



Dr con BlueXP DRaaS

NetApp Solutions

NetApp
August 24, 2024

Sommario

- Dr con BlueXP DRaaS 1
- Panoramica 1
- Dr utilizzando BlueXP DRaaS per datastore NFS 1
- Dr utilizzando BlueXP DRaaS per archivi dati VMFS 22

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"](#)

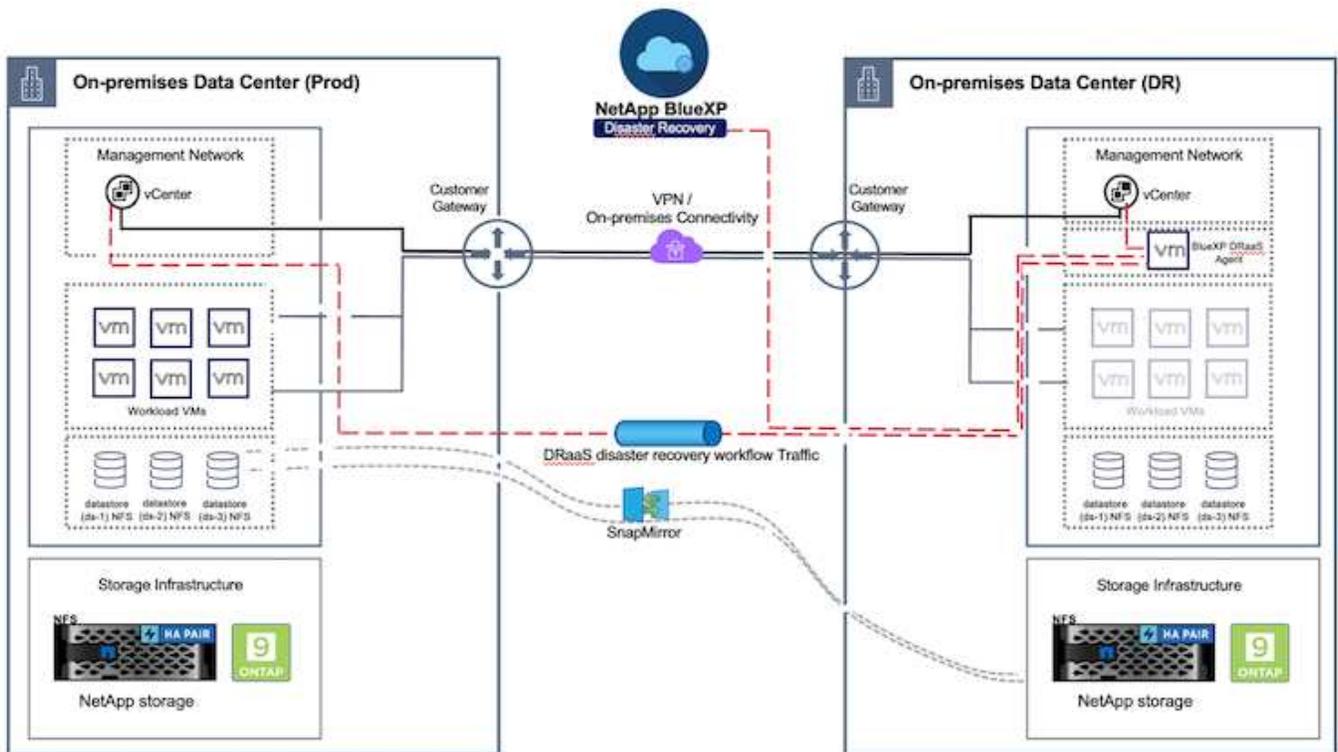
Dr utilizzando BlueXP DRaaS per datastore NFS

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.

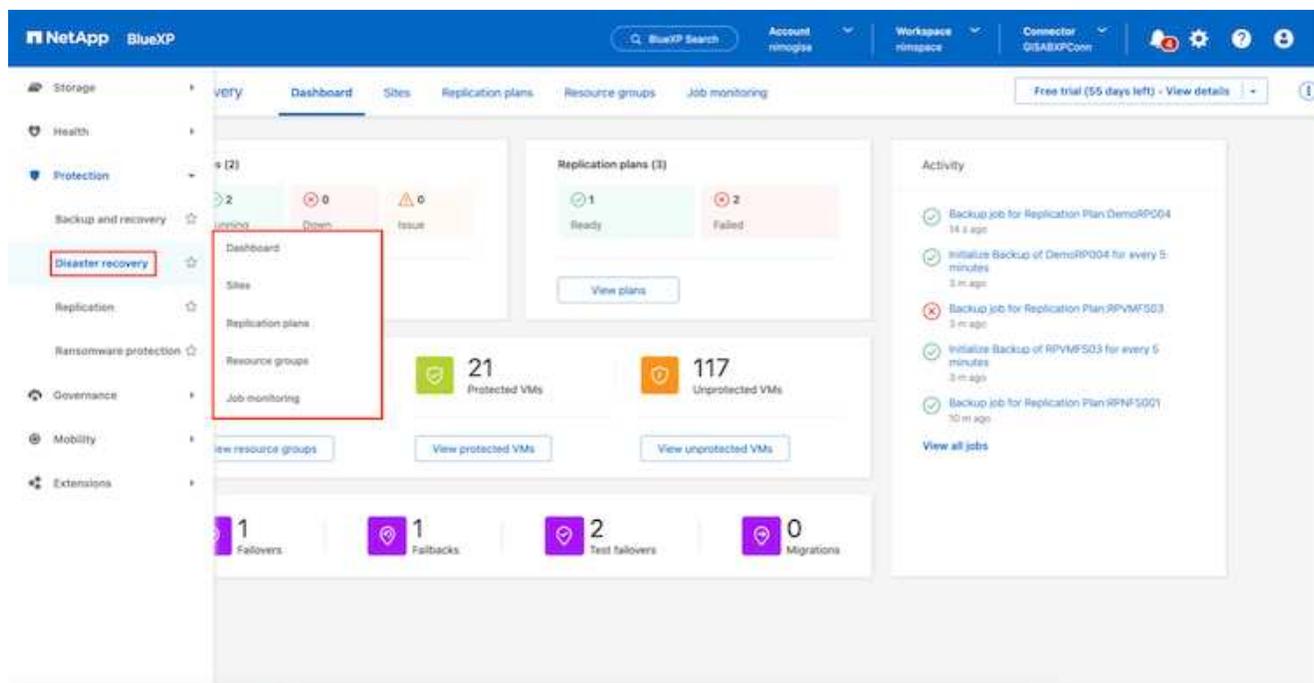


Per iniziare

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 .



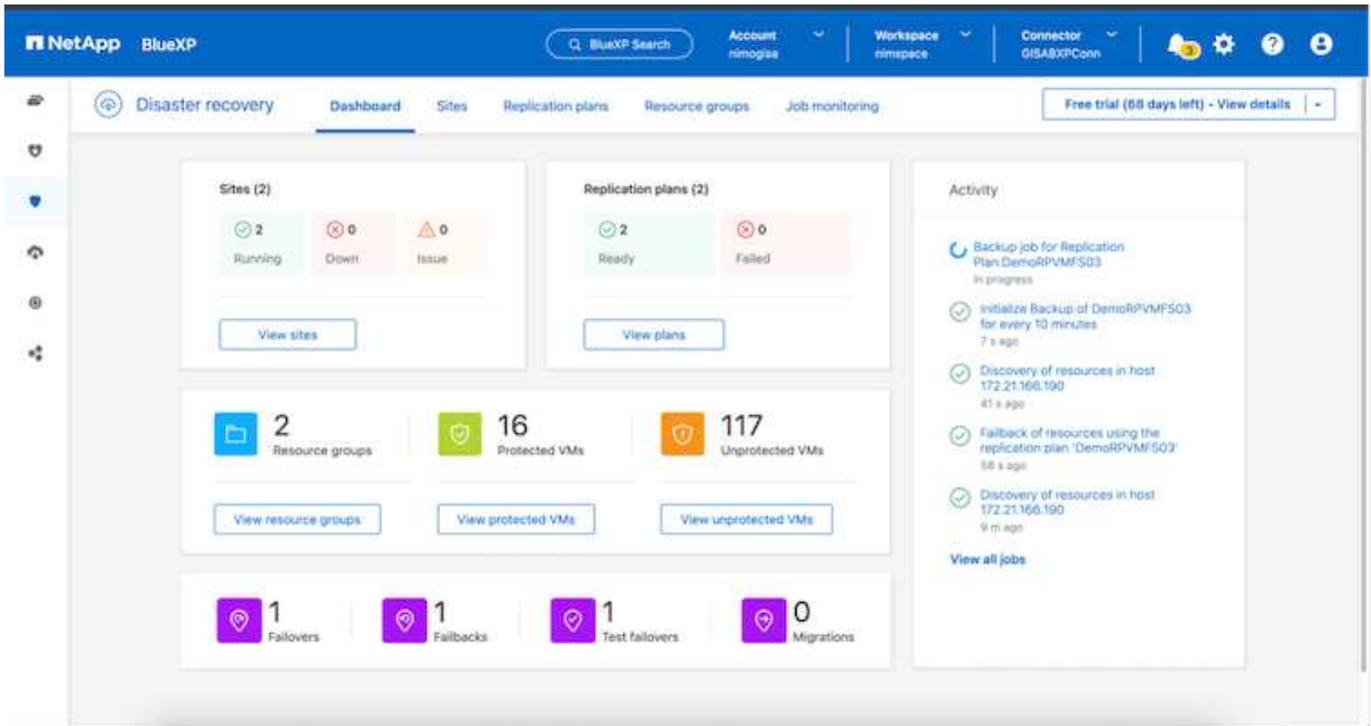
Prima di configurare il piano di disaster recovery, verificare che siano soddisfatti i seguenti prerequisiti:

- 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.



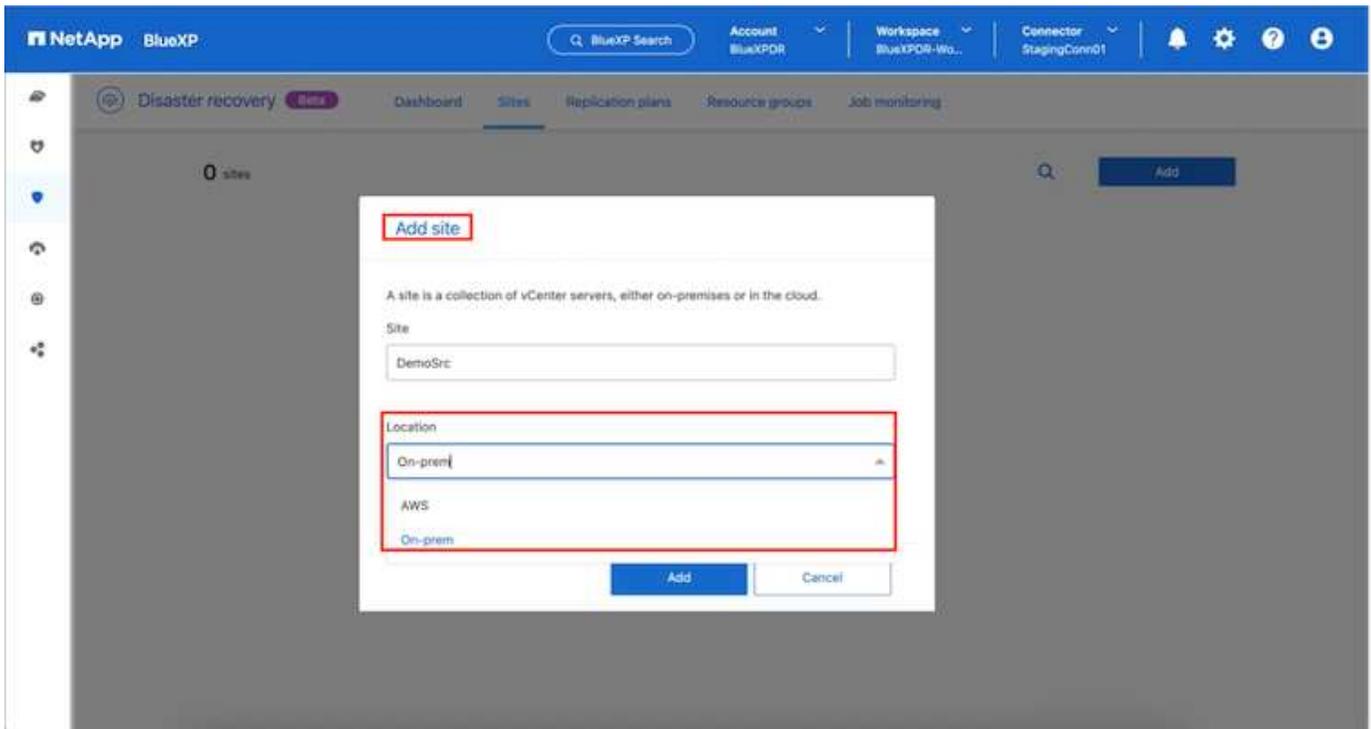
NetApp consiglia di implementare BlueXP Connector nel sito di destinazione o in un terzo sito, in modo che BlueXP Connector possa comunicare attraverso la rete con le risorse di origine e di destinazione.



Configurazione del disaster recovery BlueXP

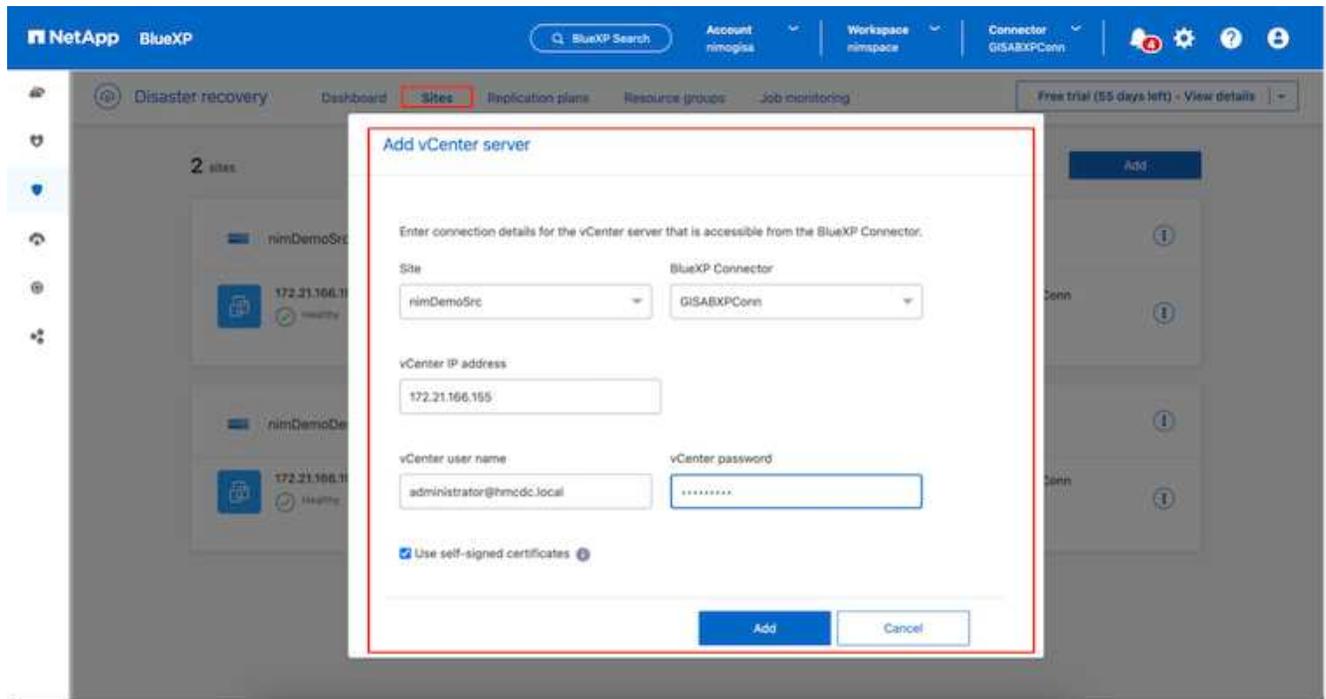
Il primo passo per prepararsi al disaster recovery è il rilevamento e l'aggiunta delle risorse di storage e vCenter on-premise al disaster recovery di BlueXP.

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**.

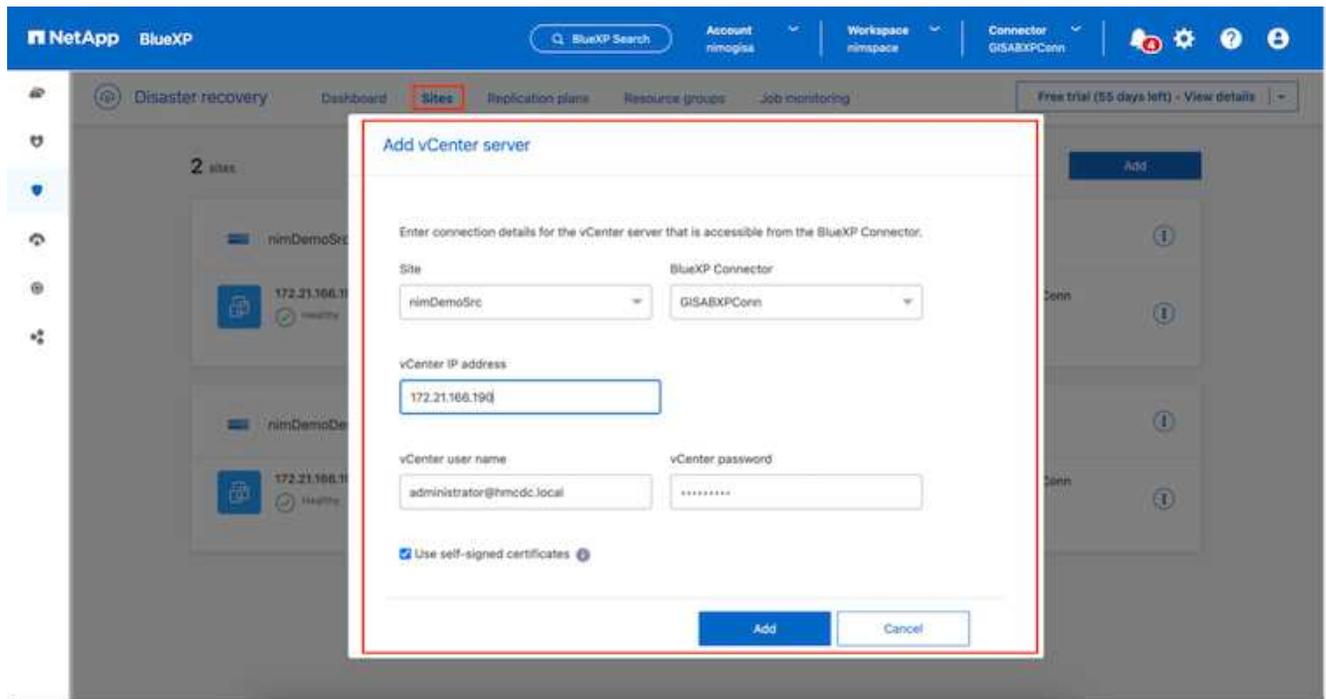


Aggiungere le seguenti piattaforme:

- **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.

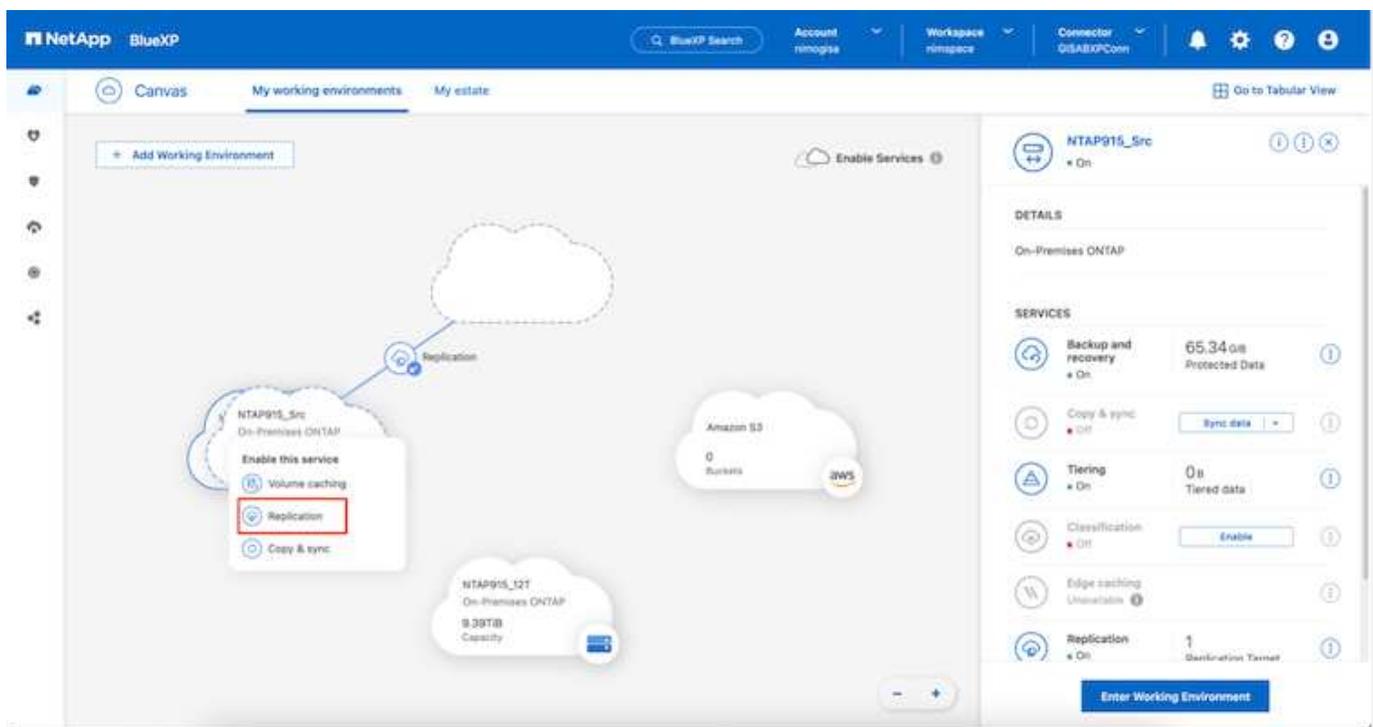
Per i casi in cui lo storage primario non viene completamente perso, SnapMirror fornisce un metodo efficiente per la risincronizzazione dei siti primario e di DR. SnapMirror può risincronizzare i due siti, trasferendo solo i dati modificati o nuovi al sito primario dal sito di DR, semplicemente invertendo 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.

