Documentazione NetApp Disaster Recovery

NetApp Disaster Recovery

NetApp
February 04, 2026

Sommario

Documentazione NetApp Disaster Recovery

Note di rilascio

Novità di NetApp Disaster Recovery

Scopri le novità di NetApp Disaster Recovery.

12 gennaio 2026

Versione 4.2.9

Supporto per più agenti Console in ambienti on-premise

Se utilizzi il Disaster Recovery in locale, ora puoi distribuire un agente Console per ogni istanza di vCenter, migliorando la resilienza.

Ad esempio, se si dispone di due siti (siti A e B), il sito A può avere l'agente console A collegato a vCenter 1, distribuzione ONTAP 1 e distribuzione ONTAP 2. Il sito B può avere l'agente Console B collegato alle distribuzioni vCenter 2 e ONTAP 3 e 4.

Per informazioni sull'agente Console in Disaster Recovery, vedere "Creare l'agente della console".

Aggiungere VM dopo il failover per i piani di replicazione utilizzando la protezione basata su datastore

Quando viene attivato il failover, qualsiasi piano di replica che utilizza la protezione basata su datastore include le VM aggiunte al datastore, a condizione che siano state rilevate. È necessario fornire i dettagli di mappatura per le VM aggiunte prima del completamento del failover.

Per maggiori informazioni, vedere "Failover delle applicazioni".

Nuove notifiche e-mail

Disaster Recovery ora fornisce notifiche e-mail per i seguenti eventi:

- Avvicinamento al limite di utilizzo della capacità
- Generazione del report completata
- Fallimenti lavorativi
- Scadenza o violazioni della licenza

Miglioramenti di Swagger

Ora è possibile accedere alla documentazione di Swagger dall'interno di Disaster Recovery. In Disaster Recovery, seleziona **Impostazioni**, quindi **Documentazione API** per collegarti a Swagger oppure visita questo URL nella modalità di navigazione in incognito/privata del tuo browser: "https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas".

Interfacce utente migliorate

Disaster Recovery ora fornisce avvisi e risoluzioni degli errori migliorati. Questa versione corregge un errore che impediva la visualizzazione dei lavori annullati nell'interfaccia utente. Ora i lavori annullati sono visibili. È presente anche un nuovo avviso quando la stessa rete di destinazione viene mappata su più reti di origine diverse.

Mantieni la struttura delle cartelle della VM aggiunta come predefinita nei piani di replica

Quando si crea una replica, la nuova impostazione predefinita è quella di mantenere la struttura delle cartelle della VM. Se la destinazione di ripristino non dispone della gerarchia di cartelle originale, Disaster Recovery la crea. È possibile deselezionare questa opzione per ignorare la gerarchia delle cartelle originale.

Per maggiori informazioni, vedere "Creare un piano di replicazione".

09 dicembre 2025

Versione 4.2.8P1

Conservazione della gerarchia delle cartelle

Per impostazione predefinita, Disaster Recovery mantiene la gerarchia dell'inventario delle VM (struttura delle cartelle) durante il failover. Se la destinazione di ripristino non dispone della cartella richiesta, Disaster Recovery la crea.

Ora è possibile ignorare questa impostazione designando una nuova cartella VM padre o deselezionando l'opzione **Mantieni gerarchia cartelle originale**.

Per maggiori informazioni, vedere "Creare un piano di replicazione".

Aggiornamento semplificato dell'agente della console

Disaster Recovery ora supporta un processo semplificato per l'utilizzo di più agenti Console in un ambiente di lavoro. Per passare da un agente Console all'altro, è necessario modificare la configurazione di vCenter, riscoprire le credenziali e aggiornare i piani di replica per utilizzare il nuovo agente Console.

Per maggiori informazioni, vedere "Agenti della console Switch".

01 dicembre 2025

Versione 4.2.8

Supporto per Google Cloud VMware Engine tramite Google Cloud NetApp Volumes

NetApp Disaster Recovery ora supporta Google Cloud VMware Engine utilizzando Google Cloud NetApp Volumes per le operazioni di migrazione, failover, failback e test. Questa integrazione consente flussi di lavoro di disaster recovery senza interruzioni tra ambienti on-premise e Google Cloud.

Assicurati di rivedere il"prerequisiti" E"limitazioni" per Google Cloud.

10 novembre 2025

Versione 4.2.7

Supporto failover a cascata

Ora è possibile configurare una relazione a cascata in ONTAP e utilizzare qualsiasi parte di tale relazione di replica per il ripristino di emergenza.

Ridurre il supporto hardware VMware durante la registrazione

Disaster Recovery ora supporta il downgrade dell'hardware VMware a una versione precedente di vSphere durante la registrazione. Questa funzionalità è utile quando l'host ESX di origine esegue una versione successiva a quella del sito di ripristino di emergenza.

Per maggiori informazioni, vedere "Creare un piano di replica in NetApp Disaster Recovery".

Arresto graduale

Disaster Recovery ora arresta correttamente le VM anziché spegnerle. Se una determinata VM impiega più di dieci minuti per spegnersi, Disaster Recovery la spegne.

Supporto per script pre-backup

Ora è possibile inserire script personalizzati nel flusso di lavoro di failover da eseguire prima di creare un backup. Gli script di pre-backup consentono di controllare lo stato della VM prima che venga replicato uno snapshot e di preparare una VM per una transizione. Ad esempio, è possibile inserire uno script che smonta un mount NFS che verrà rimontato utilizzando uno script diverso dopo il failover.

Per maggiori informazioni, vedere "Creare un piano di replica in NetApp Disaster Recovery".

06 ottobre 2025

Versione 4.2.6

Il BlueXP disaster recovery è ora NetApp Disaster Recovery

Il BlueXP disaster recovery è stato rinominato NetApp Disaster Recovery.

BlueXP è ora NetApp Console

NetApp Console, basata sulle fondamenta BlueXP migliorate e ristrutturate, offre una gestione centralizzata dello storage NetApp e NetApp Data Services in ambienti on-premise e cloud di livello aziendale, offrendo informazioni in tempo reale, flussi di lavoro più rapidi e un'amministrazione semplificata, il tutto in modo altamente sicuro e conforme.

Per i dettagli su cosa è cambiato, vedere il "Note sulla versione NetApp Console".

Altri aggiornamenti

- Il supporto per Amazon Elastic VMware Service (EVS) con Amazon FSx for NetApp ONTAP era disponibile in anteprima pubblica. Con questa versione, la funzionalità è ora disponibile al pubblico. Per i dettagli, fare riferimento a"Introduzione di NetApp Disaster Recovery tramite Amazon Elastic VMware Service e Amazon FSx for NetApp ONTAP" .
- Miglioramenti nella scoperta dello storage, inclusi tempi di scoperta ridotti per le distribuzioni on-premise
- Supporto per la gestione delle identità e degli accessi (IAM), incluso il controllo degli accessi basato sui ruoli (RBAC) e autorizzazioni utente migliorate
- Supporto di anteprima privata per la soluzione Azure VMware e Cloud Volumes ONTAP. Grazie a questo supporto, ora è possibile configurare la protezione del disaster recovery da locale alla soluzione Azure VMware utilizzando l'archiviazione Cloud Volumes ONTAP .

04 agosto 2025

Versione 4.2.5P2

Aggiornamenti NetApp Disaster Recovery

Questa versione include i seguenti aggiornamenti:

- Migliorato il supporto VMFS per gestire lo stesso LUN presentato da più macchine virtuali di archiviazione.
- Migliorata la pulizia dello teardown del test per gestire il datastore già smontato e/o eliminato.
- Mappatura della subnet migliorata in modo che ora convalidi che il gateway immesso sia contenuto nella rete fornita.
- È stato risolto un problema che poteva causare il fallimento del piano di replica se il nome della VM conteneva ".com".
- È stata rimossa una restrizione che impediva al volume di destinazione di essere uguale al volume di origine durante la creazione del volume come parte della creazione del piano di replica.
- Aggiunto il supporto per un abbonamento con pagamento in base al consumo (PAYGO) a NetApp Intelligent Services in Azure Marketplace e aggiunto un collegamento ad Azure Marketplace nella finestra di dialogo della prova gratuita.

  Per i dettagli, vedere "Licenza NetApp Disaster Recovery" E "Impostare la licenza per NetApp Disaster Recovery" .

14 luglio 2025

Versione 4.2.5

Ruoli utente in NetApp Disaster Recovery

NetApp Disaster Recovery ora utilizza ruoli per gestire l'accesso di ciascun utente a funzionalità e azioni specifiche.

Il servizio utilizza i seguenti ruoli specifici di NetApp Disaster Recovery.

- **Amministratore del ripristino di emergenza**: esegue qualsiasi azione in NetApp Disaster Recovery.
- **Amministratore failover di disaster recovery**: esegue azioni di failover e migrazione in NetApp Disaster Recovery.
- **Amministratore dell'applicazione di disaster recovery**: crea e modifica piani di replica e avvia failover di prova.
- **Visualizzatore di disaster recovery**: visualizza le informazioni in NetApp Disaster Recovery, ma non può eseguire alcuna azione.

Se si fa clic sul servizio NetApp Disaster Recovery e lo si configura per la prima volta, è necessario disporre dell'autorizzazione **SnapCenterAdmin** o del ruolo **Organization Admin**.

Per i dettagli, vedere"Ruoli utente e autorizzazioni in NetApp Disaster Recovery" .

"Scopri i ruoli di accesso per tutti i servizi".

Altri aggiornamenti in NetApp Disaster Recovery

- Rilevamento di rete migliorato
- Miglioramenti della scalabilità:
  - Filtraggio per i metadati richiesti anziché per tutti i dettagli
  - Miglioramenti della scoperta per recuperare e aggiornare più velocemente le risorse della VM
  - Ottimizzazione della memoria e delle prestazioni per il recupero e l'aggiornamento dei dati
  - Miglioramenti nella creazione del client vCenter SDK e nella gestione del pool
- Gestione dei dati obsoleti alla prossima individuazione programmata o manuale:
  - Quando una VM viene eliminata in vCenter, NetApp Disaster Recovery ora la rimuove automaticamente dal piano di replica.
  - Quando un datastore o una rete vengono eliminati in vCenter, NetApp Disaster Recovery li elimina ora dal piano di replica e dal gruppo di risorse.
  - Quando un cluster, un host o un data center viene eliminato in vCenter, NetApp Disaster Recovery ora lo elimina dal piano di replica e dal gruppo di risorse.
- Ora puoi accedere alla documentazione di Swagger nella modalità di navigazione in incognito del tuo browser. È possibile accedervi da NetApp Disaster Recovery tramite l'opzione Impostazioni > Documentazione API oppure direttamente al seguente URL nella modalità di navigazione in incognito del browser: "Documentazione Swagger" .
- In alcune situazioni, dopo un'operazione di failback, l'iGroup veniva lasciato indietro al termine dell'operazione. Questo aggiornamento rimuove iGroup se è obsoleto.
- Se nel piano di replica è stato utilizzato l'FQDN NFS, NetApp Disaster Recovery ora lo risolve in un indirizzo IP. Questo aggiornamento è utile se il nome di dominio completo non è risolvibile nel sito di ripristino di emergenza.
- Miglioramenti dell'allineamento dell'interfaccia utente
- Miglioramenti del registro per acquisire i dettagli delle dimensioni di vCenter dopo la corretta individuazione

30 giugno 2025

Versione 4.2.4P2

Miglioramenti della scoperta

Questo aggiornamento migliora il processo di individuazione, riducendone il tempo necessario.

23 giugno 2025

Versione 4.2.4P1

Miglioramenti nella mappatura delle subnet

Questo aggiornamento migliora la finestra di dialogo Aggiungi e modifica mappatura subnet con una nuova funzionalità di ricerca. Ora puoi trovare rapidamente subnet specifiche inserendo termini di ricerca, semplificando la gestione delle mappature delle subnet.

09 giugno 2025

Versione 4.2.4

Supporto per la soluzione password dell'amministratore locale di Windows (LAPS)

Windows Local Administrator Password Solution (Windows LAPS) è una funzionalità di Windows che gestisce ed esegue automaticamente il backup della password di un account amministratore locale su Active Directory.

Ora è possibile selezionare le opzioni di mappatura della subnet e selezionare l'opzione LAPS fornendo i dettagli del controller di dominio. Utilizzando questa opzione non è necessario fornire una password per ciascuna delle macchine virtuali.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

13 maggio 2025

Versione 4.2.3

Mappatura della sottorete

Con questa versione, è possibile gestire gli indirizzi IP in caso di failover in un modo nuovo, utilizzando la mappatura delle subnet, che consente di aggiungere subnet per ogni 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 determina l'indirizzo IP appropriato di ogni vNIC esaminando il CIDR fornito per la rete virtuale mappata e lo utilizza per ricavare il 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.

Per i dettagli sull'inclusione della mappatura delle subnet nei tuoi siti, fai riferimento a "Aggiungi siti server vCenter" .

Protezione contro gli ostacoli

Ora è possibile ignorare la protezione in modo che il servizio non crei automaticamente una relazione di protezione 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.

Quando si avvia un failover, per impostazione predefinita il servizio crea automaticamente una relazione di protezione inversa per ogni volume nel piano di replica, se il sito di origine originale è online. Ciò significa che il servizio crea una relazione SnapMirror dal sito di destinazione al sito di origine. Il servizio inverte automaticamente anche la relazione SnapMirror quando si avvia un failback.

Quando si avvia un failover, ora è possibile scegliere l'opzione **Salta protezione**. In questo modo il servizio non inverte automaticamente la relazione SnapMirror . Invece, lascia il volume scrivibile su entrambi i lati del piano di replicazione.

Dopo che il sito di origine originale è di nuovo online, è possibile stabilire 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.

Per i dettagli sulla protezione da salto, fare riferimento a "Eseguire il failover delle applicazioni su un sito remoto" .

Aggiornamenti della pianificazione SnapMirror nel piano di replica

NetApp Disaster Recovery supporta ora l'uso di soluzioni di gestione degli snapshot esterni, come lo scheduler di policy nativo ONTAP SnapMirror o integrazioni di terze parti con ONTAP. 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.

Per configurare, nella sezione Piano di replica > Mapping delle risorse, selezionare la casella di controllo **Usa backup e pianificazioni di conservazione gestiti dalla piattaforma** durante la configurazione del mapping dei datastore.

Quando l'opzione è selezionata, 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.

Per i dettagli sull'utilizzo di soluzioni snapshot esterne nel piano di replica, fare riferimento a "Creare un piano di replicazione" .

16 aprile 2025

Versione 4.2.2

Rilevamento pianificato per le VM

NetApp Disaster Recovery esegue la rilevazione una volta ogni 24 ore. Con questa versione, ora puoi personalizzare la pianificazione dell'individuazione in base alle tue esigenze e ridurre l'impatto sulle prestazioni quando necessario. Ad esempio, se si dispone di un numero elevato di VM, è possibile impostare la pianificazione dell'individuazione in modo che venga eseguita ogni 48 ore. 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 non si desidera pianificare l'individuazione, è possibile disattivare l'opzione di individuazione pianificata e aggiornare manualmente l'individuazione in qualsiasi momento.

Per i dettagli, fare riferimento a "Aggiungi siti server vCenter" .

Supporto del datastore del gruppo di risorse

In precedenza, era possibile creare gruppi di risorse solo tramite VM. Con questa versione è possibile creare un gruppo di risorse in base ai datastore. Quando si crea un piano di replicazione e si crea un gruppo di risorse per tale piano, verranno elencate tutte le VM in un datastore. Questa opzione è utile se si dispone di un numero elevato di VM e si desidera raggrupparle in base al datastore.

È possibile creare un gruppo di risorse con un 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.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Notifiche di prova gratuita o scadenza della licenza

Questa versione fornisce notifiche che la prova gratuita scadrà tra 60 giorni per garantire che tu abbia il tempo di ottenere una licenza. Questa versione fornisce anche notifiche il giorno in cui scade la licenza.

Notifica degli aggiornamenti del servizio

Con questa versione, nella parte superiore viene visualizzato un banner per indicare che i servizi vengono aggiornati e che il servizio è in modalità di manutenzione. Il banner appare quando il servizio è in fase di aggiornamento e scompare al termine dell'aggiornamento. Mentre l'aggiornamento è in corso, puoi continuare a lavorare nell'interfaccia utente, ma non puoi inviare nuovi lavori. I lavori pianificati verranno eseguiti una volta completato l'aggiornamento e il servizio tornerà in modalità di produzione.

10 marzo 2025

Versione 4.2.1

Supporto proxy intelligente

L'agente NetApp Console supporta il proxy intelligente. Il proxy intelligente è un modo leggero, sicuro ed efficiente per connettere il tuo sistema locale a NetApp Disaster Recovery. Fornisce una connessione sicura tra il tuo sistema e NetApp Disaster Recovery senza richiedere una VPN o un accesso diretto a Internet. Questa implementazione proxy ottimizzata scarica il traffico API all'interno della rete locale.

Quando viene configurato un proxy, NetApp Disaster Recovery tenta di comunicare direttamente con VMware o ONTAP e utilizza il proxy configurato se la comunicazione diretta fallisce.

L'implementazione del proxy NetApp Disaster Recovery richiede la comunicazione sulla porta 443 tra l'agente della console e tutti i server vCenter e gli array ONTAP che utilizzano un protocollo HTTPS. L'agente NetApp Disaster Recovery all'interno dell'agente Console comunica direttamente con VMware vSphere, VC o ONTAP quando esegue qualsiasi azione.

Per ulteriori informazioni sul proxy intelligente per NetApp Disaster Recovery, vedere "Configura la tua infrastruttura per NetApp Disaster Recovery" .

Per ulteriori informazioni sulla configurazione generale del proxy nella NetApp Console, vedere "Configurare l'agente della console per utilizzare un server proxy" .

Interrompi la prova gratuita in qualsiasi momento

Puoi interrompere la prova gratuita in qualsiasi momento oppure attendere la sua scadenza.

Vedere "Termina la prova gratuita" .

19 febbraio 2025

Versione 4.2

Supporto ASA r2 per VM e datastore su storage VMFS

Questa versione di NetApp Disaster Recovery fornisce supporto per ASA r2 per VM e datastore su storage VMFS. Su un sistema ASA r2, il software ONTAP supporta le funzionalità SAN essenziali, rimuovendo al contempo le funzionalità non supportate negli ambienti SAN.

Questa versione supporta le seguenti funzionalità per ASA r2:

- Provisioning del gruppo di coerenza per l'archiviazione primaria (solo gruppo di coerenza flat, ovvero un solo livello senza una struttura gerarchica)
- Operazioni di backup (gruppo di coerenza) inclusa l'automazione SnapMirror

Il supporto per ASA r2 in NetApp Disaster Recovery utilizza ONTAP 9.16.1.

Sebbene i datastore possano essere montati su un volume ONTAP o su un'unità di storage ASA r2, un gruppo di risorse in NetApp Disaster Recovery non può includere sia un datastore da ONTAP che uno da ASA r2. È possibile selezionare un datastore da ONTAP o un datastore da ASA r2 in un gruppo di risorse.

30 ottobre 2024

Segnalazione

Ora puoi generare e scaricare report che ti aiuteranno ad analizzare il tuo panorama. I report predefiniti riepilogano i failover e i failback, mostrano i dettagli della replica su tutti i siti e mostrano i dettagli dei processi degli ultimi sette giorni.

Fare riferimento a "Creare report di ripristino di emergenza" .

Prova gratuita di 30 giorni

Ora puoi registrarti per una prova gratuita di 30 giorni di NetApp Disaster Recovery. In precedenza, le prove gratuite duravano 90 giorni.

Fare riferimento a "Impostare la licenza" .

Disabilitare e abilitare i piani di replicazione

Una versione precedente includeva aggiornamenti alla struttura della pianificazione dei test di failover, necessari per supportare le pianificazioni giornaliere e settimanali. Questo aggiornamento richiedeva di disabilitare e riabilitare tutti i piani di replica esistenti, in modo da poter utilizzare le nuove pianificazioni dei test di failover giornalieri e settimanali. Si tratta di un requisito una tantum.

Ecco come fare:

1. Dal menu, seleziona **Piani di replicazione**.
2. Selezionare un piano e fare clic sull'icona Azioni per visualizzare il menu a discesa.
3. Selezionare **Disabilita**.
4. Dopo qualche minuto, seleziona **Abilita**.

Mappatura delle cartelle

Quando si crea un piano di replica e si mappano le risorse di elaborazione, è ora possibile mappare le cartelle in modo che le VM vengano ripristinate in una cartella specificata per data center, cluster e host.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Dettagli della VM disponibili per failover, failback e failover di prova

Quando si verifica un errore e si avvia un failover, si esegue un failback o si testa il failover, ora è possibile visualizzare i dettagli delle VM e identificare quali VM non sono state riavviate.

Fare riferimento a "Eseguire il failover delle applicazioni su un sito remoto" .

Ritardo di avvio della VM con sequenza di avvio ordinata

Quando si crea un piano di replica, è ora possibile impostare un ritardo di avvio per ogni macchina virtuale nel piano. Ciò consente di impostare una sequenza di avvio delle VM per garantire che tutte le VM con priorità uno siano in esecuzione prima dell'avvio delle VM con priorità successiva.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Informazioni sul sistema operativo della VM

Quando si crea un piano di replicazione, è ora possibile visualizzare il sistema operativo per ogni macchina virtuale nel piano. Ciò è utile per decidere come raggruppare le VM in un gruppo di risorse.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Aliasing del nome della VM

Quando si crea un piano di replica, è ora possibile aggiungere un prefisso e un suffisso ai nomi delle VM sul sito di disaster recovery. Ciò consente di utilizzare un nome più descrittivo per le VM nel piano.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Pulisci i vecchi snapshot

È possibile eliminare tutti gli snapshot che non sono più necessari oltre il numero di conservazione specificato. Gli snapshot potrebbero accumularsi nel tempo quando si riduce il numero di snapshot conservati; ora è possibile rimuoverli per liberare spazio. Puoi farlo in qualsiasi momento su richiesta o quando elimini un piano di replicazione.

Per i dettagli, fare riferimento a "Gestisci siti, gruppi di risorse, piani di replica, datastore e informazioni sulle macchine virtuali" .

Riconciliare gli snapshot

Ora puoi riconciliare gli snapshot non sincronizzati tra l'origine e la destinazione. Ciò potrebbe verificarsi se gli snapshot vengono eliminati su una destinazione esterna a NetApp Disaster Recovery. Il servizio elimina automaticamente lo snapshot sulla sorgente ogni 24 ore. Tuttavia, è possibile eseguire questa operazione su richiesta. Questa funzionalità consente di garantire che gli snapshot siano coerenti in tutti i siti.

Per i dettagli, fare riferimento a "Gestire i piani di replicazione" .

20 settembre 2024

Supporto per datastore VMware VMFS da locale a locale

Questa versione include il supporto per le VM montate su datastore VMware vSphere Virtual Machine File System (VMFS) per iSCSI e FC protetti su storage locale. In precedenza, il servizio forniva un'anteprima tecnologica che supportava gli archivi dati VMFS per iSCSI e FC.

Ecco alcune considerazioni aggiuntive riguardanti i protocolli iSCSI e FC:

- Il supporto FC è per i protocolli front-end client, non per la replica.
- NetApp Disaster Recovery supporta solo una singola LUN per volume ONTAP . Il volume non deve avere più LUN.
- Per qualsiasi piano di replica, il volume ONTAP di destinazione deve utilizzare gli stessi protocolli del volume ONTAP di origine che ospita le VM protette. Ad esempio, se la sorgente utilizza un protocollo FC, anche la destinazione dovrebbe utilizzare FC.

02 agosto 2024

Supporto per datastore VMware VMFS da locale a locale per FC

Questa versione include un'anteprima tecnologica del supporto per le VM montate su datastore VMware vSphere Virtual Machine File System (VMFS) per FC protette su storage locale. In precedenza, il servizio forniva un'anteprima tecnologica che supportava i datastore VMFS per iSCSI.

NetApp non addebita alcun costo per la capacità di carico di lavoro visualizzata in anteprima.

Annullamento del lavoro

Con questa versione, è ora possibile annullare un lavoro nell'interfaccia utente di Job Monitor.

Fare riferimento a "Monitorare i lavori" .

17 luglio 2024

Pianificazioni dei test di failover

Questa versione include aggiornamenti alla struttura della pianificazione dei test di failover, necessari per supportare le pianificazioni giornaliere e settimanali. Questo aggiornamento richiede di disabilitare e riabilitare tutti i piani di replica esistenti, in modo da poter utilizzare le nuove pianificazioni dei test di failover giornalieri e settimanali. Si tratta di un requisito una tantum.

Ecco come fare:

1. Dal menu, seleziona **Piani di replicazione**.
2. Selezionare un piano e fare clic sull'icona Azioni per visualizzare il menu a discesa.
3. Selezionare **Disabilita**.
4. Dopo qualche minuto, seleziona **Abilita**.

Aggiornamenti del piano di replicazione

Questa versione include aggiornamenti ai dati del piano di replica, che risolvono il problema "snapshot non trovato". Per fare ciò, è necessario modificare il conteggio di conservazione in tutti i piani di replica su 1 e avviare uno snapshot su richiesta. Questo processo crea un nuovo backup e rimuove tutti i backup precedenti.

Ecco come fare:

1. Dal menu, seleziona **Piani di replicazione**.
2. Selezionare il piano di replicazione, selezionare la scheda **Failover mapping** e selezionare l'icona della matita **Modifica**.
3. Selezionare la freccia **Datastore** per espanderla.
4. Prendere nota del valore del conteggio di conservazione nel piano di replica. Una volta completati questi passaggi, è necessario ripristinare il valore originale.
5. Ridurre il conteggio a 1.
6. Avvia uno snapshot su richiesta. Per farlo, nella pagina Piano di replica, seleziona il piano, seleziona l'icona Azioni e seleziona **Esegui snapshot ora**.
7. Dopo aver completato correttamente il processo di snapshot, riportare il conteggio nel piano di replica al valore originale annotato nel primo passaggio.
8. Ripetere questi passaggi per tutti i piani di replicazione esistenti.

05 luglio 2024

Questa versione NetApp Disaster Recovery include i seguenti aggiornamenti:

Supporto per la serie AFF A

Questa versione supporta le piattaforme hardware NetApp AFF serie A.

Supporto per datastore VMware VMFS da locale a locale

Questa versione include un'anteprima tecnologica del supporto per le VM montate su datastore VMware vSphere Virtual Machine File System (VMFS) protetti su storage locale. Con questa versione, il disaster recovery è supportato in un'anteprima tecnologica per carichi di lavoro VMware on-premise in ambienti VMware on-premise con datastore VMFS.

NetApp non addebita alcun costo per la capacità di carico di lavoro visualizzata in anteprima.

Aggiornamenti del piano di replicazione

È possibile aggiungere un piano di replicazione più facilmente filtrando le VM in base all'archivio dati nella pagina Applicazioni e selezionando maggiori dettagli sulla destinazione nella pagina Mappatura risorse. Fare riferimento a "Creare un piano di replicazione" .

Modifica i piani di replicazione

Con questa versione, la pagina dei mapping di failover è stata migliorata per renderla più chiara.

Fare riferimento a "Gestire i piani" .

Modifica VM

Con questa versione, il processo di modifica delle VM nel piano ha incluso alcuni piccoli miglioramenti all'interfaccia utente.

Fare riferimento a "Gestire le VM" .

Aggiornamenti failover

Prima di avviare un failover, è ora possibile determinare lo stato delle VM e se sono accese o spente. Il processo di failover ora consente di acquisire uno snapshot subito o di scegliere gli snapshot.

Fare riferimento a "Eseguire il failover delle applicazioni su un sito remoto" .

Pianificazioni dei test di failover

Ora è possibile modificare i test di failover e impostare pianificazioni giornaliere, settimanali e mensili per i test di failover.

Fare riferimento a "Gestire i piani" .

Aggiornamenti alle informazioni prerequisite

Le informazioni sui prerequisiti NetApp Disaster Recovery sono state aggiornate.

Fare riferimento a "Prerequisiti NetApp Disaster Recovery" .

15 maggio 2024

Questa versione NetApp Disaster Recovery include i seguenti aggiornamenti:

Replica dei carichi di lavoro VMware da locale a locale

Questa funzionalità è ora disponibile a tutti. In precedenza si trattava di un'anteprima tecnologica con funzionalità limitate.

Aggiornamenti sulle licenze

Con NetApp Disaster Recovery puoi registrarti per una prova gratuita di 90 giorni, acquistare un abbonamento pay-as-you-go (PAYGO) con Amazon Marketplace o Bring Your Own License (BYOL), ovvero un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante commerciale NetApp o dal sito di supporto NetApp (NSS).

Per i dettagli sulla configurazione delle licenze per NetApp Disaster Recovery, fare riferimento a"Impostare la licenza" .

"Scopri di più su NetApp Disaster Recovery".

05 marzo 2024

Questa è la versione di disponibilità generale di NetApp Disaster Recovery, che include i seguenti aggiornamenti.

Aggiornamenti sulle licenze

Con NetApp Disaster Recovery puoi registrarti per una prova gratuita di 90 giorni oppure puoi optare per la soluzione BYOL (Bring Your Own License), ovvero un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante commerciale NetApp . È possibile utilizzare il numero di serie della licenza per attivare BYOL negli abbonamenti NetApp Console . I costi di NetApp Disaster Recovery si basano sulla capacità fornita dei datastore.

Per i dettagli sulla configurazione delle licenze per NetApp Disaster Recovery, fare riferimento a "Impostare la licenza" .

Per i dettagli sulla gestione delle licenze per **tutti** i servizi dati NetApp Console , fare riferimento a "Gestisci le licenze per tutti i servizi dati NetApp Console" .

Modificare gli orari

Con questa versione, è ora possibile impostare pianificazioni per testare la conformità e i test di failover, in modo da garantire che funzionino correttamente quando necessario.

Per i dettagli, fare riferimento a "Creare il piano di replicazione" .

01 febbraio 2024

Questa versione di anteprima NetApp Disaster Recovery include i seguenti aggiornamenti:

Miglioramento della rete

Con questa versione è ora possibile ridimensionare i valori della CPU e della RAM della VM. Ora è anche possibile selezionare un indirizzo IP statico o DHCP di rete per la VM.

- DHCP: se si sceglie questa opzione, è necessario fornire le credenziali per la VM.
- IP statico: è possibile selezionare le stesse informazioni o informazioni diverse dalla VM di origine. 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, la maschera di sottorete, il DNS e le informazioni sul gateway.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Script personalizzati

Ora possono essere inclusi come processi post-failover. Con gli script personalizzati, puoi far sì che NetApp Disaster Recovery esegua lo script dopo un processo di failover. Ad esempio, è possibile utilizzare uno script personalizzato per riprendere tutte le transazioni del database una volta completato il failover.

Per i dettagli, fare riferimento a "Failover su un sito remoto" .

Relazione SnapMirror

Ora è possibile creare una relazione SnapMirror durante lo sviluppo del piano di replica. In precedenza, era

necessario creare la relazione all'esterno di NetApp Disaster Recovery.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Gruppi di coerenza

Quando si crea un piano di replica, è possibile includere VM provenienti da volumi diversi e SVM diversi. NetApp Disaster Recovery crea uno snapshot del gruppo di coerenza includendo tutti i volumi e aggiorna tutte le posizioni secondarie.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Opzione di ritardo di accensione della VM

Quando si crea un piano di replicazione, è possibile aggiungere VM a un gruppo di risorse. Con i gruppi di risorse è possibile impostare un ritardo su ogni macchina virtuale in modo che si accendano in una sequenza ritardata.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

Copie snapshot coerenti con l'applicazione

È possibile specificare di 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.

Per i dettagli, fare riferimento a "Creare un piano di replicazione" .

11 gennaio 2024

Questa versione di anteprima di NetApp Disaster Recovery include i seguenti aggiornamenti:

Dashboard più veloce

Con questa versione, è possibile accedere più rapidamente alle informazioni su altre pagine della Dashboard.

"Scopri di più su NetApp Disaster Recovery".

20 ottobre 2023

Questa versione di anteprima di NetApp Disaster Recovery include i seguenti aggiornamenti.

Proteggere i carichi di lavoro VMware basati su NFS in sede

Ora con NetApp Disaster Recovery puoi proteggere i tuoi carichi di lavoro VMware on-premise basati su NFS da disastri su un altro ambiente VMware on-premise basato su NFS, oltre che sul cloud pubblico. NetApp Disaster Recovery orchestra il completamento dei piani di disaster recovery.

> Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

"Scopri di più su NetApp Disaster Recovery".

27 settembre 2023

Questa versione di anteprima di NetApp Disaster Recovery include i seguenti aggiornamenti:

Aggiornamenti della dashboard

Ora puoi selezionare le opzioni nella Dashboard, rendendo più semplice e veloce la consultazione delle informazioni. Inoltre, la Dashboard ora mostra lo stato dei failover e delle migrazioni.

Fare riferimento a "Visualizza lo stato di salute dei tuoi piani di disaster recovery nella Dashboard" .

Aggiornamenti del piano di replicazione

- **RPO**: ora è possibile immettere l'RPO (Recovery Point Objective) e il conteggio della conservazione nella sezione Datastore del piano di replica. Indica la quantità di dati che devono esistere e che non siano più vecchi del tempo impostato. Ad esempio, se lo si imposta su 5 minuti, in caso di disastro il sistema può perdere fino a 5 minuti di dati senza compromettere le esigenze aziendali critiche.

  Fare riferimento a "Creare un piano di replicazione" .

- **Miglioramenti della rete**: quando si esegue il mapping della rete tra le posizioni di origine e di destinazione nella sezione delle macchine virtuali del piano di replica, NetApp Disaster Recovery offre ora due opzioni: DHCP o IP statico. In precedenza era supportato solo DHCP. Per gli IP statici, è necessario configurare la subnet, il gateway e i server DNS. Inoltre, ora è possibile immettere le credenziali per le macchine virtuali.

  Fare riferimento a "Creare un piano di replicazione" .

- **Modifica pianificazioni**: ora puoi aggiornare le pianificazioni del piano di replicazione.

  Fare riferimento a "Gestire le risorse" .

- * Automazione SnapMirror *: durante la creazione del piano di replica in questa versione, è possibile definire la relazione SnapMirror tra volumi di origine e di destinazione in una delle seguenti configurazioni:
  - 1 a 1
  - 1 a molti in un'architettura fanout
  - Molti a 1 come gruppo di coerenza
  - Molti a molti

    Fare riferimento a "Creare un piano di replicazione" .

01 agosto 2023

Anteprima di NetApp Disaster Recovery

NetApp Disaster Recovery Preview è un servizio di disaster recovery basato su cloud che automatizza i flussi di lavoro di disaster recovery. Inizialmente, con l'anteprima di NetApp Disaster Recovery , puoi proteggere i tuoi carichi di lavoro VMware on-premise basati su NFS che eseguono lo storage NetApp su VMware Cloud (VMC) su AWS con Amazon FSx for ONTAP.

Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

"Scopri di più su NetApp Disaster Recovery".

Questa versione include i seguenti aggiornamenti:

Aggiornamento dei gruppi di risorse per l'ordine di avvio

Quando si crea un piano di disaster recovery o di replicazione, è possibile aggiungere macchine virtuali a gruppi di risorse funzionali. I gruppi di risorse consentono di inserire un set di macchine virtuali dipendenti in gruppi logici che soddisfano i requisiti. Ad esempio, i gruppi potrebbero contenere un ordine di avvio che può essere eseguito al momento del ripristino. Con questa versione, ogni gruppo di risorse può includere una o più macchine virtuali. Le macchine virtuali si accenderanno in base alla sequenza in cui le hai incluse nel piano. Fare riferimento a "Selezionare le applicazioni da replicare e assegnare gruppi di risorse" .

Verifica della replicazione

Dopo aver creato il piano di disaster recovery o di replica, 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. Fare riferimento a "Replicare le applicazioni su un altro sito" .

Il piano di replicazione mostra le pianificazioni di trasferimento dell'obiettivo del punto di ripristino (RPO)

Quando si crea un piano di disaster recovery o di replicazione, si selezionano le VM. In questa versione è ora possibile visualizzare lo SnapMirror associato a ciascuno dei volumi associati al datastore o alla VM. È anche possibile visualizzare le pianificazioni dei trasferimenti RPO associate alla pianificazione SnapMirror . RPO ti aiuta a determinare se la tua pianificazione di backup è sufficiente per il ripristino dopo un disastro. Fare riferimento a "Creare un piano di replicazione" .

Aggiornamento del Job Monitor

La pagina Job Monitor ora include un'opzione Aggiorna, che consente di ottenere uno stato aggiornato delle operazioni. Fare riferimento a "Monitorare i lavori di ripristino di emergenza" .

18 maggio 2023

Questa è la versione iniziale di NetApp Disaster Recovery.

Servizio di disaster recovery basato su cloud

NetApp Disaster Recovery è un servizio di disaster recovery basato su cloud che automatizza i flussi di lavoro di disaster recovery. Inizialmente, con l'anteprima di NetApp Disaster Recovery , puoi proteggere i tuoi carichi di lavoro VMware on-premise basati su NFS che eseguono lo storage NetApp su VMware Cloud (VMC) su AWS con Amazon FSx for ONTAP.

"Scopri di più su NetApp Disaster Recovery".

Limitazioni nel NetApp Disaster Recovery

Le limitazioni note identificano piattaforme, dispositivi o funzioni che non sono supportati da questa versione del servizio o che non interagiscono correttamente con esso.

Attendi il completamento del failback prima di eseguire l'individuazione

Una volta completato un failover, non avviare manualmente l'individuazione sul vCenter di origine. Attendere il completamento del failback, quindi avviare l'individuazione sul vCenter di origine.

La NetApp Console potrebbe non rilevare Amazon FSx for NetApp ONTAP

A volte, la NetApp Console non rileva i cluster Amazon FSx for NetApp ONTAP . Ciò potrebbe essere dovuto al fatto che le credenziali FSx non erano corrette.

Soluzione alternativa: aggiungere il cluster Amazon FSx for NetApp ONTAP nella NetApp Console e aggiornare periodicamente il cluster per visualizzare eventuali modifiche.

Se è necessario rimuovere il cluster ONTAP FSx da NetApp Disaster Recovery, completare i seguenti passaggi:

1. Nell'agente NetApp Console , utilizzare le opzioni di connettività del provider cloud, connettersi alla VM Linux su cui è in esecuzione l'agente Console, riavviare il servizio "occm" utilizzando `docker restart occm` comando.

Fare riferimento a "Gestisci gli agenti della console esistenti" .

1. Nella pagina Sistemi NetApp Console , aggiungere nuovamente il sistema Amazon FSx for ONTAP e fornire le credenziali FSx.

   Fare riferimento a "Creare un file system Amazon FSx for NetApp ONTAP" .

2. Da NetApp Disaster Recovery, seleziona **Siti**, nella riga vCenter seleziona l'opzione **Azioni***  **e dal menu Azioni, seleziona *Aggiorna** per aggiornare la scoperta FSx in NetApp Disaster Recovery.

   In questo modo si riscopre l'archivio dati, le sue macchine virtuali e la sua relazione di destinazione.

Limitazioni con Google Cloud NetApp Volumes

- Dopo aver eseguito un test di failover, è necessario attendere almeno 52 ore per eliminare il volume clone. È necessario eliminare il volume manualmente. Dopo 52 ore, è possibile testare nuovamente il failover.
- Se una qualsiasi parte dell'operazione di montaggio fallisce, il failover non avrà esito positivo e i processi scadranno. Google impiega fino a tre giorni per esaminare il problema, durante i quali tutte le operazioni relative al datastore su vCenter vengono bloccate.

Iniziare

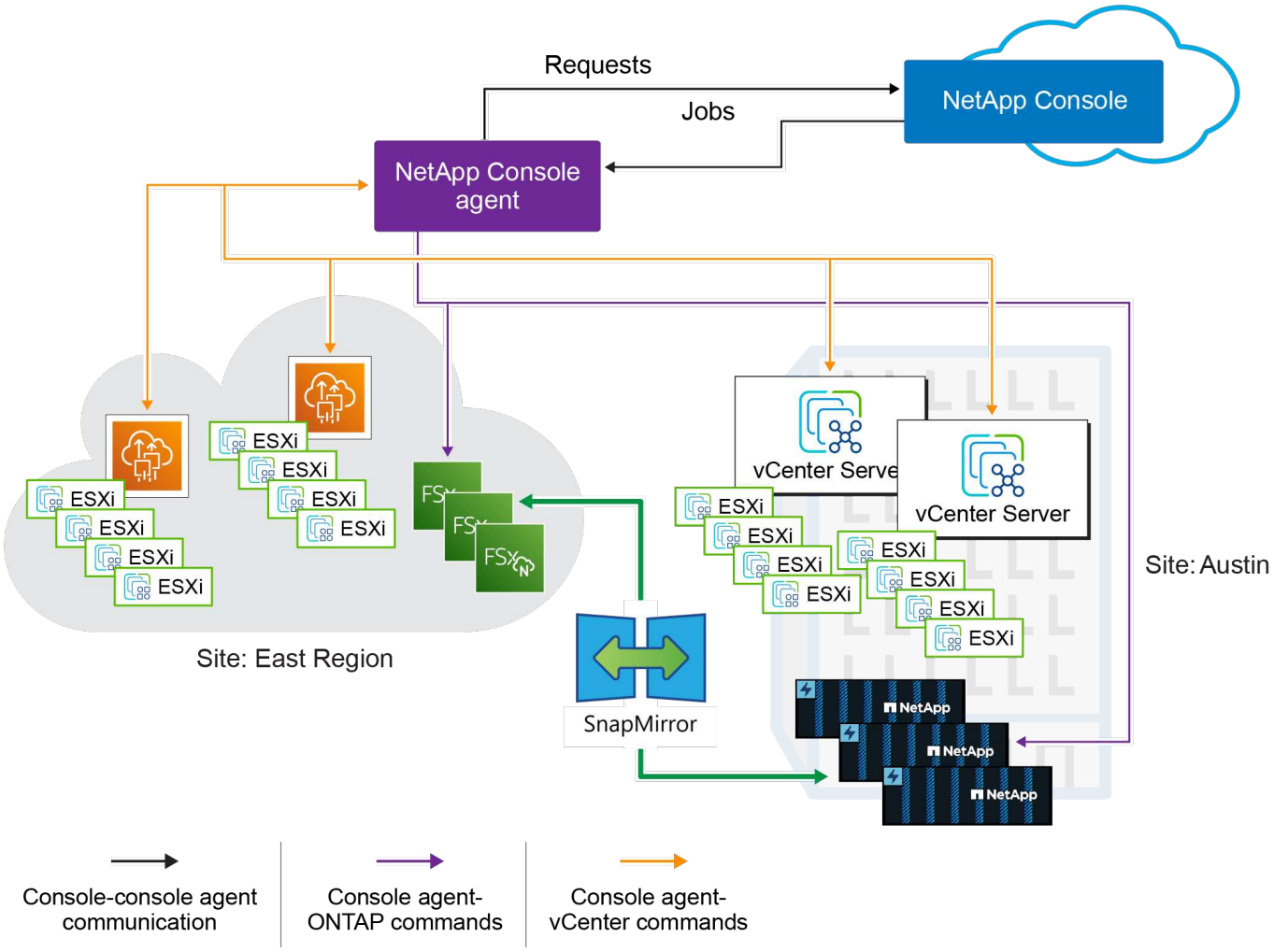
Scopri di più su NetApp Disaster Recovery per VMware

Il disaster recovery nel cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati. Con NetApp Disaster Recovery per VMware, puoi replicare i carichi di lavoro delle VM VMware o dei datastore locali che eseguono lo storage ONTAP in un data center software-defined VMware in un cloud pubblico utilizzando lo storage cloud NetApp o in un altro ambiente VMware locale con storage ONTAP come sito di disaster recovery. È possibile utilizzare Disaster Recovery anche per migrare i carichi di lavoro delle VM da un sito all'altro.

NetApp Disaster Recovery è un servizio di disaster recovery basato su cloud che automatizza i flussi di lavoro di disaster recovery. Con NetApp Disaster Recovery puoi proteggere i tuoi carichi di lavoro locali basati su NFS e i datastore VMware vSphere Virtual Machine File System (VMFS) per iSCSI e FC che eseguono lo storage NetApp su uno dei seguenti:

- Amazon Elastic VMware Service (EVS) con Amazon FSx for NetApp ONTAP Per i dettagli, fare riferimento a"Introduzione di NetApp Disaster Recovery tramite Amazon Elastic VMware Service e Amazon FSx for NetApp ONTAP" .
- VMware Cloud (VMC) su AWS con Amazon FSx for NetApp ONTAP
- Soluzione Azure VMware (AVS) con NetApp Cloud Volumes ONTAP (iSCSI) (anteprima privata)
- Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes
- Un altro ambiente VMware basato su NFS e/o VMFS (iSCSI/FC) in sede con storage ONTAP

NetApp Disaster Recovery utilizza la tecnologia ONTAP SnapMirror con orchestrazione VMware nativa integrata per proteggere le VM VMware e le relative immagini del sistema operativo su disco, mantenendo al contempo tutti i vantaggi di efficienza di storage di ONTAP. Il Disaster Recovery utilizza queste tecnologie come trasporto di replica al sito di disaster recovery. Ciò consente la migliore efficienza di archiviazione del settore (compressione e deduplicazione) sui siti primari e secondari.



NetApp Console

È possibile accedere a NetApp Disaster Recovery tramite la NetApp Console.

NetApp Console offre una gestione centralizzata dei servizi di storage e dati NetApp in ambienti on-premise e cloud di livello aziendale. La console è necessaria per accedere e utilizzare i servizi dati NetApp . In quanto interfaccia di gestione, consente di gestire numerose risorse di archiviazione da un'unica interfaccia. Gli amministratori della console possono controllare l'accesso allo storage e ai servizi per tutti i sistemi all'interno dell'azienda.

Per iniziare a utilizzare NetApp Console non è necessaria una licenza o un abbonamento e verranno addebitati costi solo quando sarà necessario distribuire gli agenti della console nel cloud per garantire la connettività ai sistemi di storage o ai servizi dati NetApp . Tuttavia, alcuni servizi dati NetApp accessibili dalla Console sono concessi in licenza o basati su abbonamento.

Scopri di più su "NetApp Console" .

Vantaggi dell'utilizzo di NetApp Disaster Recovery per VMware

NetApp Disaster Recovery offre i seguenti vantaggi:

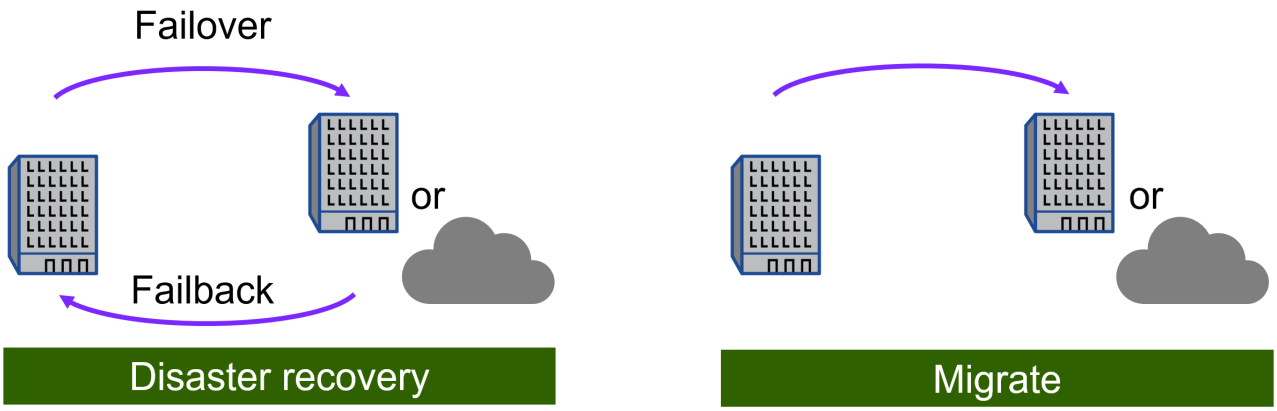
- Esperienza utente semplificata per l'individuazione e il ripristino delle applicazioni in vCenter con più operazioni di ripristino point-in-time.

- Minore costo totale di proprietà con riduzione dei costi operativi e possibilità di creare e adattare piani di disaster recovery con risorse minime.
- Prontezza continua al ripristino in caso di emergenza con test di failover virtuale che non interrompono le operazioni. È possibile testare regolarmente i piani di failover DR senza influire sui carichi di lavoro di produzione.
- Tempi di attuazione più rapidi grazie a cambiamenti dinamici nel tuo ambiente IT e alla possibilità di affrontarli nei tuoi piani di disaster recovery.
- Possibilità di gestire sia lo storage che i livelli virtuali tramite l'orchestrazione backend di ONTAP e VMware contemporaneamente, senza la necessità di appliance server virtuali (VSA) da distribuire e gestire.
- Le soluzioni DR per VMware possono richiedere molte risorse. Molte soluzioni DR replicano le VM a livello virtuale VMware utilizzando VSA, che possono consumare più risorse di elaborazione e perdere le preziose efficienze di archiviazione di ONTAP. Poiché Disaster Recovery utilizza la tecnologia ONTAP SnapMirror , è in grado di replicare i dati dagli archivi dati di produzione al sito DR utilizzando il nostro modello di replica incrementale-perenne con tutte le efficienze di compressione e deduplicazione dei dati nativi di ONTAP.

Cosa puoi fare con NetApp Disaster Recovery per VMware

NetApp Disaster Recovery ti consente di sfruttare appieno diverse tecnologie NetApp per raggiungere i seguenti obiettivi:

- Replica le app VMware dal tuo sito di produzione locale a un sito remoto di disaster recovery nel cloud o in locale utilizzando la replica SnapMirror .
- Migra i carichi di lavoro VMware dal tuo sito originale a un altro sito.
- Eseguire un test di failover. Quando si esegue questa operazione, il servizio crea macchine virtuali temporanee. Disaster Recovery crea un nuovo volume FlexClone dallo snapshot selezionato e un datastore temporaneo, supportato dal volume FlexClone , viene mappato 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.
- In caso di disastro, esegui il failover del tuo sito primario su richiesta sul sito di disaster recovery, che può essere VMware Cloud su AWS con Amazon FSx for NetApp ONTAP o un ambiente VMware locale con ONTAP.
- Dopo aver risolto il disastro, eseguire il failback su richiesta dal sito di disaster recovery al sito primario.
- Raggruppare le VM o gli archivi dati in gruppi di risorse logici per una gestione efficiente.



