Utilizzare NetApp Disaster Recovery

NetApp Disaster Recovery

NetApp
January 12, 2026

Sommario

Utilizzare NetApp Disaster Recovery

Panoramica di NetApp Disaster Recovery

Utilizzando NetApp Disaster Recovery, è possibile raggiungere i seguenti obiettivi:

- "Visualizza lo stato di salute dei tuoi piani di disaster recovery" .
- "Aggiungi siti vCenter" .
- "Crea gruppi di risorse per organizzare insieme le VM"
- "Creare un piano di ripristino in caso di disastro" .
- "Replicare le app VMware"dal tuo sito principale a un sito remoto di disaster recovery nel cloud utilizzando la replica SnapMirror .
- "Migrazione delle app VMware"dal tuo sito principale a un altro sito.
- "Testare il failover"senza interrompere le macchine virtuali originali.
- In caso di disastro,"esegui il failover del tuo sito primario" su VMware Cloud su AWS con FSx per NetApp ONTAP.
- Dopo che il disastro è stato risolto,"fallire indietro" dal sito di ripristino in caso di disastro al sito primario.
- "Monitorare le operazioni di ripristino in caso di disastro"nella pagina Monitoraggio lavori.

Visualizza lo stato dei tuoi piani NetApp Disaster Recovery sulla Dashboard

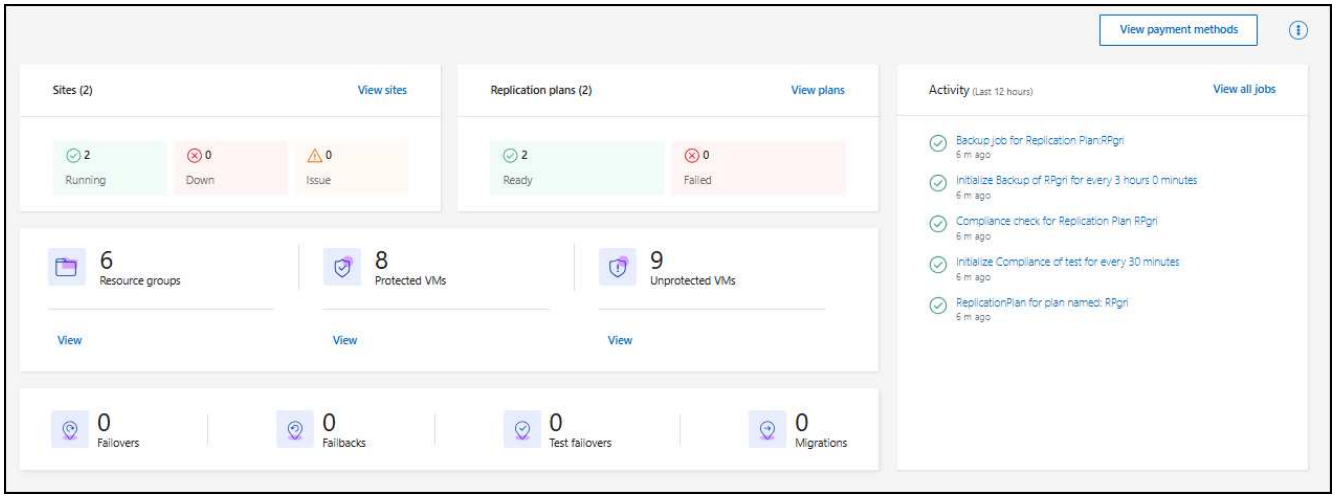
Utilizzando la dashboard di NetApp Disaster Recovery , puoi determinare lo stato di salute dei tuoi siti di disaster recovery e dei piani di replica. È possibile verificare rapidamente quali siti e piani sono integri, disconnessi o degradati.

Ruolo di NetApp Console obbligatorio Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore dell'applicazione di ripristino di emergenza o visualizzatore del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu NetApp Disaster Recovery , selezionare **Dashboard**.



4. Esaminare le seguenti informazioni sulla Dashboard:
   - **Siti**: visualizza lo stato di salute dei tuoi siti. Un sito può avere uno dei seguenti stati:
     - **In esecuzione**: vCenter è connesso, funzionante e funzionante.
     - **Giù**: vCenter non è raggiungibile o presenta problemi di connettività.
     - **Problema**: vCenter non è raggiungibile o presenta problemi di connettività.

       Per visualizzare i dettagli del sito, seleziona **Visualizza tutto** per uno stato oppure **Visualizza siti** per visualizzarli tutti.
   - **Piani di replicazione**: visualizza lo stato di avanzamento dei tuoi piani. Un piano può avere uno dei seguenti stati:
     - **Pronto**
     - **Fallito**

       Per rivedere i dettagli del piano di replicazione, selezionare **Visualizza tutto** per uno stato oppure **Visualizza piani di replicazione** per visualizzarli tutti.
   - **Gruppi di risorse**: visualizza lo stato di integrità dei tuoi gruppi di risorse. Un gruppo di risorse può avere uno dei seguenti stati:
   - **VM protette**: le VM fanno parte di un gruppo di risorse.
   - **VM non protette**: le VM non fanno parte di un gruppo di risorse.

     Per rivedere i dettagli, seleziona il link **Visualizza** sotto ciascuno.
   - Numero di failover, failover di test e migrazioni. Ad esempio, se hai creato due piani e hai effettuato la migrazione alle destinazioni, il conteggio delle migrazioni verrà visualizzato come "2".
5. Esaminare tutte le operazioni nel riquadro Attività. Per visualizzare tutte le operazioni sul Job Monitor, selezionare **Visualizza tutti i lavori**.

Aggiungere vCenter a un sito in NetApp Disaster Recovery

Prima di poter creare un piano di disaster recovery, è necessario aggiungere un server vCenter primario a un sito e un sito di disaster recovery vCenter di destinazione nella NetApp Console.

Assicurarsi che sia il vCenter di origine che quello di destinazione utilizzino lo stesso agente NetApp Console .

Dopo aver aggiunto i vCenter, NetApp Disaster Recovery esegue un'analisi approfondita degli ambienti vCenter, inclusi cluster vCenter, host ESXi, datastore, spazio di archiviazione, dettagli delle macchine virtuali, repliche SnapMirror e reti di macchine virtuali.

*Ruolo richiesto NetApp Console * Amministratore dell'organizzazione, Amministratore di cartelle o progetti o Amministratore del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Informazioni su questo compito

Se hai aggiunto vCenter nelle versioni precedenti e desideri personalizzare la pianificazione dell'individuazione, devi modificare il sito del server vCenter e impostare la pianificazione.

NetApp Disaster Recovery esegue la rilevazione una volta ogni 24 ore. Dopo aver configurato un sito, puoi modificare in seguito vCenter per personalizzare la pianificazione dell'individuazione in base alle tue esigenze. Ad esempio, se si dispone di un numero elevato di VM, è possibile impostare la pianificazione dell'individuazione in modo che venga eseguita ogni 23 ore e 59 minuti. Se si dispone di un numero limitato di VM, è possibile impostare la pianificazione dell'individuazione in modo che venga eseguita ogni 12 ore. L'intervallo minimo è di 30 minuti e quello massimo è di 24 ore.

Per ottenere le informazioni più aggiornate sul tuo ambiente, dovresti prima eseguire alcune rilevazioni manuali. Dopodiché puoi impostare la pianificazione in modo che venga eseguita automaticamente.

Se si dispone di vCenter di versioni precedenti e si desidera modificare il momento in cui viene eseguita l'individuazione, modificare il sito del server vCenter e impostare la pianificazione.

Le VM appena aggiunte o eliminate vengono riconosciute durante la successiva individuazione pianificata o durante un'individuazione manuale immediata.

Le VM possono essere protette solo se il piano di replica si trova in uno dei seguenti stati:

- Pronto
- Failback eseguito
- Test failover eseguito

Cluster vCenter in un sito Ogni sito contiene uno o più vCenter. Questi vCenter utilizzano uno o più cluster di storage ONTAP per ospitare datastore NFS o VMFS.

Un cluster vCenter può risiedere in un solo sito. Per aggiungere un cluster vCenter a un sito, sono necessarie le seguenti informazioni:

- L'indirizzo IP di gestione vCenter o FQDN
- Credenziali per un account vCenter con i privilegi richiesti per eseguire le operazioni. Vedere"privilegi vCenter richiesti" per maggiori informazioni.
- Per i siti VMware ospitati nel cloud, le chiavi di accesso al cloud richieste
- Un certificato di sicurezza per accedere al tuo vCenter.

Il servizio supporta certificati di sicurezza autofirmati o certificati provenienti da un'autorità di certificazione (CA) centrale.

Passi

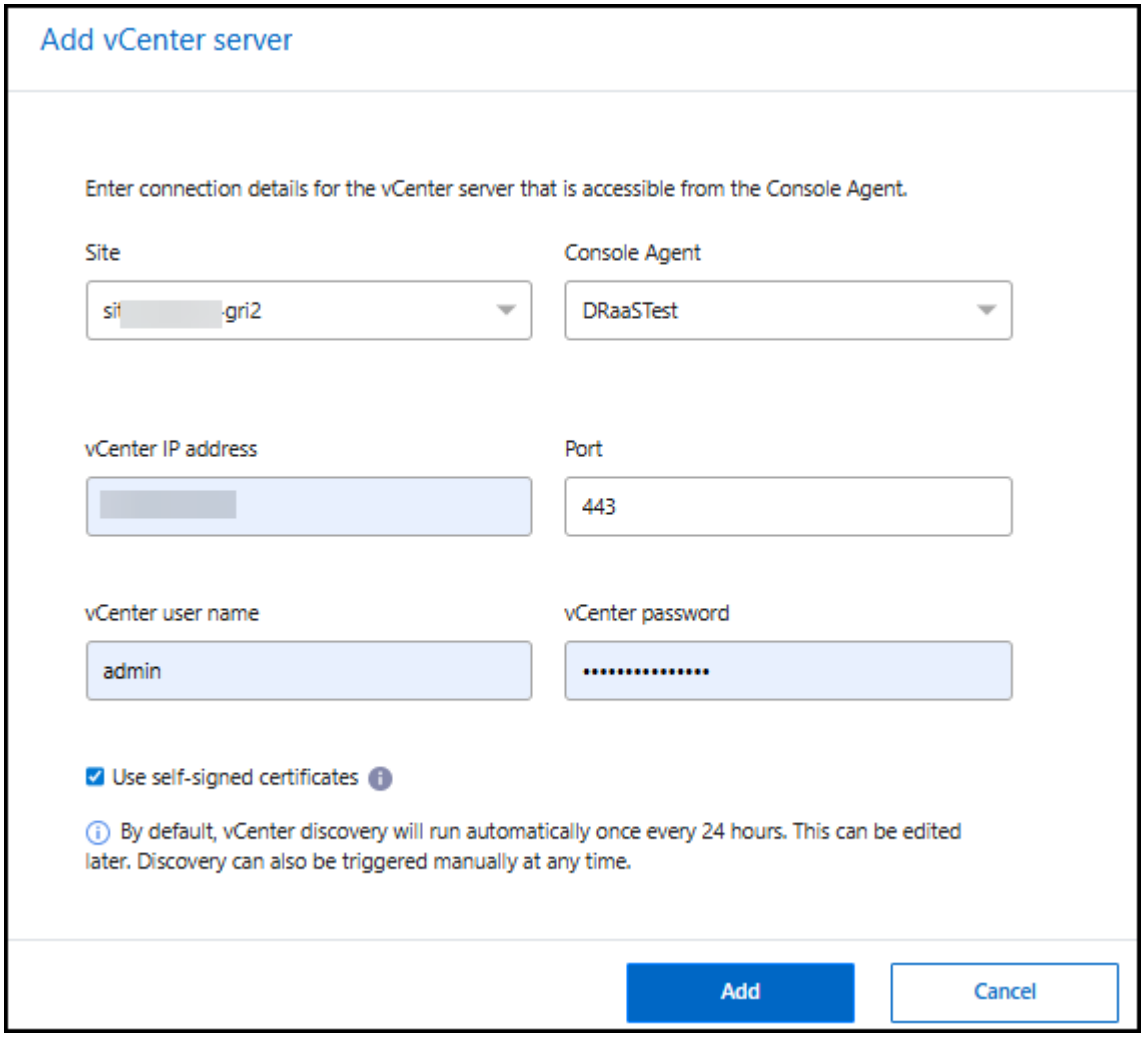
1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.

   Se è la prima volta che utilizzi NetApp Disaster Recovery, devi aggiungere le informazioni di vCenter. Se hai già aggiunto informazioni vCenter, vedrai la dashboard.

   A seconda del tipo di sito che stai aggiungendo, vengono visualizzati campi diversi.

3. Se esistono già alcuni siti vCenter e si desidera aggiungerne altri, selezionare **Siti** dal menu, quindi selezionare **Aggiungi**.
4. Nella pagina Siti, seleziona il sito e seleziona **Aggiungi vCenter**.
5. **Origine**: selezionare **Scopri server vCenter** per immettere informazioni sul sito vCenter di origine.

   Per aggiungere altri siti vCenter, selezionare **Siti**, quindi **Aggiungi**.



   - Selezionare un sito, quindi l'agente NetApp Console e fornire le credenziali vCenter.

- **Solo per siti on-premise:** Per accettare certificati autofirmati per il vCenter di origine, selezionare la casella.

> I certificati autofirmati non sono sicuri quanto gli altri certificati. Se il tuo vCenter **NON** è configurato con certificati dell'autorità di certificazione (CA), dovresti selezionare questa casella; in caso contrario, la connessione al vCenter non funzionerà.

6. Selezionare **Aggiungi**.

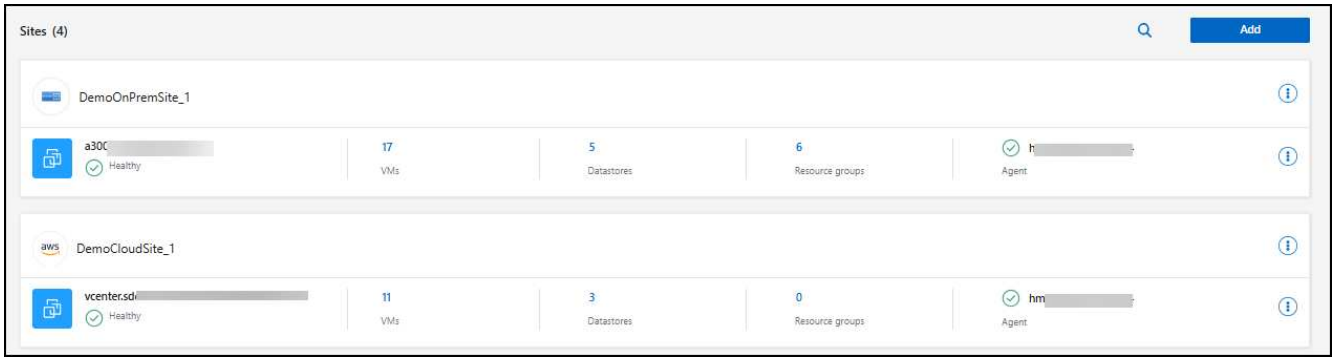
   Quindi aggiungere un vCenter di destinazione.

7. Aggiungere nuovamente un sito per il vCenter di destinazione.
8. Di nuovo, seleziona **Aggiungi vCenter** e aggiungi le informazioni sul vCenter di destinazione.
9. **Bersaglio**:

   a. Scegli il sito di destinazione e la posizione. Se la destinazione è il cloud, selezionare **AWS**.
      - (Si applica solo ai siti cloud) **Token API**: inserisci il token API per autorizzare l'accesso al servizio per la tua organizzazione. Crea il token API specificando ruoli specifici di organizzazione e servizio.
      - (Si applica solo ai siti cloud) **ID organizzazione lungo**: immettere l'ID univoco per l'organizzazione. È possibile identificare questo ID facendo clic sul nome utente nella sezione Account della NetApp Console.

   b. Selezionare **Aggiungi**.

      I vCenter di origine e di destinazione vengono visualizzati nell'elenco dei siti.



10. Per visualizzare l'avanzamento dell'operazione, dal menu selezionare **Monitoraggio lavori**.

Aggiungere la mappatura della subnet per un sito vCenter

È possibile gestire gli indirizzi IP nelle operazioni di failover utilizzando la mappatura delle subnet, che consente di aggiungere subnet per ciascun vCenter. In questo modo si definiscono il CIDR IPv4, il gateway predefinito e il DNS per ogni rete virtuale.

In caso di failover, NetApp Disaster Recovery utilizza il CIDR della rete mappata per assegnare a ciascuna vNIC un nuovo indirizzo IP.

Per esempio:

- ReteA = 10.1.1.0/24
- ReteB = 192.168.1.0/24

VM1 ha una vNIC (10.1.1.50) connessa alla ReteA. Nelle impostazioni del piano di replica, la rete A è mappata sulla rete B.

In caso di failover, NetApp Disaster Recovery sostituisce la parte di rete dell'indirizzo IP originale (10.1.1) e mantiene l'indirizzo host (.50) dell'indirizzo IP originale (10.1.1.50). Per VM1, NetApp Disaster Recovery esamina le impostazioni CIDR per NetworkB e utilizza la porzione di rete NetworkB 192.168.1, mantenendo la porzione host (.50) per creare il nuovo indirizzo IP per VM1. Il nuovo IP diventa 192.168.1.50.

