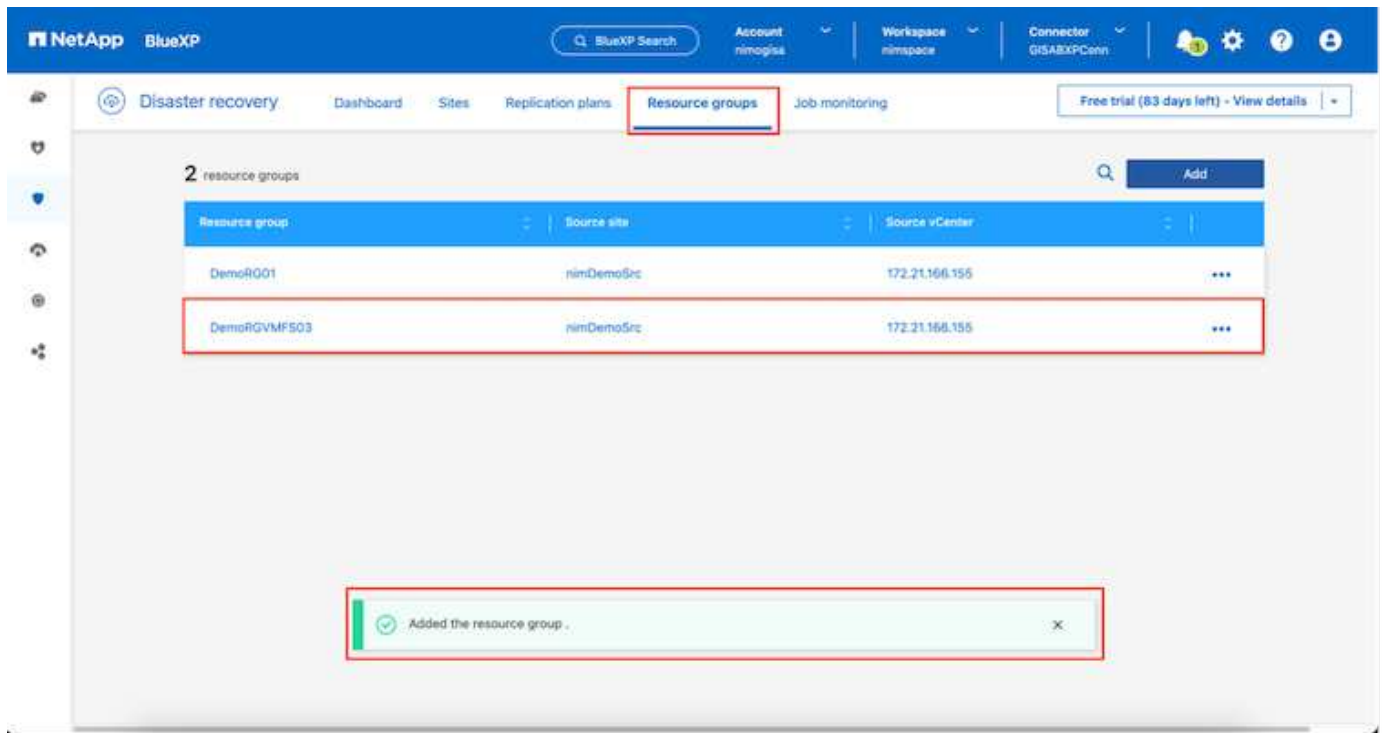
Oltre agli approcci sopra descritti, la replica SnapMirror può essere creata anche tramite ONTAP CLI o System Manager. Independentemente dall'approccio utilizzato per sincronizzare i dati tramite SnapMirror, BlueXP DRaaS orchestra il flusso di lavoro per operazioni di disaster recovery efficienti e senza interruzioni.

Cosa può fare per te il BlueXP disaster recovery ?

Dopo aver aggiunto i siti di origine e di destinazione, il BlueXP disaster recovery esegue automaticamente un'analisi approfondita e visualizza le VM insieme ai metadati associati. Il BlueXP disaster recovery rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle VM e li popola.

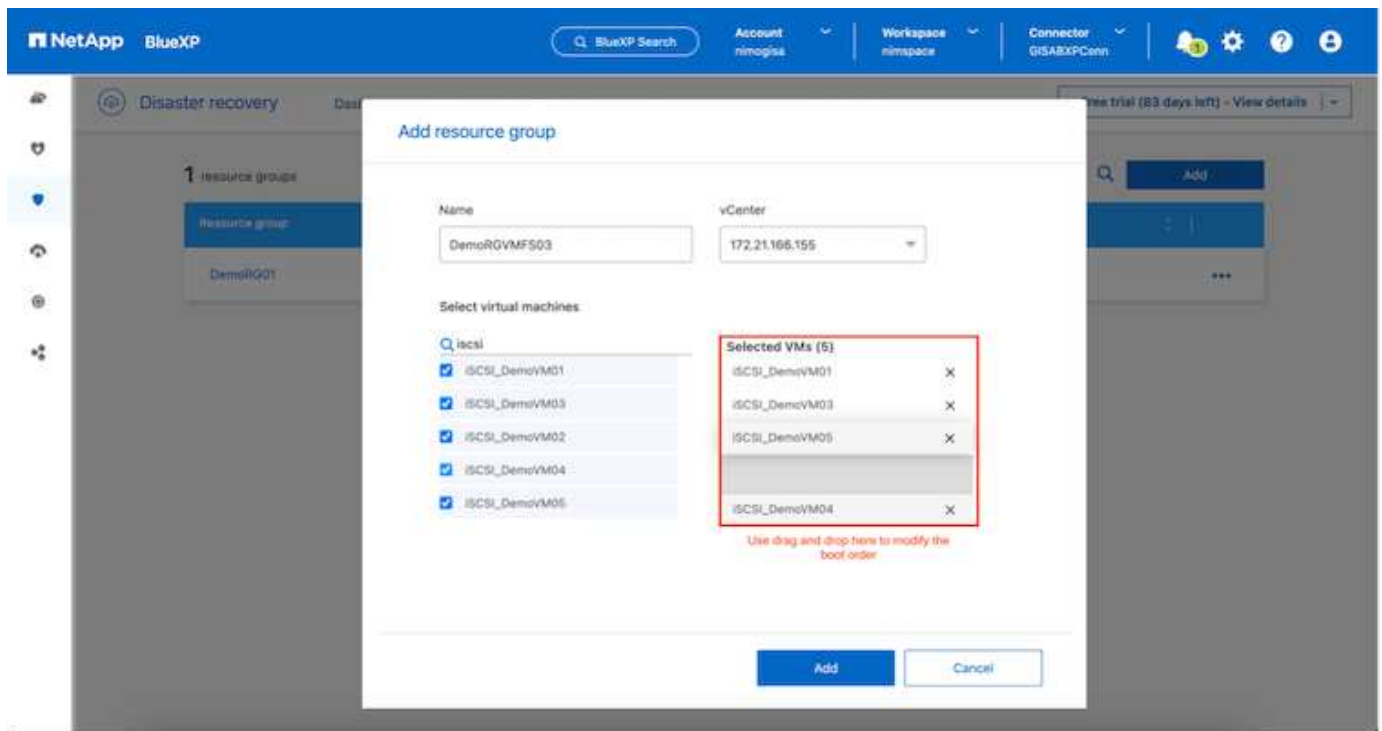


Dopo aver aggiunto i siti, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse BlueXP disaster recovery consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti al momento del ripristino. Per iniziare a creare gruppi di risorse, vai su **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.