La configurazione del server vSphere viene eseguita al di fuori di NetApp Disaster Recovery in vSphere Server.

Costo

NetApp non addebita alcun costo per l'utilizzo della versione di prova di NetApp Disaster Recovery.

NetApp Disaster Recovery può essere utilizzato con una licenza NetApp o con un piano di abbonamento annuale tramite Amazon Web Services.

Alcune versioni includono un'anteprima tecnologica. NetApp non addebita alcun costo per la capacità di carico di lavoro visualizzata in anteprima. Vedere"Novità di NetApp Disaster Recovery" per informazioni sulle ultime anteprime tecnologiche.

Licenza

È possibile utilizzare i seguenti tipi di licenza:

- Registrati per una prova gratuita di 30 giorni.
- Acquista un abbonamento pay-as-you-go (PAYGO) con Amazon Web Services (AWS) Marketplace o Microsoft Azure Marketplace. Questa licenza consente di acquistare una licenza a capacità protetta fissa senza alcun impegno a lungo termine.
- Bring your own license (BYOL), ovvero un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante commerciale NetApp . È possibile utilizzare il numero di serie della licenza per attivare BYOL nella NetApp Console.

Le licenze per tutti i servizi dati NetApp vengono gestite tramite abbonamenti nella NetApp Console. Dopo aver configurato BYOL, nella Console potrai vedere una licenza attiva per il servizio.

La licenza del servizio è basata sulla quantità di dati ospitati sui volumi ONTAP protetti. Il servizio determina quali volumi devono essere presi in considerazione ai fini della licenza, mappando le VM protette ai rispettivi datastore vCenter. Ogni datastore è ospitato su un volume ONTAP o LUN. La capacità utilizzata segnalata da ONTAP per quel volume o LUN viene utilizzata per le determinazioni delle licenze.

I volumi protetti possono ospitare molte VM. Alcuni potrebbero non far parte di un gruppo di risorse NetApp

Disaster Recovery . In ogni caso, lo spazio di archiviazione utilizzato da tutte le VM su quel volume o LUN viene utilizzato per raggiungere la capacità massima della licenza.

> I costi NetApp Disaster Recovery si basano sulla capacità utilizzata dei datastore sul sito di origine quando è presente almeno una VM dotata di un piano di replica. La capacità per un datastore sottoposto a failover non è inclusa nella capacità consentita. Per un BYOL, se i dati superano la capacità consentita, le operazioni nel servizio sono limitate finché non si ottiene una licenza di capacità aggiuntiva o non si aggiorna la licenza nella NetApp Console.

Per i dettagli sulla configurazione delle licenze per NetApp Disaster Recovery, fare riferimento a"Impostare la licenza NetApp Disaster Recovery" .

Prova gratuita di 30 giorni

Puoi provare NetApp Disaster Recovery utilizzando la versione di prova gratuita di 30 giorni.

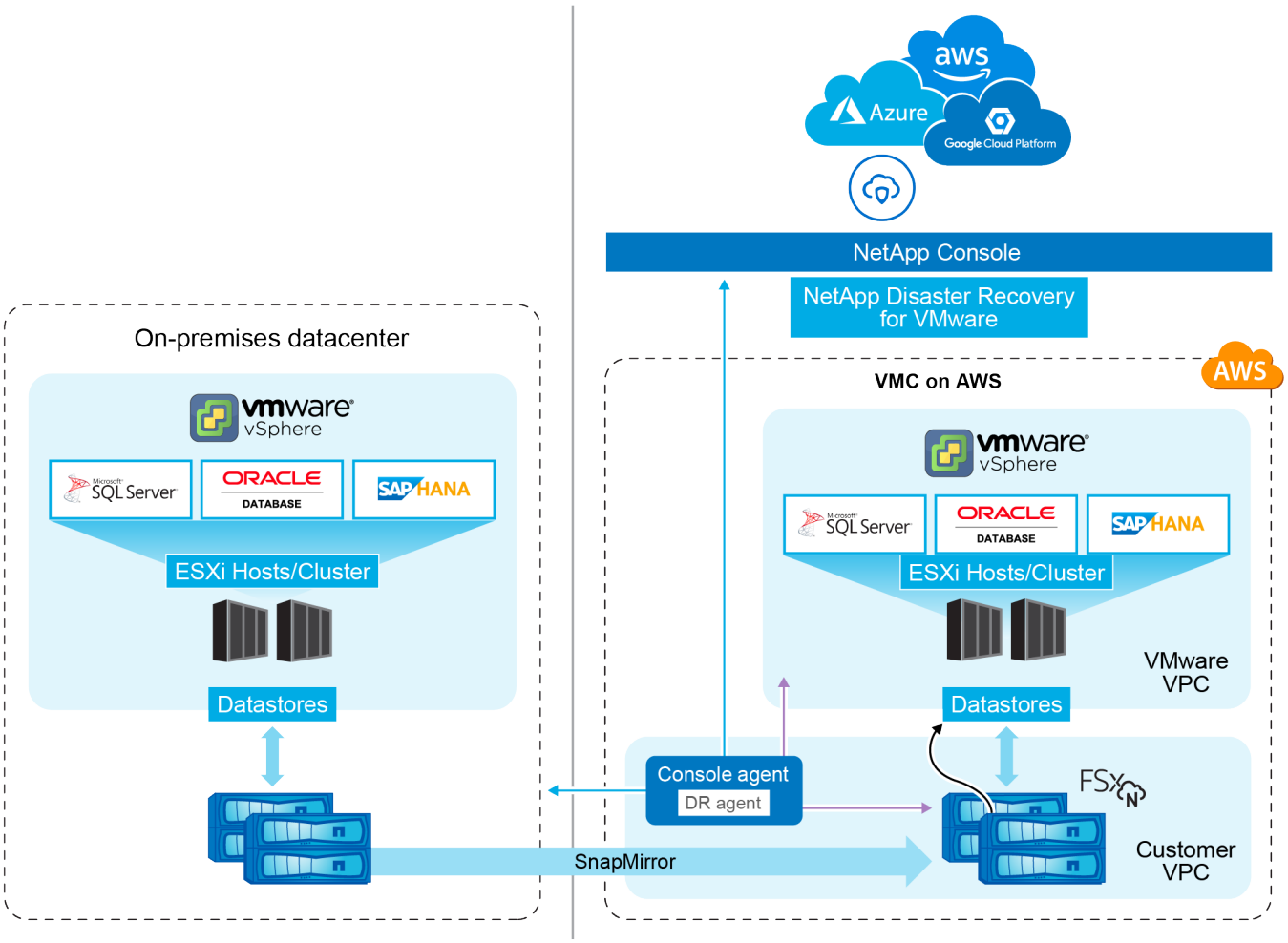
Per continuare dopo il periodo di prova di 30 giorni, dovrai ottenere un abbonamento Pay-as-you-go (PAYGO) dal tuo provider cloud o acquistare una licenza BYOL da NetApp.

Puoi acquistare una licenza in qualsiasi momento e non ti verrà addebitato alcun costo fino al termine del periodo di prova di 30 giorni.

Come funziona NetApp Disaster Recovery

NetApp Disaster Recovery è un servizio ospitato nell'ambiente SaaS (Software as a Service) NetApp Console . Disaster Recovery può ripristinare carichi di lavoro replicati da un sito locale ad Amazon FSx for ONTAP o a un altro sito locale. Questo servizio automatizza il ripristino dal livello SnapMirror , tramite la registrazione della macchina virtuale su VMware Cloud su AWS e la mappatura di rete direttamente sulla piattaforma di virtualizzazione e sicurezza di rete VMware, NSX-T. Questa funzionalità è inclusa in tutti gli ambienti Virtual Machine Cloud.

NetApp Disaster Recovery utilizza la tecnologia ONTAP SnapMirror , che garantisce una replica altamente efficiente e preserva l'efficienza degli snapshot incrementali e permanenti ONTAP . La replica SnapMirror garantisce che le copie snapshot coerenti con l'applicazione siano sempre sincronizzate e che i dati siano utilizzabili immediatamente dopo un failover.



In caso di emergenza, questo servizio consente di ripristinare le macchine virtuali nell'altro ambiente VMware locale o VMC interrompendo le relazioni SnapMirror e rendendo attivo il sito di destinazione.

- Il servizio consente inoltre di eseguire il failback delle macchine virtuali nella posizione di origine.
- È possibile testare il processo di failover del disaster recovery senza interrompere le macchine virtuali originali. Il test ripristina le macchine virtuali su una rete isolata creando un FlexClone del volume.
- Per il processo di failover o di test failover, puoi scegliere lo snapshot più recente (predefinito) o selezionato da cui ripristinare la macchina virtuale.

Componenti del Disaster Recovery

Disaster Recovery utilizza i seguenti componenti per garantire il ripristino di emergenza per i carichi di lavoro VMware:

- * NetApp Console*: l'interfaccia utente per la gestione dei piani di disaster recovery. Puoi utilizzare la NetApp Console per creare e gestire piani di replica, gruppi di risorse e operazioni di failover nei tuoi ambienti on-premise e cloud.
- **Agente console**: un componente software leggero che viene eseguito nella rete ospitata nel cloud o nell'ambiente VMware locale. Comunica con la NetApp Console e gestisce la replica dei dati tra l'ambiente locale e il sito di disaster recovery. L'agente Console è installato su una macchina virtuale nel tuo ambiente VMware.
- * Cluster di archiviazione ONTAP *: i cluster di archiviazione ONTAP sono i sistemi di archiviazione

principali che ospitano i carichi di lavoro VMware. I cluster di archiviazione ONTAP forniscono l'infrastruttura di archiviazione di base per i piani di disaster recovery. Disaster Recovery utilizza le API di archiviazione ONTAP per gestire cluster di archiviazione ONTAP quali array locali e soluzioni basate su cloud, come Amazon FSx for NetApp ONTAP.

- **Server vCenter**: VMware vCenter è il server di gestione per l'ambiente VMware. Gestisce gli host ESXi e i relativi datastore. L'agente Console comunica con VMware vCenter per gestire la replica dei dati tra l'ambiente locale e il sito di disaster recovery. Ciò include la registrazione di LUN e volumi ONTAP come datastore, la riconfigurazione delle VM e l'avvio e l'arresto delle VM.

Il flusso di lavoro di protezione del Disaster Recovery

Quando un piano di replica viene assegnato a un gruppo di risorse, Disaster Recovery esegue un controllo di individuazione di tutti i componenti nel gruppo di risorse e nel piano per garantire che il piano possa essere attivato.

Se questo controllo ha esito positivo, Disaster Recovery esegue i seguenti passaggi di inizializzazione:

1. Per ogni VM nel gruppo di risorse di destinazione, identificare il datastore VMware di hosting.
2. Per ogni datastore VMware trovato, identificare il FlexVol volume o LUN ONTAP di hosting.
3. Per ogni volume ONTAP e LUN trovati, determinare se esiste una relazione SnapMirror tra i volumi di origine e un volume di destinazione nel sito di destinazione.
    a. Se non esiste alcuna relazione SnapMirror preesistente, creare nuovi volumi di destinazione e una nuova relazione SnapMirror tra ciascun volume di origine non protetto.
    b. Se esiste una relazione SnapMirror preesistente, utilizzare tale relazione per eseguire tutte le operazioni di replica.

Dopo che Disaster Recovery ha creato e inizializzato tutte le relazioni, a ogni backup pianificato il servizio esegue i seguenti passaggi di protezione dei dati:

1. Per ogni VM contrassegnata come "coerente con l'applicazione", utilizzare VMtools per impostare l'applicazione supportata su uno stato di backup.
2. Crea un nuovo snapshot di tutti i volumi ONTAP che ospitano datastore VMware protetti.
3. Eseguire un'operazione di aggiornamento SnapMirror per replicare tali snapshot nel cluster ONTAP di destinazione.
4. Determinare se il numero di snapshot conservati ha superato la conservazione massima degli snapshot definita nel piano di replica ed eliminare eventuali snapshot estranei sia dal volume di origine che da quello di destinazione.

Destinazioni di protezione supportate e tipi di datastore

Tipi di datastore supportati NetApp Disaster Recovery supporta i seguenti tipi di datastore:

- Datastore NFS ospitati su volumi ONTAP FlexVol residenti su cluster ONTAP .
- Datastore del file system della macchina virtuale VMware vSphere (VMFS) che utilizzano il protocollo iSCSI o FC

Obiettivi di protezione supportati

- VMware Cloud (VMC) su AWS con Amazon FSx for NetApp ONTAP
- Un altro ambiente VMware basato su NFS in sede con storage ONTAP o un VMSF FC/iSCSI in sede

- Servizio Amazon Elastic VMware
- Soluzione Azure VMware (AVS) con NetApp Cloud Volumes ONTAP (iSCSI) (anteprima privata)
- Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes

Termini che potrebbero aiutarti con NetApp Disaster Recovery

Potrebbe essere utile comprendere la terminologia relativa al disaster recovery.

- **Datastore**: un contenitore dati VMware vCenter che utilizza un file system per contenere i file VMDK. I tipi di datastore tipici sono NFS, VMFS, vSAN o vVol. Disaster Recovery supporta i datastore NFS e VMFS. Ogni datastore VMware è ospitato su un singolo volume ONTAP o LUN. Disaster Recovery supporta datastore NFS e VMFS ospitati su volumi FlexVol residenti su cluster ONTAP .
- **Piano di replicazione**: un insieme di regole sulla frequenza con cui vengono eseguiti i backup e su come gestire gli eventi di failover. I piani vengono assegnati a uno o più gruppi di risorse.
- **Recovery Point Objective (RPO)**: la quantità massima di perdita di dati accettabile in caso di disastro. L'RPO è definito nella frequenza di replicazione dei dati o nella pianificazione della replicazione del piano di replica.
- **Obiettivo temporale di ripristino (RTO)**: il tempo massimo accettabile per il ripristino dopo un disastro. L'RTO è definito nel piano di replicazione e corrisponde al tempo necessario per effettuare il failover sul sito DR e riavviare tutte le VM.
- **Gruppo di risorse**: un contenitore logico che consente di gestire più VM come un'unica unità. Una VM può trovarsi in un solo gruppo di risorse alla volta. È possibile creare un gruppo di risorse per ogni applicazione o carico di lavoro che si desidera proteggere.
- **Sito**: un contenitore logico in genere associato a un data center fisico o a una posizione cloud che ospita uno o più cluster vCenter e storage ONTAP .

Prerequisiti NetApp Disaster Recovery

Prima di utilizzare NetApp Disaster Recovery, assicurati che il tuo ambiente soddisfi i requisiti di storage ONTAP , cluster VMware vCenter e NetApp Console .

Versioni del software

Componente	Versione minima
Amazon FSx for NetApp ONTAP	Ultima versione disponibile
Google Cloud VMware Engine che utilizza Google Cloud NetApp Volumes	Ultima versione disponibile
Software ONTAP	ONTAP 9.10.0 o successivo
VMware Cloud per AWS	Ultima versione disponibile
VMware vCenter on-premise	7.0u3 o successivo

Prerequisiti e considerazioni di Google Cloud

Con Disaster Recovery su Google Cloud VMware Engine tramite Google Cloud NetApp Volumes, assicurati di configurare le autorizzazioni corrette e di rispettare le considerazioni indicate.

- Contatta il team Google SRE per consentire l'inserimento nell'elenco di:
  - API di sincronizzazione per trasferire snapshot dall'archiviazione locale a Google Cloud NetApp Volumes.
  - il progetto Google con il motore VMware per la creazione, il montaggio e lo smontaggio di datastore.
- Devi"Invia una richiesta per consentire la replica ibrida dei tuoi volumi" .
- Siate consapevoli del"Quote e limiti Google Cloud NetApp Volumes" .
- È possibile aggiungere un solo volume o datastore a un piano di replica.
- Rivedere il"limitazioni" .

Considerazioni sul failover

- Il failover è supportato solo utilizzando lo snapshot più recente. Se necessario, puoi creare un nuovo snapshot durante il failover (ovvero, l'opzione di snapshot selettivo deve essere disabilitata).
- Non è possibile creare un nuovo snapshot dopo il failover.
- Non è possibile conservare e riconciliare gli snapshot dopo il failover.

Considerazioni sul failback

- Il failback è possibile solo con l'opzione snapshot selettiva. Non è possibile eseguire un failback eseguendo un nuovo snapshot.
- Se si rimuove il peering dei cluster tra l'archiviazione locale e i cluster di archiviazione Google Cloud NetApp Volumes , è necessario cancellare manualmente la voce relativa al peering delle VM di archiviazione e del cluster dal cluster locale. Per maggiori informazioni, vedere "Elimina una relazione peer vserver".

Autorizzazioni di Google Cloud

Al servizio principale in Google Cloud devono essere assegnati i seguenti ruoli o autorizzazioni equivalenti:

- "Ruolo di amministratore di calcolo"
- "Autorizzazioni di Google Cloud per NetApp Console"
- "Amministrazione di Google Cloud NetApp Volumes"
- "Amministratore del servizio VMware Engine"

Autorizzazioni NetApp Console

L'utente NetApp Console deve avere i seguenti ruoli:

- "Amministratore di Google Cloud NetApp Volumes"
- "Amministratore SnapCenter"
- "Amministratore del failover del ripristino di emergenza"

Prerequisiti di archiviazione ONTAP

Questi prerequisiti si applicano sia a ONTAP che ad Amazon FSX per le istanze NetApp ONTAP .

- I cluster di origine e di destinazione devono avere una relazione peer.
- L'SVM che ospita i volumi di disaster recovery deve essere presente nel cluster di destinazione.
- L'SVM di origine e l'SVM di destinazione devono avere una relazione peer.
- Se si esegue la distribuzione con Amazon FSx for NetApp ONTAP, si applica il seguente prerequisito:
  - Nella tua VPC deve essere presente un'istanza Amazon FSx for NetApp ONTAP per ospitare i datastore VMware DR. Per iniziare, vedere"la documentazione Amazon FSx per ONTAP" .

Prerequisiti dei cluster VMware vCenter

Questi prerequisiti si applicano sia ai cluster vCenter on-premise sia al data center software-defined (SDDC) VMware Cloud for AWS.

- Revisione"privilegi vCenter" necessario per NetApp Disaster Recovery.
- Tutti i cluster VMware che si desidera vengano gestiti NetApp Disaster Recovery utilizzano volumi ONTAP per ospitare tutte le VM che si desidera proteggere.
- Tutti i datastore VMware da gestire tramite NetApp Disaster Recovery devono utilizzare uno dei seguenti protocolli:
  - NFS
  - VMFS che utilizza il protocollo iSCSI o FC
- VMware vSphere versione 7.0 Update 3 (7.0v3) o successiva
- Se si utilizza VMware Cloud SDDC, si applicano i seguenti prerequisiti.
  - Nella VMware Cloud Console, utilizzare i ruoli di servizio Amministratore e Amministratore NSX Cloud. Utilizzare anche il proprietario dell'organizzazione per il ruolo Organizzazione. Fare riferimento a "Utilizzo di VMware Cloud Foundations con AWS FSx per la documentazione NetApp ONTAP" .
  - Collegare VMware Cloud SDDC all'istanza Amazon FSx for NetApp ONTAP . Fare riferimento a "Informazioni sull'integrazione di VMware Cloud su AWS con Amazon FSx for NetApp ONTAP" .

Prerequisiti NetApp Console

Inizia con la NetApp Console

Se non l'hai ancora fatto, "iscriviti alla NetApp Console e crea un'organizzazione" .

Raccogli le credenziali per ONTAP e VMware

- Le credenziali Amazon FSx for ONTAP e AWS devono essere aggiunte al sistema all'interno del progetto NetApp Console che gestisce NetApp Disaster Recovery.
- NetApp Disaster Recovery richiede le credenziali vCenter. Quando si aggiunge un sito in NetApp Disaster Recovery, è necessario immettere le credenziali vCenter.

  Per un elenco dei privilegi vCenter necessari, fare riferimento a"Privilegi vCenter necessari per NetApp Disaster Recovery" . Per istruzioni su come aggiungere un sito, fare riferimento a"Aggiungi un sito" .

Creare l'agente NetApp Console

L'agente Console è un componente software che consente alla Console di comunicare con lo storage ONTAP e i cluster VMware vCenter. È necessario affinché Disaster Recovery funzioni correttamente. L'agente risiede nella tua rete privata (un data center locale o un VPC cloud) e comunica con le tue istanze di archiviazione ONTAP e con qualsiasi componente aggiuntivo di server e applicazioni. Per il Disaster Recovery, si tratta dell'accesso ai cluster vCenter gestiti.

È necessario configurare un agente Console nella NetApp Console. Quando si utilizza l'agente, questo includerà le funzionalità appropriate per il servizio Disaster Recovery.

- NetApp Disaster Recovery funziona solo con la distribuzione dell'agente in modalità standard. Vedere "Introduzione alla NetApp Console in modalità standard" .
- Assicurarsi che sia il cluster di origine che quello di destinazione vCenter utilizzino lo stesso agente Console.
- Tipo di agente console necessario:
  - **Disaster recovery da on-premises a on-premises**: installa l'agente Console on-premises nel sito di disaster recovery. Utilizzando questo metodo, un guasto del sito primario non impedisce al servizio di riavviare le risorse virtuali nel sito DR. Fare riferimento a "Installa e configura l'agente Console in locale".

    Disaster Recovery supporta anche l'utilizzo di più agenti Console con configurazioni on-premise. In questo scenario, gli agenti della console indirizzano le azioni ai cluster di array vCenter e ONTAP , mentre l'origine e la destinazione avrebbero ciascuna il proprio agente della console. Si consiglia di utilizzare più agenti della console per ridurre la latenza e migliorare i tempi di ripristino in caso di errore di un agente o di un sito della console.

  - **Da locale ad AWS**: installa l'agente della console per AWS nella tua VPC AWS. Fare riferimento a "Opzioni di installazione dell'agente console in AWS" .

    Per le connessioni da locale a locale, utilizzare l'agente Console locale. Per gli ambienti on-premise su AWS, utilizzare l'agente AWS Console, che ha accesso al vCenter on-premise di origine e al vCenter on-premise di destinazione.

  - L'agente Console installato deve essere in grado di accedere a tutte le istanze del cluster VMware vCenter e agli host ESXi gestiti dai cluster vCenter che Disaster Recovery gestirà.
- Tutti gli array ONTAP da gestire tramite NetApp Disaster Recovery devono essere aggiunti a qualsiasi sistema all'interno del progetto NetApp Console che verrà utilizzato per gestire NetApp Disaster Recovery.

  Vedere "Scopri i cluster ONTAP on-premise" .
- Per informazioni sulla configurazione di un proxy intelligente per NetApp Disaster Recovery, vedere"Configura la tua infrastruttura per NetApp Disaster Recovery" .

Prerequisiti del carico di lavoro

Per garantire il successo dei processi di coerenza delle applicazioni, applicare i seguenti prerequisiti:

- Assicurarsi che gli strumenti VMware (o gli strumenti Open VM) siano in esecuzione sulle VM che verranno protette.
- Per le VM Windows che eseguono Microsoft SQL Server, Oracle Database o entrambi, i database devono avere i relativi VSS Writer abilitati.

- I database Oracle in esecuzione su un sistema operativo Linux devono avere l'autenticazione utente del sistema operativo abilitata per il ruolo SYSDBA del database Oracle.

Ulteriori informazioni

- Privilegi richiesti vCenter
- Prerequisiti per Amazon EVS con NetApp Disaster Recovery

Avvio rapido per NetApp Disaster Recovery

Ecco una panoramica dei passaggi necessari per iniziare a utilizzare NetApp Disaster Recovery. I link presenti in ogni passaggio ti conducono a una pagina che fornisce maggiori dettagli.

Rivedere i prerequisiti

"Assicurati che il tuo sistema soddisfi questi requisiti" .

Configura NetApp Disaster Recovery

- "Impostare l'infrastruttura per il servizio" .
- "Impostare la licenza" .

Cosa succederà adesso?

Dopo aver configurato il servizio, ecco cosa potresti fare.

- "Aggiungi i tuoi siti vCenter a NetApp Disaster Recovery" .
- "Crea il tuo primo gruppo di risorse" .
- "Crea il tuo primo piano di replicazione" .
- "Replicare le applicazioni su un altro sito" .
- "Eseguire il failover delle applicazioni su un sito remoto" .
- "Eseguire il failback delle applicazioni sul sito di origine originale" .
- "Gestisci siti, gruppi di risorse e piani di replicazione" .
- "Monitorare le operazioni di ripristino in caso di disastro" .

Configura la tua infrastruttura per NetApp Disaster Recovery

Per utilizzare NetApp Disaster Recovery, è necessario eseguire alcuni passaggi per configurarlo sia in Amazon Web Services (AWS) sia nella NetApp Console.

Revisione"prerequisiti" per garantire che il tuo sistema sia pronto.

È possibile utilizzare NetApp Disaster Recovery nelle seguenti infrastrutture:

- DR cloud ibrido che replica un data center VMware più ONTAP locale in un'infrastruttura DR AWS basata su VMware Cloud on AWS e Amazon FSx for NetApp ONTAP.
- DR cloud privato che replica un VMware più ONTAP vCenter locale su un altro VMware più ONTAP vCenter locale.

Cloud ibrido con VMware Cloud e Amazon FSx for NetApp ONTAP

Questo metodo consiste in un'infrastruttura vCenter di produzione locale che utilizza datastore ospitati su volumi ONTAP FlexVol mediante un protocollo NFS. Il sito DR è costituito da una o più istanze VMware Cloud SDDC che utilizzano datastore ospitati su volumi FlexVol forniti da una o più istanze FSx for ONTAP mediante un protocollo NFS.

I siti di produzione e DR sono collegati tramite una connessione sicura compatibile con AWS. I tipi di connessione più comuni sono una VPN sicura (privata o fornita da AWS), AWS Direct Connect o altri metodi di interconnessione approvati.

Per il Disaster Recovery che coinvolge l'infrastruttura cloud AWS, è necessario utilizzare l'agente Console per AWS. L'agente deve essere installato nella stessa VPC dell'istanza FSx for ONTAP . Se sono state distribuite istanze FSx for ONTAP aggiuntive in altre VPC, la VPC che ospita l'agente deve avere accesso alle altre VPC.

Zone di disponibilità AWS

AWS supporta la distribuzione di soluzioni in una o più zone di disponibilità (AZ) all'interno di una determinata regione. Disaster Recovery utilizza due servizi ospitati su AWS: VMware Cloud per AWS e AWS FSx per NetApp ONTAP.

- **VMware Cloud per AWS**: supporta la distribuzione in un ambiente SDDC con cluster esteso a singola AZ o a doppia AZ. Disaster Recovery supporta una distribuzione SDDC con singola AZ solo per Amazon VMware Cloud per AWS.
- **AWS FSx per NetApp ONTAP**: quando viene distribuito in una configurazione dual-AZ, ogni volume è di proprietà di un singolo sistema FSx. Ogni volume è di proprietà di un singolo sistema FSx. I dati del volume vengono replicati sul secondo sistema FSx. I sistemi FSx per ONTAP possono essere implementati in distribuzioni con una o due zone di disponibilità (AZ). Disaster Recovery supporta FSx sia con AZ singola che multi-AZ per distribuzioni FSx per ONTAP .

BEST PRACTICE: per la configurazione del sito AWS DR, NetApp consiglia di utilizzare distribuzioni single-AZ sia per le istanze VMware Cloud che AWS FSx per ONTAP . Poiché AWS viene utilizzato per il DR, non vi è alcun vantaggio nell'introdurre più AZ. Le zone di disponibilità multiple possono aumentare i costi e la complessità.

Da locale ad AWS

AWS fornisce i seguenti metodi per connettere i data center privati al cloud AWS. Ogni soluzione ha i suoi vantaggi e i suoi costi da considerare.

- **AWS Direct Connect**: si tratta di un'interconnessione cloud AWS situata nella stessa area geografica del tuo data center privato e fornita da un partner AWS. Questa soluzione fornisce una connessione sicura e privata tra il tuo data center locale e il cloud AWS senza la necessità di una connessione Internet pubblica. Questo è il metodo di connessione più diretto ed efficiente offerto da AWS.
- **AWS Internet Gateway**: fornisce connettività pubblica tra le risorse cloud AWS e le risorse di elaborazione esterne. Questo tipo di connessione viene solitamente utilizzato per fornire servizi a clienti esterni, come il

servizio HTTP/HTTPS, in cui la sicurezza non è un requisito. Non esiste alcun controllo sulla qualità del servizio, sulla sicurezza o sulla garanzia di connettività. Per questo motivo, questo metodo di connessione non è consigliato per connettere un data center di produzione al cloud.

- **AWS Site-Site VPN**: questa connessione di rete privata virtuale può essere utilizzata per fornire connessioni di accesso sicure insieme a un provider di servizi Internet pubblico. La VPN crittografa e decrittografa tutti i dati in transito da e verso il cloud AWS. Le VPN possono essere basate su software o hardware. Per le applicazioni aziendali, il fornitore di servizi Internet pubblici (ISP) dovrebbe offrire garanzie di qualità del servizio per assicurare che siano fornite larghezza di banda e latenza adeguate per la replica DR.

MIGLIOR PRASSI: Per la configurazione del sito AWS DR, NetApp consiglia di utilizzare AWS Direct Connect. Questa soluzione garantisce le massime prestazioni e sicurezza per le applicazioni aziendali. Se non è disponibile, è opportuno utilizzare una connessione ISP pubblica ad alte prestazioni insieme a una VPN. Assicurarsi che l'ISP offra livelli di servizio QoS commerciali per garantire prestazioni di rete adeguate.

Interconnessioni VPC-VPC

AWS offre i seguenti tipi di interconnessioni VPC-VPC. Ogni soluzione ha i suoi vantaggi e i suoi costi da considerare.

- **VPC Peering**: si tratta di una connessione privata tra due VPC. È il metodo di connessione più diretto ed efficiente offerto da AWS. Il peering VPC può essere utilizzato per connettere VPC nella stessa regione AWS o in regioni AWS diverse.
- **AWS Internet Gateway**: in genere viene utilizzato per fornire connessioni tra risorse AWS VPC e risorse ed endpoint non AWS. Tutto il traffico segue un percorso "a forcina" in cui il traffico VPC destinato a un'altra VPC esce dall'infrastruttura AWS tramite il gateway Internet e ritorna all'infrastruttura AWS tramite lo stesso gateway o un gateway diverso. Questo non è un tipo di connessione VPC adatto per le soluzioni VMware aziendali.
- **AWS Transit Gateway**: si tratta di un tipo di connessione centralizzata basata su router che consente a ogni VPC di connettersi a un singolo gateway centrale, che funge da hub centrale per tutto il traffico da VPC a VPC. Può anche essere collegato alla tua soluzione VPN per consentire alle risorse del data center locale di accedere alle risorse ospitate su AWS VPC. Questo tipo di connessione richiede in genere un costo aggiuntivo per essere implementata.

BEST PRACTICE: per le soluzioni DR che coinvolgono VMware Cloud e un singolo FSx per ONTAP VPC, NetApp consiglia di utilizzare la connessione peer VPC. Se vengono distribuite più VPC FSx for ONTAP , consigliamo di utilizzare un AWS Transit Gateway per ridurre il sovraccarico di gestione di più connessioni peer VPC.

Preparati alla protezione on-premise-to-cloud con AWS

Per configurare NetApp Disaster Recovery per la protezione on-premise-to-cloud tramite AWS, è necessario configurare quanto segue:

- Configurare AWS FSx per NetApp ONTAP
- Configura VMware Cloud su AWS SDDC

Configurare AWS FSx per NetApp ONTAP

- Creare un file system Amazon FSx for NetApp ONTAP .
  - Fornire e configurare FSx per ONTAP. Amazon FSx for NetApp ONTAP è un servizio completamente gestito che fornisce un archivio file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità, basato sul file system NetApp ONTAP .

    - Segui i passaggi in "Rapporto tecnico 4938: Montare Amazon FSx ONTAP come datastore NFS con VMware Cloud su AWS" E "Avvio rapido per Amazon FSx for NetApp ONTAP" per predisporre e configurare FSx per ONTAP.
- Aggiungere Amazon FSx per ONTAP al sistema e aggiungere le credenziali AWS per FSx per ONTAP.
- Crea o verifica la tua SVM ONTAP di destinazione in AWS FSx per l'istanza ONTAP .
- Configurare la replica tra il cluster ONTAP locale di origine e l'istanza FSx for ONTAP nella NetApp Console.

Fare riferimento a "come configurare un sistema FSx per ONTAP" per i passaggi dettagliati.

Configura VMware Cloud su AWS SDDC

"VMware Cloud su AWS"fornisce un'esperienza cloud-native per carichi di lavoro basati su VMware nell'ecosistema AWS. Ogni data center software-defined VMware (SDDC) viene eseguito in un Amazon Virtual Private Cloud (VPC) e fornisce uno stack VMware completo (incluso vCenter Server), networking software-defined NSX-T, storage software-defined vSAN e uno o più host ESXi che forniscono risorse di elaborazione e storage ai carichi di lavoro.

Per configurare un ambiente VMware Cloud su AWS, seguire i passaggi in "Distribuisci e configura l'ambiente di virtualizzazione su AWS" Un gruppo di spie luminose può essere utilizzato anche per scopi di ripristino in caso di disastro.

Cloud privato

È possibile utilizzare NetApp Disaster Recovery per proteggere le VM VMware ospitate su uno o più cluster vCenter replicando i datastore delle VM su un altro cluster vCenter nello stesso data center privato oppure in un data center remoto privato o collocato.

Per le situazioni da locale a locale, installare l'agente Console in una delle sedi fisiche.

Disaster Recovery supporta la replica da sito a sito tramite Ethernet e TCP/IP. Assicurarsi che sia disponibile una larghezza di banda adeguata per supportare le velocità di modifica dei dati sulle VM del sito di produzione, in modo che tutte le modifiche possano essere replicate sul sito DR entro l'intervallo di tempo previsto dal Recovery Point Objective (RPO).

Preparati per la protezione on-premises-to-on-premises

Prima di configurare NetApp Disaster Recovery per la protezione on-premise-to-on-premise, assicurarsi che siano soddisfatti i seguenti requisiti:

- Deposito ONTAP
    - Assicurati di avere le credenziali ONTAP .
    - Crea o verifica il tuo sito di disaster recovery.
    - Crea o verifica la tua destinazione ONTAP SVM.
    - Assicurarsi che le SVM ONTAP di origine e di destinazione siano in peering.
- Cluster vCenter
    - Assicurarsi che le VM che si desidera proteggere siano ospitate su datastore NFS (utilizzando volumi ONTAP NFS) o datastore VMFS (utilizzando LUN iSCSI NetApp).
    - Revisione"privilegi vCenter" necessario per NetApp Disaster Recovery.

- Creare un account utente per il ripristino di emergenza (non l'account amministratore vCenter predefinito) e assegnare i privilegi vCenter all'account.

Supporto proxy intelligente

L'agente NetApp Console supporta il proxy intelligente. Il proxy intelligente è un modo leggero, sicuro ed efficiente per connettere il tuo ambiente locale alla NetApp Console. Fornisce una connessione sicura tra il tuo sistema e il servizio Console senza richiedere una VPN o un accesso diretto a Internet. Questa implementazione proxy ottimizzata scarica il traffico API all'interno della rete locale.

Quando viene configurato un proxy, NetApp Disaster Recovery tenta di comunicare direttamente con VMware o ONTAP e utilizza il proxy configurato se la comunicazione diretta fallisce.

L'implementazione del proxy NetApp Disaster Recovery richiede la comunicazione sulla porta 443 tra l'agente della console e tutti i server vCenter e gli array ONTAP che utilizzano un protocollo HTTPS. L'agente NetApp Disaster Recovery all'interno dell'agente Console comunica direttamente con VMware vSphere, VC o ONTAP quando esegue qualsiasi azione.

Per ulteriori informazioni sulla configurazione generale del proxy nella NetApp Console, vedere "Configurare l'agente della console per utilizzare un server proxy" .

Accedi a NetApp Disaster Recovery

Per accedere al servizio NetApp Disaster Recovery è possibile utilizzare la NetApp Console .

Per effettuare l'accesso, puoi utilizzare le credenziali del sito di supporto NetApp oppure puoi registrarti per un accesso cloud NetApp utilizzando il tuo indirizzo email e una password. "Scopri di più sull'accesso" .

Attività specifiche richiedono ruoli utente specifici. "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".

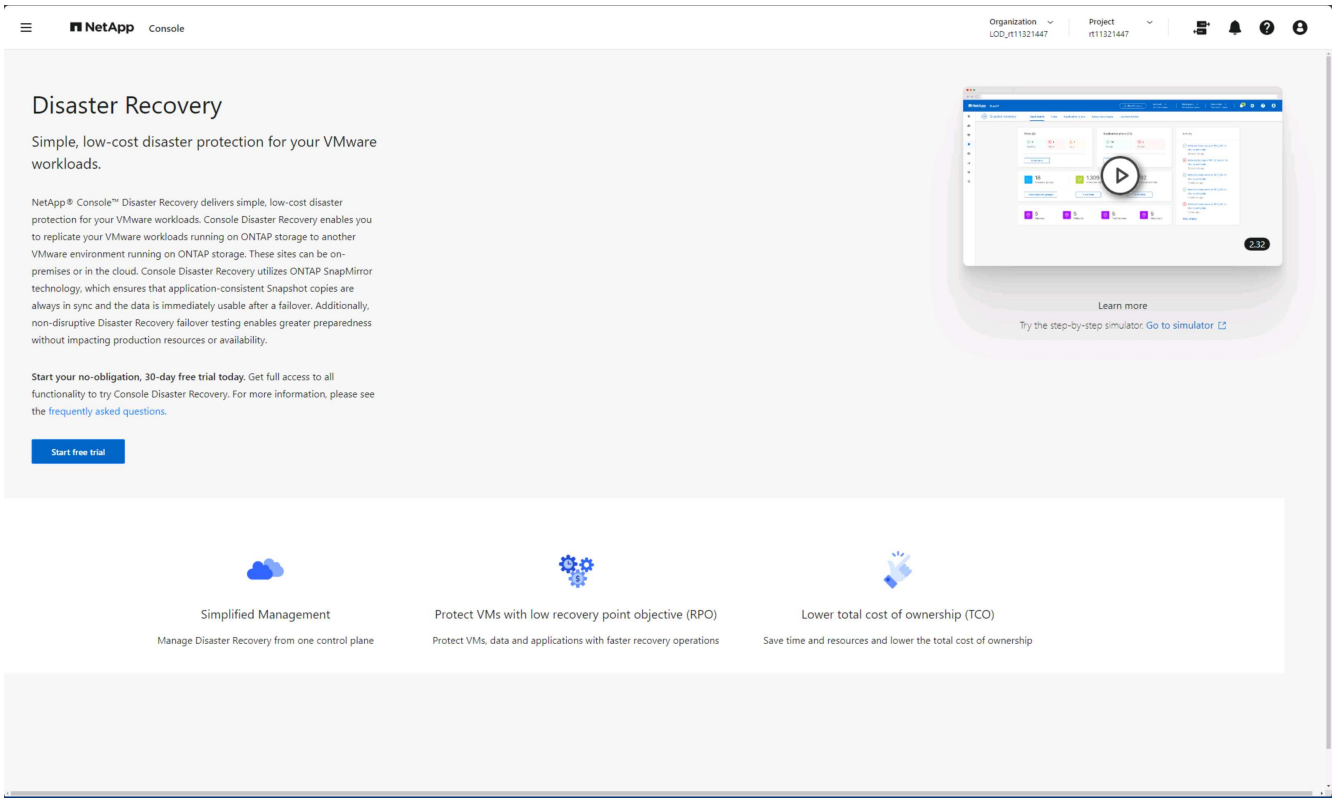
Passi

1. Apri un browser web e vai su "NetApp Console" .

   Viene visualizzata la pagina di accesso NetApp Console .

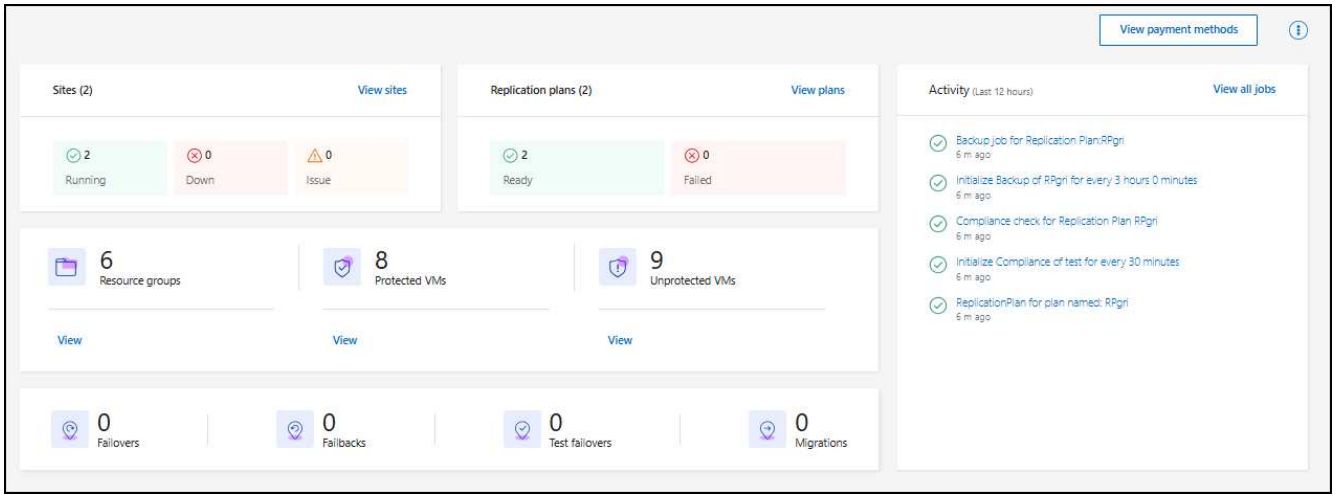
2. Accedi alla NetApp Console.
3. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.

   Se è la prima volta che accedi a questo servizio, verrà visualizzata la landing page e potrai registrarti per una prova gratuita.



In caso contrario, viene visualizzata la Dashboard NetApp Disaster Recovery .

- Se non hai ancora aggiunto un agente NetApp Console , dovrai aggiungerne uno. Per aggiungere l'agente, fare riferimento a "Scopri di più sugli agenti della console" .
- Se sei un utente NetApp Console con un agente esistente, quando selezioni "Disaster recovery" viene visualizzato un messaggio relativo alla registrazione.
- Se stai già utilizzando il servizio, quando selezioni "Disaster recovery" viene visualizzata la Dashboard.



Impostare la licenza per NetApp Disaster Recovery

Con NetApp Disaster Recovery puoi utilizzare diversi piani di licenza, tra cui una prova gratuita, un abbonamento a consumo o la possibilità di utilizzare la tua licenza.

*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 i ruoli di accesso per tutti i servizi".

Opzioni di licenza È possibile utilizzare le seguenti opzioni di licenza:

- Registrati per una prova gratuita di 30 giorni.
- Acquista un abbonamento pay-as-you-go (PAYGO) ad Amazon Web Services (AWS) Marketplace o a Microsoft Azure Marketplace.
- Bring your own license (BYOL), ovvero un file di licenza NetApp (NLF) che puoi ottenere dal tuo rappresentante commerciale NetApp . È possibile utilizzare il numero di serie della licenza per attivare BYOL nella NetApp Console.

> I costi NetApp Disaster Recovery si basano sulla capacità utilizzata dei datastore sul sito di origine quando è presente almeno una VM dotata di un piano di replica. La capacità per un datastore sottoposto a failover non è inclusa nella capacità consentita. Per un BYOL, se i dati superano la capacità consentita, le operazioni nel servizio sono limitate finché non si ottiene una licenza di capacità aggiuntiva o non si aggiorna la licenza nella NetApp Console.

"Scopri di più sugli abbonamenti".

Una volta terminato il periodo di prova gratuito o scaduta la licenza, potrai comunque effettuare le seguenti operazioni nel servizio:

- Visualizza qualsiasi risorsa, ad esempio un carico di lavoro o un piano di replicazione.
- Eliminare qualsiasi risorsa, ad esempio un carico di lavoro o un piano di replica.
- Esegui tutte le operazioni pianificate create durante il periodo di prova o in base alla licenza.

Provalo utilizzando una prova gratuita di 30 giorni

Puoi provare NetApp Disaster Recovery utilizzando la versione di prova gratuita di 30 giorni.

> Durante la sperimentazione non sono previsti limiti di capienza.

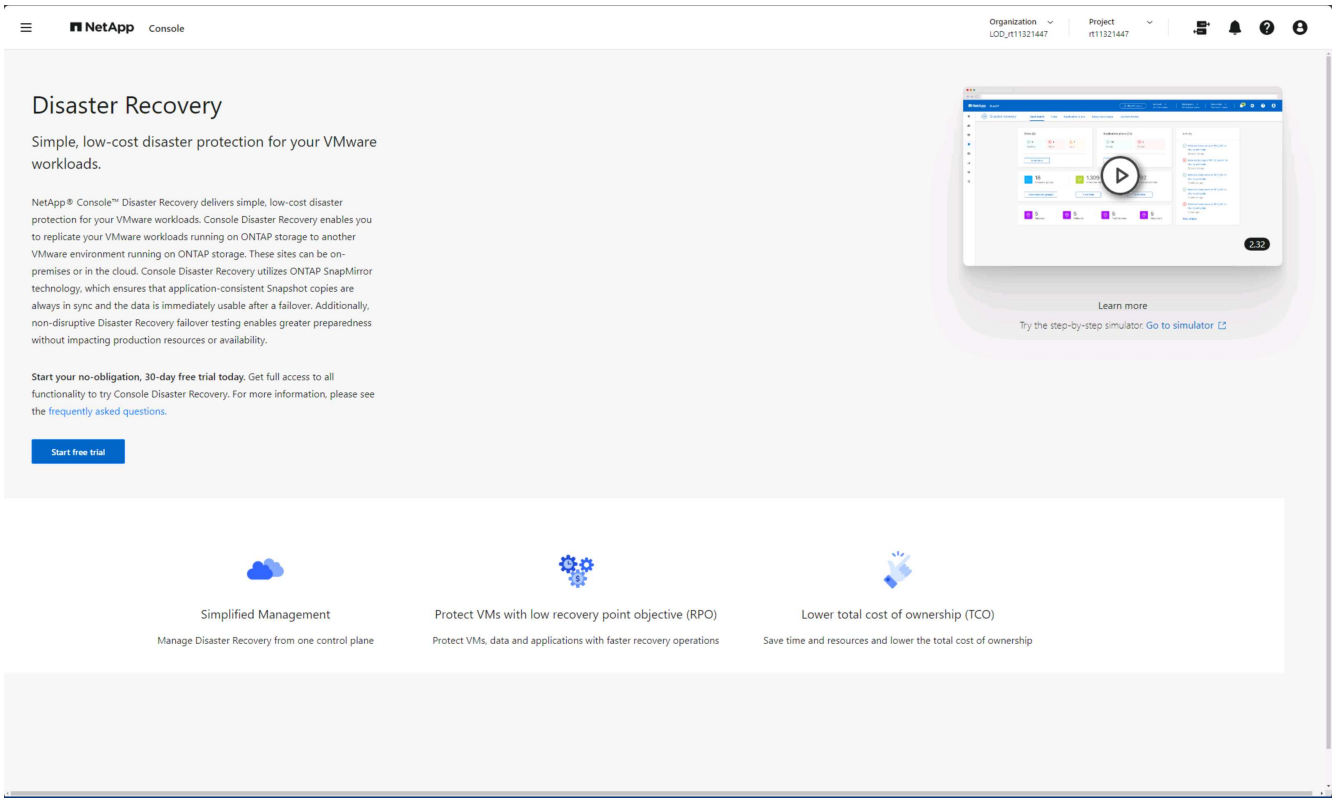
Per continuare dopo il periodo di prova, dovrai acquistare una licenza BYOL o un abbonamento AWS PAYGO. Puoi ottenere una licenza in qualsiasi momento e non ti verrà addebitato alcun costo fino al termine del periodo di prova.

Durante la prova avrai piena funzionalità.

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 accedi a questo servizio, verrà visualizzata la pagina di destinazione.



3. Se non hai ancora aggiunto un agente Console per altri servizi, aggiungine uno.

   Per aggiungere un agente Console, fare riferimento a "Scopri di più sugli agenti della console" .

4. Dopo aver configurato l'agente, nella landing page NetApp Disaster Recovery , il pulsante per aggiungere l'agente si trasforma in un pulsante per avviare una prova gratuita. Seleziona **Inizia la prova gratuita**.
5. Iniziamo aggiungendo vCenter.

   Per maggiori dettagli, vedere "Aggiungi siti vCenter" .

