Documentazione di disaster recovery di BlueXP

BlueXP disaster recovery

NetApp
July 25, 2025

Sommario

Documentazione di disaster recovery di BlueXP . . . 1
Note di rilascio . . . 2
Novità di disaster recovery BlueXP . . . 2
14 luglio 2025 . . . 2
30 giugno 2025 . . . 3
23 giugno 2025 . . . 3
9 giugno 2025 . . . 3
13 maggio 2025 . . . 3
16 aprile 2025 . . . 5
10 marzo 2025 . . . 6
19 febbraio 2025 . . . 6
30 ottobre 2024 . . . 7
20 settembre 2024 . . . 8
2 agosto 2024 . . . 9
17 luglio 2024 . . . 9
5 luglio 2024 . . . 10
15 maggio 2024 . . . 11
5 marzo 2024 . . . 11
1 febbraio 2024 . . . 12
11 gennaio 2024 . . . 13
20 ottobre 2023 . . . 13
27 settembre 2023 . . . 13
1 agosto 2023 . . . 14
18 maggio 2023 . . . 15
Limitazioni nel ripristino di emergenza di BlueXP . . . 15
Attendere il completamento del failback prima di eseguire il rilevamento . . . 15
BlueXP potrebbe non scoprire Amazon FSX per NetApp ONTAP . . . 15
Inizia subito . . . 17
Scopri le funzionalità di disaster recovery di BlueXP per VMware . . . 17
Vantaggi dell’utilizzo di BlueXP per il disaster recovery per VMware . . . 18
Cosa puoi fare con il disaster recovery BlueXP per VMware . . . 18
Costo . . . 19
Licensing . . . 19
prova gratuita di 30 giorni . . . 20
Come funziona il disaster recovery di BlueXP . . . 20
Termini e condizioni per il disaster recovery di BlueXP . . . 22
Prerequisiti per il disaster recovery di BlueXP . . . 22
Prerequisiti per lo storage ONTAP . . . 22
Prerequisiti dei cluster VMware vCenter . . . 22
Prerequisiti di BlueXP . . . 23
Prerequisiti dei carichi di lavoro . . . 24
Avvio rapido del disaster recovery di BlueXP . . . 24
Configura l’infrastruttura per il disaster recovery di BlueXP . . . 24

Preparati al disaster recovery con BlueXP per la protezione on-premise . . . 25
Preparati al disaster recovery di BlueXP per la protezione on-premise nel cloud con AWS . . . 25
Accedi al disaster recovery di BlueXP . . . 26
Imposta le licenze per il disaster recovery di BlueXP . . . 27
Provalo con una prova gratuita di 30 giorni . . . 28
Al termine della prova, iscriviti attraverso AWS Marketplace . . . 29
Al termine della prova, acquista una licenza BYOL tramite NetApp . . . 29
Aggiorna la tua licenza BlueXP alla scadenza . . . 30
Termina la prova gratuita . . . 30
Domande frequenti sul disaster recovery di BlueXP . . . 31
USA il disaster recovery di BlueXP . . . 33
USA la panoramica sul disaster recovery di BlueXP . . . 33
Visualizza lo stato di integrità dei tuoi piani di disaster recovery BlueXP sulla Dashboard . . . 33
Aggiungere vCenter a un sito nel ripristino di emergenza di BlueXP . . . 35
Aggiungere la mappatura della subnet per un sito vCenter . . . 37
Modificare il sito del server vCenter e personalizzare la pianificazione del rilevamento . . . 39
Aggiornare la ricerca manualmente . . . 41
Crea un gruppo di risorse per organizzare insieme le VM nel ripristino di emergenza di BlueXP . . . 42
Creare un piano di replicazione nel ripristino di emergenza di BlueXP . . . 45
Creare il piano . . . 46
Modificare le pianificazioni per verificare la conformità e garantire il funzionamento dei test di failover . . . 55
Replica le applicazioni su un altro sito con il ripristino di emergenza di BlueXP . . . 57
Migrazione delle applicazioni su un altro sito con il ripristino di emergenza di BlueXP . . . 58
Eseguire il failover delle applicazioni su un sito remoto con il ripristino di emergenza BlueXP . . . 58
Verificare il processo di failover . . . 59
Ripulire l'ambiente di test dopo un test di failover . . . 60
Esegui il failover del sito di origine su un sito di disaster recovery . . . 60
Ripristina le applicazioni alla fonte originale con il ripristino di emergenza BlueXP . . . 61
Gestisci siti, gruppi di risorse, piani di replica, datastore e informazioni sulle macchine virtuali con il disaster recovery di BlueXP . . . 62
Gestire i siti vCenter . . . 63
Gestire i gruppi di risorse . . . 63
Gestire i piani di replica . . . 63
Visualizzare informazioni sui datastore . . . 66
Visualizzare le informazioni sulle macchine virtuali . . . 67
Monitorare i processi di disaster recovery di BlueXP . . . 67
Visualizzare i lavori . . . 67
Annullare un lavoro . . . 67
Crea report di ripristino di emergenza BlueXP . . . 68
Riferimento . . . 69
Privilegi vCenter necessari per il disaster recovery di BlueXP . . . 69
Accesso basato sui ruoli BlueXP disaster recovery alle funzionalità . . . 71
Utilizza il disaster recovery di BlueXP con Amazon EVS . . . 72
Introduzione del disaster recovery di BlueXP tramite Amazon Elastic VMware Service e Amazon FSx per NetApp ONTAP . . . 72