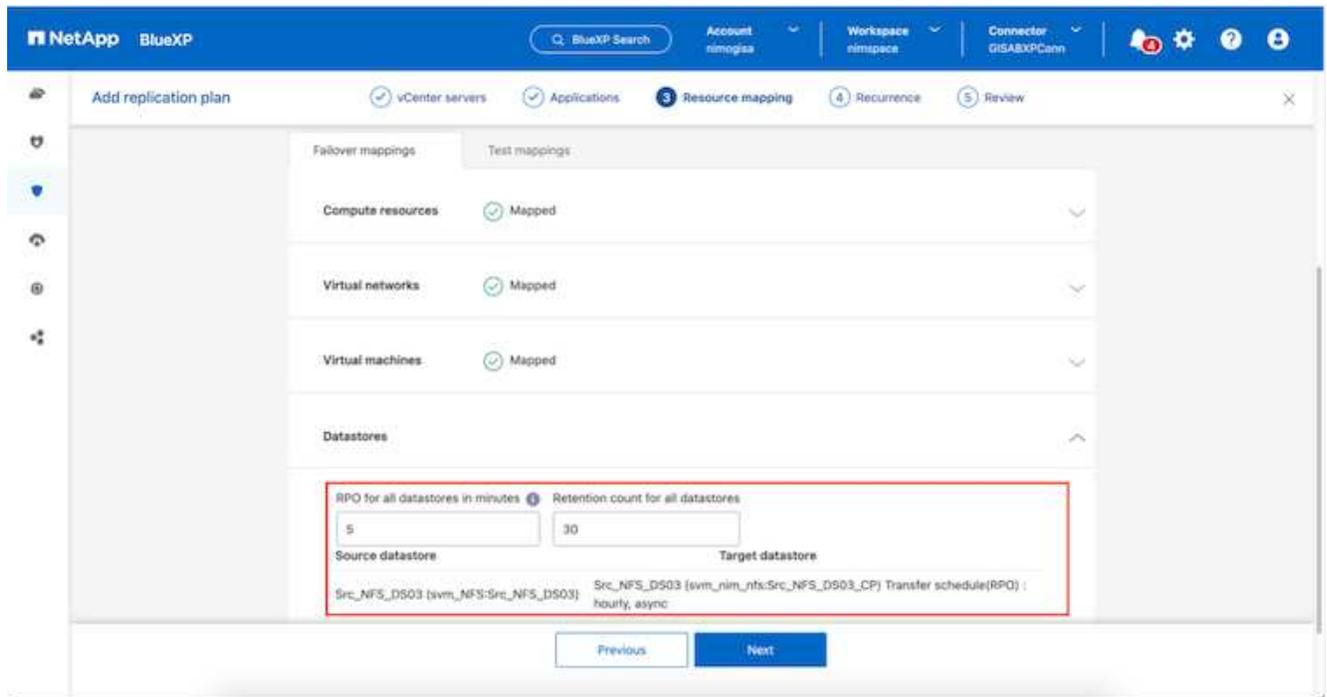
Come configurarlo per il Disaster Recovery VMware

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:

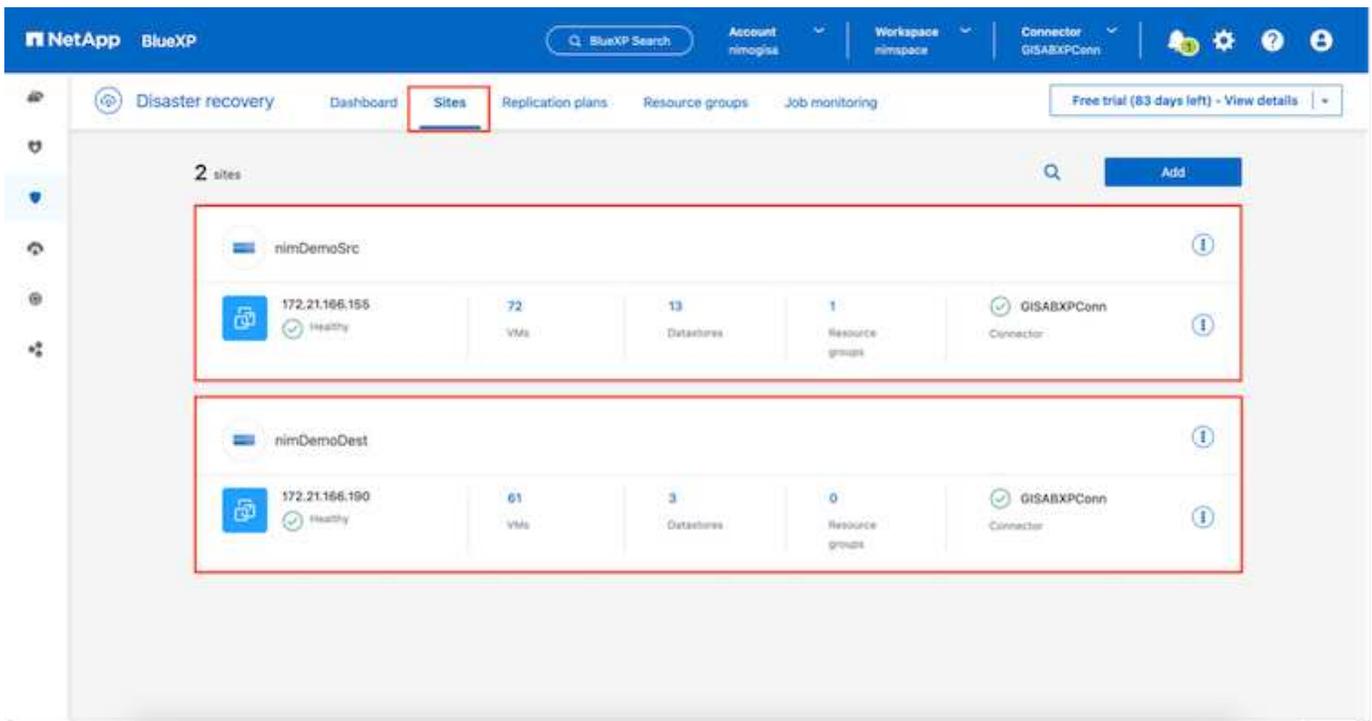
- I cluster di origine e di destinazione hanno una relazione peer.
- La SVM di origine e la SVM di destinazione hanno una relazione di tipo peer.



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.

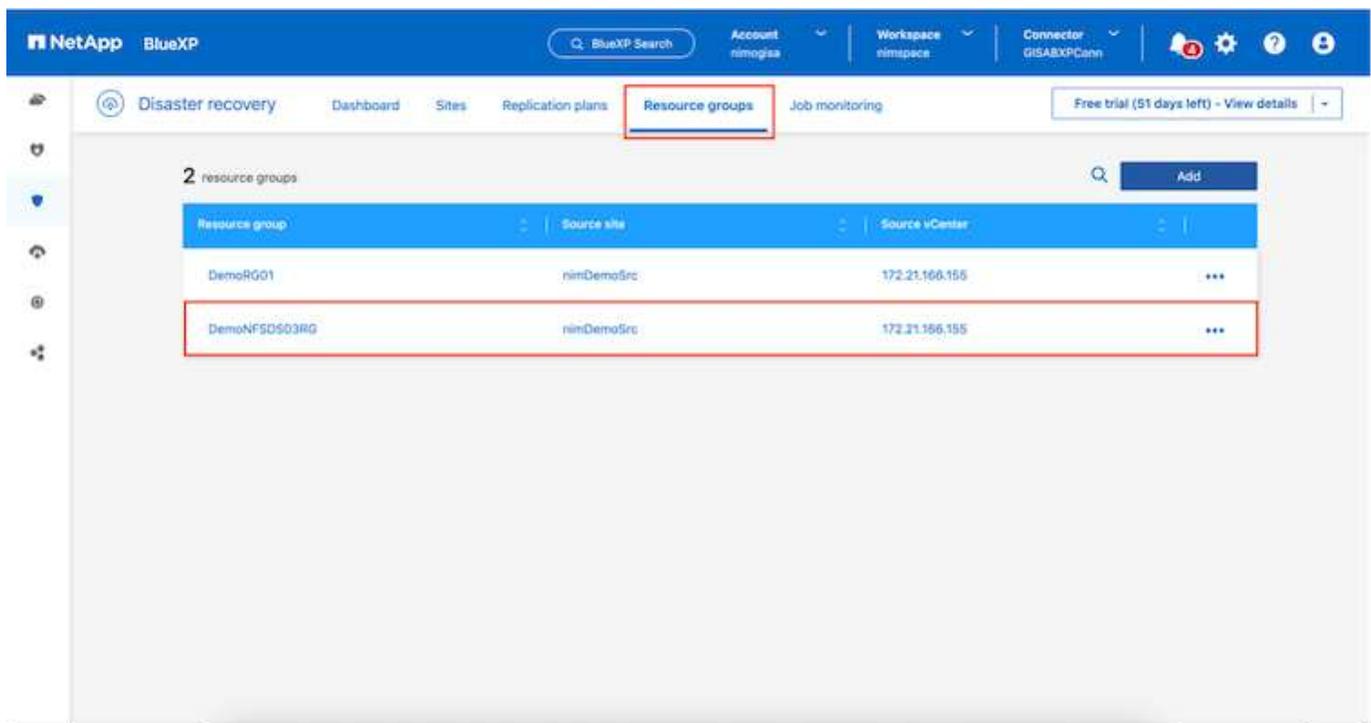
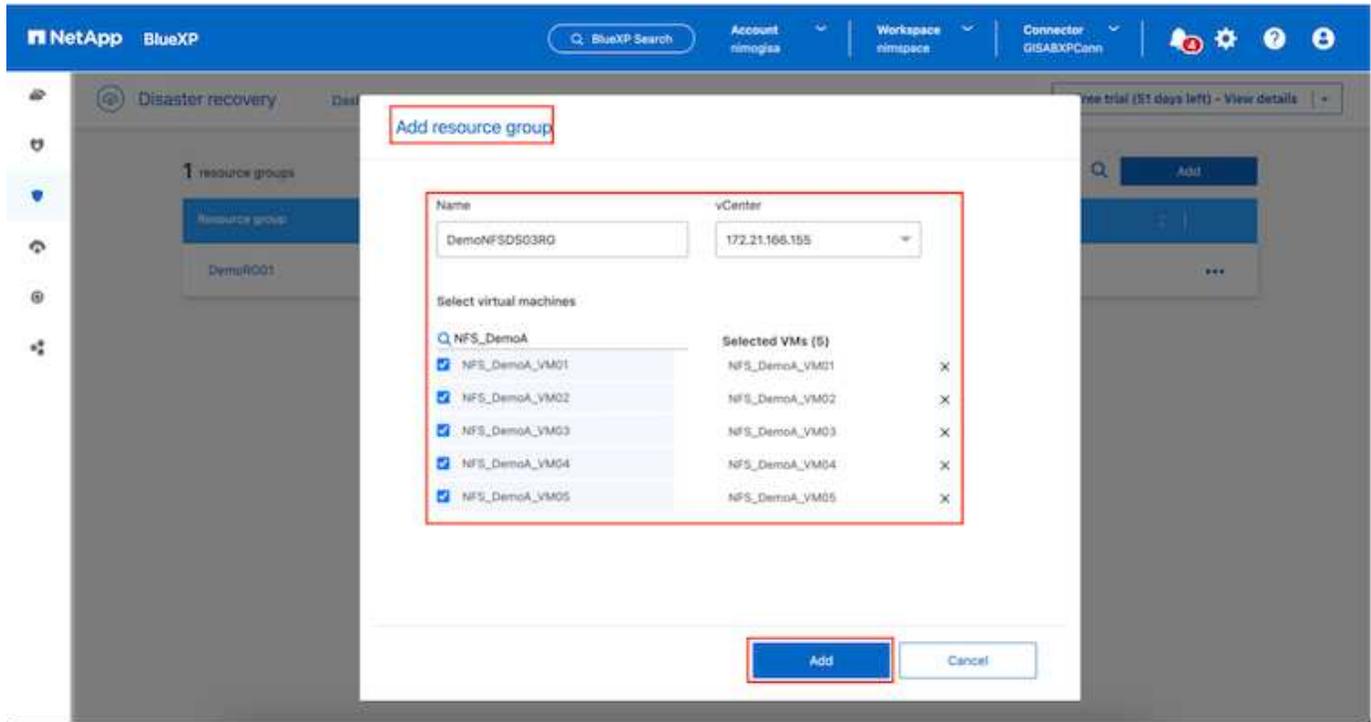
In che modo il disaster recovery di BlueXP può aiutarti?

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.



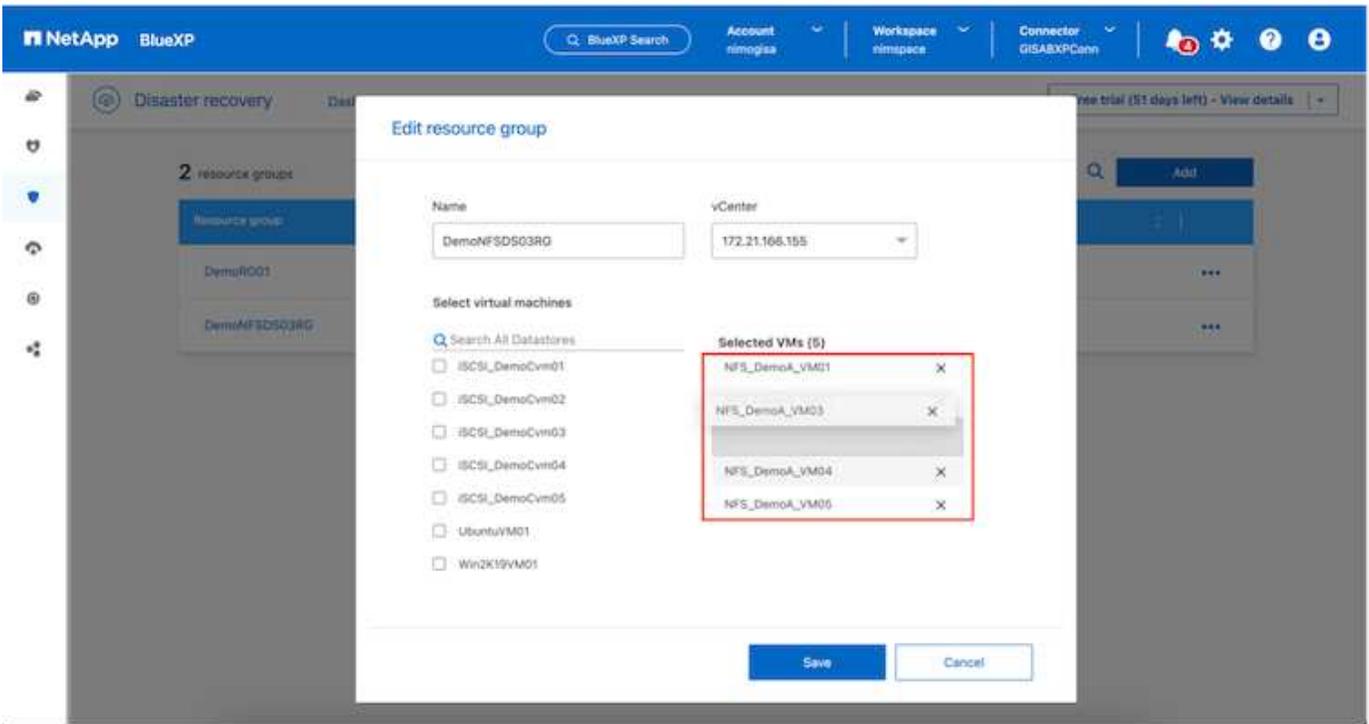
Una volta aggiunti i siti, è possibile raggruppare le macchine virtuali in gruppi di risorse. I gruppi di risorse per il

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**.

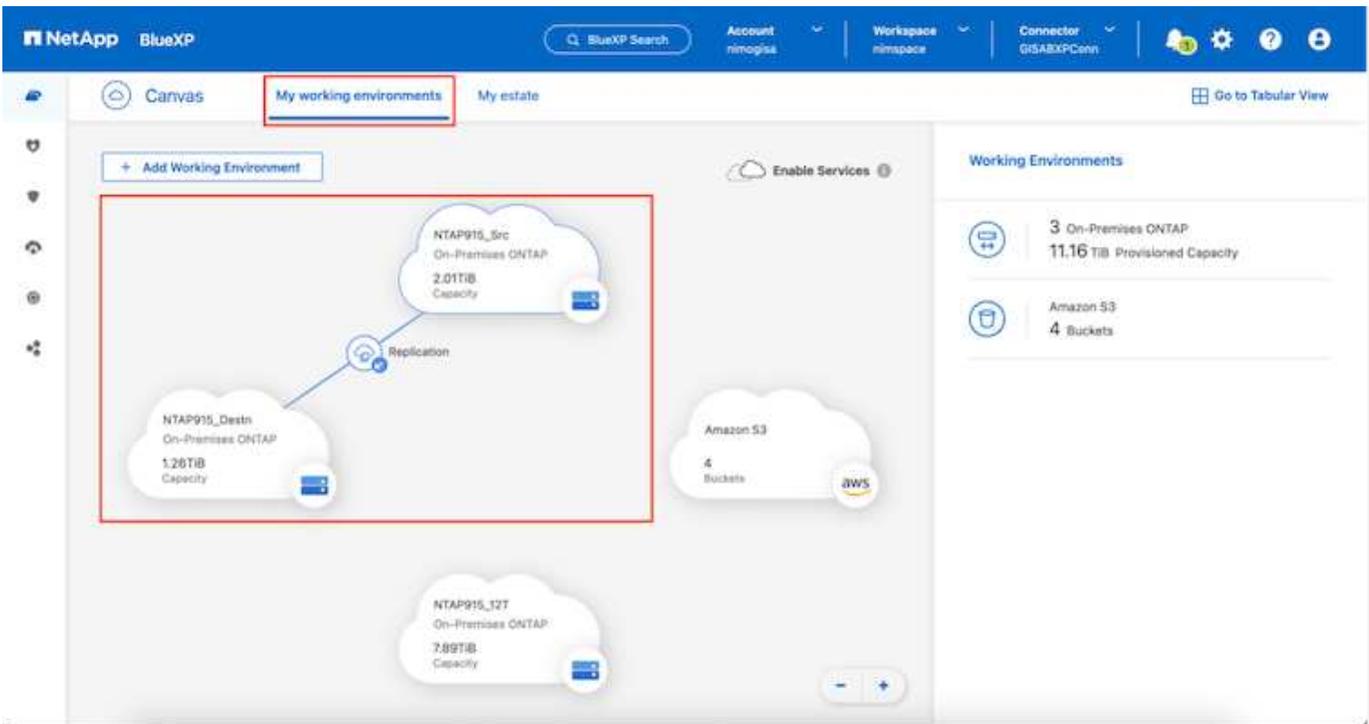


Il gruppo di risorse può anche essere creato durante la creazione di un piano di replica.

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



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.



Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
	NTAP915_Src	NTAP915_Destn				30.3 MB
✓	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:15 388.63 MiB
✓	Src_250_Vol01 NTAP915_Src	Src_250_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12: 79.23 MiB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12: 24.64 MiB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12: 47.38 MiB
✓	Src_JSCSI_DS04 NTAP915_Src	Src_JSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12: 108.87 MiB
✓	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12: 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**.

Innanzitutto, selezionare vCenter di origine, quindi il vCenter 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.

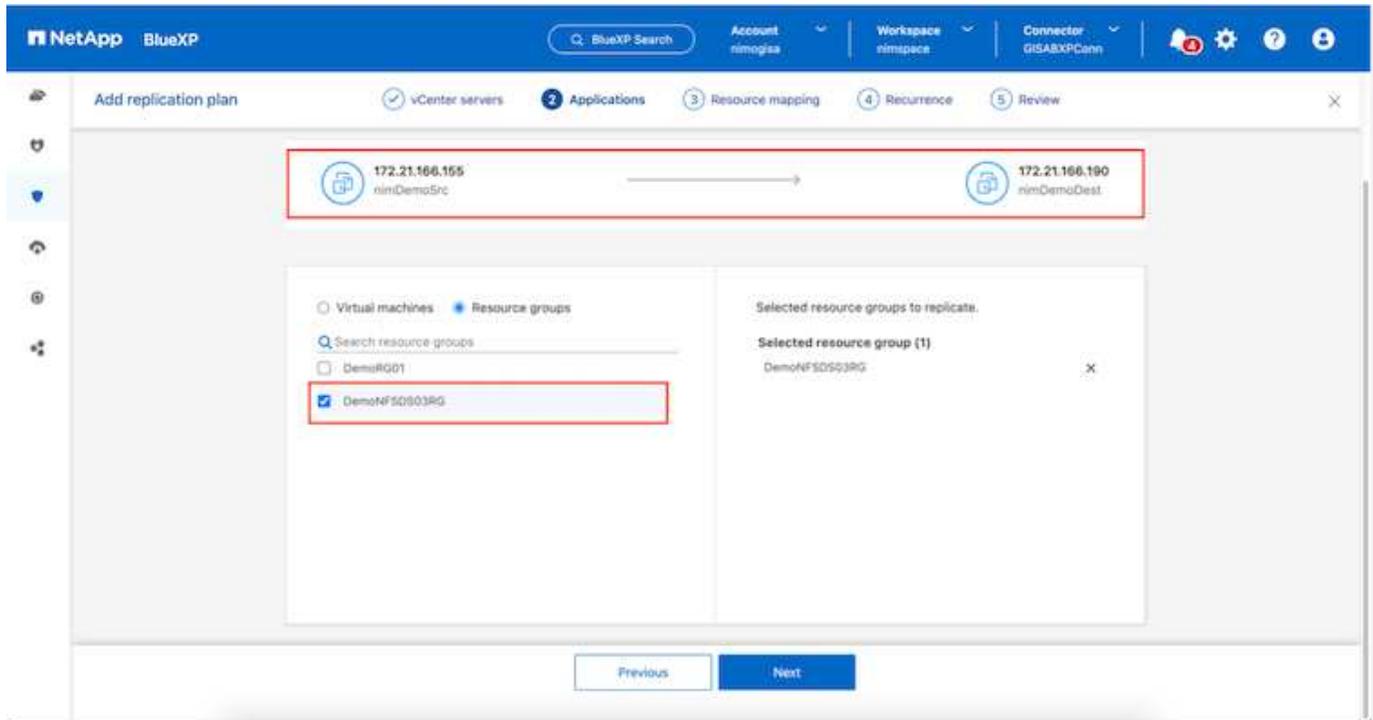
Source vCenter: 172.21.166.155

Target vCenter: 172.21.166.190

Cancel Next

Il 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.

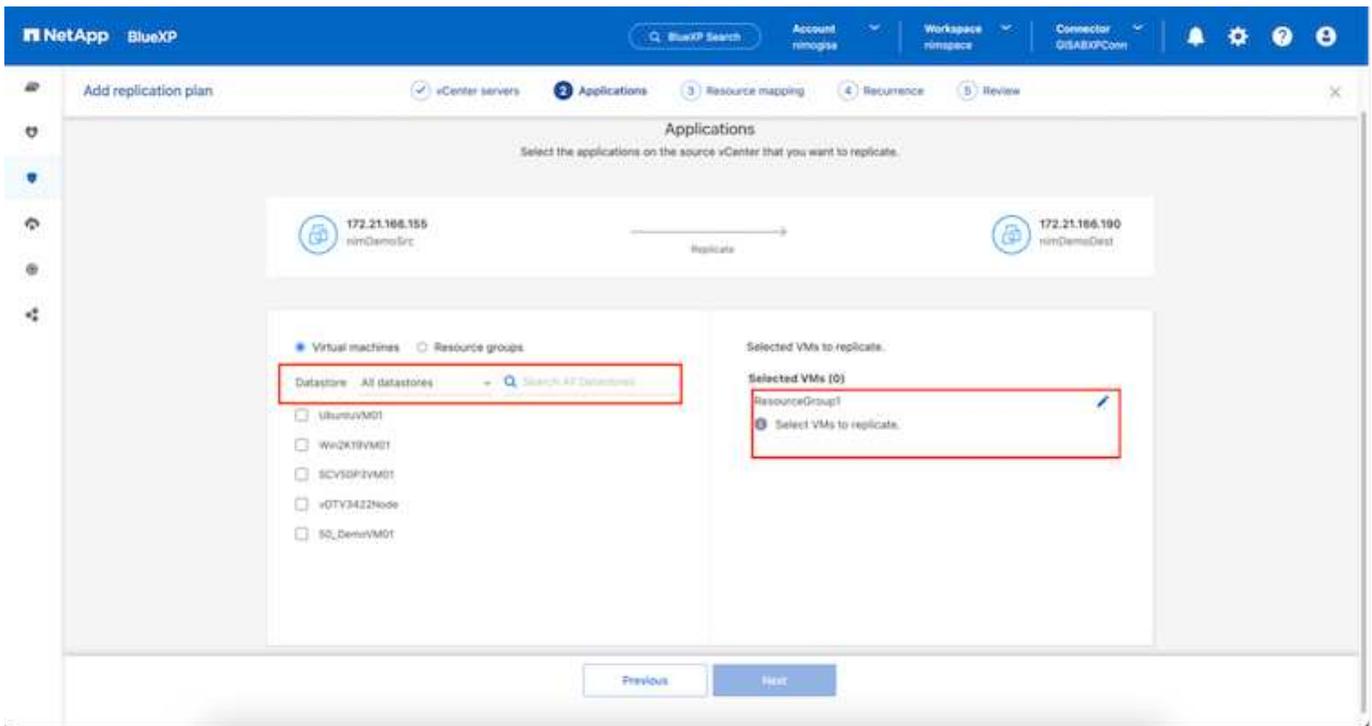


Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine di accensione delle macchine virtuali durante il processo di ripristino.