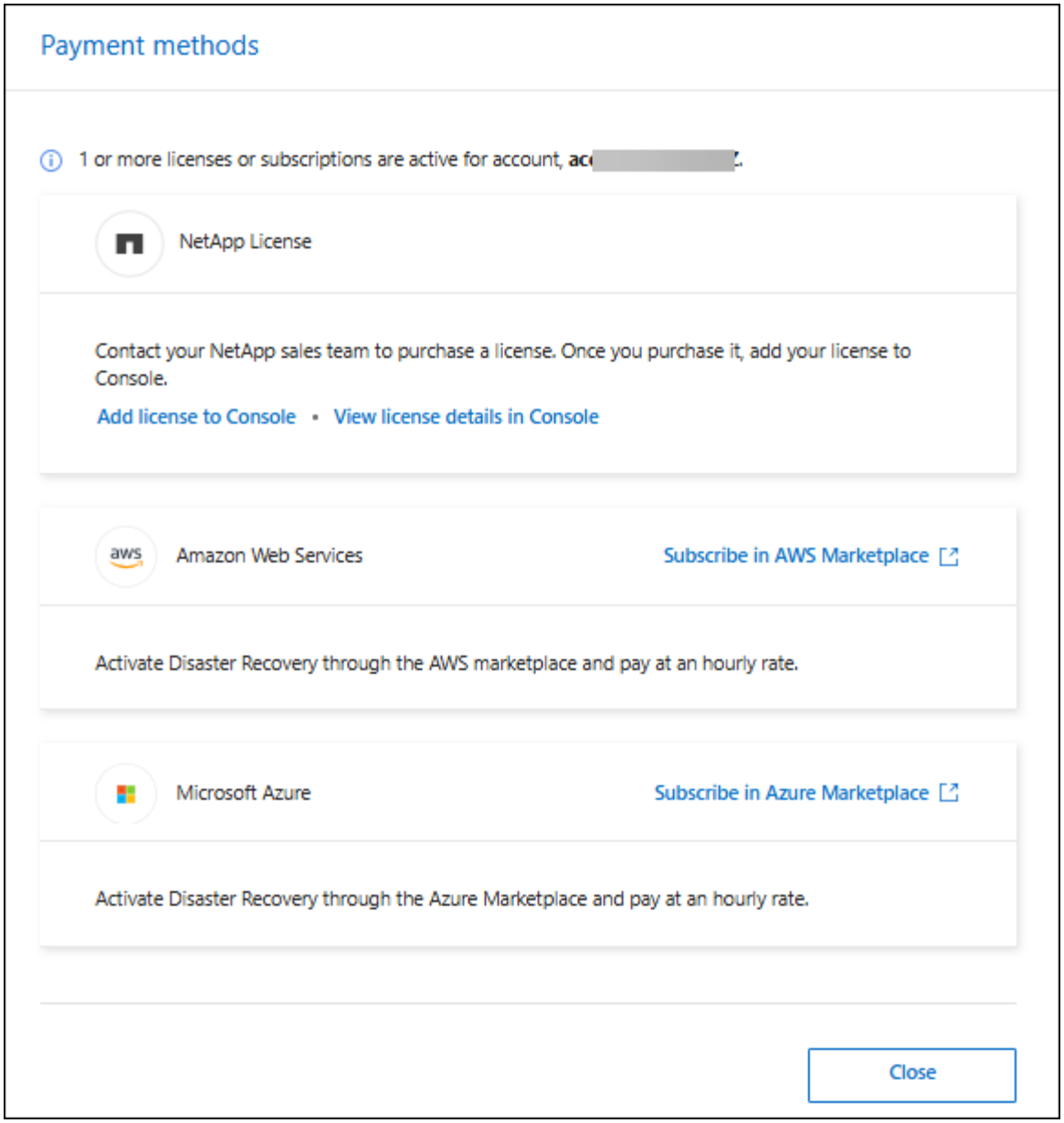
Dopo la fine della prova, abbonati tramite uno dei Marketplace

Al termine del periodo di prova gratuito, potrai acquistare una licenza da NetApp o abbonarti tramite AWS Marketplace o Microsoft Azure Marketplace. Questa procedura fornisce una panoramica di alto livello su come abbonarsi direttamente in uno dei Marketplace.

Passi

1. In NetApp Disaster Recovery viene visualizzato un messaggio che indica che la prova gratuita sta per scadere. Nel messaggio, seleziona **Abbonati o acquista una licenza**.

   Oppure, da , seleziona **Visualizza metodi di pagamento**.



2. Seleziona **Iscriviti in AWS Marketplace** o **Iscriviti in Azure Marketplace**.
3. Utilizza AWS Marketplace o Microsoft Azure Marketplace per abbonarti a * NetApp Disaster Recovery*.
4. Quando si torna a NetApp Disaster Recovery, un messaggio informa che l'abbonamento è stato effettuato.

   È possibile visualizzare i dettagli dell'abbonamento nella pagina di abbonamento NetApp Console . "Scopri di più sulla gestione degli abbonamenti con la NetApp Console".

Al termine del periodo di prova, acquista una licenza BYOL tramite NetApp

Al termine del periodo di prova, potrai acquistare una licenza tramite il tuo rappresentante commerciale NetApp .

Se si utilizza la propria licenza (BYOL), la configurazione include l'acquisto della licenza, l'ottenimento del file di licenza NetApp (NLF) e l'aggiunta della licenza alla NetApp Console.

Aggiungi la licenza alla NetApp Console* Dopo aver acquistato la licenza NetApp Disaster Recovery da un

rappresentante commerciale NetApp , puoi gestirla nella console.

"Scopri come aggiungere licenze con la NetApp Console".

Aggiorna la tua licenza quando scade

Se il termine della licenza si avvicina alla data di scadenza o se la capacità della licenza sta raggiungendo il limite, verrai avvisato nell'interfaccia utente NetApp Disaster Recovery . È possibile aggiornare la licenza NetApp Disaster Recovery prima della scadenza, in modo da non interrompere l'accesso ai dati scansionati.

Questo messaggio appare anche nella NetApp Console e in "Notifiche" .

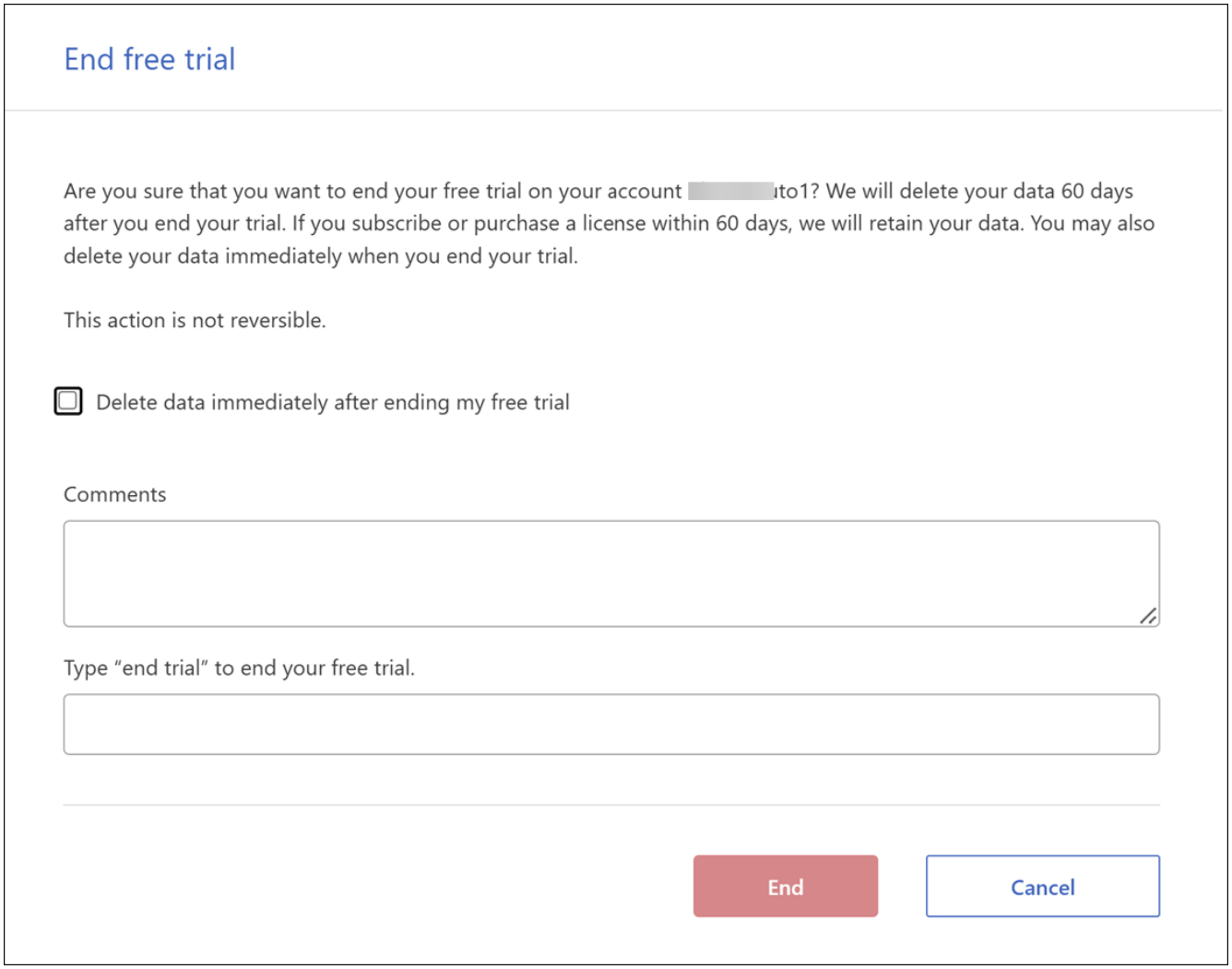
"Scopri come aggiornare le licenze con la NetApp Console".

Termina la prova gratuita

Puoi interrompere la prova gratuita in qualsiasi momento oppure attendere la sua scadenza.

Passi

1. In NetApp Disaster Recovery, seleziona **Prova gratuita - Visualizza dettagli**.
2. Nei dettagli a discesa, seleziona **Termina prova gratuita**.



3. Se desideri eliminare tutti i dati, seleziona **Elimina i dati subito dopo aver terminato la prova gratuita**.

   In questo modo vengono eliminate tutte le pianificazioni, i piani di replica, i gruppi di risorse, i vCenter e i siti. I dati di audit, i registri delle operazioni e la cronologia dei lavori vengono conservati fino alla fine del ciclo di vita del prodotto.

   > Se termini il periodo di prova gratuito, non richiedi l'eliminazione dei dati e non acquisti una licenza o un abbonamento, NetApp Disaster Recovery eliminerà tutti i tuoi dati 60 giorni dopo la fine del periodo di prova gratuito.

4. Digitare "fine prova" nella casella di testo.
5. Selezionare **Fine**.

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

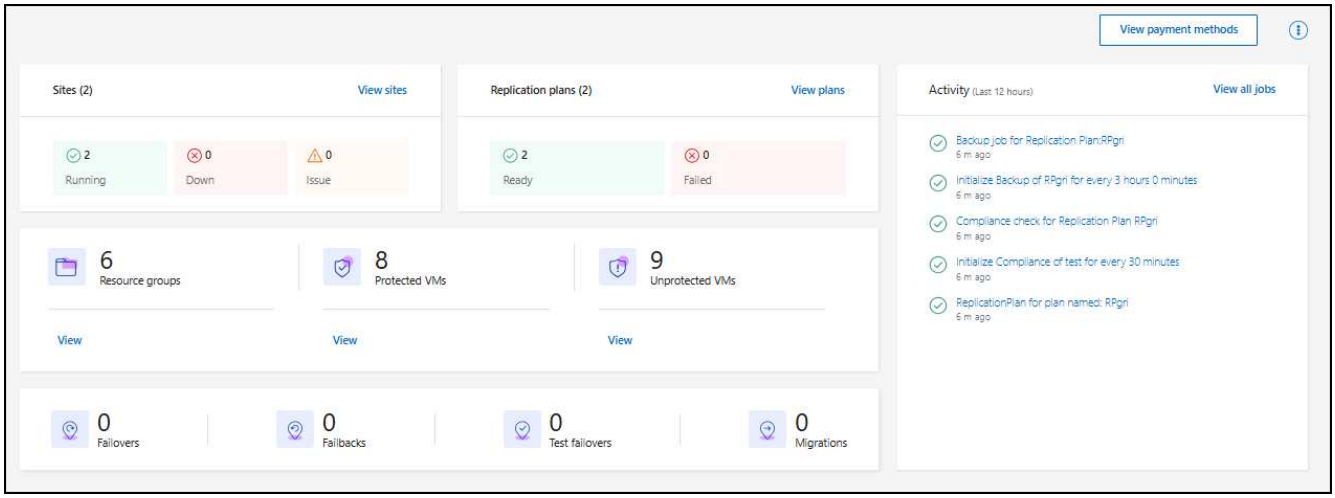
Utilizzando la dashboard di NetApp Disaster Recovery , puoi determinare lo stato di salute dei tuoi siti di disaster recovery e dei piani di replica. È possibile verificare rapidamente quali siti e piani sono integri, disconnessi o degradati.

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

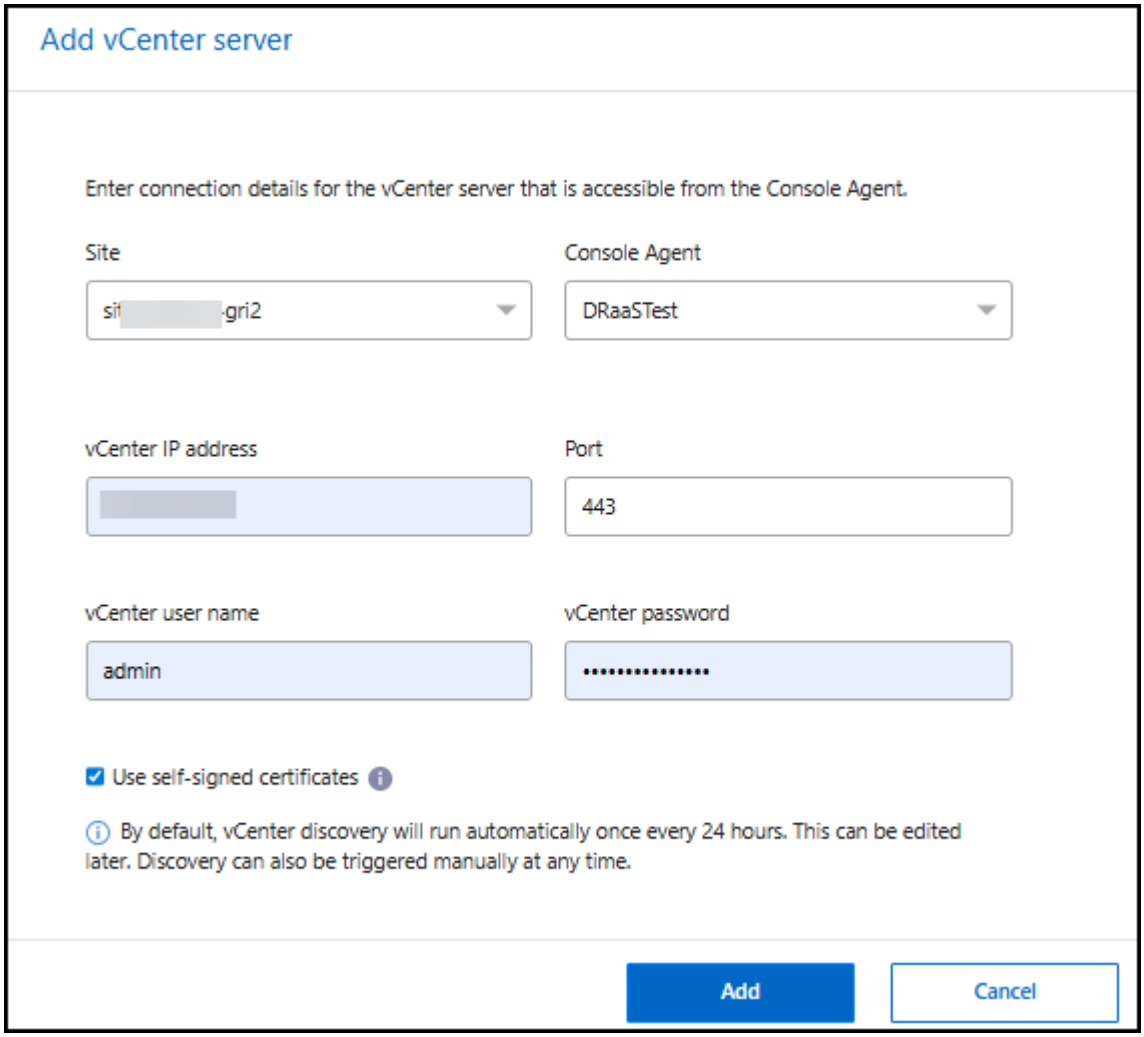
1. Accedi al "NetApp Console" .
2. Dal menu di navigazione a sinistra NetApp Console , selezionare **Protezione** > **Disaster recovery**.

   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**.

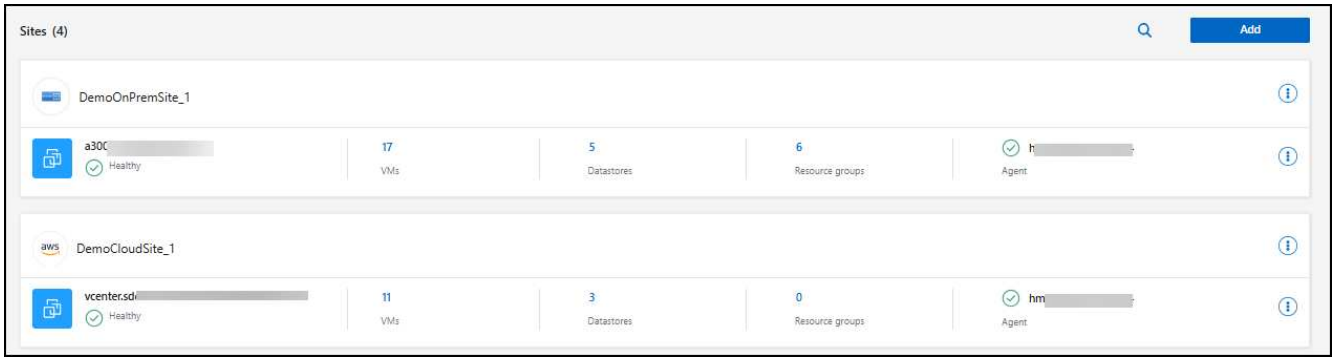
   Quindi aggiungere un vCenter di destinazione.

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.

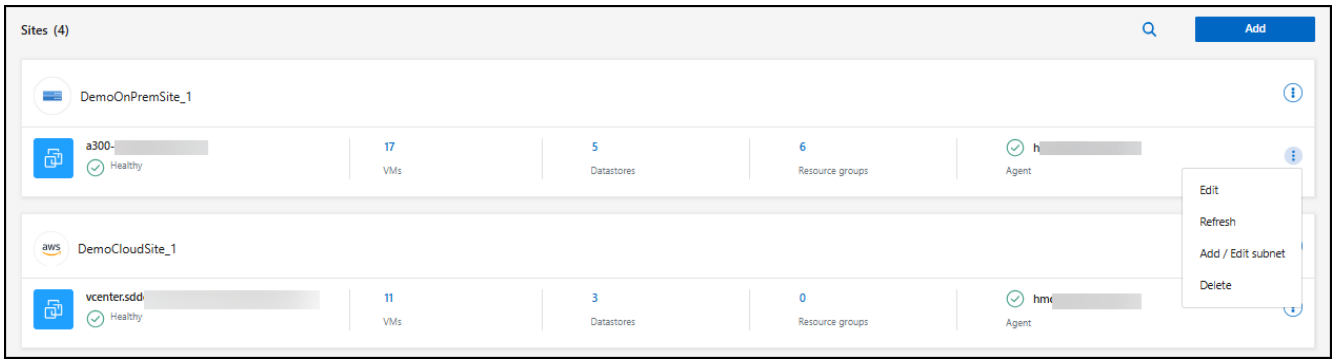
In sintesi, l'indirizzo host rimane lo stesso, mentre l'indirizzo di rete viene sostituito con quello configurato nella mappatura della subnet del sito. Ciò consente di gestire più facilmente la riassegnazione degli indirizzi IP in caso di failover, soprattutto se si hanno centinaia di reti e migliaia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

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

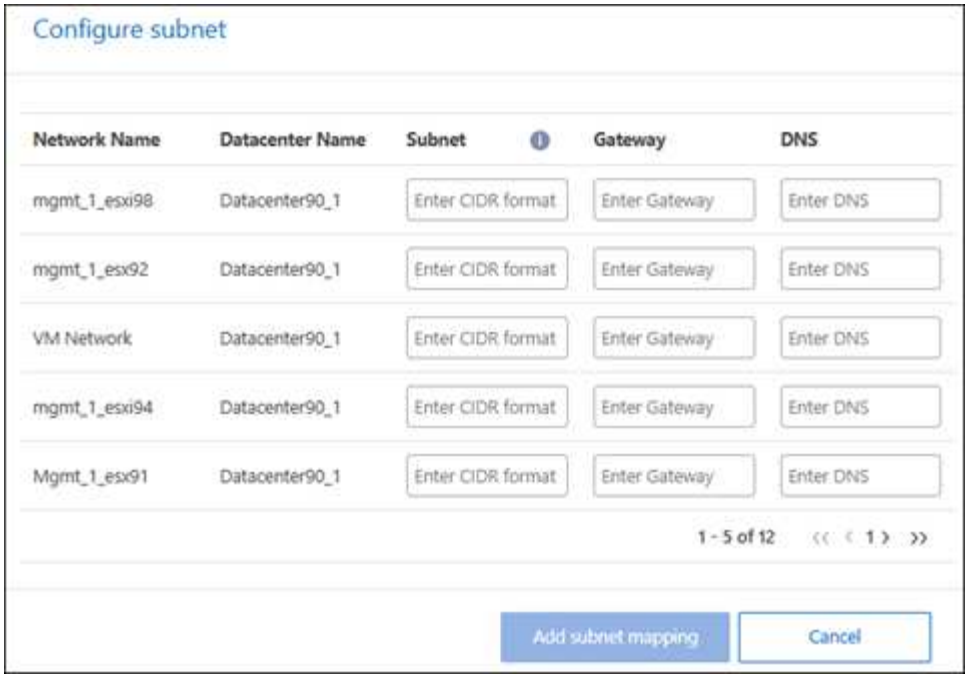
- Per prima cosa, aggiungi la mappatura della subnet per ogni sito vCenter.
- In secondo luogo, nel piano di replicazione, indicare che si desidera utilizzare il mapping delle subnet nella scheda Macchine virtuali e nel campo IP di destinazione.

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

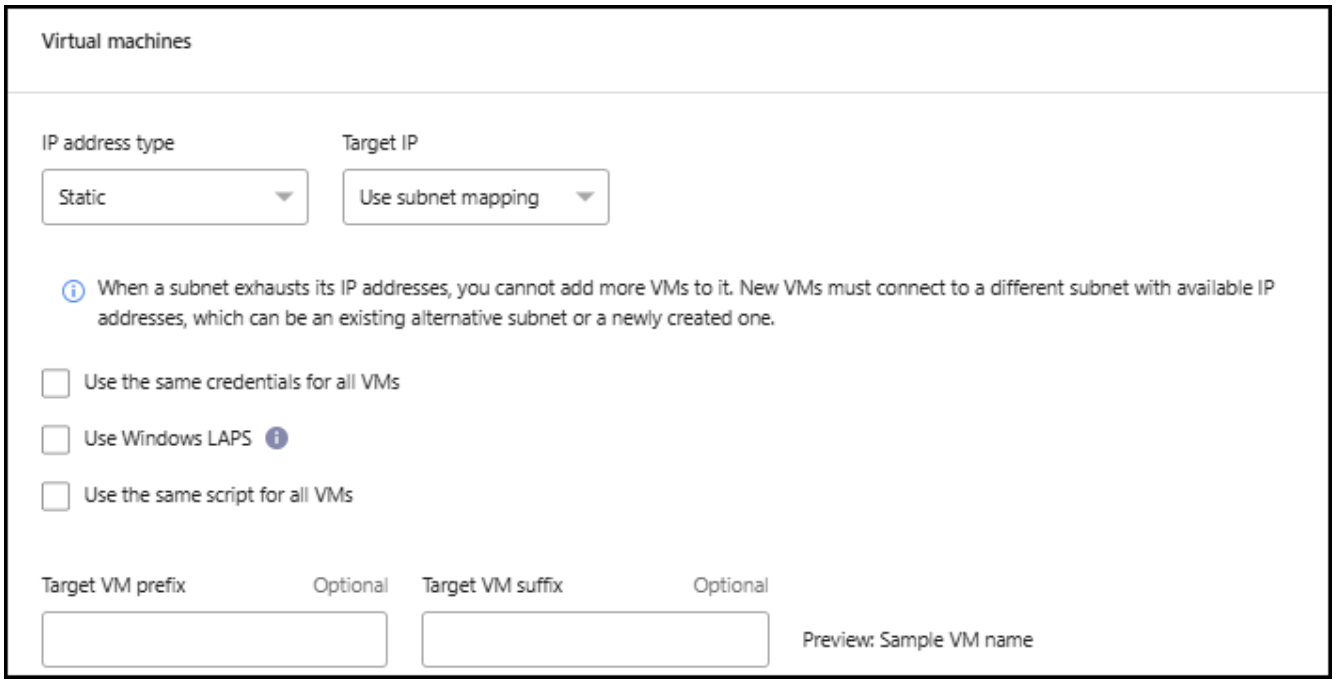
Quando si crea un piano di replicazione, è possibile selezionare il mapping della subnet per il piano di replicazione.

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

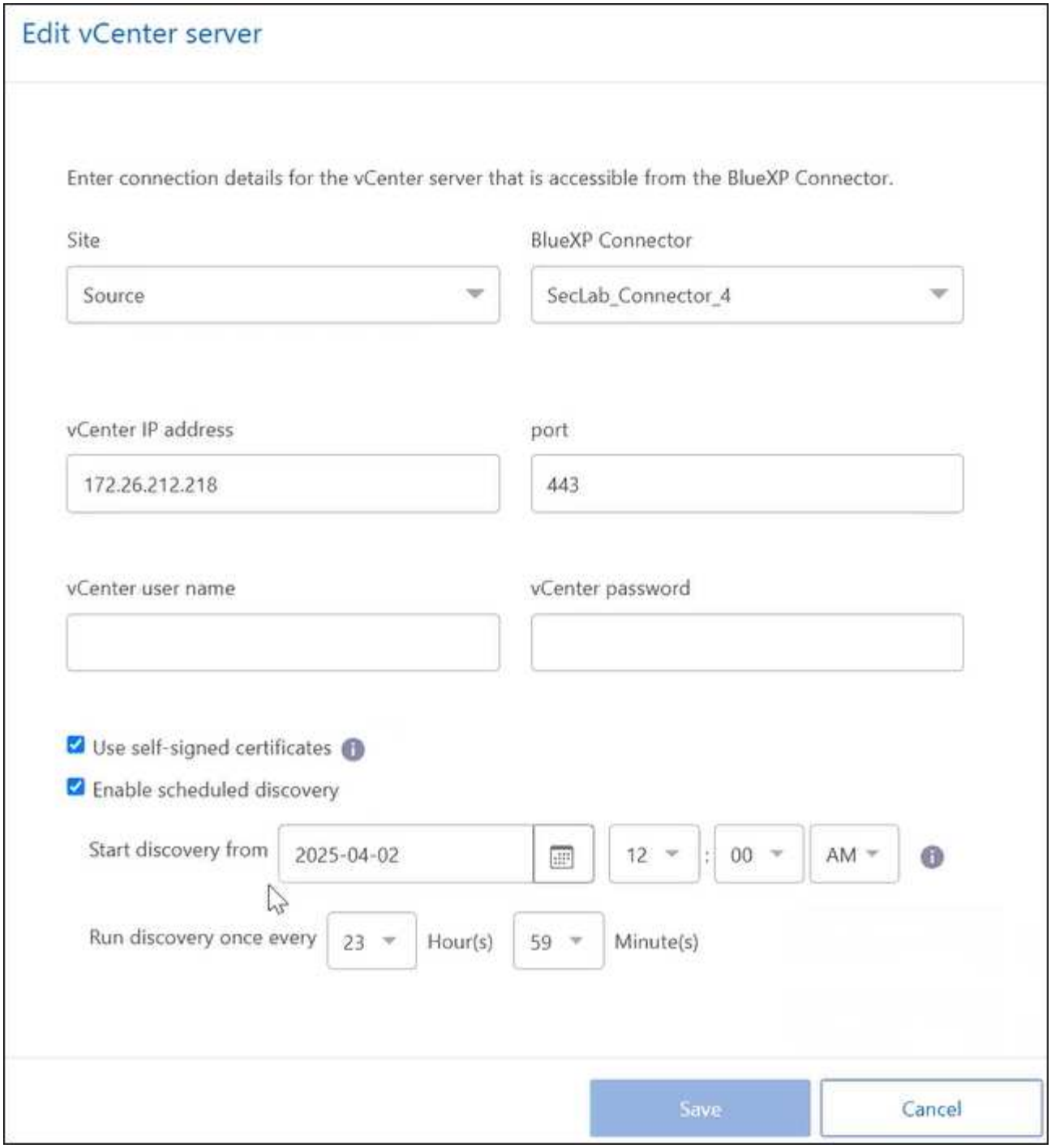
È possibile modificare il sito del server vCenter per personalizzare la pianificazione dell'individuazione. Ad esempio, se si dispone di un numero elevato di VM, è possibile impostare la pianificazione dell'individuazione in modo che venga eseguita ogni 23 ore e 59 minuti. Se si dispone di un numero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

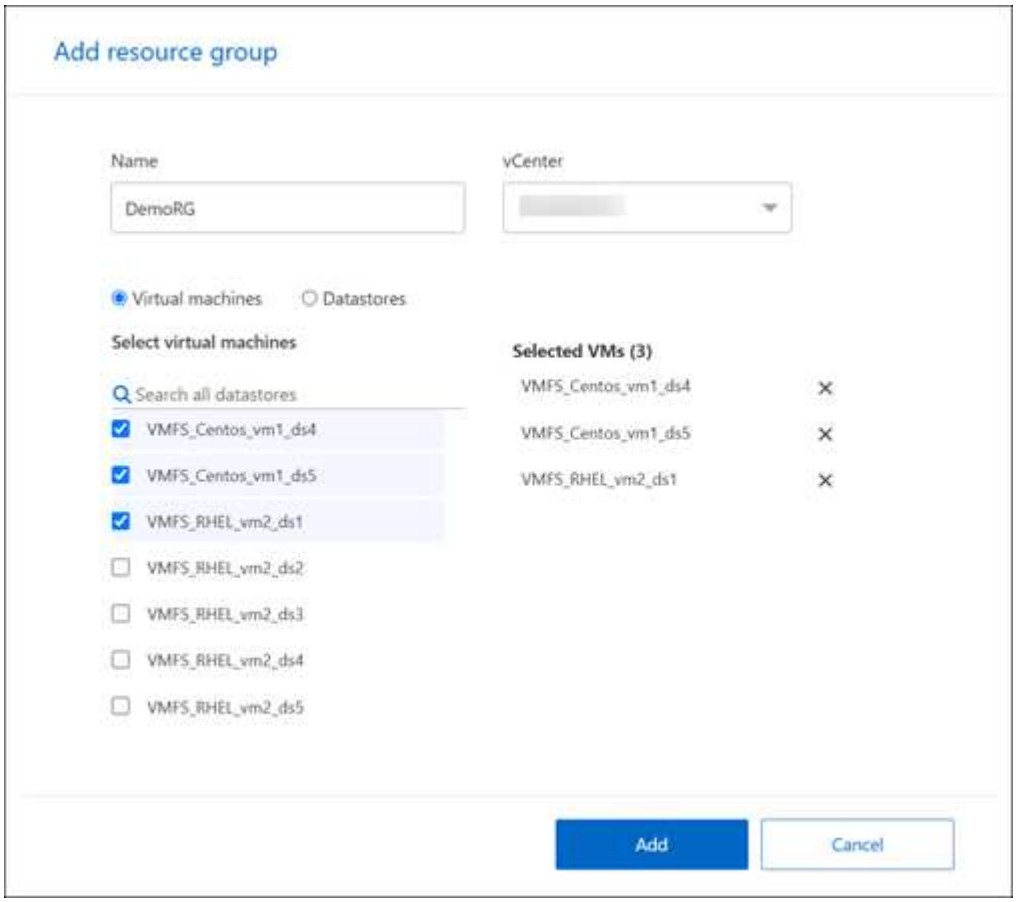
- Prima di aggiungere datastore ai gruppi di risorse, avviare prima un'individuazione manuale o un'individuazione pianificata delle VM. Ciò garantisce che le VM vengano rilevate ed elencate nel gruppo di risorse. Se non si avvia un'individuazione manuale, le VM potrebbero non essere elencate nel gruppo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

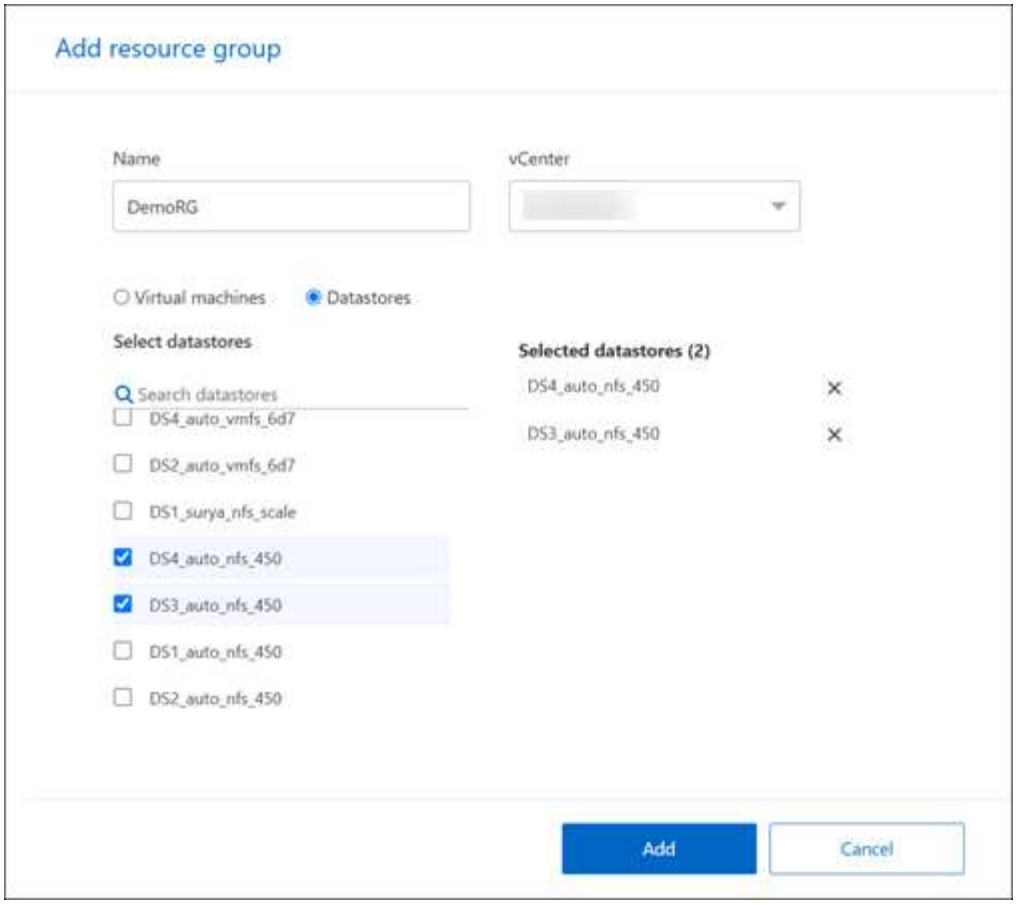
MIGLIOR PRATICITÀ: Organizzare le VM prima di implementare NetApp Disaster Recovery per ridurre al minimo la "proliferazione degli archivi dati". Posizionare le VM che necessitano di protezione su un sottoinsieme di datastore e posizionare le VM che non saranno protette su un sottoinsieme diverso di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

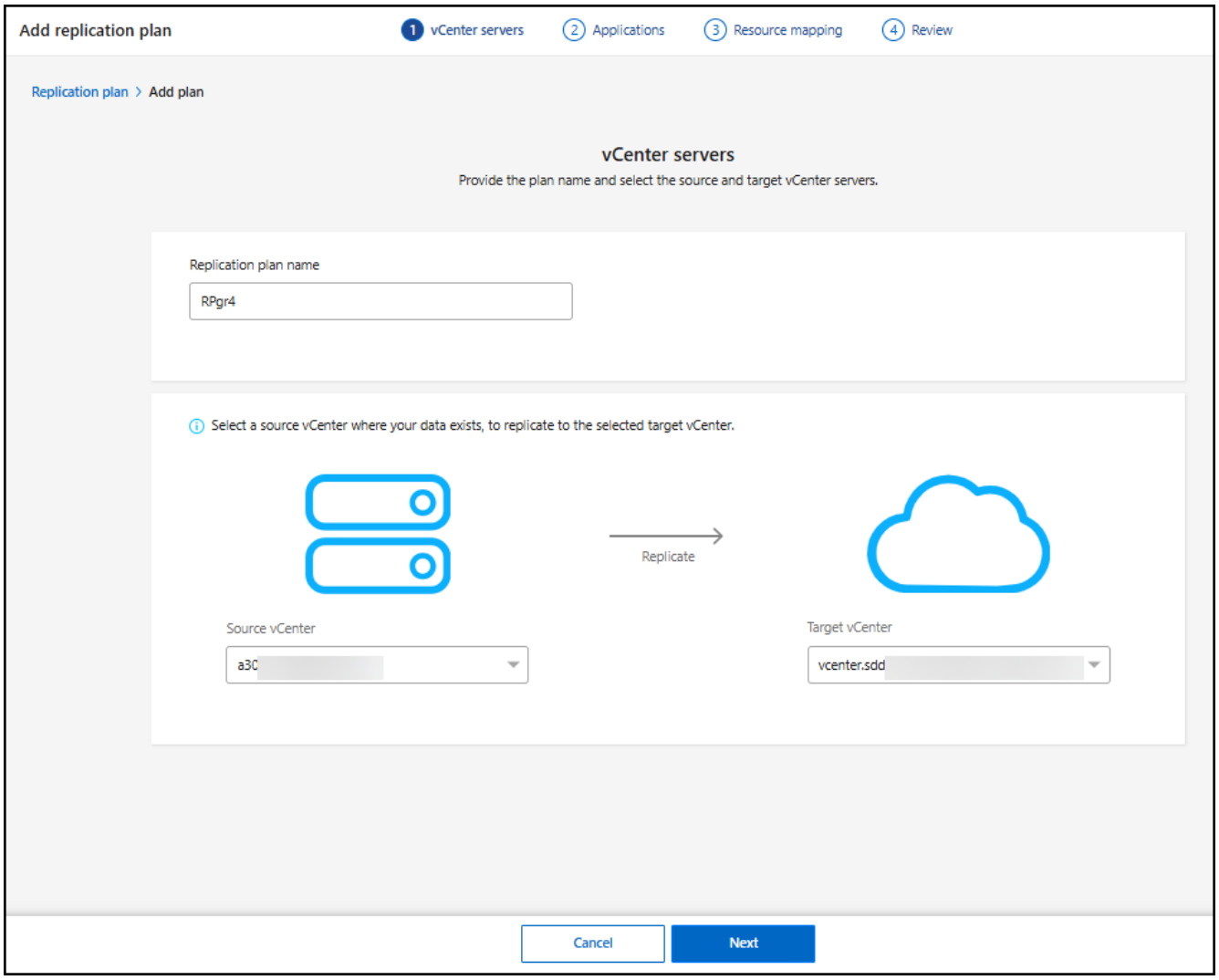
- Utilizzare le stesse credenziali per tutte le VM nel piano.
- Utilizzare lo stesso script per tutte le VM nel piano.
- Utilizzare la stessa subnet, DNS e gateway per tutte le VM nel piano.

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.

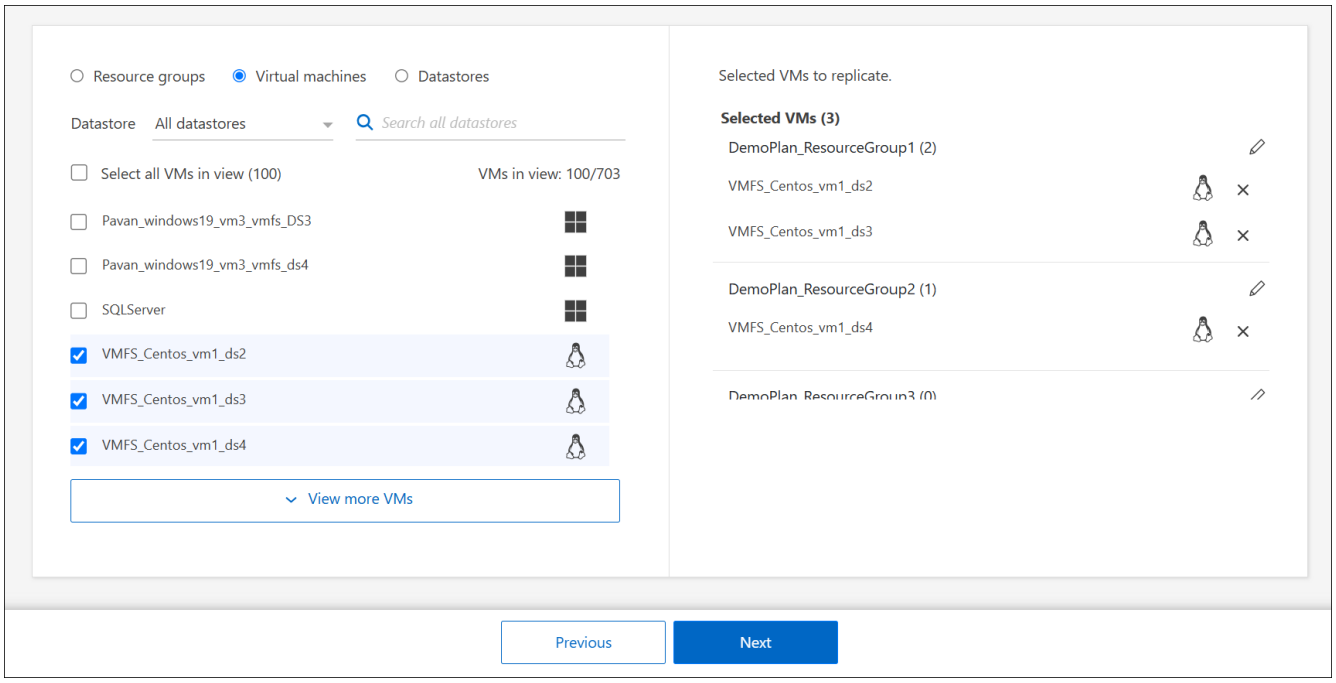
Crea un set dedicato separato di mappature per i tuoi test di failover per impedire che VMS venga connesso alle reti di produzione utilizzando gli stessi indirizzi IP.

Passi

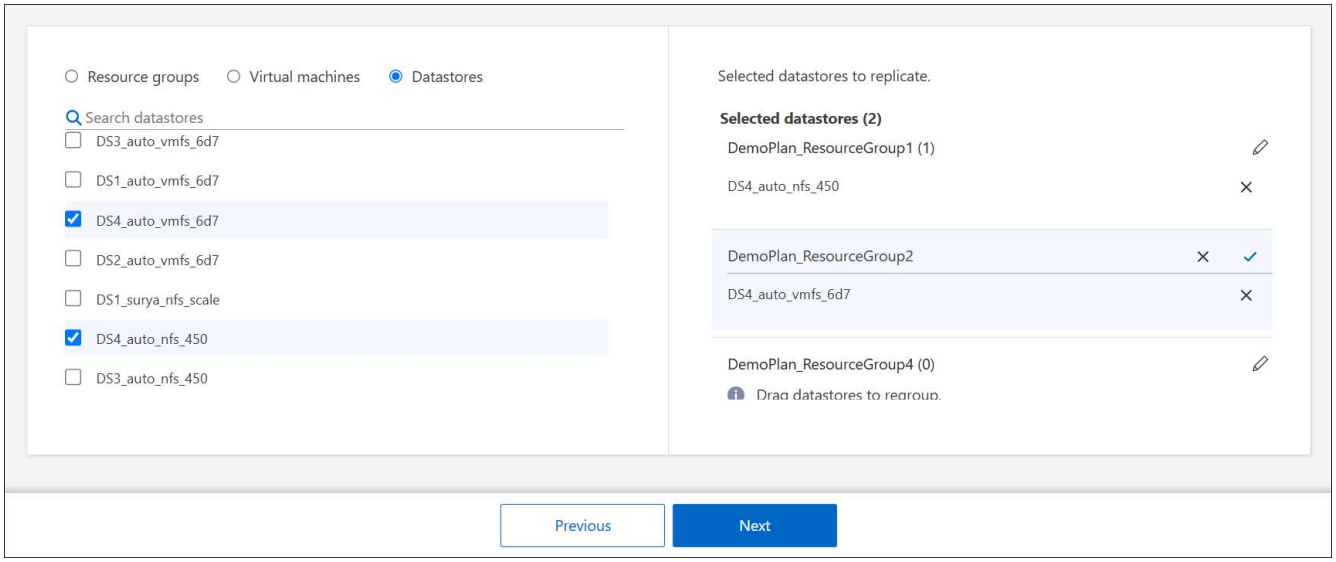
1. Selezionare **Macchine virtuali** o **Datastore**.
2. Facoltativamente, è possibile cercare una VM o un datastore specifico per nome.
3. Sul lato sinistro della pagina Applicazioni, seleziona le VM o i datastore che desideri proteggere e assegnali al gruppo selezionato.

   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.

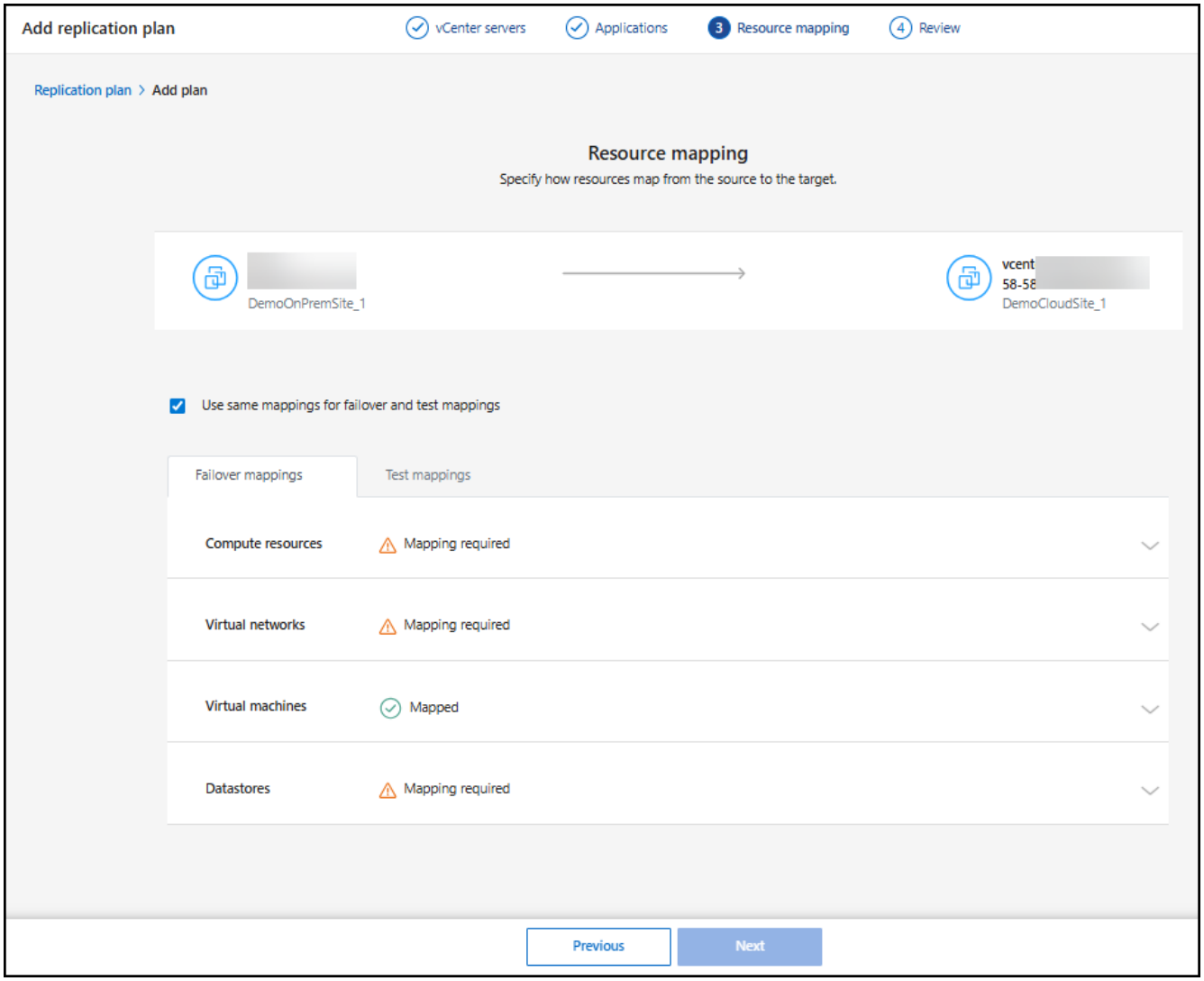
Se si prevede di eseguire failover di prova come parte del piano di ripristino di emergenza, è necessario fornire un set di mapping di failover di prova per garantire che le VM avviate durante il test di failover non interferiscano con le VM di produzione. È possibile ottenere questo risultato fornendo 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.

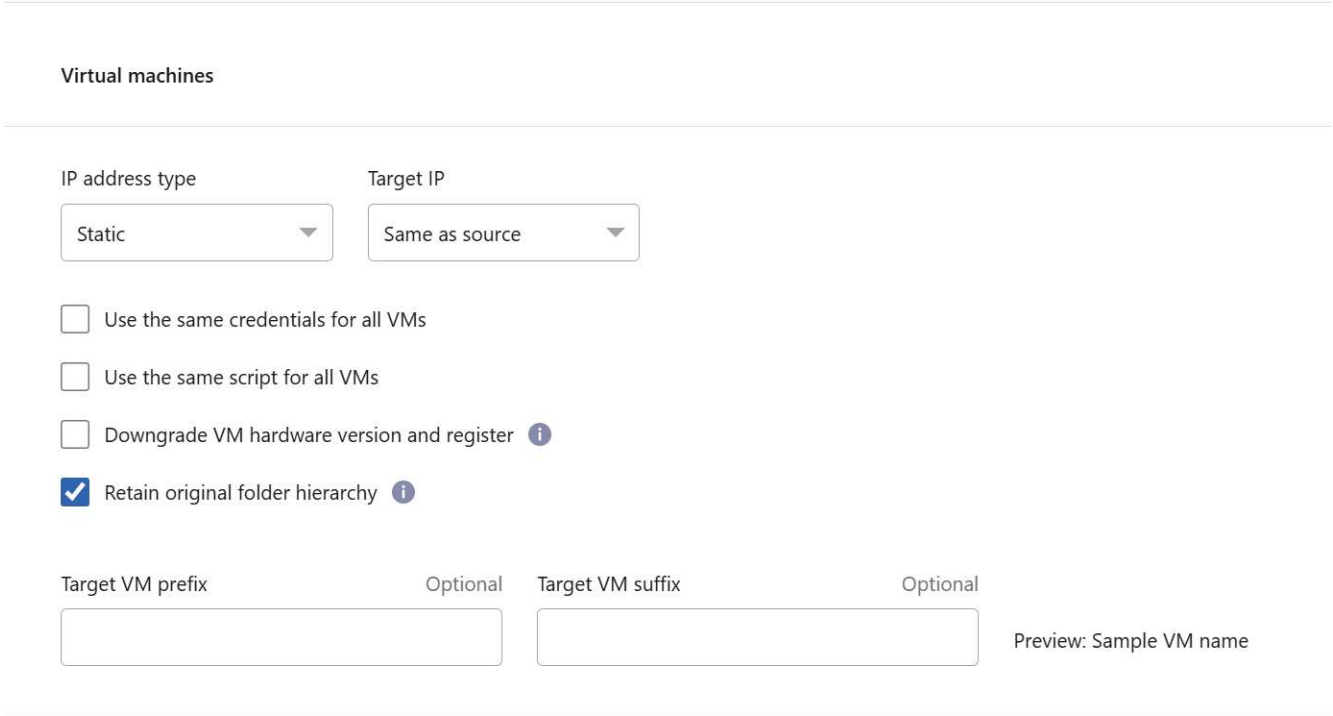
Al livello più basilare (e predefinito), le impostazioni utilizzano semplicemente le stesse impostazioni di rete TCP/IP per ogni VM sul sito di destinazione utilizzate sul sito di origine. Ciò richiede la configurazione delle stesse impostazioni TCP/IP sulle reti virtuali di origine e di destinazione.