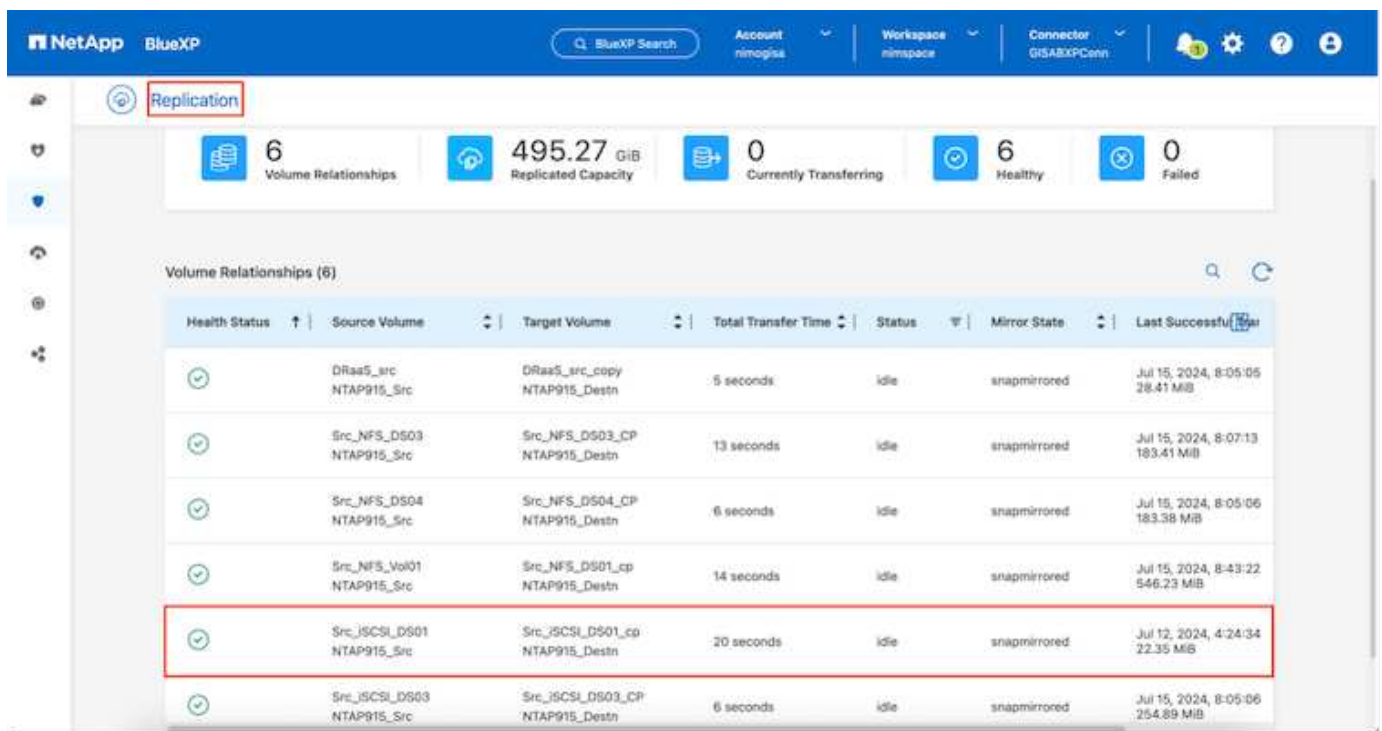
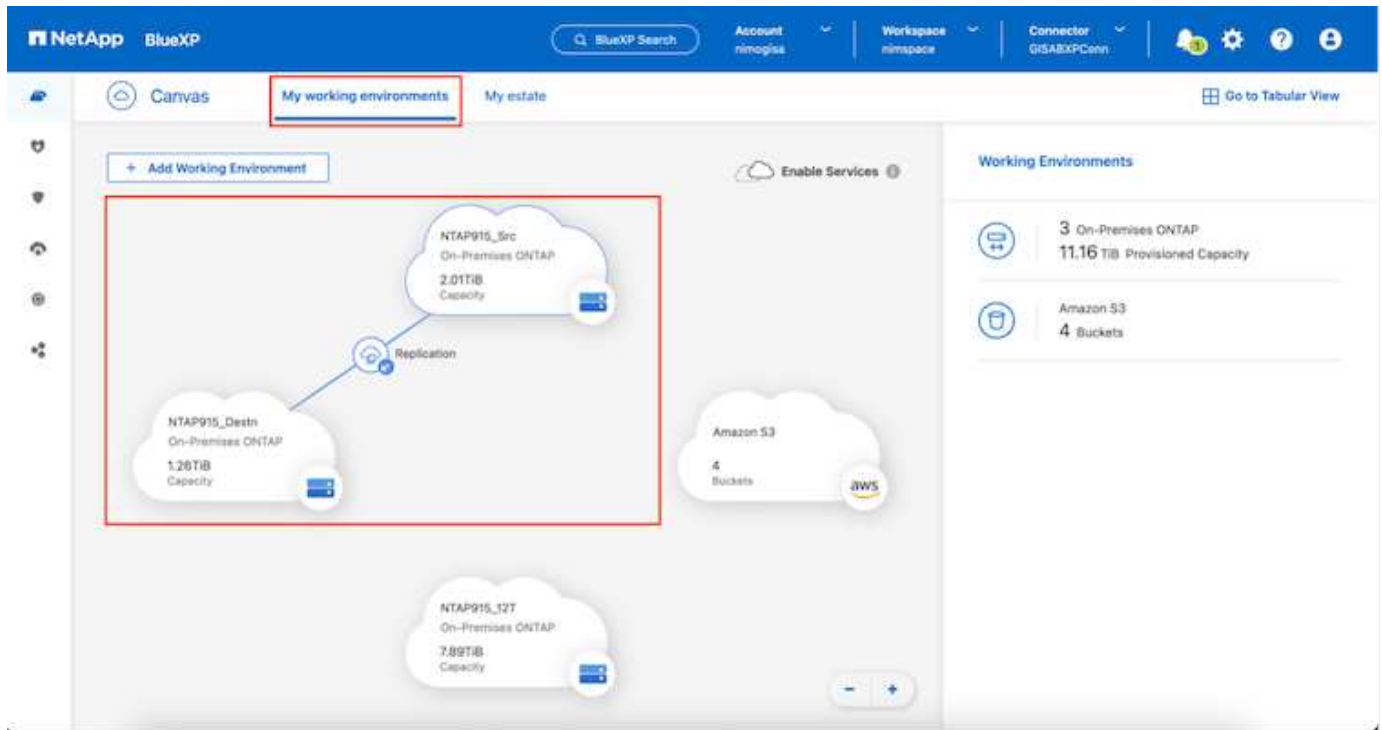


Il gruppo di risorse può essere creato anche durante la creazione di un piano di replica.