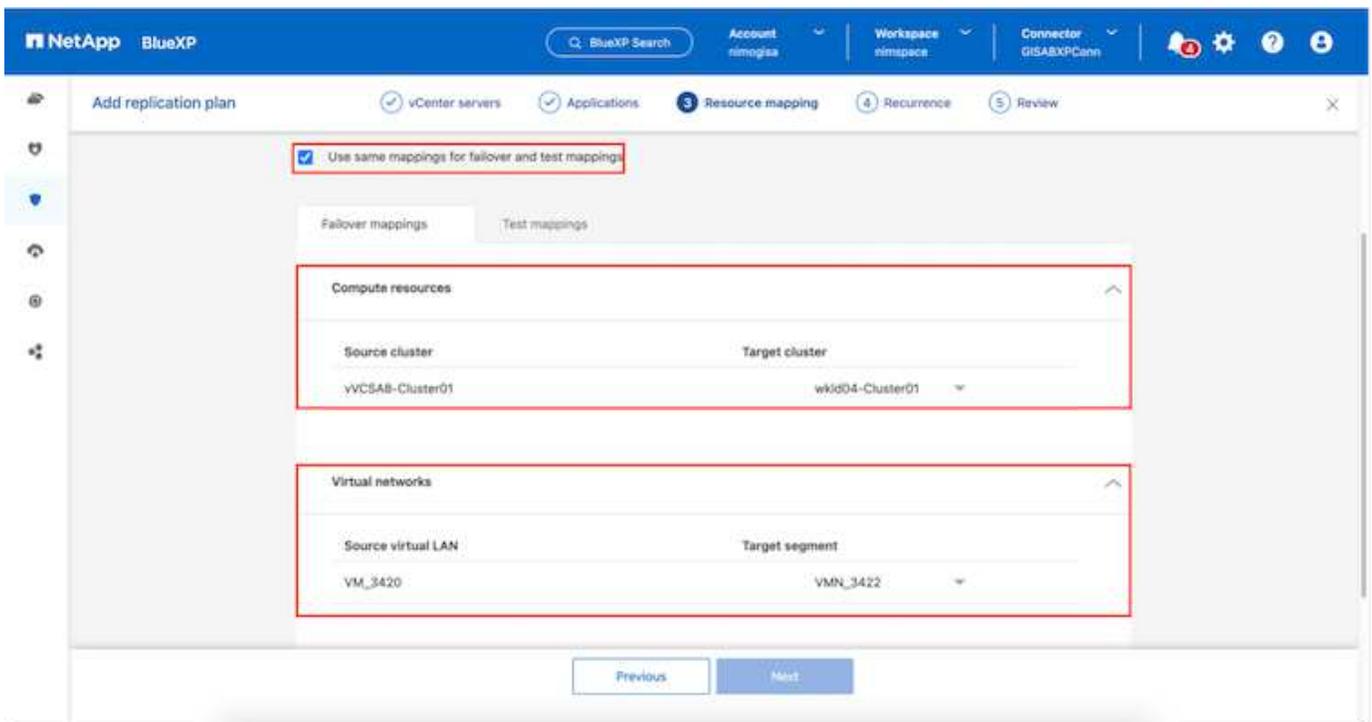


Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Due gruppi di risorse vengono avviati in parallelo.

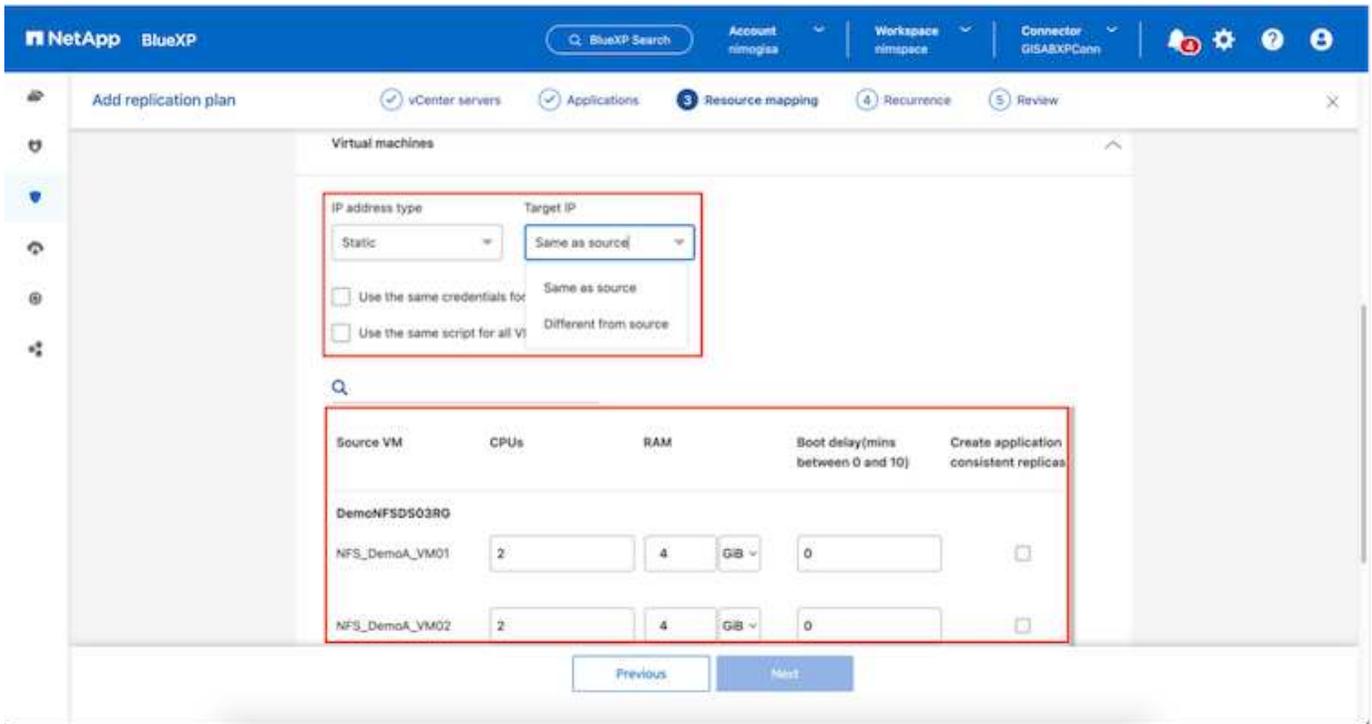
Lo screenshot seguente mostra la possibilità di filtrare le macchine virtuali o gli archivi dati specifici in base ai requisiti organizzativi se i gruppi di risorse non vengono creati in precedenza.



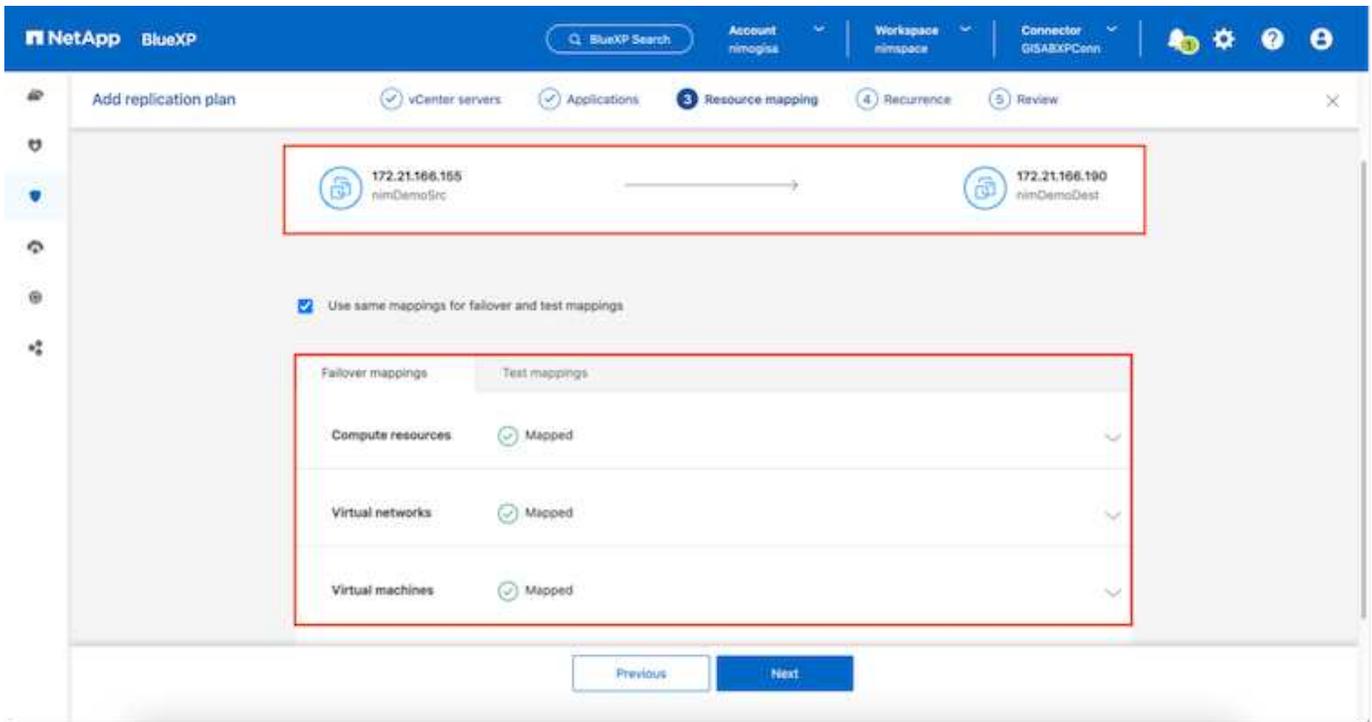
Una volta selezionati i gruppi di risorse, creare le mappature di failover. In questo passaggio, specificare il modo in cui le risorse dell'ambiente di origine vengono mappate alla destinazione. Sono incluse le risorse di elaborazione e le reti virtuali. Personalizzazione IP, pre e post-script, ritardi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



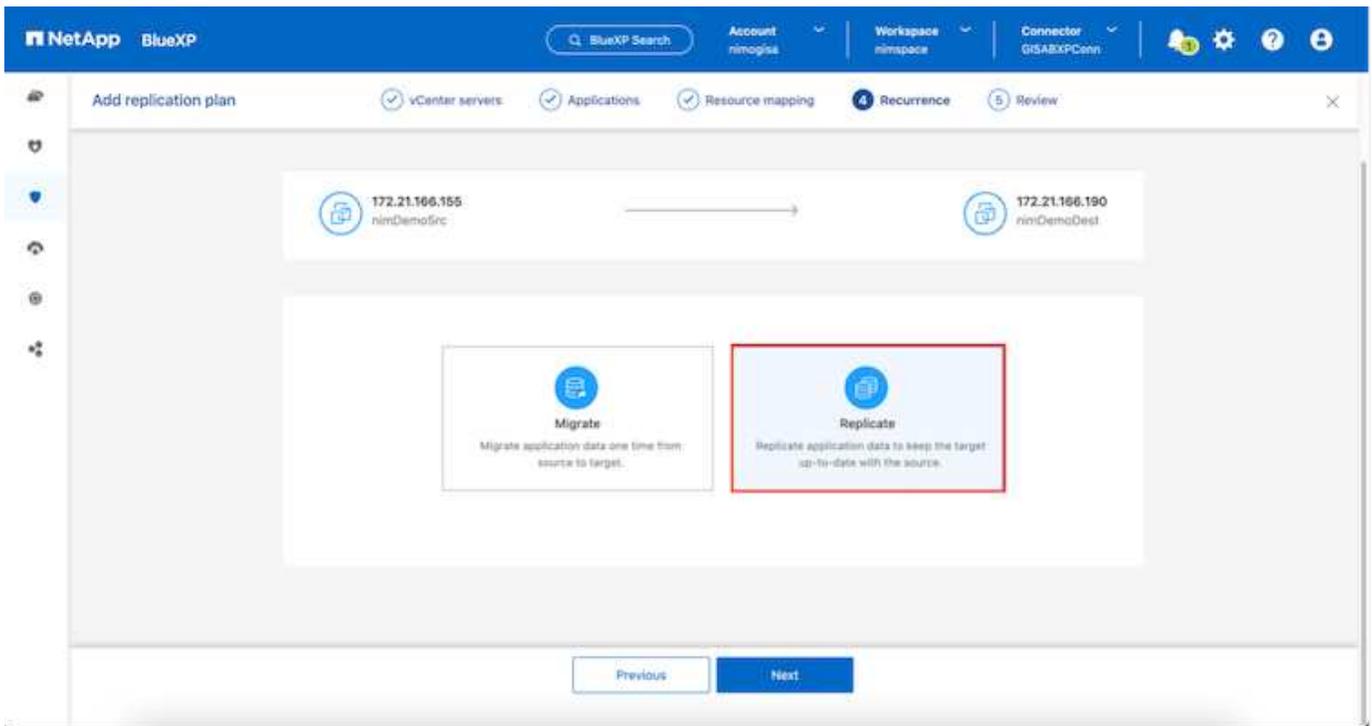
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per impostare mappature diverse per l'ambiente di test, selezionare l'opzione Test mapping (Test mapping) dopo aver deselezionato la casella di controllo come illustrato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



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



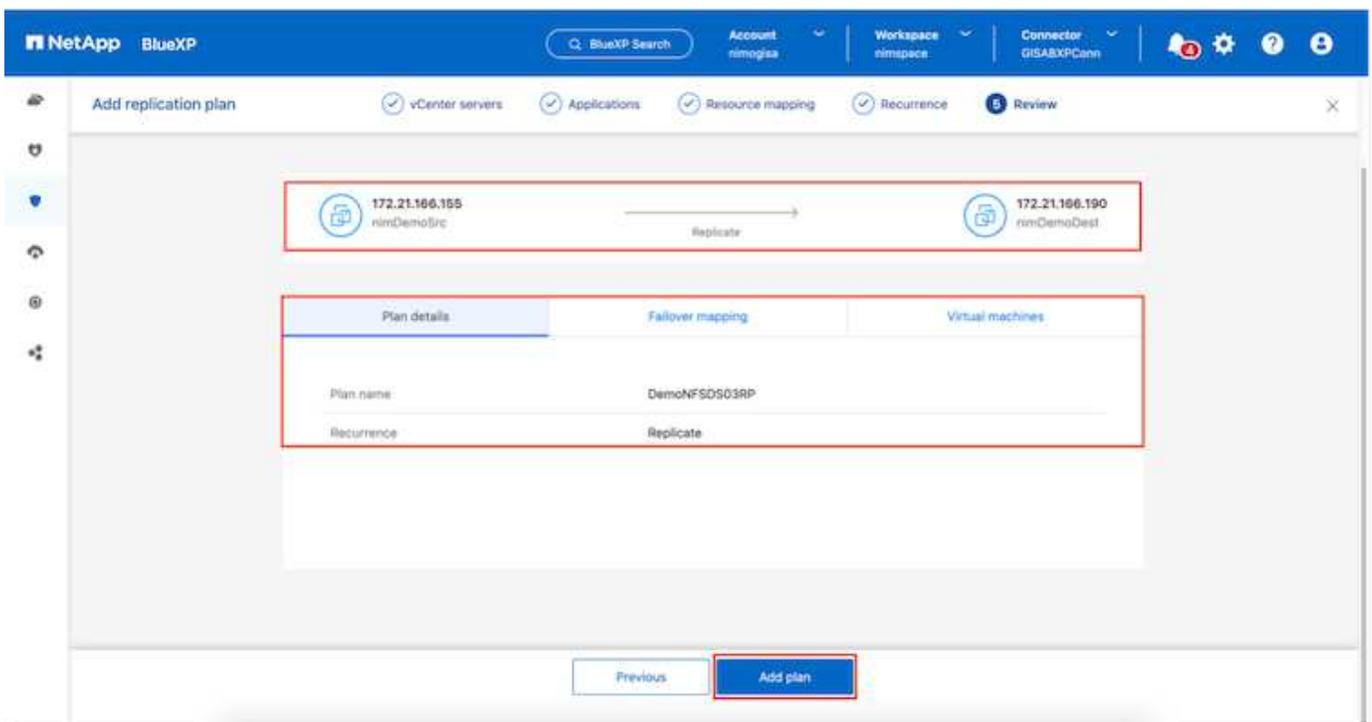
Selezionare il tipo di ricorrenza. In poche parole, selezionare l'opzione Migrate (migrazione una tantum tramite failover) o Replica continua ricorrente. In questa procedura dettagliata, l'opzione Replica è selezionata.

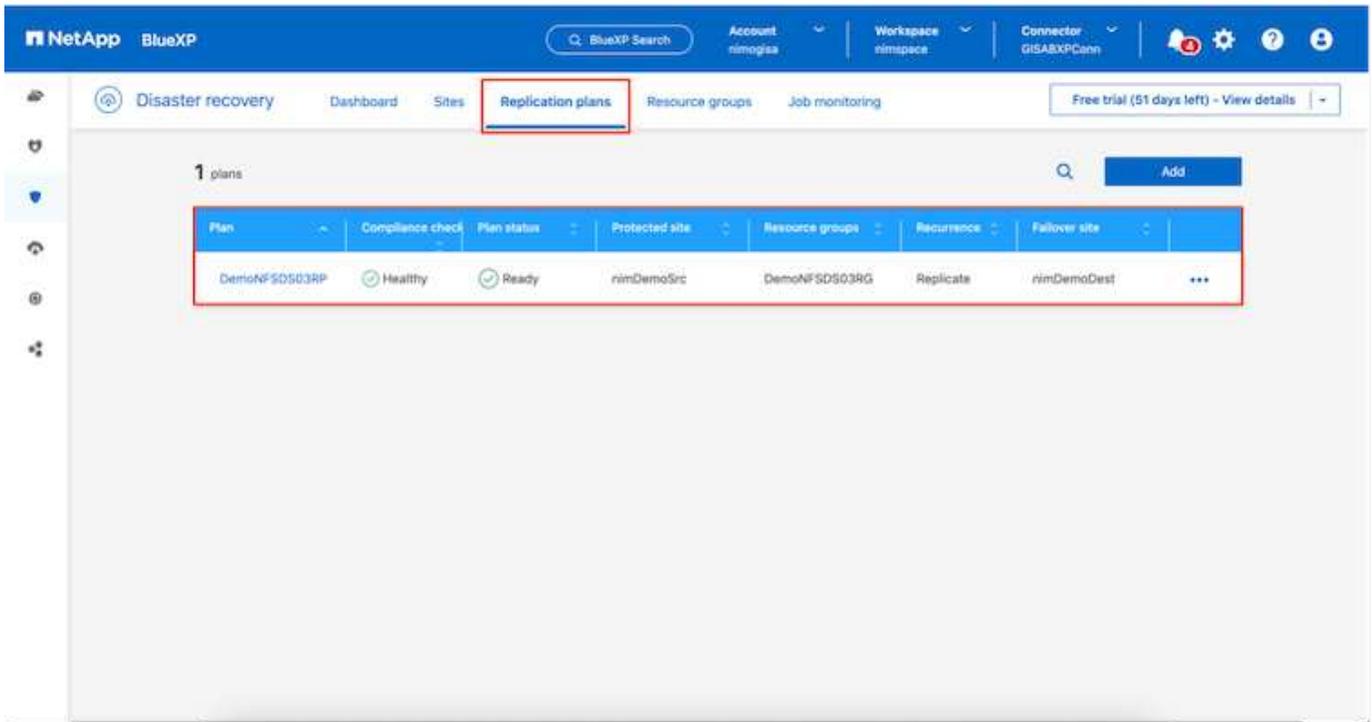


Al termine, rivedere le mappature create e fare clic su **Aggiungi piano**.



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.



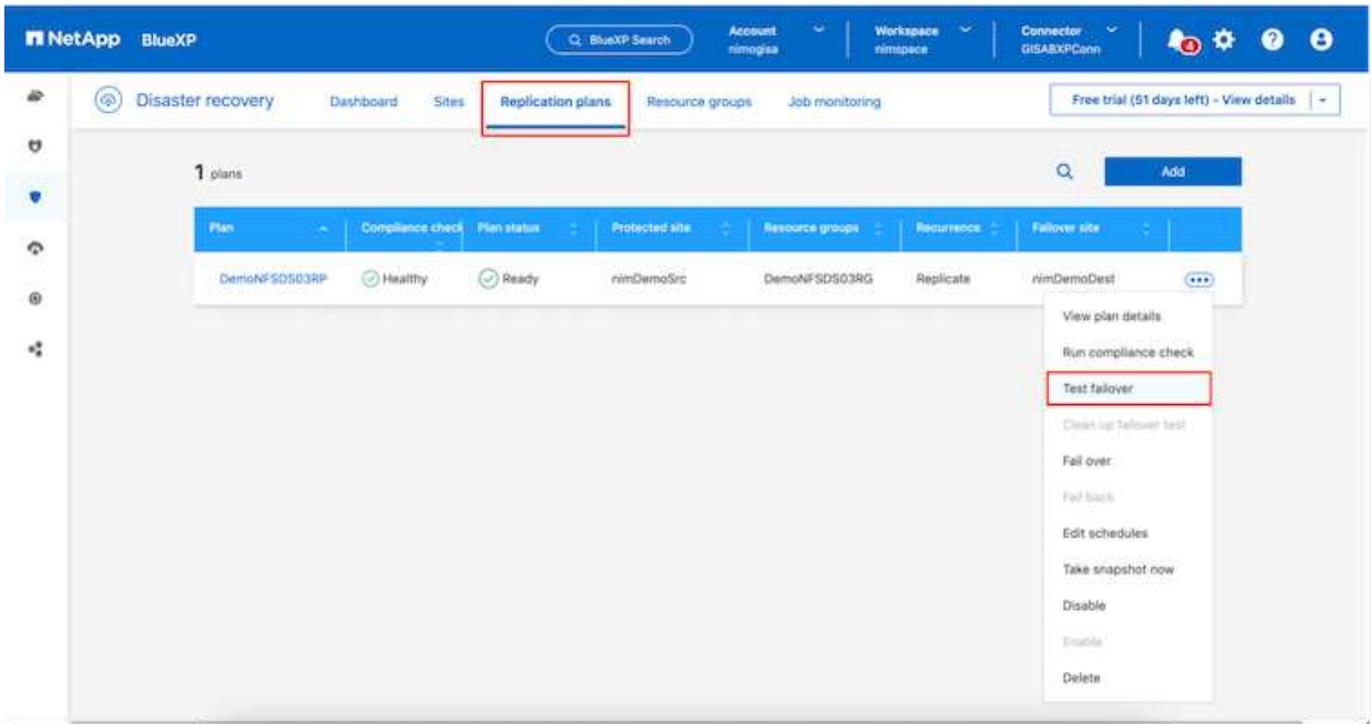


BlueXP DRaaS è costituito dai seguenti flussi di lavoro:

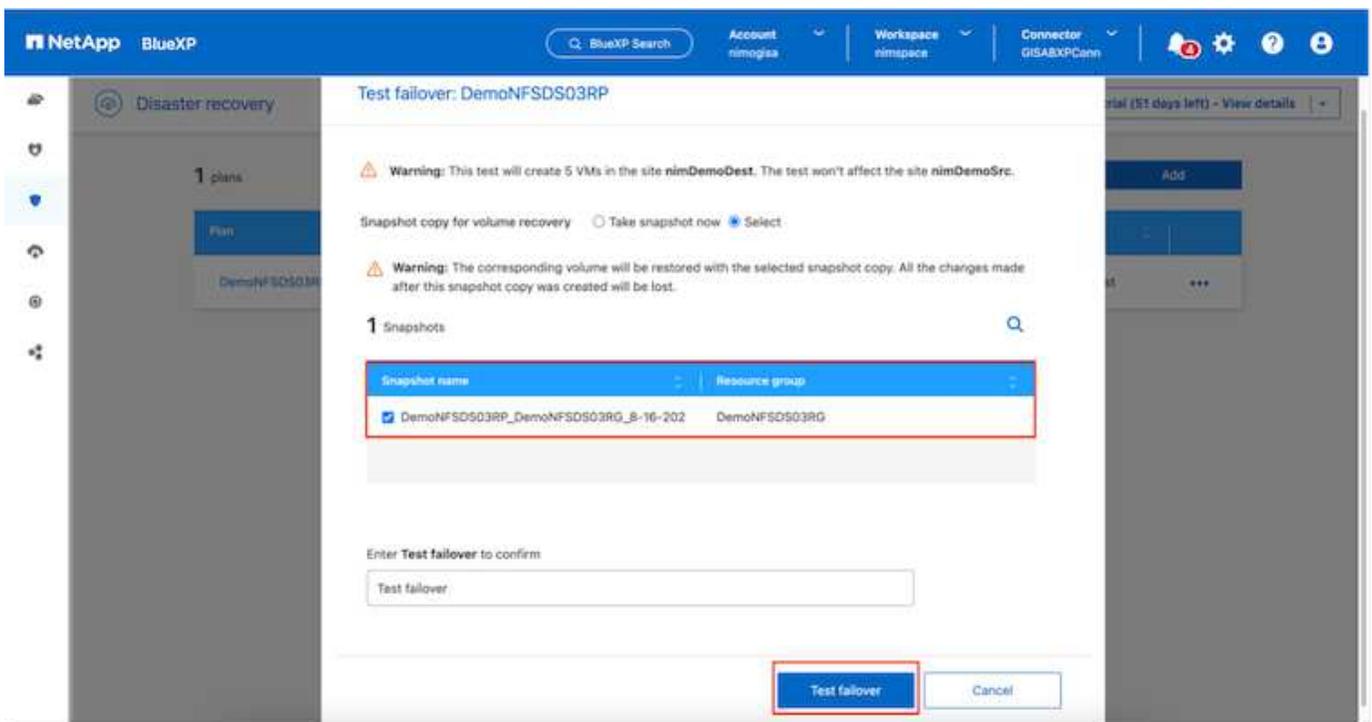
- Failover di test (incluse simulazioni periodiche automatizzate)
- Test di failover di cleanup
- Failover
- Failback

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.