Panoramica della soluzione di disaster recovery di BlueXP tramite Amazon EVS e Amazon FSs per NetApp ONTAP . . . 73
Installa il connettore BlueXP per il ripristino di emergenza di BlueXP . . . 75
Configurare il disaster recovery di BlueXP per Amazon EVS . . . 75
Creare piani di replicazione per Amazon EVS . . . 87
Eseguire operazioni di piano di replicazione con il ripristino di emergenza BlueXP . . . 100
Conoscenza e supporto . . . 113
Registrati per ricevere assistenza . . . 113
Panoramica sulla registrazione del supporto . . . 113
Registrare BlueXP per ricevere assistenza NetApp . . . 113
Associare le credenziali NSS per il supporto Cloud Volumes ONTAP . . . 116
Richiedi assistenza . . . 117
Ottieni supporto per un file service del cloud provider . . . 117
Utilizzare le opzioni di supporto automatico . . . 118
Crea un caso con il supporto NetApp . . . 118
Gestire i casi di supporto (anteprima) . . . 120
Note legali . . . 123
Copyright . . . 123
Marchi . . . 123
Brevetti . . . 123
Direttiva sulla privacy . . . 123
Open source . . . 123

Documentazione di disaster recovery di BlueXP

Note di rilascio

Novità di disaster recovery BlueXP

Scopri le novità del disaster recovery BlueXP.

14 luglio 2025

Versione 4.2.5

Ruoli utente nel BlueXP disaster recovery

Il BlueXP disaster recovery ora utilizza ruoli per gestire l'accesso di ciascun utente a specifiche funzionalità e azioni.

Il servizio utilizza i seguenti ruoli specifici per il BlueXP disaster recovery.

- **Amministratore del ripristino di emergenza**: esegue qualsiasi azione nel BlueXP disaster recovery.
- **Amministratore del failover del disaster recovery**: esegue azioni di failover e migrazione nel BlueXP 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 nel BlueXP disaster recovery, ma non può eseguire alcuna azione.

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

Per ulteriori informazioni, vedere "Ruoli utente e autorizzazioni nel BlueXP disaster recovery".

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

Altri aggiornamenti nel BlueXP disaster recovery

- Rilevamento della 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 e nella gestione del pool di vCenter SDK
- Gestione dei dati obsoleti alla prossima individuazione programmata o manuale:
  - Quando una VM viene eliminata in vCenter, la BlueXP disaster recovery ora la rimuove automaticamente dal piano di replica.
  - Quando un datastore o una rete vengono eliminati in vCenter, la BlueXP 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, la BlueXP disaster recovery lo elimina ora dal piano di replica e dal gruppo di risorse.

- Ora puoi accedere alla documentazione di Swagger in modalità di navigazione in incognito. Puoi accedervi da BlueXP disaster recovery tramite l'opzione Impostazioni > Documentazione API o direttamente al seguente URL in modalità di navigazione in incognito: "Documentazione Swagger" .
- In alcune situazioni, dopo un'operazione di failback, l'iGroup veniva lasciato indietro al termine dell'operazione. Questo aggiornamento rimuove l'iGroup se è obsoleto.
- Se il nome di dominio completo NFS è stato utilizzato nel piano di replica, il BlueXP 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 disaster recovery.
- Miglioramenti dell'allineamento dell'interfaccia utente
- Miglioramenti del registro per acquisire i dettagli delle dimensioni di vCenter dopo la scoperta riuscita

30 giugno 2025

Versione 4.2.4P2

Miglioramenti della scoperta

Questo aggiornamento migliora il processo di individuazione, riducendone i tempi necessari.