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.

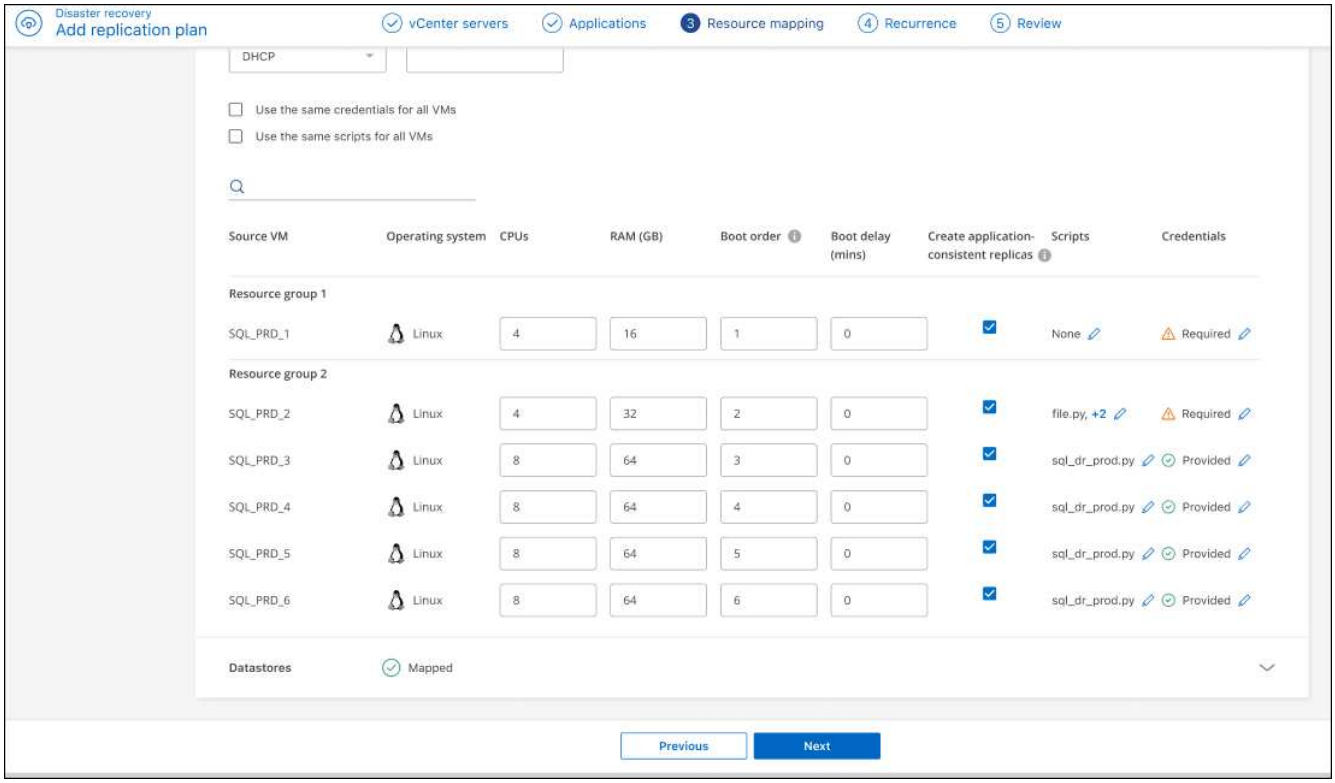
- **Prefisso e suffisso della VM di destinazione**: nei dettagli delle macchine virtuali, è possibile aggiungere facoltativamente un prefisso e un suffisso a ciascun nome di VM sottoposto a failover. Ciò può essere utile per differenziare le VM sottoposte a failover dalle VM di produzione in esecuzione 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.

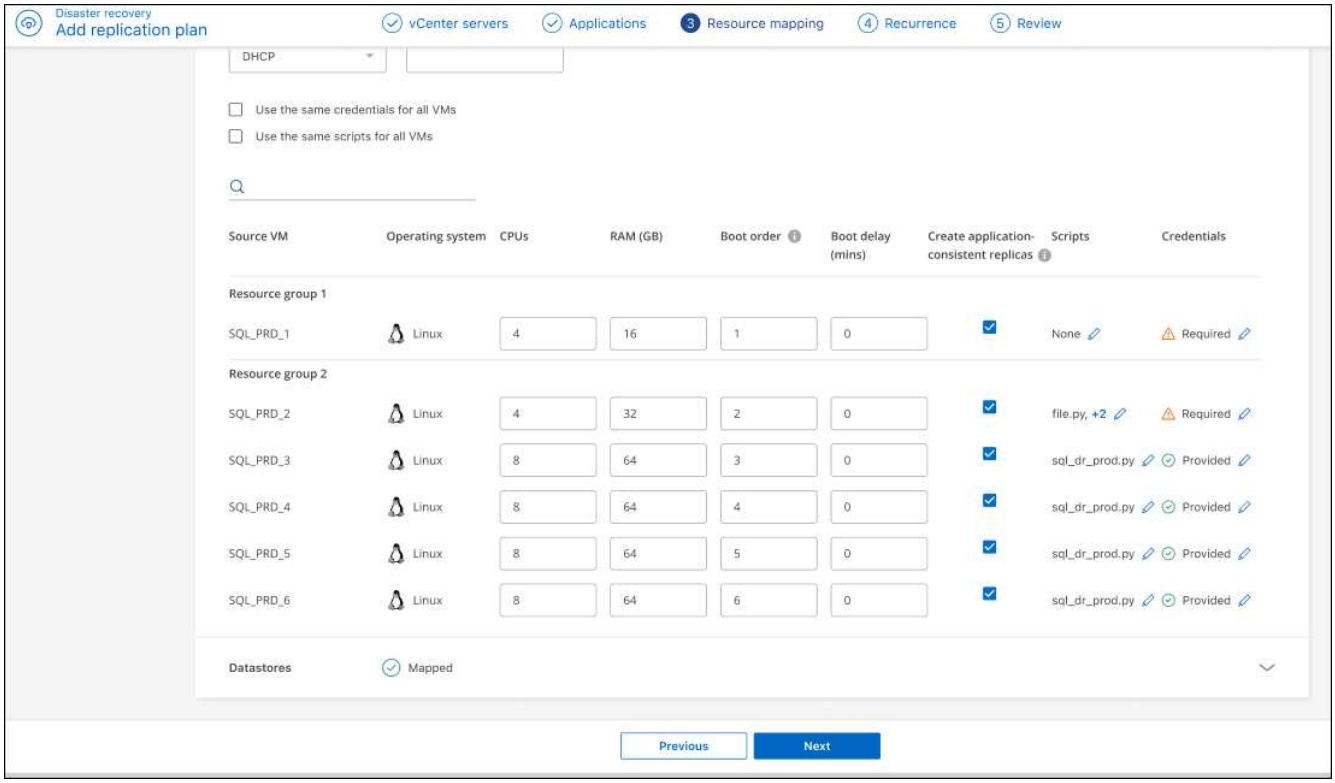
  Disaster Recovery avvia in parallelo tutte le VM con lo stesso numero di ordine di avvio.

  - 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.

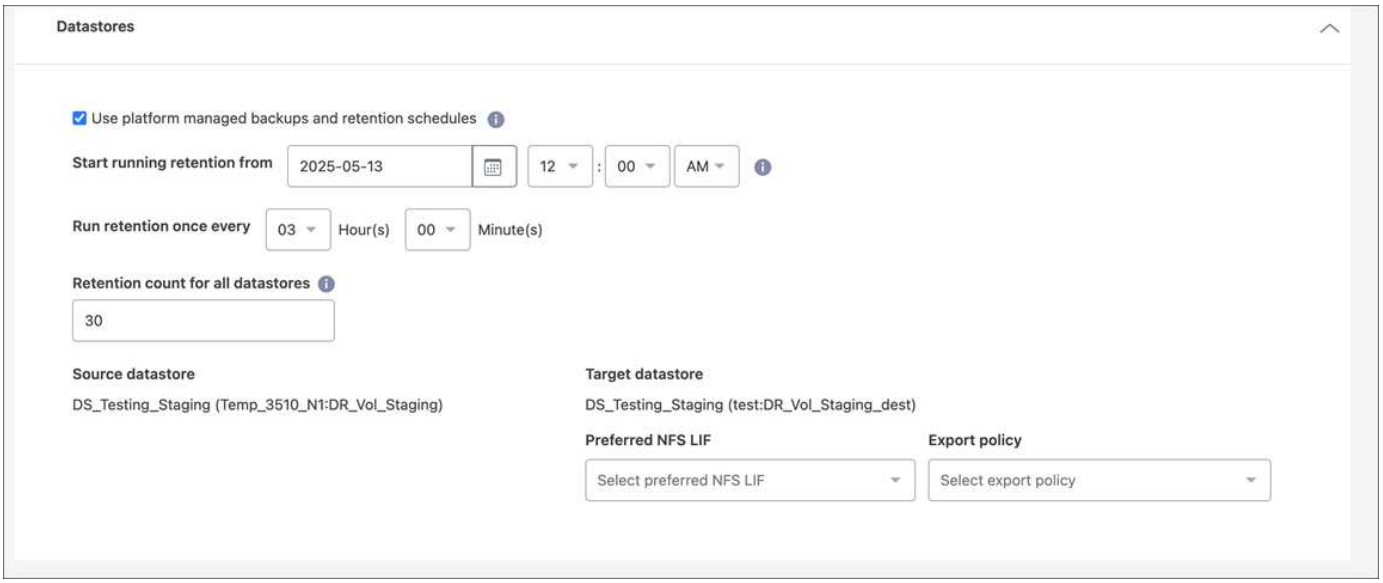
Per abilitare repliche coerenti con l'applicazione delle VM e dei relativi datastore di hosting, selezionare la casella accanto a **Crea repliche coerenti con l'applicazione** per ogni VM e fornire le credenziali di accesso guest con i privilegi appropriati.

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.

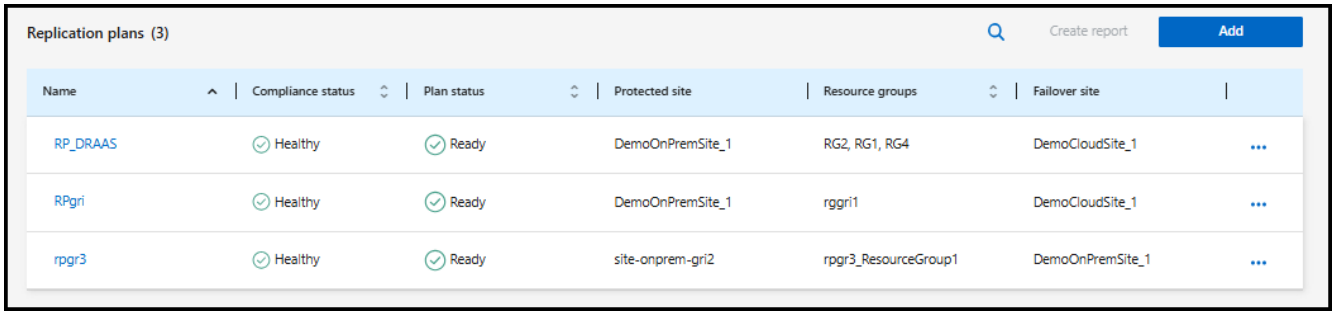
- **Impatto sui tempi di conformità**: quando viene creato un piano di replica, il servizio crea per impostazione predefinita una pianificazione di conformità. Il tempo di conformità predefinito è di 30 minuti. Per modificare questo orario, è possibile modificare la pianificazione nel piano di replica.
- **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.

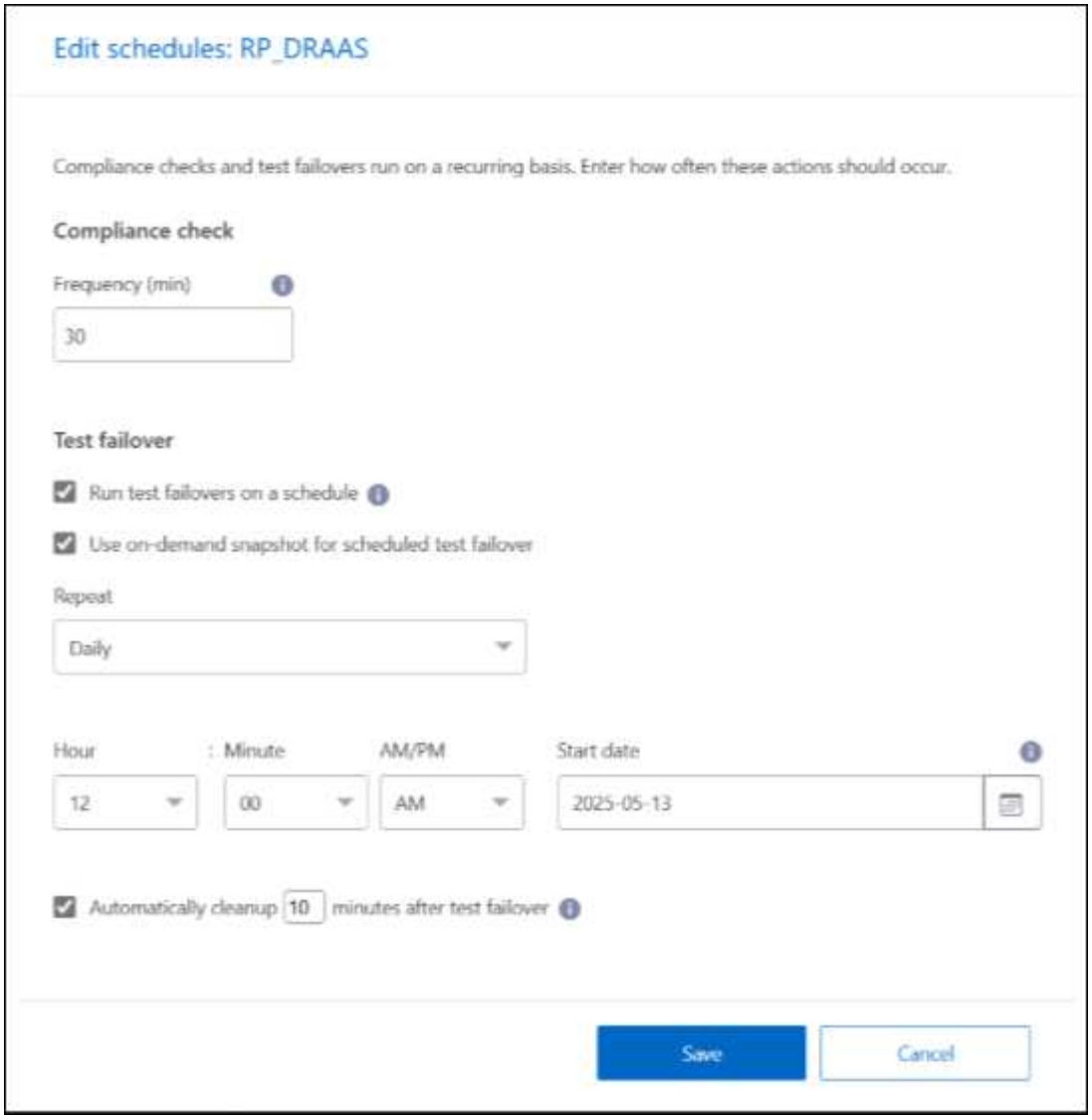
In base alla pianificazione, viene eseguito il test di failover, che garantisce che i carichi di lavoro vengano spostati verso la destinazione specificata dal piano di replica.

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.

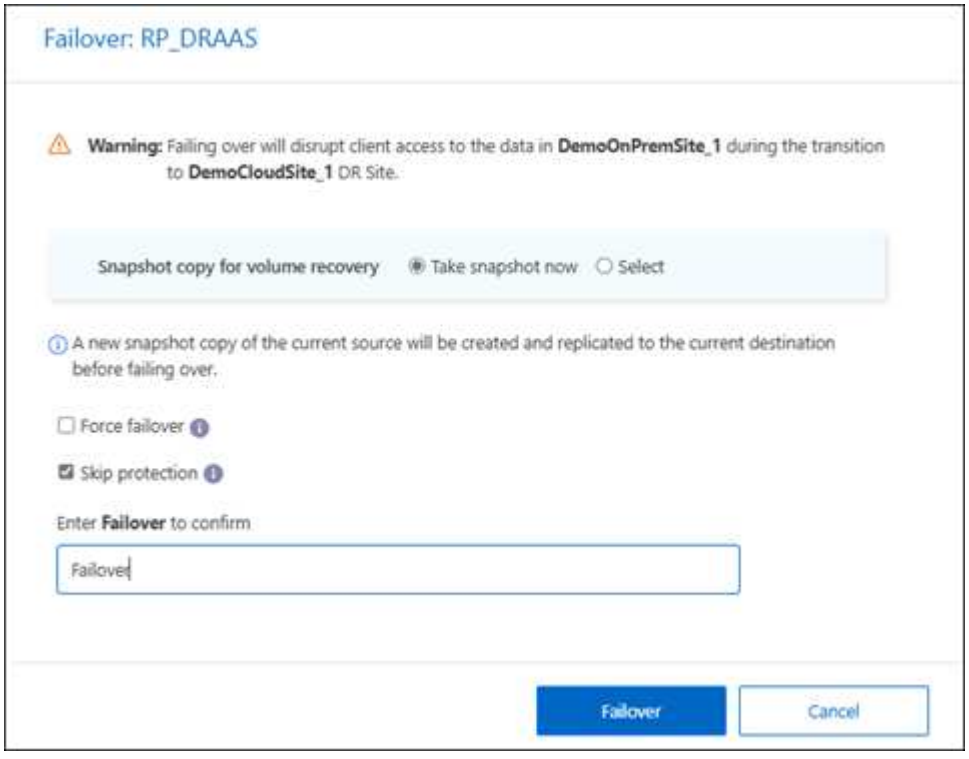
- Le macchine virtuali di destinazione vengono registrate in vCenter come nuovi datastore.
- Le macchine virtuali di destinazione vengono accese in base all'ordine di avvio acquisito nella pagina Gruppi di risorse.
- Se il vCenter di origine è ancora attivo, spegnere tutte le VM lato origine su cui è 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

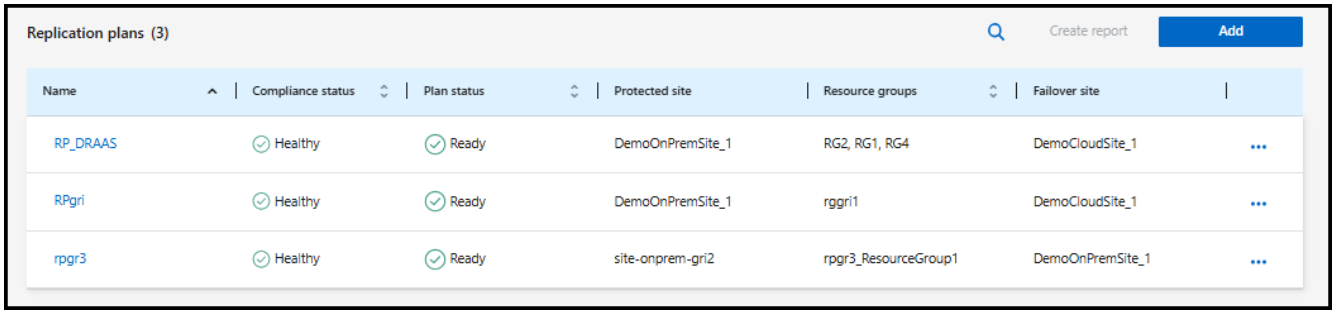
È possibile disattivare, attivare ed eliminare i piani di replica. È possibile modificare gli orari.

*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**.

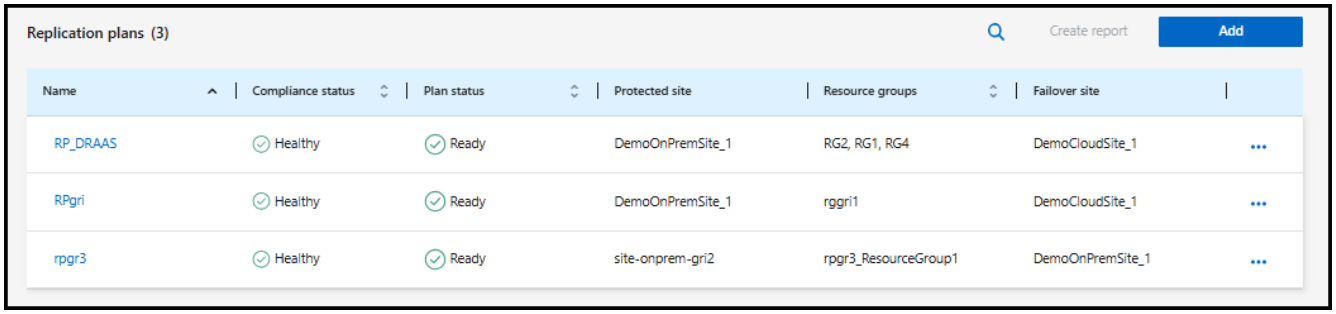
Riconcilia gli snapshot su richiesta

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**.

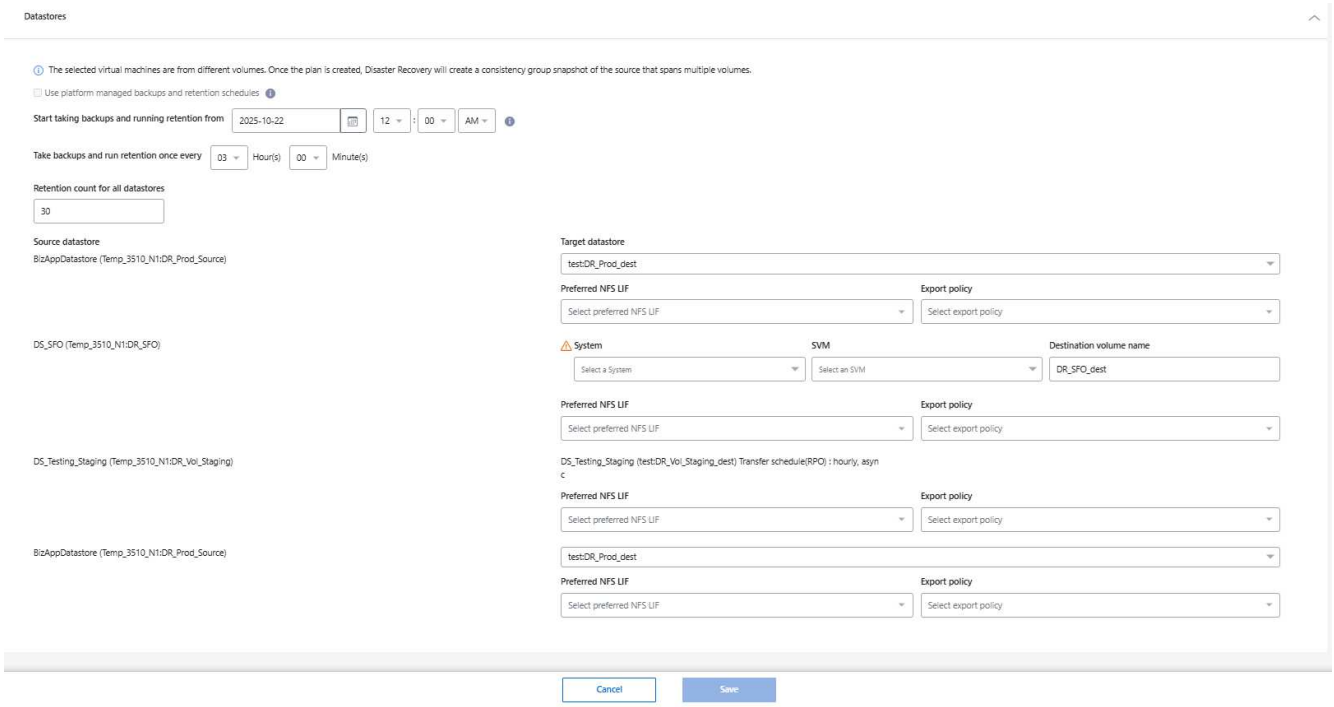
Modifica il conteggio di conservazione per le pianificazioni di failover

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.

Riferimento

Privilegi richiesti vCenter per NetApp Disaster Recovery

Affinché NetApp Disaster Recovery possa svolgere i suoi servizi, l'account vCenter deve disporre di un set minimo di privilegi vCenter. Questi privilegi includono la registrazione e la deregistrazione di datastore, l'avvio e l'arresto di macchine virtuali (VM) e la riconfigurazione delle VM.

La tabella seguente elenca tutti i privilegi richiesti affinché NetApp Disaster Recovery possa interfacciarsi con un vCenter cluster.

Tipo	Nome del privilegio (vSphere client)	Nome privilegio (API)	Descrizione
Datastore	Datastore.Config	Configura datastore	Consente di configurare un datastore.
	Datastore.Elimina	Rimuovi datastore	Consente di rimuovere un datastore.
	Datastore.Rename	Rinomina datastore	Consente di rinominare un datastore.
Cartella	Folder.Create	Crea cartella	Consente di creare una nuova cartella.
	Folder.Delete	Elimina cartella	Permette di eliminare una cartella. Richiede privilegi sia sull'oggetto che sul suo genitore.
	Folder.Rename	Rinomina cartella	Consente di modificare il nome di una cartella.
Rete	Network.Assign	Assegna rete	Consente di assegnare una rete a una VM.
	Network.Config	Configurare	Consente di configurare una rete.

Tipo	Nome del privilegio (vSphere client)	Nome privilegio (API)	Descrizione
Configurazione della macchina virtuale	VirtualMachine.Config.AdvancedConfig	Configurazione avanzata	Consente di aggiungere o modificare parametri avanzati nel file di configurazione della VM.
	VirtualMachine.Config.Settings	Modifica impostazioni	Consente di modificare le impostazioni generali della VM.
	VirtualMachine.Config.CPUCount	Modifica il conteggio della CPU	Consente di modificare il numero di CPU virtuali.
	VirtualMachine.Config.Memory	Modifica memoria	Consente di modificare la quantità di memoria allocata alla VM.
	VirtualMachine.Config.Resource	Cambia risorsa	Consente di modificare la configurazione delle risorse dei nodi VM in un pool di risorse.
	VirtualMachine.Config.Rename	Rinomina	Consente di rinominare una VM o modificarne le note.
	VirtualMachine.Config.EditDevice	Modificare le impostazioni del dispositivo	Consente di modificare le proprietà di un dispositivo esistente.
	VirtualMachine.Config.ReloadFromPath	Ricarica dal percorso	Consente di modificare un percorso di configurazione di una VM preservandone l'identità.
	VirtualMachine.Config.ResetGuestInfo	Reimposta le informazioni guest	Consente di modificare le informazioni del sistema operativo guest per una VM.
Guest della macchina virtuale	VirtualMachine.GuestOperations.ModifyAliases	Modifica dell'alias dell'operazione guest	Consente di modificare l'alias per la VM.
	VirtualMachine.GuestOperations.QueryAliases	Query alias operazione guest	Consente di interrogare l'alias di una VM.
	VirtualMachine.GuestOperations.Modifica	Modifiche alle operazioni guest	Consente operazioni di modifica, incluso il trasferimento di un file alla VM.
	VirtualMachine.GuestOperations.Execute	Esecuzione del programma guest	Consente l'esecuzione di un'applicazione all'interno della VM.
	VirtualMachine.GuestOperations.Query	Query sulle operazioni guest	Consente di interrogare il sistema operativo guest. Le operazioni includono l'elenco dei file.

Tipo	Nome del privilegio (vSphere client)	Nome privilegio (API)	Descrizione
Interazione macchina virtuale	VirtualMachine.Interact.AnswerQuestion	Rispondi alla domanda	Consente di risolvere i problemi durante le transizioni di stato della VM o gli errori di runtime.
	VirtualMachine.Interact.PowerOff	Spegni	Consente di spegnere una VM accesa.
	VirtualMachine.Interact.PowerOn	Accendi	Consente di accendere o riprendere una VM.
	VirtualMachine.Interact.ToolsInstall	Installazione di VMware Tools	Consente il montaggio/smontaggio del programma di installazione di VMware Tools.
	VirtualMachine.Inventory.CreateFromExisting	Crea da esistente	Consente la clonazione o la distribuzione di una VM da un template.
	VirtualMachine.Inventory.Create	Crea nuovo	Consente di creare una VM e allocare risorse.
	VirtualMachine.Inventory.Register	Registrati	Consente di aggiungere una VM esistente a un inventario.
	VirtualMachine.Inventory.Delete	Rimuovi	Consente di eliminare una VM e i suoi file. Richiede privilegi sia sull'oggetto che sul suo genitore.
	VirtualMachine.Inventory.Unregister	Annulla registrazione	Consente di annullare la registrazione di una VM. Questa autorizzazione richiede privilegi sia sull'oggetto che sul suo padre.
Provisioning di macchine virtuali	VirtualMachine.Provisioning.Clone	Clona macchina virtuale	Consente di clonare una VM e allocare risorse.
	VirtualMachine.Provisioning.Customize	Personalizza guest	Consente di personalizzare il sistema operativo guest della VM.
	VirtualMachine.Provisioning.ModifyCustSpecs	Modifica specifica di personalizzazione	Consente di creare, modificare o eliminare specifiche di personalizzazione.
	VirtualMachine.Provisioning.ReadCustSpecs	Leggi le specifiche di personalizzazione	Consente di leggere una specifica di personalizzazione per una VM.
Configurazione del servizio macchina virtuale	VirtualMachine.Namespace.Query	Configurazioni del servizio di query	Consente di recuperare un elenco di servizi VM.
	VirtualMachine.Namespace.ReadContent	Leggi la configurazione del servizio	Consente di recuperare la configurazione del servizio VM esistente.

Tipo	Nome del privilegio (vSphere client)	Nome privilegio (API)	Descrizione
Istantanea della macchina virtuale	VirtualMachine.State.CreateSnapshot	Crea snapshot	Consente di creare uno snapshot dallo stato corrente della VM.
	VirtualMachine.State.RemoveSnapshot	Rimuovi snapshot	Consente di rimuovere uno snapshot.
	VirtualMachine.State.RenameSnapshot	Rinomina snapshot	Consente di rinominare uno snapshot o di aggiornarne la descrizione.
	VirtualMachine.State.RevertToSnapshot	Ripristina allo snapshot	Consente di ripristinare la VM allo stato di un determinato snapshot.

Cambiare gli agenti della console quando si utilizza NetApp Disaster Recovery

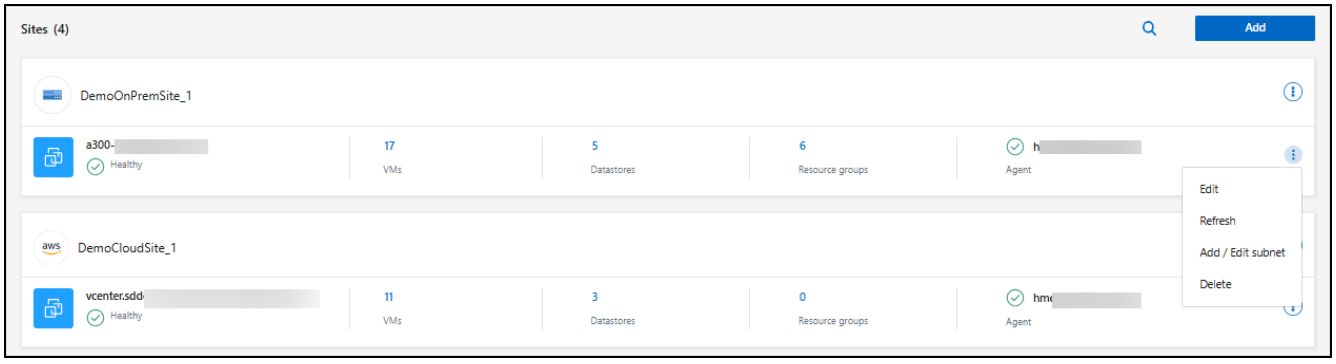
NetApp Console supporta l'utilizzo di più agenti Console con un unico ambiente di lavoro. L'utilizzo di più agenti Console può essere utile per mantenere l'accesso alle risorse durante l'esecuzione della manutenzione su un altro agente Console o in caso di errore di un agente Console. Poiché ogni agente della console ha un identificatore univoco, la commutazione impropria degli agenti della console può compromettere la disponibilità delle risorse in un ambiente di lavoro.

Prima di iniziare

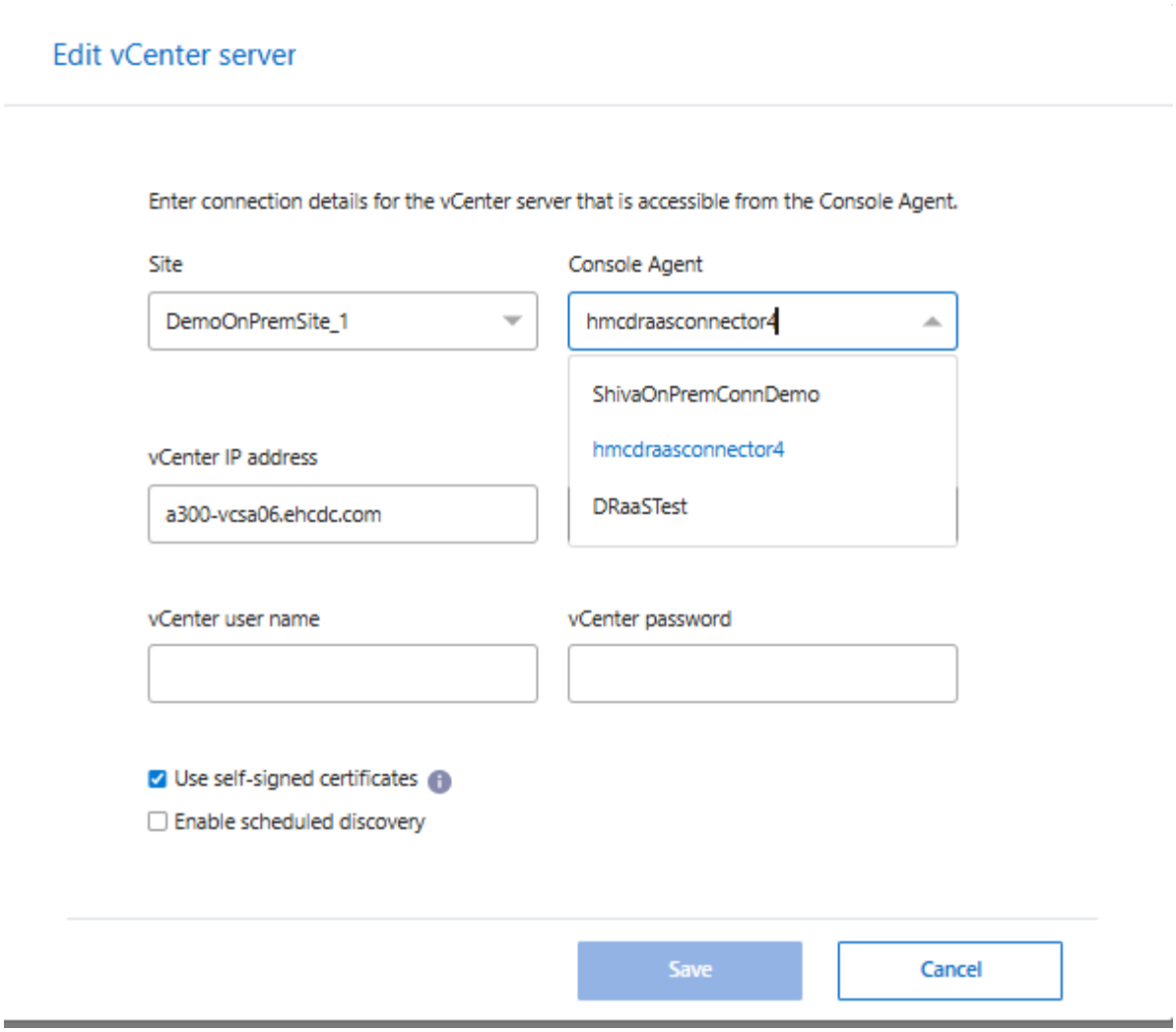
- Devi avereaggiunti almeno due agenti Console per il tuo ambiente di lavoro .
- Entrambi gli agenti della console devono contenere gli stessi cluster ONTAP .

Passi

1. In Disaster Recovery, seleziona **Siti**.
2. È necessario modificare l'agente della console sia per il vCenter di origine che per quello di destinazione. Identifica i vCenter che desideri modificare. Selezionare il menu azioni per vCenter, quindi **Modifica**.



3. Selezionare l'agente della console che si desidera utilizzare dal menu a discesa e immettere nuovamente il nome utente e la password di vCenter. Seleziona **Salva**.



4. Ripetere i passaggi 2 e 3 per ogni vCenter aggiuntivo che si desidera modificare.
5. Nel vCenter modificato, aggiorna il vCenter per individuare il nuovo agente Console. Ripetere questo passaggio per ogni vCenter modificato.
6. In Disaster Recovery, accedere a **Piani di replica**.
7. Identificare i piani di replicazione che si desidera utilizzare per riprendere i flussi di lavoro. Seleziona il menu delle azioni … quindi **Aggiorna risorse**. È possibile monitorare lo stato dei lavori in **Monitoraggio lavori**.

Ulteriori informazioni

- "Scopri di più sugli agenti della console"

Utilizzare NetApp Disaster Recovery con Amazon EVS

Introduzione di NetApp Disaster Recovery tramite Amazon Elastic VMware Service e Amazon FSx for NetApp ONTAP

I clienti dipendono sempre più dalle infrastrutture virtualizzate per i carichi di lavoro di elaborazione di produzione, come quelle basate su VMware vSphere. Poiché queste macchine virtuali (VM) sono diventate sempre più critiche per le loro attività, i clienti

devono proteggerle dagli stessi tipi di disastri a cui sono soggette le loro risorse di elaborazione fisiche. Le soluzioni di disaster recovery (DR) attualmente offerte sono complesse, costose e richiedono molte risorse. NetApp, il più grande fornitore di storage utilizzato per infrastrutture virtualizzate, ha un interesse personale nel garantire che le VM dei suoi clienti siano protette allo stesso modo in cui proteggiamo i dati ospitati nello storage ONTAP di qualsiasi tipo. Per raggiungere questo obiettivo, NetApp ha creato il servizio NetApp Disaster Recovery .

Una delle principali sfide di qualsiasi soluzione DR è la gestione dei costi incrementali di acquisto, configurazione e manutenzione di risorse di elaborazione, rete e storage aggiuntive, solo per fornire un'infrastruttura di replica e ripristino DR. Un'opzione diffusa per proteggere le risorse virtuali critiche in sede è quella di utilizzare risorse virtuali ospitate nel cloud come infrastruttura di replica e ripristino DR. Amazon è un esempio di una soluzione di questo tipo, in grado di fornire risorse convenienti e compatibili con le infrastrutture VM ospitate da NetApp ONTAP .

Amazon ha presentato Amazon Elastic VMware Service (Amazon EVS) che abilita VMware Cloud Foundation all'interno del tuo cloud privato virtuale (VPC). Amazon EVS offre la resilienza e le prestazioni di AWS insieme al noto software e agli strumenti VMware, consentendo di integrare Amazon EVS vCenters come estensione della tua infrastruttura virtualizzata locale.

Sebbene Amazon EVS includa risorse di storage, l'utilizzo di storage nativo può ridurne l'efficacia per le organizzazioni con carichi di lavoro ad alto consumo di storage. In questi casi, l'abbinamento di Amazon EVS con Amazon FSx for NetApp ONTAP (Amazon FSxN) può fornire una soluzione di storage più flessibile. Inoltre, quando si utilizzano le soluzioni di storage NetApp ONTAP in locale per ospitare l'infrastruttura VMware, l'utilizzo di Amazon EVS con FSx per ONTAP significa ottenere le migliori funzionalità di interoperabilità e protezione dei dati tra le infrastrutture in locale e quelle ospitate nel cloud.

Per informazioni su Amazon FSx for NetApp ONTAP, vedere "Introduzione ad Amazon FSx for NetApp ONTAP" .

Panoramica della soluzione NetApp Disaster Recovery tramite Amazon EVS e Amazon FSs per NetApp ONTAP

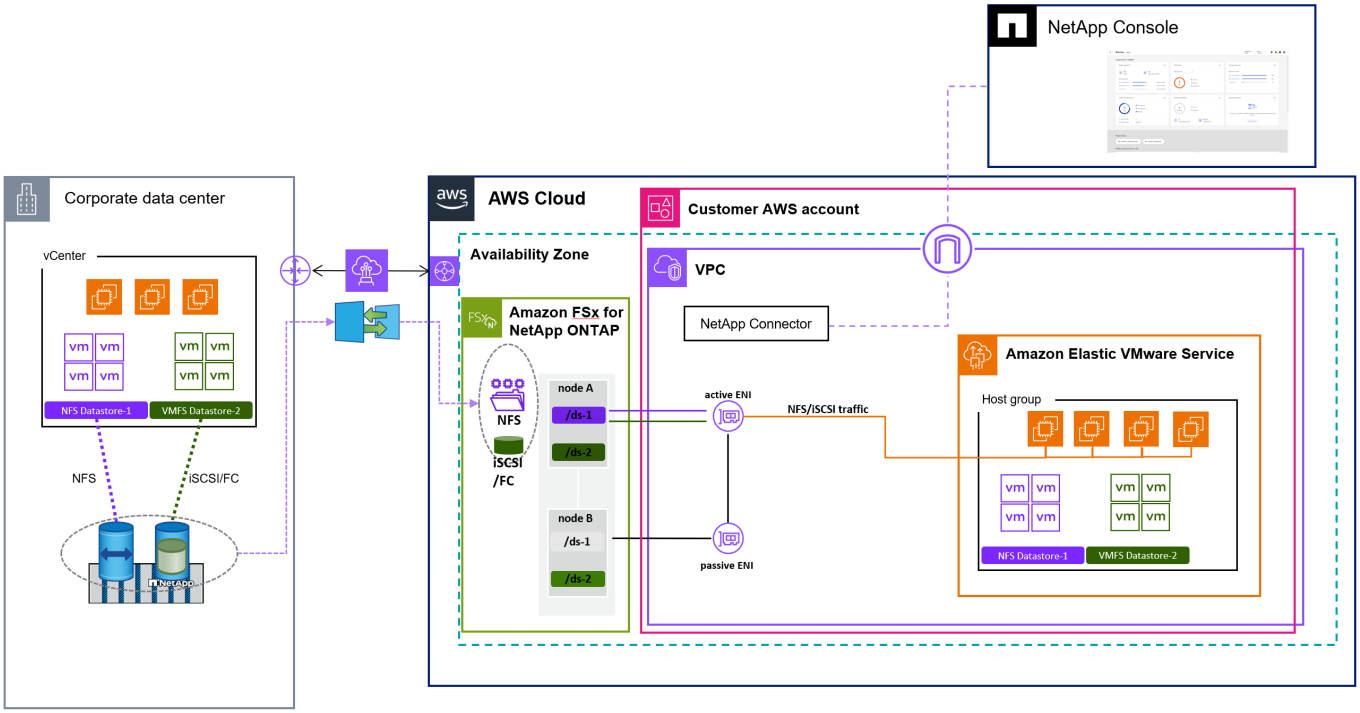
NetApp Disaster Recovery è un servizio a valore aggiunto ospitato nell'ambiente software-as-a-service NetApp Console , che dipende dall'architettura principale NetApp Console . Diversi componenti principali costituiscono il servizio DR per la protezione VMware all'interno della Console.

Per una panoramica completa della soluzione NetApp Disaster Recovery , vedere"Scopri di più su NetApp Disaster Recovery per VMware" .

Se desideri proteggere le tue macchine virtuali VMware ospitate in locale su Amazon AWS, utilizza il servizio per eseguire il backup su Amazon EVS con Amazon FSx for NetApp ONTAP .

La figura seguente mostra come funziona il servizio per proteggere le VM con Amazon EVS.

Panoramica di NetApp Disaster Recovery con Amazon EVS e FSx per ONTAP



1. Amazon EVS viene distribuito nel tuo account in una configurazione con un'unica zona di disponibilità (AZ) e all'interno del tuo Virtual Private Cloud (VPC).
2. Un file system FSx per ONTAP viene distribuito nella stessa zona di disponibilità della distribuzione Amazon EVS. Il file system si connette ad Amazon EVS direttamente tramite un'interfaccia di rete elastica (ENI), una connessione peer VPC o un AmazonTransit Gateway.
3. L'agente NetApp Console è installato nella tua VPC. L'agente NetApp Console ospita più servizi di gestione dei dati (chiamati agenti), tra cui l'agente NetApp Disaster Recovery che gestisce il DR dell'infrastruttura VMware sia sui data center fisici locali sia sulle risorse ospitate su Amazon AWS.
4. L'agente NetApp Disaster Recovery comunica in modo sicuro con il servizio ospitato nel cloud NetApp Console per ricevere attività e distribuirle alle istanze di storage vCenter e ONTAP appropriate, sia in locale che ospitate su AWS.
5. È possibile creare un piano di replica utilizzando la console dell'interfaccia utente ospitata nel cloud NetApp Console , indicando le VM da proteggere, la frequenza con cui tali VM devono essere protette e le procedure da eseguire per riavviare tali VM in caso di failover dal sito locale.
6. Il piano di replicazione determina quali datastore vCenter ospitano le VM protette e i volumi ONTAP che ospitano tali datastore. Se i volumi non esistono ancora sul cluster FSx for ONTAP , NetApp Disaster Recovery li crea automaticamente.
7. Viene creata una relazione SnapMirror per ciascun volume ONTAP di origine identificato per ciascun volume ONTAP di destinazione ospitato da FSx for ONTAP e viene creata una pianificazione di replicazione basata sull'RPO fornito dall'utente nel piano di replicazione.
8. In caso di guasto del sito primario, un amministratore avvia un processo di failover manuale all'interno della NetApp Console e seleziona un backup da utilizzare come punto di ripristino.
9. L'agente NetApp Disaster Recovery attiva i volumi di protezione dei dati ospitati da FSx per ONTAP .
10. L'agente registra ogni volume FSx for ONTAP attivato con Amazon EVS vCenter, registra ogni VM protetta con Amazon EVS vCenter e avvia ciascuna di esse in base alle regole predefinite contenute nel piano di replica.

Installa l’agente NetApp Console per NetApp Disaster Recovery

Un agente NetApp Console consente di connettere le distribuzioni NetApp Console alla propria infrastruttura per orchestrare in modo sicuro soluzioni su AWS, Azure, Google Cloud o ambienti on-premises. L’agente Console esegue le azioni che la NetApp Console deve eseguire per gestire la propria infrastruttura dati. L’agente Console interroga costantemente il livello software as a service NetApp Disaster Recovery per eventuali azioni da intraprendere.

Per NetApp Disaster Recovery, le azioni eseguite orchestrano i cluster VMware vCenter e le istanze di storage ONTAP utilizzando API native per ciascun servizio, al fine di fornire protezione alle VM di produzione in esecuzione in una posizione on-premises. Sebbene l’agente Console possa essere installato in qualsiasi posizione della rete, si consiglia di installare l’agente Console nel sito di disaster recovery per NetApp Disaster Recovery. L’installazione nel sito di DR garantisce che, in caso di guasto del sito primario, l’interfaccia utente della NetApp Console mantenga la connessione all’agente Console e possa orchestrare il processo di ripristino all’interno di tale sito di DR.

Installazione

- Per utilizzare il Disaster Recovery, installare l’agente Console in modalità standard. Per ulteriori informazioni sui tipi di installazione dell’agente Console, visitare "Scopri le modalità di distribuzione della NetApp Console".

I passaggi specifici di installazione dell’agente Console dipendono dal tipo di distribuzione. Vedere "Scopri di più sugli agenti della console" per ulteriori informazioni.

> Il metodo più semplice per installare l’agente Console con Amazon AWS è utilizzare AWS Marketplace. Per dettagli sull’installazione dell’agente Console tramite AWS Marketplace, vedere "Crea un agente della Console da AWS Marketplace".

Configurare NetApp Disaster Recovery per Amazon EVS

Panoramica sulla configurazione NetApp Disaster Recovery per Amazon EVS

Dopo aver installato l’agente NetApp Console , è necessario integrare tutte le risorse di storage ONTAP e VMware vCenter che parteciperanno al processo di disaster recovery con NetApp Disaster Recovery.

- "Prerequisiti per Amazon EVS con NetApp Disaster Recovery"
- "Aggiungere array di storage ONTAP a NetApp Disaster Recovery"
- "Abilita NetApp Disaster Recovery per Amazon EVS"
- "Aggiungere siti vCenter a NetApp Disaster Recovery"
- "Aggiungere cluster vCenter a NetApp Disaster Recovery"

Prerequisiti per Amazon EVS con NetApp Disaster Recovery

Assicurati di esaminare e soddisfare i requisiti per configurare Amazon EVS con NetApp Disaster Recovery.

Prerequisiti

- Rivedi il "prerequisiti generali per il Disaster Recovery".
- Creare un account utente vCenter con i privilegi VMware specifici richiesti affinché NetApp Disaster Recovery esegua le operazioni necessarie.