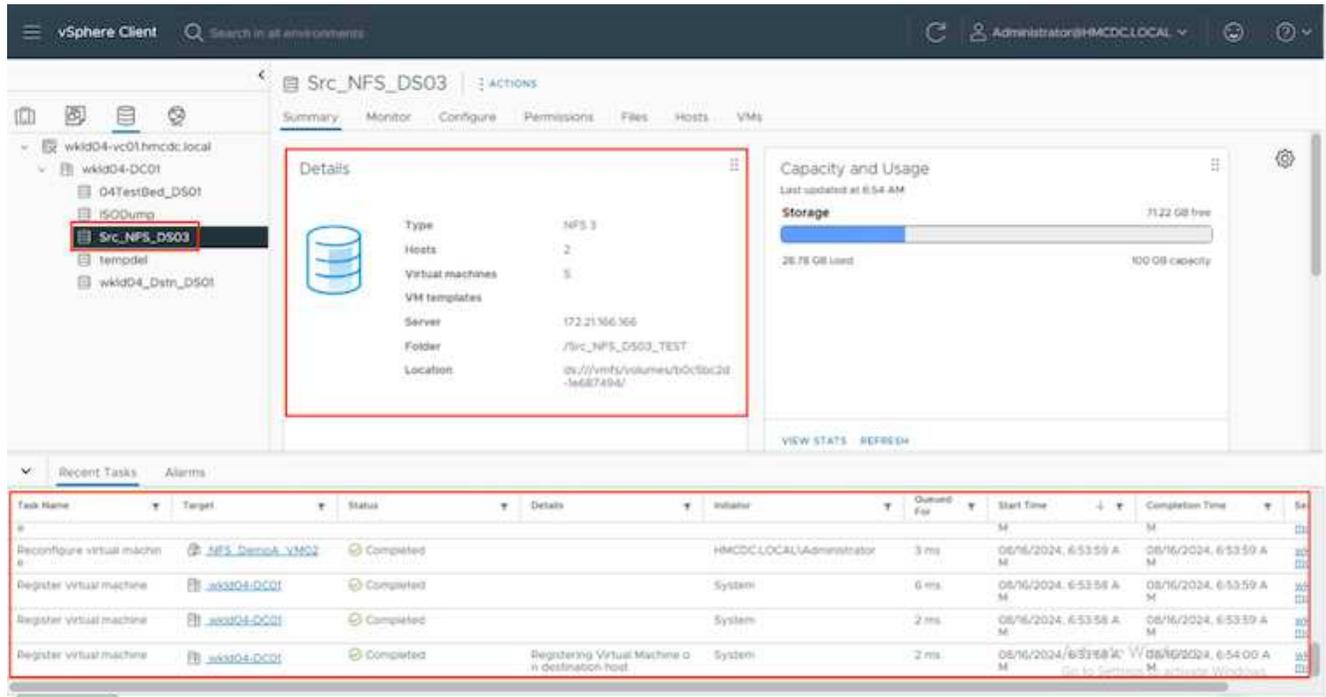
BlueXP DRaaS incorpora la capacità di selezionare lo snapshot come funzionalità opzionale nell'operazione di test failover. Questa funzionalità consente all'amministratore VMware di verificare che eventuali modifiche apportate di recente nell'ambiente vengano replicate nel sito di destinazione e quindi 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:

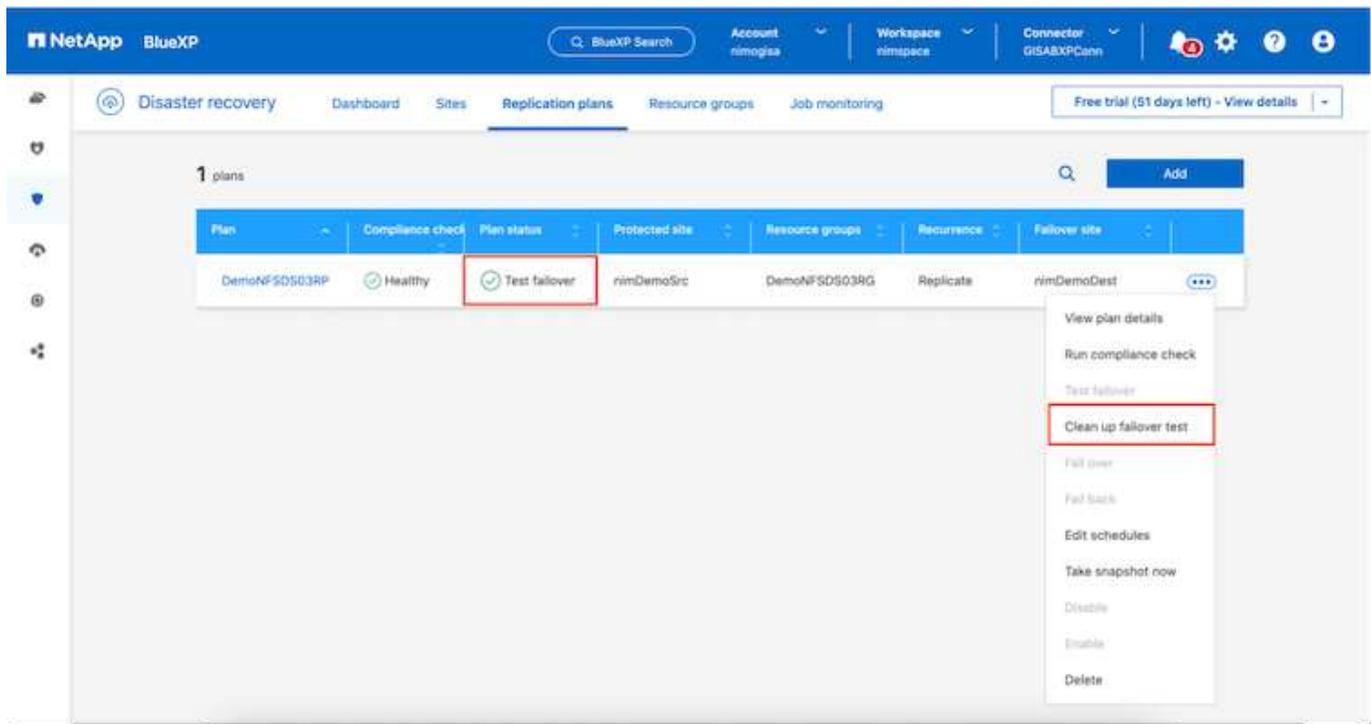
- Attivazione di relazioni SnapMirror per aggiornare lo storage nel sito di destinazione con eventuali modifiche recenti apportate nel sito di produzione.

- 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.



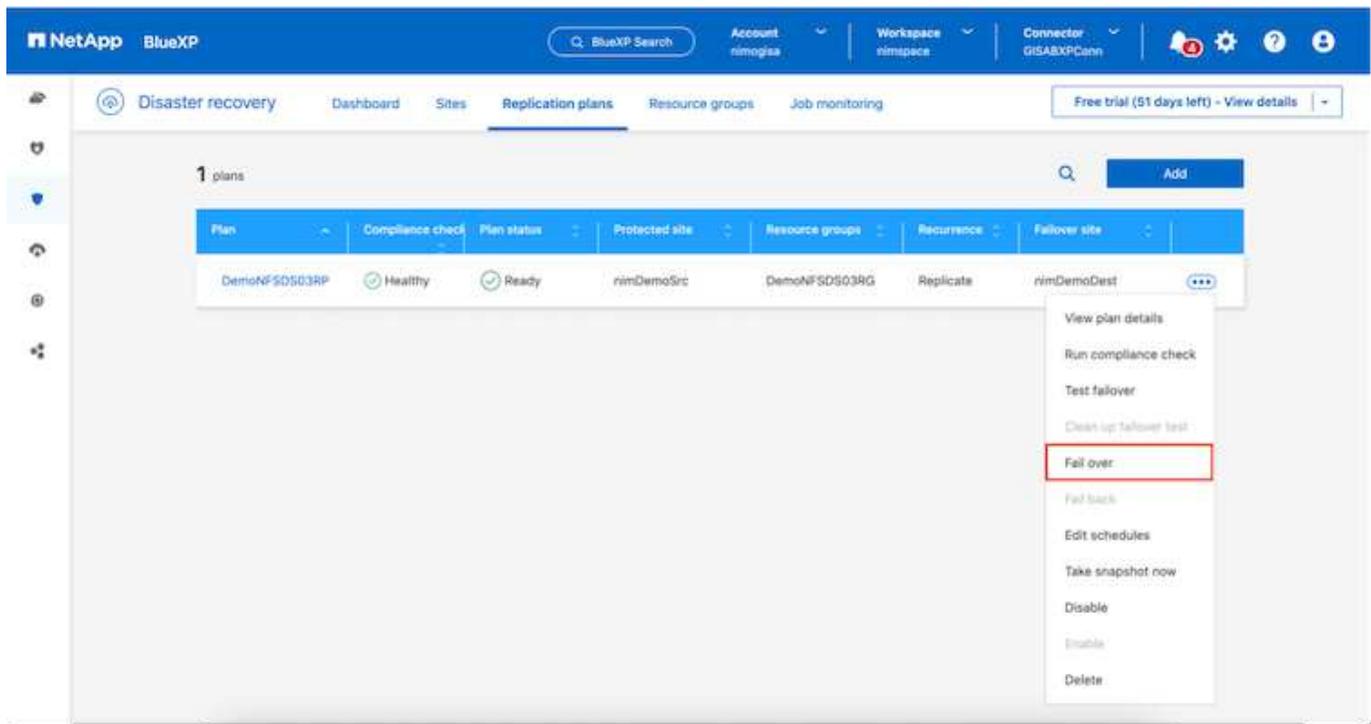
Questa azione ripristina le macchine virtuali (VM) e lo stato del piano di replica allo stato pronto.

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.

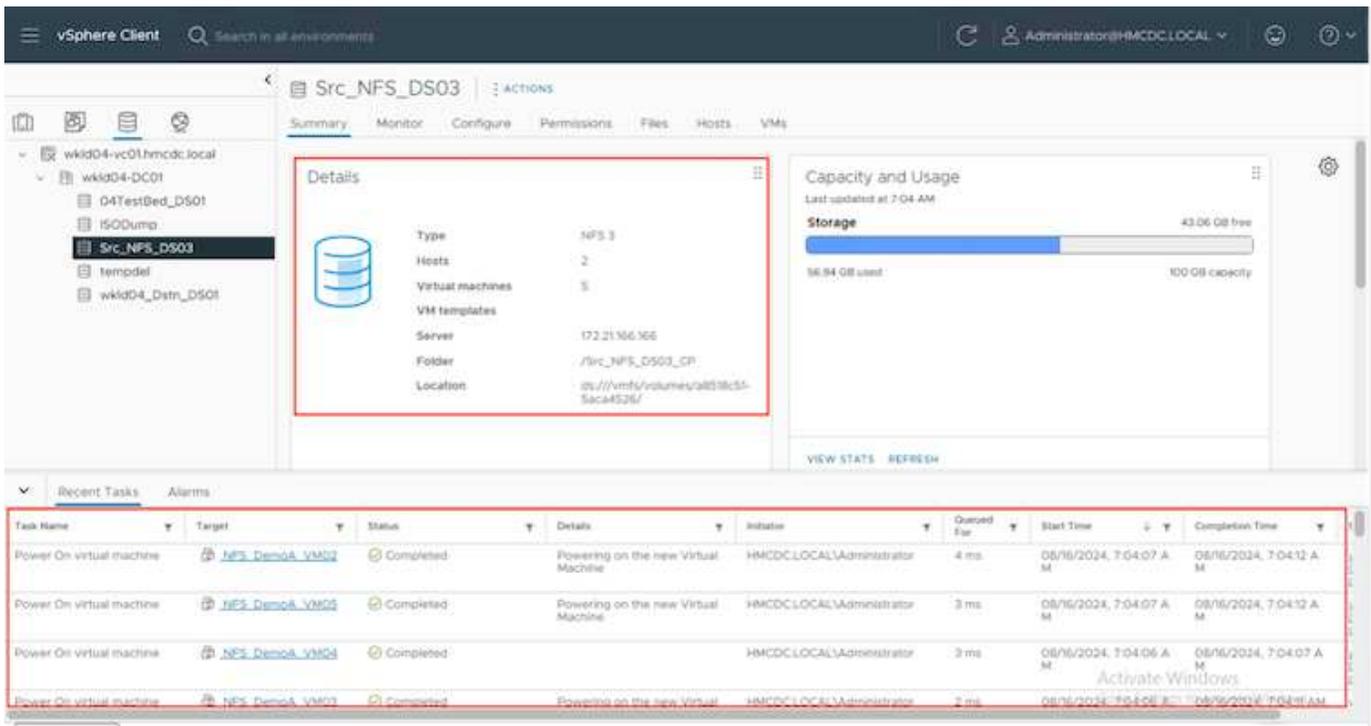
Migrazione pianificata e failover

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.



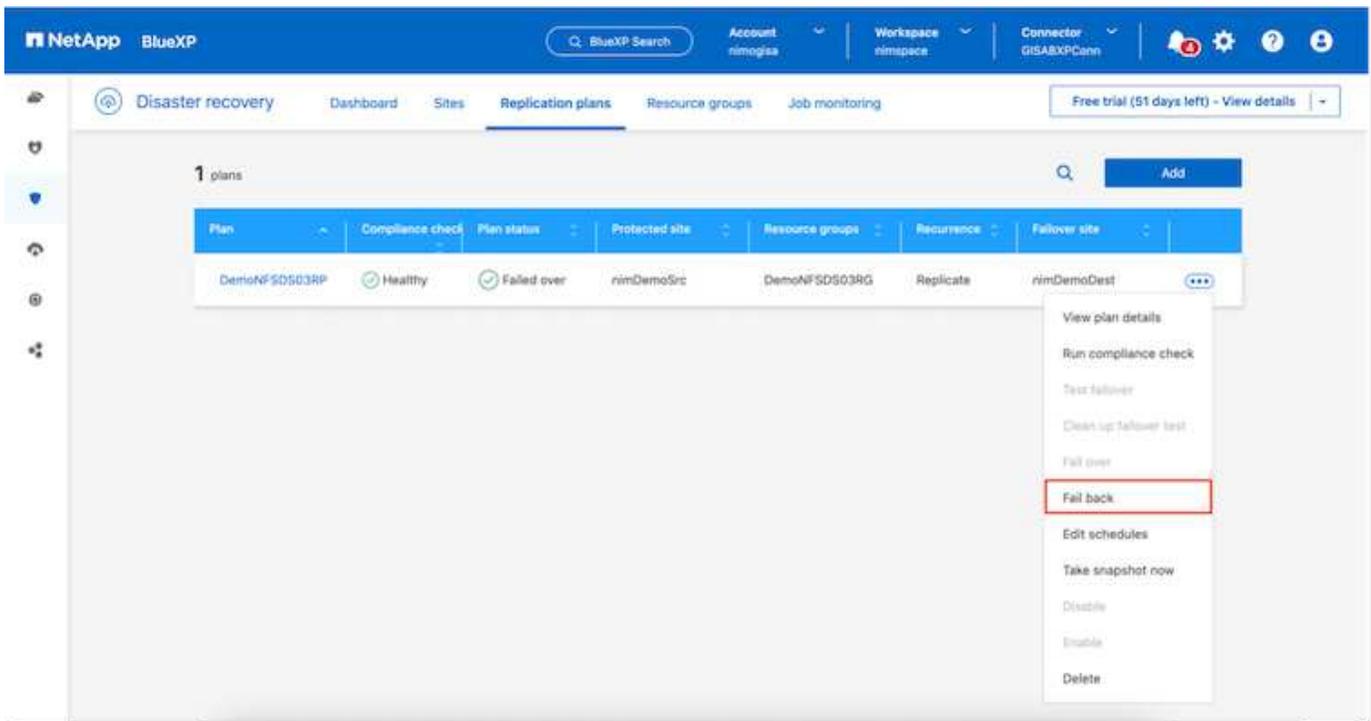
Quando l'amministratore VMware esegue un'operazione di failover, BlueXP DRaaS automatizza le seguenti attività:

- 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:

- Spegner 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

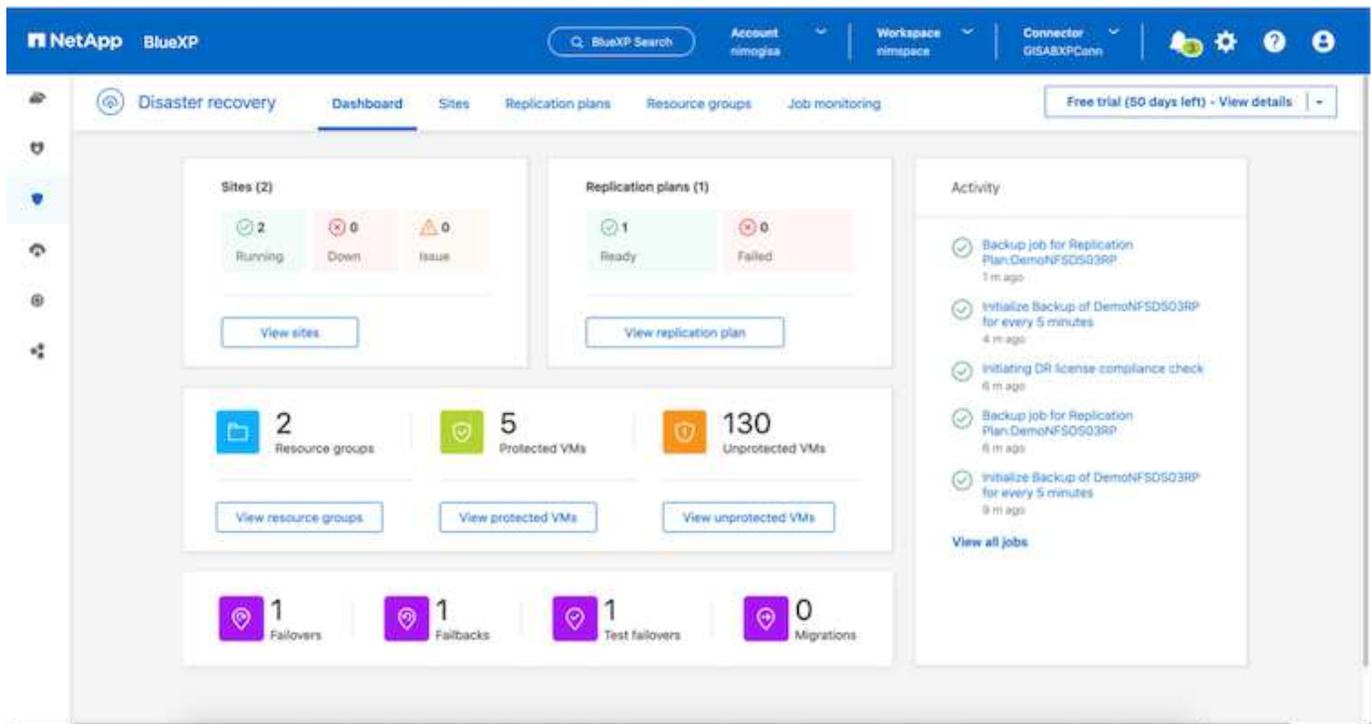
Da BlueXP o dalla CLI di ONTAP, puoi monitorare lo stato di salute della replica per i volumi del datastore appropriati e lo stato di un failover o di un failover di test può essere monitorato tramite il monitoraggio dei processi.

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...	-	Cancel job?
3549cc9c-aa4e-45e	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4af1	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 DemoNFSD503RP 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 DemoNFSD503R...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-6f77-459f	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bffc018e-ca3a-409d	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebef-498e	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-9830-4c5	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



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](#)".