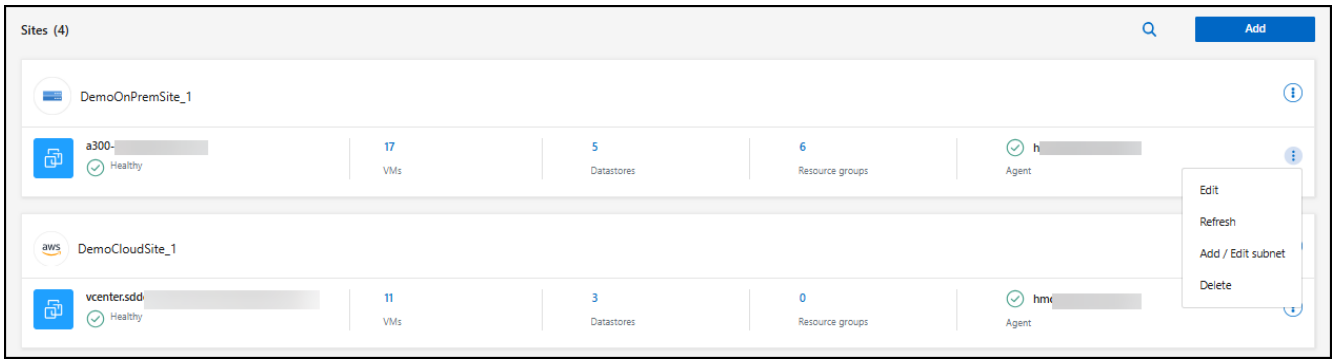
In sintesi, l'indirizzo host rimane lo stesso, mentre l'indirizzo di rete viene sostituito con quello configurato nella mappatura della subnet del sito. Ciò consente di gestire più facilmente la riassegnazione degli indirizzi IP in caso di failover, soprattutto se si hanno centinaia di reti e migliaia di VM da gestire.

L'utilizzo della mappatura delle subnet è un processo facoltativo in due fasi:

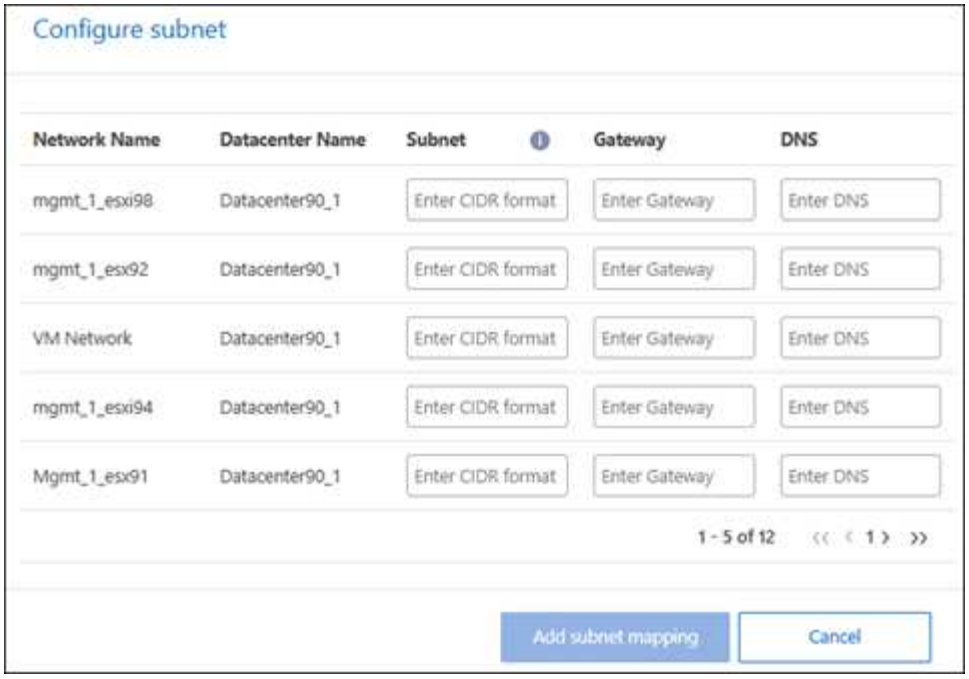
- Per prima cosa, aggiungi la mappatura della subnet per ogni sito vCenter.
- In secondo luogo, nel piano di replicazione, indicare che si desidera utilizzare il mapping delle subnet nella scheda Macchine virtuali e nel campo IP di destinazione.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Siti**.
2. Dalle azioni icona a destra, seleziona **Aggiungi subnet**.



Viene visualizzata la pagina Configura subnet:



3. Nella pagina Configura subnet, immettere le seguenti informazioni:
   a. Subnet: immettere il CIDR IPv4 per la subnet fino a /32.

> La notazione CIDR è un metodo per specificare gli indirizzi IP e le relative maschere di rete. /24 indica la netmask. Il numero è costituito da un indirizzo IP, in cui il numero dopo "/" indica quanti bit dell'indirizzo IP indicano la rete. Ad esempio, 192.168.0.50/24, l'indirizzo IP è 192.168.0.50 e il numero totale di bit nell'indirizzo di rete è 24. 192.168.0.50 255.255.255.0 diventa 192.168.0.0/24.

   b. Gateway: immettere il gateway predefinito per la subnet.
   c. DNS: immettere il DNS per la subnet.
4. Selezionare **Aggiungi mappatura subnet**.

Selezionare la mappatura della subnet per un piano di replicazione

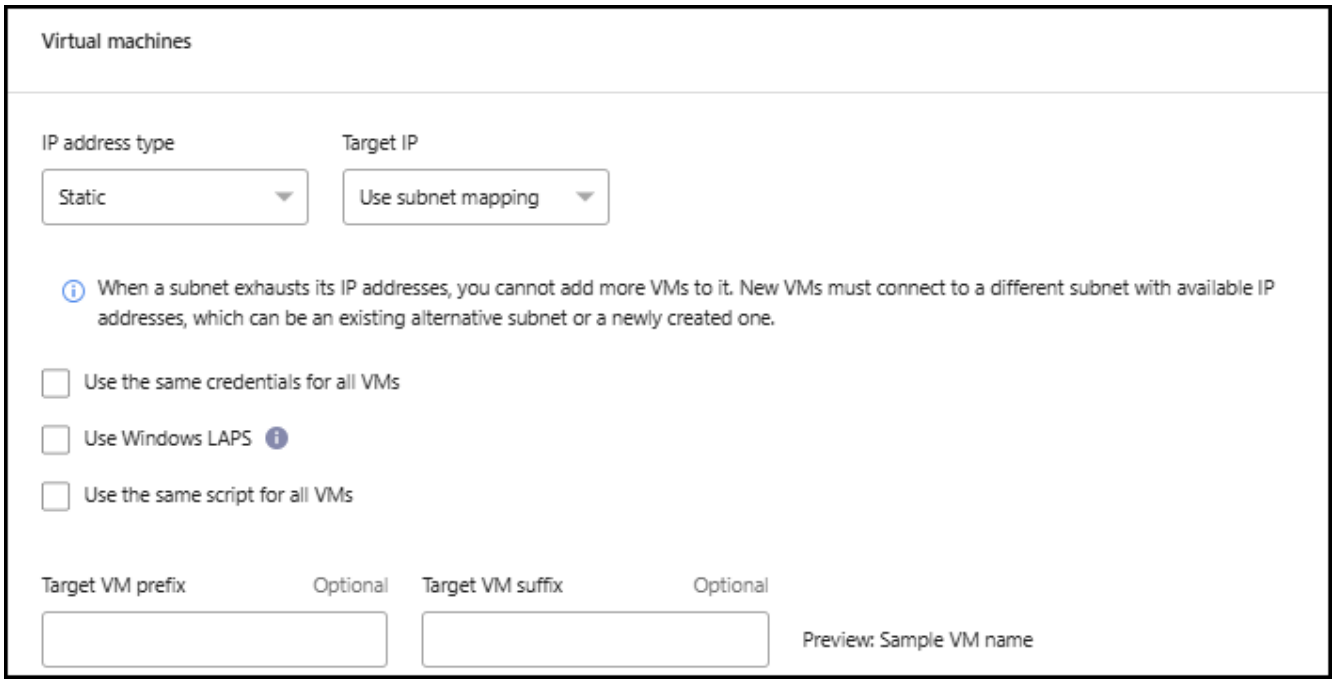
Quando si crea un piano di replicazione, è possibile selezionare il mapping della subnet per il piano di replicazione.

L'utilizzo della mappatura delle subnet è un processo facoltativo in due fasi:

- Per prima cosa, aggiungi la mappatura della subnet per ogni sito vCenter.
- In secondo luogo, nel piano di replicazione, indicare che si desidera utilizzare il mapping delle subnet.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.
2. Selezionare **Aggiungi** per aggiungere un piano di replicazione.
3. Completare i campi come di consueto, aggiungendo i server vCenter, selezionando i gruppi di risorse o le applicazioni e completando i mapping.
4. Nella pagina Piano di replicazione > Mappatura delle risorse, selezionare la sezione **Macchine virtuali**.



5. Nel campo **IP di destinazione**, seleziona **Usa mappatura subnet** dall'elenco a discesa.

> Se sono presenti due VM (ad esempio, una è Linux e l'altra è Windows), le credenziali sono necessarie solo per Windows.

6. Proseguire con la creazione del piano di replicazione.

Modifica il sito del server vCenter e personalizza la pianificazione dell'individuazione

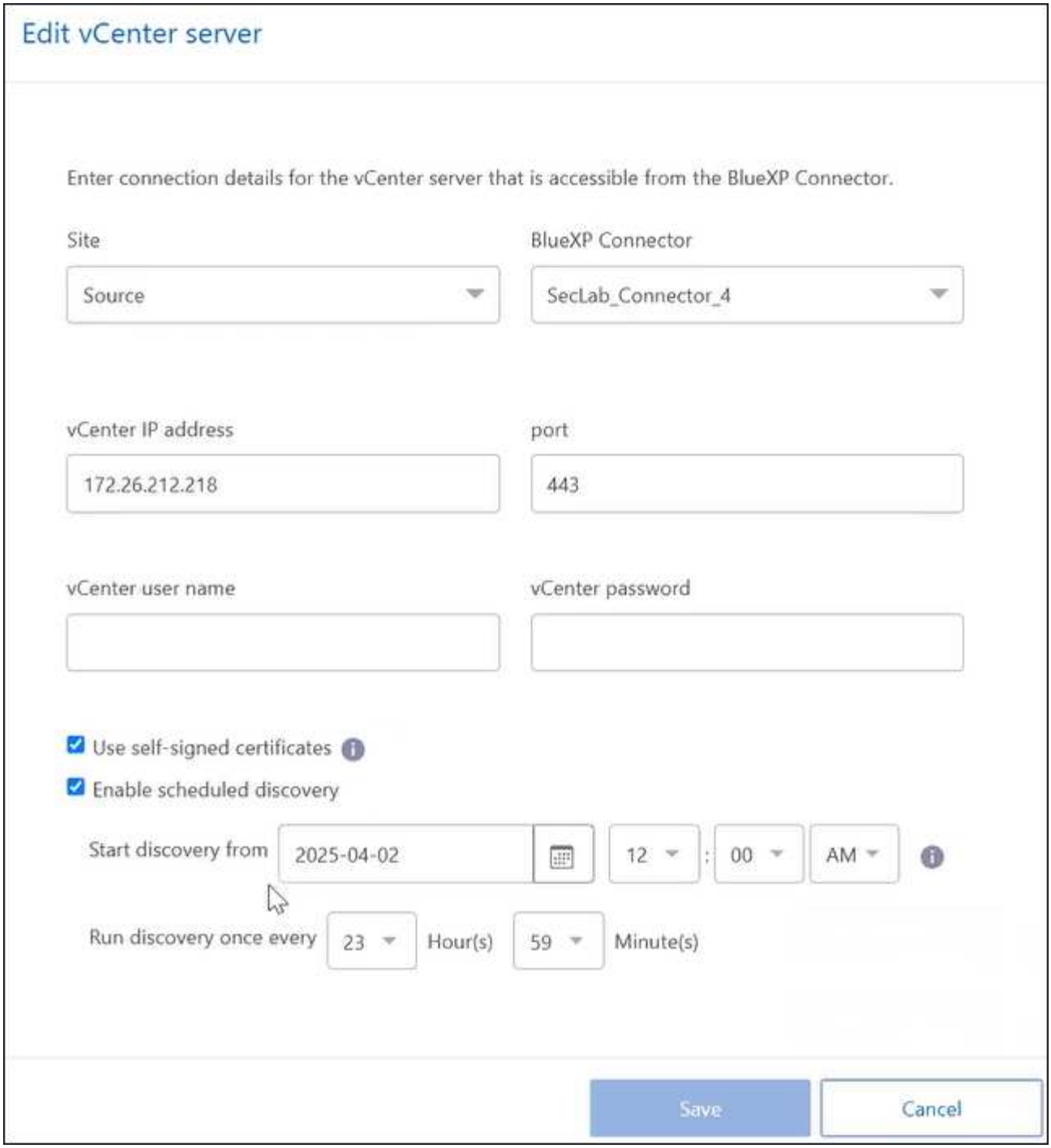
È possibile modificare il sito del server vCenter per personalizzare la pianificazione dell'individuazione. Ad esempio, se si dispone di un numero elevato di VM, è possibile impostare la pianificazione dell'individuazione in modo che venga eseguita ogni 23 ore e 59 minuti. Se si dispone di un numero limitato di VM, è possibile impostare la pianificazione dell'individuazione in modo che venga eseguita ogni 12 ore.

Se si dispone di vCenter di versioni precedenti e si desidera modificare il momento in cui viene eseguita l'individuazione, modificare il sito del server vCenter e impostare la pianificazione.

Se non si desidera pianificare l'individuazione, è possibile disattivare l'opzione di individuazione pianificata e aggiornare manualmente l'individuazione in qualsiasi momento.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Siti**.
2. Seleziona il sito che vuoi modificare.
3. Seleziona le azioni icona sulla destra e seleziona **Modifica**.
4. Nella pagina Modifica server vCenter, modificare i campi secondo necessità.
5. Per personalizzare la pianificazione dell'individuazione, seleziona la casella **Abilita individuazione pianificata** e seleziona l'intervallo di data e ora desiderato.



6. Seleziona **Salva**.

Aggiorna manualmente la scoperta

È possibile aggiornare manualmente la scoperta in qualsiasi momento. Questa operazione è utile se hai aggiunto o rimosso VM e vuoi aggiornare le informazioni in NetApp Disaster Recovery.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Siti**.
2. Seleziona il sito che vuoi aggiornare.
3.

Seleziona le azioni  icona sulla destra e seleziona **Aggiorna**.

Crea un gruppo di risorse per organizzare insieme le VM in NetApp Disaster Recovery

Dopo aver aggiunto i siti vCenter, è possibile creare gruppi di risorse per proteggere le VM per VM o datastore come un'unica unità. I gruppi di risorse consentono di organizzare un set di VM dipendenti in gruppi logici che soddisfano i requisiti. Ad esempio, è possibile raggruppare le VM associate a un'applicazione oppure le applicazioni che hanno livelli simili. Come altro esempio, i gruppi potrebbero contenere ordini di avvio ritardati che possono essere eseguiti al momento del ripristino.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Informazioni su questo compito

È possibile raggruppare le VM stesse o le VM nei datastore.

È possibile creare gruppi di risorse utilizzando i seguenti metodi:

- Dall'opzione Gruppi di risorse
- Mentre si crea un piano di disaster recovery o di replicazione. Se si dispone di numerose VM ospitate da un cluster vCenter di origine, potrebbe essere più semplice creare i gruppi di risorse durante la creazione del piano di replica. Per istruzioni sulla creazione di gruppi di risorse durante la creazione di un piano di replica, vedere"Creare un piano di replicazione" .

Ogni gruppo di risorse può includere una o più VM o datastore. Le VM si accenderanno in base alla sequenza in cui le includi nel piano di replica. È possibile modificare l'ordine trascinando le VM o i datastore verso l'alto o verso il basso nell'elenco dei gruppi di risorse.

Informazioni sui gruppi di risorse

I gruppi di risorse consentono di combinare VM o datastore come se fossero un'unica unità.

Ad esempio, un'applicazione POS potrebbe utilizzare diverse VM per database, logica aziendale e vetrine. È possibile gestire tutte queste VM con un unico gruppo di risorse. Impostare gruppi di risorse per applicare le regole del piano di replica per l'ordine di avvio delle VM, la connessione di rete e il ripristino di tutte le VM necessarie per l'applicazione.

Come funziona?

NetApp Disaster Recovery protegge le VM replicando i volumi ONTAP sottostanti e le LUN che ospitano le VM nel gruppo di risorse. Per fare ciò, il sistema interroga vCenter per ottenere il nome di ciascun archivio dati che ospita le VM in un gruppo di risorse. NetApp Disaster Recovery identifica quindi il volume ONTAP di origine o la LUN che ospita tale archivio dati. Tutta la protezione viene eseguita a livello di volume ONTAP utilizzando la replica SnapMirror .