> Si consiglia di **non** utilizzare l'account amministratore predefinito "administrator@vsphere.com". Invece, è necessario creare un account utente specifico per NetApp Disaster Recovery su tutti i cluster vCenter che parteciperanno al processo di disaster recovery. Per un elenco dei privilegi specifici richiesti, vedere "Privilegi vCenter necessari per NetApp Disaster Recovery".

- Assicurarsi che tutti gli archivi dati vCenter che ospiteranno le VM protette da Disaster Recovery siano posizionati su NetApp ONTAP risorse di storage.

  Disaster Recovery supporta NFS e VMFS su iSCSI (e non FC) quando si utilizza Amazon FSx su NetApp ONTAP. Sebbene Disaster Recovery supporti FC, Amazon FSx for NetApp ONTAP non lo fa.

- Assicurati che il tuo Amazon EVS vCenter sia connesso a un Amazon FSx for NetApp ONTAP storage cluster.
- Assicurarsi che VMware tools siano installati su tutte le VM protette.
- Assicurati che la tua rete locale sia connessa alla tua rete AWS VPC tramite un metodo di connessione approvato da Amazon. Si consiglia di utilizzare AWS Direct Connect, AWS Private Link o una AWS Site-to-Site VPN.
- Esaminare e garantire la conformità con i requisiti di connessione e porta per EVS con Disaster Recovery:

Fonte	Destinazione	Porta	Dettagli
Amazon FSxN	ONTAP on-premise	TCP 11104, 11105, ICMP	SnapMirror
ONTAP on-premise	Amazon FSxN	TCP 11104, 11105, ICMP	SnapMirror
Agente NetApp Console	ONTAP on-premise	TCP 443, solo ICMP	chiamate API
Agente NetApp Console	Amazon FSxN	TCP 441, solo ICMP	chiamate API
Agente NetApp Console	vCenter (in sede, EVS), host ESXi (in sede, EVS)	443	Chiamate API, esecuzione di script

Aggiungi array locali al sistema NetApp Console per Amazon EVS con NetApp Disaster Recovery

Prima di utilizzare NetApp Disaster Recovery, è necessario aggiungere istanze di storage locali e ospitate sul cloud al sistema NetApp Console .

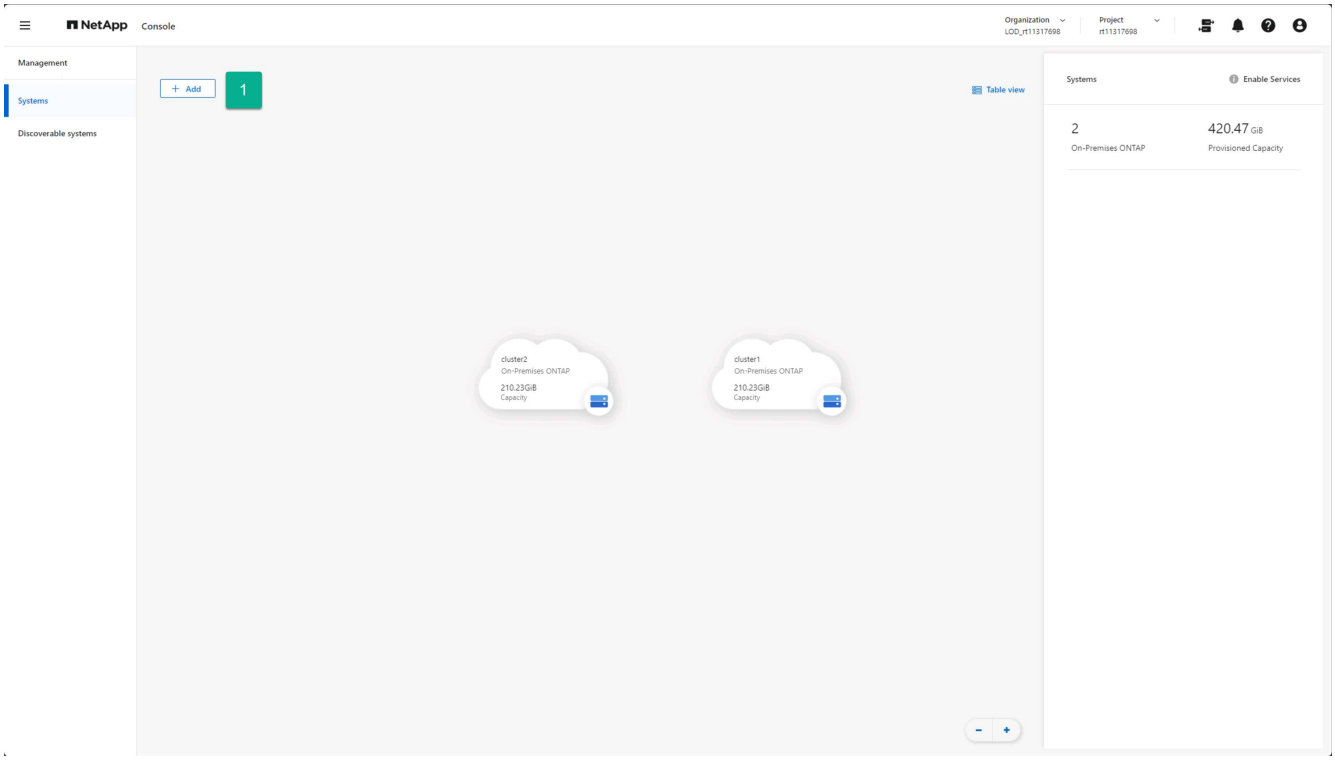
Devi fare quanto segue:

- Aggiungi array locali al tuo sistema NetApp Console .
- Aggiungi istanze Amazon FSx for NetApp ONTAP (FSx for ONTAP) al tuo sistema NetApp Console .

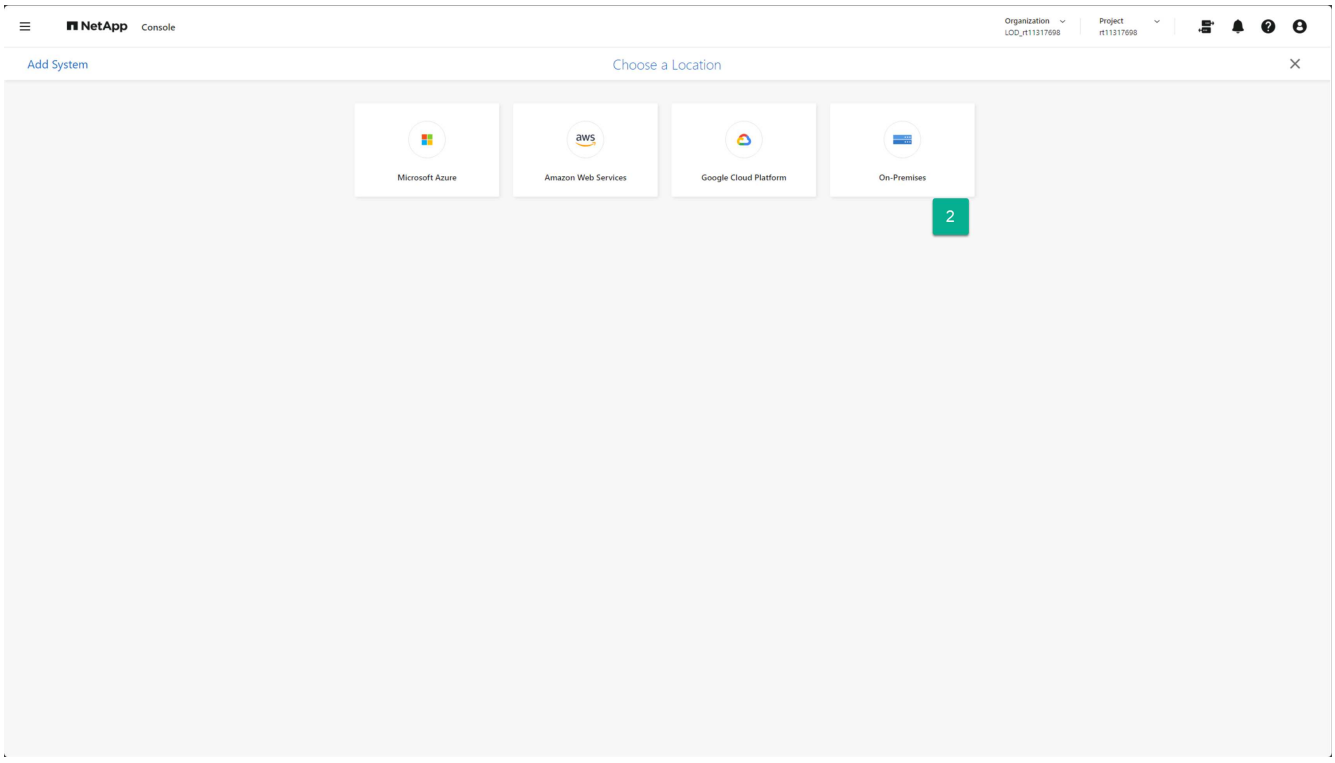
Aggiungere array di storage locali al sistema NetApp Console

Aggiungi risorse di storage ONTAP on-premise al tuo sistema NetApp Console .

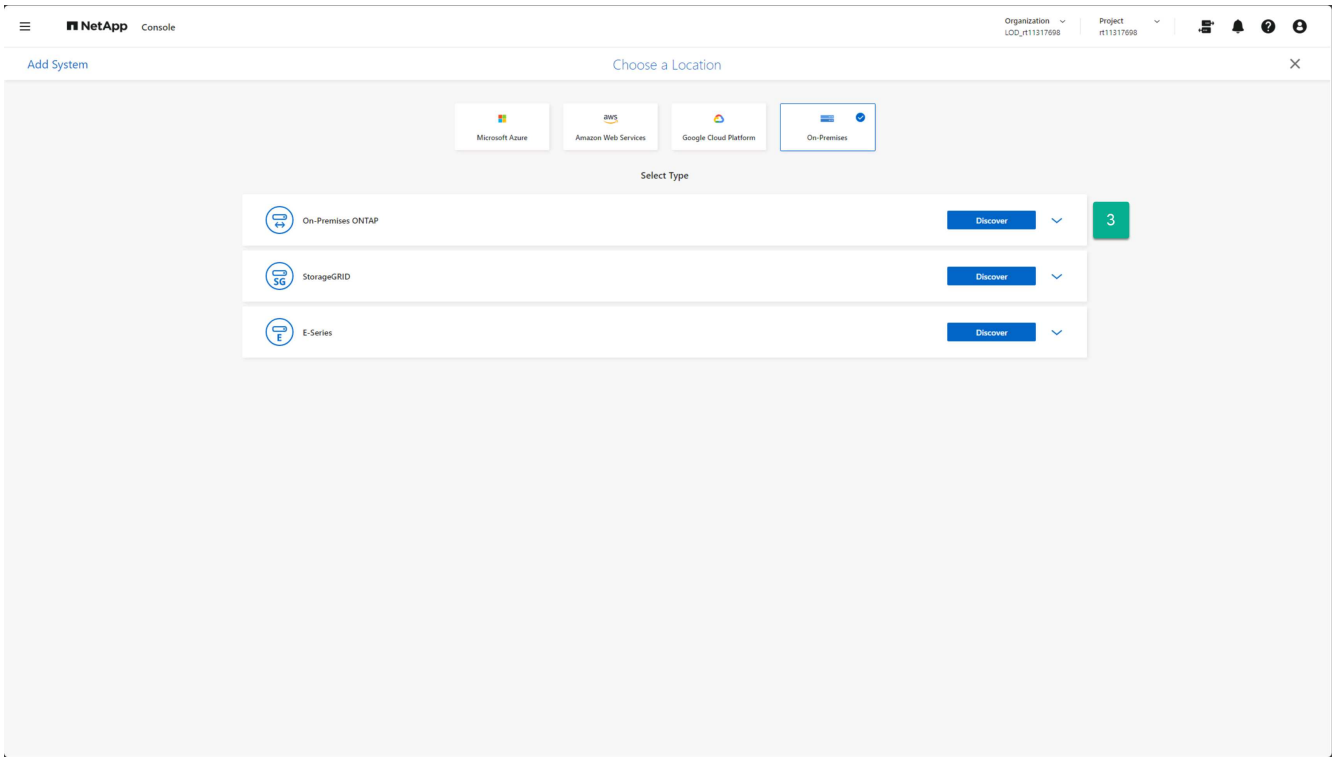
1. Dalla pagina Sistemi NetApp Console , selezionare **Aggiungi sistema**.



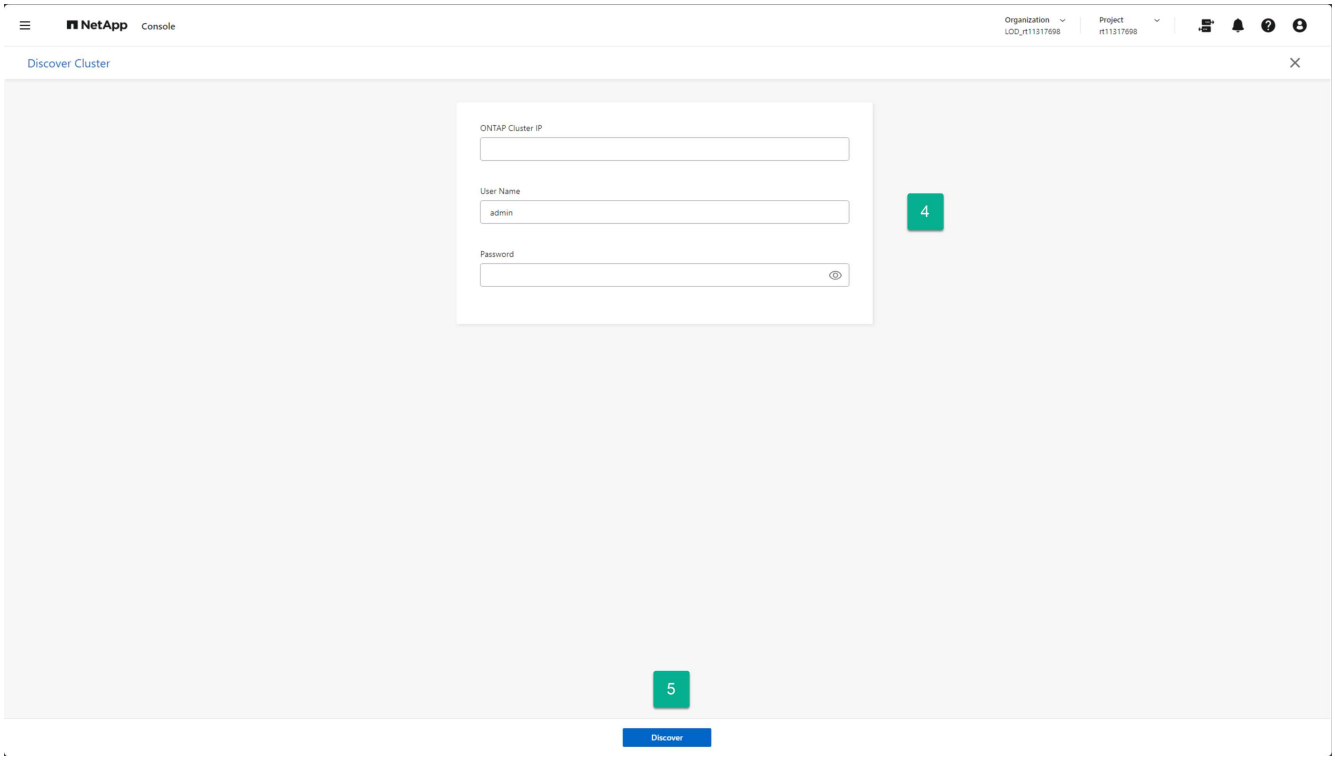
2. Nella pagina Aggiungi sistema, seleziona la scheda **On-Premises**.



3. Selezionare **Scopri** sulla scheda ONTAP On-Premises.



4. Nella pagina Scopri cluster, inserisci le seguenti informazioni:
   a. L'indirizzo IP della porta di gestione del cluster array ONTAP
   b. Il nome utente dell'amministratore
   c. La password dell'amministratore
5. Seleziona **Scopri** in fondo alla pagina.

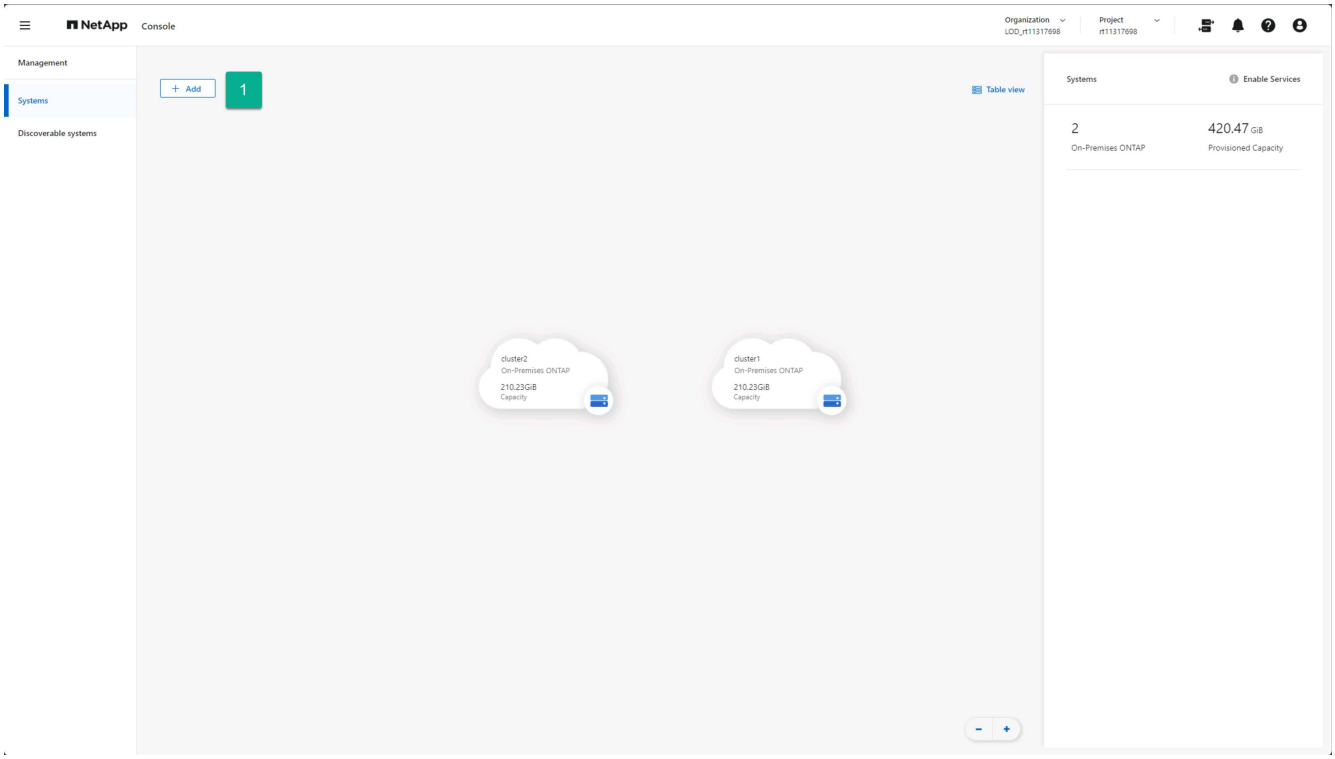


6. Ripetere i passaggi da 1 a 5 per ogni array ONTAP che ospiterà i datastore vCenter.

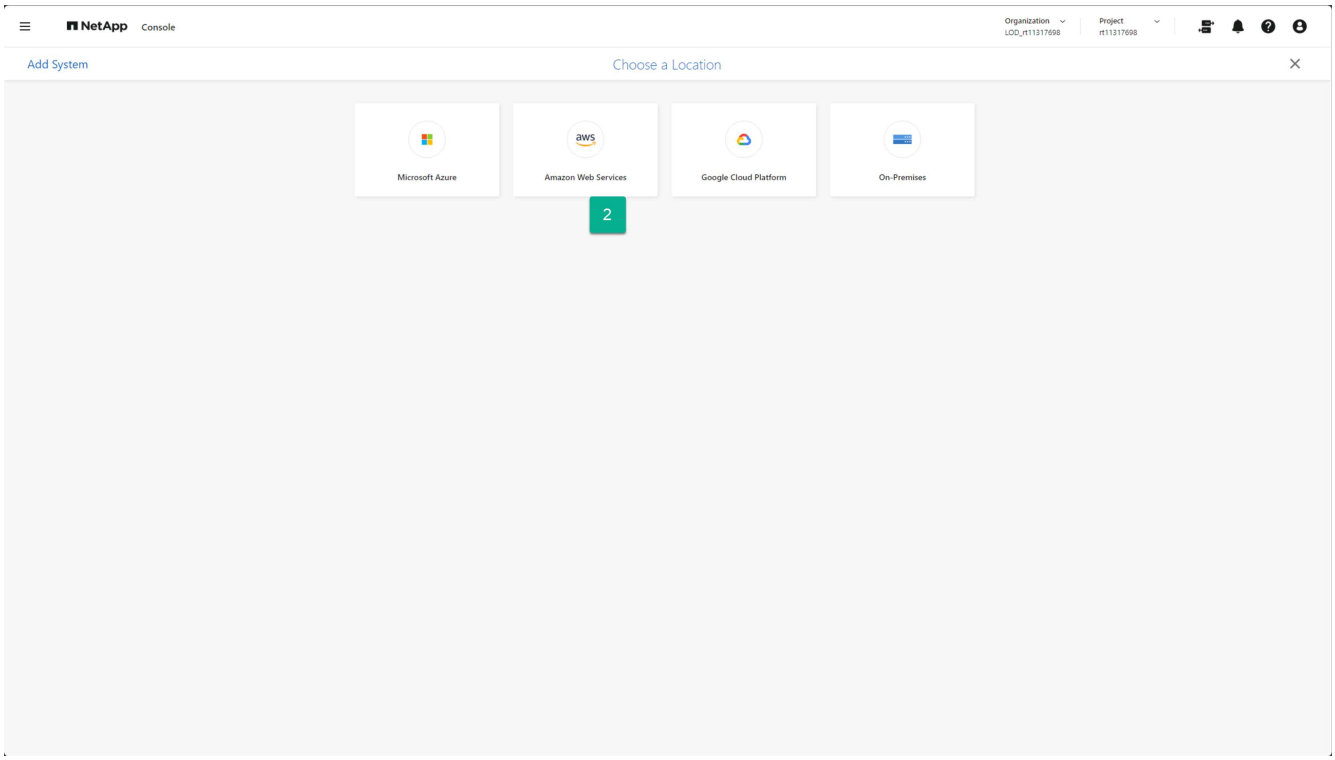
Aggiungere istanze di storage Amazon FSx for NetApp ONTAP al sistema NetApp Console

Successivamente, aggiungi risorse di storage Amazon FSx for NetApp ONTAP al tuo sistema NetApp Console .

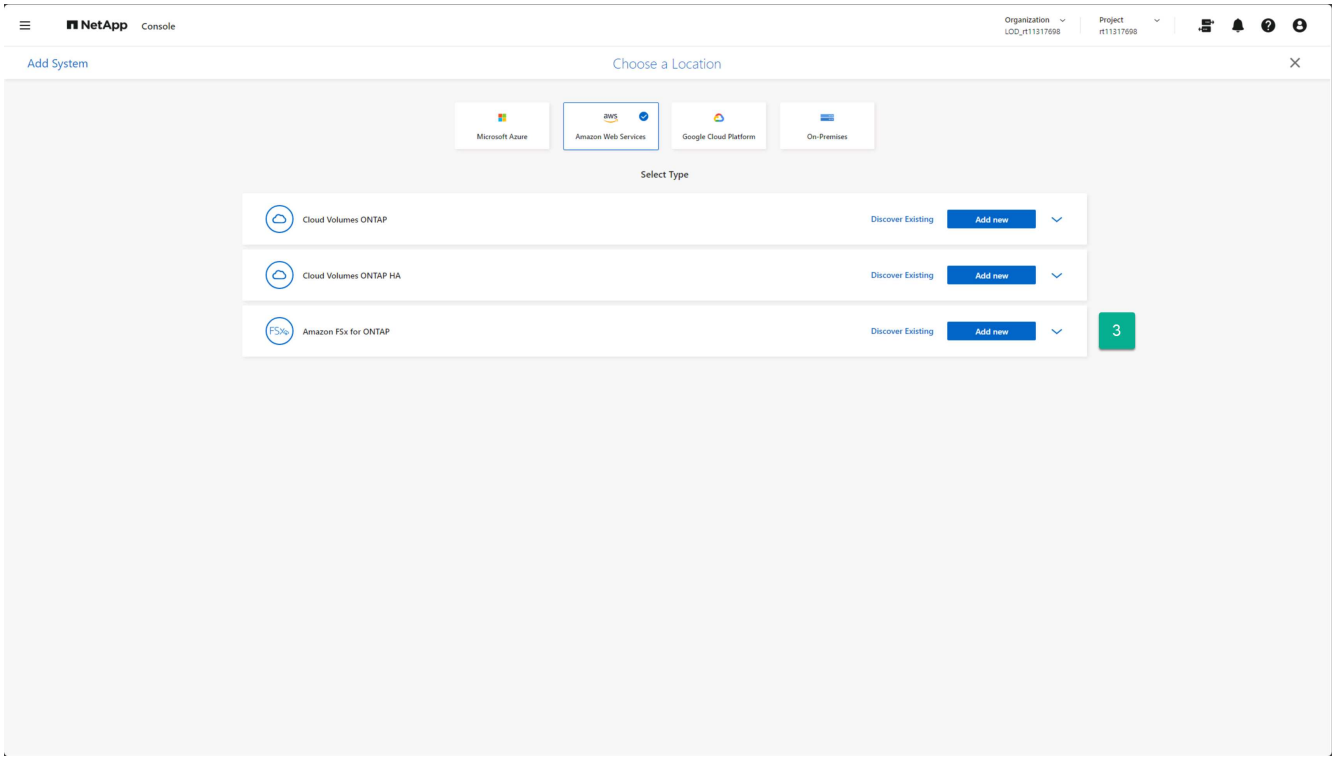
1. Dalla pagina Sistemi NetApp Console , selezionare **Aggiungi sistema**.



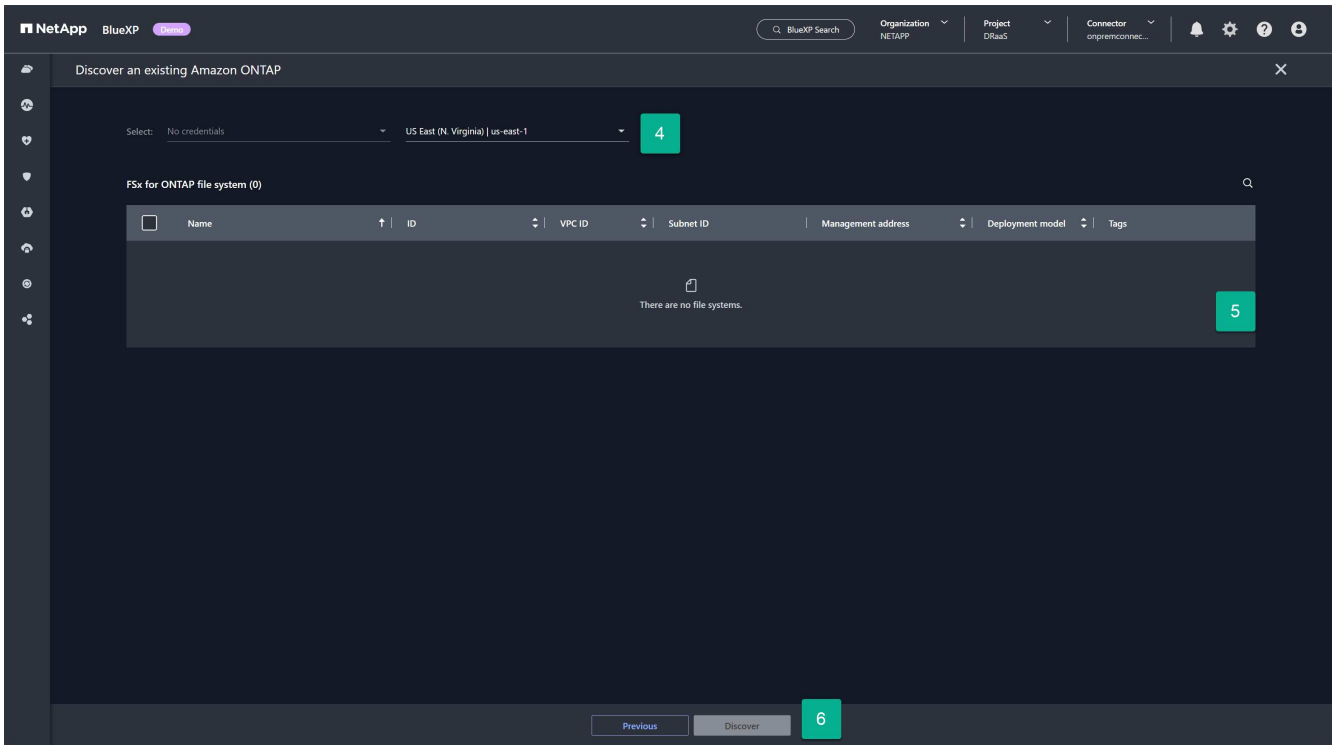
2. Nella pagina Aggiungi sistema, seleziona la scheda **Amazon Web Services**.



3. Selezionare il collegamento **Scopri esistente** sulla scheda Amazon FSx per ONTAP .



4. Selezionare le credenziali e la regione AWS che ospita l'istanza FSx for ONTAP .
5. Selezionare uno o più file system FSx for ONTAP da aggiungere.
6. Seleziona **Scopri** in fondo alla pagina.



7. Ripetere i passaggi da 1 a 6 per ogni istanza di FSx for ONTAP che ospiterà i datastore vCenter.

Aggiungi il servizio NetApp Disaster Recovery al tuo account NetApp Console per Amazon EVS

NetApp Disaster Recovery è un prodotto con licenza che deve essere acquistato prima di poter essere utilizzato. Esistono diversi tipi di licenze e diversi modi per acquistarle. Una licenza ti dà il diritto di proteggere una quantità specifica di dati per un determinato periodo di tempo.

Per ulteriori informazioni sulle licenze NetApp Disaster Recovery , vedere"Impostare la licenza per NetApp Disaster Recovery" .

Tipi di licenza

Esistono due tipi principali di licenza:

- NetApp offre un"Licenza di prova di 30 giorni" che puoi utilizzare per valutare NetApp Disaster Recovery utilizzando le tue risorse ONTAP e VMware. Questa licenza garantisce 30 giorni di utilizzo per una quantità illimitata di capacità protetta.
- Acquista una licenza di produzione se desideri una protezione DR oltre il periodo di prova di 30 giorni. Questa licenza può essere acquistata tramite i marketplace di qualsiasi partner cloud di NetApp, ma per questa guida consigliamo di acquistare la licenza marketplace per NetApp Disaster Recovery tramite Amazon AWS Marketplace. Per saperne di più sull'acquisto di una licenza tramite Amazon Marketplace, vedere"Iscriviti tramite AWS Marketplace" .

Dimensiona le tue esigenze di capacità di disaster recovery

Prima di acquistare la licenza, è necessario comprendere quanta capacità di archiviazione ONTAP è necessario proteggere. Uno dei vantaggi dell'utilizzo dello storage NetApp ONTAP è l'elevata efficienza con cui NetApp archivia i dati. Tutti i dati memorizzati in un volume ONTAP , come ad esempio un datastore VMware che ospita VM, sono archiviati in modo altamente efficiente. ONTAP utilizza di default tre tipi di efficienza di archiviazione durante la scrittura dei dati su un archivio fisico: compattazione, deduplicazione e compressione. Il risultato netto è un'efficienza di archiviazione compresa tra 1,5:1 e 4:1, a seconda del tipo di dati archiviati. Infatti, NetApp offre un "garanzia di efficienza di archiviazione" per determinati carichi di lavoro.

Ciò può essere vantaggioso perché NetApp Disaster Recovery calcola la capacità ai fini della concessione delle licenze dopo che sono state applicate tutte le efficienze di archiviazione ONTAP . Ad esempio, supponiamo di aver predisposto un datastore NFS da 100 terabyte (TiB) all'interno di vCenter per ospitare 100 VM che si desidera proteggere tramite il servizio. Inoltre, supponiamo che quando i dati vengono scritti sul volume ONTAP , le tecniche di efficienza di archiviazione applicate automaticamente comportino un consumo di soli 33 TiB da parte di tali VM (efficienza di archiviazione 3:1). NetApp Disaster Recovery deve essere concesso in licenza solo per 33 TiB, non per 100 TiB. Ciò può rappresentare un vantaggio notevole per il costo totale di proprietà della soluzione DR rispetto ad altre soluzioni DR.

Passi

1. Per determinare la quantità di dati consumata su ciascun volume che ospita un datastore VMware da proteggere, determinare il consumo di capacità su disco eseguendo il comando ONTAP CLI per ciascun volume: `volume show-space -volume < volume name > -vserver < SVM name >.`