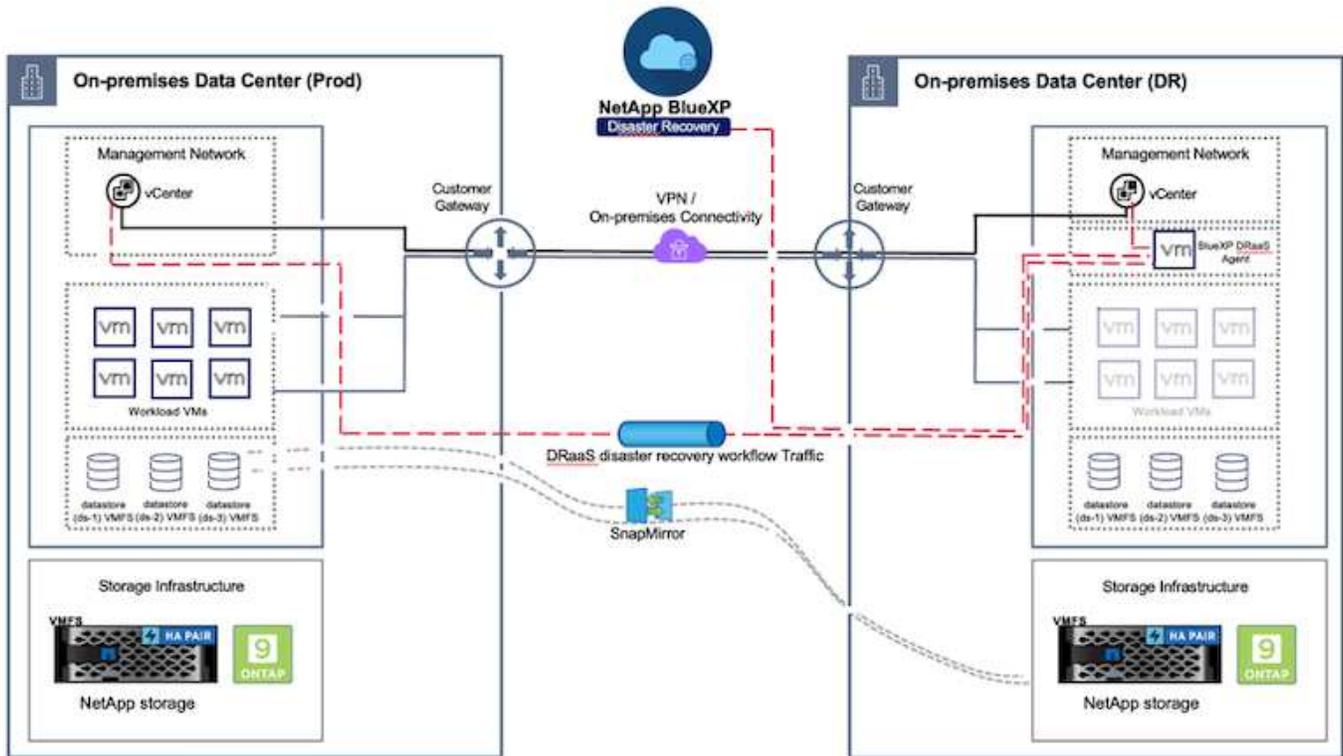
Dr utilizzando BlueXP DRaaS per archivi dati VMFS

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

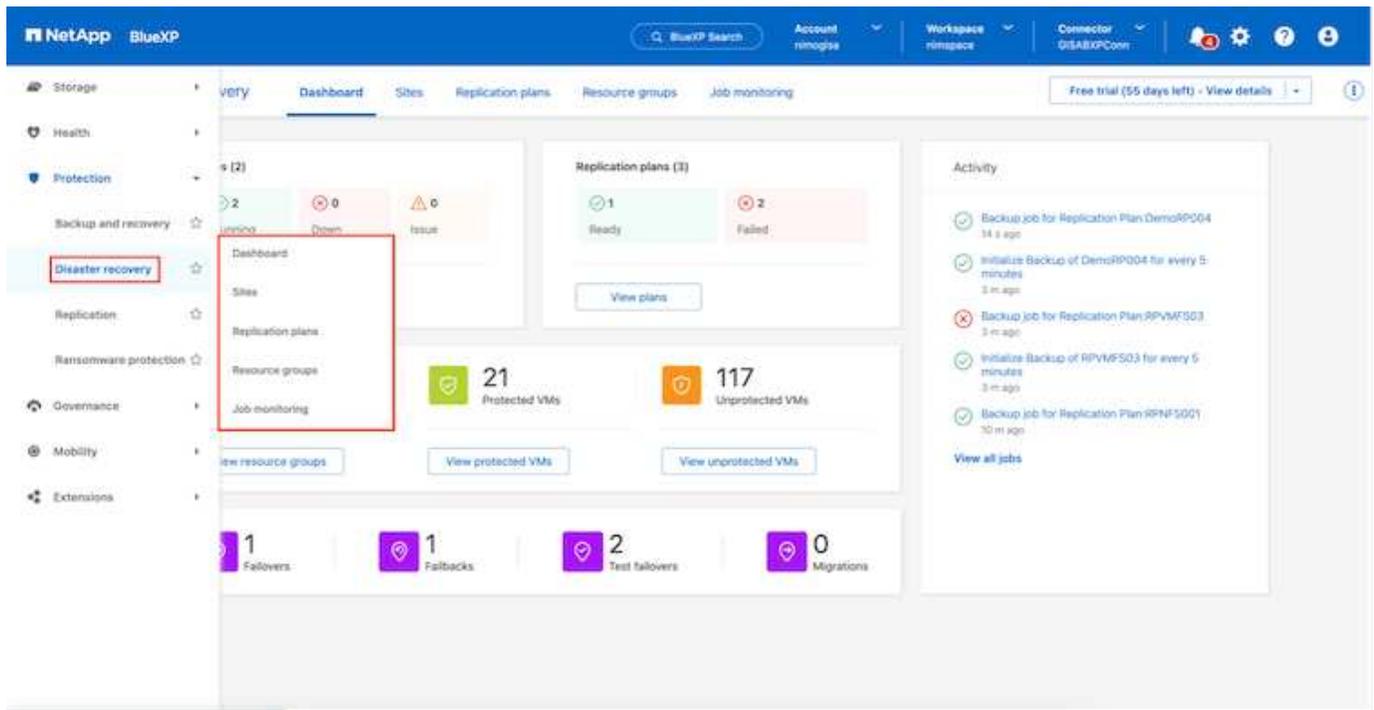
recovery di BlueXP sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore VMFS dall'ultima snapshot replicata nel sito di disaster recovery. Una volta completato il test di DR, i clienti possono semplicemente eliminare l'ambiente di test senza alcun 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 .



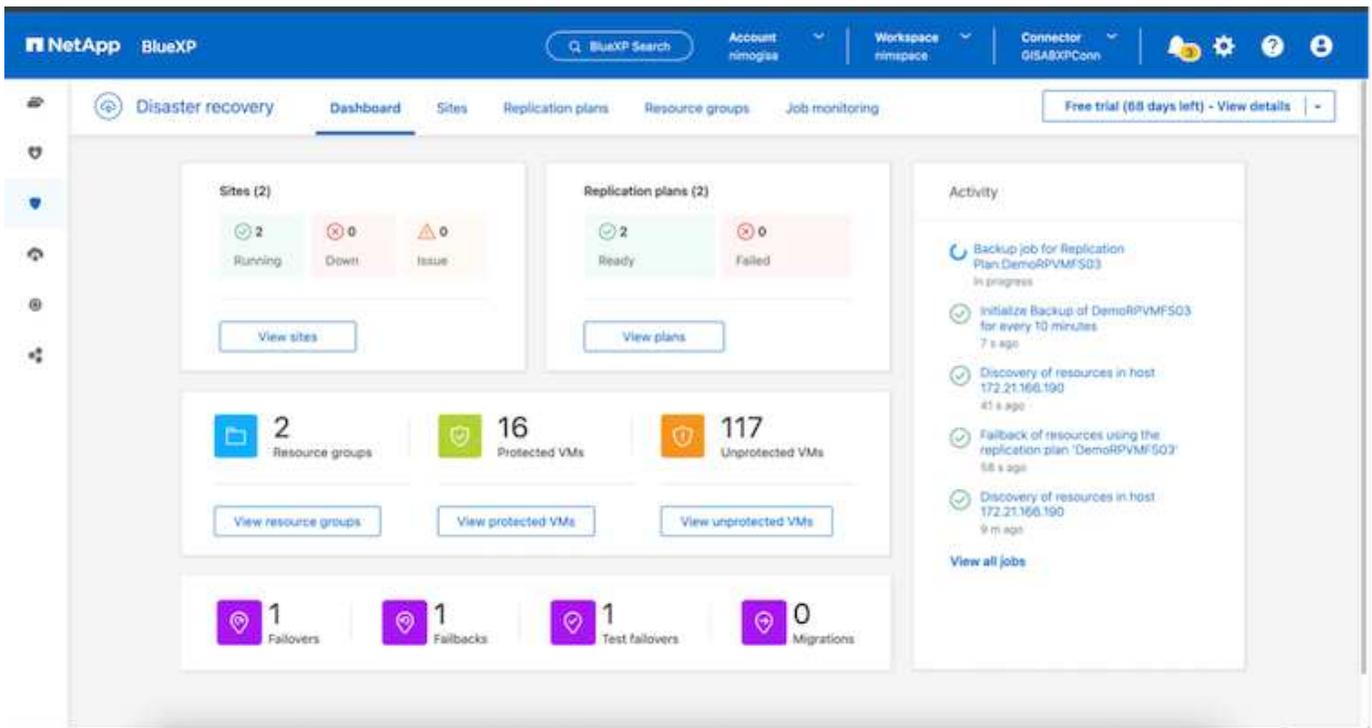
Prima di configurare il piano di disaster recovery, verificare che siano soddisfatti i seguenti prerequisiti:

- 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.



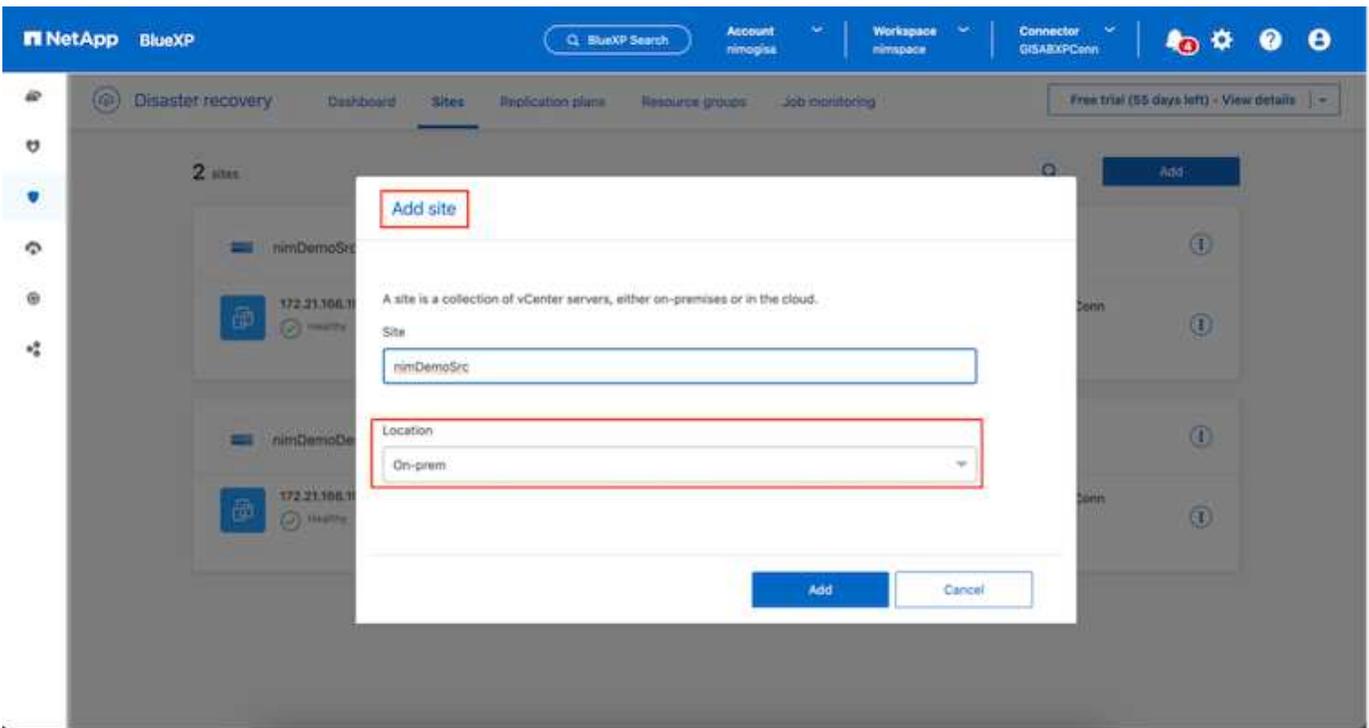
Durante la scrittura di questo documento, il supporto per datastore VMFS da on-premise a on-premise è in anteprima tecnologica. La funzionalità è supportata con datastore VMFS basati su protocollo FC e iSCSI.

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 .

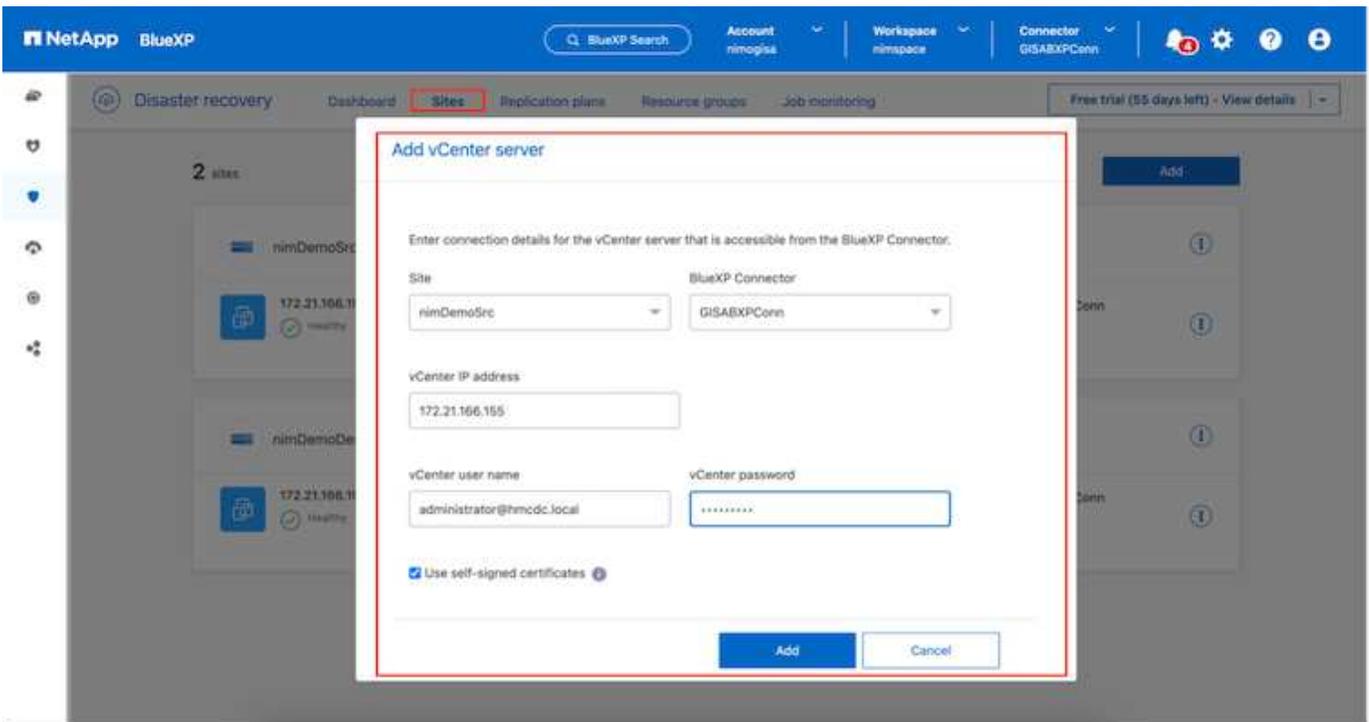


Verifica che i sistemi storage ONTAP vengano aggiunti all'ambiente di lavoro all'interno del Canvas. Aprire la console BlueXP e selezionare **protezione > Ripristino di emergenza** dal menu di navigazione sinistro. Selezionare **Scopri i server vCenter** o utilizzare il menu principale, selezionare **Siti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

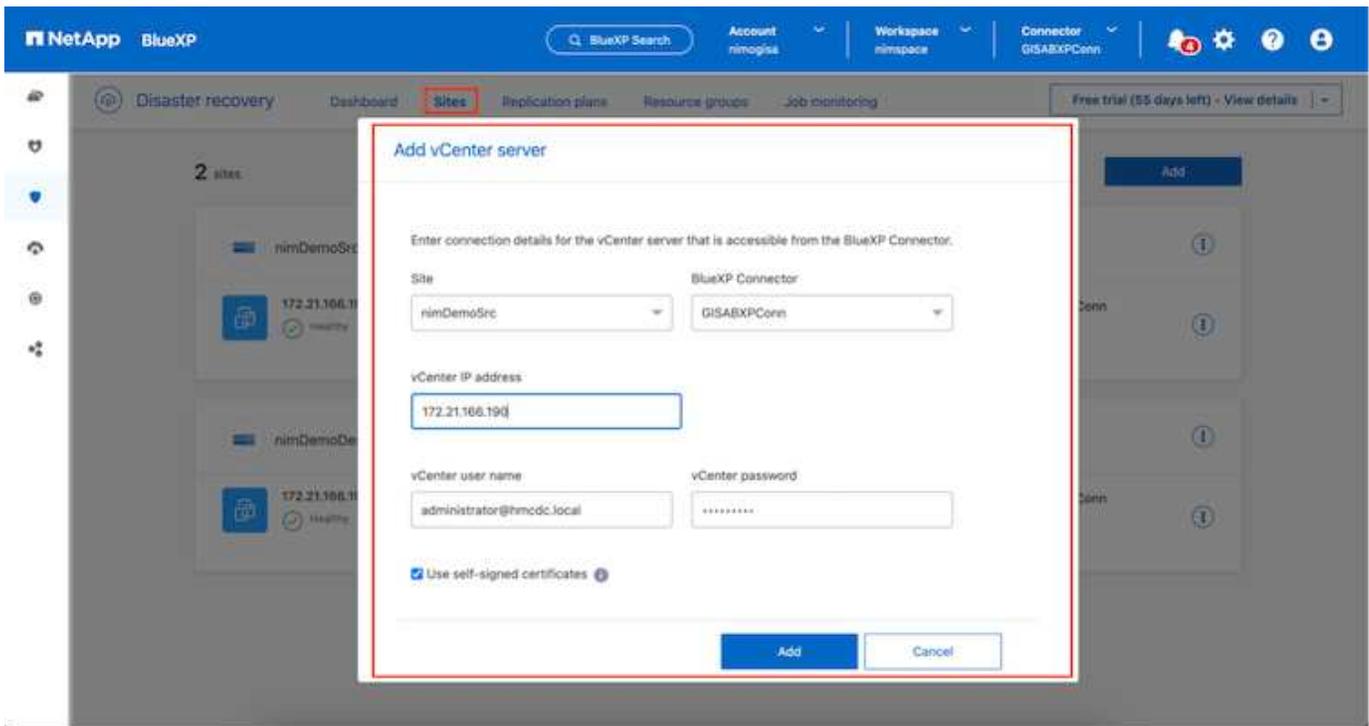


Aggiungere le seguenti piattaforme:

- **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

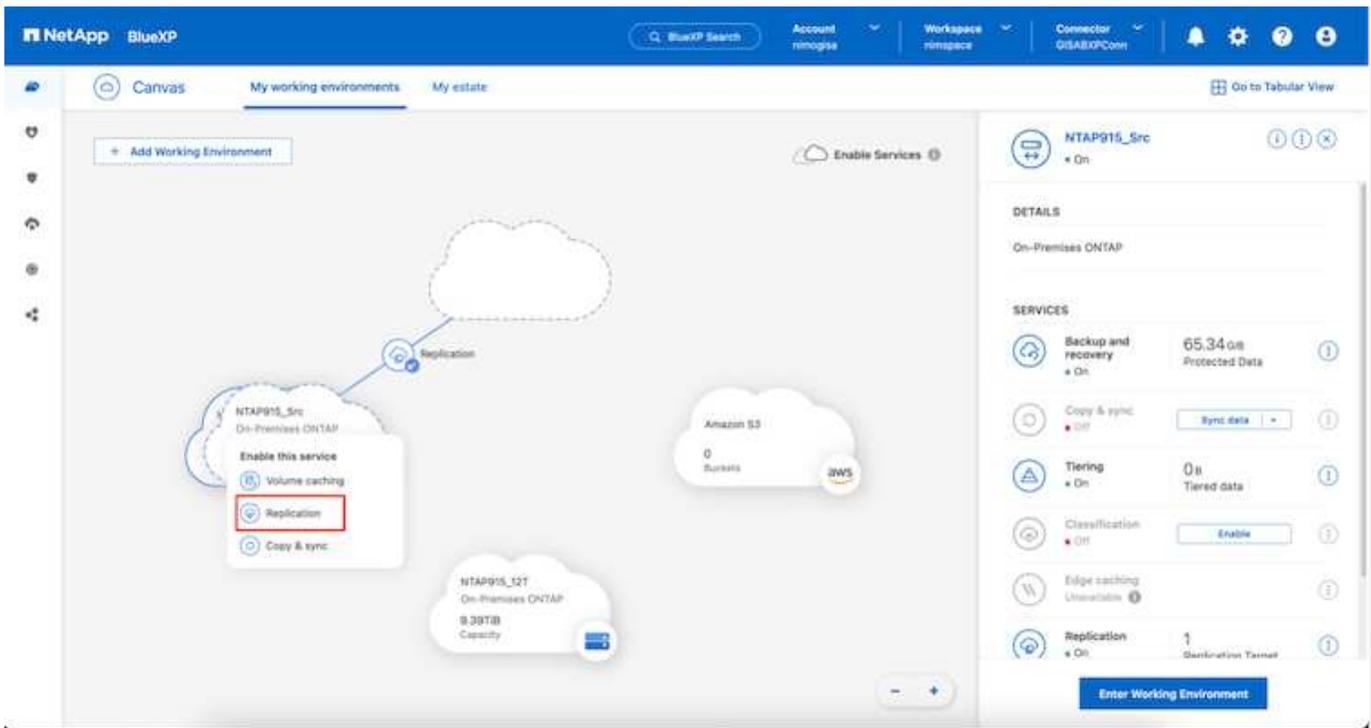
SnapMirror utilizza le snapshot ONTAP per gestire il trasferimento dei dati da una posizione all'altra. Inizialmente, una copia completa basata su uno snapshot del volume di origine viene copiata nella destinazione per eseguire una sincronizzazione di base. Quando si verificano modifiche ai dati nell'origine, 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.

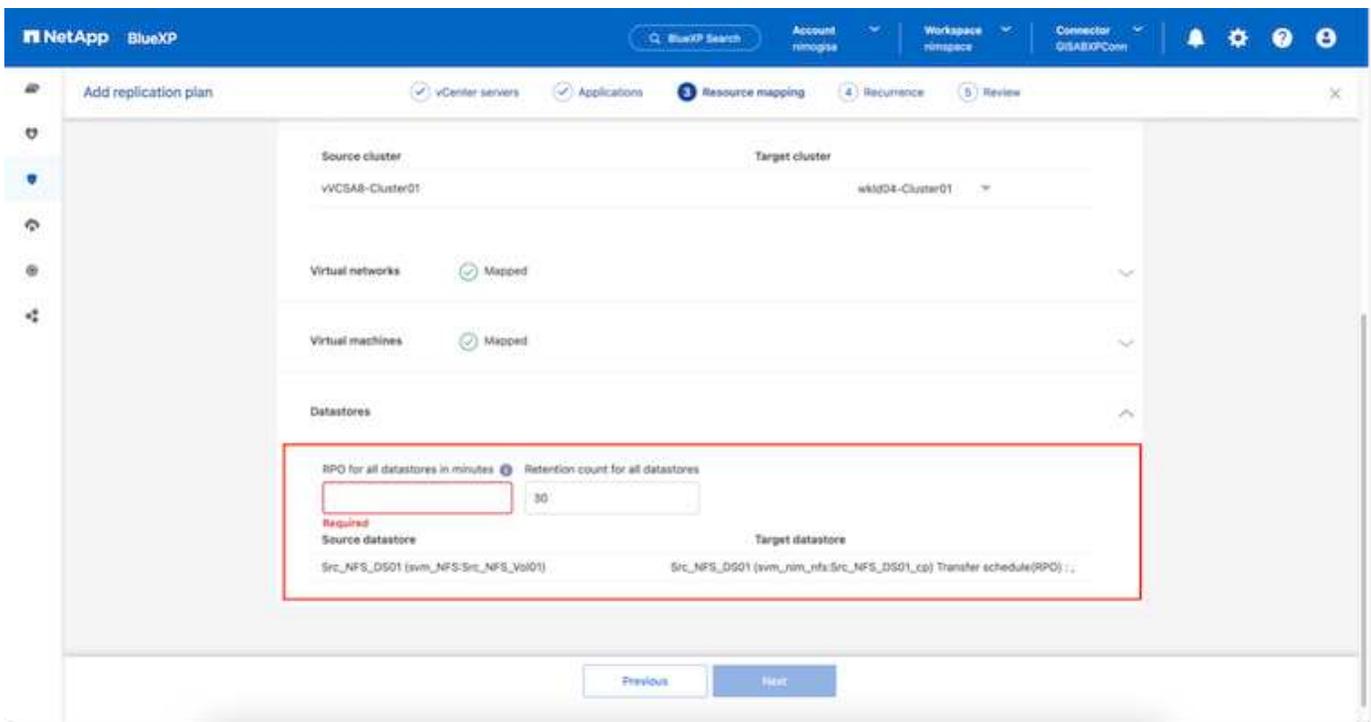
Come configurarlo per il Disaster Recovery VMware

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.