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

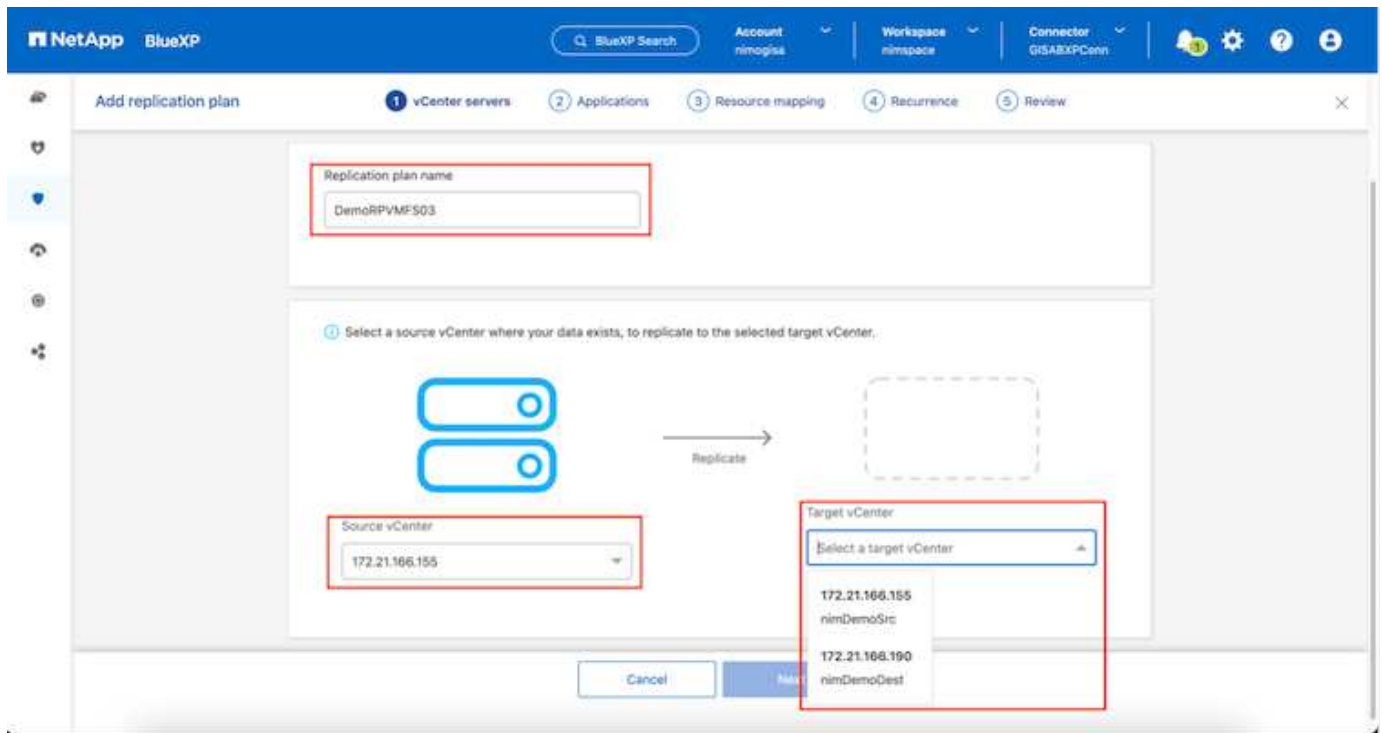


Una volta creati i gruppi di risorse, il passaggio successivo consiste nel creare il progetto di esecuzione o un piano per ripristinare macchine virtuali e applicazioni in caso di disastro. Come indicato nei prerequisiti, la replica SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.

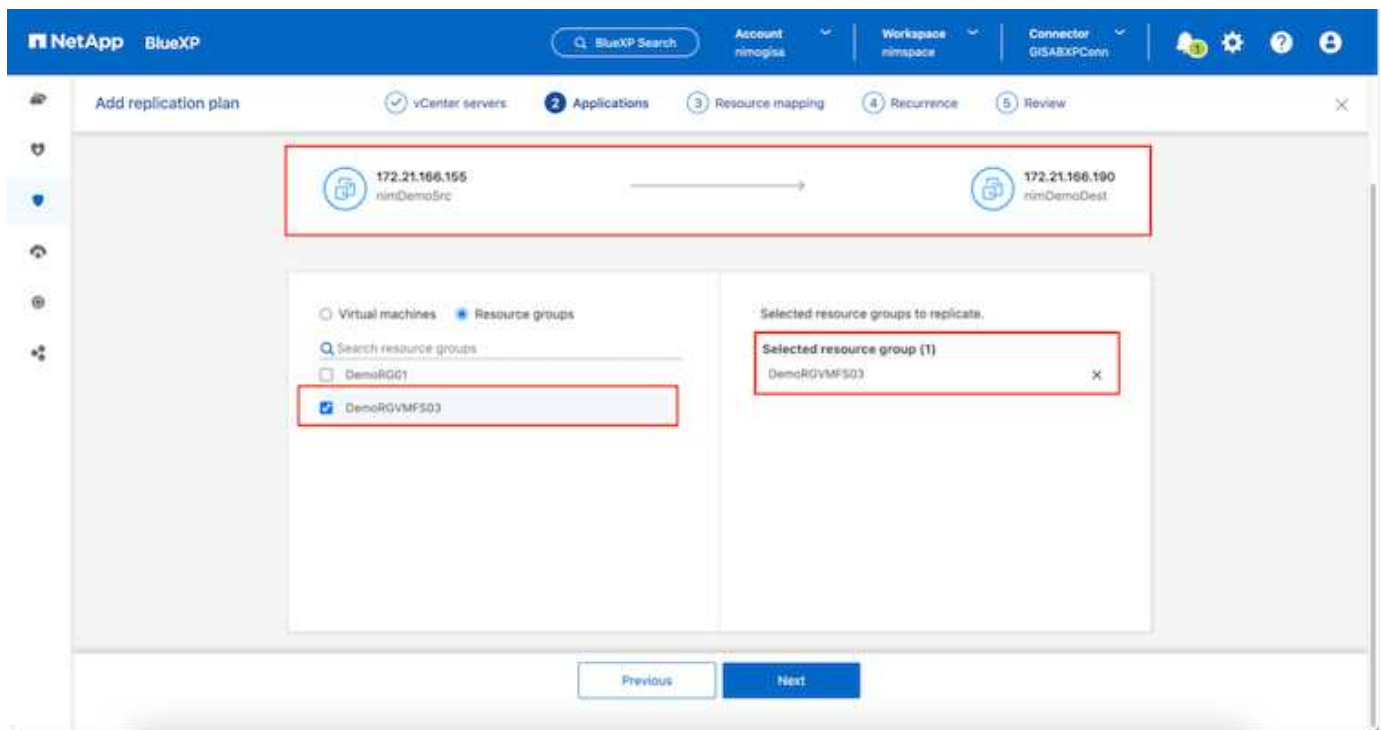


Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire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

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.



Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono essere ripristinate le macchine virtuali delle applicazioni.

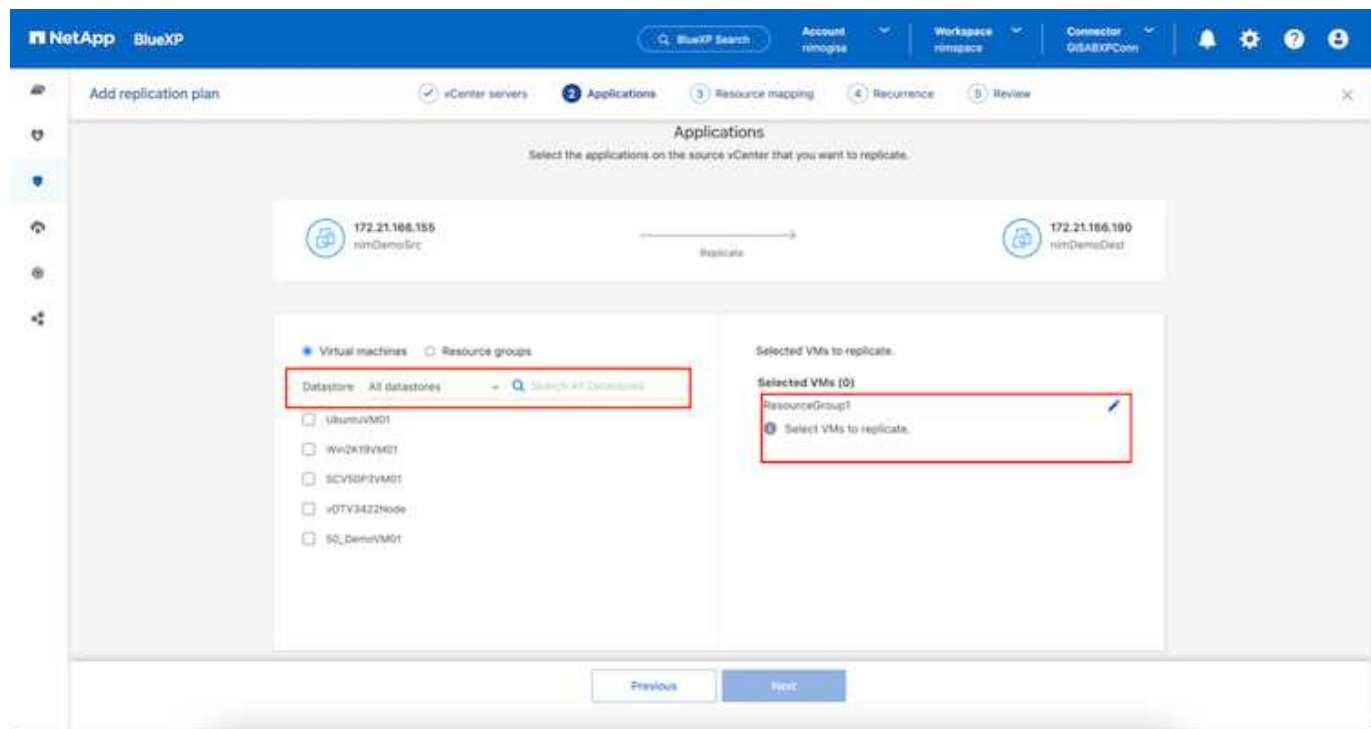


Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.