Se le VM nel gruppo di risorse sono ospitate su archivi dati diversi, NetApp Disaster Recovery utilizza uno dei seguenti metodi per creare uno snapshot coerente con i dati dei volumi ONTAP o LUN.

Posizione relativa dei volumi FlexVol	Processo di replica snapshot
Archivi dati multipli: volumi FlexVol nello **stesso SVM**	• Gruppo di coerenza ONTAP creato • Istantanee del gruppo di coerenza prese • Eseguita la replica SnapMirror con ambito volume
Archivi dati multipli - Volumi FlexVol in **più SVM**	• API ONTAP : `cg_start` . Mette in modalità silenziosa tutti i volumi in modo che sia possibile creare snapshot e avvia snapshot con ambito volume di tutti i volumi del gruppo di risorse. • API ONTAP : `cg_end` . Riprende l'I/O su tutti i volumi e abilita la replica SnapMirror con ambito volume dopo l'acquisizione degli snapshot.

Quando si creano gruppi di risorse, tenere presente i seguenti aspetti:

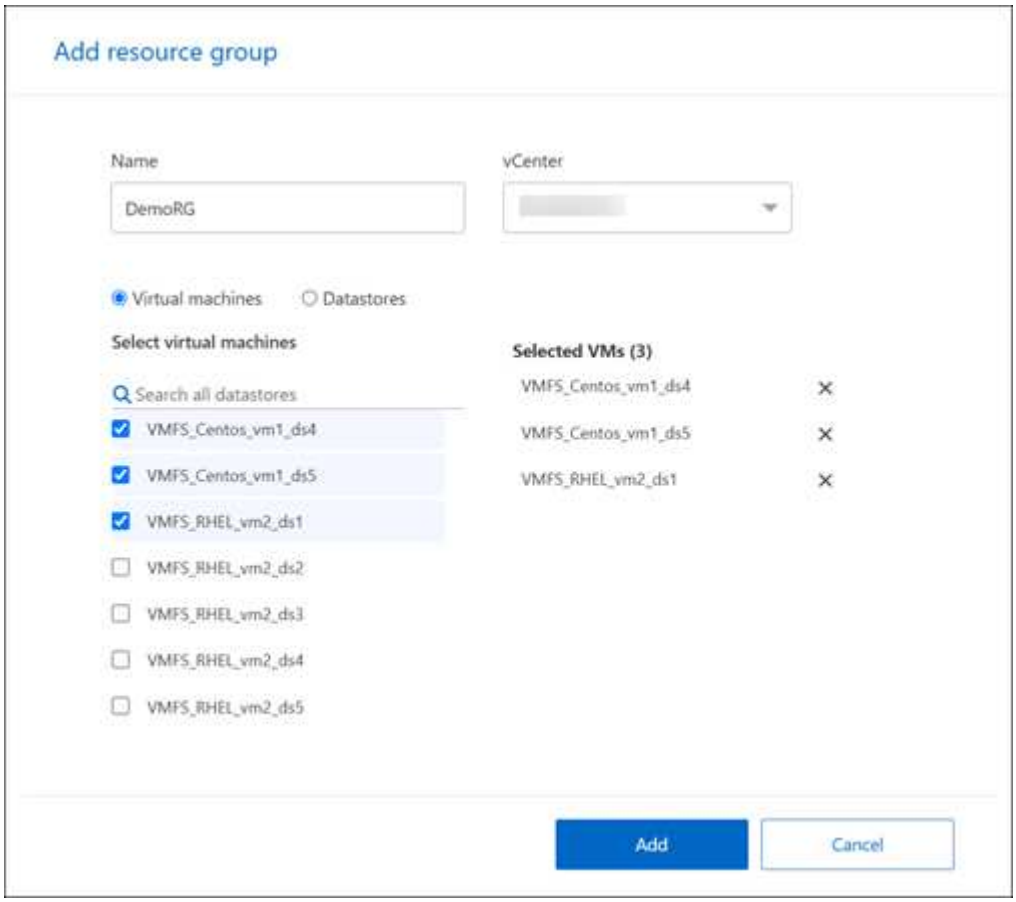
- Prima di aggiungere datastore ai gruppi di risorse, avviare prima un'individuazione manuale o un'individuazione pianificata delle VM. Ciò garantisce che le VM vengano rilevate ed elencate nel gruppo di risorse. Se non si avvia un'individuazione manuale, le VM potrebbero non essere elencate nel gruppo di risorse.
- Assicurarsi che nel datastore sia presente almeno una VM. Se non sono presenti VM nel datastore, Disaster Recovery non rileva il datastore.
- Un singolo datastore non dovrebbe ospitare VM protette da più di un piano di replica.
- Non ospitare VM protette e non protette sullo stesso datastore. Se le VM protette e non protette sono ospitate sullo stesso datastore, potrebbero verificarsi i seguenti problemi:
  - Poiché NetApp Disaster Recovery utilizza SnapMirror e il sistema replica interi volumi ONTAP , la capacità utilizzata di tale volume viene utilizzata per le considerazioni relative alle licenze. In questo caso, lo spazio del volume consumato dalle VM protette e non protette verrebbe incluso in questo calcolo.
  - Se è necessario eseguire il failover del gruppo di risorse e dei relativi datastore sul sito di disaster recovery, tutte le VM non protette (VM che non fanno parte del gruppo di risorse, ma sono ospitate sul volume ONTAP) non saranno più presenti sul sito di origine a seguito del processo di failover, con conseguente errore delle VM non protette sul sito di origine. Inoltre, NetApp Disaster Recovery non avvierà le VM non protette nel sito vCenter di failover.
- Per proteggere una VM, questa deve essere inclusa in un gruppo di risorse.

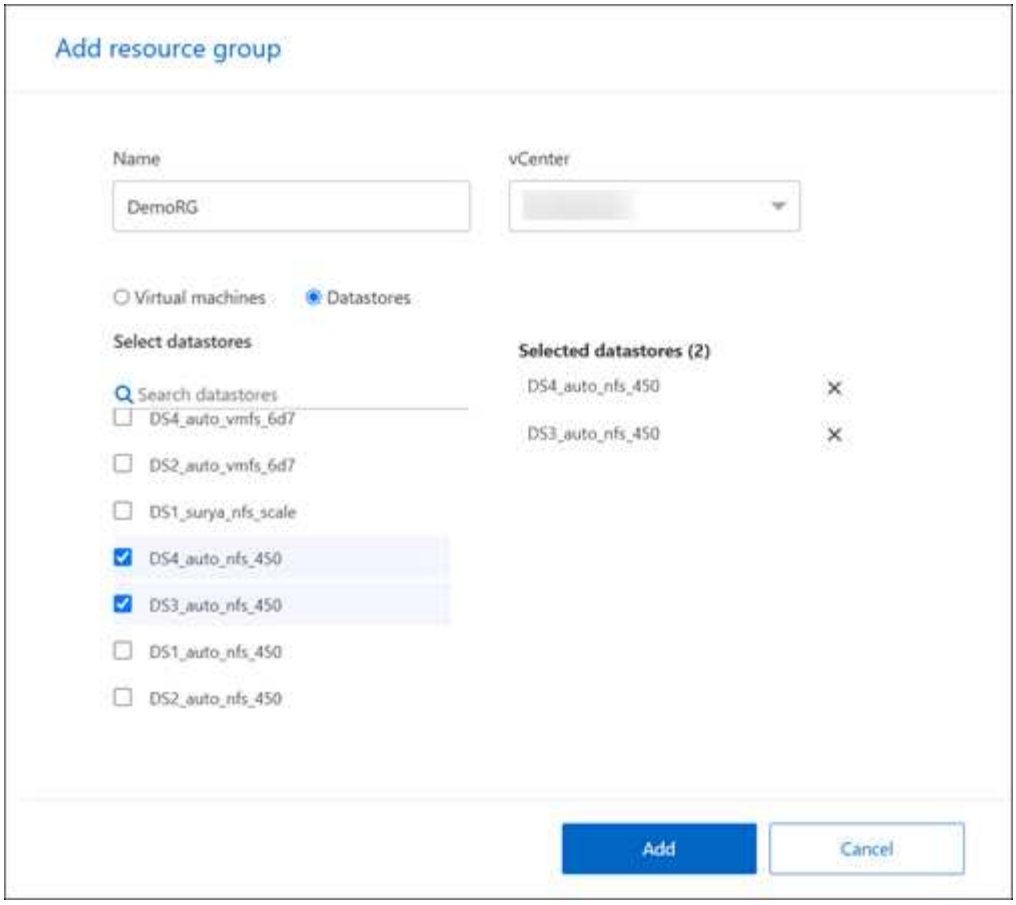
MIGLIOR PRATICITÀ: Organizzare le VM prima di implementare NetApp Disaster Recovery per ridurre al minimo la "proliferazione degli archivi dati". Posizionare le VM che necessitano di protezione su un sottoinsieme di datastore e posizionare le VM che non saranno protette su un sottoinsieme diverso di datastore. Assicurarsi che le VM su un determinato datastore non siano protette da piani di replica diversi.

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu NetApp Disaster Recovery , selezionare **Gruppi di risorse**.

4. Selezionare **Aggiungi**.
5. Immettere un nome per il gruppo di risorse.
6. Selezionare il cluster vCenter di origine in cui si trovano le VM.
7. Selezionare **Macchine virtuali** o **Datastore** a seconda del tipo di ricerca desiderata.
8. Selezionare la scheda **Aggiungi gruppi di risorse**. Il sistema elenca tutti i datastore o le VM nel cluster vCenter selezionato. Se hai selezionato **Datastore**, il sistema elenca tutti i datastore nel cluster vCenter selezionato. Se hai selezionato **Macchine virtuali**, il sistema elenca tutte le VM nel cluster vCenter selezionato.
9. Sul lato sinistro della pagina Aggiungi gruppi di risorse, seleziona le VM che desideri proteggere.





10. Facoltativamente, è possibile modificare l'ordine delle VM sulla destra trascinando ciascuna VM verso l'alto o verso il basso nell'elenco. Le VM si accenderanno in base alla sequenza in cui le includi.
11. Selezionare **Aggiungi**.

Creare un piano di replica in NetApp Disaster Recovery

Dopo aver aggiunto i siti vCenter, sei pronto per creare un disaster recovery o un *piano di replica*. I piani di replica gestiscono la protezione dei dati dell'infrastruttura VMware. Selezionare i vCenter di origine e di destinazione, scegliere i gruppi di risorse e raggruppare le modalità di ripristino e accensione delle applicazioni. Ad esempio, è possibile raggruppare le macchine virtuali (VM) associate a un'applicazione oppure le applicazioni che hanno livelli simili. Tali piani sono talvolta chiamati *blueprint*.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Informazioni su questo compito

È possibile creare un piano di replicazione e anche modificare le pianificazioni per la conformità e i test. Eseguire failover di prova delle VM senza influire sui carichi di lavoro di produzione.

È possibile proteggere più VM su più datastore. NetApp Disaster Recovery crea gruppi di coerenza ONTAP per tutti i volumi ONTAP che ospitano datastore VM protetti.

Le VM possono essere protette solo se il piano di replica si trova in uno dei seguenti stati:

- Pronto
- Failback eseguito
- Test failover eseguito

Snapshot del piano di replicazione

Disaster Recovery mantiene lo stesso numero di snapshot sui cluster di origine e di destinazione. Per impostazione predefinita, il servizio esegue un processo di riconciliazione degli snapshot ogni 24 ore per garantire che il numero di snapshot sui cluster di origine e di destinazione sia lo stesso.

Le seguenti situazioni possono causare una differenza nel numero di snapshot tra i cluster di origine e di destinazione:

- In alcune situazioni, le operazioni ONTAP esterne al Disaster Recovery possono aggiungere o rimuovere snapshot dal volume:
  - Se mancano snapshot sul sito di origine, gli snapshot corrispondenti sul sito di destinazione potrebbero essere eliminati, a seconda del criterio SnapMirror predefinito per la relazione.
  - Se mancano snapshot sul sito di destinazione, il servizio potrebbe eliminare gli snapshot corrispondenti sul sito di origine durante il successivo processo di riconciliazione degli snapshot pianificato, a seconda del criterio SnapMirror predefinito per la relazione.
- Una riduzione del numero di snapshot conservati nel piano di replica può far sì che il servizio elimini gli snapshot più vecchi sia sul sito di origine che su quello di destinazione per soddisfare il numero di snapshot di conservazione appena ridotto.

In questi casi, Disaster Recovery rimuove gli snapshot più vecchi dai cluster di origine e di destinazione al successivo controllo di coerenza. In alternativa, l'amministratore può eseguire una pulizia immediata dello snapshot selezionando **Azioni*** **sull'icona del piano di replica e selezionando *Pulisci snapshot**.

Il servizio esegue controlli di simmetria degli snapshot ogni 24 ore.

Prima di iniziare

- Prima di creare una relazione SnapMirror , configurare il cluster e il peering SVM al di fuori del Disaster Recovery.
- Con Google Cloud, puoi aggiungere un solo volume o datastore a un piano di replica.

> Organizza le tue VM prima di implementare NetApp Disaster Recovery per ridurre al minimo la "proliferazione incontrollata degli archivi dati". Posizionare le VM che necessitano di protezione su un sottoinsieme di datastore e posizionare le VM che non saranno protette su un sottoinsieme diverso di datastore. Utilizzare la protezione basata su datastore per garantire che le VM su un dato datastore siano protette.

Crea il piano

Una procedura guidata ti guiderà attraverso questi passaggi:

- Selezionare i server vCenter.
- Selezionare le VM o gli archivi dati che si desidera replicare e assegnare gruppi di risorse.
- Illustra il modo in cui le risorse dall'ambiente di origine vengono mappate alla destinazione.
- Imposta la frequenza di esecuzione del piano, esegui uno script ospitato da guest, imposta l'ordine di avvio e seleziona l'obiettivo del punto di ripristino.
- Rivedi il piano.

Quando si crea il piano, è necessario seguire queste linee guida:

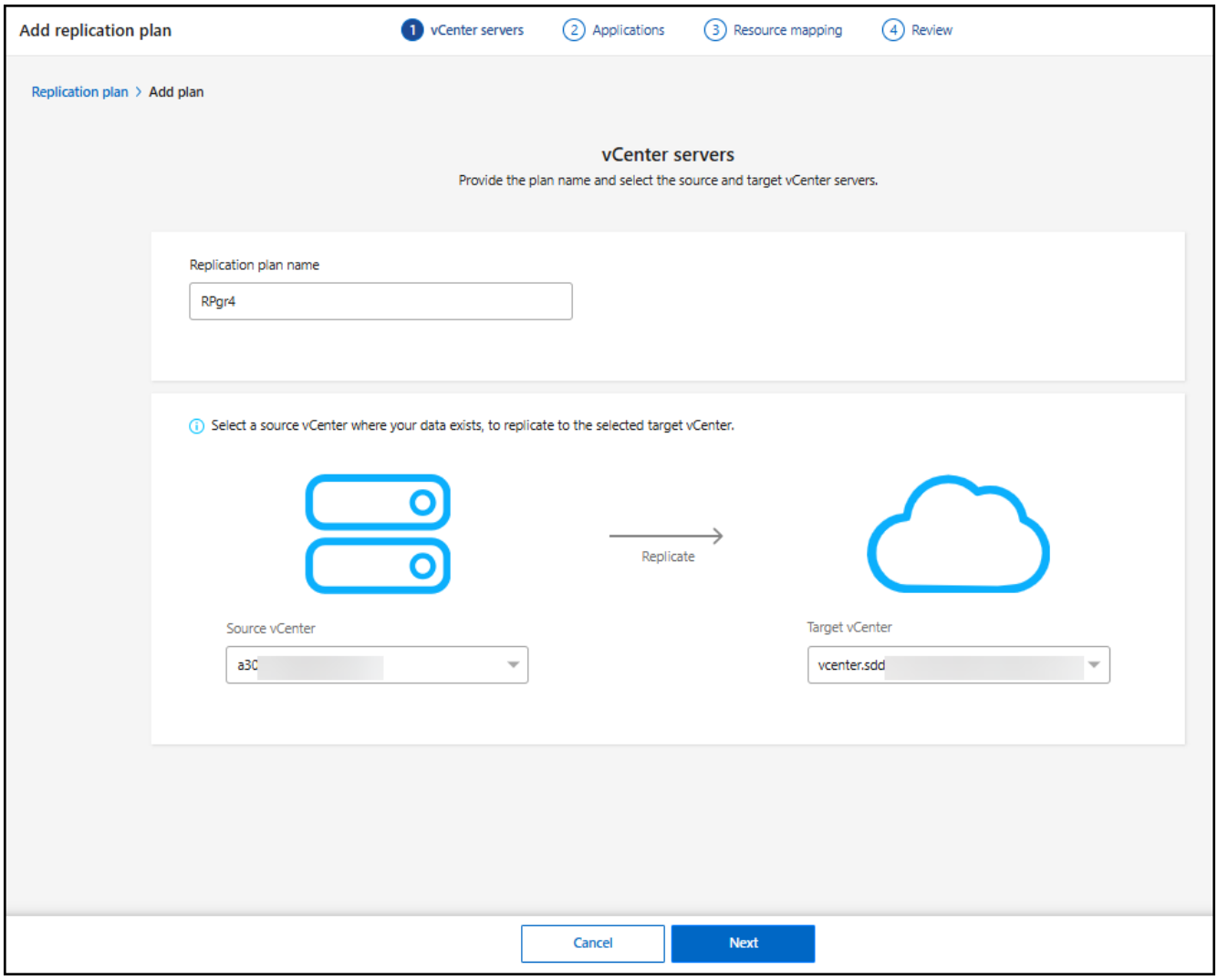
- Utilizzare le stesse credenziali per tutte le VM nel piano.
- Utilizzare lo stesso script per tutte le VM nel piano.
- Utilizzare la stessa subnet, DNS e gateway per tutte le VM nel piano.