   Per esempio:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                  Used      Used%
------------------------------      --------     ------
User Data                             163.4MB         3%
Filesystem Metadata                     172KB         0%
Inodes                                 2.93MB         0%
Snapshot Reserve                      292.9MB         5%
Total Metadata                          185KB         0%
Total Used                            459.4MB         8%
Total Physical Used                   166.4MB         3%
```

2. Notare il valore **Totale fisico utilizzato** per ciascun volume. Questa è la quantità di dati che NetApp Disaster Recovery deve proteggere ed è il valore che utilizzerai per determinare quanta capacità devi concedere in licenza.

Aggiungere siti in NetApp Disaster Recovery per Amazon EVS

Prima di poter proteggere l'infrastruttura delle VM, è necessario identificare quali cluster VMware vCenter ospitano le VM da proteggere e dove si trovano tali vCenter. Il primo passo è creare un sito che rappresenti i data center di origine e di destinazione. Un sito è un dominio di errore o un dominio di ripristino.

Devi creare quanto segue:

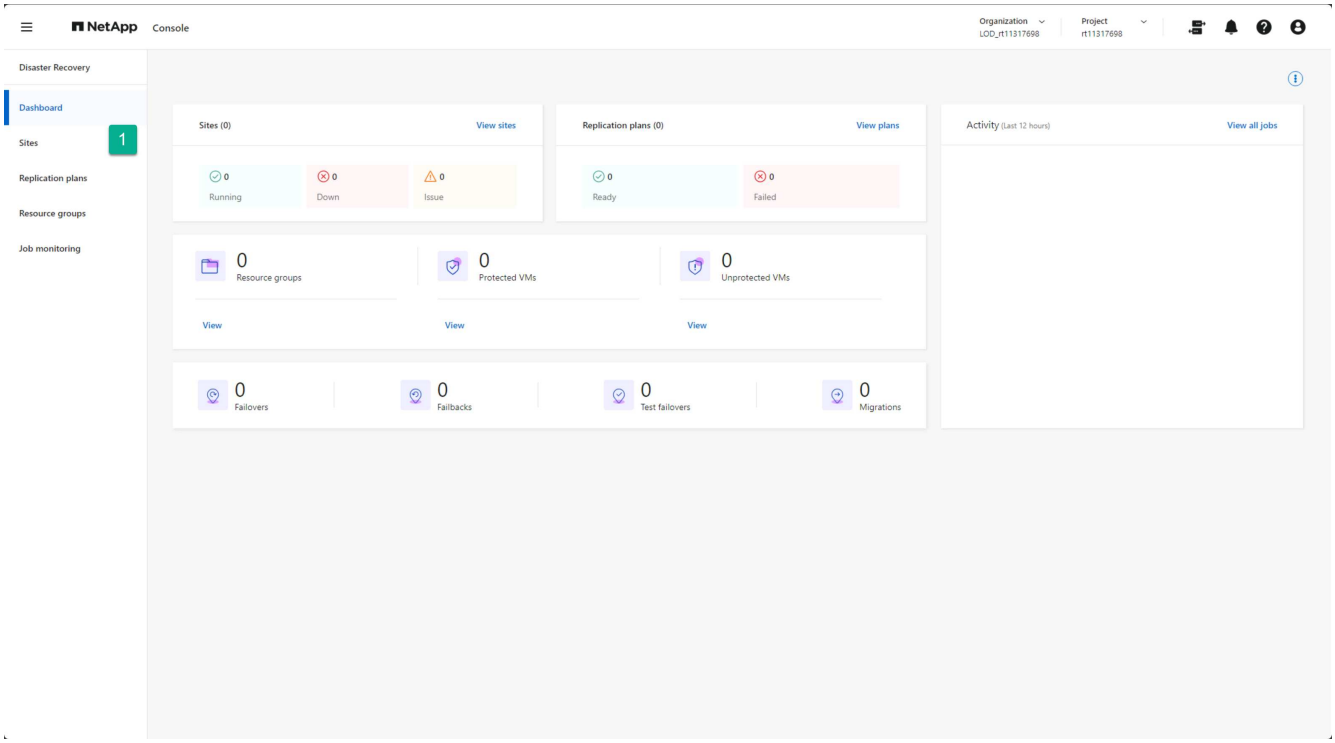
- Un sito che rappresenta ogni data center di produzione in cui risiedono i cluster vCenter di produzione
- Un sito per il tuo data center cloud Amazon EVS/ Amazon FSx for NetApp ONTAP

Crea siti on-premise

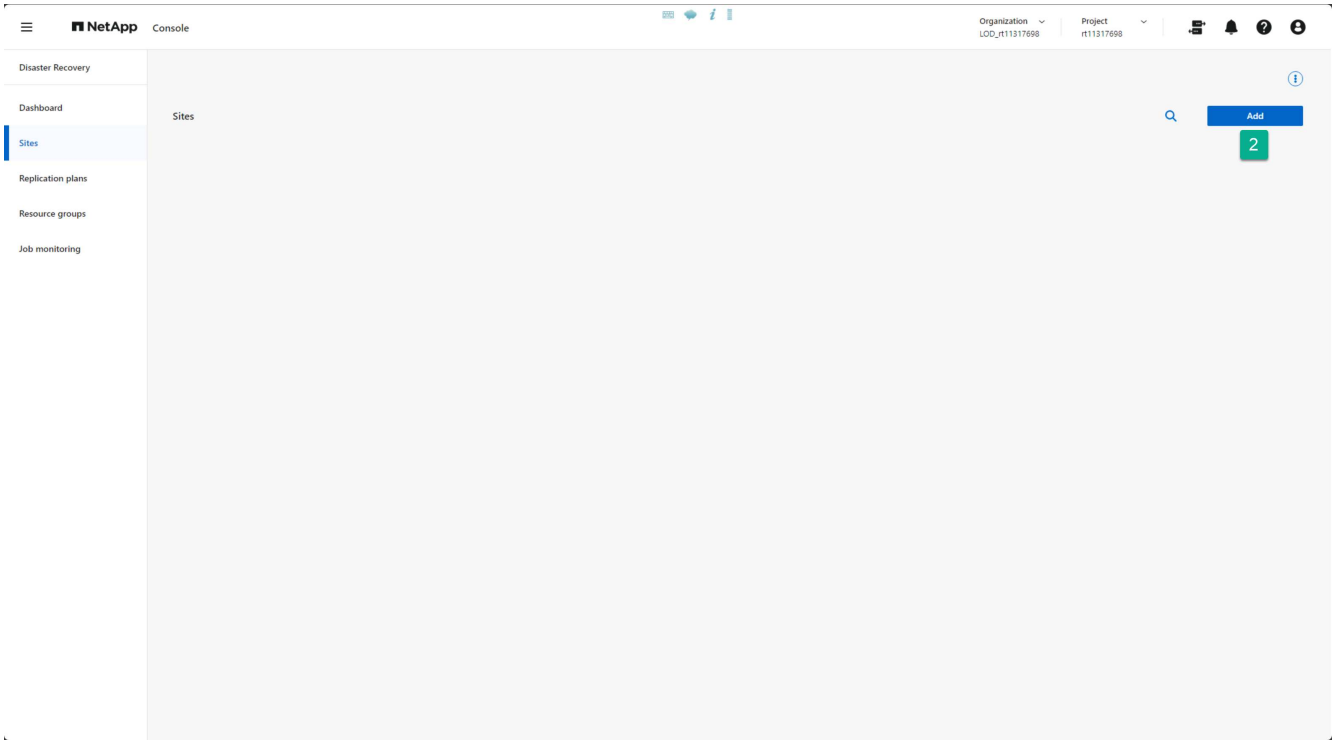
Creare un sito vCenter di produzione.

Passi

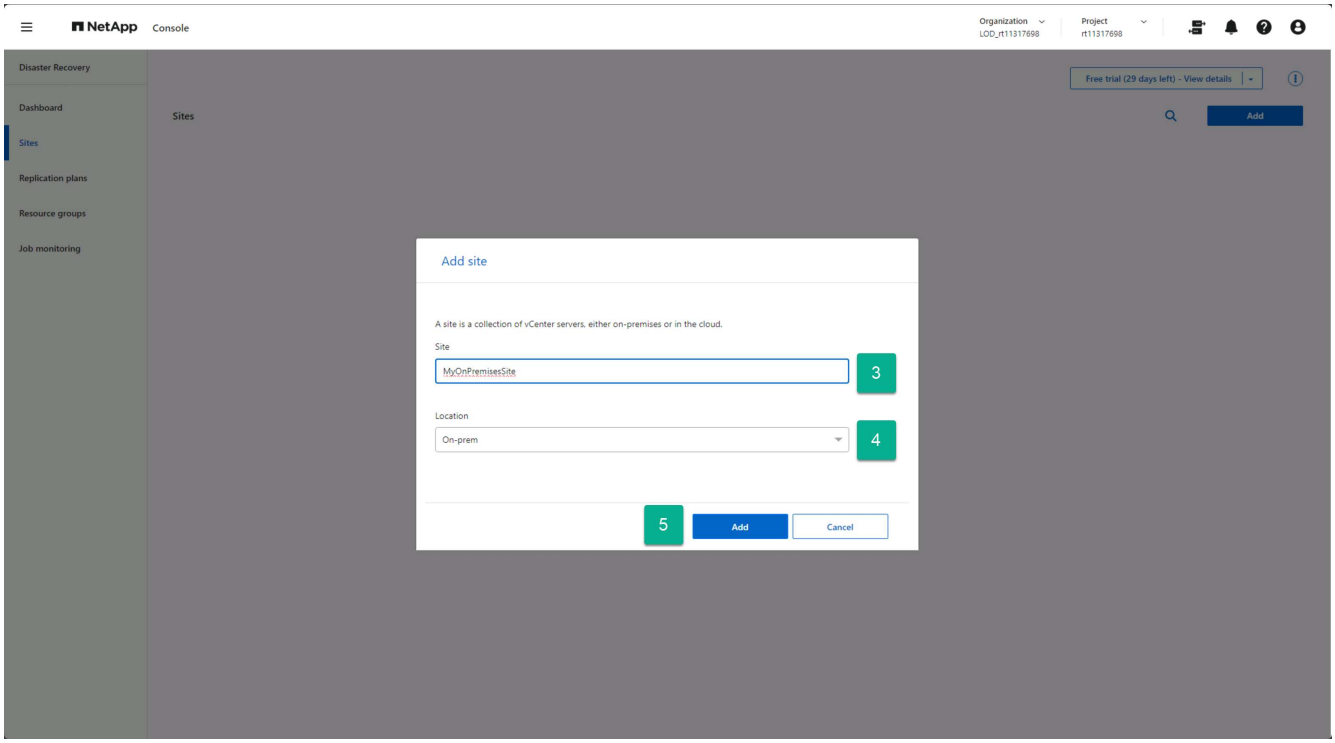
1. Dalla barra di navigazione sinistra NetApp Console , selezionare **Protezione** > **Disaster Recovery**.
2. Da qualsiasi pagina di NetApp Disaster Recovery, seleziona l'opzione **Siti**.



3. Dall'opzione Siti, seleziona **Aggiungi**.



4. Nella finestra di dialogo Aggiungi sito, immettere un nome per il sito.
5. Selezionare "In sede" come posizione.
6. Selezionare **Aggiungi**.

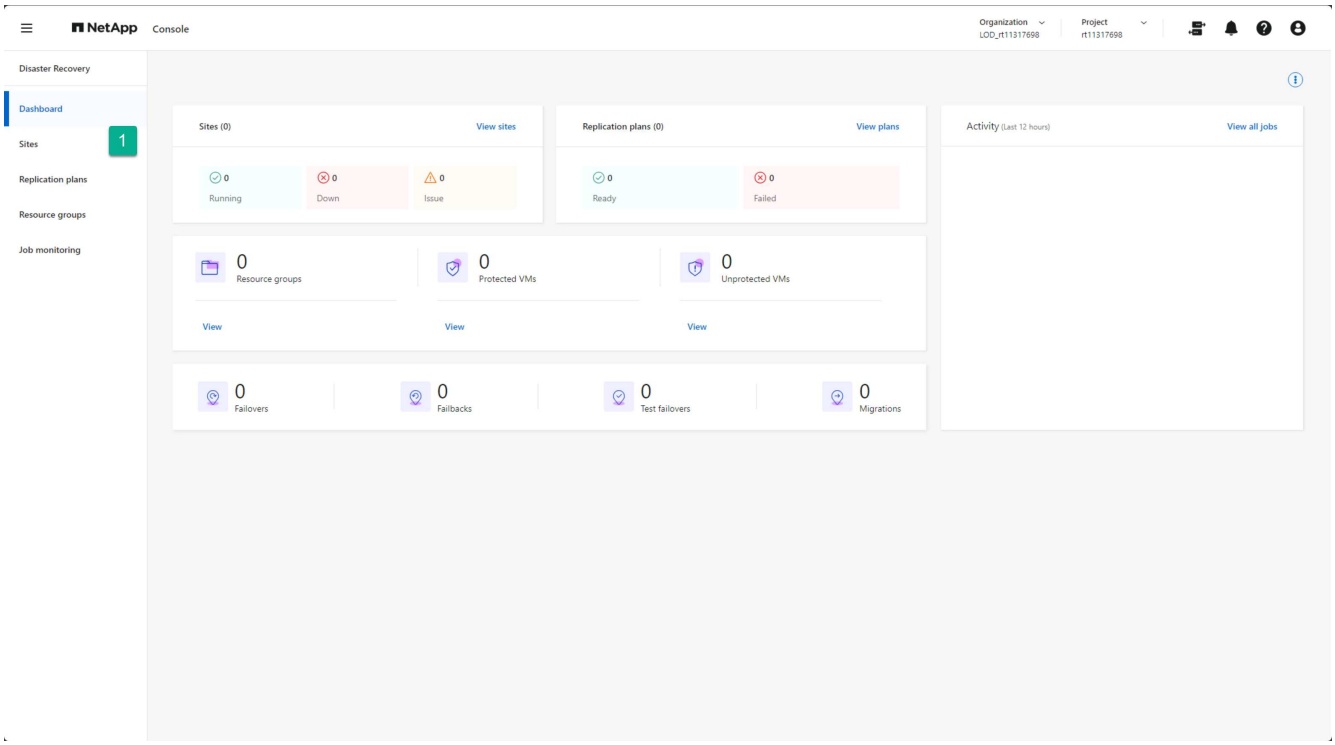


Se disponi di altri siti di produzione vCenter, puoi aggiungerli seguendo gli stessi passaggi.

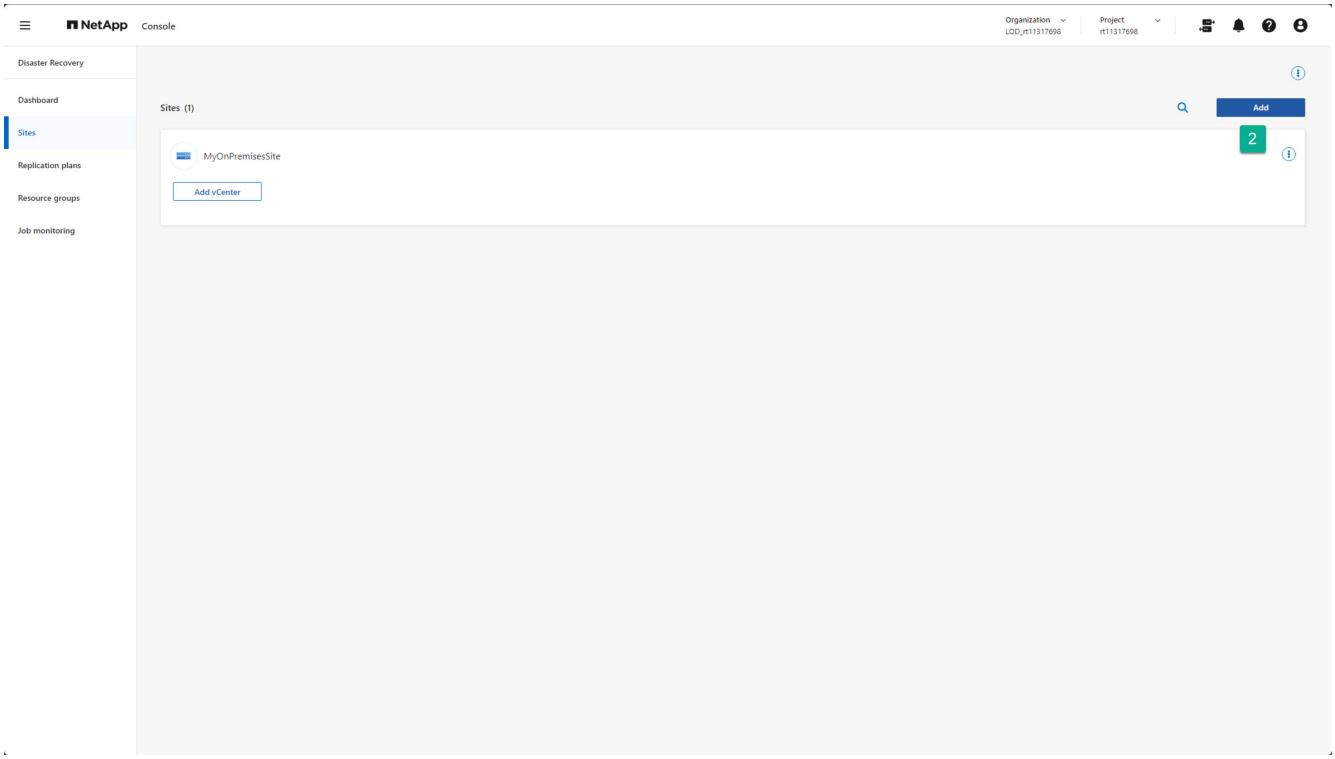
Crea siti cloud Amazon

Creare un sito DR per Amazon EVS utilizzando Amazon FSx for NetApp ONTAP .

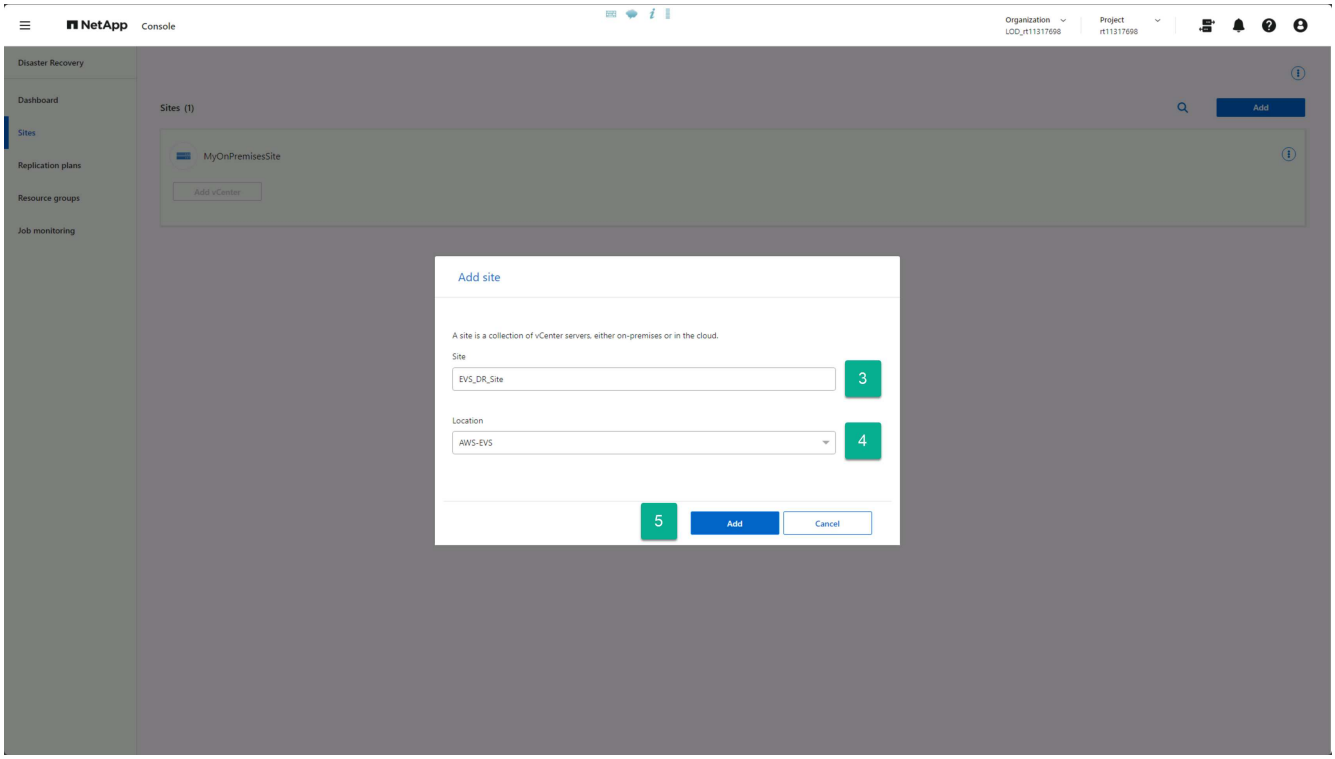
1. Da qualsiasi pagina di NetApp Disaster Recovery, seleziona l'opzione **Siti**.



2. Dall'opzione Siti, seleziona **Aggiungi**.



3. Nella finestra di dialogo Aggiungi sito, immettere un nome per il sito.
4. Selezionare "AWS-EVS" come posizione.
5. Selezionare **Aggiungi**.



Risultato

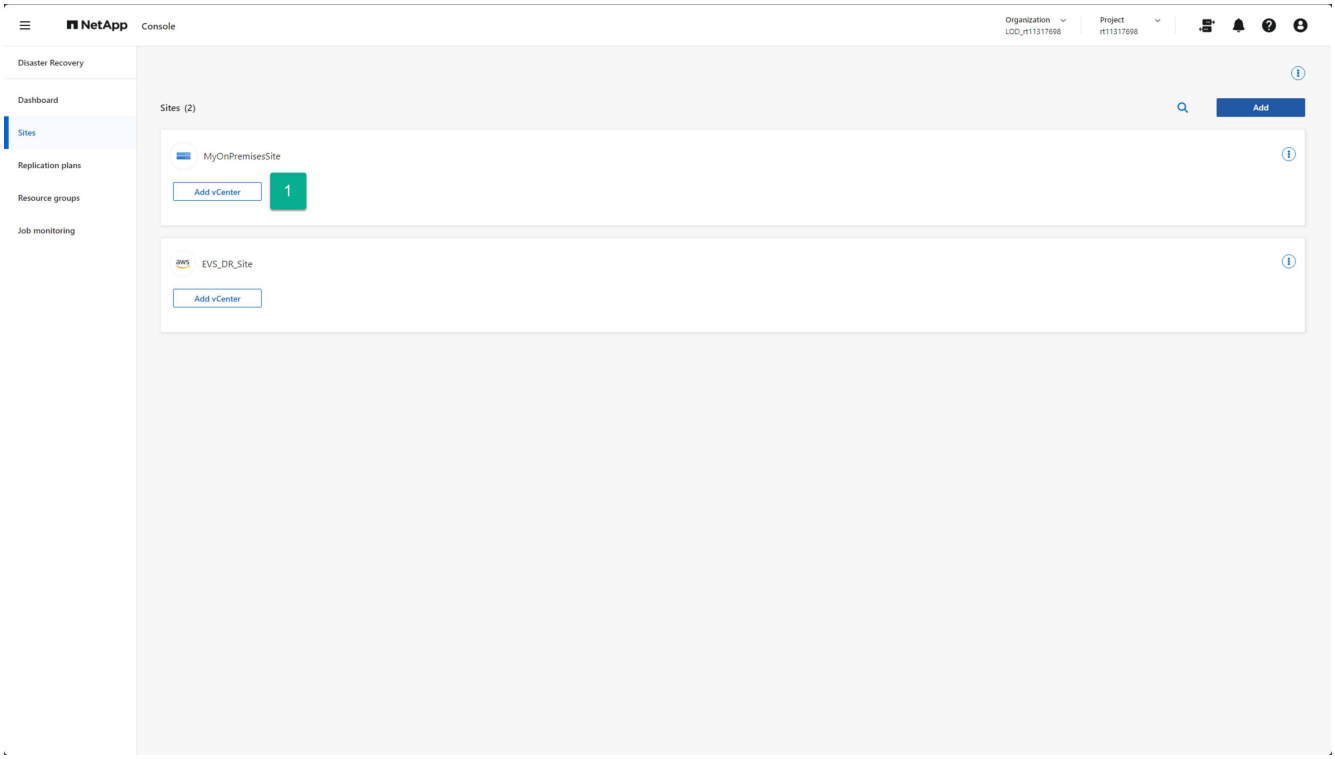
Ora hai creato un sito di produzione (sorgente) e un sito DR (destinazione).

Aggiungi cluster locali e Amazon EVS vCenter in NetApp Disaster Recovery

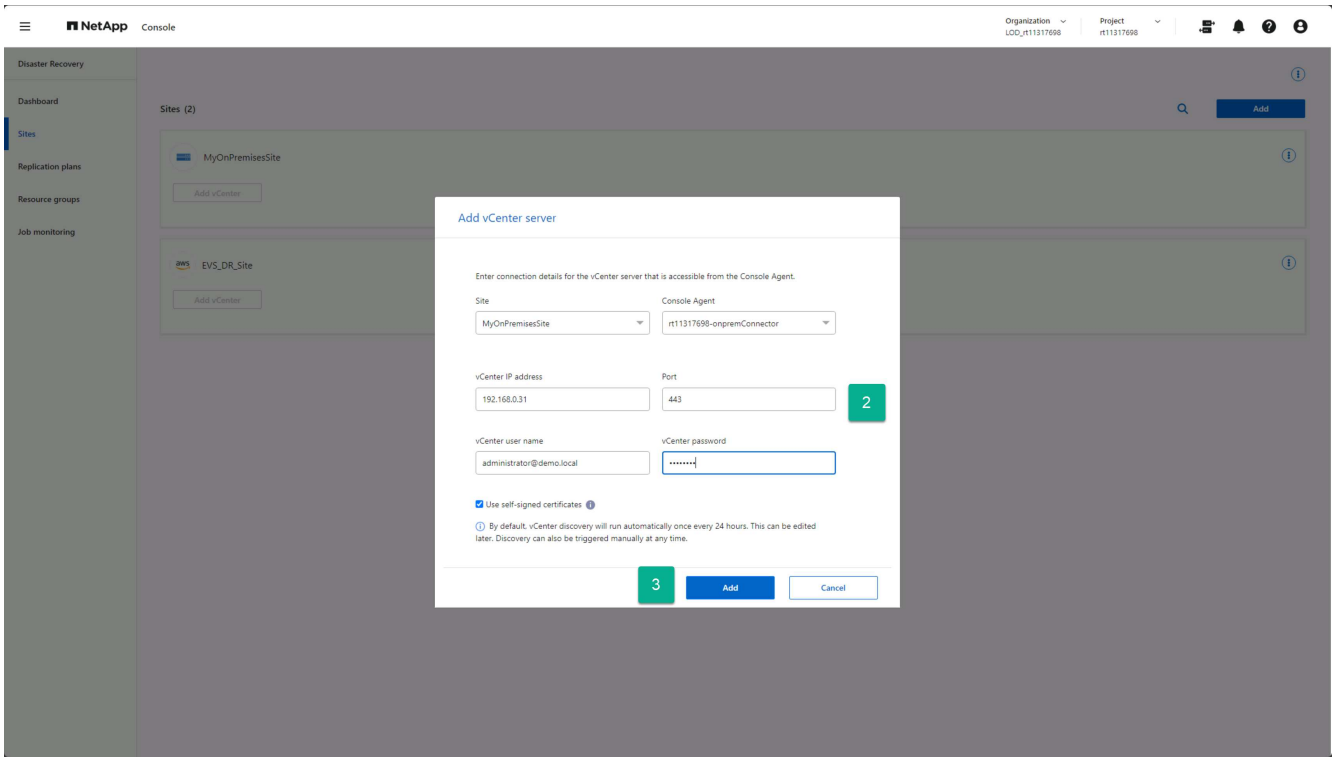
Dopo aver creato i siti, puoi aggiungere i cluster vCenter a ciascun sito in NetApp Disaster Recovery. Quando abbiamo creato ogni sito, abbiamo indicato ogni tipologia di sito. In questo modo viene indicato a NetApp Disaster Recovery quale tipo di accesso è richiesto per i vCenter ospitati in ciascun tipo di sito. Uno dei vantaggi di Amazon EVS è che non esiste una vera e propria distinzione tra un vCenter Amazon EVS e un vCenter locale. Entrambi richiedono le stesse informazioni di connessione e autenticazione.

Passaggi per aggiungere un vCenter a ciascun sito

1. Dall'opzione **Siti**, seleziona **Aggiungi vCenter** per il sito desiderato.



2. Nella finestra di dialogo Aggiungi server vCenter, seleziona o fornisci le seguenti informazioni:
   a. L'agente NetApp Console ospitato nel tuo AWS VPC.
   b. L'indirizzo IP o FQDN per il vCenter da aggiungere.
   c. Se diverso, modificare il valore della porta impostandolo sulla porta TCP utilizzata dal gestore cluster vCenter.
   d. Il nome utente vCenter per l'account creato in precedenza che verrà utilizzato da NetApp Disaster Recovery per gestire vCenter.
   e. La password vCenter per il nome utente fornito.
   f. Se la tua azienda utilizza un'autorità di certificazione (CA) esterna o vCenter Endpoint Certificate Store per accedere ai tuoi vCenter, deseleziona la casella di controllo **Usa certificati autofirmati**. Altrimenti, lasciare la casella selezionata.
3. Selezionare **Aggiungi**.



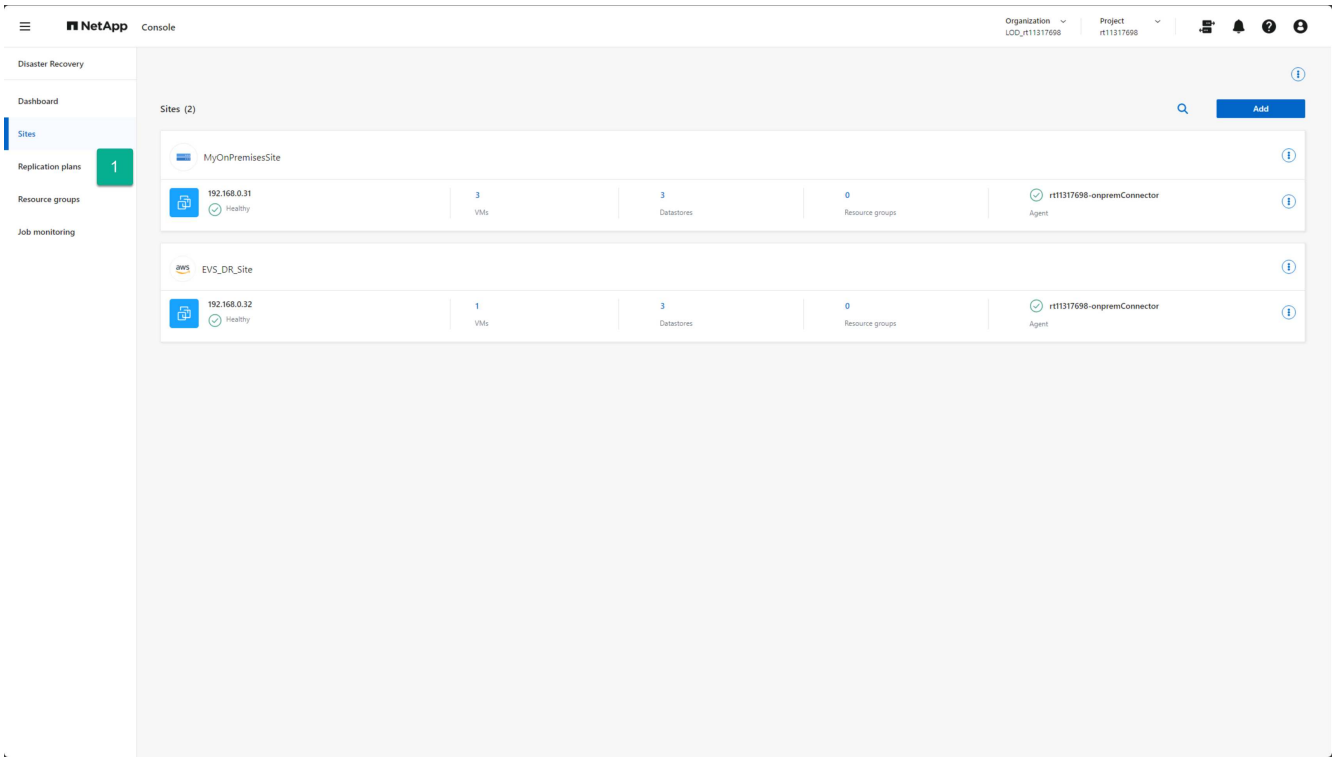
Creare piani di replicazione per Amazon EVS

Creazione di piani di replica nella panoramica NetApp Disaster Recovery

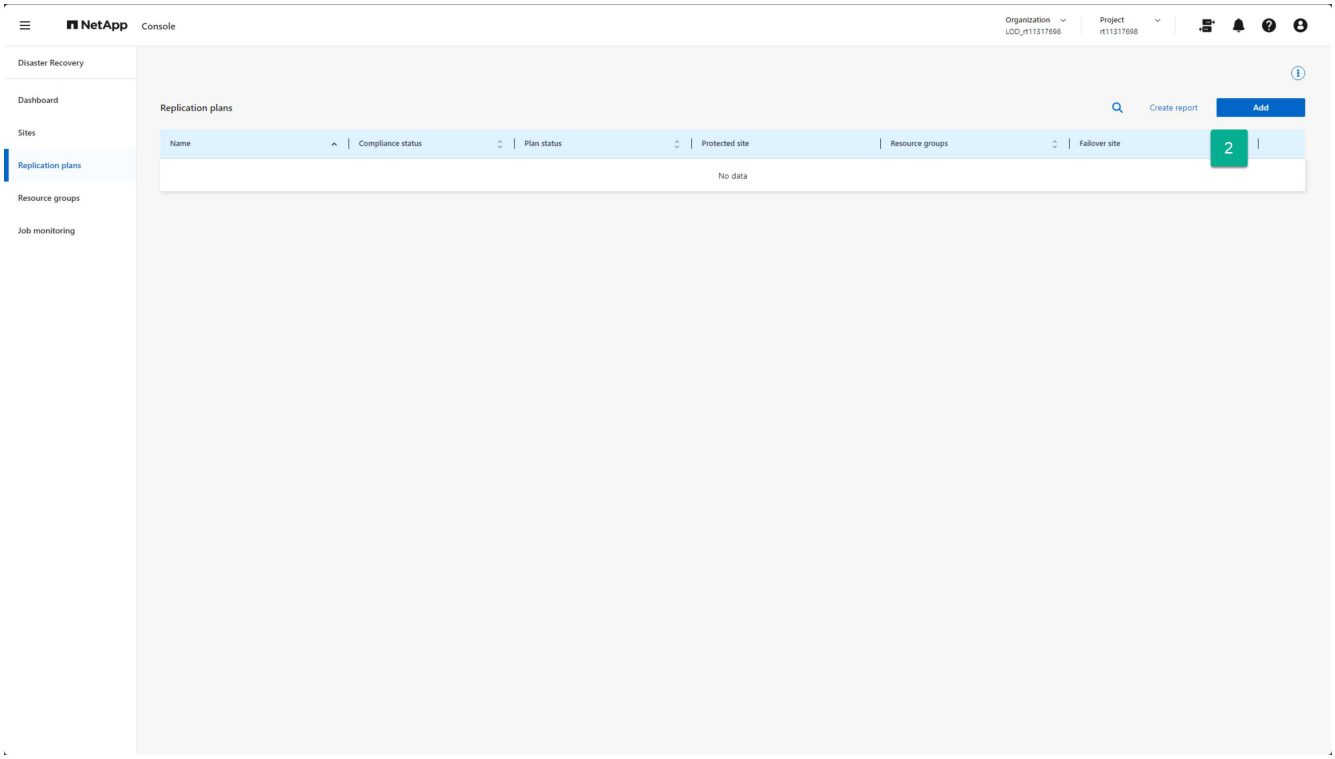
Dopo aver protetto i vCenter sul sito locale e aver configurato un sito Amazon EVS per utilizzare Amazon FSx for NetApp ONTAP come destinazione DR, è possibile creare un piano di replica (RP) per proteggere qualsiasi set di VM ospitate sul cluster vCenter all'interno del sito locale.

Per avviare il processo di creazione del piano di replicazione:

1. Da qualsiasi schermata di NetApp Disaster Recovery , selezionare l'opzione **Piani di replica**.



2. Nella pagina Piani di replica, seleziona **Aggiungi**.



Si apre la procedura guidata Crea piano di replica.

Continua con"Creazione guidata piano di replicazione Passaggio 1" .

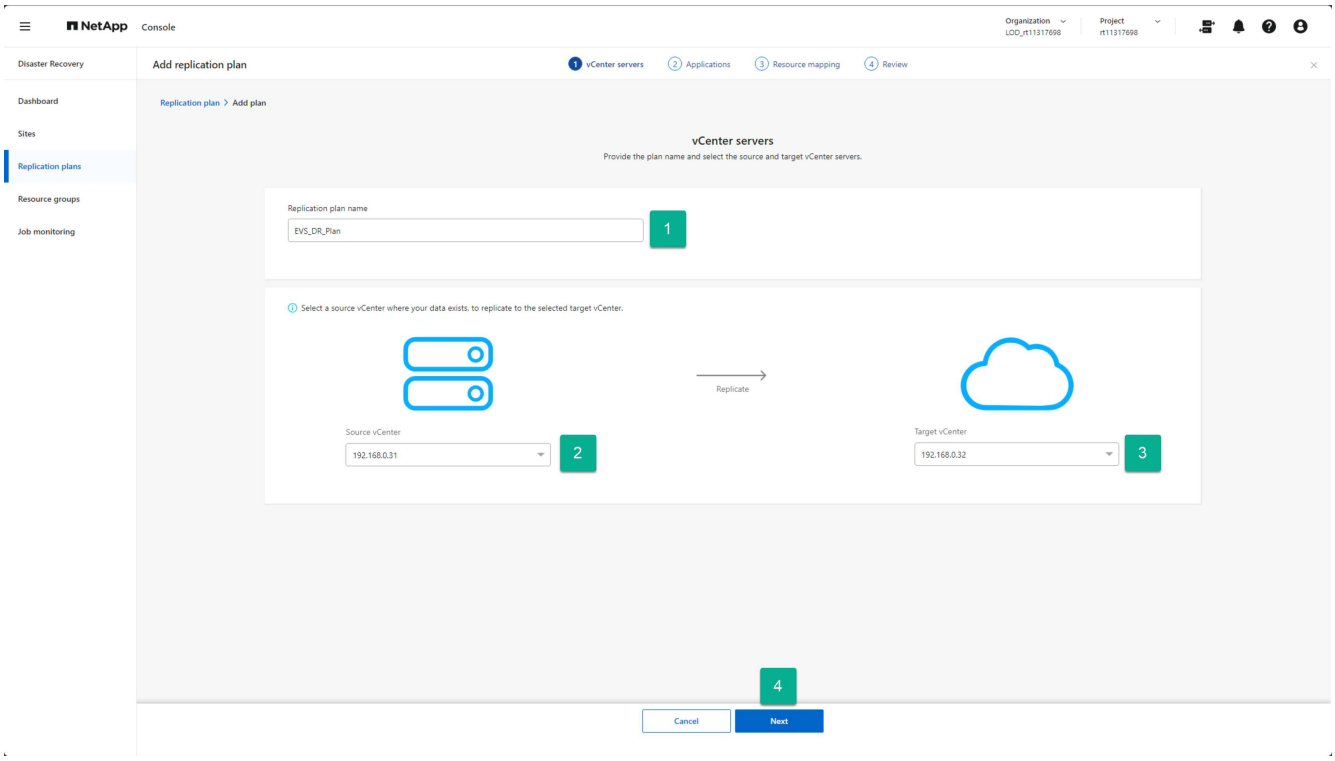
Creare un piano di replica: Passaggio 1: selezionare vCenter in NetApp Disaster Recovery

Per prima cosa, utilizzando NetApp Disaster Recovery, fornisci un nome per il piano di replica e seleziona i vCenter di origine e di destinazione per la replica.

1. Immettere un nome univoco per il piano di replicazione.

   Per i nomi dei piani di replicazione sono consentiti solo caratteri alfanumerici e caratteri di sottolineatura (_).

2. Selezionare un cluster vCenter di origine.
3. Selezionare un cluster vCenter di destinazione.
4. Selezionare **Avanti**.



Continua con"Creazione guidata piano di replicazione Passaggio 2" .

Creare un piano di replica: Passaggio 2: selezionare le risorse VM in NetApp Disaster Recovery

Selezionare le macchine virtuali da proteggere tramite NetApp Disaster Recovery.

Esistono diversi modi per selezionare le VM da proteggere:

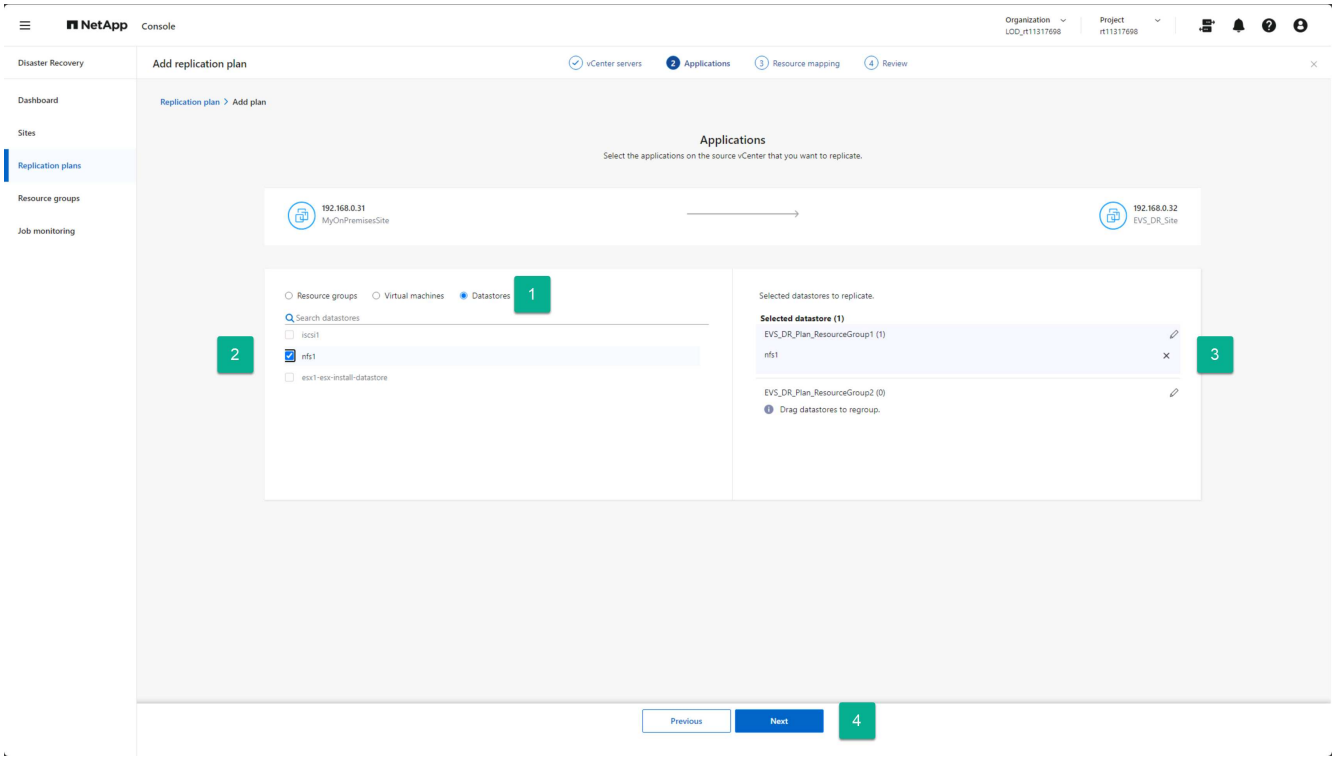
- **Seleziona singole VM**: facendo clic sul pulsante **Macchine virtuali** è possibile selezionare le singole VM da proteggere. Quando selezioni ogni VM, il servizio la aggiunge a un gruppo di risorse predefinito situato sul lato destro dello schermo.
- **Seleziona gruppi di risorse creati in precedenza**: puoi creare gruppi di risorse personalizzati in anticipo utilizzando l'opzione Gruppo di risorse dal menu NetApp Disaster Recovery . Questo non è un requisito, poiché è possibile utilizzare gli altri due metodi per creare un gruppo di risorse come parte del processo del piano di replica. Per maggiori dettagli, vedere "Creare un piano di replicazione" .

- **Seleziona interi datastore vCenter**: se hai molte VM da proteggere con questo piano di replica, potrebbe non essere altrettanto efficiente selezionare singole VM. Poiché NetApp Disaster Recovery utilizza la replica SnapMirror basata sul volume per proteggere le VM, tutte le VM residenti in un datastore verranno replicate come parte del volume. Nella maggior parte dei casi, è necessario che NetApp Disaster Recovery protegga e riavvii tutte le VM presenti nel datastore. Utilizzare questa opzione per indicare al servizio di aggiungere all'elenco delle VM protette tutte le VM ospitate su un datastore selezionato.

Per questa istruzione guidata, selezioniamo l'intero datastore vCenter.

Passaggi per accedere a questa pagina

1. Dalla pagina **Piano di replicazione**, passare alla sezione **Applicazioni**.
2. Esaminare le informazioni nella pagina **Applicazioni** che si apre.



Passaggi per selezionare il/i datastore/i:

1. Selezionare **Datastore**.
2. Seleziona le caselle di controllo accanto a ciascun datastore che desideri proteggere.
3. (Facoltativamente) Rinominare il gruppo di risorse con un nome appropriato selezionando l'icona della matita accanto al nome del gruppo di risorse.
4. Selezionare **Avanti**.

Continua con"Creazione guidata piano di replicazione Passaggio 3" .

Creare un piano di replicazione: Passaggio 3 - Mappare le risorse in NetApp Disaster Recovery

Dopo aver ottenuto un elenco delle VM che si desidera proteggere tramite NetApp Disaster Recovery, fornire le informazioni di mapping del failover e di configurazione della VM da utilizzare durante un failover.

È necessario mappare quattro tipi principali di informazioni:

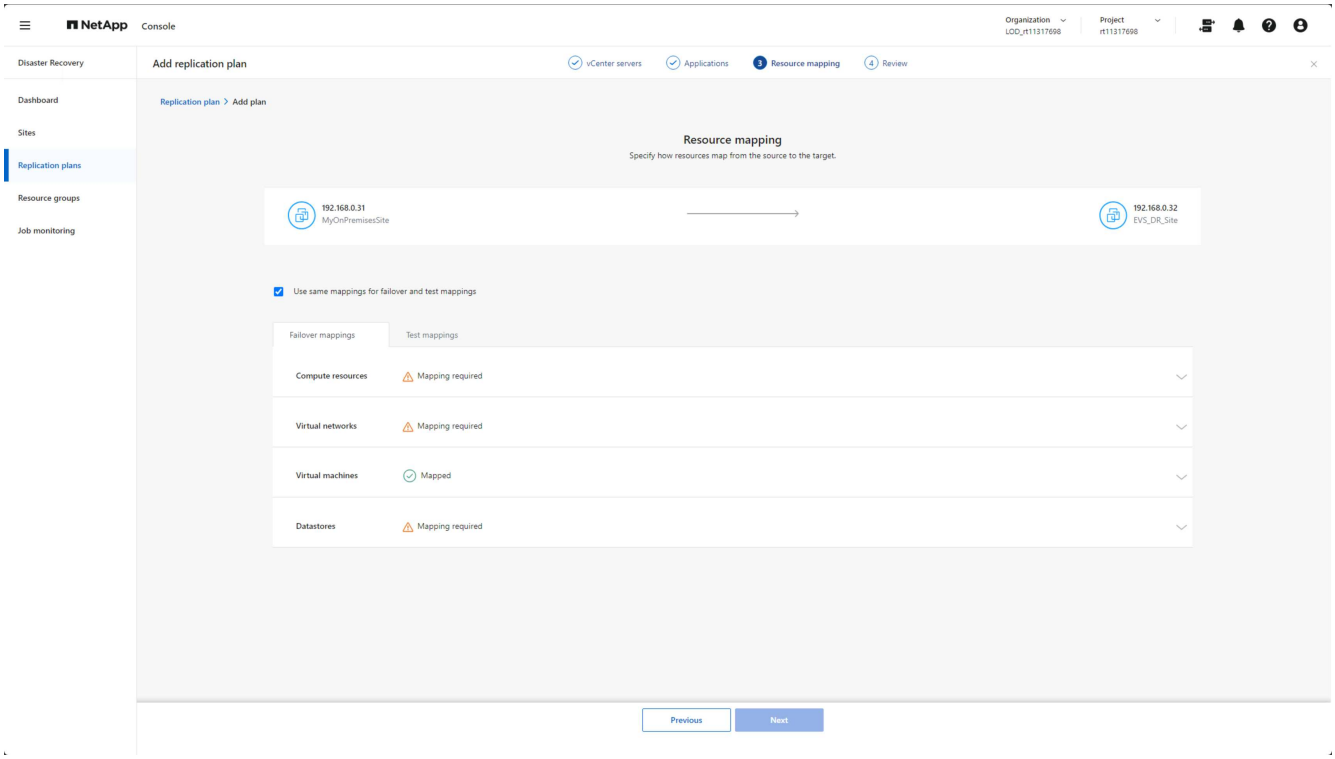
- Risorse di calcolo
- Reti virtuali
- Riconfigurazione della VM
- Mappatura del datastore

Ogni VM richiede i primi tre tipi di informazioni. La mappatura del datastore è necessaria per ogni datastore che ospita le VM da proteggere.

- Le sezioni con l'icona di attenzione ( ) richiedono di fornire informazioni sulla mappatura.
- La sezione contrassegnata con l'icona di spunta ( ) sono stati mappati o hanno mappature predefinite. Esaminateli per assicurarvi che la configurazione attuale soddisfi i vostri requisiti.

Passaggi per accedere a questa pagina

1. Dalla pagina **Piano di replicazione**, passare alla sezione **Mappatura delle risorse**.
2. Esaminare le informazioni nella pagina **Mappatura delle risorse** che si apre.



3. Per aprire ciascuna categoria di mappature richiesta, selezionare la freccia rivolta verso il basso (**v**) accanto alla sezione.

Mappatura delle risorse di calcolo

Poiché un sito potrebbe ospitare più data center virtuali e più cluster vCenter, è necessario identificare su quale cluster vCenter ripristinare le VM in caso di failover.

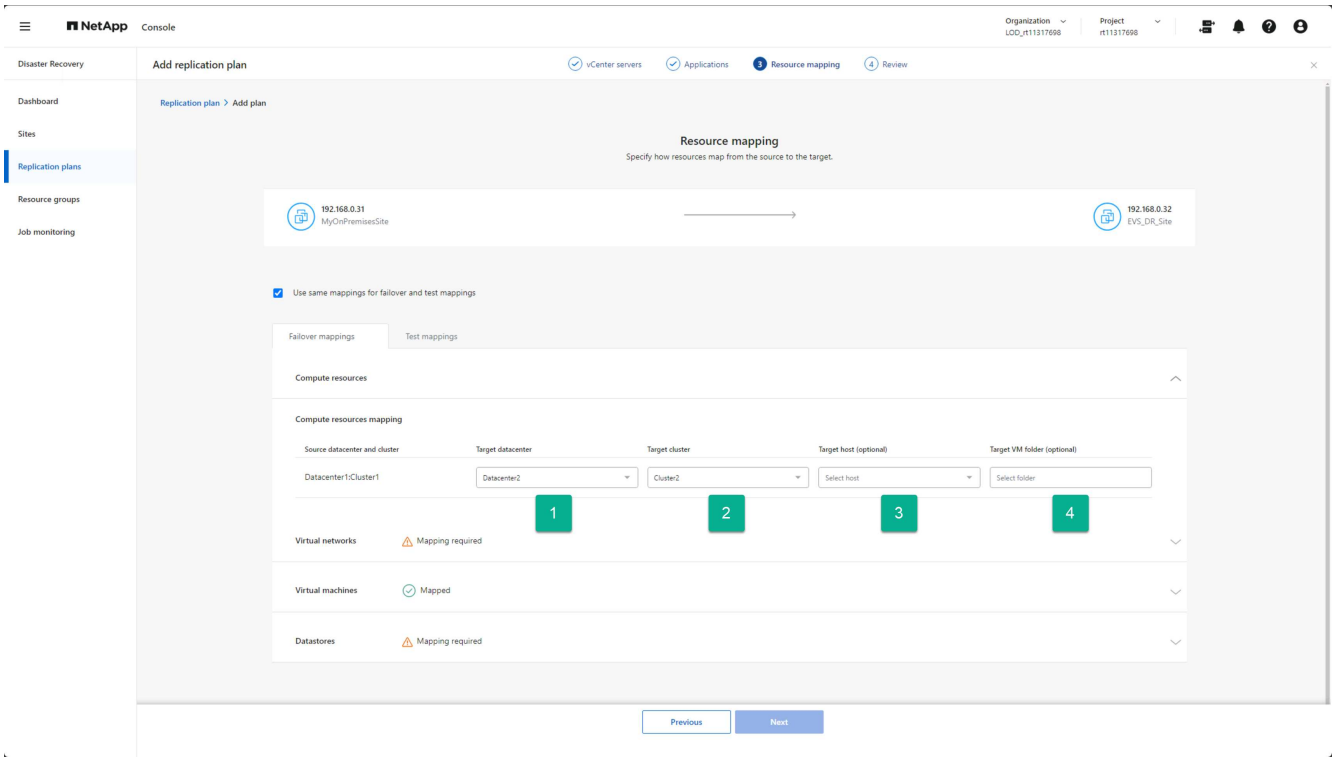
Passaggi per mappare le risorse di calcolo

1. Selezionare il data center virtuale dall'elenco dei data center presenti nel sito DR.
2. Selezionare il cluster che ospiterà i datastore e le VM dall'elenco dei cluster all'interno del data center virtuale selezionato.
3. (Facoltativo) Selezionare un host di destinazione nel cluster di destinazione.

   Questo passaggio non è necessario perché NetApp Disaster Recovery seleziona il primo host aggiunto al cluster in vCenter. A quel punto, le VM continuano a essere eseguite su quell'host ESXi oppure VMware DRS sposta la VM su un host ESXi diverso, a seconda delle necessità e in base alle regole DRS configurate.

4. (Facoltativo) Fornire il nome di una cartella vCenter di livello superiore in cui collocare le registrazioni delle VM.

   Questa operazione è necessaria per le tue esigenze organizzative e non è obbligatoria.

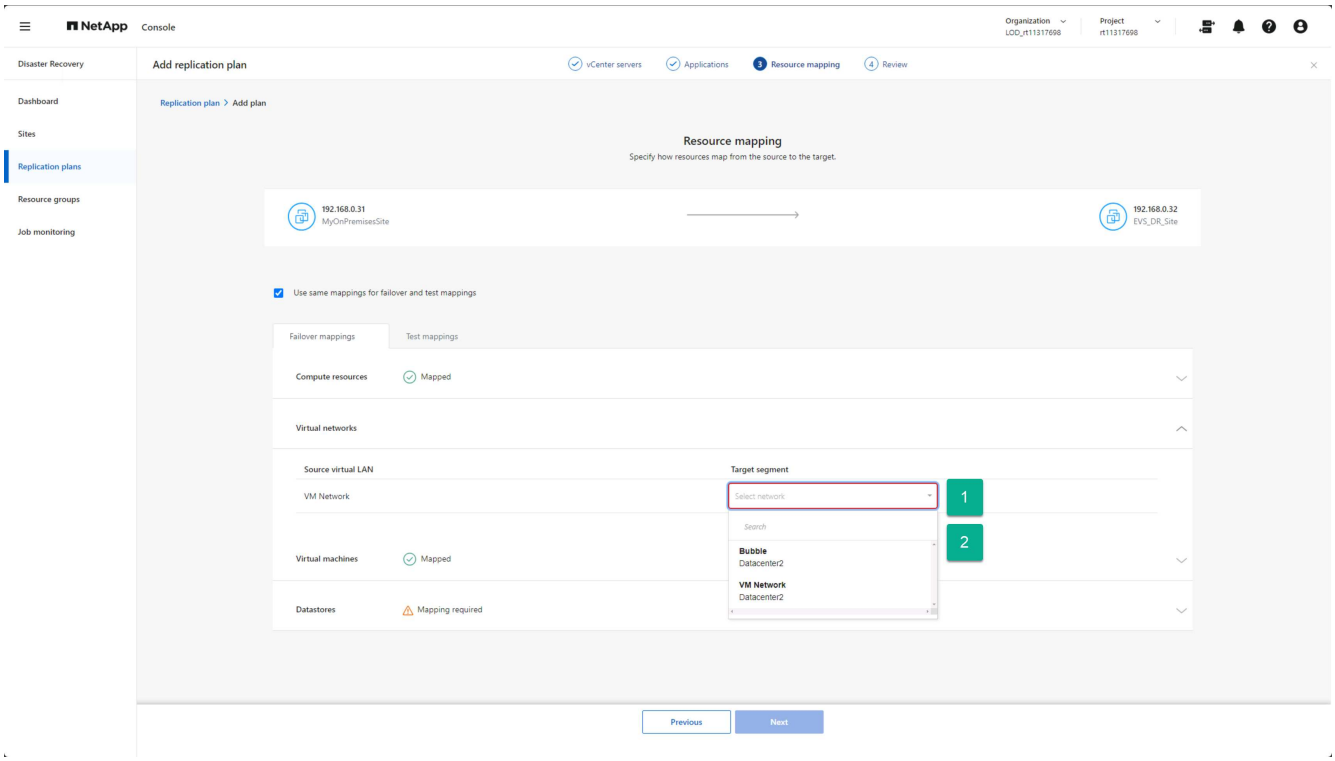


Mappare le risorse di rete virtuale

Ogni VM può avere una o più schede di rete virtuali connesse a reti virtuali all'interno dell'infrastruttura di rete vCenter. Per garantire che ogni VM sia correttamente connessa alle reti desiderate al riavvio nel sito DR, identificare a quali reti virtuali del sito DR connettere queste VM. Per fare ciò, mappare ogni rete virtuale nel sito locale a una rete associata nel sito DR.

Seleziona la rete virtuale di destinazione su cui mappare ciascuna rete virtuale di origine

1. Selezionare il segmento Target dall'elenco a discesa.
2. Ripetere il passaggio precedente per ogni rete virtuale di origine elencata.



Definire le opzioni per la riconfigurazione della VM durante il failover

Potrebbero essere necessarie modifiche per ciascuna VM affinché funzioni correttamente nel sito DR vCenter. La sezione Macchine virtuali consente di apportare le modifiche necessarie.

Per impostazione predefinita, NetApp Disaster Recovery utilizza per ogni macchina virtuale le stesse impostazioni utilizzate nel sito locale di origine. Ciò presuppone che le VM utilizzino lo stesso indirizzo IP, la stessa CPU virtuale e la stessa configurazione DRAM virtuale.

Riconfigurazione della rete

I tipi di indirizzo IP supportati sono statico e DHCP. Per gli indirizzi IP statici, sono disponibili le seguenti impostazioni IP di destinazione:

- **Uguale alla sorgente**: come suggerisce il nome, il servizio utilizza sulla VM di destinazione lo stesso indirizzo IP utilizzato sulla VM nel sito di origine. Per fare ciò, è necessario configurare le reti virtuali mappate nel passaggio precedente con le stesse impostazioni di subnet.
- **Diverso dall'origine**: il servizio fornisce un set di campi di indirizzo IP per ogni VM che devono essere configurati per la subnet appropriata utilizzata sulla rete virtuale di destinazione, mappata nella sezione precedente. Per ogni VM è necessario fornire un indirizzo IP, una subnet mask, un DNS e i valori del gateway predefinito. Facoltativamente, utilizzare le stesse impostazioni di subnet mask, DNS e gateway per tutte le VM per semplificare il processo quando tutte le VM si collegano alla stessa subnet.
- **Mappatura subnet**: questa opzione riconfigura l'indirizzo IP di ogni VM in base alla configurazione CIDR della rete virtuale di destinazione. Per utilizzare questa funzionalità, assicurarsi che ogni rete virtuale di vCenter disponga di un'impostazione CIDR definita all'interno del servizio, come modificato nelle informazioni di vCenter nella pagina Siti.

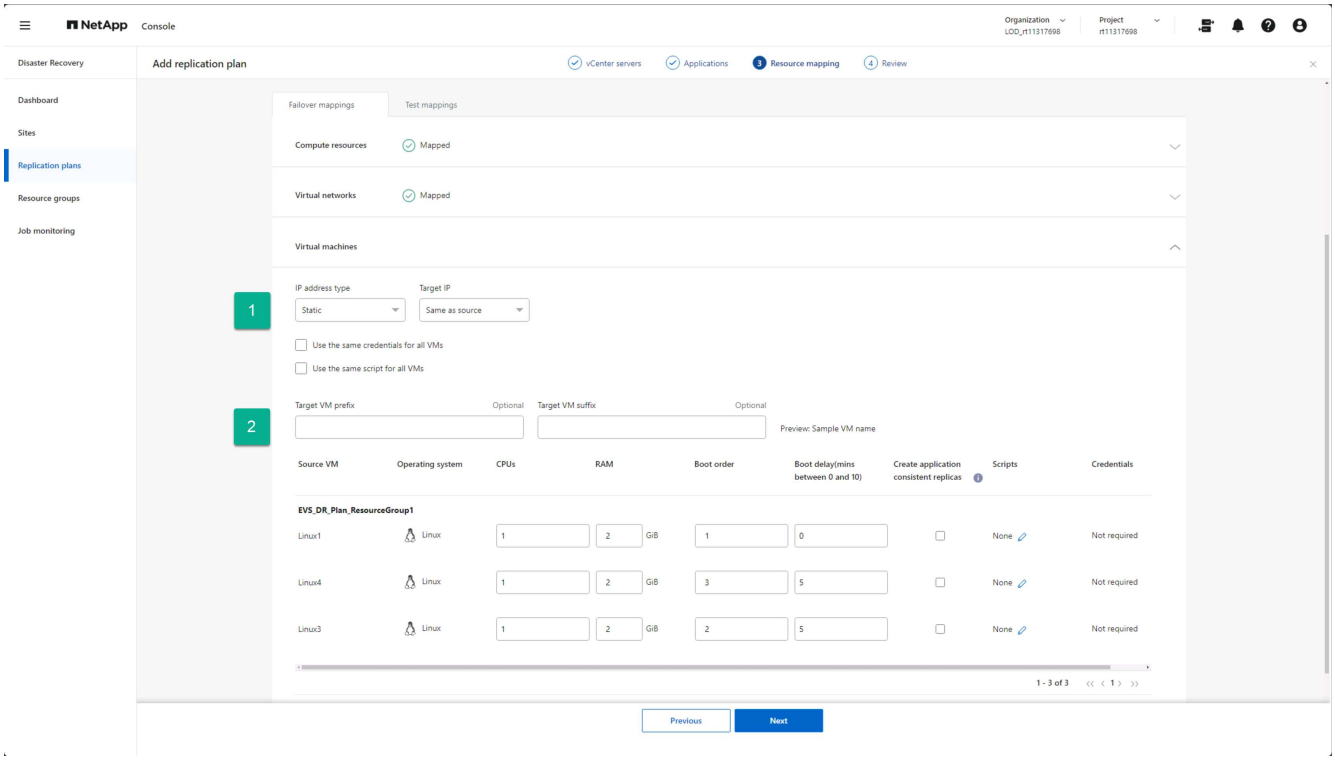
Dopo aver configurato le subnet, il mapping delle subnet utilizza lo stesso componente unità dell'indirizzo IP sia per la configurazione della VM di origine che di destinazione, ma sostituisce il componente subnet dell'indirizzo IP in base alle informazioni CIDR fornite. Questa funzionalità richiede inoltre che sia la rete

virtuale di origine che quella di destinazione abbiano la stessa classe di indirizzo IP (la `/xx` componente del CIDR). Ciò garantisce che nel sito di destinazione siano disponibili indirizzi IP sufficienti per ospitare tutte le VM protette.

Per questa configurazione EVS, presumiamo che le configurazioni IP di origine e di destinazione siano le stesse e non richiedano alcuna riconfigurazione aggiuntiva.

Apportare modifiche alla riconfigurazione delle impostazioni di rete

1. Selezionare il tipo di indirizzamento IP da utilizzare per le VM sottoposte a failover.
2. (Facoltativo) Fornire uno schema di ridenominazione delle VM per le VM riavviate specificando un valore di prefisso e suffisso facoltativo.

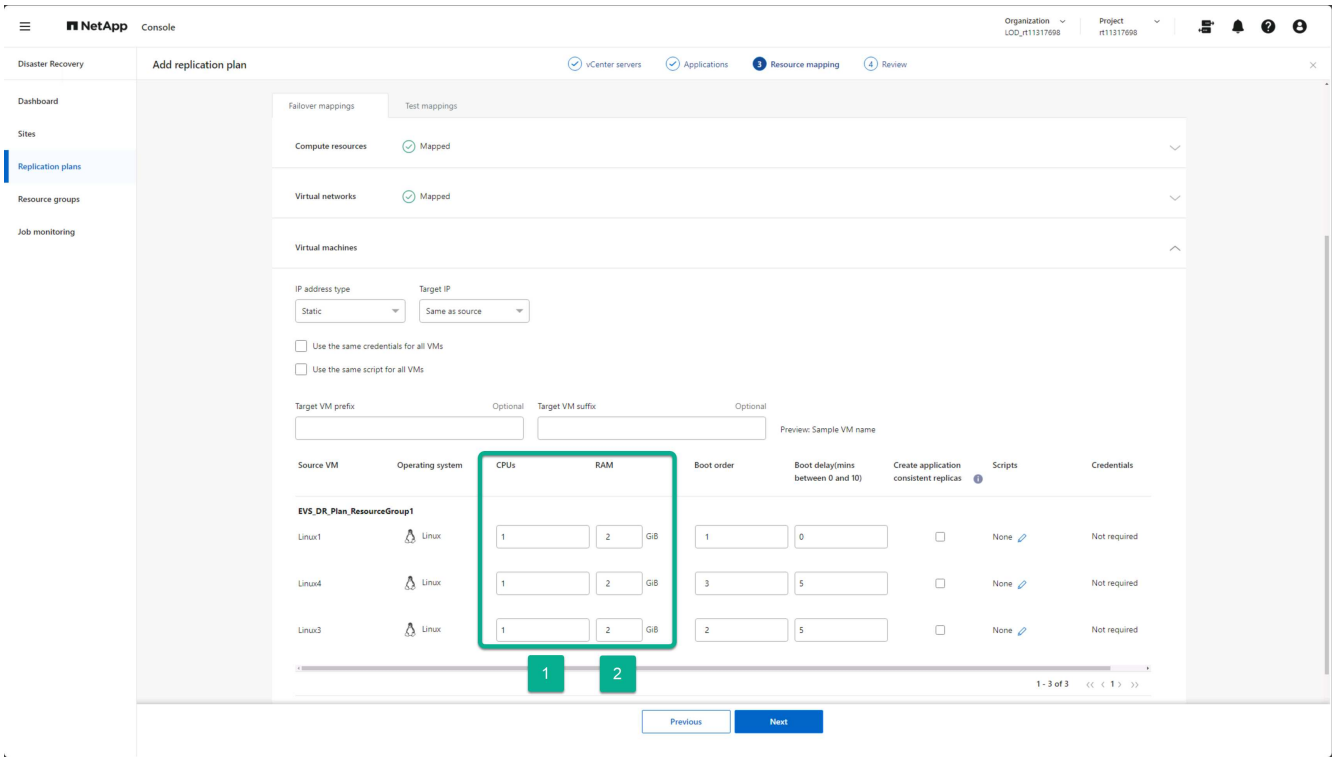


Riconfigurazione delle risorse di elaborazione della VM

Sono disponibili diverse opzioni per riconfigurare le risorse di elaborazione della VM. NetApp Disaster Recovery supporta la modifica del numero di CPU virtuali, della quantità di DRAM virtuale e del nome della VM.

Specificare eventuali modifiche alla configurazione della VM

1. (Facoltativo) Modificare il numero di CPU virtuali che ogni VM deve utilizzare. Questa operazione potrebbe essere necessaria se gli host del cluster vCenter DR non dispongono di tanti core CPU quanti ne ha il cluster vCenter di origine.
2. (Facoltativo) Modificare la quantità di DRAM virtuale che ogni VM deve utilizzare. Questa operazione potrebbe essere necessaria se gli host del cluster vCenter DR non dispongono della stessa quantità di DRAM fisica degli host del cluster vCenter di origine.

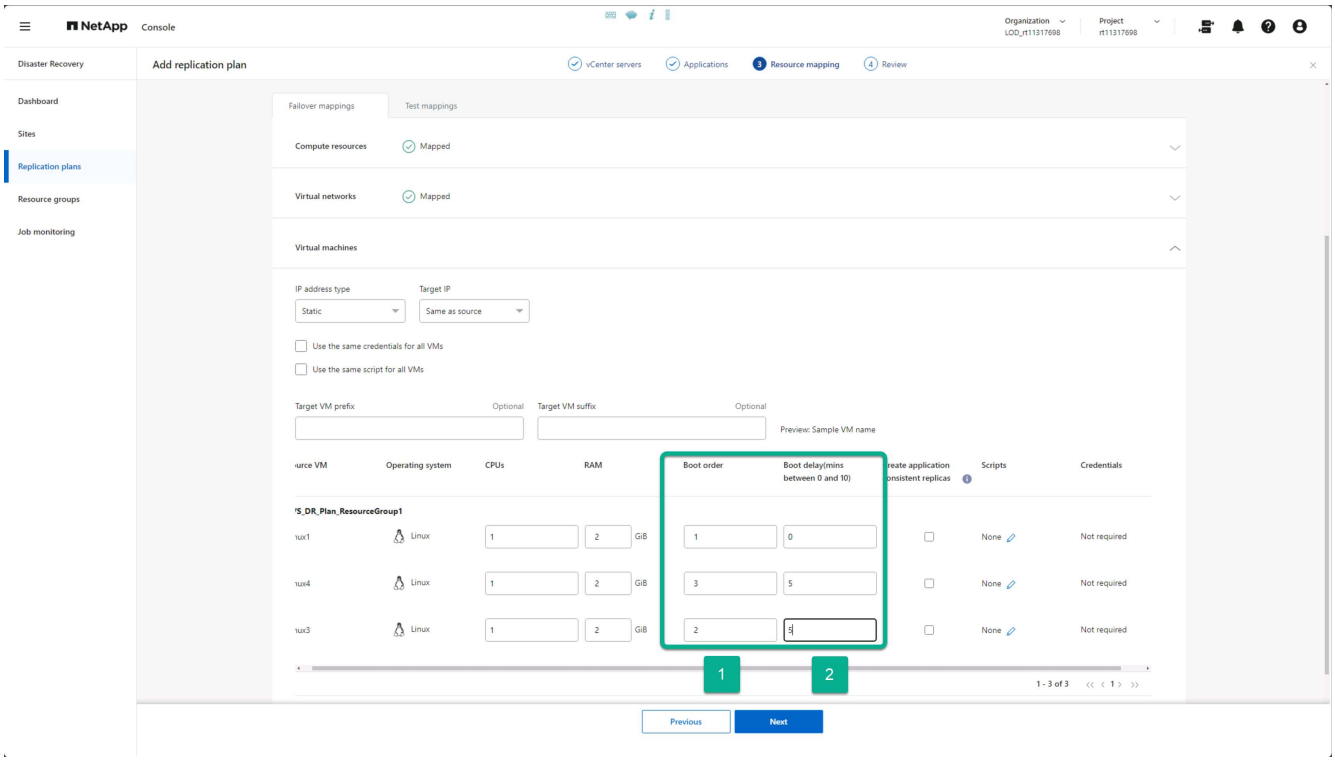


Ordine di avvio

NetApp Disaster Recovery supporta il riavvio ordinato delle VM in base a un campo di ordine di avvio. Il campo Ordine di avvio indica come vengono avviate le VM in ciascun gruppo di risorse. Le VM con lo stesso valore nel campo Ordine di avvio vengono avviate in parallelo.

Modificare le impostazioni dell'ordine di avvio

1. (Facoltativo) Modifica l'ordine in cui desideri che le tue VM vengano riavviate. Questo campo accetta qualsiasi valore numerico. NetApp Disaster Recovery tenta di riavviare in parallelo le VM che hanno lo stesso valore numerico.