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

La schermata seguente mostra l'opzione per filtrare macchine virtuali o datastore specifici in base ai requisiti organizzativi se i gruppi di risorse non sono stati creati in precedenza.



Una volta selezionati i gruppi di risorse, creare i mapping di failover. In questo passaggio, specificare come le risorse dall'ambiente di origine vengono mappate alla destinazione. Ciò include risorse di elaborazione e reti virtuali. Personalizzazione IP, pre- e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento a ["Creare un piano di replicazione"](#).

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

| Source VM | CPU | RAM | Boot delay (mins between 0 and 10) | Create application consistent replicas | Scripts |
|-------------|-----|-------|------------------------------------|--|---------|
| DemoR001 | | | | | |
| S0_DemoVM | 2 | 4 GiB | 0 | <input type="checkbox"/> | None |
| S0_DemoVM01 | 2 | 4 GiB | 0 | <input type="checkbox"/> | None |
| S0_DemoVM02 | 2 | 4 GiB | 0 | <input type="checkbox"/> | None |

Previous Next



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 Mappatura test dopo aver deselezionato la casella di controllo come mostrato di seguito:

Resource mapping

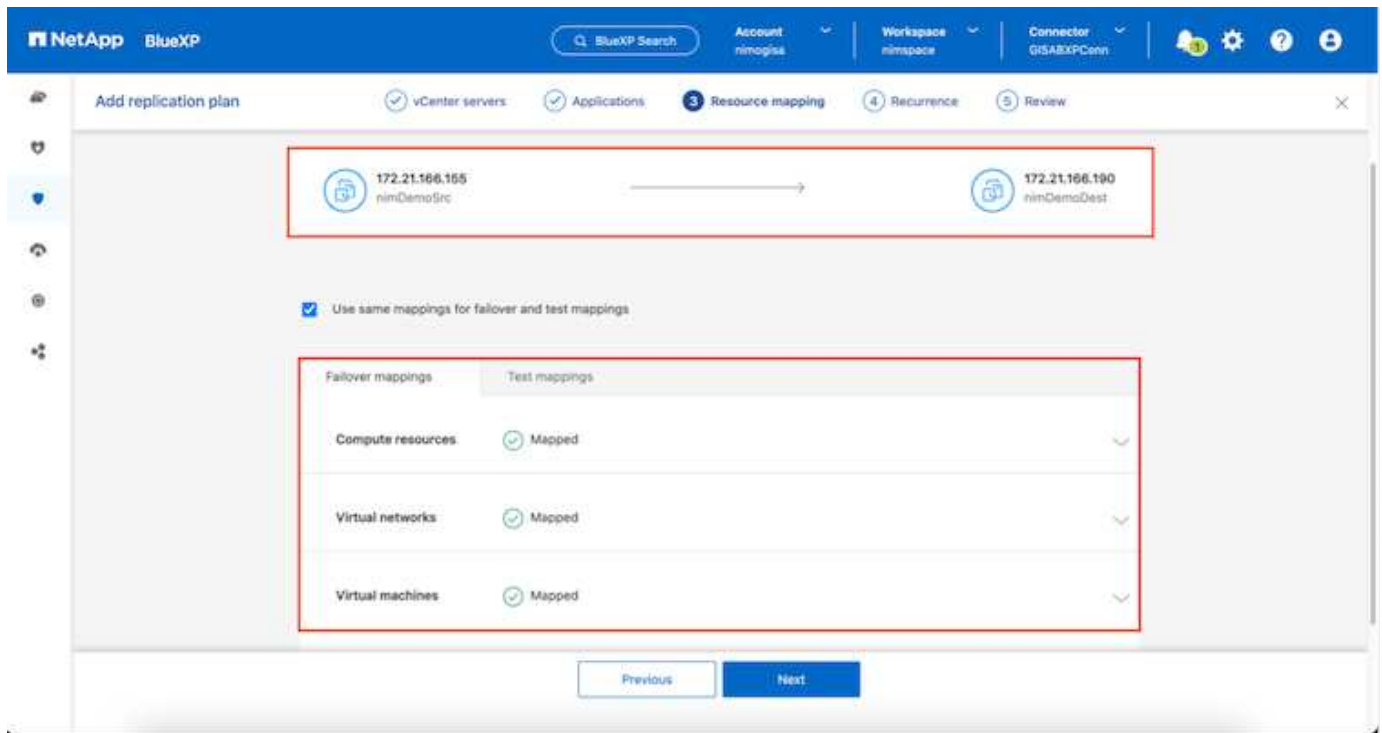
Specify how resources map from the source to the target.

172.21.166.155 nrmDemoSrc → 172.21.166.190 nrmDemoDest

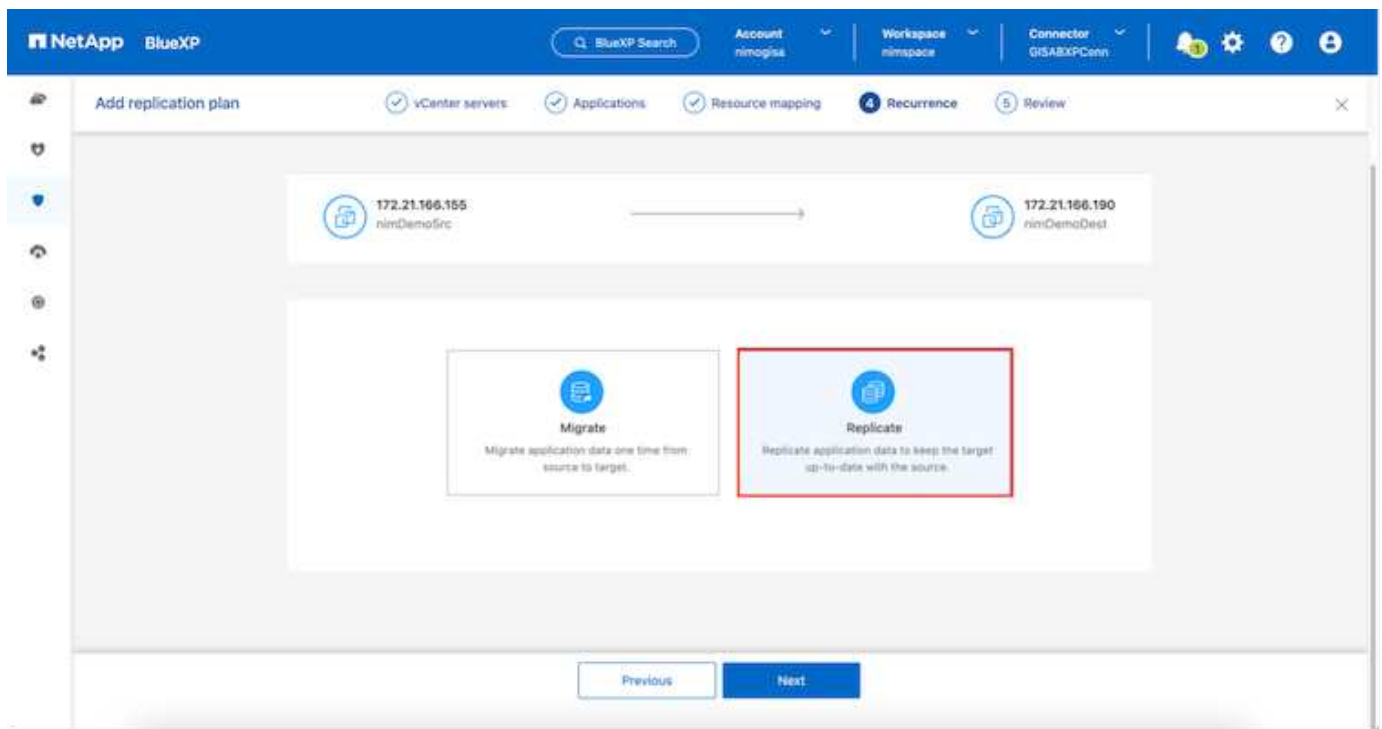
☒ Use same mappings for failover and test mappings