Seleziona i server vCenter

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

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica** e quindi **Aggiungi**. In alternativa, se hai appena iniziato a utilizzare il servizio, seleziona **Aggiungi piano di replicazione** dalla Dashboard.



4. Creare un nome per il piano di replicazione.
5. Selezionare i vCenter di origine e di destinazione dagli elenchi vCenter di origine e di destinazione.
6. Selezionare **Avanti**.

Selezionare le applicazioni da replicare e assegnare gruppi di risorse

Il passaggio successivo consiste nel raggruppare le VM o gli archivi dati richiesti in gruppi di risorse funzionali. I gruppi di risorse consentono di proteggere un set di VM o datastore con uno snapshot comune.

Quando selezioni le applicazioni nel piano di replica, puoi vedere il sistema operativo per ogni VM o datastore nel piano. Ciò è utile per decidere come raggruppare le VM o gli archivi dati in un gruppo di risorse.

Ogni gruppo di risorse può includere una o più VM o datastore.

Quando si creano gruppi di risorse, tenere presente i seguenti aspetti:

- Prima di aggiungere datastore ai gruppi di risorse, avviare prima un'individuazione manuale o un'individuazione pianificata delle VM. Ciò garantisce che le VM vengano rilevate ed elencate nel gruppo di risorse. Se non si attiva un'individuazione manuale, le VM potrebbero non essere elencate nel gruppo di risorse.

- Assicurarsi che nel datastore sia presente almeno una VM. Se non sono presenti VM nel datastore, il datastore non verrà rilevato.
- Un singolo datastore non dovrebbe ospitare VM protette da più di un piano di replica.
- Non ospitare VM protette e non protette sullo stesso datastore. Se le VM protette e non protette sono ospitate sullo stesso datastore, potrebbero verificarsi i seguenti problemi:
  - Poiché NetApp Disaster Recovery utilizza SnapMirror e il sistema replica interi volumi ONTAP , la capacità utilizzata di tale volume viene utilizzata per le considerazioni relative alle licenze. In questo caso, lo spazio del volume consumato dalle VM protette e non protette verrebbe incluso in questo calcolo.
  - Se è necessario eseguire il failover del gruppo di risorse e dei relativi datastore sul sito di disaster recovery, tutte le VM non protette (VM che non fanno parte del gruppo di risorse, ma sono ospitate sul volume ONTAP) non saranno più presenti sul sito di origine a seguito del processo di failover, con conseguente errore delle VM non protette sul sito di origine. Inoltre, NetApp Disaster Recovery non avvierà le VM non protette nel sito vCenter di failover.
- Per proteggere una VM, questa deve essere inclusa in un gruppo di risorse.

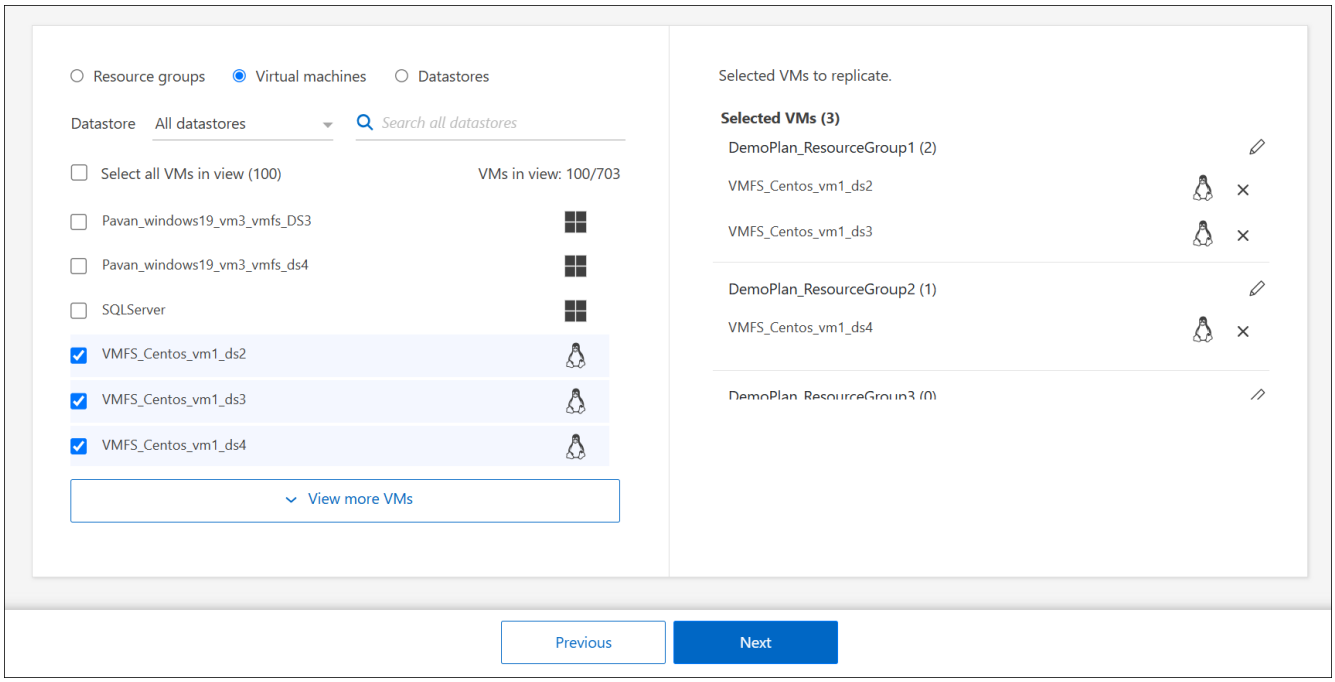
Crea un set dedicato separato di mappature per i tuoi test di failover per impedire che VMS venga connesso alle reti di produzione utilizzando gli stessi indirizzi IP.

Passi

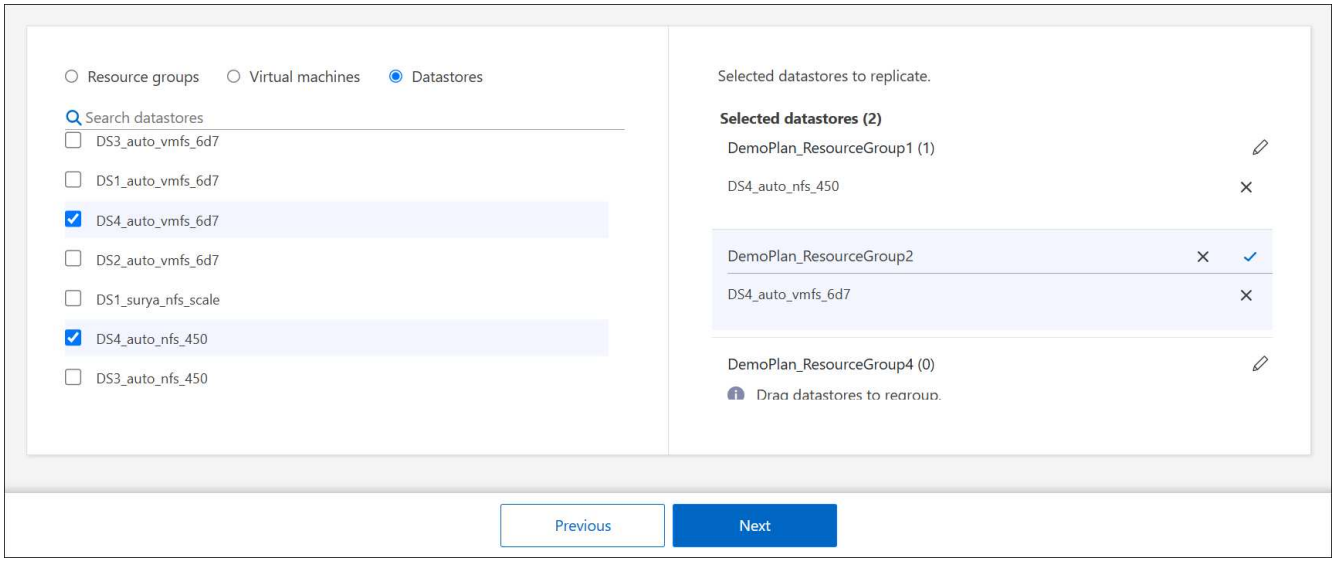
1. Selezionare **Macchine virtuali** o **Datastore**.
2. Facoltativamente, è possibile cercare una VM o un datastore specifico per nome.
3. Sul lato sinistro della pagina Applicazioni, seleziona le VM o i datastore che desideri proteggere e assegnali al gruppo selezionato.

   Il vCenter di origine deve risiedere nel vCenter locale. Il vCenter di destinazione può essere un secondo vCenter on-premise nello stesso sito o in un sito remoto, oppure un data center software-defined (SDDC) basato su cloud, come VMware Cloud su AWS. Entrambi i vCenter dovrebbero essere già aggiunti all'ambiente di lavoro di Disaster Recovery.

   La risorsa selezionata viene automaticamente aggiunta al gruppo 1 e viene avviato un nuovo gruppo 2. Ogni volta che si aggiunge una risorsa all'ultimo gruppo, viene aggiunto un altro gruppo.



Oppure, per i datastore:



4. Facoltativamente, esegui una delle seguenti operazioni:
   - Per cambiare il nome del gruppo, clicca sul gruppo *Modifica* icona.
   - Per rimuovere una risorsa da un gruppo, seleziona **X** accanto alla risorsa.
   - Per spostare una risorsa in un gruppo diverso, trascinala e rilasciala nel nuovo gruppo.

   Per spostare un datastore in un gruppo di risorse diverso, deselezionare il datastore indesiderato e inviare il piano di replica. Quindi, crea o modifica l'altro piano di replicazione e seleziona nuovamente il dataastore.

5. Selezionare **Avanti**.

Mappare le risorse di origine sulla destinazione

Nella fase di mappatura delle risorse, specificare in che modo le risorse dall'ambiente di origine devono essere mappate alla destinazione. Quando si crea un piano di replica, è possibile impostare un ritardo e un ordine di avvio per ogni macchina virtuale nel piano. Ciò consente di impostare una sequenza per l'avvio delle VM.

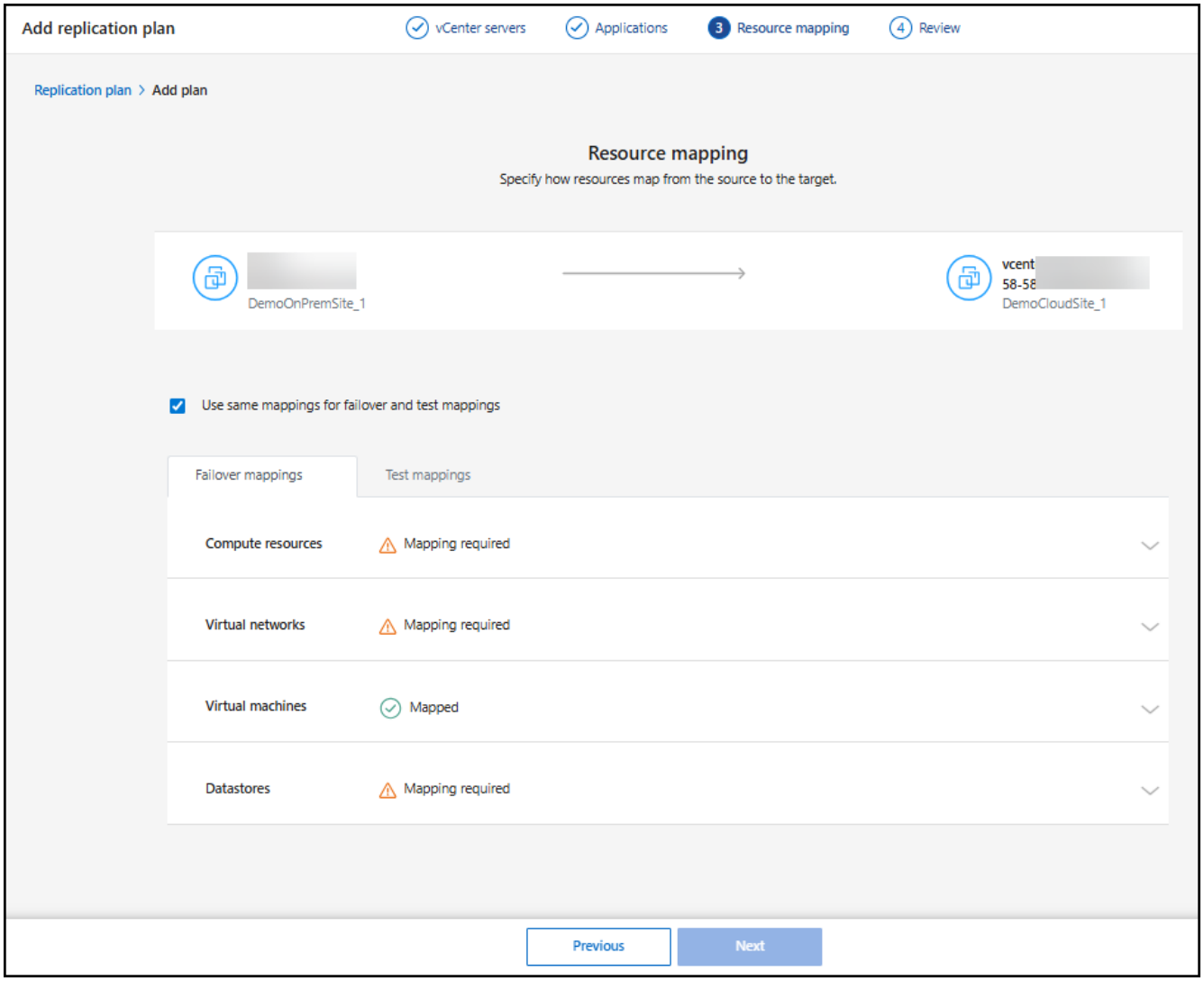
Se si prevede di eseguire failover di prova come parte del piano di ripristino di emergenza, è necessario fornire un set di mapping di failover di prova per garantire che le VM avviate durante il test di failover non interferiscano con le VM di produzione. È possibile ottenere questo risultato fornendo alle VM di prova indirizzi IP diversi oppure mappando le schede di rete virtuali delle VM di prova a una rete diversa, isolata dalla produzione ma con la stessa configurazione IP (denominata *bubble* o *rete di prova*).

Prima di iniziare

Se si desidera creare una relazione SnapMirror in questo servizio, il cluster e il relativo peering SVM devono essere già stati configurati al di fuori di NetApp Disaster Recovery.

Passi

1. Nella pagina Mappatura risorse, seleziona la casella per utilizzare le stesse mappature sia per le operazioni di failover che per quelle di test.



2. Nella scheda Mapping failover, seleziona la freccia rivolta verso il basso a destra di ogni risorsa e mappa le risorse in ogni sezione:

- Risorse di calcolo
- Reti virtuali
- Macchine virtuali
- Datastore

Risorse della mappa > Sezione Risorse di calcolo

La sezione Risorse di calcolo definisce dove verranno ripristinate le VM dopo un failover. Mappare il data center e il cluster vCenter di origine su un data center e un cluster di destinazione.

Facoltativamente, le VM possono essere riavviate su uno specifico host vCenter ESXi. Se VMWare DRS è abilitato, è possibile spostare automaticamente la VM su un host alternativo, se necessario, per soddisfare i criteri DR configurati.

Facoltativamente, è possibile posizionare tutte le VM in questo piano di replica in una cartella univoca con vCenter. Ciò fornisce un modo semplice per organizzare rapidamente le VM sottoposte a failover all'interno di vCenter.

Selezionare la freccia rivolta verso il basso accanto a **Risorse di calcolo**.

- **Data center di origine e di destinazione**
- **Cluster di destinazione**
- **Host di destinazione** (facoltativo): dopo aver selezionato il cluster, è possibile impostare queste informazioni.

Se un vCenter dispone di un Distributed Resource Scheduler (DRS) configurato per gestire più host in un cluster, non è necessario selezionare un host. Se selezioni un host, NetApp Disaster Recovery posizionerà tutte le VM sull'host selezionato. * **Cartella VM di destinazione** (facoltativa): crea una nuova cartella radice per archiviare le VM selezionate.

Risorse della mappa > Sezione Reti virtuali

Le VM utilizzano NIC virtuali connesse a reti virtuali. Nel processo di failover, il servizio connette queste NIC virtuali alle reti virtuali definite nell'ambiente VMware di destinazione. Per ogni rete virtuale di origine utilizzata dalle VM nel gruppo di risorse, il servizio richiede un'assegnazione di rete virtuale di destinazione.