2. (Facoltativo) Specificare un ritardo da utilizzare tra ogni riavvio della VM. Il tempo viene inserito dopo il completamento del riavvio di questa VM e prima delle VM con il numero di ordine di avvio successivo più alto. Questo numero è espresso in minuti.



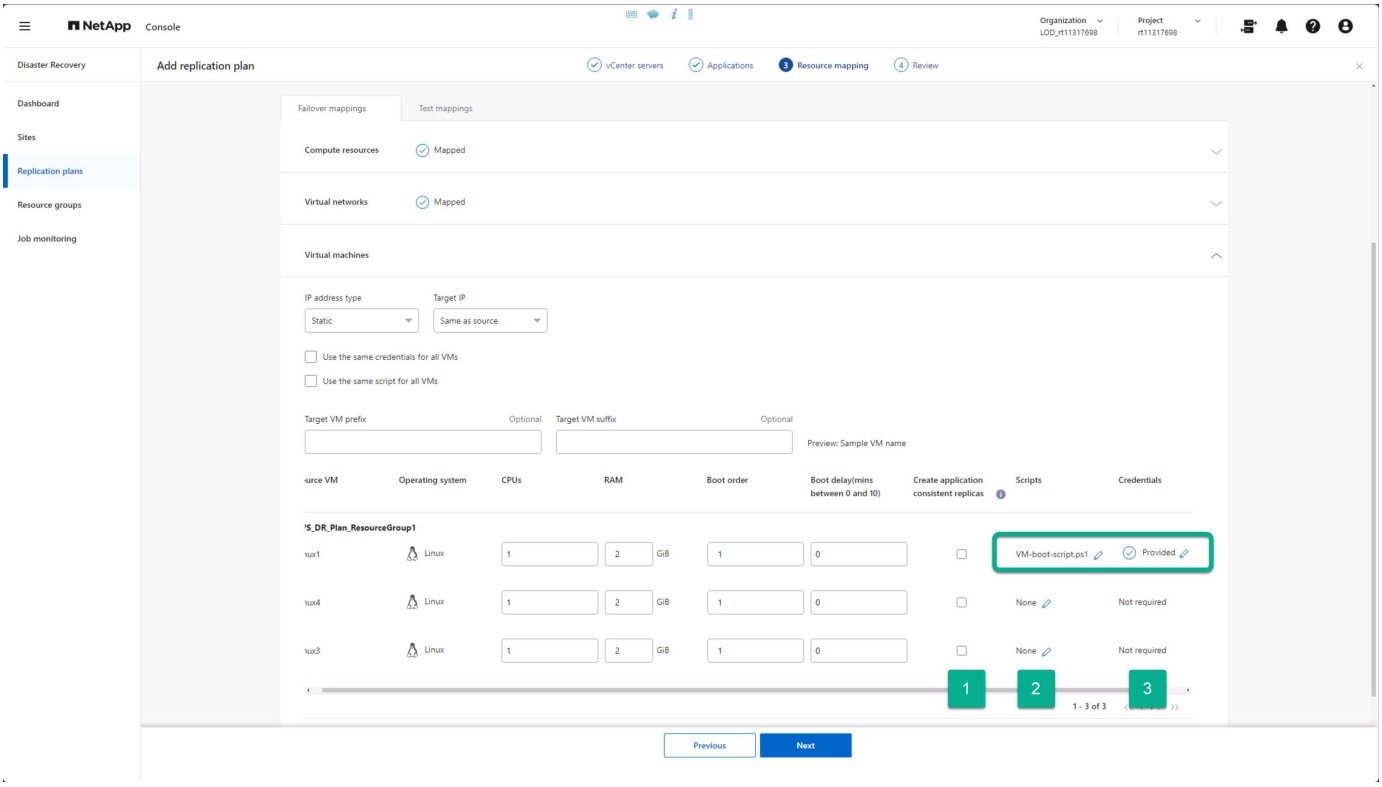
Operazioni personalizzate del sistema operativo guest

NetApp Disaster Recovery supporta l'esecuzione di alcune operazioni del sistema operativo guest per ogni VM:

- NetApp Disaster Recovery può eseguire backup coerenti con l'applicazione delle VM che eseguono database Oracle e database Microsoft SQL Server.
- NetApp Disaster Recovery può eseguire script personalizzati adatti al sistema operativo guest per ogni VM. Per eseguire tali script sono necessarie credenziali utente accettabili per il sistema operativo guest, con ampi privilegi per eseguire le operazioni elencate nello script.

Modificare le operazioni personalizzate del sistema operativo guest di ogni VM

1. (Facoltativo) Selezionare la casella di controllo **Crea repliche coerenti con l'applicazione** se la VM ospita un database Oracle o SQL Server.
2. (Facoltativo) Per eseguire azioni personalizzate all'interno del sistema operativo guest come parte del processo di avvio, caricare uno script per tutte le VM. Per eseguire un singolo script in tutte le VM, utilizzare la casella di controllo evidenziata e compilare i campi.
3. Per eseguire determinate modifiche alla configurazione sono necessarie credenziali utente con autorizzazioni adeguate. Fornire le credenziali nei seguenti casi:
    - Uno script verrà eseguito all'interno della VM dal sistema operativo guest.
    - È necessario eseguire uno snapshot coerente con l'applicazione.



Archivi dati cartografici

Il passaggio finale nella creazione di un piano di replicazione è identificare il modo in cui ONTAP dovrebbe proteggere i datastore. Queste impostazioni definiscono l'obiettivo del punto di ripristino (RPO) dei piani di replica, quanti backup devono essere mantenuti e dove replicare i volumi ONTAP di hosting di ciascun datastore vCenter.

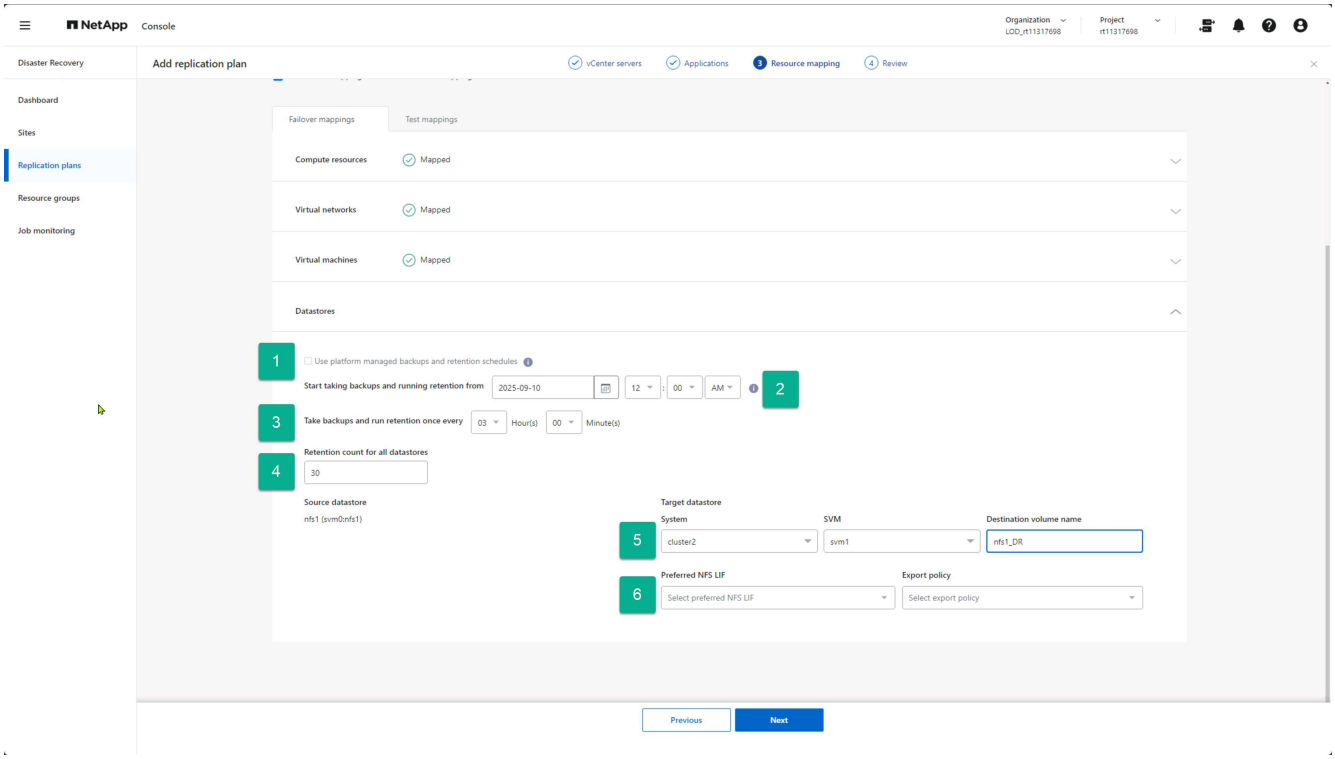
Per impostazione predefinita, NetApp Disaster Recovery gestisce la propria pianificazione di replica degli snapshot; tuttavia, facoltativamente, è possibile specificare di utilizzare la pianificazione dei criteri di replica SnapMirror esistente per la protezione del datastore.

Inoltre, è possibile personalizzare facoltativamente quali LIF (interfacce logiche) dei dati e criteri di esportazione utilizzare. Se non si specificano queste impostazioni, NetApp Disaster Recovery utilizza tutti i dati LIF associati al protocollo appropriato (NFS, iSCSI o FC) e utilizza la policy di esportazione predefinita per i volumi NFS.

Per configurare la mappatura del datastore (volume)

1. (Facoltativo) Decidi se desideri utilizzare una pianificazione di replica ONTAP SnapMirror esistente o se desideri che NetApp Disaster Recovery gestisca la protezione delle tue VM (impostazione predefinita).
2. Fornire un punto di partenza da cui stabilire quando il servizio dovrebbe iniziare a eseguire i backup.
3. Specificare la frequenza con cui il servizio deve eseguire un backup e replicarlo nel cluster Amazon FSx for NetApp ONTAP di destinazione DR.
4. Specificare quanti backup storici devono essere conservati. Il servizio mantiene lo stesso numero di backup sul cluster di archiviazione di origine e di destinazione.
5. (Facoltativo) Selezionare un'interfaccia logica predefinita (LIF dati) per ciascun volume. Se non viene selezionato nulla, vengono configurati tutti i LIF di dati nell'SVM di destinazione che supportano il protocollo di accesso al volume.
6. (Facoltativo) Selezionare una policy di esportazione per tutti i volumi NFS. Se non selezionato, viene

utilizzata la politica di esportazione predefinita



Continua con"Creazione guidata piano di replicazione Passaggio 4" .

Creare un piano di replica: Passaggio 4 - Verificare le impostazioni in NetApp Disaster Recovery

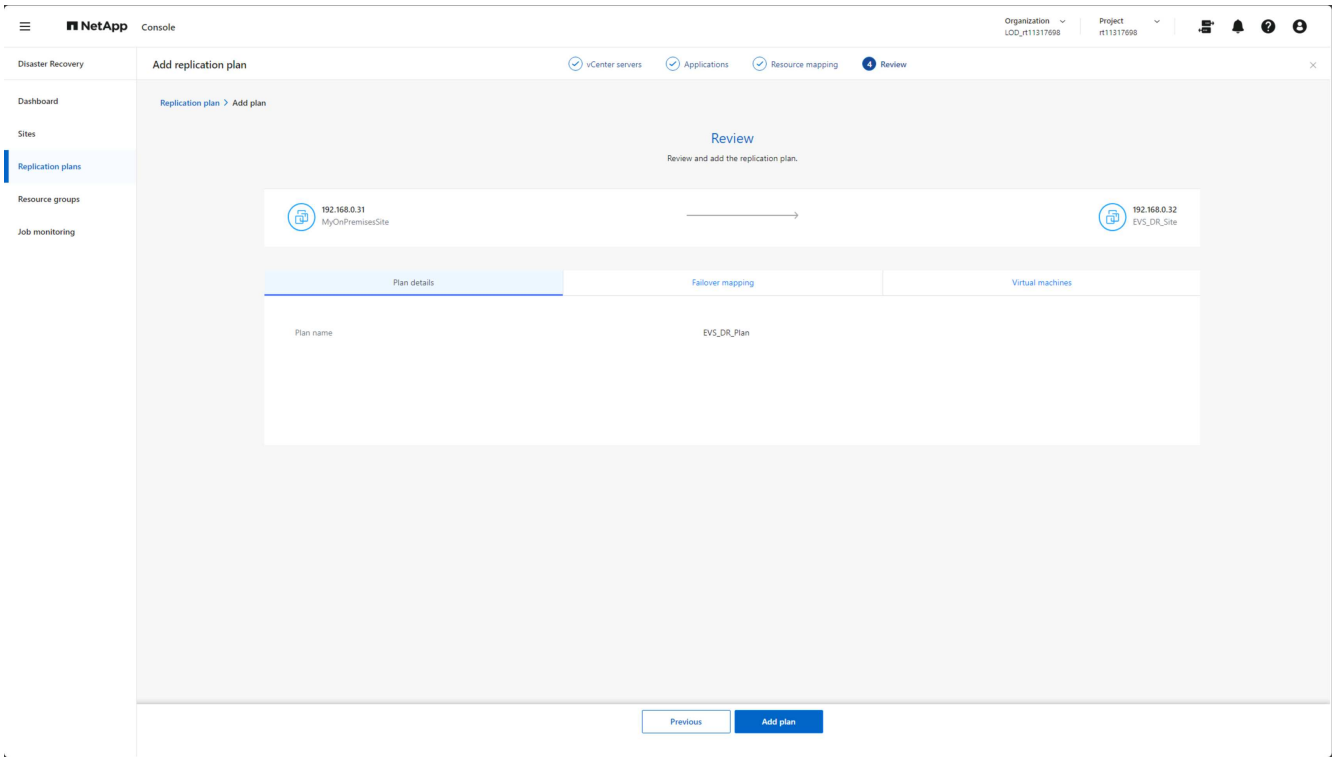
Dopo aver aggiunto le informazioni sul piano di replica in NetApp Disaster Recovery, verificare che le informazioni immesse siano corrette.

Passi

1. Selezionare **Salva** per rivedere le impostazioni prima di attivare il piano di replica.

   È possibile selezionare ciascuna scheda per rivedere le impostazioni e apportare modifiche a qualsiasi scheda selezionando l'icona della matita.

   Revisione delle impostazioni del piano di replicazione



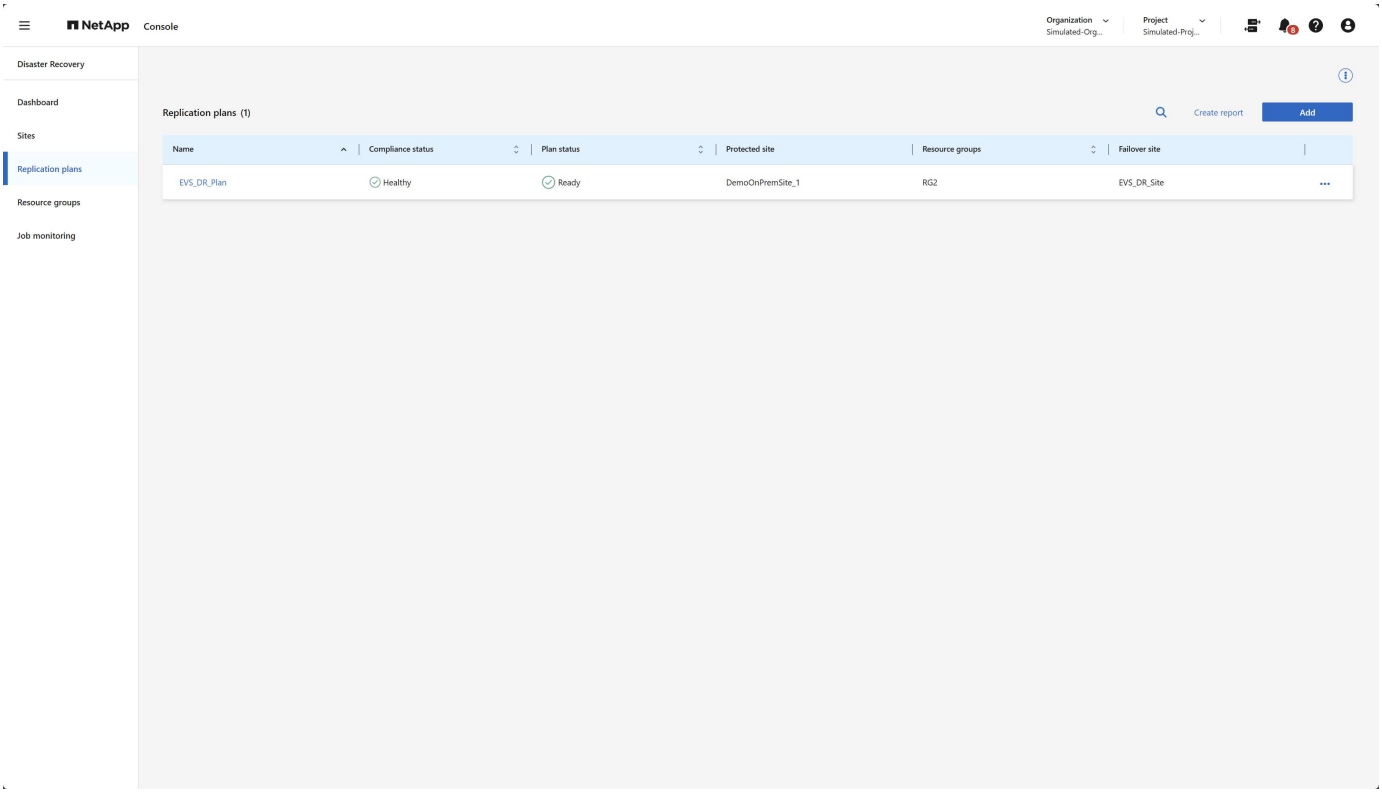
2. Quando sei sicuro che tutte le impostazioni siano corrette, seleziona **Aggiungi piano** nella parte inferiore dello schermo.

Continua con"Verificare il piano di replicazione" .

Verificare che tutto funzioni in NetApp Disaster Recovery

Dopo aver aggiunto il piano di replica in NetApp Disaster Recovery, si torna alla pagina Piani di replica, dove è possibile visualizzare i piani di replica e il relativo stato. È necessario verificare che il piano di replicazione sia nello stato **Integro**. In caso contrario, è necessario controllare lo stato del piano di replicazione e correggere eventuali problemi prima di procedere.

Figura: Pagina dei piani di replicazione



NetApp Disaster Recovery esegue una serie di test per verificare che tutti i componenti (cluster ONTAP , cluster vCenter e VM) siano accessibili e nello stato corretto affinché il servizio protegga le VM. Questo è chiamato controllo di conformità e viene eseguito regolarmente.

Nella pagina Piani di replicazione puoi vedere le seguenti informazioni:

- Stato dell'ultimo controllo di conformità
- Lo stato di replicazione del piano di replicazione
- Il nome del sito protetto (di origine)
- L'elenco dei gruppi di risorse protetti dal piano di replica
- Il nome del sito di failover (destinazione)

Eseguire operazioni di piano di replica con NetApp Disaster Recovery

Utilizzare NetApp Disaster Recovery con Amazon EVS e Amazon FSx for NetApp ONTAP per eseguire le seguenti operazioni: failover, failover di prova, aggiornamento delle risorse, migrazione, acquisizione immediata di uno snapshot, disabilitazione/abilitazione del piano di replica, pulizia dei vecchi snapshot, riconciliazione degli snapshot, eliminazione del piano di replica e modifica delle pianificazioni.

Failover

L'operazione principale che potresti dover eseguire è quella che speri non accada mai: il failover sul data center DR (di destinazione) in caso di un guasto catastrofico nel sito di produzione locale.

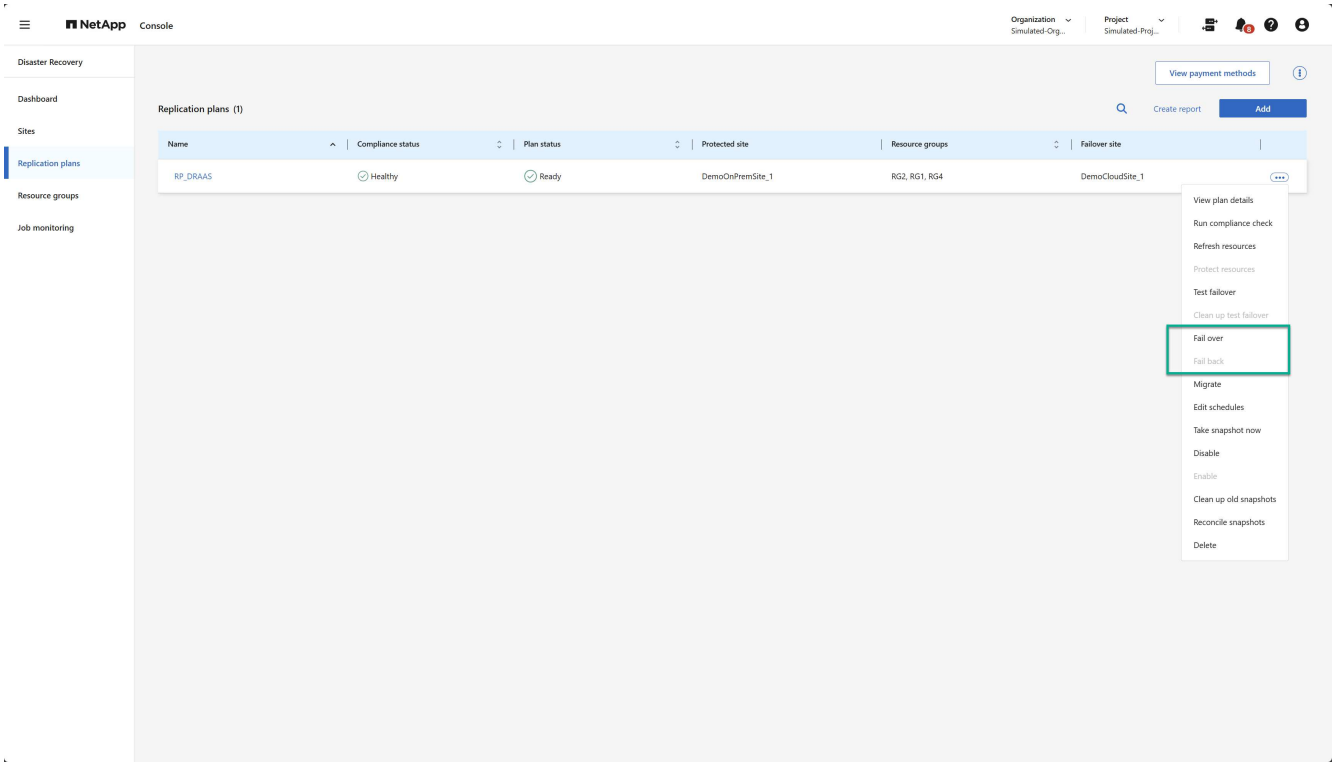
Il failover è un processo avviato manualmente.

Passaggi per accedere all'operazione di failover

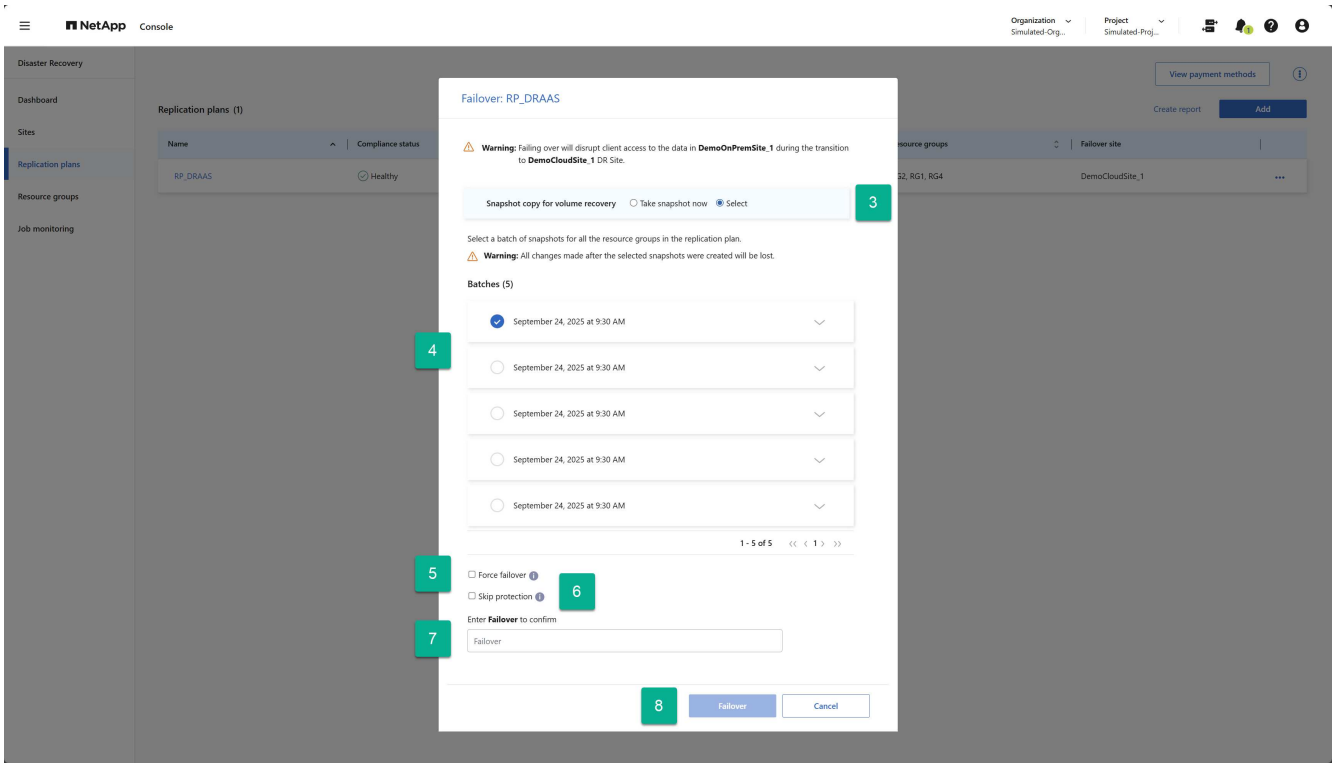
1. Dalla barra di navigazione sinistra NetApp Console , selezionare **Protezione** > **Disaster Recovery**.
2. Dal menu NetApp Disaster Recovery , selezionare **Piani di replica**.

Passaggi per eseguire un failover

1. Dalla pagina Piani di replica, seleziona l'opzione Azioni del piano di replica ••• .
2. Selezionare **Fail over**.



3. Se il sito di produzione (protetto) non è accessibile, selezionare uno snapshot creato in precedenza come immagine di ripristino. Per farlo, seleziona **Seleziona**.
4. Selezionare il backup da utilizzare per il ripristino.
5. (Facoltativo) Selezionare se si desidera che NetApp Disaster Recovery forzi il processo di failover indipendentemente dallo stato del piano di replica. Questa soluzione dovrebbe essere adottata solo come ultima risorsa.
6. (Facoltativo) Selezionare se si desidera che NetApp Disaster Recovery crei automaticamente una relazione di protezione inversa dopo il ripristino del sito di produzione.
7. Digita la parola "Failover" per confermare che desideri procedere.
8. Selezionare **Failover**.



Failover di prova

Un failover di test è simile a un failover, ma con due differenze.

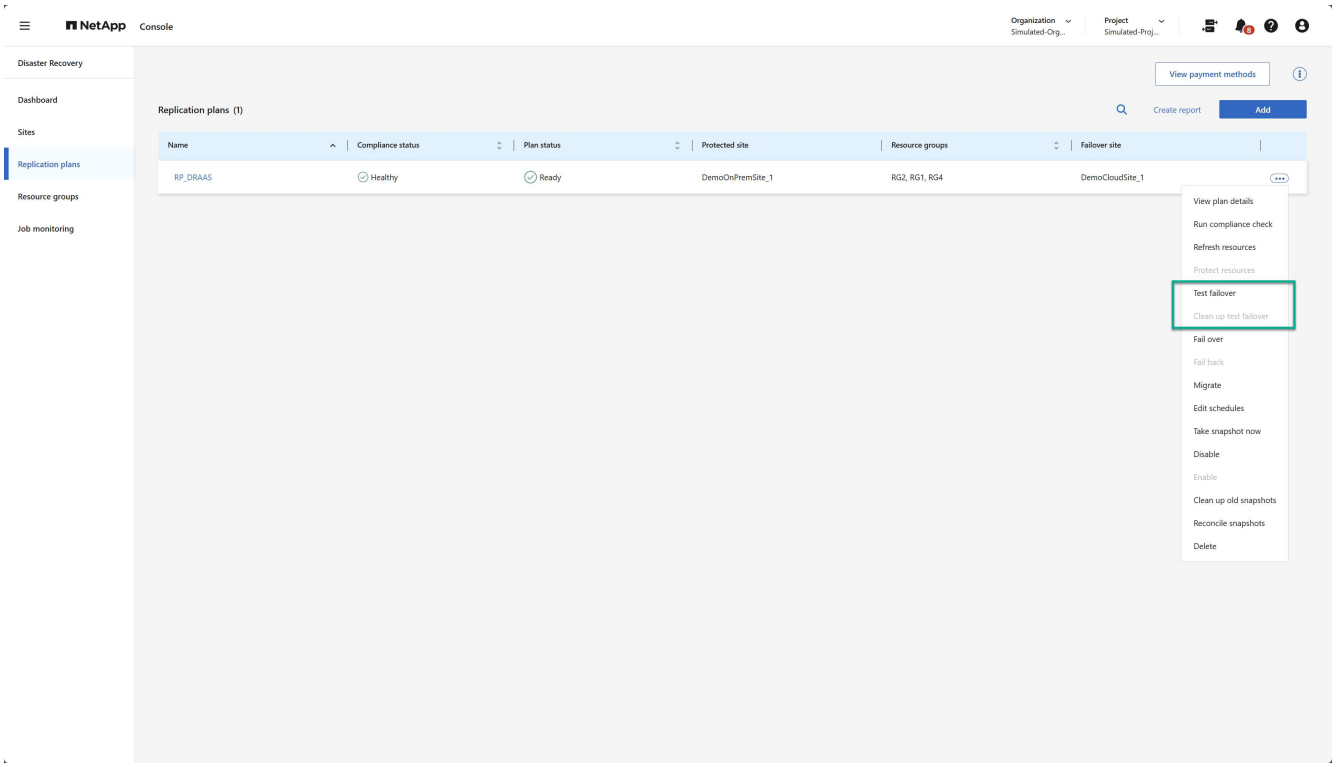
- Il sito di produzione è ancora attivo e tutte le VM funzionano ancora come previsto.
- La protezione NetApp Disaster Recovery delle VM di produzione continua.

Ciò viene realizzato utilizzando volumi ONTAP FlexClone nativi nel sito di destinazione. Per saperne di più sul failover di test, vedere"Eseguire il failover delle applicazioni su un sito remoto | Documentazione NetApp" .

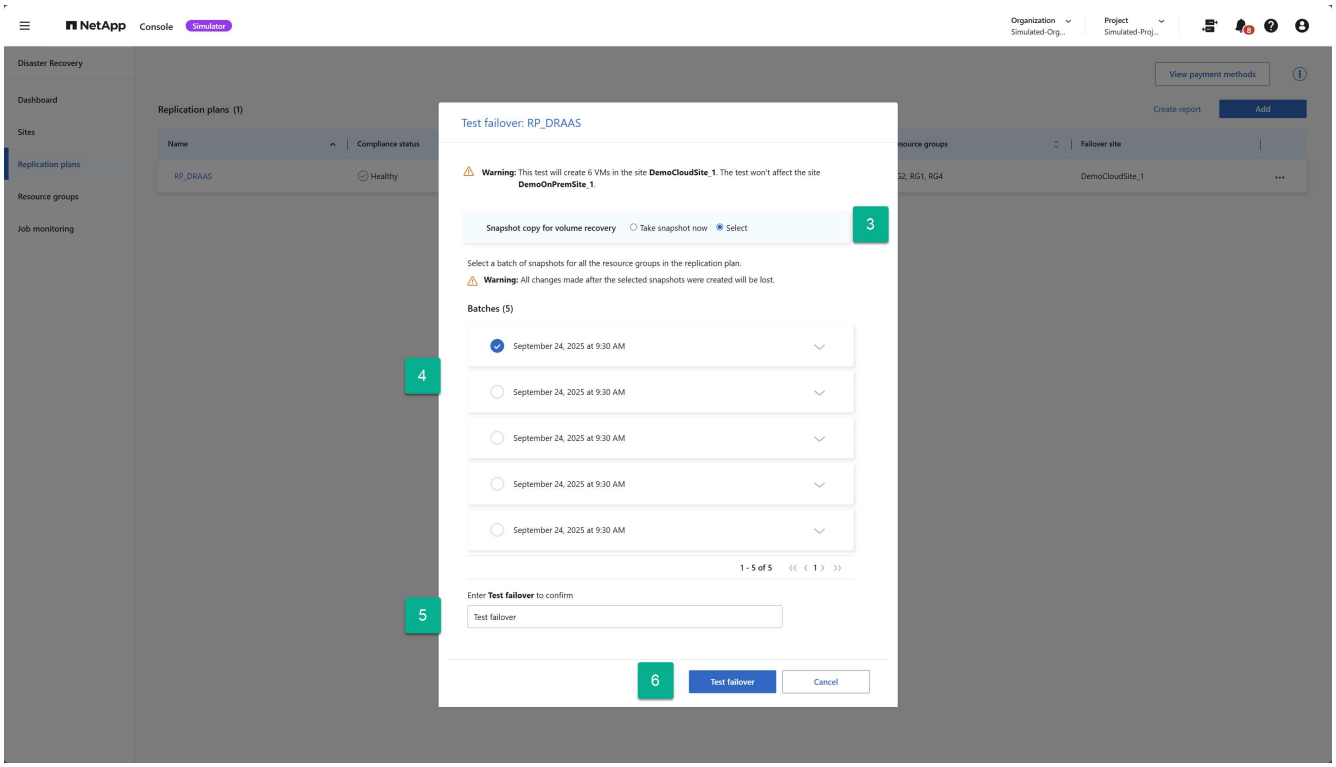
I passaggi per eseguire un failover di prova sono identici a quelli utilizzati per eseguire un failover reale, con la differenza che si utilizza l'operazione Failover di prova nel menu contestuale del piano di replica.

Passi

1. Selezionare l'opzione Azioni del piano di replicazione ••• .
2. Selezionare **Test failover** dal menu.



3. Decidi se vuoi ottenere lo stato più recente dell'ambiente di produzione (Esegui snapshot ora) o utilizzare un backup del piano di replica creato in precedenza (Seleziona)
4. Se hai scelto un backup creato in precedenza, seleziona il backup da utilizzare per il ripristino.
5. Digitare la parola "Test failover" per confermare che si desidera procedere.
6. Selezionare **Test failover**.

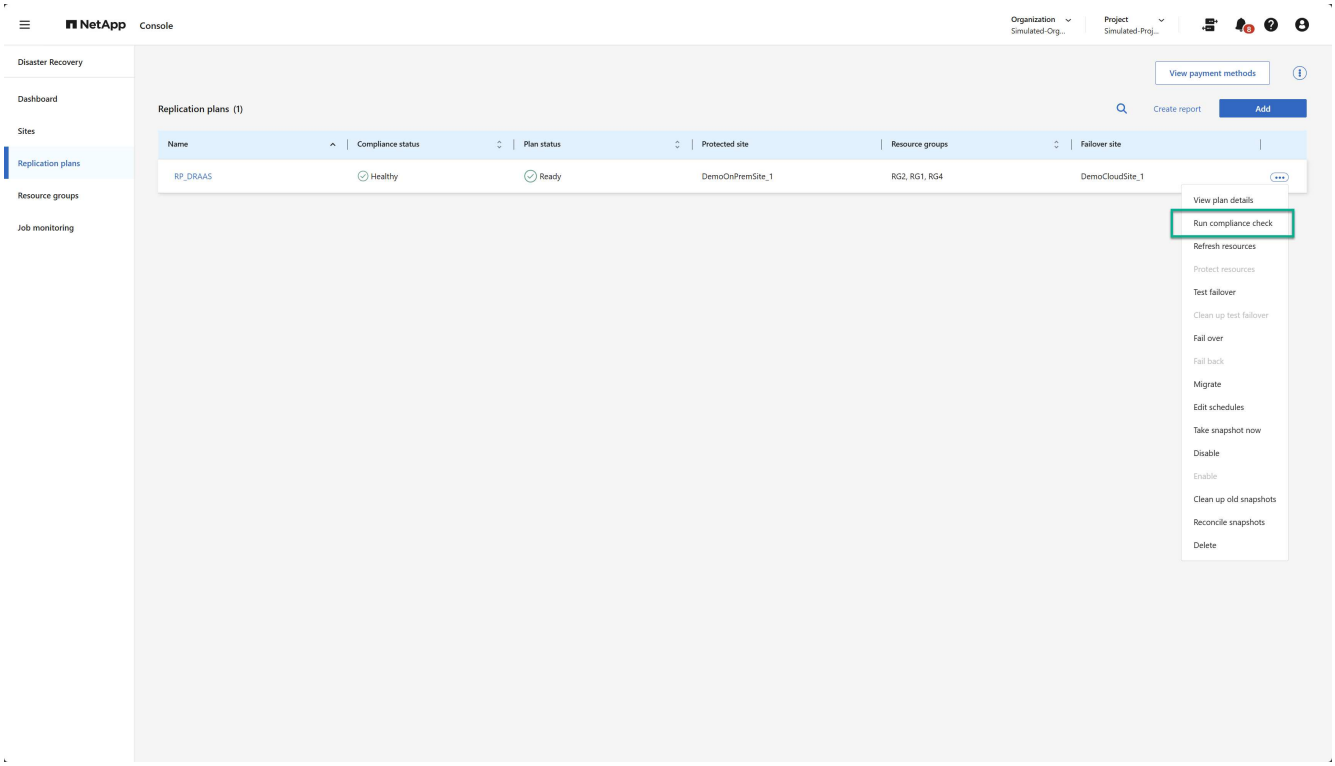


Eseguire un controllo di conformità

Per impostazione predefinita, i controlli di conformità vengono eseguiti ogni tre ore. In qualsiasi momento potresti voler eseguire manualmente un controllo di conformità.

Passi

1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Selezionare l'opzione **Esegui controllo di conformità** dal menu Azioni del piano di replicazione:



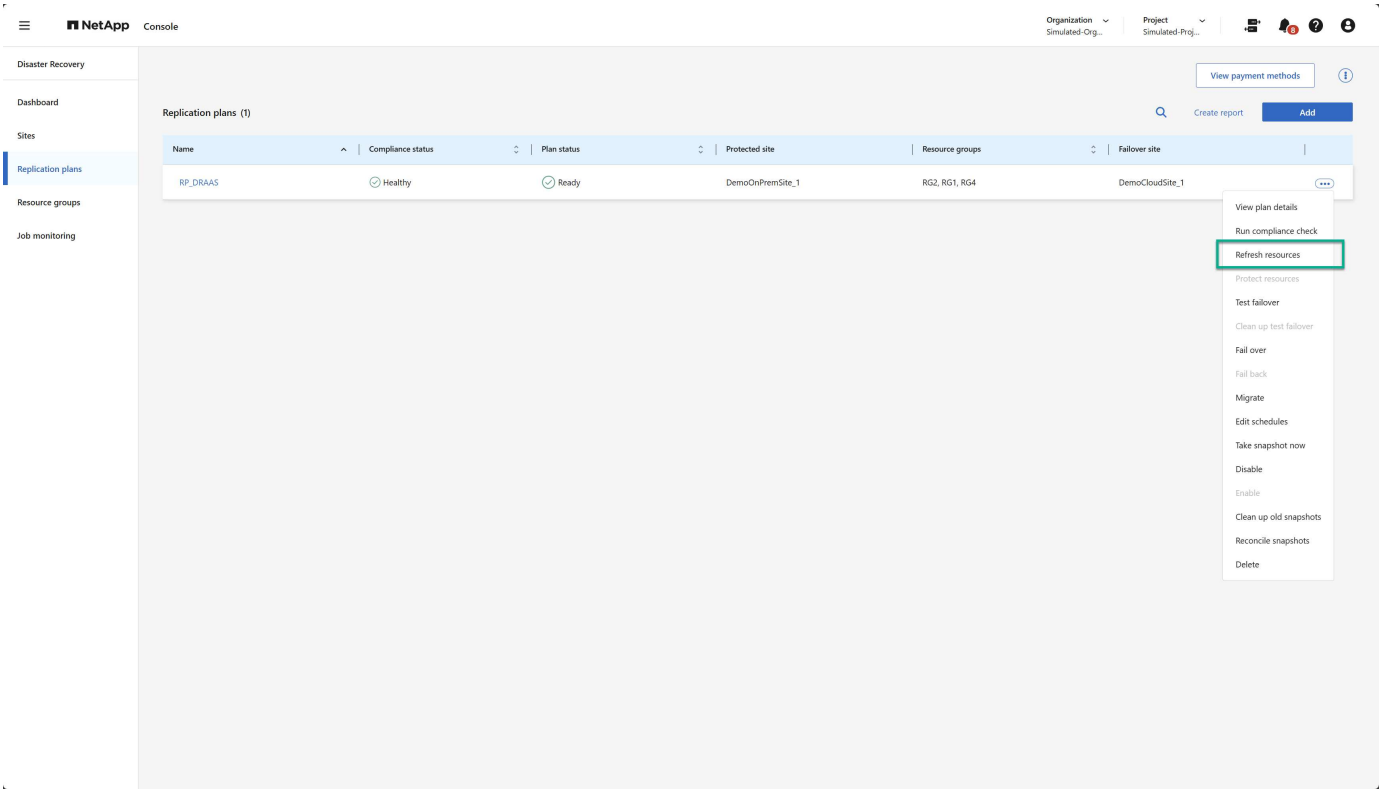
3. Per modificare la frequenza con cui NetApp Disaster Recovery esegue automaticamente i controlli di conformità, selezionare l'opzione **Modifica pianificazioni** dal menu Azioni del piano di replica.

Aggiorna le risorse

Ogni volta che si apportano modifiche all'infrastruttura virtuale, ad esempio aggiungendo o eliminando VM, aggiungendo o eliminando datastore o spostando VM tra datastore, è necessario eseguire un aggiornamento dei cluster vCenter interessati nel servizio NetApp Disaster Recovery . Per impostazione predefinita, il servizio esegue questa operazione automaticamente una volta ogni 24 ore, ma un aggiornamento manuale garantisce che le informazioni più recenti sull'infrastruttura virtuale siano disponibili e prese in considerazione per la protezione DR.

Ci sono due casi in cui è necessario un aggiornamento:

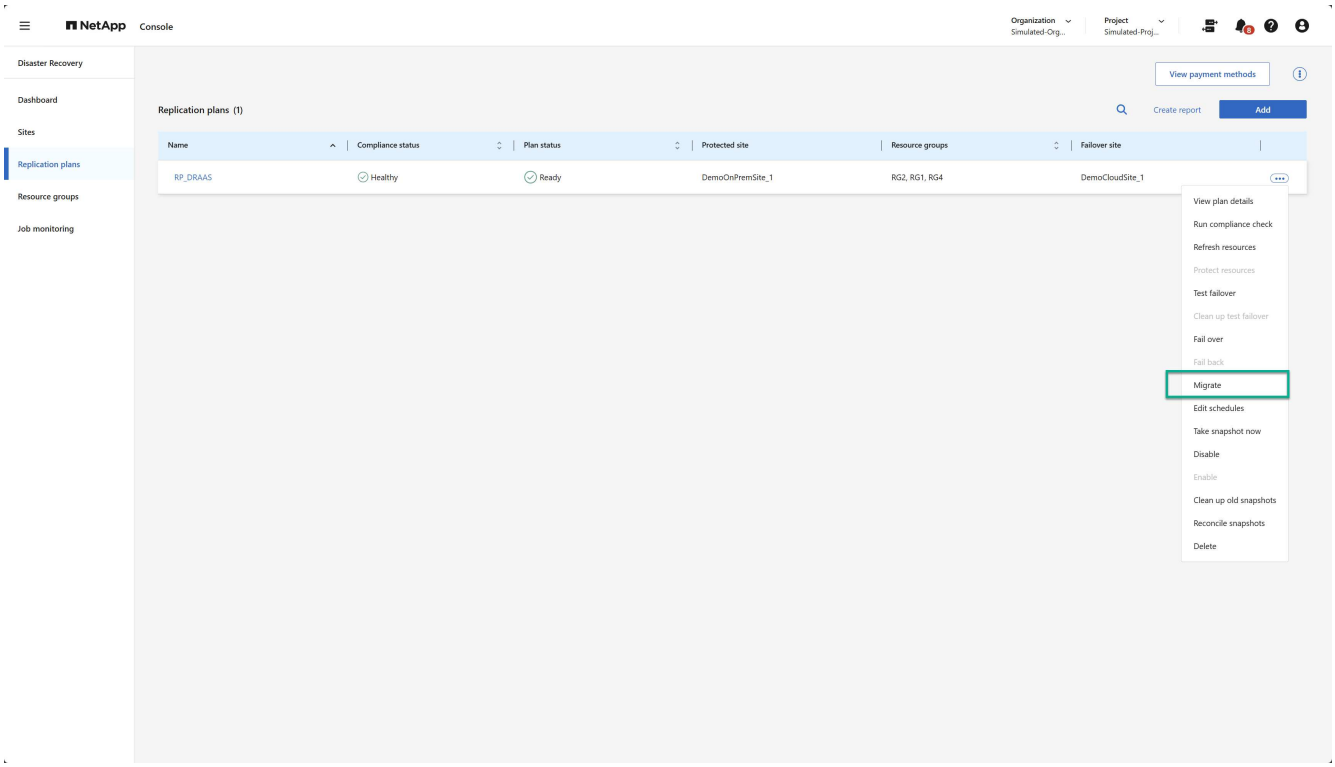
- Aggiornamento vCenter: esegui un aggiornamento vCenter ogni volta che le VM vengono aggiunte, eliminate o spostate da un cluster vCenter:
- Aggiornamento del piano di replica: esegui un aggiornamento del piano di replica ogni volta che una VM viene spostata tra datastore nello stesso cluster vCenter di origine.



Migrare

Sebbene NetApp Disaster Recovery venga utilizzato principalmente per casi di disaster recovery, può anche consentire spostamenti una tantum di un set di VM dal sito di origine al sito di destinazione. Potrebbe essere utilizzato per un progetto di migrazione concertata verso il cloud oppure per evitare disastri, come maltempo, conflitti politici o altri potenziali eventi catastrofici temporanei.

1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Per spostare le VM in un piano di replicazione nel cluster Amazon EVS di destinazione, selezionare **Migra** dal menu Azioni del piano di replicazione:

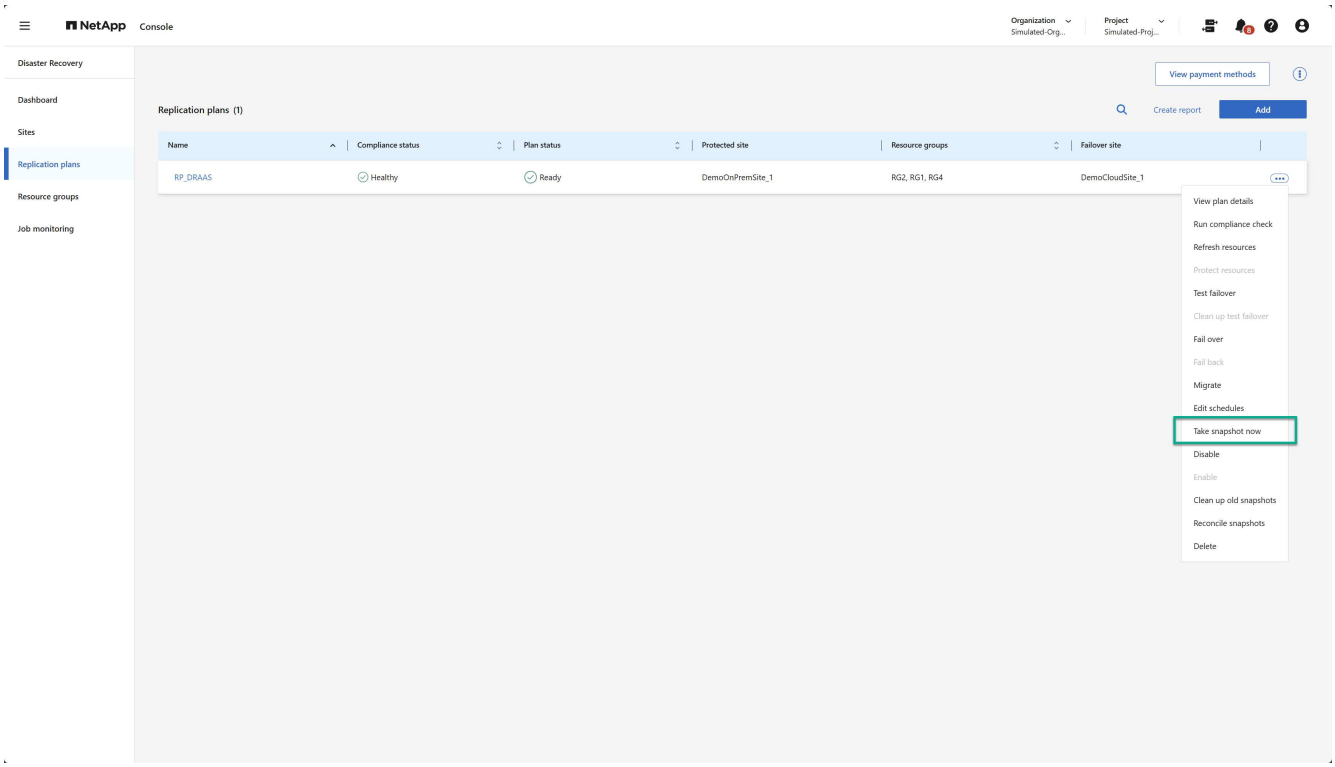


3. Immettere le informazioni nella finestra di dialogo Migra.

Scatta un'istantanea ora

In qualsiasi momento è possibile acquisire un'istantanea immediata del piano di replicazione. Questo snapshot è incluso nelle considerazioni NetApp Disaster Recovery impostate dal conteggio di conservazione degli snapshot del piano di replica.

1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Per acquisire immediatamente uno snapshot delle risorse del piano di replica, selezionare **Esegui snapshot ora** nel menu Azioni del piano di replica:

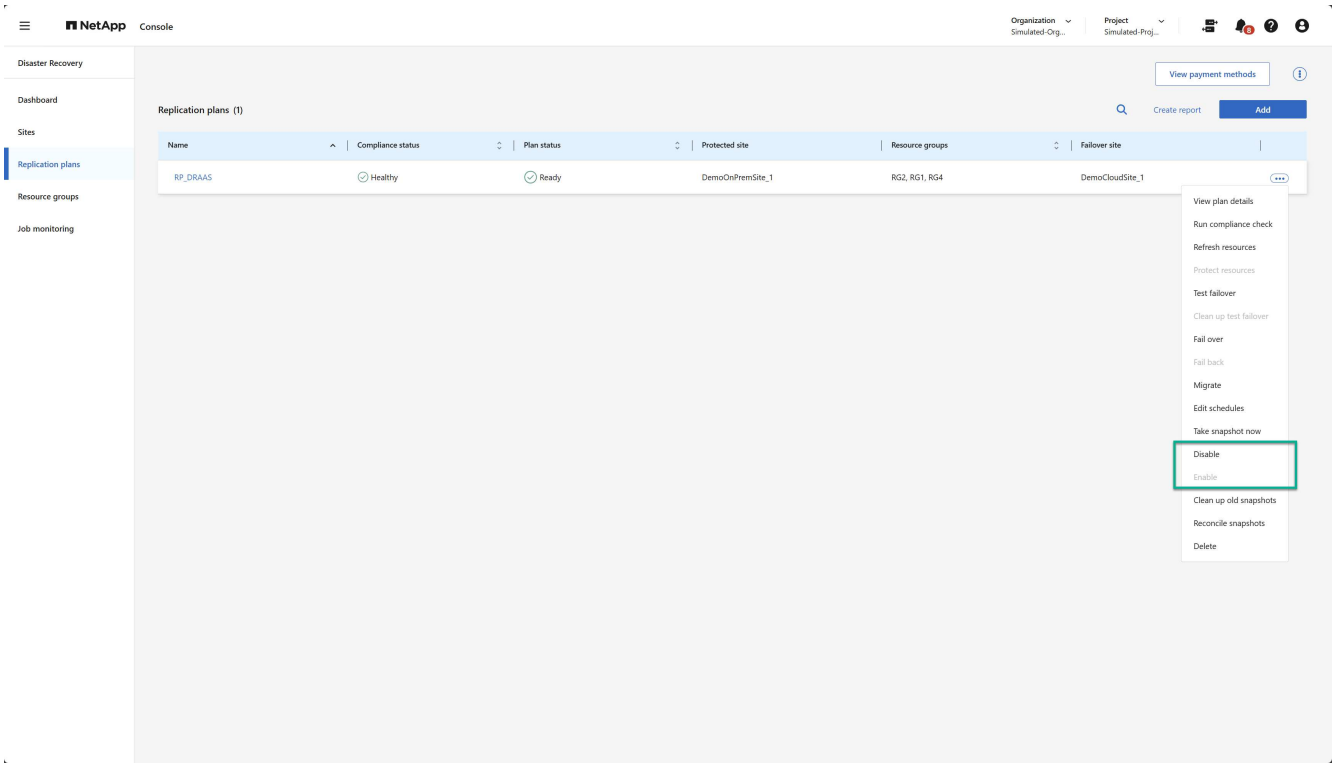


Disabilita o abilita il piano di replicazione

Potrebbe essere necessario interrompere temporaneamente il piano di replicazione per eseguire alcune operazioni o operazioni di manutenzione che potrebbero avere un impatto sul processo di replicazione. Il servizio fornisce un metodo per arrestare e avviare la replica.

1. Per interrompere temporaneamente la replica, selezionare **Disabilita** nel menu Azioni del piano di replica.
2. Per riavviare la replica, selezionare **Abilita** nel menu Azioni del piano di replica.

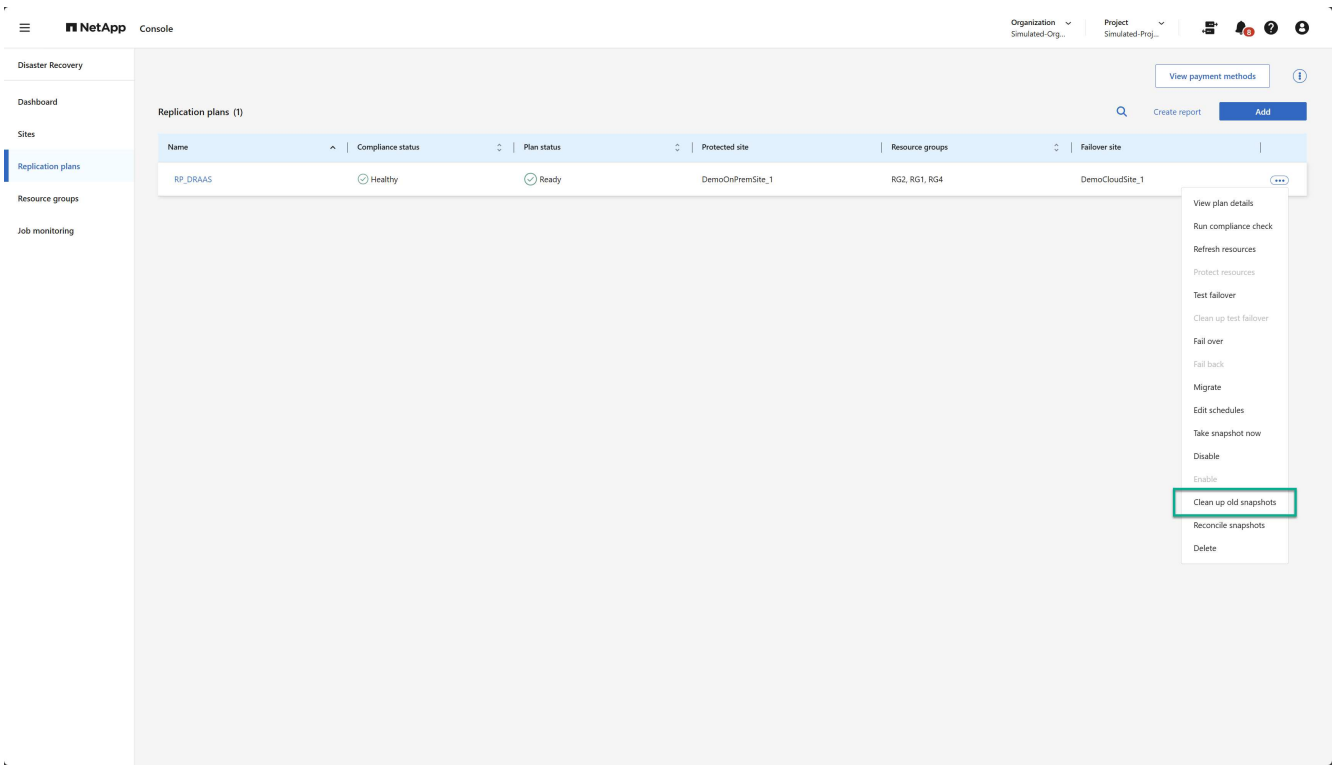
   Quando il piano di replica è attivo, il comando **Abilita** è disattivato. Quando il piano di replica è disabilitato, il comando **Disabilita** è disattivato.



Pulisci i vecchi snapshot

Potrebbe essere opportuno ripulire gli snapshot più vecchi conservati nei siti di origine e di destinazione. Ciò può accadere se il conteggio di conservazione degli snapshot del piano di replica viene modificato.

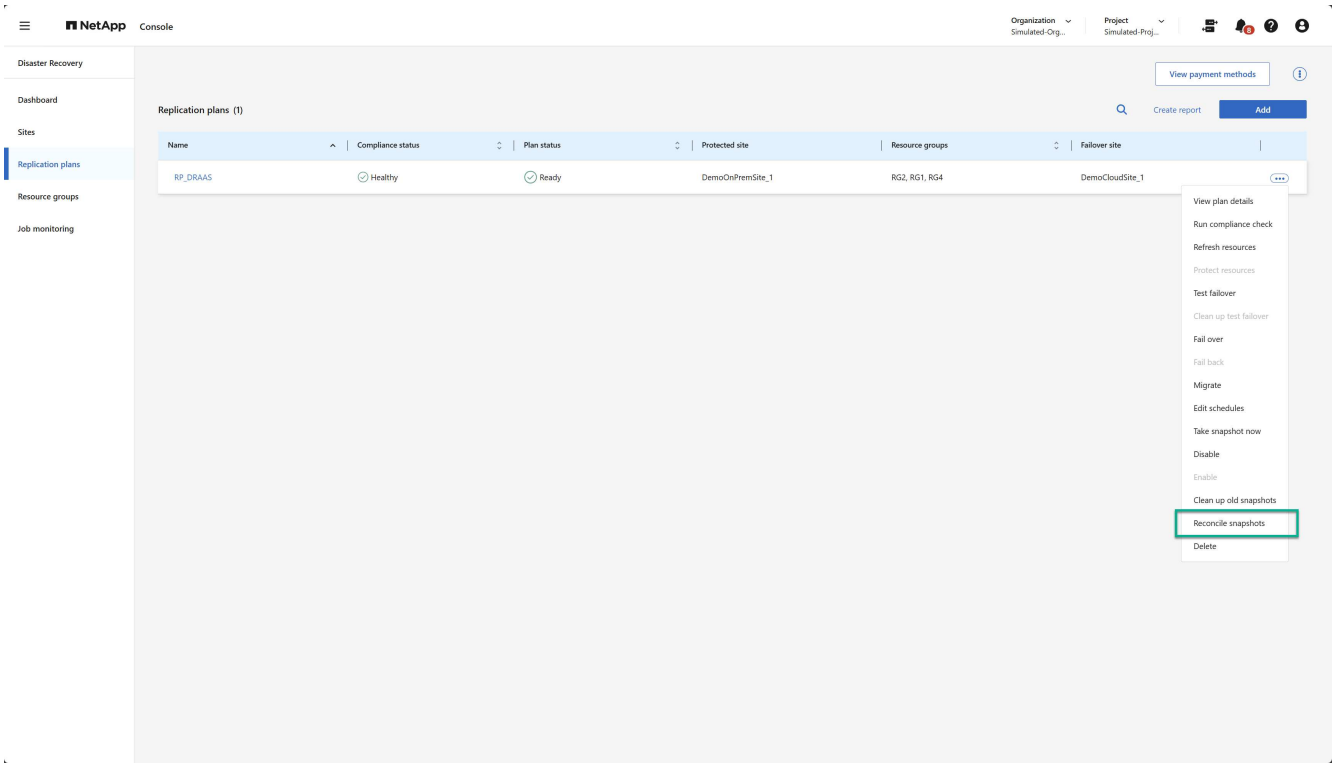
1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Per rimuovere manualmente questi snapshot più vecchi, selezionare **Pulisci snapshot vecchi** dal menu Azioni del piano di replica.



Riconciliare gli snapshot

Poiché il servizio orchestra gli snapshot del volume ONTAP , è possibile per un amministratore di storage ONTAP eliminare direttamente gli snapshot utilizzando ONTAP System Manager, ONTAP CLI o le API REST ONTAP senza che il servizio ne sia a conoscenza. Il servizio elimina automaticamente ogni 24 ore tutti gli snapshot presenti sul cluster di origine che non si trovano sul cluster di destinazione. Tuttavia, è possibile eseguire questa operazione su richiesta. Questa funzionalità consente di garantire che gli snapshot siano coerenti in tutti i siti.

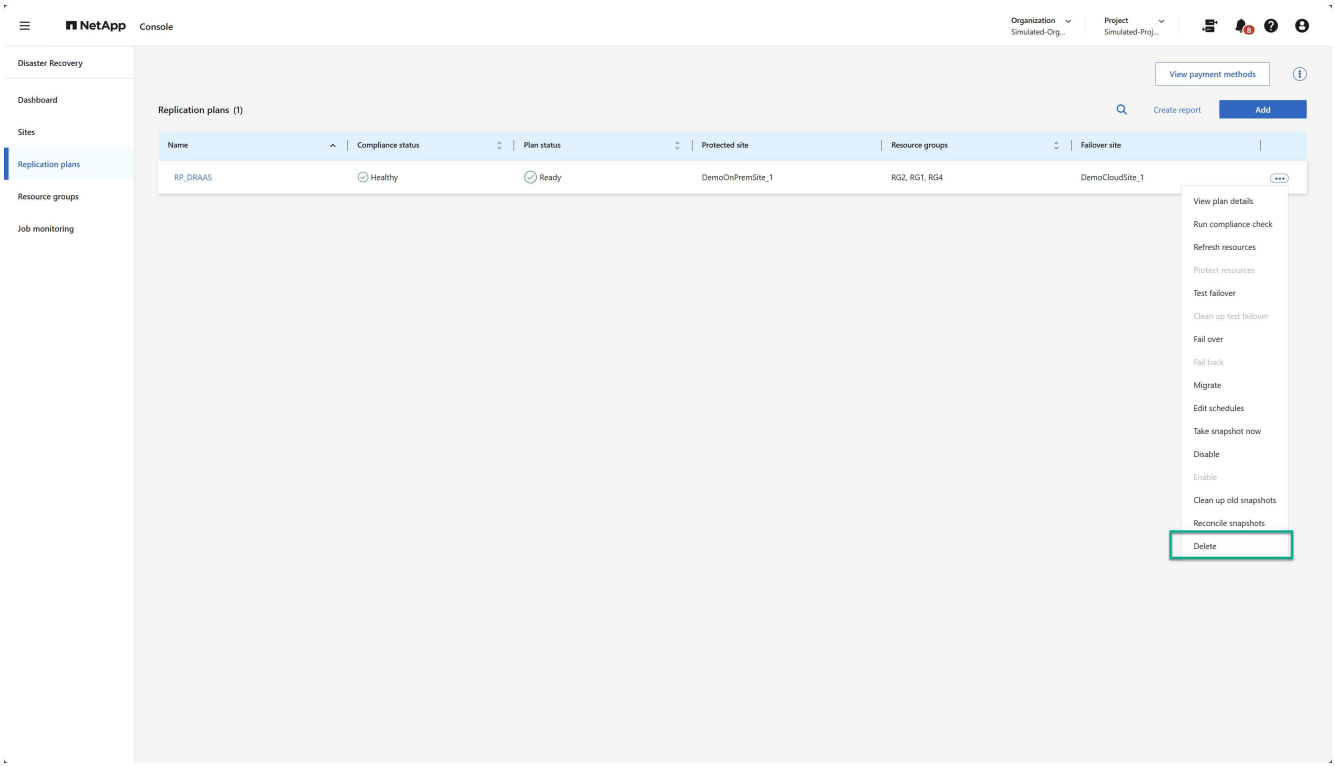
1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Per eliminare gli snapshot dal cluster di origine che non esistono nel cluster di destinazione, selezionare **Riconcilia snapshot** dal menu Azioni del piano di replica.



Elimina piano di replicazione

Se il piano di replicazione non è più necessario, è possibile eliminarlo.

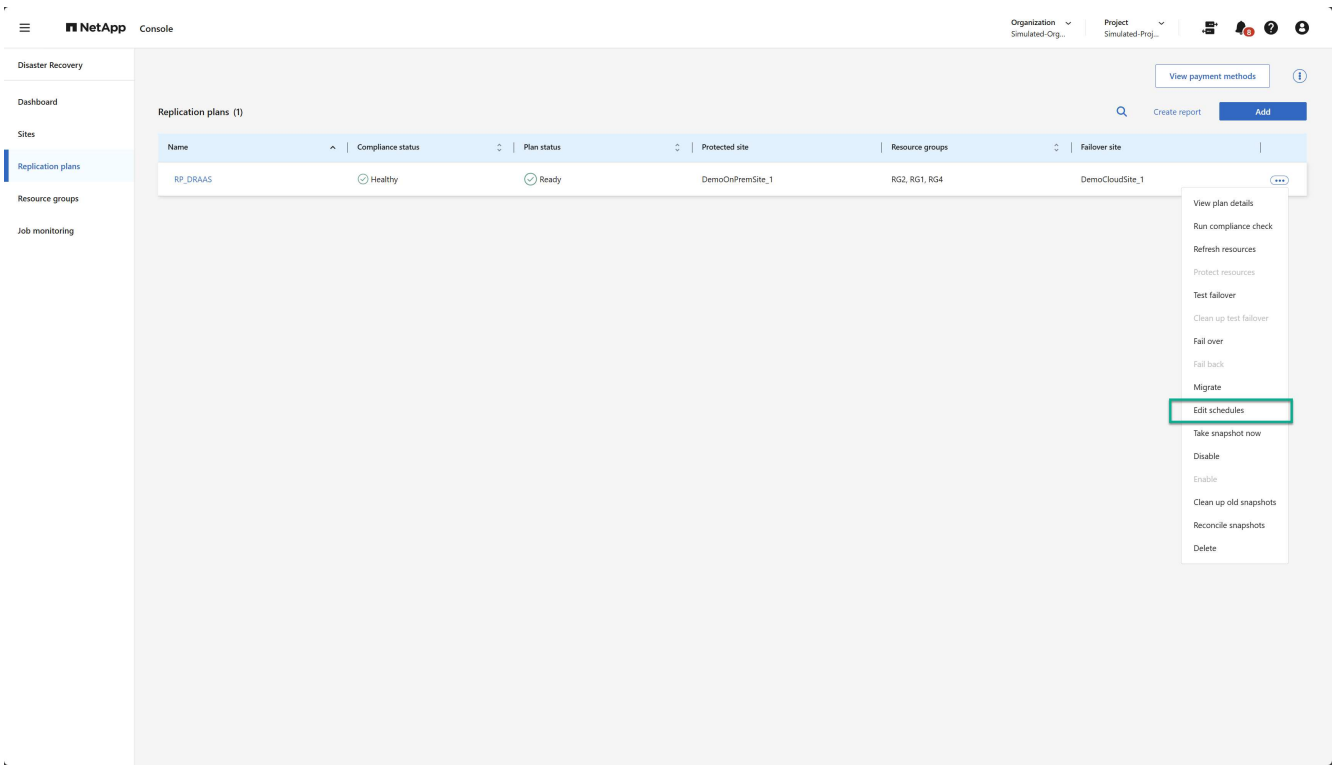
1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Per eliminare il piano di replicazione, selezionare **Elimina** dal menu contestuale del piano di replicazione.



Modificare gli orari

Due operazioni vengono eseguite automaticamente con cadenza regolare: i failover dei test e i controlli di conformità.

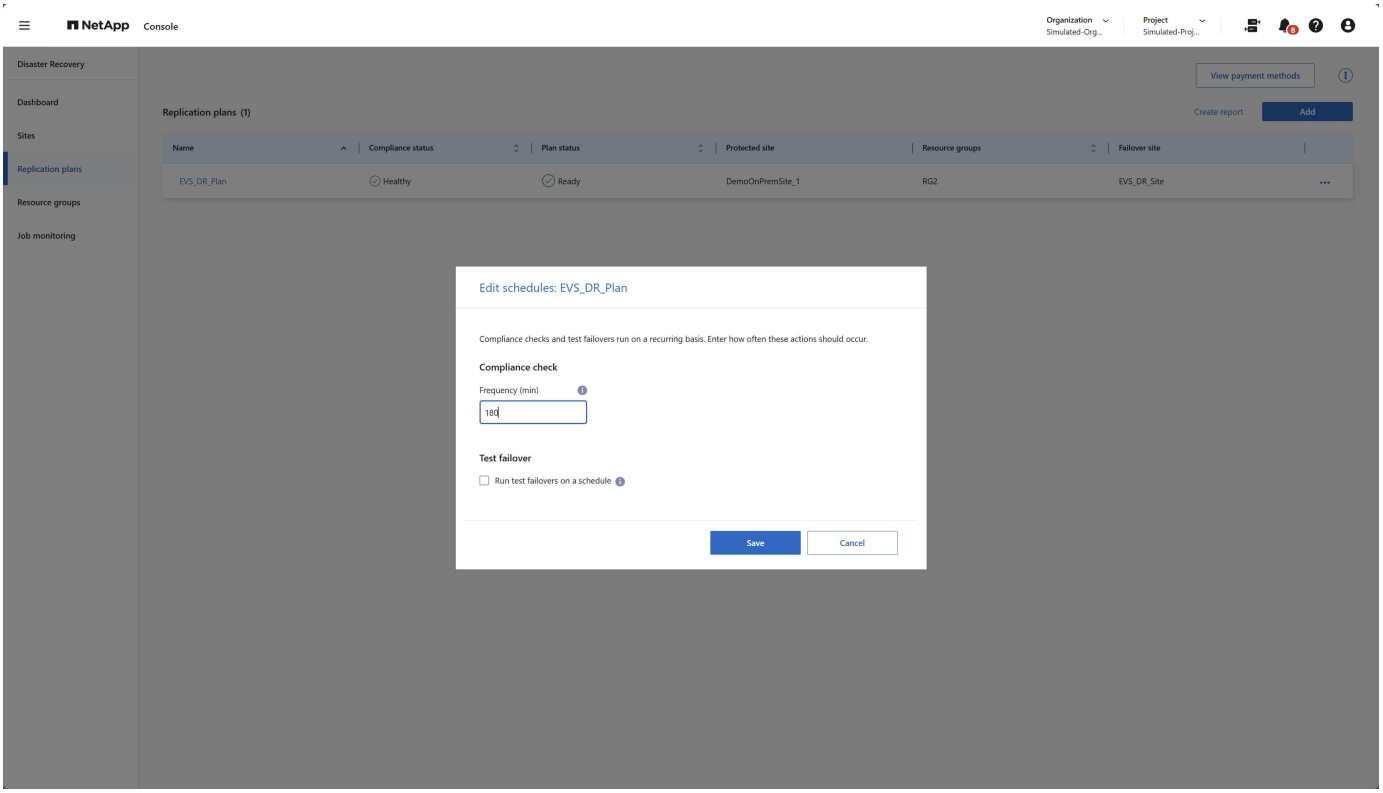
1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Per modificare queste pianificazioni per una di queste due operazioni, selezionare **Modifica pianificazioni** per il piano di replica.



Modifica l'intervallo di controllo della conformità

Per impostazione predefinita, i controlli di conformità vengono eseguiti ogni tre ore. È possibile modificare l'intervallo tra 30 minuti e 24 ore.

Per modificare questo intervallo, modificare il campo Frequenza nella finestra di dialogo Modifica pianificazioni:



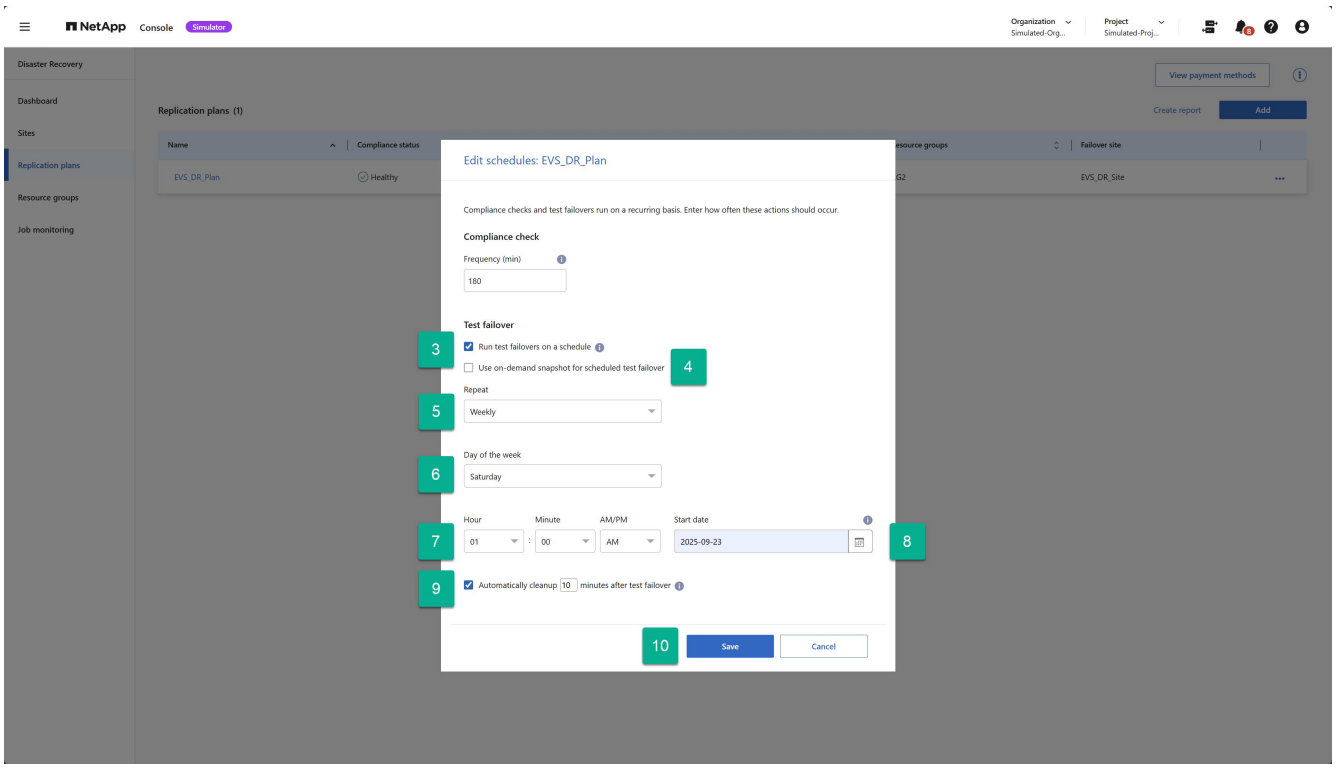
Pianificare failover di test automatizzati

Per impostazione predefinita, i failover dei test vengono eseguiti manualmente. È possibile pianificare failover di test automatici, che contribuiscono a garantire che i piani di replica funzionino come previsto. Per saperne di più sul processo di failover di test, vedere"Testare il processo di failover" .

Passaggi per pianificare i failover dei test