Failover mappings Test mappings

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



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



Una volta fatto, rivedi le mappature create e poi fai clic su Aggiungi piano.

NetApp BlueXP

BlueXP Search | Account nimoglia | Workspace nimspace | Connector GISABXPCConn

Add replication plan | vCenter servers | Applications | Resource mapping | Recurrence | **5 Review**

172.21.166.155
nimDemoSrc

Replicate

172.21.166.190
nimDemoDest

Plan details | Failover mapping | Virtual machines

Plan name: DemoRPMVF503

Recurrence: Replicate

Previous | **Add plan**

NetApp BlueXP

BlueXP Search | Account nimoglia | Workspace nimspace | Connector GISABXPCConn

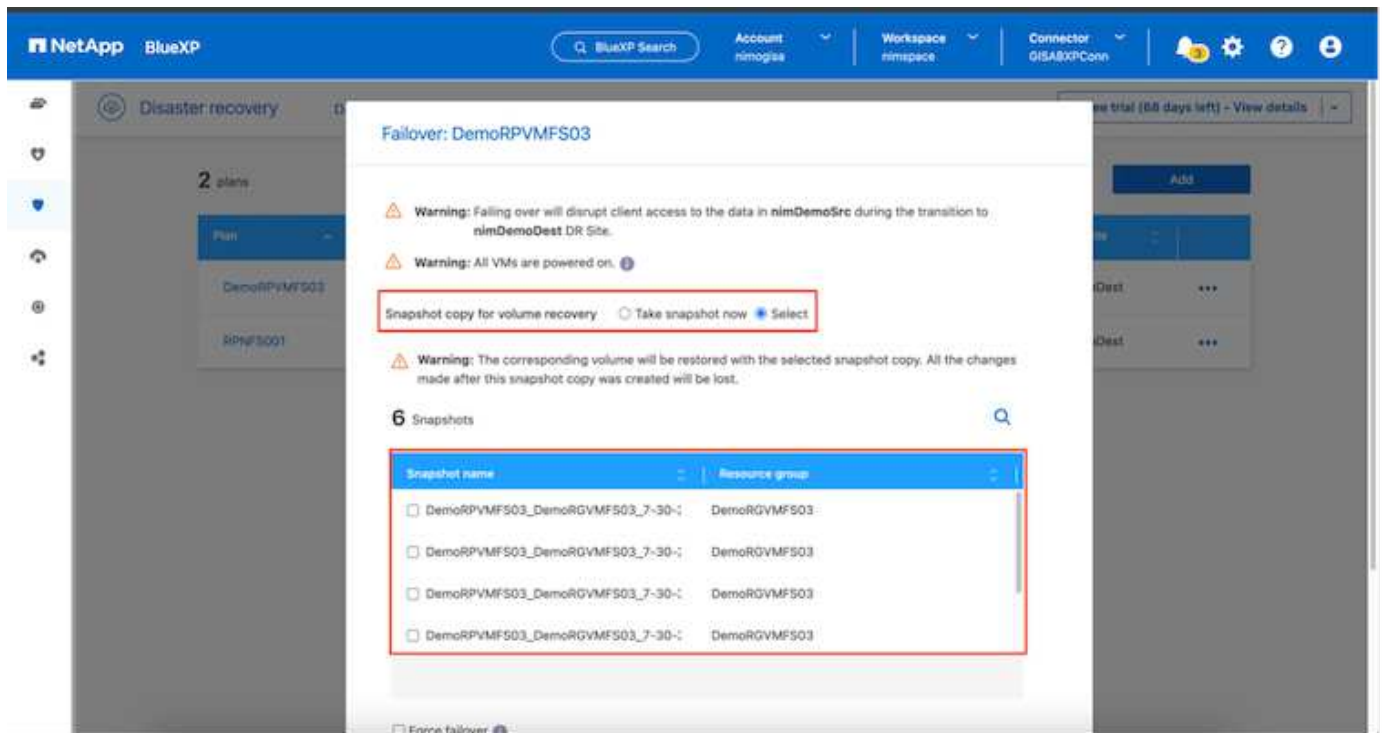
Disaster recovery | Dashboard | Sites | **Replication plans** | Resource groups | Job monitoring