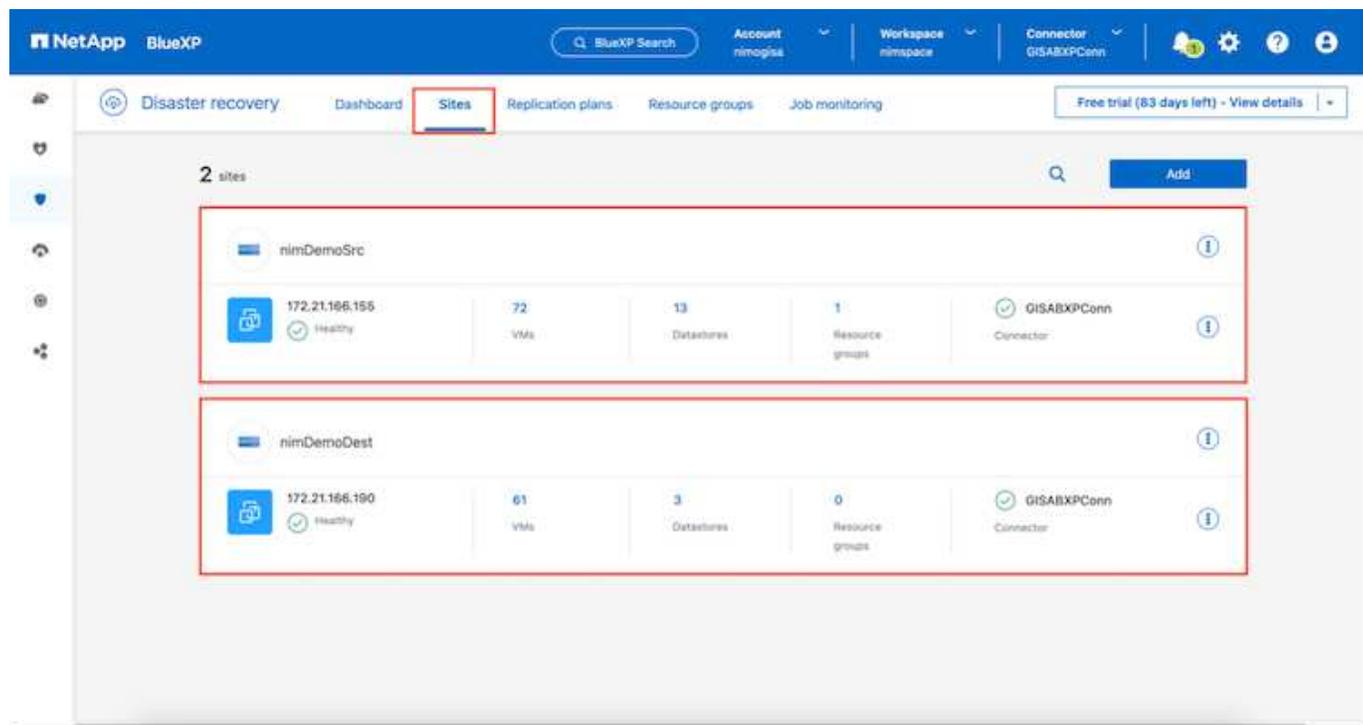
Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS raccoglie la relazione e continua con il resto delle operazioni del workflow.



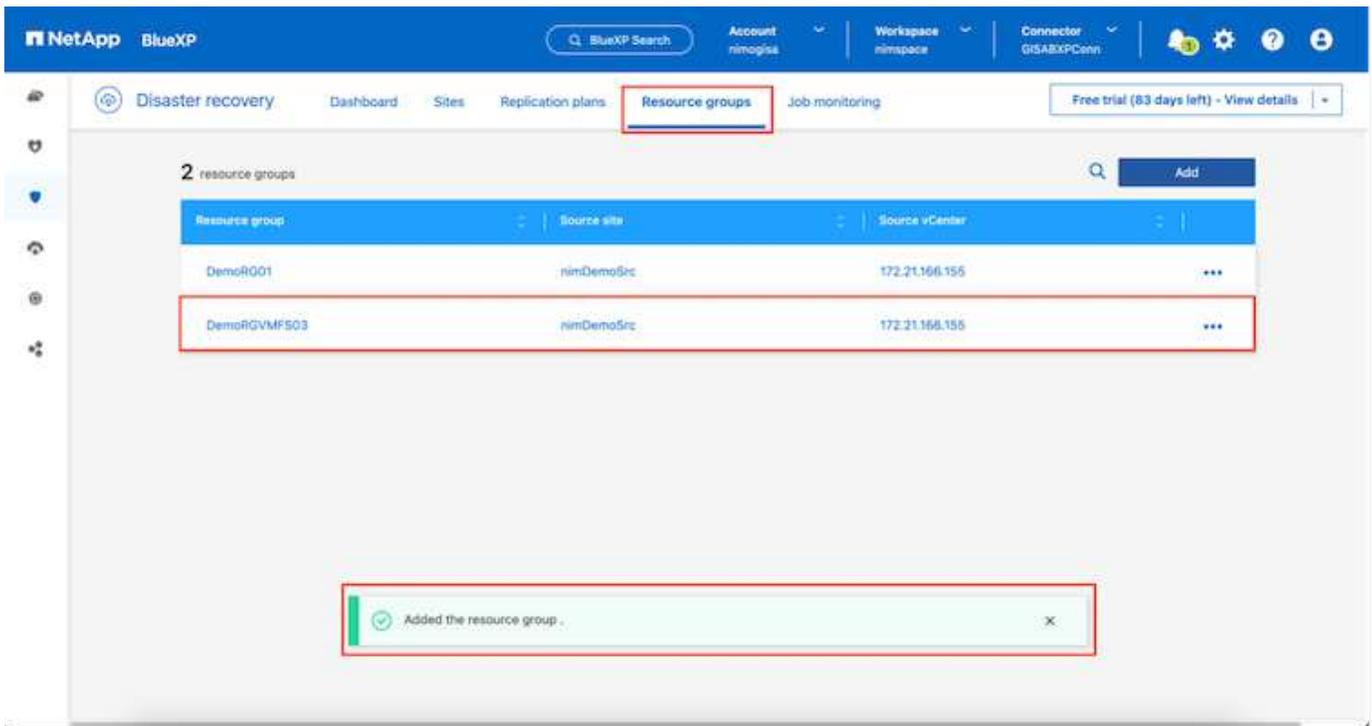
A parte gli approcci sopra indicati, è possibile creare la replica di SnapMirror anche tramite l'interfaccia a riga di comando di ONTAP o System Manager. Independentemente dall'approccio utilizzato per sincronizzare i dati utilizzando SnapMirror, BlueXP DRaaS orchestra il workflow per operazioni di disaster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

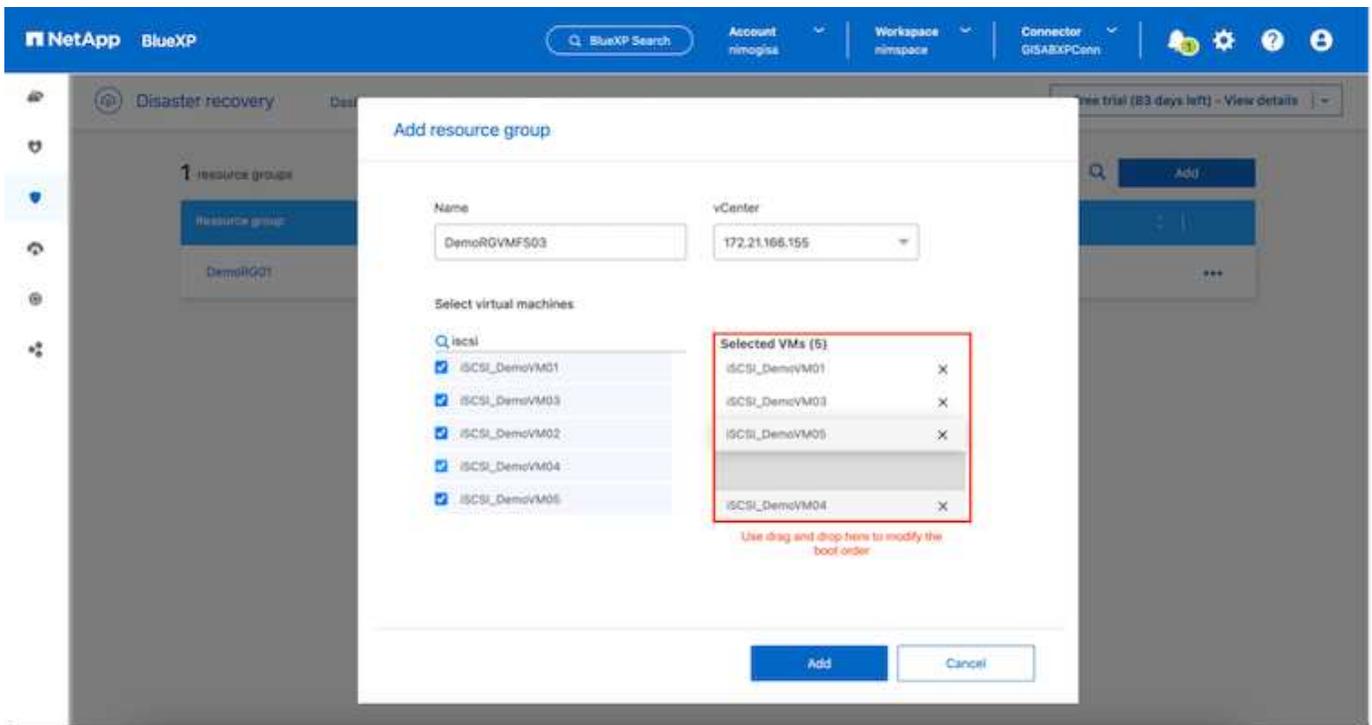


Una volta aggiunti i siti, è possibile raggruppare le macchine virtuali in gruppi di risorse. I gruppi di risorse per il disaster recovery di BlueXP consentono di raggruppare una serie di macchine virtuali dipendenti in gruppi logici che contengono gli ordini di avvio e i ritardi di avvio che possono 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**.

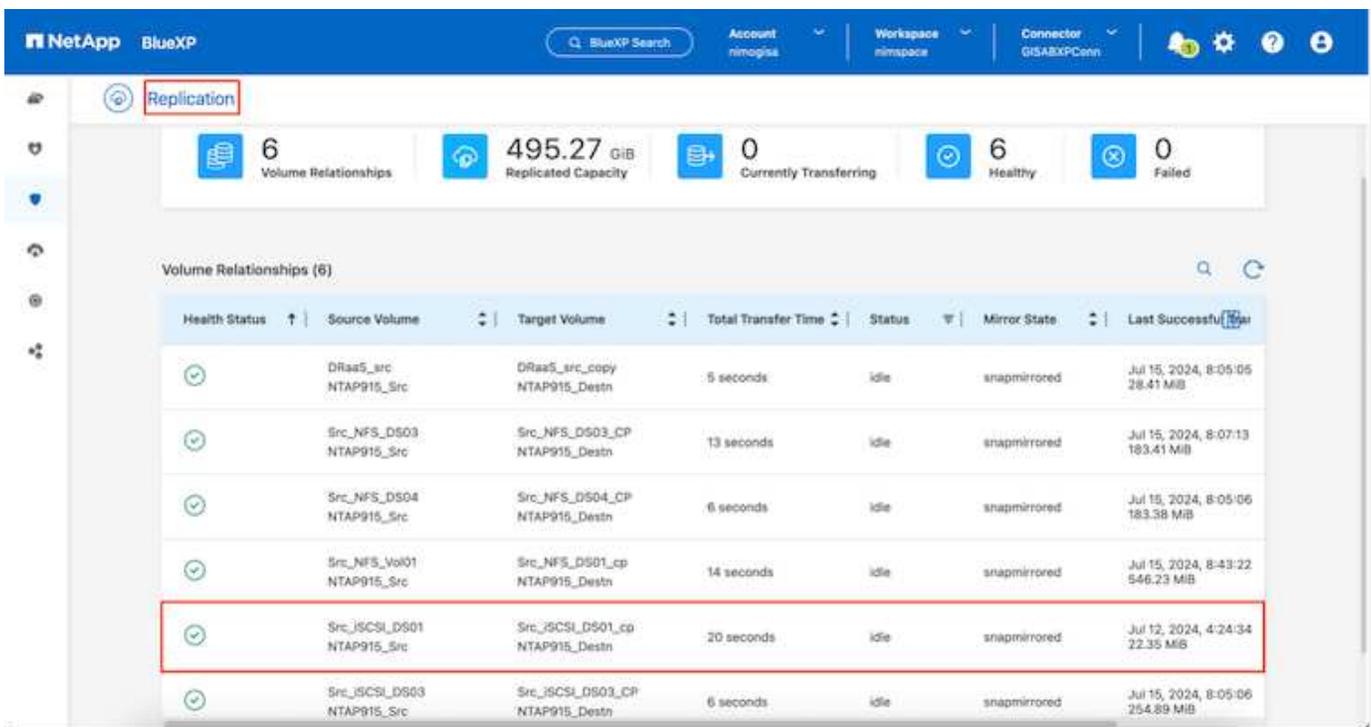
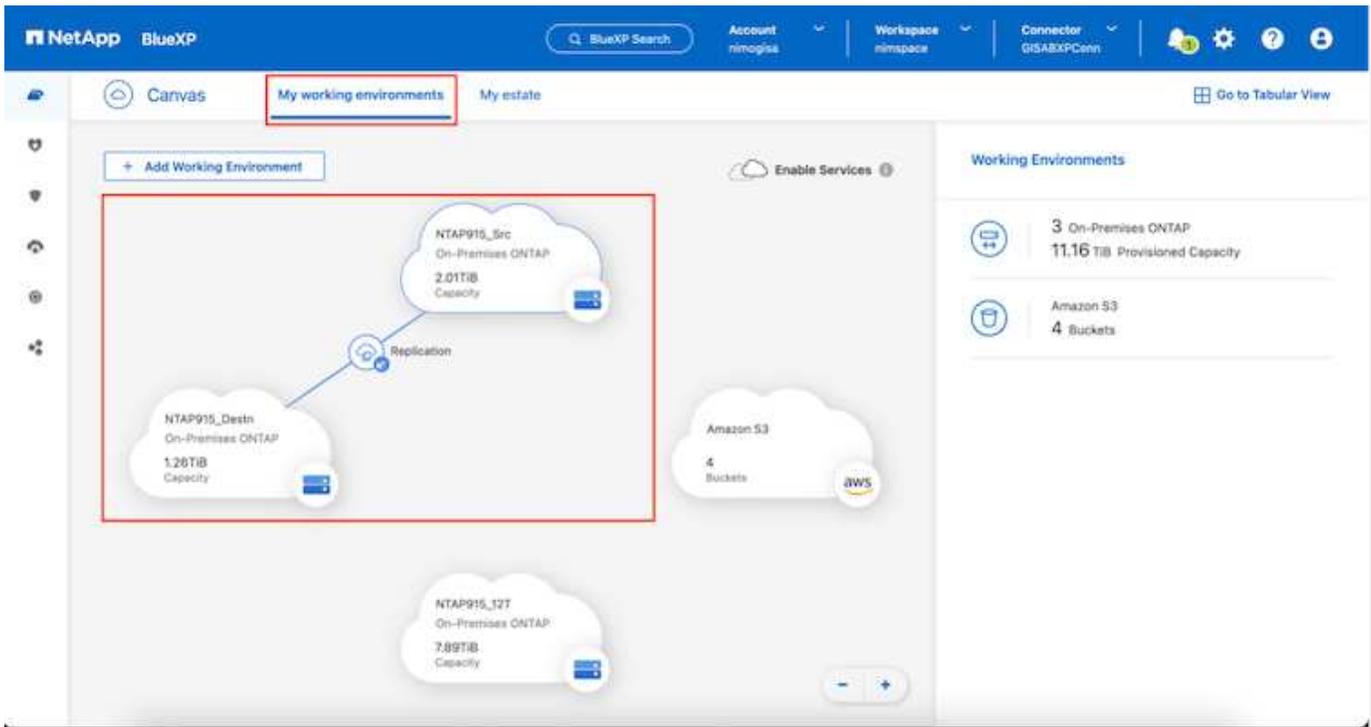


 Il gruppo di risorse può anche essere creato durante la creazione di un piano di replica.

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

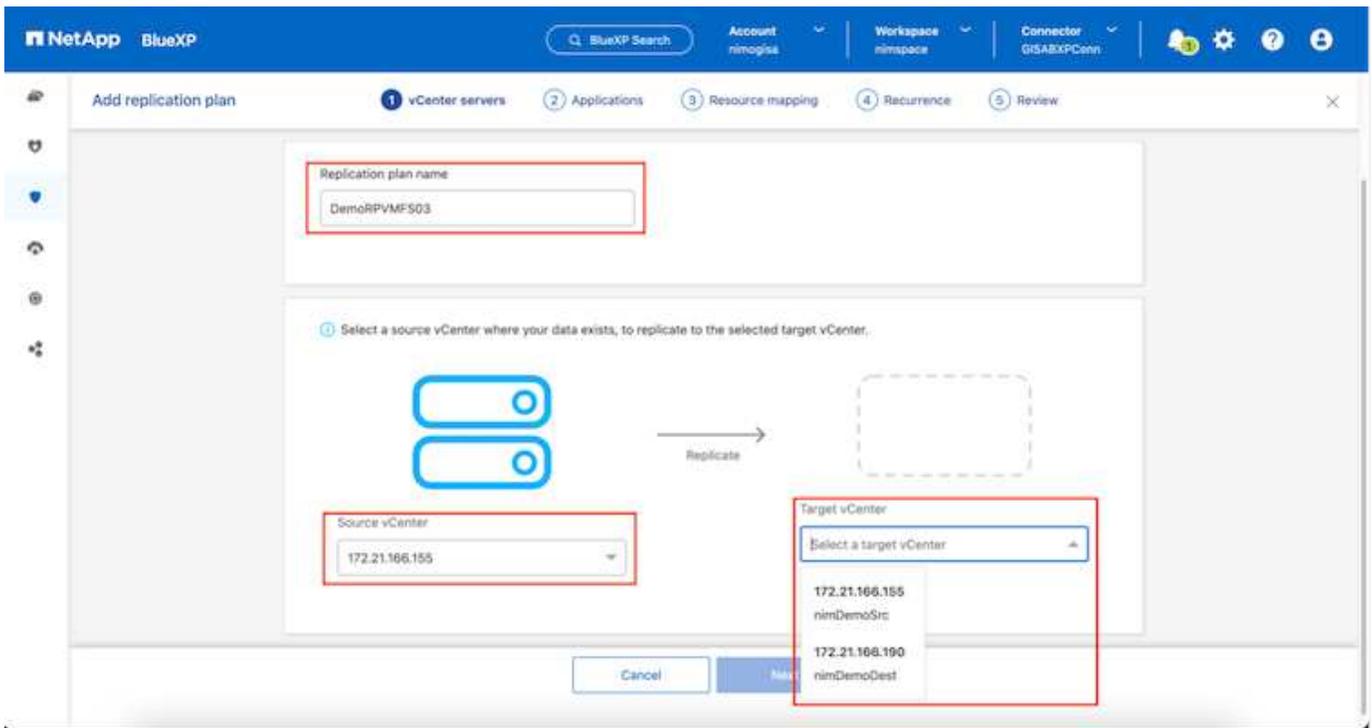


Una volta creati i gruppi di risorse, il passo successivo è creare il piano di esecuzione o un piano per il ripristino di macchine e applicazioni virtuali in caso di emergenza. Come menzionato nei prerequisiti, la replica di SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla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

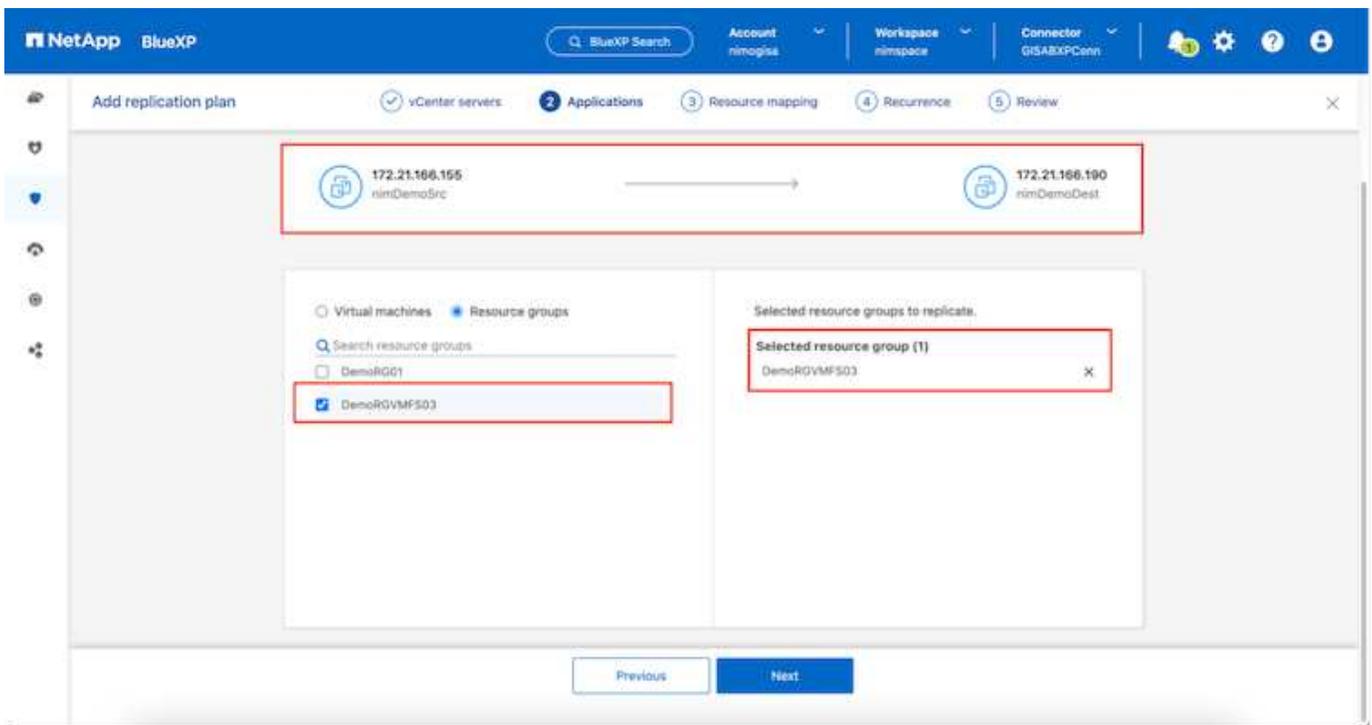


Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire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

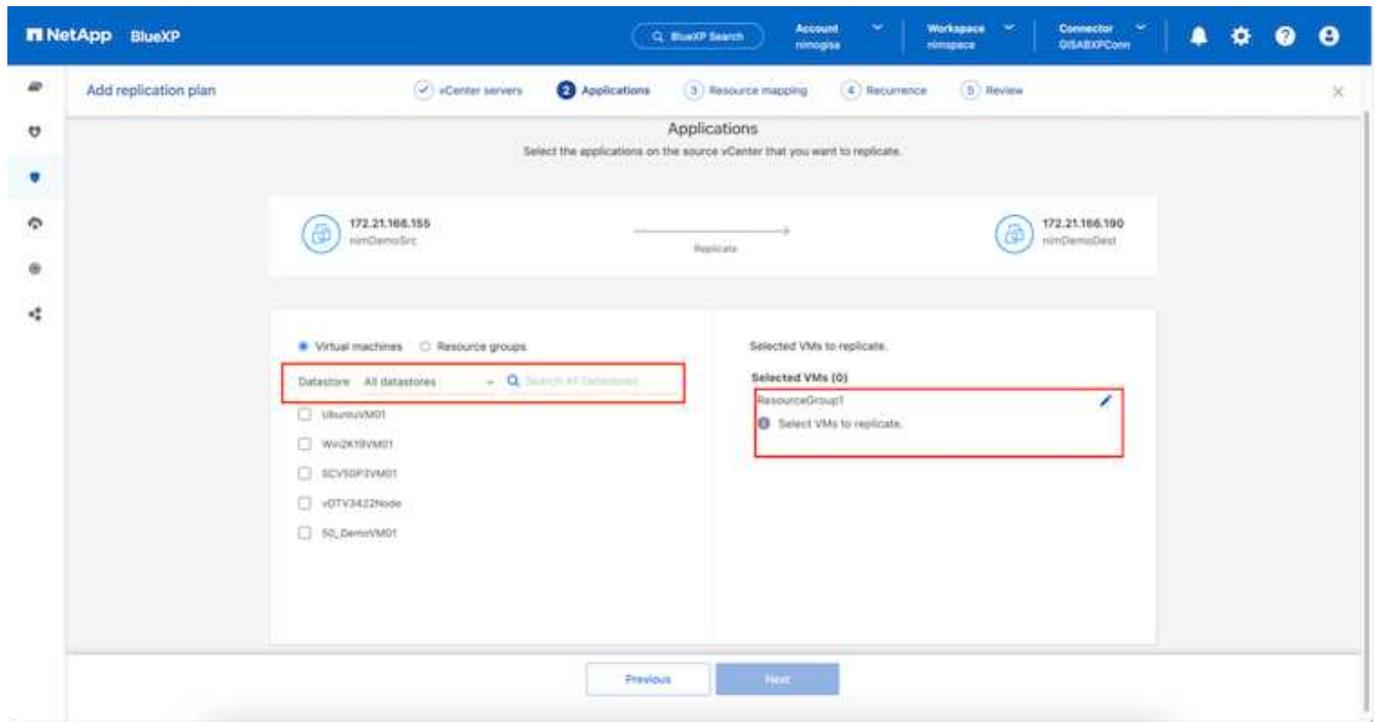


Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine di accensione delle macchine virtuali durante il processo di ripristino.