1. Seleziona l'opzione *Azioni* ••• accanto al piano di replicazione.
2. Selezionare **Esegui failover**.
3. Selezionare la casella di controllo **Esegui failover di test in base a una pianificazione**.
4. (Facoltativo) Selezionare **Usa snapshot su richiesta per failover di test pianificato**.
5. Selezionare un tipo di intervallo nel menu a discesa Ripeti.
6. Selezionare quando eseguire il failover di prova
   a. Settimanale: seleziona il giorno della settimana
   b. Mensile: seleziona il giorno del mese
7. Scegli l'ora del giorno in cui eseguire il failover di prova
8. Scegli la data di inizio.
9. Decidi se desideri che il servizio pulisca automaticamente l'ambiente di test e per quanto tempo desideri che l'ambiente di test venga eseguito prima che venga avviato il processo di pulizia.

10. Seleziona **Salva**.



Domande frequenti su NetApp Disaster Recovery

Questa sezione FAQ può aiutarti se stai cercando una risposta rapida a una domanda.

Qual è l'URL NetApp Disaster Recovery ? Per l'URL, in un browser, inserisci: "https://console.netapp.com/" per accedere alla console NetApp .

È necessaria una licenza per utilizzare NetApp Disaster Recovery? Per un accesso completo è necessaria una licenza NetApp Disaster Recovery . Tuttavia, puoi provarlo con la versione di prova gratuita.

Per i dettagli sulla configurazione delle licenze per NetApp Disaster Recovery, fare riferimento a"Impostare la licenza NetApp Disaster Recovery" .

Come si accede a NetApp Disaster Recovery? NetApp Disaster Recovery non richiede alcuna abilitazione. L'opzione di ripristino di emergenza viene visualizzata automaticamente nel menu di navigazione sinistro della NetApp Console .

Conoscenza e supporto

Registrati per ricevere supporto

Per ricevere supporto tecnico specifico per NetApp Console e le sue soluzioni di storage e servizi dati è necessaria la registrazione al supporto. La registrazione del supporto è inoltre richiesta per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP .

La registrazione per il supporto non abilita il supporto NetApp per un servizio file del provider cloud. Per assistenza tecnica relativa a un servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla sezione "Ottenere assistenza" nella documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Panoramica della registrazione del supporto

Per attivare il diritto al sostegno sono previste due modalità di registrazione:

- Registrando il numero di serie del tuo account NetApp Console (il numero di serie di 20 cifre 960xxxxxxxx che si trova nella pagina Risorse di supporto nella Console).

  Questo funge da ID di abbonamento unico per qualsiasi servizio all'interno della Console. Ogni account Console deve essere registrato.

- Registrazione dei numeri di serie di Cloud Volumes ONTAP associati a un abbonamento nel marketplace del tuo provider cloud (si tratta di numeri di serie a 20 cifre 909201xxxxxxxx).

  Questi numeri di serie sono comunemente denominati *numeri di serie PAYGO* e vengono generati dalla NetApp Console al momento della distribuzione Cloud Volumes ONTAP .

La registrazione di entrambi i tipi di numeri di serie consente funzionalità quali l'apertura di ticket di supporto e la generazione automatica di casi. La registrazione viene completata aggiungendo gli account NetApp Support Site (NSS) alla Console come descritto di seguito.

Registra NetApp Console per il supporto NetApp

Per registrarsi per ricevere supporto e attivare il diritto al supporto, un utente del tuo account NetApp Console deve associare un account NetApp Support Site al proprio accesso alla Console. La modalità di registrazione per l'assistenza NetApp varia a seconda che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite la Console.

Passi

1. Selezionare **Amministrazione** > **Credenziali**.

2. Selezionare **Credenziali utente**.
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp (NSS).
4. Per confermare che il processo di registrazione è andato a buon fine, seleziona l'icona Aiuto e poi **Supporto**.

   La pagina **Risorse** dovrebbe mostrare che il tuo account Console è registrato per il supporto.

   Tieni presente che gli altri utenti della Console non vedranno lo stesso stato di registrazione del supporto se non hanno associato un account NetApp Support Site al loro login. Tuttavia, ciò non significa che il tuo account non sia registrato per l'assistenza. Se un utente dell'organizzazione ha seguito questi passaggi, il tuo account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp esistente con licenze e numeri di serie esistenti ma *nessun* account NSS, devi creare un account NSS e associarlo al tuo accesso alla Console.

Passi

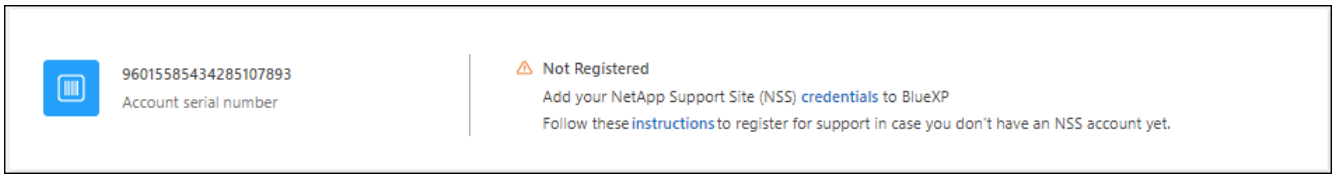
1. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account della console (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione dell'account.
2. Associa il tuo nuovo account NSS al tuo accesso alla Console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Novità assoluta per NetApp

Se sei un nuovo utente NetApp e non hai un account NSS, segui i passaggi indicati di seguito.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.
2. Individua il numero di serie del tuo ID account nella pagina di registrazione del supporto.



3. Vai a "Sito di registrazione del supporto NetApp" e seleziona **Non sono un cliente NetApp registrato**.
4. Compila i campi obbligatori (quelli contrassegnati da asterischi rossi).
5. Nel campo **Linea di prodotti**, seleziona **Cloud Manager** e poi seleziona il tuo fornitore di fatturazione applicabile.
6. Copia il numero di serie del tuo account dal passaggio 2 sopra, completa il controllo di sicurezza e conferma di aver letto l'Informativa globale sulla privacy dei dati di NetApp.

   Per finalizzare questa transazione sicura, verrà inviata immediatamente un'e-mail alla casella di posta indicata. Se l'e-mail di convalida non arriva entro pochi minuti, assicurati di controllare la cartella spam.

7. Conferma l'azione dall'interno dell'e-mail.

   La conferma invia la richiesta a NetApp e ti consiglia di creare un account sul sito di supporto NetApp .

8. Crea un account del sito di supporto NetApp completando il "Modulo di registrazione utente del sito di supporto NetApp"
   a. Assicurati di selezionare il livello utente appropriato, che in genere è **Cliente NetApp /Utente finale**.
   b. Assicurati di copiare il numero di serie dell'account (960xxxx) utilizzato sopra per il campo del numero di serie. Ciò velocizzerà l'elaborazione.

Dopo aver finito

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di onboarding una tantum per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp , associalo al tuo accesso alla console completando i passaggi indicati di seguitoCliente esistente con un account NSS .

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

L'associazione delle credenziali del sito di supporto NetApp al tuo account della console è necessaria per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP a consumo per il supporto

  Per attivare il supporto per il tuo sistema e accedere alle risorse di supporto tecnico NetApp è necessario fornire il tuo account NSS.

- Distribuzione di Cloud Volumes ONTAP quando si utilizza la propria licenza (BYOL)

  È necessario fornire il proprio account NSS affinché la Console possa caricare la chiave di licenza e abilitare l'abbonamento per il periodo acquistato. Ciò include aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP all'ultima versione

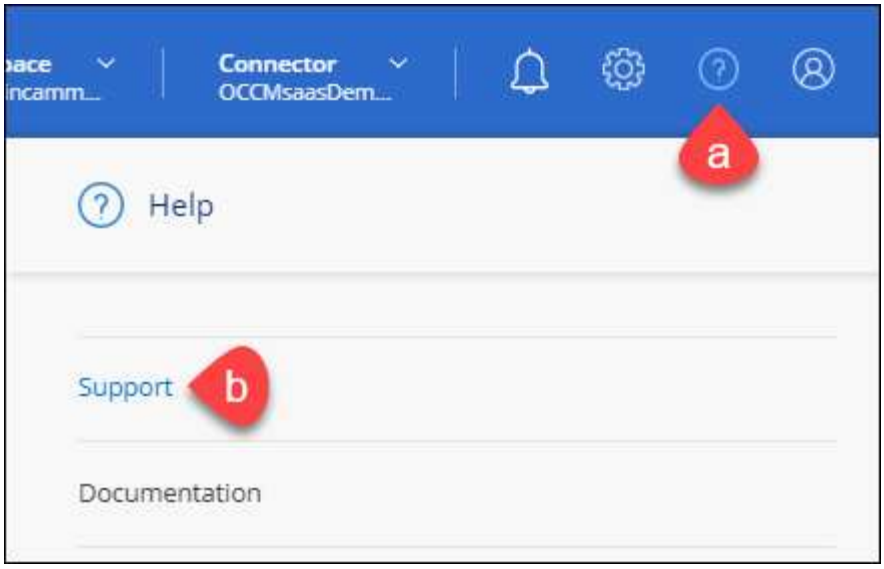
L'associazione delle credenziali NSS al tuo account NetApp Console è diversa dall'associazione dell'account NSS all'accesso utente della Console.

Queste credenziali NSS sono associate al tuo ID account Console specifico. Gli utenti che appartengono all'organizzazione Console possono accedere a queste credenziali da **Supporto > Gestione NSS**.

- Se disponi di un account a livello cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o rivenditore, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Passi

1. Nell'angolo in alto a destra della Console, seleziona l'icona Aiuto e seleziona **Supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, seleziona **Continua** per essere reindirizzato alla pagina di accesso di Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e le licenze.

4. Nella pagina di accesso, inserisci l'indirizzo email e la password registrati sul sito di supporto NetApp per eseguire il processo di autenticazione.

   Queste azioni consentono alla Console di utilizzare il tuo account NSS per attività quali download di licenze, verifica di aggiornamenti software e future registrazioni di supporto.

   Notare quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account ospite o temporaneo). È possibile avere più account NSS a livello di cliente.
   - Può esserci un solo account NSS se tale account è un account a livello di partner. Se provi ad aggiungere account NSS a livello di cliente ed esiste già un account a livello di partner, riceverai il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account poiché sono già presenti utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS preesistenti a livello di cliente e si tenta di aggiungere un account a livello di partner.

   - Dopo aver effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che corrisponde al tuo indirizzo email. Nella pagina **Gestione NSS**, puoi visualizzare la tua email da ••• menu.

   - Se hai bisogno di aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Aggiorna credenziali** in ••• menu.

     Utilizzando questa opzione ti verrà richiesto di effettuare nuovamente l'accesso. Si noti che il token per questi account scade dopo 90 giorni. Verrà pubblicata una notifica per avvisarti di ciò.

Ottieni aiuto

NetApp fornisce supporto per NetApp Console e i suoi servizi cloud in vari modi. Sono disponibili ampie opzioni di auto-supporto gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include supporto tecnico remoto tramite ticket web.

Ottieni supporto per un servizio file di un provider cloud

Per il supporto tecnico relativo al servizio file di un provider cloud, alla sua infrastruttura o a qualsiasi soluzione che utilizzi il servizio, fare riferimento alla documentazione del prodotto in questione.

- "Amazon FSx per ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Per ricevere supporto tecnico specifico per NetApp e le sue soluzioni di storage e servizi dati, utilizzare le opzioni di supporto descritte di seguito.

Utilizzare opzioni di auto-supporto

Queste opzioni sono disponibili gratuitamente, 24 ore al giorno, 7 giorni alla settimana:

- Documentazione

  La documentazione NetApp Console che stai visualizzando.

- "Base di conoscenza"

  Cerca nella knowledge base NetApp per trovare articoli utili per la risoluzione dei problemi.

- "Comunità"

  Unisciti alla community NetApp Console per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo aver attivato il supporto.

Prima di iniziare

- Per utilizzare la funzionalità **Crea un caso**, devi prima associare le credenziali del sito di supporto NetApp all'accesso alla console. "Scopri come gestire le credenziali associate al tuo accesso alla Console" .
- Se stai aprendo un caso per un sistema ONTAP che ha un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Nella pagina **Risorse**, seleziona una delle opzioni disponibili in Supporto tecnico:

a. Seleziona **Chiamaci** se desideri parlare con qualcuno al telefono. Verrai indirizzato a una pagina su netapp.com in cui sono elencati i numeri di telefono che puoi chiamare.

b. Seleziona **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp :

   - **Servizio**: seleziona il servizio a cui è associato il problema. Ad esempio, * NetApp Console* quando si tratta di un problema specifico di supporto tecnico con flussi di lavoro o funzionalità all'interno della Console.
   - **Sistema**: se applicabile all'archiviazione, selezionare * Cloud Volumes ONTAP* o **On-Prem** e quindi l'ambiente di lavoro associato.

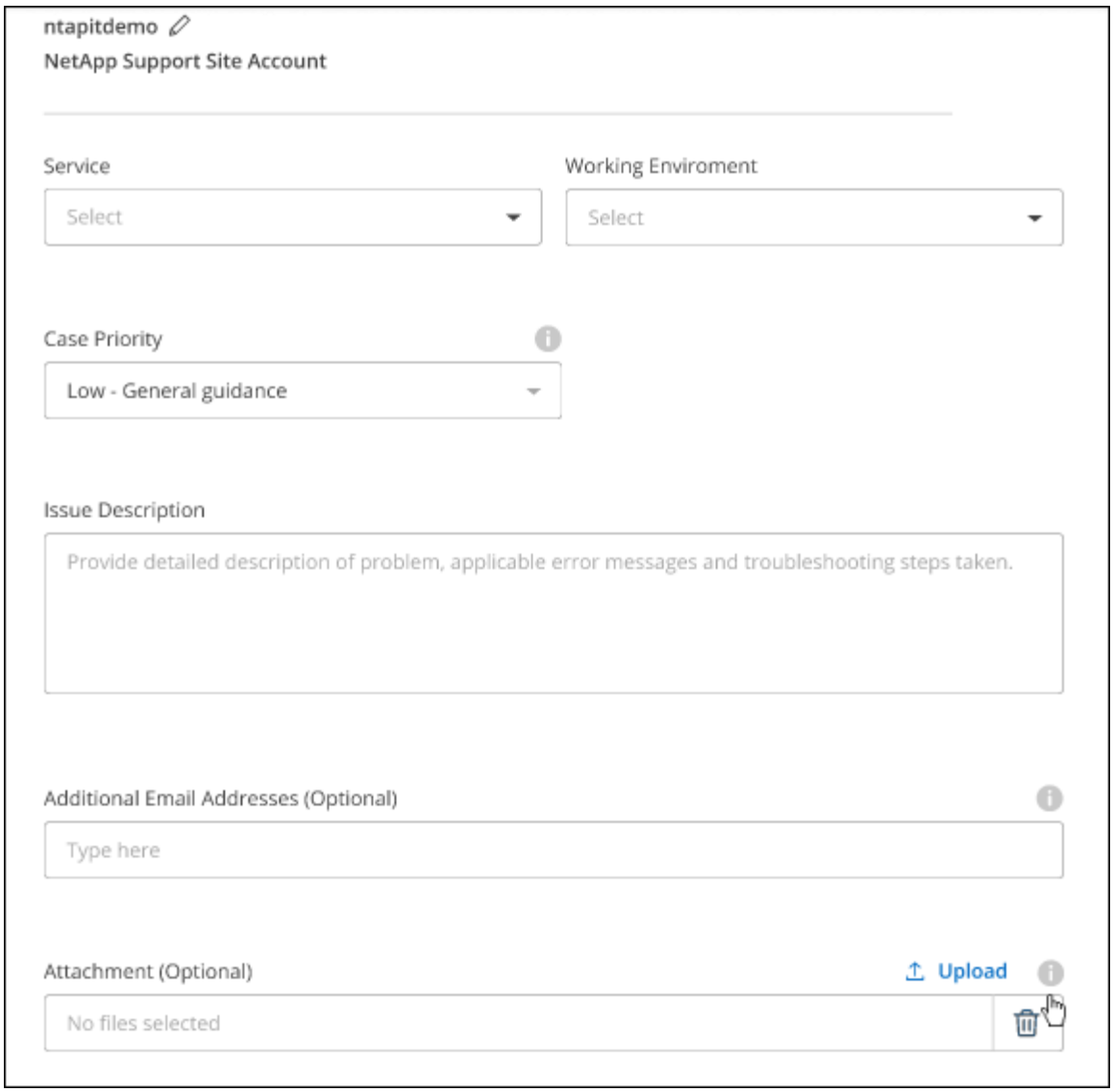
     L'elenco dei sistemi rientra nell'ambito dell'organizzazione della Console e dell'agente della Console selezionato nel banner in alto.

   - **Priorità del caso**: scegli la priorità del caso, che può essere Bassa, Media, Alta o Critica.

     Per saperne di più su queste priorità, passa il mouse sull'icona informativa accanto al nome del campo.

   - **Descrizione del problema**: fornisci una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o passaggi per la risoluzione dei problemi eseguiti.
   - **Indirizzi email aggiuntivi**: inserisci altri indirizzi email se desideri informare qualcun altro di questo problema.
   - **Allegato (facoltativo)**: carica fino a cinque allegati, uno alla volta.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Dopo aver finito

Apparirà una finestra pop-up con il numero del tuo caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei tuoi casi di supporto, puoi selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzarne i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso contro il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società registrata a cui è associato non corrispondono alla stessa società registrata per il numero di serie dell'account NetApp Console (ad esempio 960xxxx) o il numero di serie dell'ambiente di lavoro. Puoi richiedere assistenza utilizzando una delle seguenti opzioni:

- Invia un caso non tecnico a https://mysupport.netapp.com/site/help

Gestisci i tuoi casi di supporto

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente dalla Console. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

Notare quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base al tuo account NSS utente.

  I risultati nella tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come Priorità e Stato. Altre colonne forniscono solo funzionalità di ordinamento.

  Per maggiori dettagli, vedere i passaggi riportati di seguito.
- A livello di singolo caso, offriamo la possibilità di aggiornare le note del caso o di chiudere un caso che non sia già nello stato Chiuso o In attesa di chiusura.

Passi

1. Nella NetApp Console, seleziona **Guida > Supporto**.
2. Seleziona **Gestione casi** e, se richiesto, aggiungi il tuo account NSS alla Console.

   La pagina **Gestione casi** mostra i casi aperti relativi all'account NSS associato al tuo account utente della Console. Si tratta dello stesso account NSS che appare in cima alla pagina **Gestione NSS**.
3. Facoltativamente, modifica le informazioni visualizzate nella tabella:
   - In **Casi dell'organizzazione**, seleziona **Visualizza** per visualizzare tutti i casi associati alla tua azienda.
   - Modifica l'intervallo di date scegliendo un intervallo di date esatto o un intervallo di tempo diverso.
   - Filtra il contenuto delle colonne.
   - Modifica le colonne che appaiono nella tabella selezionando e quindi scegli le colonne che desideri visualizzare.
4. Gestisci un caso esistente selezionando e selezionando una delle opzioni disponibili:
   - **Visualizza caso**: visualizza i dettagli completi su un caso specifico.
   - **Aggiorna note sul caso**: fornisci ulteriori dettagli sul tuo problema o seleziona **Carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Chiudi caso**: fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politica sulla riservatezza

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

"Avviso per NetApp Disaster Recovery"