È possibile assegnare più reti virtuali di origine alla stessa rete virtuale di destinazione. Ciò potrebbe tuttavia creare conflitti nella configurazione della rete IP. È possibile mappare più reti di origine su una singola rete di destinazione per garantire che tutte le reti di origine abbiano la stessa configurazione.

Nella scheda Mapping failover, seleziona la freccia rivolta verso il basso accanto a **Reti virtuali**. Selezionare la LAN virtuale di origine e la LAN virtuale di destinazione.

Selezionare la mappatura di rete sulla LAN virtuale appropriata. Le LAN virtuali dovrebbero essere già predisposte, quindi selezionare la LAN virtuale appropriata per mappare la VM.

Risorse della mappa > sezione macchine virtuali

È possibile configurare ciascuna VM nel gruppo di risorse protetto dal piano di replica in modo che si adatti all'ambiente virtuale vCenter di destinazione impostando una delle seguenti opzioni:

- Il numero di CPU virtuali
- La quantità di DRAM virtuale
- La configurazione dell'indirizzo IP
- La possibilità di eseguire script shell del sistema operativo guest come parte del processo di failover
- La possibilità di modificare i nomi delle VM sottoposte a failover utilizzando un prefisso e un suffisso univoci
- La possibilità di impostare l'ordine di riavvio durante il failover della VM

Nella scheda Mapping failover, seleziona la freccia rivolta verso il basso accanto a **Macchine virtuali**.

L'impostazione predefinita per le VM è mappata. La mappatura predefinita utilizza le stesse impostazioni utilizzate dalle VM nell'ambiente di produzione (stesso indirizzo IP, subnet mask e gateway).

Se si apportano modifiche alle impostazioni predefinite, è necessario modificare il campo IP di destinazione in "Diverso dall'origine".

Se modifichi le impostazioni in "Diverso dall'origine", devi fornire le credenziali del sistema operativo guest della VM.

Questa sezione potrebbe visualizzare campi diversi a seconda della selezione effettuata.

È possibile aumentare o diminuire il numero di CPU virtuali assegnate a ciascuna VM sottoposta a failover. Tuttavia, ogni VM richiede almeno una CPU virtuale. È possibile modificare il numero di CPU virtuali e di DRAM virtuale assegnate a ciascuna VM. Il motivo più comune per cui potresti voler modificare le impostazioni predefinite della CPU virtuale e della DRAM virtuale è se i nodi del cluster vCenter di destinazione non dispongono di tante risorse disponibili quanto il cluster vCenter di origine.

Impostazioni di rete Disaster Recovery supporta un ampio set di opzioni di configurazione per le reti VM. Potrebbe essere necessario modificarli se il sito di destinazione dispone di reti virtuali che utilizzano impostazioni TCP/IP diverse rispetto alle reti virtuali di produzione sul sito di origine.

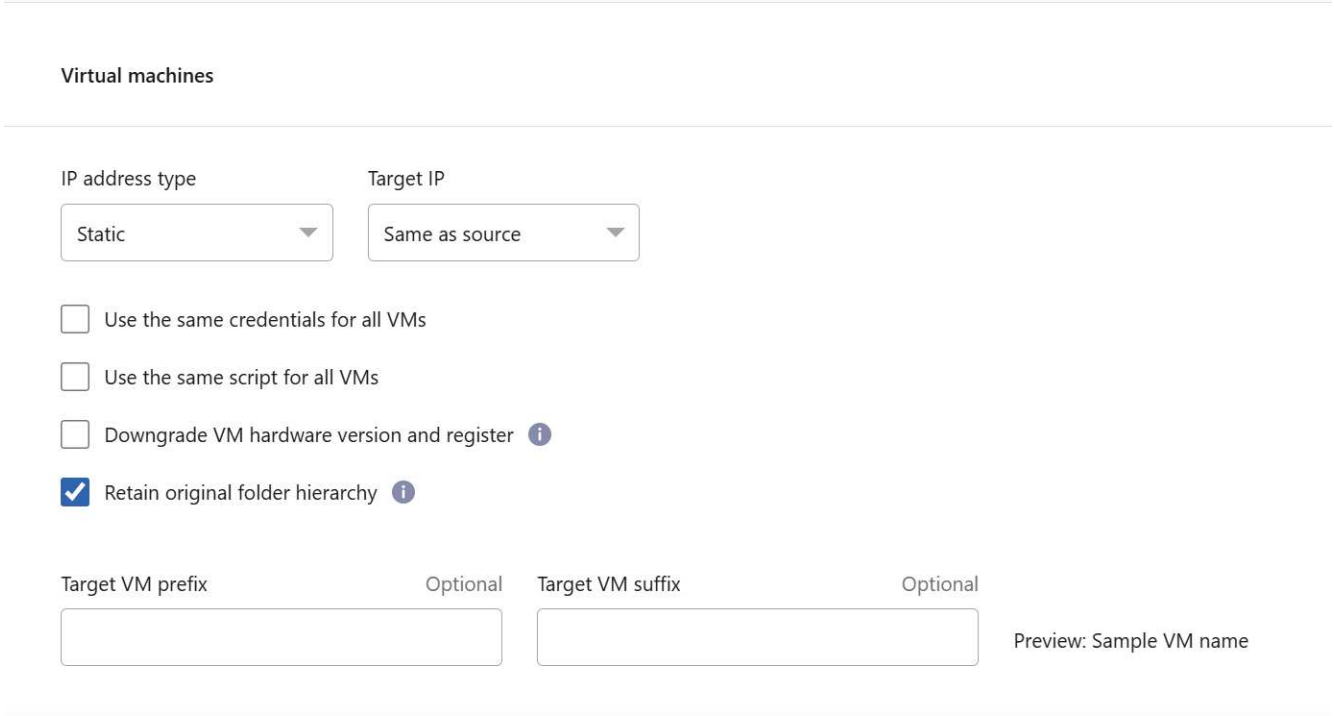
Al livello più basilare (e predefinito), le impostazioni utilizzano semplicemente le stesse impostazioni di rete TCP/IP per ogni VM sul sito di destinazione utilizzate sul sito di origine. Ciò richiede la configurazione delle stesse impostazioni TCP/IP sulle reti virtuali di origine e di destinazione.

Il servizio supporta le impostazioni di rete della configurazione IP statica o Dynamic Host Configuration Protocol (DHCP) per le VM. DHCP fornisce un metodo basato su standard per configurare dinamicamente le impostazioni TCP/IP di una porta di rete host. DHCP deve fornire, come minimo, un indirizzo TCP/IP e può anche fornire un indirizzo gateway predefinito (per il routing verso una connessione Internet esterna), una subnet mask e un indirizzo del server DNS. DHCP è comunemente utilizzato per i dispositivi informatici degli utenti finali, come i computer desktop, i laptop e le connessioni dei telefoni cellulari dei dipendenti, ma può essere utilizzato anche per qualsiasi dispositivo informatico di rete, come i server.

- Opzione **Utilizza le stesse impostazioni di subnet mask, DNS e gateway**: poiché queste impostazioni sono in genere le stesse per tutte le VM connesse alle stesse reti virtuali, potrebbe essere più semplice configurarle una volta e lasciare che Disaster Recovery utilizzi le impostazioni per tutte le VM nel gruppo di risorse protetto dal piano di replica. Se alcune VM utilizzano impostazioni diverse, è necessario deselezionare questa casella e specificare tali impostazioni per ciascuna VM.
- **Tipo di indirizzo IP**: riconfigurare la configurazione delle VM in modo che corrisponda ai requisiti della rete virtuale di destinazione. NetApp Disaster Recovery offre due opzioni: DHCP o IP statico. Per gli IP statici, configurare la subnet mask, il gateway e i server DNS. Inoltre, immettere le credenziali per le VM.

- **DHCP**: selezionare questa impostazione se si desidera che le VM ottengano le informazioni sulla configurazione di rete da un server DHCP. Se si sceglie questa opzione, si forniscono solo le credenziali per la VM.
- **IP statico**: selezionare questa impostazione se si desidera specificare manualmente le informazioni di configurazione IP. È possibile selezionare una delle seguenti opzioni: uguale all'origine, diverso dall'origine o mappatura della subnet. Se si sceglie lo stesso della fonte, non è necessario immettere le credenziali. D'altro canto, se si sceglie di utilizzare informazioni diverse dalla fonte, è possibile fornire le credenziali, l'indirizzo IP della VM, la subnet mask, il DNS e le informazioni sul gateway. Le credenziali del sistema operativo guest della VM devono essere fornite a livello globale o a livello di ciascuna VM.

  Ciò può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o per eseguire test di disaster recovery senza dover predisporre un'infrastruttura VMware fisica uno a uno.



- **Script**: è possibile includere script personalizzati ospitati dal sistema operativo guest in formato .sh, .bat o .ps1 come processi post. Grazie agli script personalizzati, Disaster Recovery può eseguire lo script dopo un failover, un failback e processi di migrazione. Ad esempio, è possibile utilizzare uno script personalizzato per riprendere tutte le transazioni del database una volta completato il failover. Il servizio può eseguire script all'interno di VM che eseguono Microsoft Windows o qualsiasi variante Linux supportata con parametri della riga di comando supportati. È possibile assegnare uno script a singole VM o a tutte le VM nel piano di replica.

  Per abilitare l'esecuzione degli script con il sistema operativo guest della VM, devono essere soddisfatte le seguenti condizioni:

  - VMware Tools deve essere installato sulla VM.
  - Per eseguire lo script è necessario fornire credenziali utente appropriate con privilegi adeguati sul sistema operativo guest.
  - Facoltativamente, includi un valore di timeout in secondi per lo script.

VM che eseguono Microsoft Windows: possono eseguire script batch di Windows (.bat) o PowerShell (ps1). Gli script di Windows possono utilizzare argomenti della riga di comando. Formatta ogni argomento nel `arg_name$value` formato, dove `arg_name` è il nome dell'argomento e `$value` è il valore dell'argomento e un punto e virgola separa ciascuno `argument$value` paio.

VM che eseguono Linux: possono eseguire qualsiasi script shell (.sh) supportato dalla versione di Linux utilizzata dalla VM. Gli script Linux possono utilizzare argomenti della riga di comando. Fornire gli argomenti in un elenco di valori separati da punto e virgola. Gli argomenti denominati non sono supportati. Aggiungi ogni argomento al `Arg[x]` elenco degli argomenti e fare riferimento a ciascun valore utilizzando un puntatore in `Arg[x]` matrice, ad esempio, `value1;value2;value3` .

- **Esegui il downgrade della versione hardware della VM e registra**: seleziona questa opzione se la versione dell'host ESX di destinazione è precedente a quella di origine, in modo che corrispondano durante la registrazione.
- **Mantieni la gerarchia delle cartelle originale**: per impostazione predefinita, Disaster Recovery conserva la gerarchia dell'inventario delle VM (struttura delle cartelle) in caso di failover. Se la destinazione di ripristino *non* ha la gerarchia di cartelle originale, Disaster Recovery la crea.

  Deselezionare questa casella per ignorare la gerarchia delle cartelle originale.

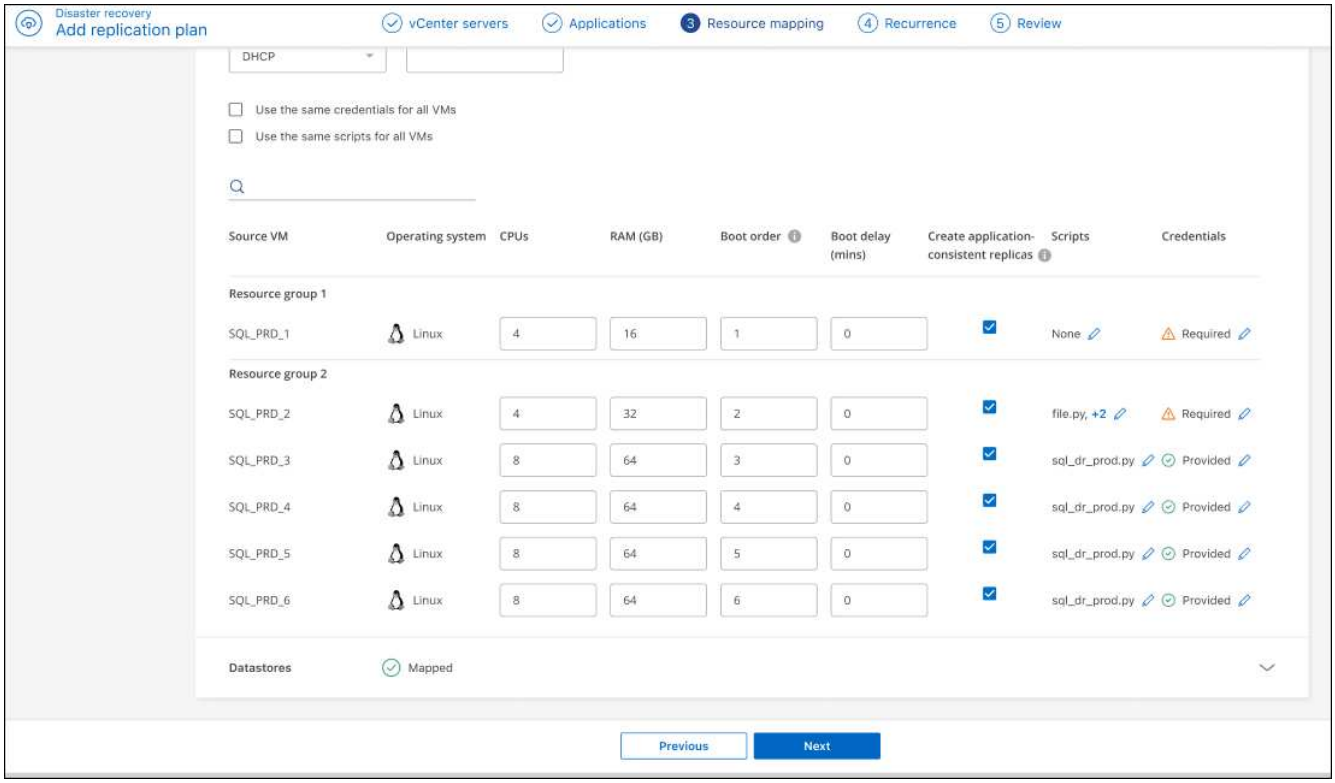
- **Prefisso e suffisso della VM di destinazione**: nei dettagli delle macchine virtuali, è possibile aggiungere facoltativamente un prefisso e un suffisso a ciascun nome di VM sottoposto a failover. Ciò può essere utile per differenziare le VM sottoposte a failover dalle VM di produzione in esecuzione sullo stesso cluster vCenter. Ad esempio, è possibile aggiungere il prefisso "DR-" e il suffisso "-failover" al nome della VM. In caso di emergenza, alcune persone aggiungono un secondo vCenter di produzione per ospitare temporaneamente le VM in un sito diverso. L'aggiunta di un prefisso o di un suffisso può aiutare a identificare rapidamente le VM sottoposte a failover. È possibile utilizzare il prefisso o il suffisso anche negli script personalizzati.

  È possibile utilizzare il metodo alternativo di impostazione della cartella VM di destinazione nella sezione Risorse di calcolo.

- **CPU e RAM della VM di origine**: nei dettagli delle macchine virtuali, è possibile ridimensionare facoltativamente i parametri della CPU e della RAM della VM.

  È possibile configurare la DRAM in gigabyte (GiB) o megabyte (MiB). Sebbene ogni VM richieda almeno un MiB di RAM, la quantità effettiva deve garantire che il sistema operativo guest della VM e tutte le applicazioni in esecuzione possano funzionare in modo efficiente.



- **Ordine di avvio**: è possibile modificare l'ordine di avvio dopo un failover per tutte le macchine virtuali selezionate nei gruppi di risorse. Per impostazione predefinita, tutte le VM vengono avviate insieme in parallelo; tuttavia, è possibile apportare modifiche in questa fase. Ciò è utile per garantire che tutte le VM con priorità uno siano in esecuzione prima che vengano avviate le VM con priorità successiva.