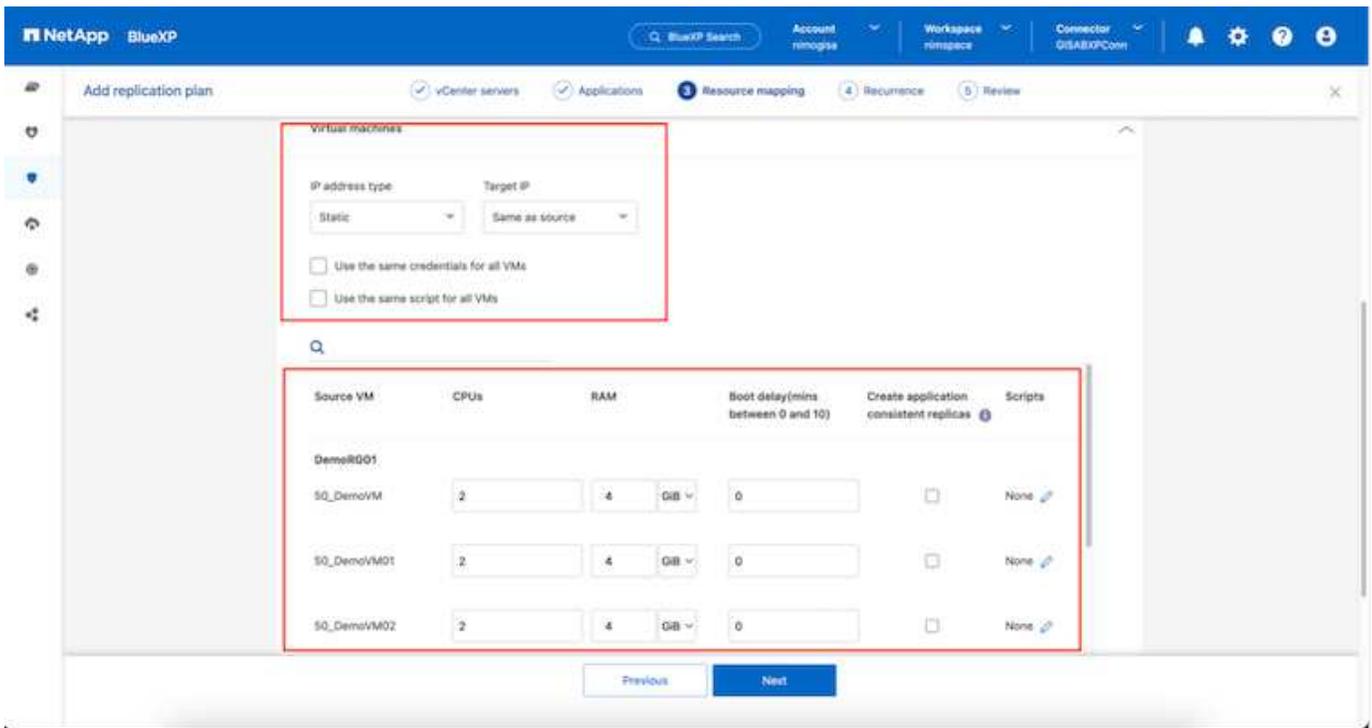


Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Due gruppi di risorse vengono avviati in parallelo.

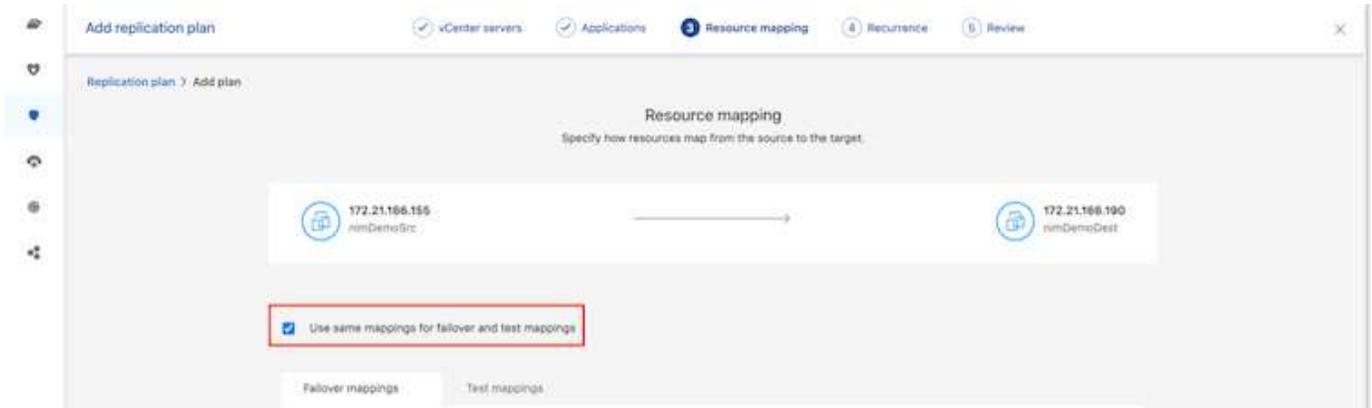
Lo screenshot seguente mostra la possibilità di filtrare le macchine virtuali o gli archivi dati specifici in base ai requisiti organizzativi se i gruppi di risorse non vengono creati in precedenza.



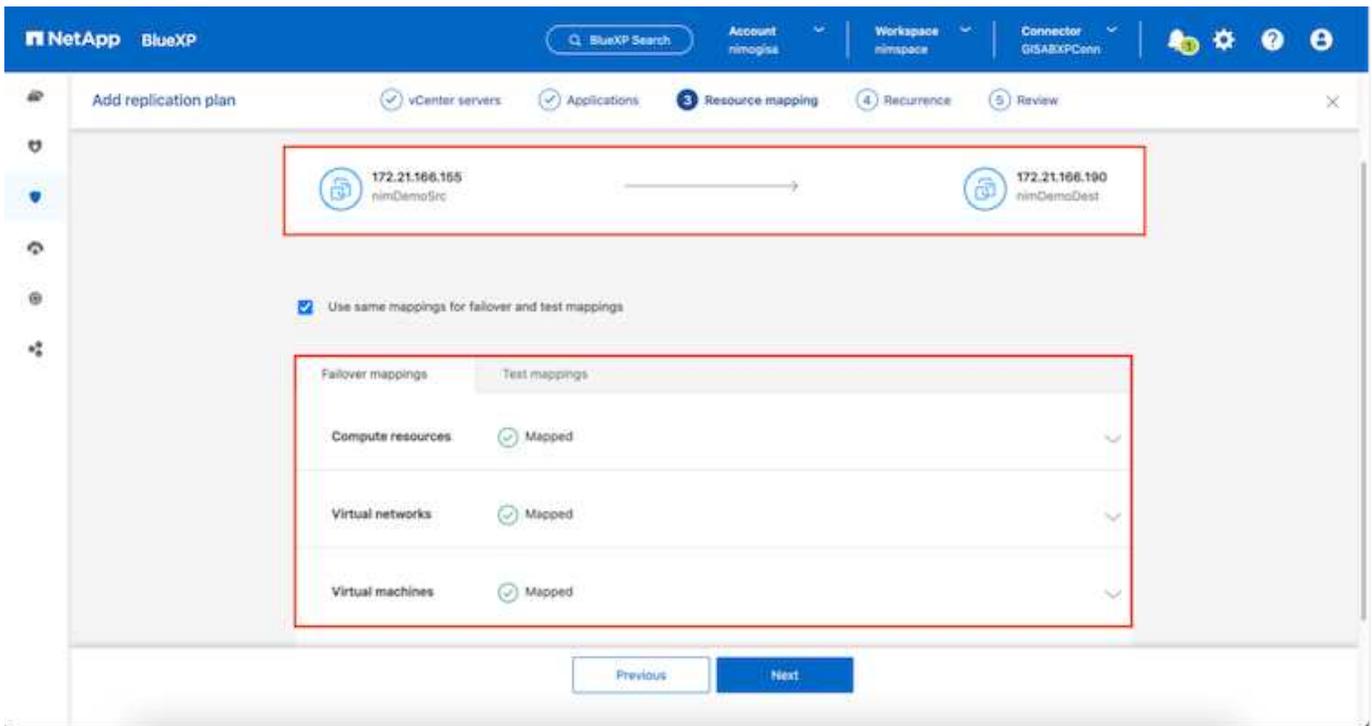
Una volta selezionati i gruppi di risorse, creare le mappature di failover. In questo passaggio, specificare il modo in cui le risorse dell'ambiente di origine vengono mappate alla destinazione. Sono incluse le risorse di elaborazione e le reti virtuali. Personalizzazione IP, pre e post-script, ritardi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



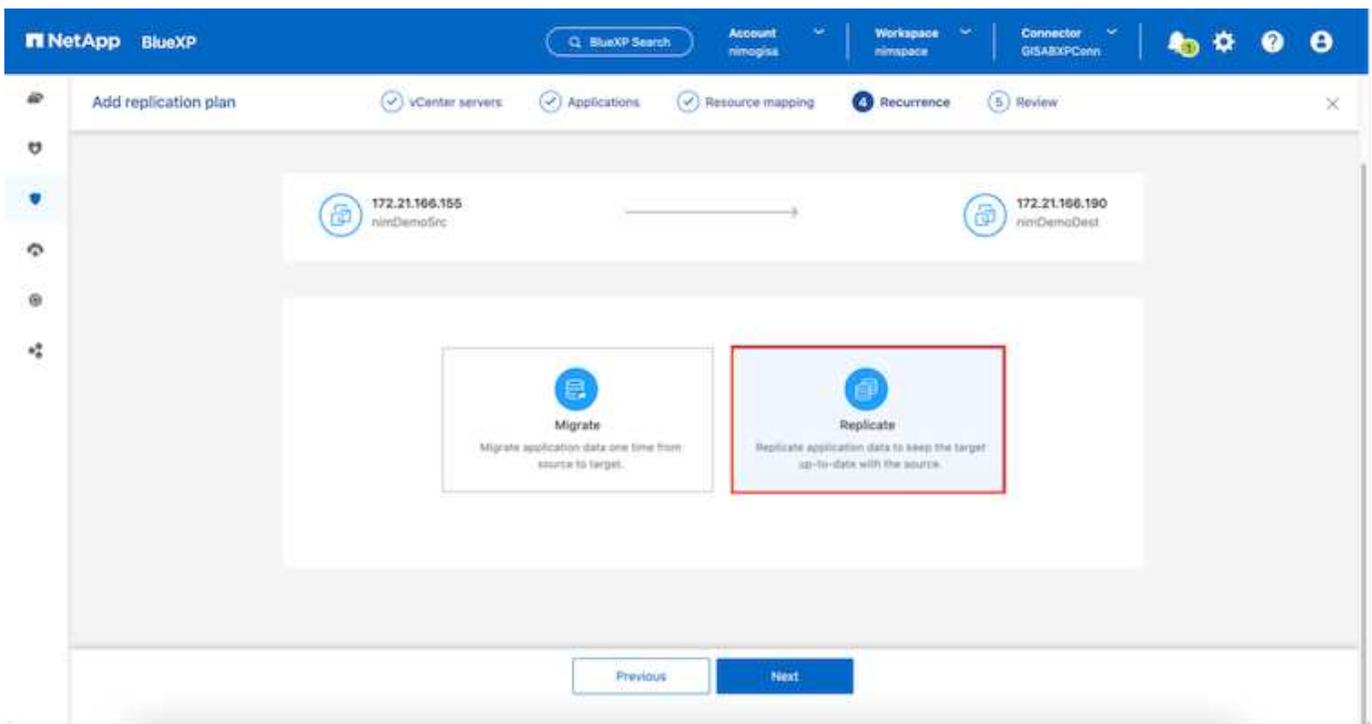
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per applicare mappature diverse per l'ambiente di test, selezionare l'opzione Test mapping (Test mapping) dopo aver deselezionato la casella di controllo come illustrato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



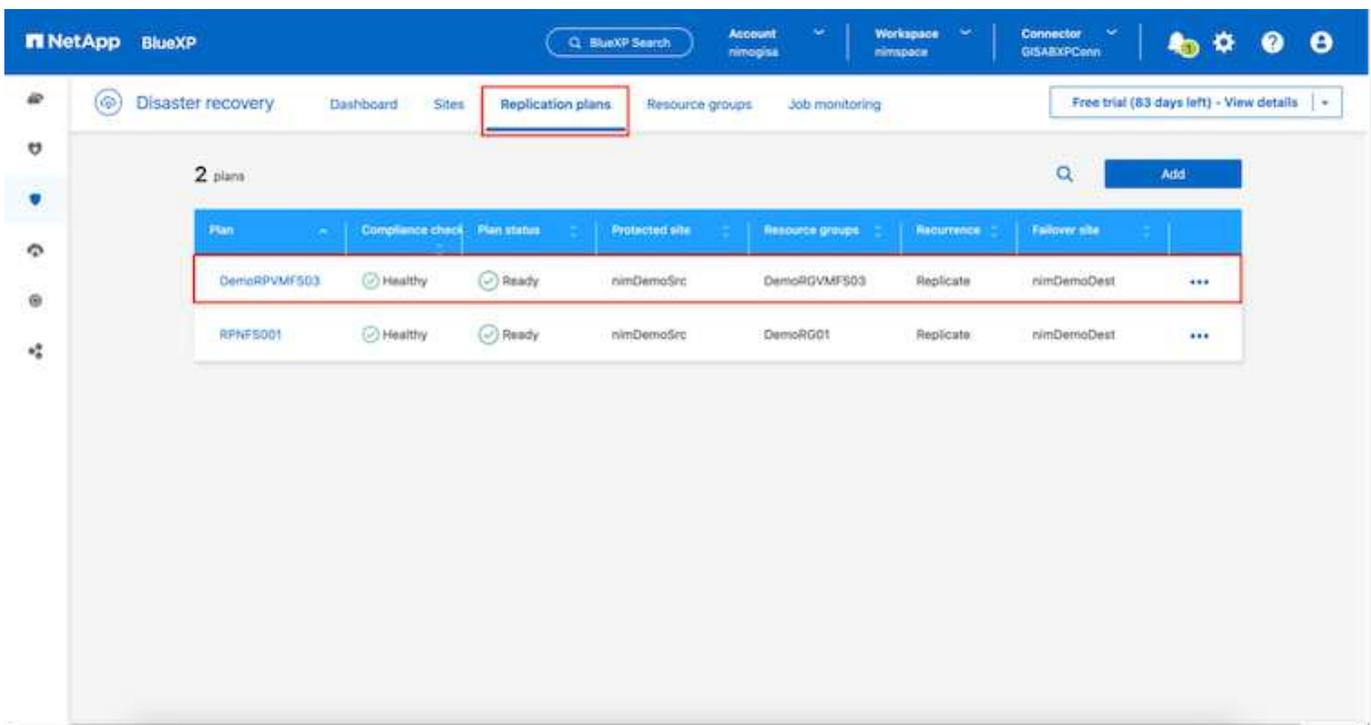
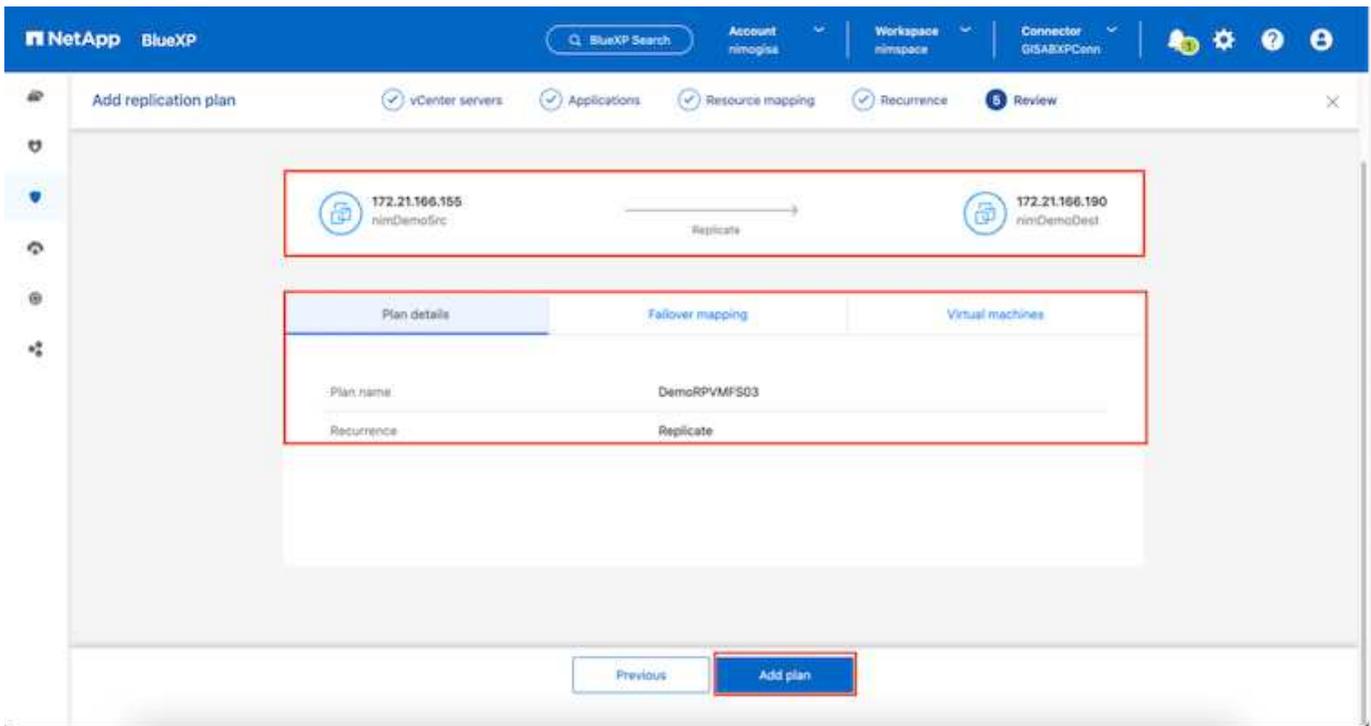
Una volta completata la mappatura delle risorse, fare clic su Avanti.



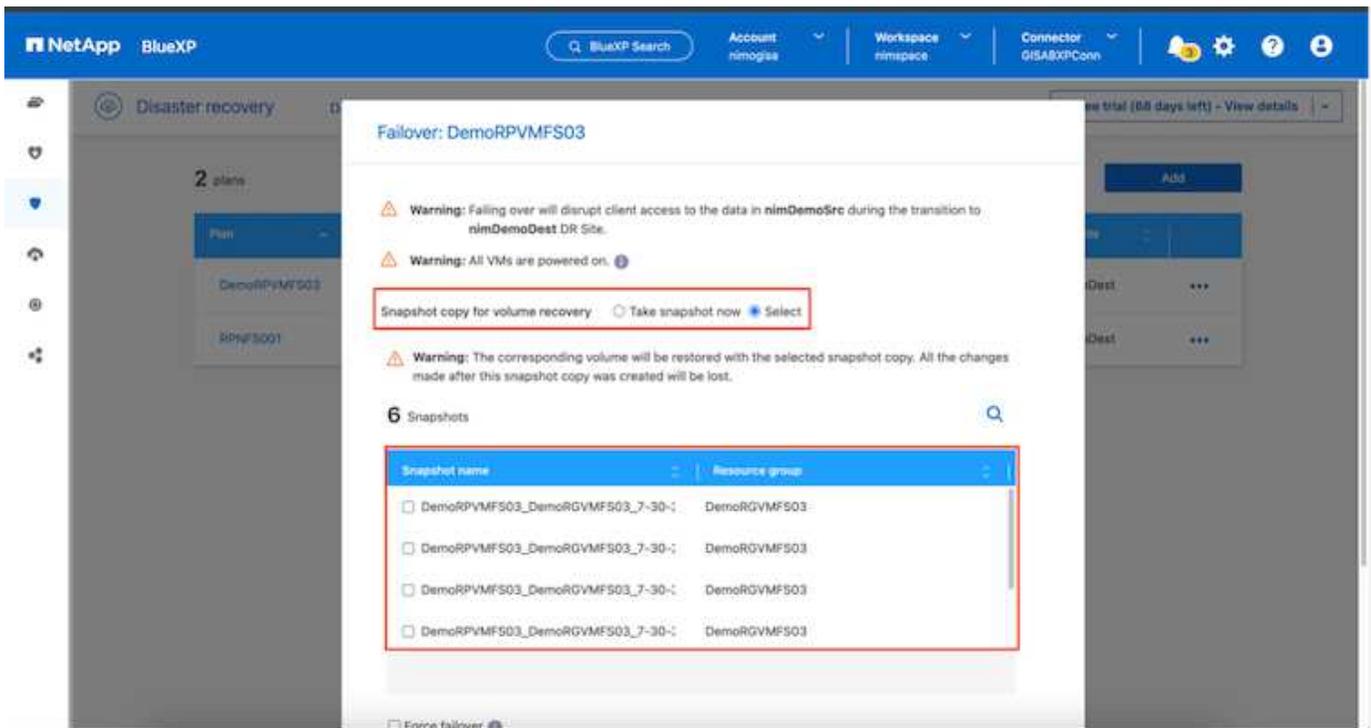
Selezionare il tipo di ricorrenza. In poche parole, selezionare l'opzione Migrate (migrazione una tantum tramite failover) o Replica continua ricorrente. In questa procedura dettagliata, l'opzione Replica è selezionata.