Free trial (83 days left) - View details

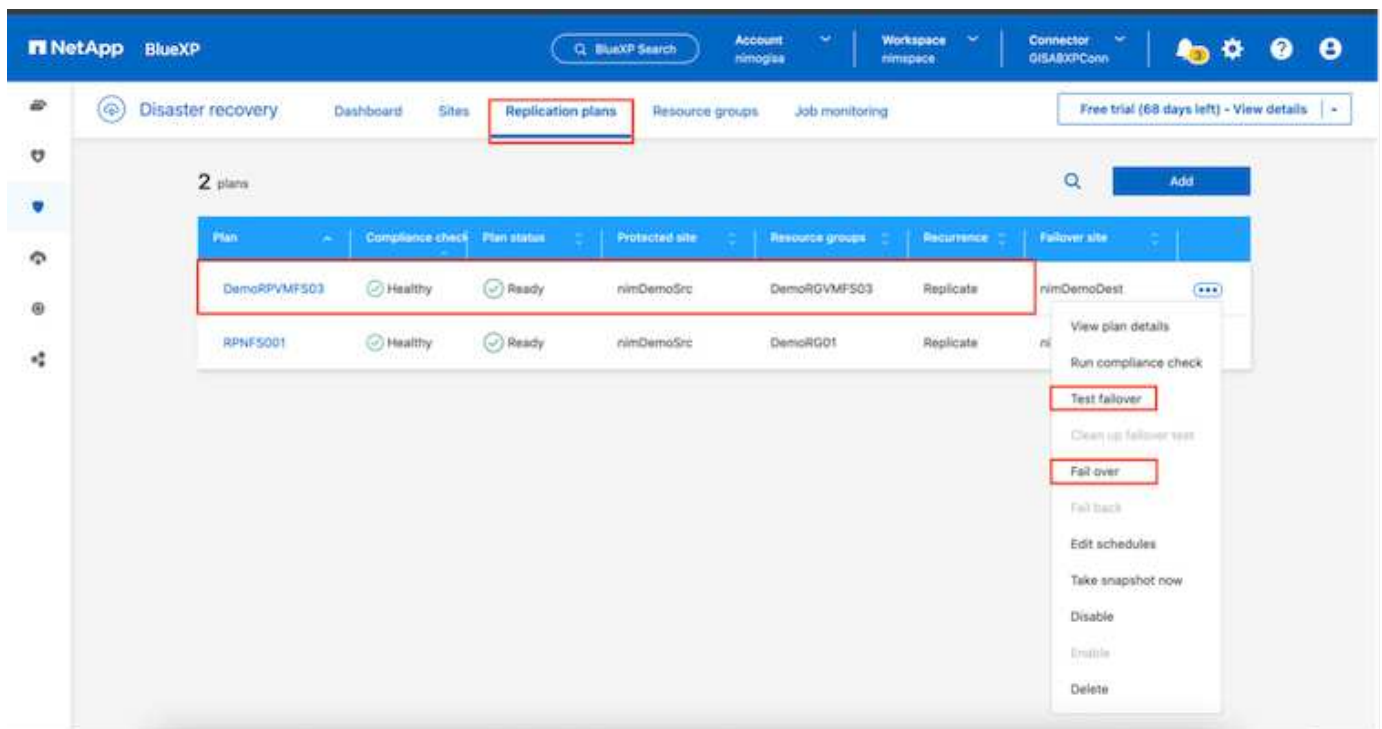
2 plans

| Plan | Compliance check | Plan status | Protected site | Resource groups | Recurrence | Failover site | |
|--------------|------------------|-------------|----------------|-----------------|------------|---------------|-----|
| DemoRPMVF503 | Healthy | Ready | nimDemoSrc | DemoRGMVF503 | Replicate | nimDemoDest | ... |
| RPHFS001 | Healthy | Ready | nimDemoSrc | DemoRG01 | Replicate | nimDemoDest | ... |

Una volta creato il piano di replicazione, è possibile eseguire il failover a seconda dei requisiti selezionando l'opzione failover, l'opzione test-failover o l'opzione migrate. Il BlueXP disaster recovery garantisce che il processo di replicazione venga eseguito secondo il 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 di un determinato momento (in base ai criteri di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile in caso di un evento di corruzione come un ransomware, in cui le repliche più recenti sono già compromesse o crittografate. Il BlueXP disaster recovery mostra tutti i punti di ripristino disponibili.



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



Cosa succede durante un'operazione di failover o di test failover?

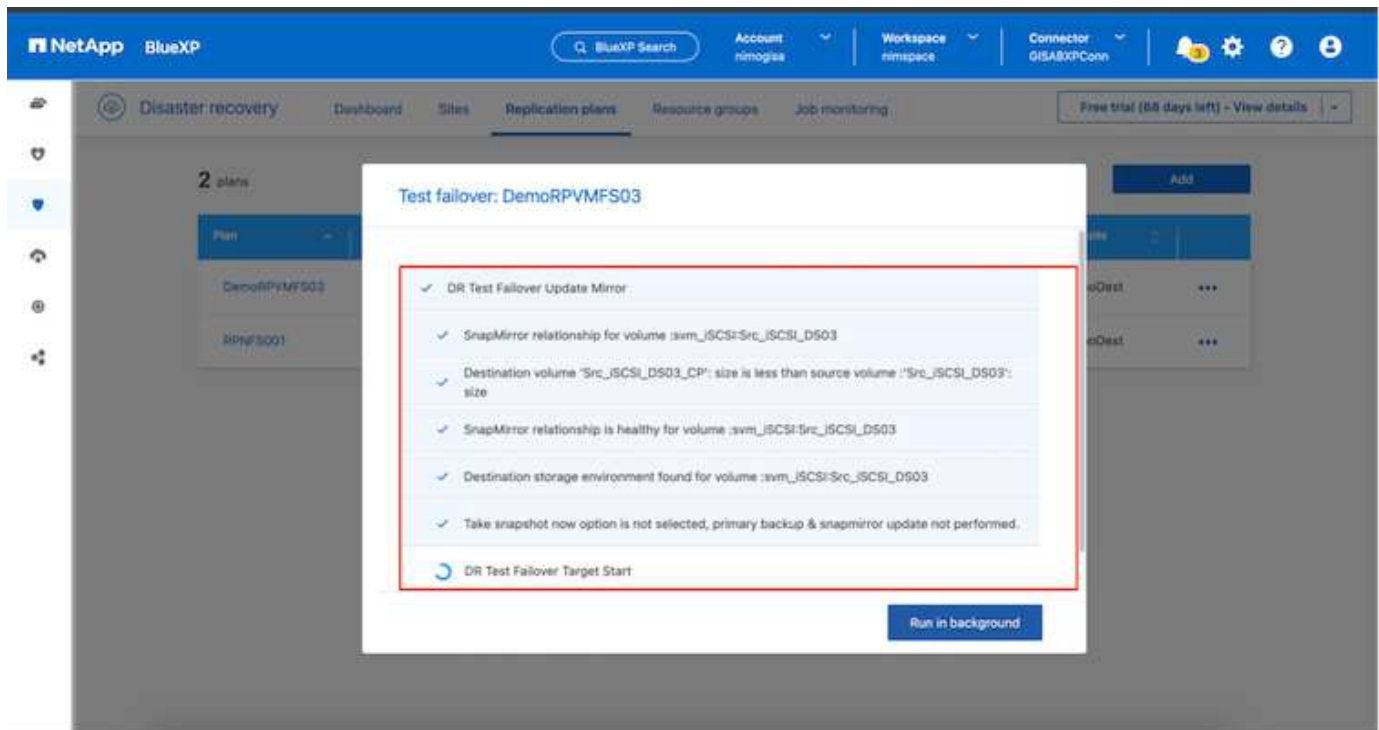
Durante un'operazione di failover di prova, il BlueXP disaster recovery crea un volume FlexClone sul sistema di archiviazione ONTAP di destinazione utilizzando la copia Snapshot più recente o uno snapshot selezionato del volume di destinazione.



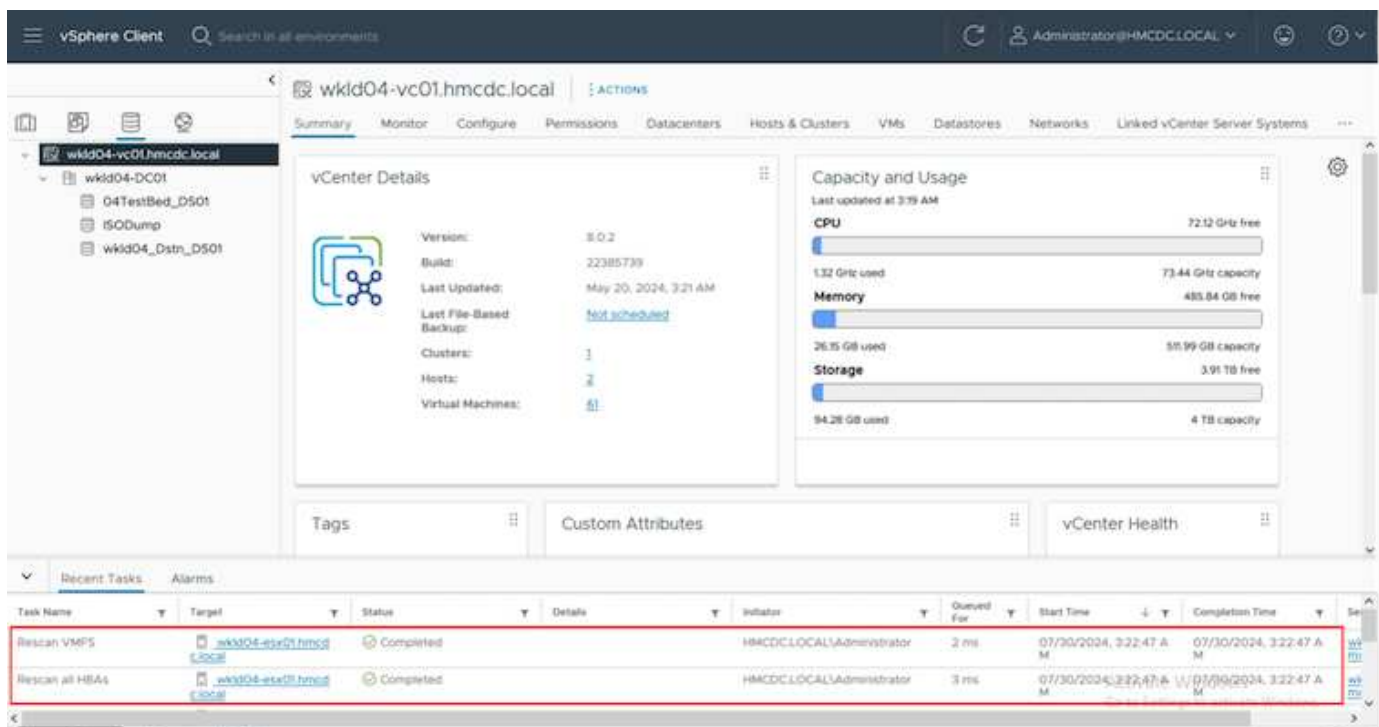
Un'operazione di failover di prova crea un volume clonato sul sistema di archiviazione ONTAP di destinazione.