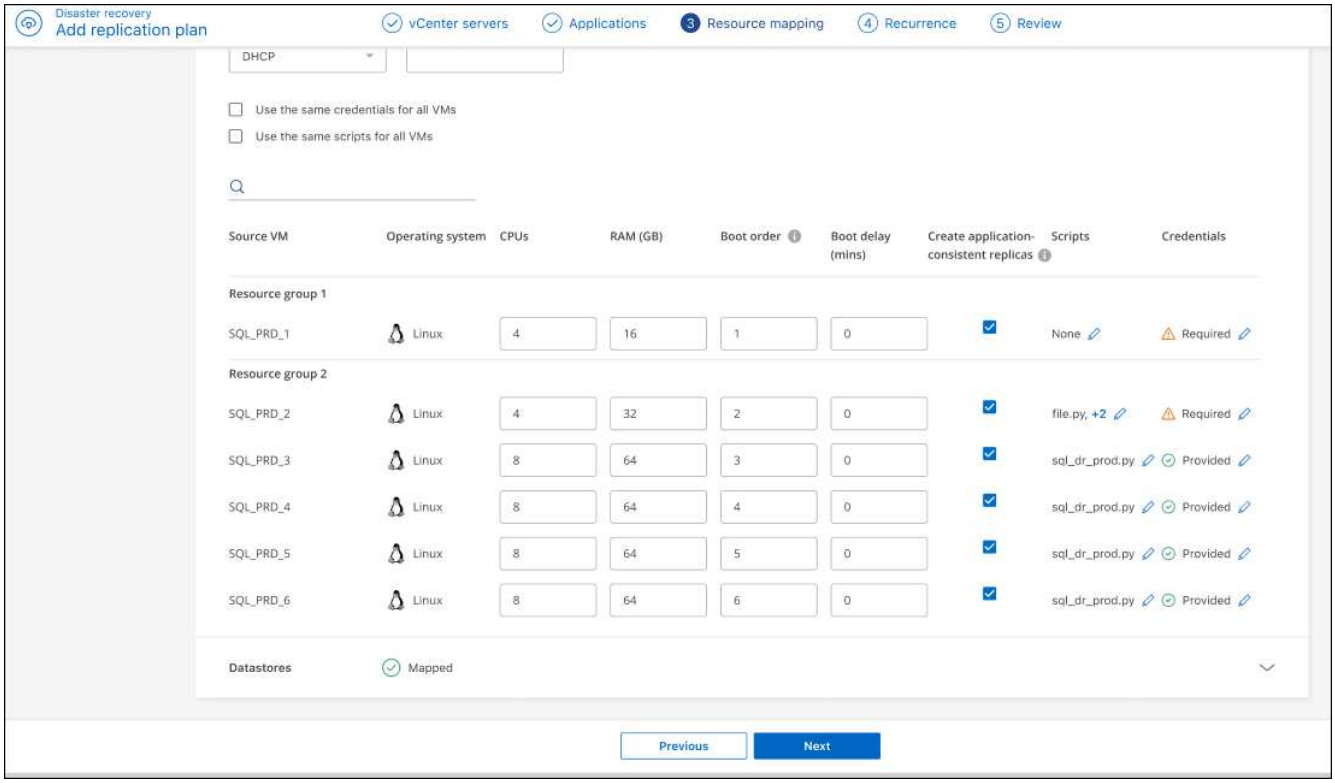
  Disaster Recovery avvia in parallelo tutte le VM con lo stesso numero di ordine di avvio.

  - Avvio sequenziale: assegna a ciascuna VM un numero univoco per avviarla nell'ordine assegnato, ad esempio 1, 2, 3, 4, 5.
  - Avvio simultaneo: assegna lo stesso numero a tutte le VM per avviarle contemporaneamente, ad esempio 1,1,1,1,2,2,3,4,4.
- **Ritardo di avvio**: regola il ritardo in minuti dell'azione di avvio, indicando la quantità di tempo che la VM attenderà prima di avviare il processo di accensione. Inserisci un valore compreso tra 0 e 10 minuti.

> Per ripristinare l'ordine di avvio predefinito, seleziona **Ripristina impostazioni VM predefinite** e poi scegli le impostazioni che desideri ripristinare ai valori predefiniti.

- **Crea repliche coerenti con l'applicazione**: indica se creare copie snapshot coerenti con l'applicazione. Il servizio metterà in pausa l'applicazione e poi eseguirà uno snapshot per ottenere uno stato coerente dell'applicazione. Questa funzionalità è supportata da Oracle in esecuzione su Windows e Linux e da SQL Server in esecuzione su Windows. Per maggiori dettagli vedi più avanti.
- **Usa Windows LAPS**: se utilizzi Windows Local Administrator Password Solution (Windows LAPS), seleziona questa casella. Questa opzione è disponibile solo se è stata selezionata l'opzione **IP statico**. Selezionando questa casella, non sarà necessario fornire una password per ciascuna delle macchine virtuali. In alternativa, è necessario fornire i dettagli del controller di dominio.

  Se non si utilizza Windows LAPS, la VM è una VM Windows e l'opzione delle credenziali nella riga della VM è abilitata. È possibile fornire le credenziali per la VM.



Creare repliche coerenti con l'applicazione

Molte VM ospitano server di database come Oracle o Microsoft SQL Server. Questi server di database richiedono snapshot coerenti con l'applicazione per garantire che il database sia in uno stato coerente quando viene eseguito lo snapshot.

Gli snapshot coerenti con l'applicazione garantiscono che il database si trovi in uno stato coerente quando viene eseguito lo snapshot. Questo è importante perché garantisce che il database possa essere ripristinato a uno stato coerente dopo un'operazione di failover o failback.

I dati gestiti dal server del database potrebbero essere ospitati sullo stesso datastore della macchina virtuale che ospita il server del database oppure su un datastore diverso. Nella tabella seguente sono illustrate le configurazioni supportate per gli snapshot coerenti con l'applicazione in Disaster Recovery:

Posizione dei dati	Supportato	Note
All'interno dello stesso datastore vCenter della VM	SÌ	Poiché il server del database e il database risiedono entrambi nello stesso datastore, sia il server che i dati saranno sincronizzati in caso di failover.

Posizione dei dati	Supportato	Note
All'interno di un datastore vCenter diverso dalla VM	NO	Disaster Recovery non è in grado di identificare quando i dati di un server di database si trovano su un diverso datastore vCenter. Il servizio non può replicare i dati, ma può replicare la VM del server del database. Sebbene i dati del database non possano essere replicati, il servizio garantisce che il server del database esegua tutti i passaggi necessari per garantire che il database sia inattivo al momento del backup della VM.
All'interno di una fonte dati esterna	NO	Se i dati risiedono su una LUN montata su guest o su una condivisione NFS, Disaster Recovery non può replicare i dati, ma può replicare la VM del server del database. Sebbene i dati del database non possano essere replicati, il servizio garantisce che il server del database esegua tutti i passaggi necessari per garantire che il database sia inattivo al momento del backup della VM.

Durante un backup pianificato, Disaster Recovery mette in pausa il server del database e quindi esegue uno snapshot della macchina virtuale che ospita il server del database. Ciò garantisce che il database sia in uno stato coerente quando viene eseguito lo snapshot.

- Per le VM Windows, il servizio utilizza il servizio Microsoft Volume Shadow Copy (VSS) per coordinarsi con uno dei due server di database.
- Per le VM Linux, il servizio utilizza un set di script per impostare il server Oracle in modalità di backup.

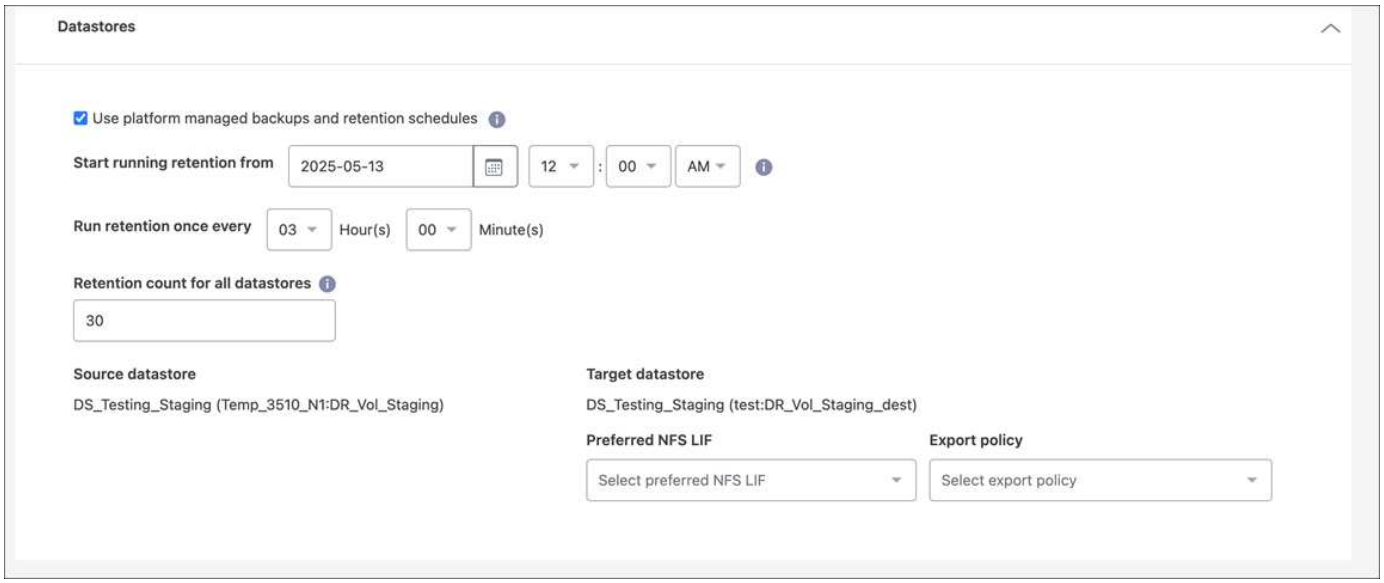
Per abilitare repliche coerenti con l'applicazione delle VM e dei relativi datastore di hosting, selezionare la casella accanto a **Crea repliche coerenti con l'applicazione** per ogni VM e fornire le credenziali di accesso guest con i privilegi appropriati.

Risorse della mappa > Sezione Datastore

Gli archivi dati VMware sono ospitati su volumi ONTAP FlexVol o su LUN iSCSI o FC ONTAP tramite VMware VMFS. Utilizzare la sezione Datastore per definire il cluster ONTAP di destinazione, la macchina virtuale di archiviazione (SVM) e il volume o LUN per replicare i dati su disco nella destinazione.

Selezionare la freccia rivolta verso il basso accanto a **Datastore**. In base alla selezione delle VM, vengono selezionate automaticamente le mappature dei datastore.

Questa sezione potrebbe essere abilitata o disabilitata a seconda della selezione effettuata.



- **Utilizza backup gestiti dalla piattaforma e pianificazioni di conservazione**: se utilizzi una soluzione di gestione degli snapshot esterna, seleziona questa casella. NetApp Disaster Recovery supporta l'uso di soluzioni di gestione degli snapshot esterni, come lo scheduler di policy nativo ONTAP SnapMirror o integrazioni di terze parti. Se ogni datastore (volume) nel piano di replicazione ha già una relazione SnapMirror gestita altrove, è possibile utilizzare tali snapshot come punti di ripristino in NetApp Disaster Recovery.

  Se si seleziona questa opzione, NetApp Disaster Recovery non configura una pianificazione di backup. Tuttavia, è comunque necessario configurare una pianificazione di conservazione perché potrebbero essere comunque acquisiti snapshot per operazioni di test, failover e failback.

  Dopo aver configurato questa funzionalità, il servizio non esegue snapshot programmati regolarmente, ma si affida all'entità esterna per l'esecuzione e l'aggiornamento di tali snapshot.

- **Ora di inizio**: immettere la data e l'ora in cui si desidera che i backup e la conservazione abbiano inizio.
- **Intervallo di esecuzione**: immettere l'intervallo di tempo in ore e minuti. Ad esempio, se si immette 1 ora, il servizio scatterà un'istantanea ogni ora.
- **Numero di conservazione**: inserisci il numero di snapshot che desideri conservare.

  Il numero di snapshot conservati, insieme alla frequenza di modifica dei dati tra ogni snapshot, determina la quantità di spazio di archiviazione consumato sia sull'origine che sulla destinazione. Più snapshot si conservano, più spazio di archiviazione viene consumato.

- **Datastore di origine e di destinazione**: se esistono più relazioni SnapMirror (fan-out), è possibile selezionare la destinazione da utilizzare. Se per un volume è già stata stabilita una relazione SnapMirror , vengono visualizzati i datastore di origine e di destinazione corrispondenti. Se si tratta di un volume che non ha una relazione SnapMirror , è possibile crearne una ora selezionando un cluster di destinazione, selezionando una SVM di destinazione e specificando un nome per il volume. Il servizio creerà il volume e la relazione SnapMirror .

  Se si desidera creare una relazione SnapMirror in questo servizio, il cluster e il relativo peering SVM devono essere già stati configurati al di fuori di NetApp Disaster Recovery.

  - Se le VM provengono dallo stesso volume e dallo stesso SVM, il servizio esegue uno snapshot ONTAP

standard e aggiorna le destinazioni secondarie.

- Se le VM provengono da volumi diversi e dallo stesso SVM, il servizio crea uno snapshot del gruppo di coerenza includendo tutti i volumi e aggiorna le destinazioni secondarie.
- Se le VM provengono da volumi diversi e da SVM diversi, il servizio esegue una fase di avvio del gruppo di coerenza e uno snapshot della fase di commit includendo tutti i volumi nello stesso cluster o in cluster diversi e aggiorna le destinazioni secondarie.
- Durante il failover, è possibile selezionare qualsiasi snapshot. Se si seleziona lo snapshot più recente, il servizio crea un backup su richiesta, aggiorna la destinazione e utilizza tale snapshot per il failover.

- **NFS LIF preferito** e **Criterio di esportazione**: in genere, lasciare che sia il servizio a selezionare il LIF NFS preferito e il criterio di esportazione. Se si desidera utilizzare un NFS LIF o un criterio di esportazione specifico, selezionare la freccia rivolta verso il basso accanto a ciascun campo e selezionare l'opzione appropriata.

  Facoltativamente, è possibile utilizzare interfacce dati specifiche (LIF) per un volume dopo un evento di failover. Ciò è utile per il bilanciamento del traffico dati se l'SVM di destinazione ha più LIF.

  Per un controllo aggiuntivo sulla sicurezza dell'accesso ai dati NAS, il servizio può assegnare a diversi volumi di datastore criteri di esportazione NAS specifici. I criteri di esportazione definiscono le regole di controllo degli accessi per i client NFS che accedono ai volumi del datastore. Se non si specifica una policy di esportazione, il servizio utilizza la policy di esportazione predefinita per l'SVM.

Si consiglia di creare una policy di esportazione dedicata che limiti l'accesso al volume *solo* agli host vCenter ESXi di origine e di destinazione che ospiteranno le VM protette. Ciò garantisce che entità esterne non possano accedere all'esportazione NFS.

Aggiungere mapping di failover di test

Passi

1. Per impostare mapping diversi per l'ambiente di test, deselezionare la casella e selezionare la scheda **Mapping test**.
2. Procedere come in precedenza per ogni scheda, ma questa volta per l'ambiente di test.

   Nella scheda Test mapping, i mapping Macchine virtuali e Datastore sono disabilitati.

Successivamente potrai testare l'intero piano. In questo momento stai configurando le mappature per l'ambiente di test.

Rivedere il piano di replicazione

Infine, prenditi qualche minuto per rivedere il piano di replicazione.

Successivamente è possibile disattivare o eliminare il piano di replica.

Passi

1. Esaminare le informazioni in ogni scheda: Dettagli del piano, Mapping del failover e VM.
2. Seleziona **Aggiungi piano**.

   Il piano viene aggiunto all'elenco dei piani.

Modificare le pianificazioni per testare la conformità e garantire il funzionamento dei test di failover

Potrebbe essere opportuno impostare delle pianificazioni per testare la conformità e i test di failover, in modo da garantire che funzionino correttamente quando necessario.

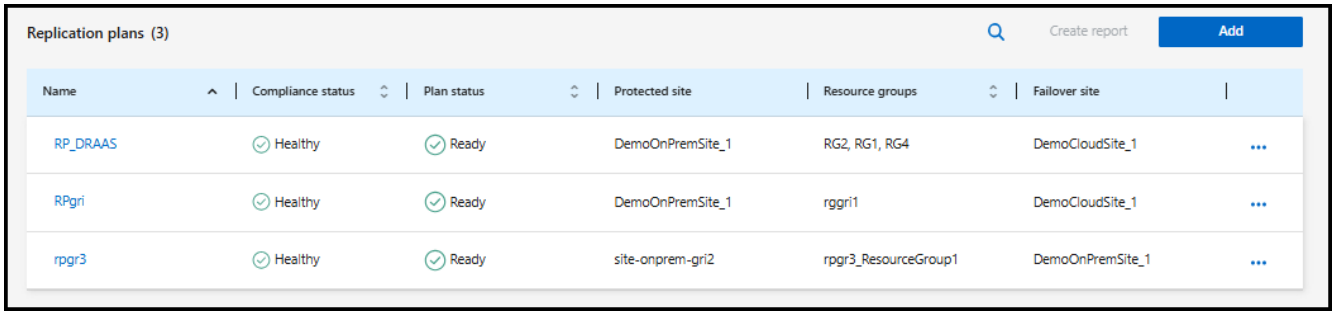
- **Impatto sui tempi di conformità**: quando viene creato un piano di replica, il servizio crea per impostazione predefinita una pianificazione di conformità. Il tempo di conformità predefinito è di 30 minuti. Per modificare questo orario, è possibile modificare la pianificazione nel piano di replica.
- **Impatto del failover di prova**: è possibile testare un processo di failover su richiesta o in base a una pianificazione. Ciò consente di testare il failover delle macchine virtuali su una destinazione specificata in un piano di replica.

  Un failover di test crea un volume FlexClone , monta il datastore e sposta il carico di lavoro su tale datastore. Un'operazione di failover di prova *non* ha alcun impatto sui carichi di lavoro di produzione, sulla relazione SnapMirror utilizzata sul sito di prova e sui carichi di lavoro protetti che devono continuare a funzionare normalmente.