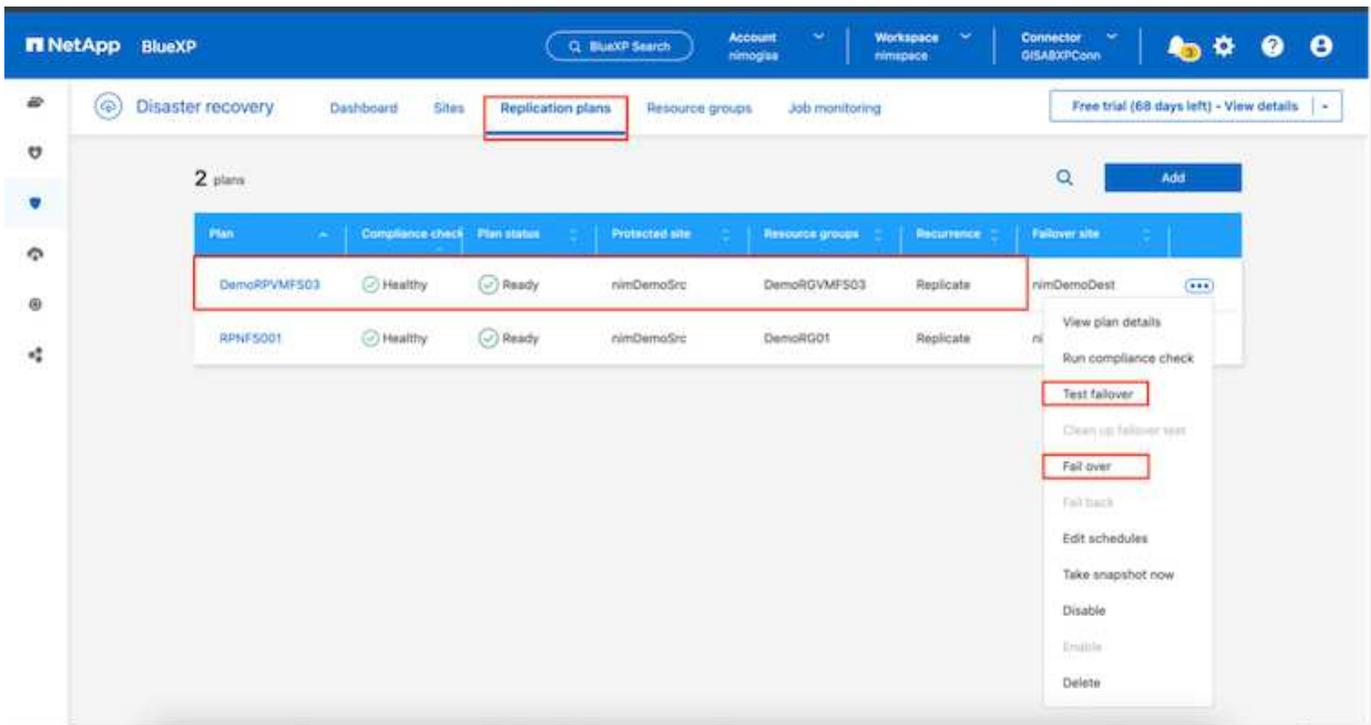
Al termine, rivedere le mappature create e fare clic su Aggiungi piano.



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?

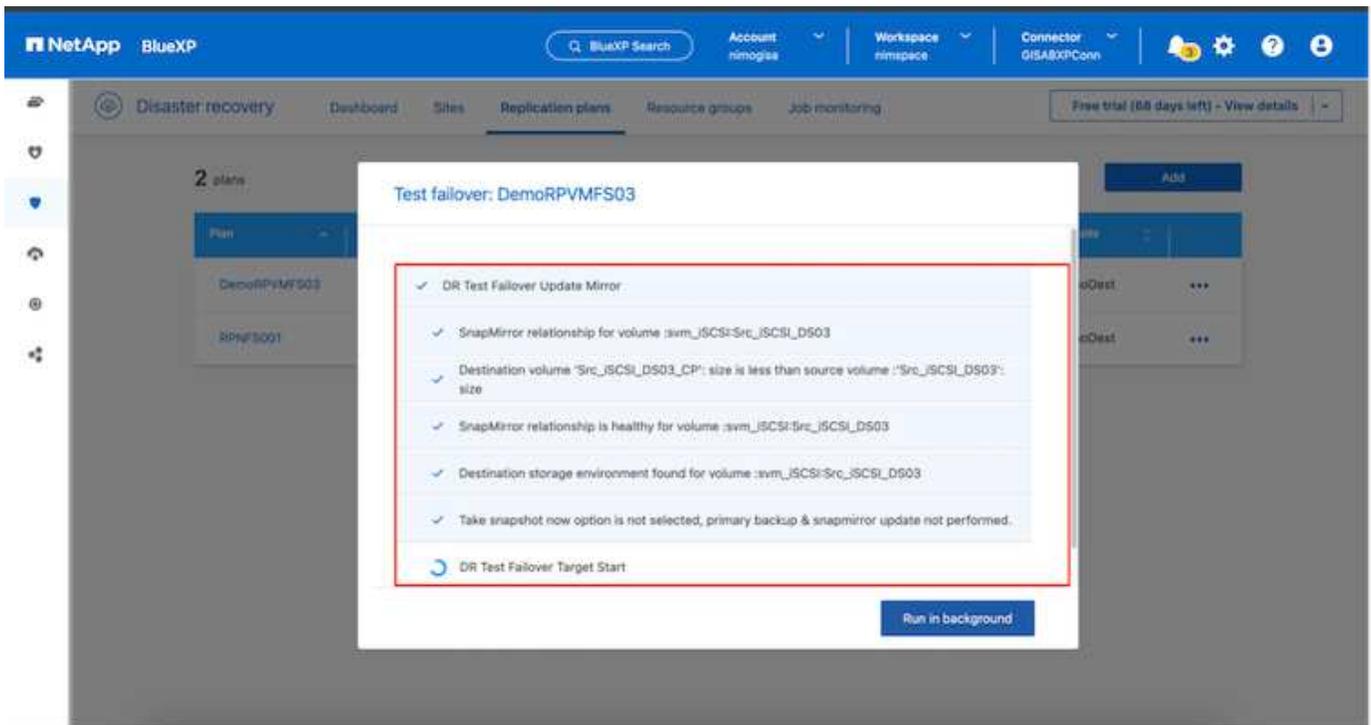
Durante un'operazione di failover di test, il disaster recovery di BlueXP crea un volume FlexClone sul sistema storage ONTAP di destinazione utilizzando l'ultima copia Snapshot o una snapshot selezionata del volume di destinazione.



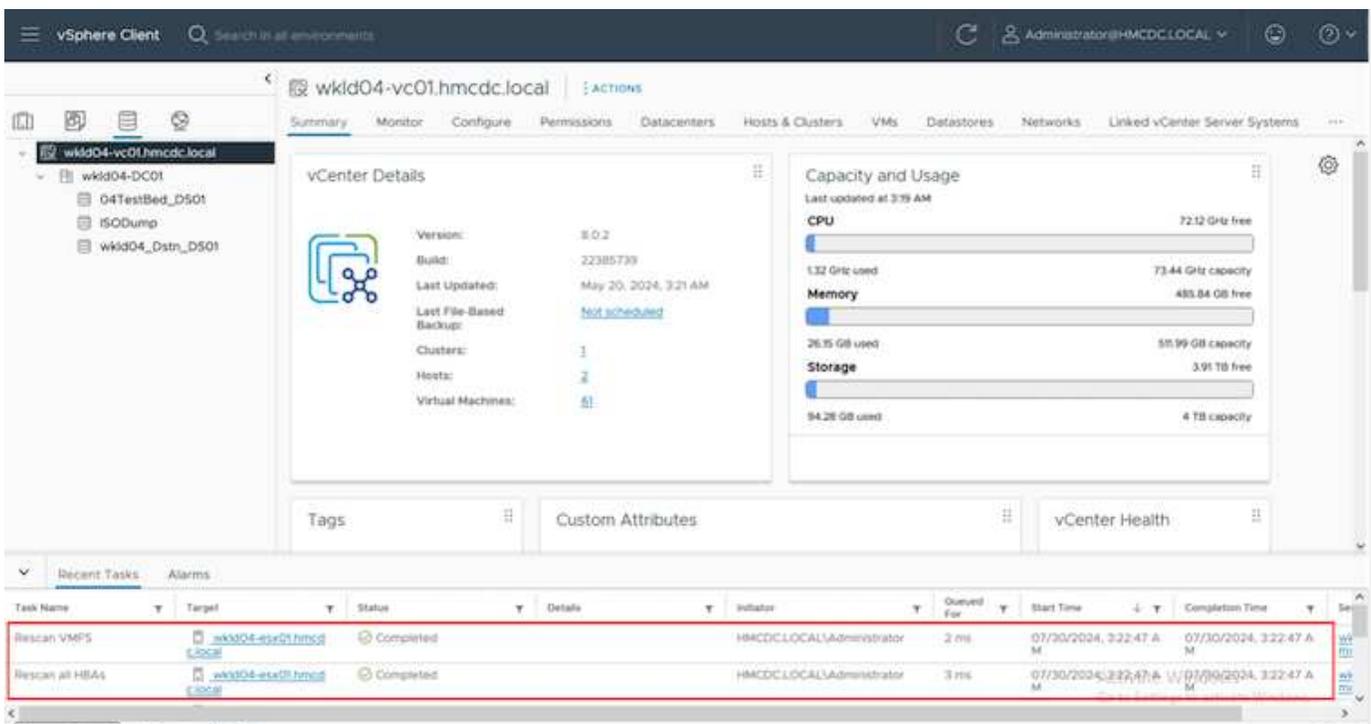
Un'operazione di test failover crea un volume clonato sul sistema di storage ONTAP di destinazione.

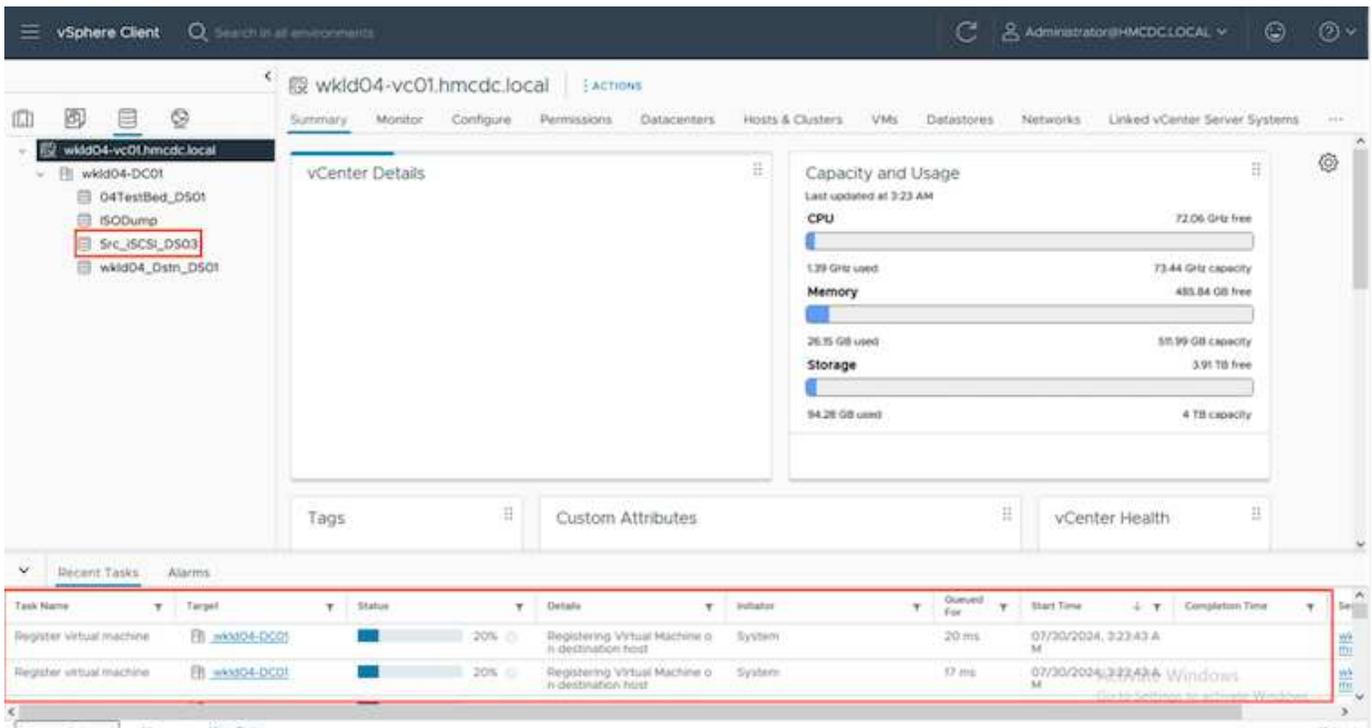


L'esecuzione di un'operazione di ripristino di prova non influisce sulla replica di SnapMirror.



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.

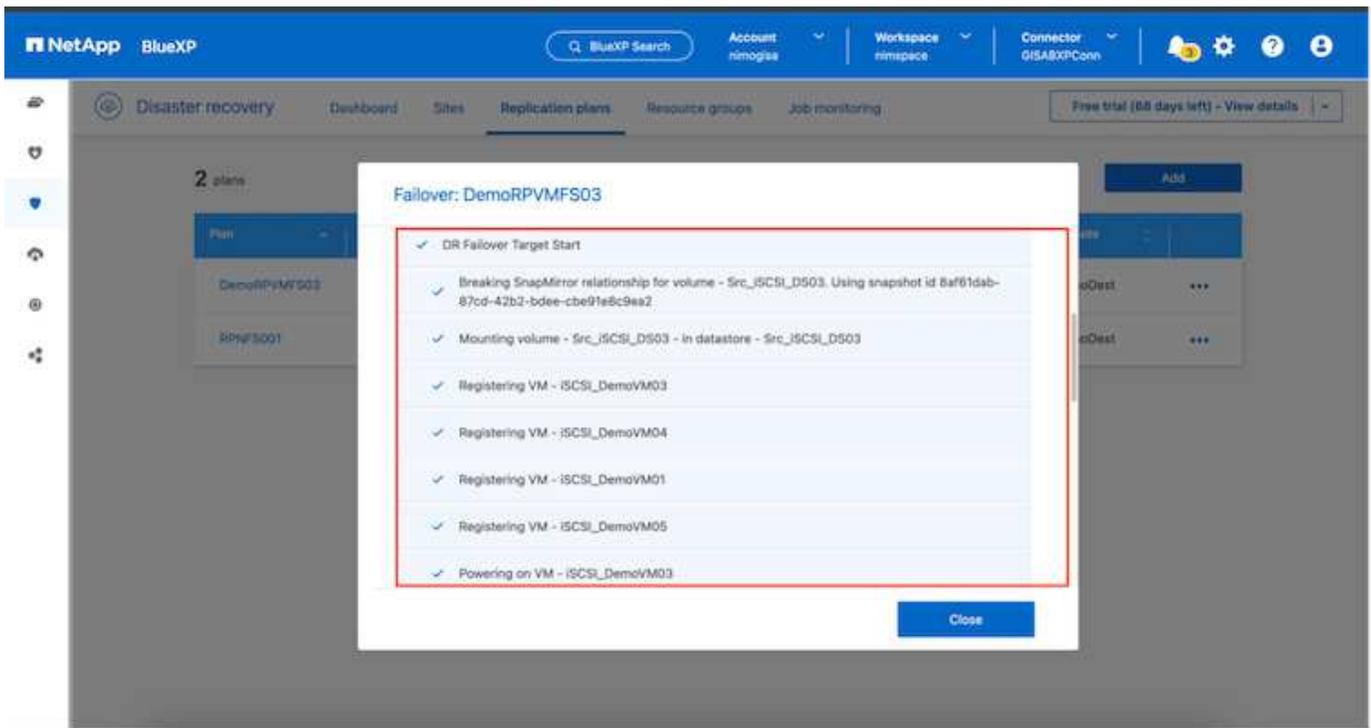




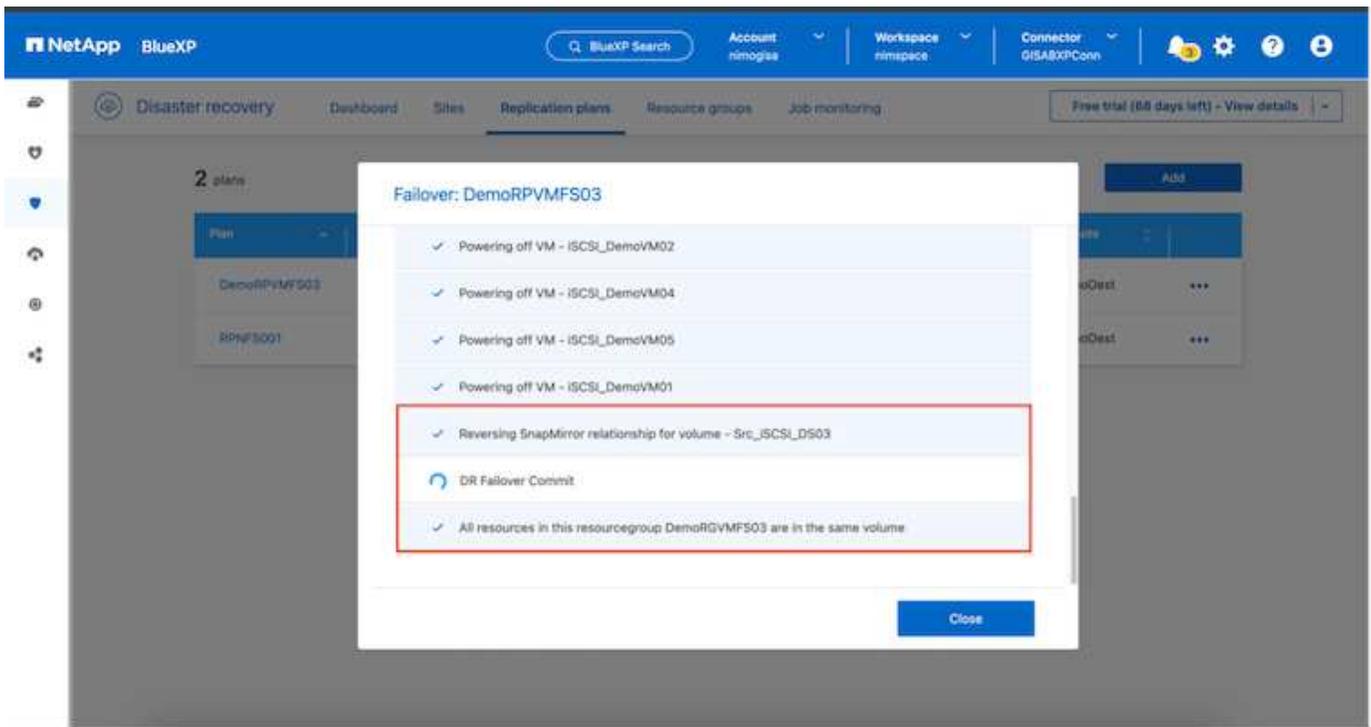
Al termine dell'operazione di failover di test, l'operazione di cleanup può essere attivata utilizzando **"Clean Up failover test"**. Durante questa operazione, il ripristino di emergenza BlueXP distrugge il volume FlexClone utilizzato nell'operazione.

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

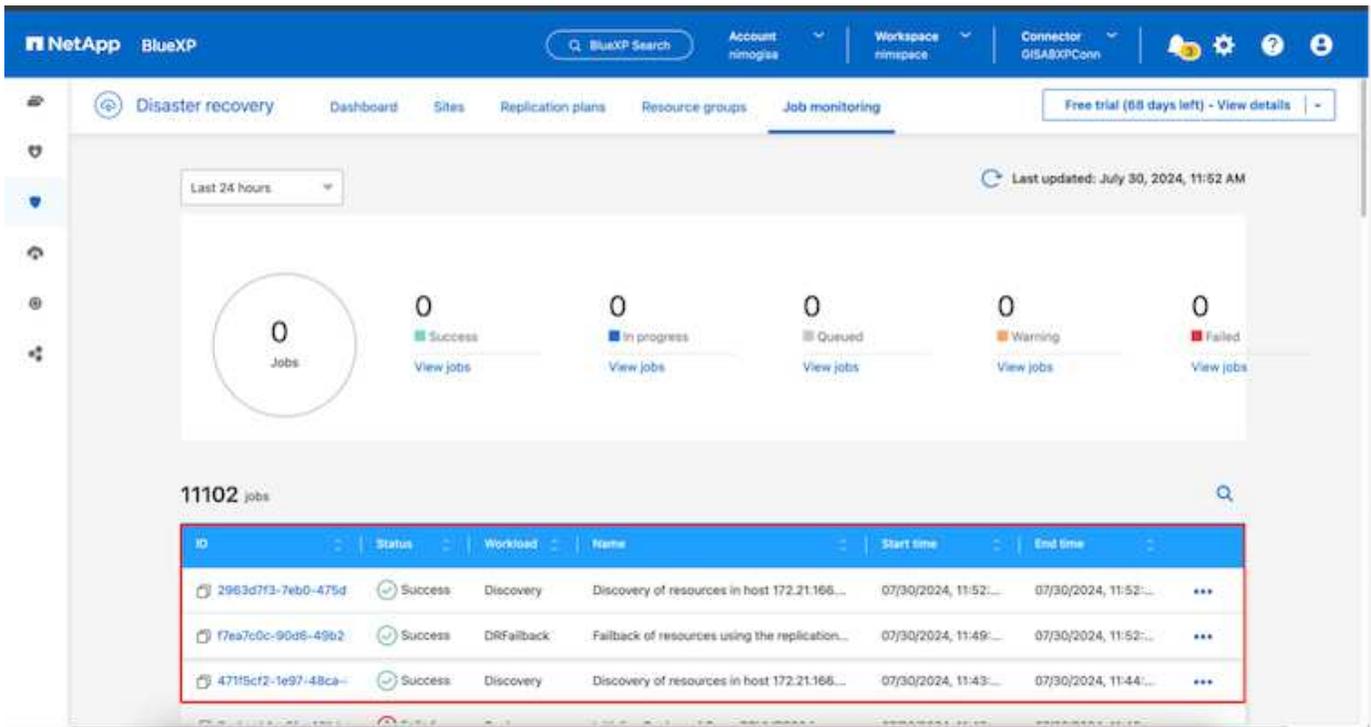


Una volta che il sito primario è in funzione, BlueXP Disaster Recovery abilita la risincronizzazione inversa di SnapMirror e abilita il failback, che può essere eseguito nuovamente con un semplice clic.



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

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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