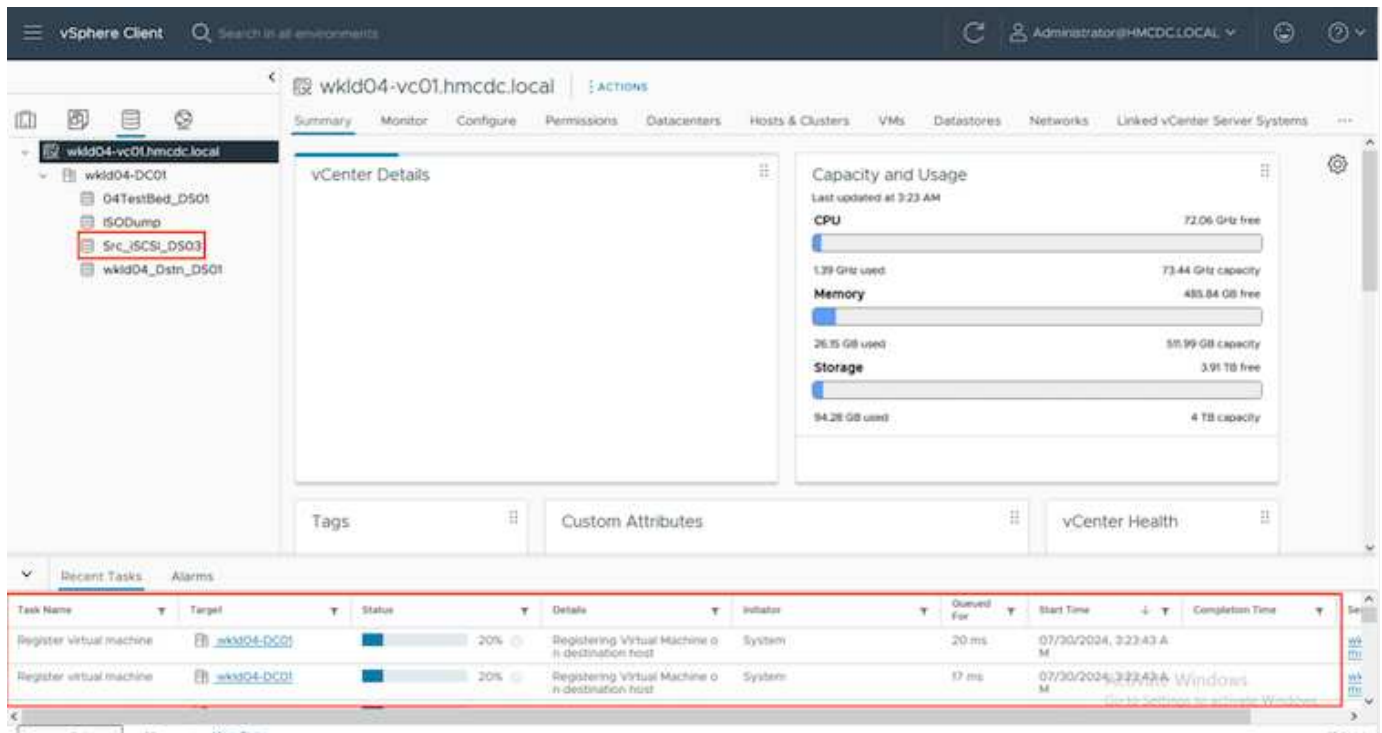


L'esecuzione di un'operazione di ripristino di prova non influisce sulla replica SnapMirror .



Durante il processo, il BlueXP disaster recovery non mappa il volume di destinazione originale. Al contrario, crea un nuovo volume FlexClone dallo Snapshot selezionato e un datastore temporaneo che supporta il volume FlexClone viene mappato sugli host ESXi.