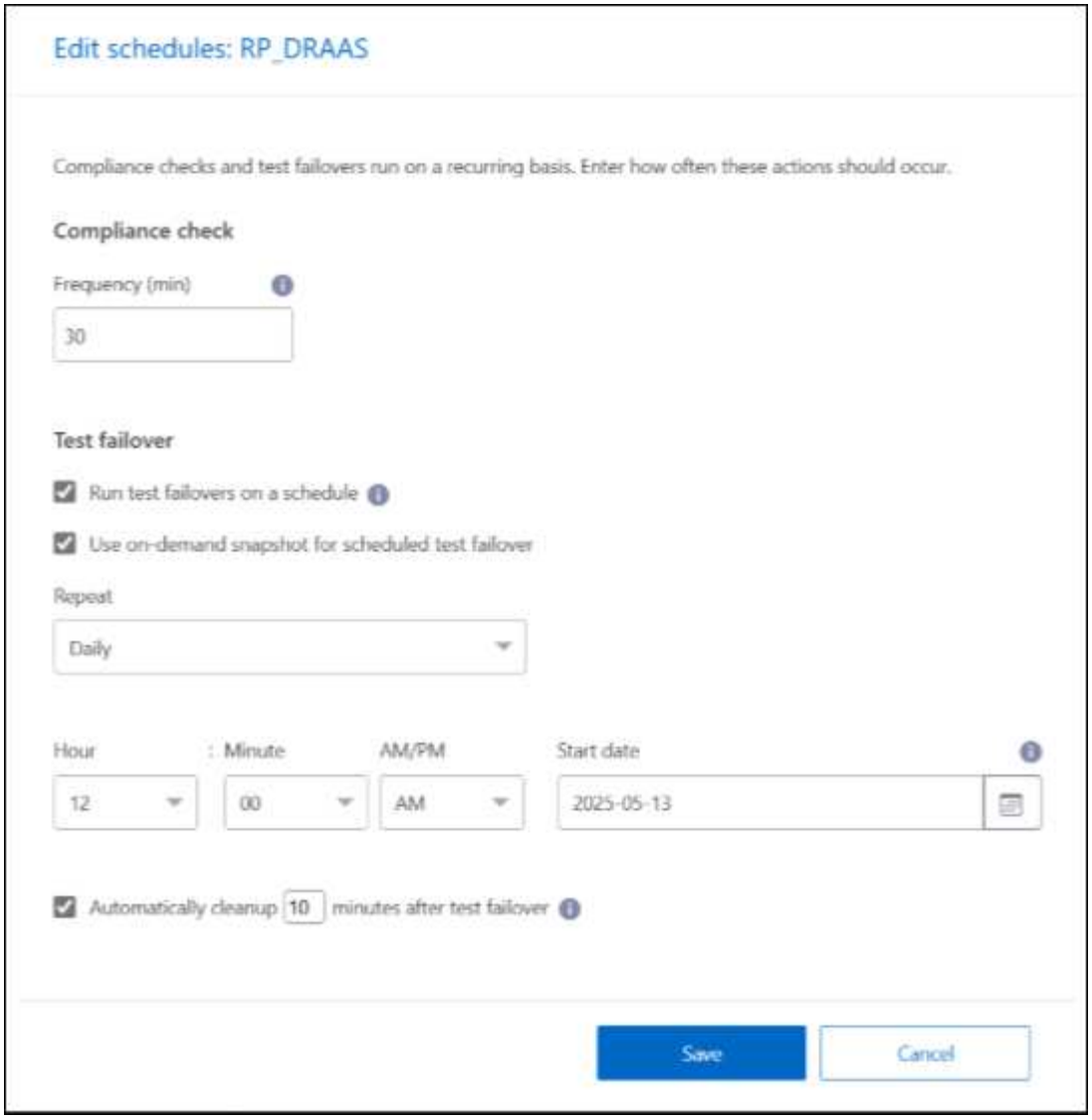
In base alla pianificazione, viene eseguito il test di failover, che garantisce che i carichi di lavoro vengano spostati verso la destinazione specificata dal piano di replica.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.



2. Seleziona **Azioni*** ••• **icona e seleziona *Modifica pianificazioni**.
3. Inserisci la frequenza in minuti con cui desideri che NetApp Disaster Recovery verifichi la conformità dei test.
4. Per verificare che i test di failover siano integri, seleziona **Esegui failover con una pianificazione mensile**.
   a. Seleziona il giorno del mese e l'ora in cui desideri che vengano eseguiti i test.
   b. Inserisci la data in formato aaaa-mm-gg in cui desideri che inizi il test.



5. **Utilizza snapshot su richiesta per il failover di test pianificato**: per acquisire un nuovo snapshot prima di avviare il failover di test automatico, selezionare questa casella.
6. Per ripulire l'ambiente di test al termine del test di failover, selezionare **Pulizia automatica dopo il failover del test** e immettere il numero di minuti che si desidera attendere prima che venga avviata la pulizia.

> Questo processo annulla la registrazione delle VM temporanee dalla posizione di test, elimina il volume FlexClone creato e smonta i datastore temporanei.

7. Seleziona **Salva**.

Replica le applicazioni su un altro sito con NetApp Disaster Recovery

Utilizzando NetApp Disaster Recovery, puoi replicare le app VMware dal tuo sito di origine a un sito remoto di disaster recovery nel cloud utilizzando la replica SnapMirror .

Dopo aver creato il piano di disaster recovery, identificato la ricorrenza nella procedura guidata e avviato una replica su un sito di disaster recovery, ogni 30 minuti NetApp Disaster Recovery verifica che la replica stia effettivamente avvenendo secondo il piano. È possibile monitorare l'avanzamento nella pagina Job Monitor.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza o amministratore del failover del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Prima di iniziare

Prima di avviare la replica, è necessario creare un piano di replica e scegliere di replicare le app. Quindi, nel menu Azioni viene visualizzata l'opzione **Replica**.

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu, seleziona **Piani di replicazione**.
4. Selezionare il piano di replicazione.
5. Sulla destra, seleziona l'opzione **Azioni*** ••• **e seleziona *Replica**.

Migra le applicazioni su un altro sito con NetApp Disaster Recovery

Utilizzando NetApp Disaster Recovery, puoi migrare le app VMware dal tuo sito di origine a un altro sito.

Dopo aver creato il piano di replica, identificato la ricorrenza nella procedura guidata e avviato la migrazione, ogni 30 minuti NetApp Disaster Recovery verifica che la migrazione stia effettivamente avvenendo secondo il piano. È possibile monitorare l'avanzamento nella pagina Job Monitor.

Prima di iniziare

Prima di avviare la migrazione, è necessario creare un piano di replicazione e scegliere di migrare le app. Quindi, nel menu Azioni viene visualizzata l'opzione **Migra**.

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu, seleziona **Piani di replicazione**.
4. Selezionare il piano di replicazione.
5. Sulla destra, seleziona l'opzione **Azioni*** ••• **e seleziona *Migra**.

Esegui il failover delle applicazioni su un sito remoto con NetApp Disaster Recovery

In caso di disastro, esegui il failover del tuo sito VMware locale principale su un altro sito VMware locale o su VMware Cloud su AWS. È possibile testare il processo di failover per garantirne il successo quando necessario.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza o amministratore del failover del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Informazioni su questo compito

Durante un failover, Disaster Recovery utilizza per impostazione predefinita la copia snapshot SnapMirror più recente, anche se è possibile selezionare uno snapshot specifico da uno snapshot point-in-time (in base ai criteri di conservazione di SnapMirror). Utilizzare l'opzione point-in-time se le repliche più recenti sono compromesse, ad esempio durante un attacco ransomware.

Questo processo varia a seconda che il sito di produzione sia integro e che si stia eseguendo un failover sul sito di disaster recovery per motivi diversi da un guasto critico dell'infrastruttura:

- Errore critico del sito di produzione in cui il cluster vCenter o ONTAP di origine non è accessibile: NetApp Disaster Recovery consente di selezionare qualsiasi snapshot disponibile da cui effettuare il ripristino.
- L'ambiente di produzione è integro: puoi scegliere "Esegui uno snapshot ora" oppure selezionare uno snapshot creato in precedenza.

Questa procedura interrompe la relazione di replica, mette offline le VM di origine vCenter, registra i volumi come datastore nel vCenter di disaster recovery, riavvia le VM protette utilizzando le regole di failover nel piano e abilita la lettura/scrittura sul sito di destinazione.

Testare il processo di failover

Prima di avviare il failover, è possibile testare il processo. Il test non mette offline le macchine virtuali.

Durante un test di failover, Disaster Recovery crea temporaneamente macchine virtuali. Risaster Recovery mappa un datastore temporaneo che supporta il volume FlexClone sugli host ESXi.

Questo processo non consuma ulteriore capacità fisica sullo storage ONTAP locale o sullo storage ONTAP FSx per NetApp in AWS. Il volume di origine originale non viene modificato e i processi di replica possono continuare anche durante il ripristino di emergenza.

Una volta terminato il test, dovresti reimpostare le macchine virtuali con l'opzione **Pulisci test**. Sebbene questa operazione sia consigliata, non è obbligatoria.

Un'operazione di failover di prova *non* ha alcun impatto sui carichi di lavoro di produzione, sulla relazione SnapMirror utilizzata sul sito di prova e sui carichi di lavoro protetti che devono continuare a funzionare normalmente.

Per un failover di prova, Disaster Recovery esegue le seguenti operazioni:

- Eseguire controlli preliminari sul cluster di destinazione e sulla relazione SnapMirror .

- Crea un nuovo volume FlexClone dallo snapshot selezionato per ciascun volume ONTAP protetto sul cluster ONTAP del sito di destinazione.
- Se alcuni datastore sono VMFS, creare e mappare un iGroup su ogni LUN.
- Registrare le macchine virtuali di destinazione in vCenter come nuovi datastore.
- Accendere le macchine virtuali di destinazione in base all'ordine di avvio acquisito nella pagina Gruppi di risorse.
- Riattiva tutte le applicazioni di database supportate nelle VM indicate come "coerenti con l'applicazione".
- Se i cluster vCenter e ONTAP di origine sono ancora attivi, creare una relazione SnapMirror in direzione inversa per replicare eventuali modifiche durante lo stato di failover sul sito di origine originale.

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.
4. Selezionare il piano di replicazione.
5. Sulla destra, seleziona l'opzione **Azioni*** ••• **e seleziona *Test failover**.
6. Nella pagina Test failover, immettere "Test failover" e selezionare **Test failover**.
7. Una volta completato il test, pulire l'ambiente di prova.

Pulisci l'ambiente di test dopo un test di failover

Una volta terminato il test di failover, è necessario ripulire l'ambiente di test. Questo processo rimuove le VM temporanee dalla posizione di test, i FlexClone e i datastore temporanei.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.
2. Selezionare il piano di replicazione.
3. Sulla destra, seleziona l'opzione **Azioni** ••• quindi **pulisci il test di failover**.
4. Nella pagina Test failover, immettere "Pulisci failover", quindi selezionare **Pulisci test failover**.

Eseguire il failover del sito di origine su un sito di ripristino di emergenza

In caso di disastro, esegui il failover del tuo sito VMware locale principale su richiesta su un altro sito VMware locale o su VMware Cloud su AWS con FSx per NetApp ONTAP.

Il processo di failover prevede le seguenti operazioni:

- Disaster Recovery esegue controlli preliminari sul cluster di destinazione e sulla relazione SnapMirror .
- Se hai selezionato l'ultima istantanea, verrà eseguito l'aggiornamento SnapMirror per replicare le modifiche più recenti.
- Le macchine virtuali di origine vengono spente.
- La relazione SnapMirror viene interrotta e il volume di destinazione viene impostato su lettura/scrittura.
- In base alla selezione dello snapshot, il file system attivo viene ripristinato allo snapshot specificato (più recente o selezionato).
- Gli archivi dati vengono creati e montati sul cluster o sull'host VMware o VMC in base alle informazioni

acquisite nel piano di replica. Se alcuni datastore sono VMFS, creare e mappare un iGroup su ogni LUN.

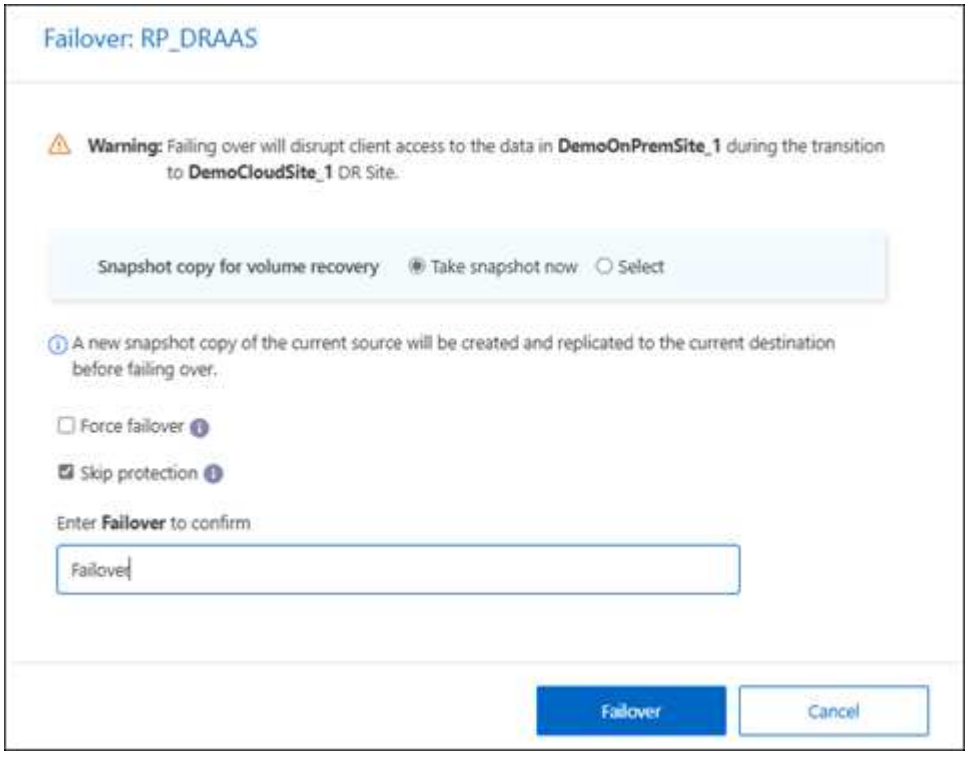
- Le macchine virtuali di destinazione vengono registrate in vCenter come nuovi datastore.
- Le macchine virtuali di destinazione vengono accese in base all'ordine di avvio acquisito nella pagina Gruppi di risorse.
- Se il vCenter di origine è ancora attivo, spegnere tutte le VM lato origine su cui è in corso il failover.
- Riattiva tutte le applicazioni di database supportate nelle VM indicate come "coerenti con l'applicazione".
- Se i cluster vCenter e ONTAP di origine sono ancora attivi, creare una relazione SnapMirror in direzione inversa per replicare eventuali modifiche durante lo stato di failover sul sito di origine originale. La relazione SnapMirror viene invertita dalla macchina virtuale di destinazione a quella di origine.

Per i piani di replica basati su datastore, se hai aggiunto e individuato delle VM ma non hai fornito dettagli di mappatura, tali VM vengono incluse nel failover. Il failover fallirà e verrà visualizzata una notifica nei processi. Per completare correttamente il failover, è necessario fornire i dettagli di mappatura.

Dopo l'avvio del failover, è possibile visualizzare le VM ripristinate nel vCenter del sito di disaster recovery (macchine virtuali, reti e datastore). Per impostazione predefinita, le macchine virtuali vengono ripristinate nella cartella Workload.

Passi

1. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.
2. Selezionare il piano di replicazione.
3. Sulla destra, seleziona l'opzione **Azioni*** ••• **e seleziona *Fail over**.



4. Nella pagina Failover, crea subito un nuovo snapshot oppure scegli uno snapshot esistente che il datastore utilizzerà come base per il ripristino. L'impostazione predefinita è l'ultima.

Verrà eseguita un'istantanea della sorgente corrente e replicata sulla destinazione corrente prima che si verifichi il failover.

5. Facoltativamente, selezionare **Forza failover** se si desidera che il failover si verifichi anche se viene rilevato un errore che normalmente ne impedirebbe il verificarsi.
6. Facoltativamente, selezionare **Ignora protezione** se si desidera che il servizio non crei automaticamente una relazione di protezione SnapMirror inversa dopo un failover del piano di replica. Questa opzione è utile se si desidera eseguire operazioni aggiuntive sul sito ripristinato prima di riportarlo online in NetApp Disaster Recovery.

È possibile impostare la protezione inversa selezionando **Proteggi risorse** dal menu Azioni del piano di replica. In questo modo si tenta di creare una relazione di replicazione inversa per ogni volume nel piano. È possibile eseguire questo processo più volte finché la protezione non viene ripristinata. Una volta ripristinata la protezione, è possibile avviare un failback nel modo consueto.

7. Digitare "failover" nella casella.
8. Selezionare **Fail over**.
9. Per controllare l'avanzamento, nel menu selezionare **Monitoraggio lavori**.