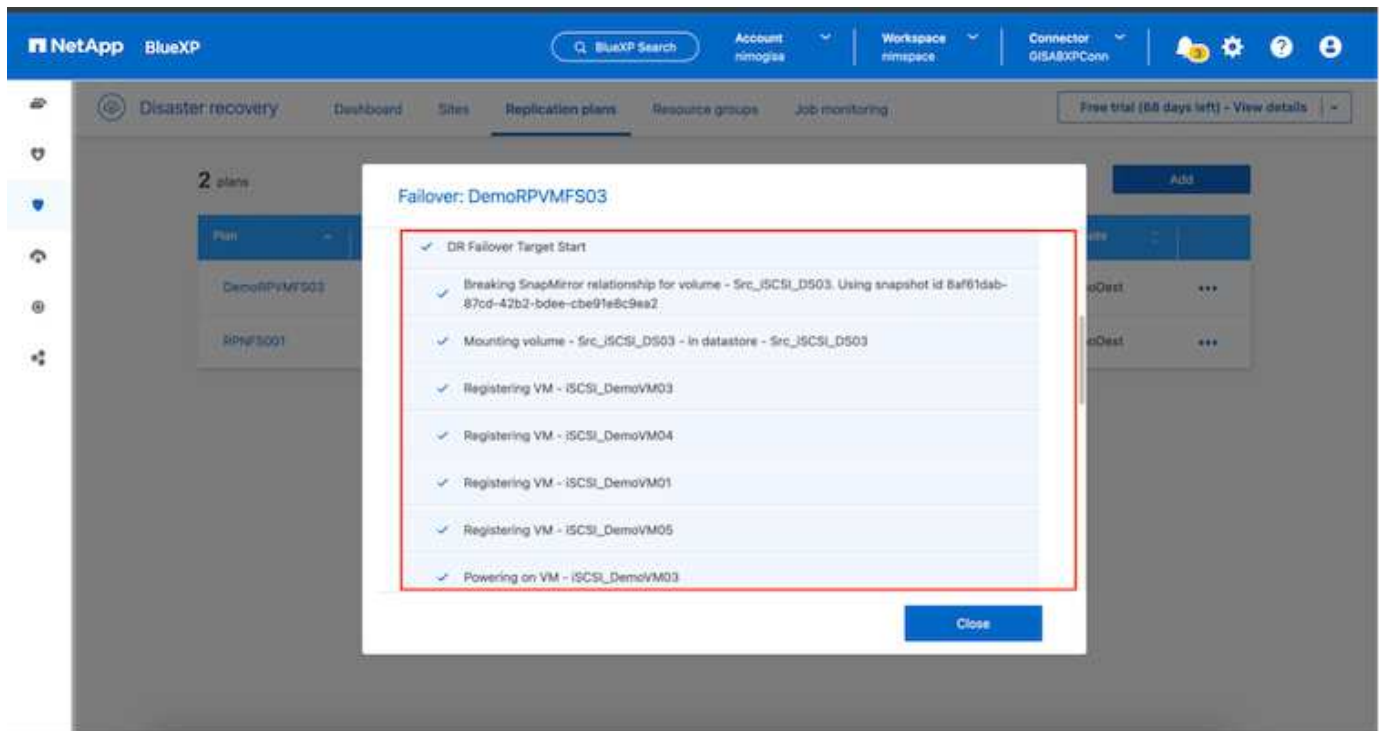




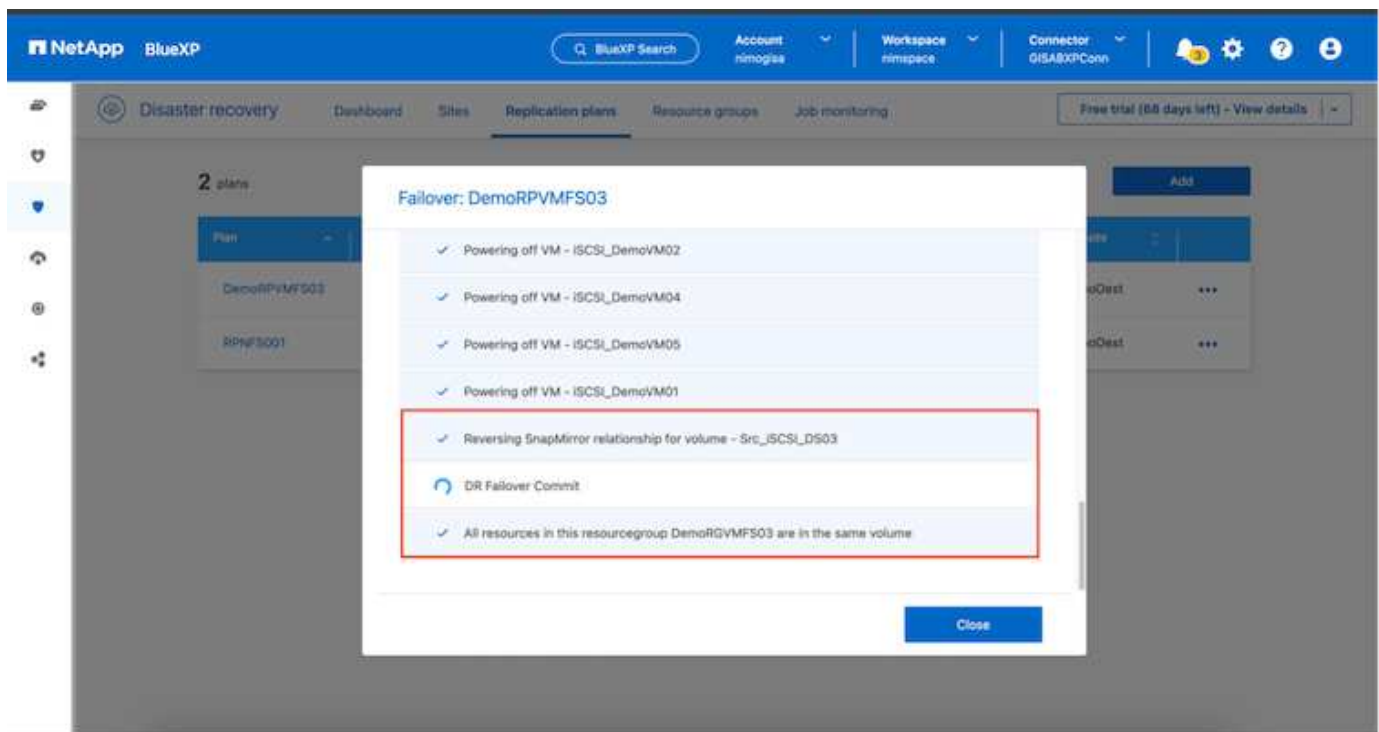
Una volta completata l'operazione di failover di prova, è possibile avviare l'operazione di pulizia utilizzando **"Clean Up failover test"**. Durante questa operazione, il BlueXP disaster recovery distrugge il volume FlexClone utilizzato nell'operazione.

In caso di un vero disastro, il BlueXP disaster recovery esegue i seguenti passaggi:

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

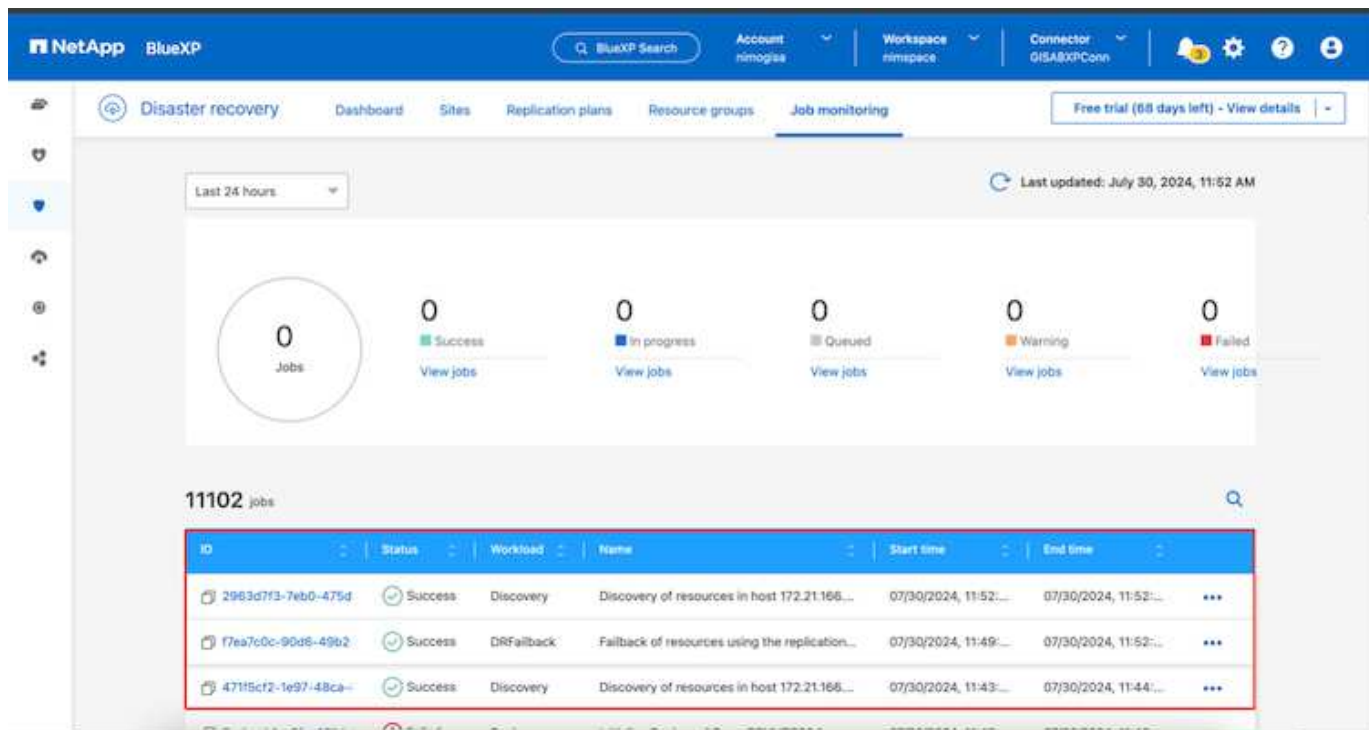


Una volta che il sito primario è attivo e funzionante, il BlueXP disaster recovery consente la risincronizzazione inversa per SnapMirror e abilita il failback, che può essere eseguito con un semplice clic.



Se si sceglie l'opzione di migrazione, questa viene considerata un evento di failover pianificato. In questo caso, viene attivato un ulteriore passaggio che consiste nello spegnimento delle macchine virtuali nel sito di origine. Il resto dei passaggi rimane lo stesso dell'evento di failover.

Da BlueXP o dalla CLI ONTAP è possibile monitorare lo stato di integrità della replica per i volumi del datastore appropriati, mentre lo stato di un failover o di un failover di prova può essere monitorato tramite Job Monitoring.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, sentiti libero di seguire il video dettagliato o di utilizzare il "[simulatore di soluzioni](#)".

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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