Ripristina le applicazioni alla fonte originale con NetApp Disaster Recovery

Dopo aver risolto un disastro, eseguire il failback dal sito di disaster recovery al sito di origine per ripristinare le normali operazioni. È possibile selezionare lo snapshot da cui effettuare il ripristino.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza o amministratore del failover del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Informazioni sul failback

In caso di failback, NetApp Disaster Recovery 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:

- Eseguire un controllo di conformità sul sito recuperato.
- Aggiornare le informazioni vCenter per ogni cluster vCenter identificato come situato nel sito ripristinato.
- Nel sito di destinazione, spegnere e annullare la registrazione delle macchine virtuali e smontare i volumi.
- Interrompere la relazione SnapMirror sulla sorgente originale per renderla di lettura/scrittura.
- Risincronizzare la relazione SnapMirror per invertire la replica.
- Accendere e registrare le macchine virtuali di origine, quindi montare i volumi sull'origine.

Prima di iniziare

Se si utilizza la protezione basata su datastore, le VM aggiunte al datastore potrebbero essere aggiunte al datastore durante il processo di failover. In tal caso, assicurarsi di fornire informazioni di mappatura aggiuntive per queste VM prima di avviare il failback. Per modificare la mappatura delle risorse, vedere "Gestire i piani di replicazione".

Passi

1. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
2. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.
3. Selezionare il piano di replicazione.
4. Sulla destra, seleziona l'opzione **Azioni*** ••• **e seleziona *Fail back**.
5. Immettere il nome del piano di replica per avviare il failback.
6. Selezionare lo snapshot per il datastore da cui effettuare il ripristino. L'impostazione predefinita è l'ultima.
7. Per monitorare l'avanzamento del processo, selezionare **Monitoraggio processo** nel menu Disaster Recovery.

Gestisci siti, gruppi di risorse, piani di replica, datastore e informazioni sulle macchine virtuali con NetApp Disaster Recovery

NetApp Disaster Recovery fornisce panoramiche e prospettive più dettagliate su tutte le tue risorse:

- Siti
- Gruppi di risorse
- Piani di replicazione
- Datastore
- Macchine virtuali

Le attività richiedono ruoli diversi NetApp Console . Per maggiori dettagli, consultare la sezione *Ruolo richiesto NetApp Console * in ogni attività.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Gestisci i siti vCenter

È possibile modificare il nome del sito vCenter e il tipo di sito (in locale o AWS).

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti o amministratore del ripristino di emergenza.

Passi

1. Dal menu, seleziona **Siti**.
2.

Seleziona l'opzione **Azioni***  **a destra del nome vCenter e seleziona *Modifica**.

3. Modificare il nome e la posizione del sito vCenter.

Gestire gruppi di risorse

È possibile creare gruppi di risorse tramite VM o datastore. Possono essere aggiunti quando si crea il piano di replicazione o in seguito.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

È possibile creare un gruppo di risorse tramite datastore nei seguenti modi:

- Quando si aggiunge un gruppo di risorse tramite datastore, è possibile visualizzare un elenco di datastore. È possibile selezionare uno o più datastore per creare un gruppo di risorse.
- Quando si crea un piano di replicazione e si crea un gruppo di risorse all'interno del piano, è possibile visualizzare le VM nei datastore.

Con i gruppi di risorse è possibile eseguire le seguenti attività:

- Cambia il nome del gruppo di risorse.
- Aggiungere VM al gruppo di risorse.
- Rimuovere le VM dal gruppo di risorse.
- Elimina gruppi di risorse.

Per i dettagli sulla creazione di un gruppo di risorse, fare riferimento a"Crea un gruppo di risorse per organizzare insieme le VM" .

Passi

1. Dal menu, seleziona **Gruppi di risorse**.
2. Per aggiungere un gruppo di risorse, seleziona **Aggiungi gruppo**.
3. È possibile modificare o eliminare il gruppo di risorse selezionando l'opzione *Azioni* ••• .

Gestire i piani di replicazione

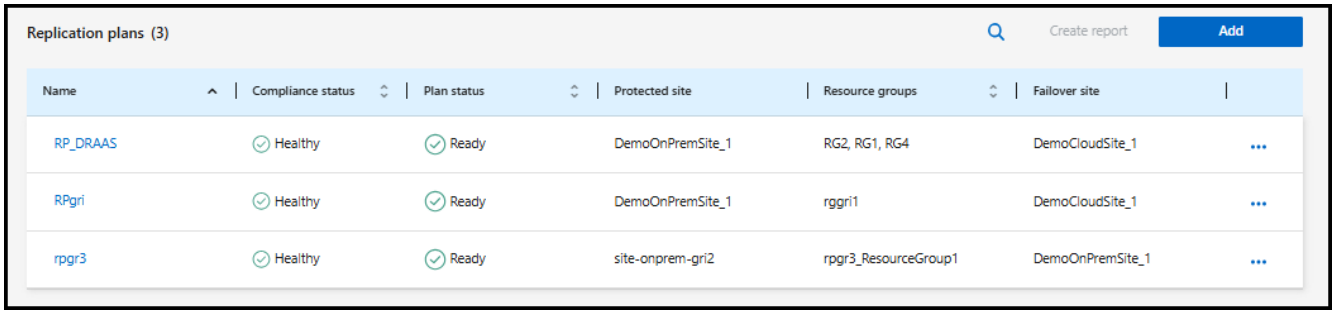
È possibile disattivare, attivare ed eliminare i piani di replica. È possibile modificare gli orari.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

- Se si desidera sospendere temporaneamente un piano di replica, è possibile disattivarlo e riattivarlo in seguito.
- Se non hai più bisogno del piano, puoi eliminarlo.

Passi

1. Dal menu, seleziona **Piani di replicazione**.



2. Per visualizzare i dettagli del piano, seleziona l'opzione **Azioni*** ••• **e seleziona *Visualizza dettagli piano**.
3. Esegui una delle seguenti operazioni:
   - Per modificare i dettagli del piano (cambiare la ricorrenza), seleziona la scheda **Dettagli del piano** e seleziona l'icona **Modifica** a destra.
   - Per modificare i mapping delle risorse, selezionare la scheda **Mapping failover** e selezionare l'icona **Modifica**.
   - Per aggiungere o modificare le macchine virtuali, selezionare la scheda **Macchine virtuali** e selezionare l'opzione **Aggiungi VM** o l'icona **Modifica**.
4. Per tornare all'elenco dei piani, seleziona "Piani di replica" nel percorso di navigazione a sinistra.
5. Per eseguire azioni con il piano, dall'elenco dei piani di replica, selezionare l'opzione **Azioni*** ••• **a destra del piano e seleziona una delle opzioni, ad esempio *Modifica pianificazioni**, **Failover di prova**, **Fail over**, **Fail back**, **Migra**, **Acquisisci snapshot ora**, **Pulisci vecchi snapshot**, **Disabilita**, **Abilita** o **Elimina**.
6. Per impostare o modificare una pianificazione del failover di prova o impostare la frequenza di controllo della conformità, selezionare l'opzione **Azioni*** ••• **a destra del piano e seleziona *Modifica pianificazioni**.
   a. Nella pagina Modifica pianificazioni, inserisci la frequenza in minuti con cui desideri che venga eseguito il controllo di conformità del failover.
   b. Selezionare **Esegui failover di test in base a una pianificazione**.
   c. Nell'opzione Ripeti, seleziona la pianificazione giornaliera, settimanale o mensile.
   d. Seleziona **Salva**.

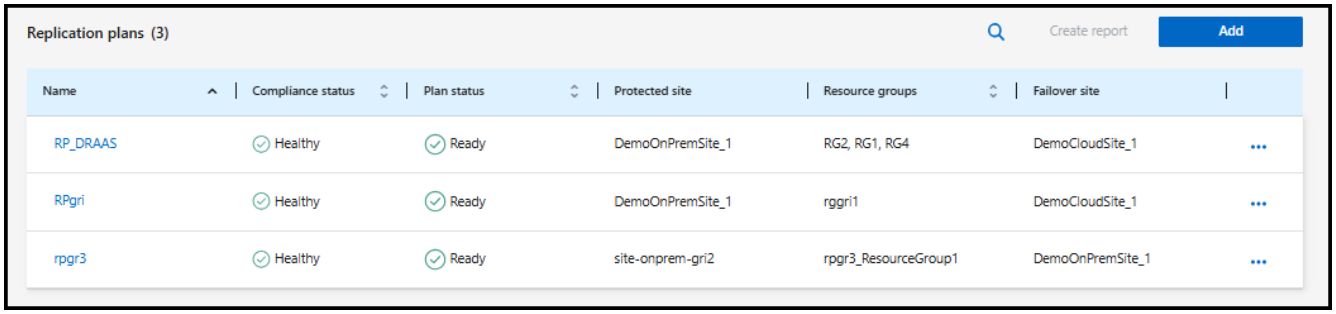
Riconcilia gli snapshot su richiesta

Disaster Recovery elimina automaticamente gli snapshot sulla sorgente ogni 24 ore. Se si scopre che gli snapshot non sono sincronizzati tra l'origine e la destinazione, è necessario risolvere la discrepanza tra gli snapshot per garantire la coerenza tra i siti.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

Passi

1. Dal menu, seleziona **Piani di replicazione**.



2. Dall'elenco dei piani di replica, seleziona l'opzione **Azioni*** ••• **quindi *Riconcilia gli snapshot**.
3. Esaminare le informazioni sulla riconciliazione.
4. Selezionare **Riconcilia**.

Elimina un piano di replicazione

Se si elimina un piano di replica, è possibile eliminare anche gli snapshot primari e secondari creati dal piano.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

Passi

1. Dal menu, seleziona **Piani di replicazione**.
2. Seleziona l'opzione **Azioni*** ••• **a destra del piano e seleziona *Elimina**.
3. Selezionare se si desidera eliminare gli snapshot primari, quelli secondari o solo i metadati creati dal piano.
4. Digitare "elimina" per confermare l'eliminazione.
5. Seleziona **Elimina**.

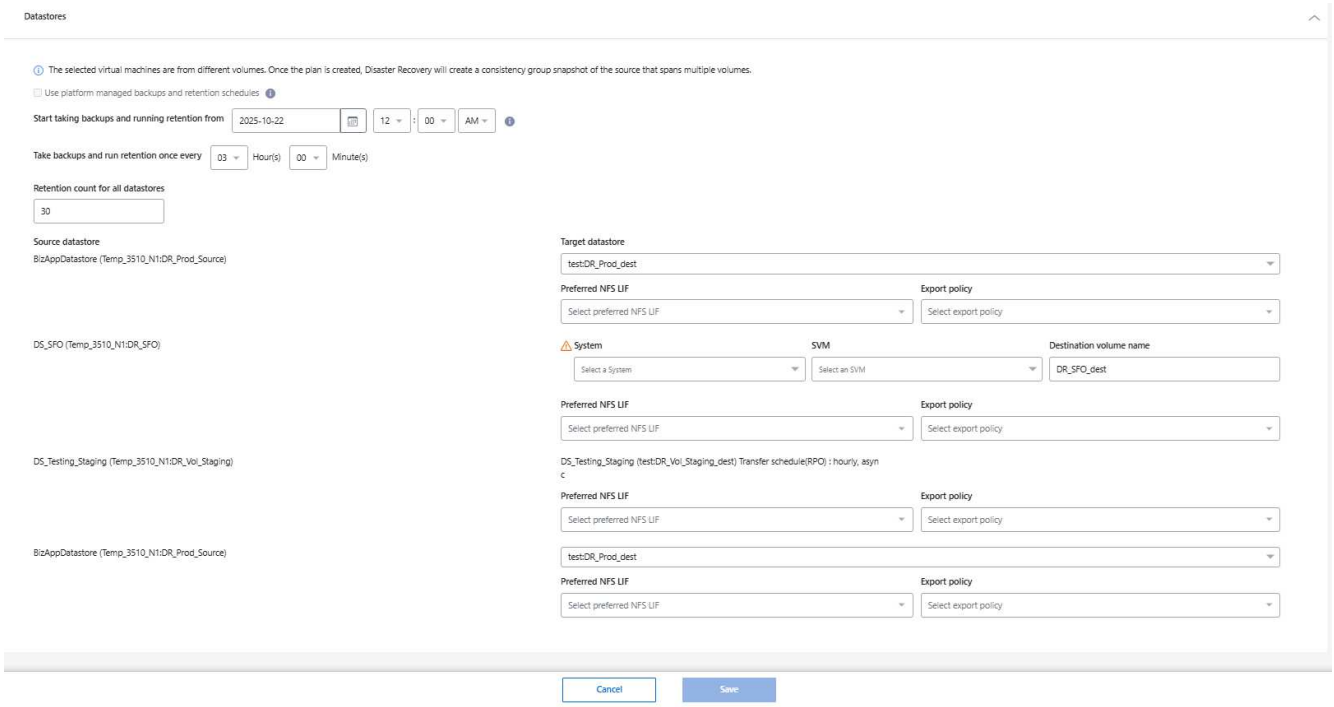
Modifica il conteggio di conservazione per le pianificazioni di failover

La modifica del conteggio di conservazione consente di aumentare o diminuire il numero di datastore salvati.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

Passi

1. Dal menu, seleziona **Piani di replicazione**.
2. Selezionare il piano di replicazione, quindi la scheda **Failover mapping**. Selezionare l'icona a forma di matita **Modifica**.
3. Selezionare la freccia rivolta verso il basso nella riga **Datastore** per espanderla.



4. Modificare il valore del **Conteggio di conservazione per tutti gli archivi dati**.
5. Dopo aver selezionato il piano di replica, seleziona il menu Azioni, quindi seleziona **Pulisci vecchi snapshot** per rimuovere i vecchi snapshot sulla destinazione in modo che corrispondano al nuovo conteggio di conservazione.

Visualizza le informazioni sui datastore

È possibile visualizzare informazioni sul numero di datastore presenti nell'origine e nella destinazione.

Ruolo di NetApp Console obbligatorio Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza, amministratore dell'applicazione di ripristino di emergenza o visualizzatore del ripristino di emergenza.

Passi

1. Dal menu, seleziona **Dashboard**.
2. Selezionare vCenter nella riga del sito.
3. Selezionare **Datastore**.
4. Visualizza le informazioni sui datastore.

Visualizza le informazioni sulle macchine virtuali

È possibile visualizzare informazioni sul numero di macchine virtuali presenti sull'origine e sulla destinazione, nonché sulla CPU, sulla memoria e sulla capacità disponibile.

Ruolo di NetApp Console obbligatorio Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza, amministratore dell'applicazione di ripristino di emergenza o visualizzatore del ripristino di emergenza.

Passi

1. Dal menu, seleziona **Dashboard**.
2. Selezionare vCenter nella riga del sito.
3. Seleziona **Macchine virtuali**.
4. Visualizza le informazioni sulle macchine virtuali.

Monitorare i lavori di NetApp Disaster Recovery

È possibile monitorare tutti i processi NetApp Disaster Recovery e determinarne l'avanzamento.

Visualizza i lavori

Ruolo di NetApp Console obbligatorio Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore dell'applicazione di ripristino di emergenza o visualizzatore del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dal menu, seleziona **Monitoraggio lavori**.
4. Esplora tutti i lavori correlati alle operazioni e controlla i relativi timestamp e stato.
5. Per visualizzare i dettagli di un lavoro specifico, seleziona la riga corrispondente.
6. Per aggiornare le informazioni, seleziona **Aggiorna**.

Annullare un lavoro

Se un lavoro è in corso o in coda e non si desidera che continui, è possibile annullarlo. Potresti voler annullare un lavoro se è bloccato nello stesso stato e vuoi liberare l'operazione successiva nella coda. Potresti voler annullare un lavoro prima che scada.

*Ruolo obbligatorio NetApp Console * Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti, amministratore del ripristino di emergenza, amministratore del failover del ripristino di emergenza o amministratore dell'applicazione di ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni in NetApp Disaster Recovery". "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi".

Passi

1. Dalla barra di navigazione sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
2. Dal menu, seleziona **Monitoraggio lavori**.
3. Nella pagina Monitoraggio lavori, annota l'ID del lavoro che desideri annullare.

   Il lavoro deve essere nello stato "In corso" o "In coda".

4. Nella colonna Azioni, seleziona **Annulla processo**.

Creare report NetApp Disaster Recovery

Esaminare i report di NetApp Disaster Recovery può aiutarti ad analizzare la tua preparazione al disaster recovery. I report predefiniti includono un riepilogo dei failover dei test, dettagli del piano di replica e dettagli dei lavori su tutti i siti all'interno di un account negli ultimi sette giorni.

È possibile scaricare i report in formato PDF, HTML o JSON.

Il link per il download è valido per sei ore.

Passi

1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.
3. Dalla barra di navigazione sinistra NetApp Console , selezionare **Piani di replica**.
4. Seleziona **Crea report**.
5. Selezionare il tipo di formato del file e il periodo di tempo compreso negli ultimi 7 giorni.
6. Seleziona **Crea**.

   La visualizzazione del report potrebbe richiedere alcuni minuti.

7. Per scaricare un report, seleziona **Scarica report** e selezionalo nella cartella Download dell'amministratore.

Informazioni sul copyright

Informazioni sul marchio commerciale