23 giugno 2025

Versione 4.2.4P1

Miglioramenti della mappatura delle subnet

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

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

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

13 maggio 2025

Versione 4.2.3

Mappatura subnet

Con questa release, è possibile gestire gli indirizzi IP in caso di failover in un nuovo modo utilizzando la mappatura delle subnet, che consente di aggiungere sottoreti per ogni vCenter. In tal caso, definire IPv4 CIDR,

il gateway predefinito e il DNS per ogni rete virtuale.

In caso di failover, BlueXP Disaster Recovery determina l'indirizzo IP appropriato di ogni vNIC guardando il CIDR fornito per la rete virtuale mappata e la utilizza per derivare il nuovo indirizzo IP.

Ad esempio:

- Rete a = 10,1.1.0/24
- Rete B = 192.168.1.0/24

VM1 dispone di una vNIC (10,1.1,50) collegata a NetworkA. NetworkA viene mappato su NetworkB nelle impostazioni del piano di replica.

In caso di failover, il disaster recovery di BlueXP sostituisce la parte Network dell'indirizzo IP originale (10,1.1) e mantiene l'indirizzo host (.50) dell'indirizzo IP originale (10,1.1,50). Per VM1, BlueXP 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.

Riassumendo, l'indirizzo dell'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 al momento del failover, specialmente se si devono gestire centinaia di reti e migliaia di macchine virtuali.

Per ulteriori informazioni sull'inclusione della mappatura delle subnet nei siti, fare riferimento a "Aggiungere i siti del server vCenter".

Protezione di salto

È ora possibile ignorare la protezione in modo che il servizio non crei automaticamente una relazione di protezione inversa dopo il failover di un piano di replica. Questa funzione è utile se si desidera eseguire operazioni aggiuntive sul sito ripristinato prima di riportarlo online all'interno del disaster recovery di BlueXP .

All'avvio di un failover, per impostazione predefinita il servizio crea automaticamente una relazione di protezione inversa per ogni volume del piano di replica, se il sito di origine è online. Questo significa che il servizio crea una relazione SnapMirror dal sito di destinazione al sito di origine. Inoltre, il servizio inverte automaticamente la relazione SnapMirror quando si avvia un failback.

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

Una volta che il sito di origine è tornato in linea, è possibile stabilire la protezione inversa selezionando **Proteggi risorse** dal menu azioni piano di replica. Questo tenta di creare una relazione di replica inversa per ogni volume nel piano. È possibile eseguire questo processo ripetutamente fino a quando non viene ripristinata la protezione. Una volta ripristinata la protezione, è possibile avviare un failback nel modo usuale.

Per ulteriori dettagli sulla protezione da saltare, fare riferimento alla "Eseguire il failover delle applicazioni in un sito remoto".

SnapMirror pianifica gli aggiornamenti nel piano di replica

Il disaster recovery di BlueXP ora supporta l'utilizzo di soluzioni di gestione delle snapshot esterne, come lo scheduler nativo delle policy ONTAP SnapMirror o integrazioni di terze parti con ONTAP. Se ogni datastore (volume) nel piano di replica dispone già di una relazione SnapMirror che viene gestita altrove, puoi utilizzare tali snapshot come punti di recovery nel disaster recovery di BlueXP .

Per configurare, nella sezione piano di replica > mappatura delle risorse, selezionare la casella di controllo **utilizza piani di backup gestiti dalla piattaforma e piani di conservazione** durante la configurazione della mappatura degli archivi dati.

Quando l'opzione è selezionata, il ripristino di emergenza BlueXP non configura una pianificazione di backup. Tuttavia, è comunque necessario configurare un piano di conservazione, perché potrebbe essere ancora necessario creare snapshot per le operazioni di test, failover e failback.

Dopo la configurazione, il servizio non acquisisce istantanee pianificate regolarmente, ma si affida all'entità esterna per acquisire e aggiornare tali istantanee.

Per informazioni dettagliate sull'utilizzo di soluzioni snapshot esterne nel piano di replica, fare riferimento a "Creare un piano di replica".

16 aprile 2025

Versione 4.2.2

Rilevamento pianificato per le VM

Il disaster recovery di BlueXP esegue il rilevamento ogni 24 ore. Con questa release, è ora possibile personalizzare la pianificazione delle rilevazioni in modo da soddisfare le proprie esigenze e ridurre l'impatto sulle prestazioni quando necessario. Ad esempio, se si dispone di un numero elevato di macchine virtuali, è possibile impostare la pianificazione del rilevamento in modo che venga eseguita ogni 48 ore. Se si dispone di un numero limitato di macchine virtuali, è possibile impostare la pianificazione del rilevamento in modo che venga eseguita ogni 12 ore.

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

Per ulteriori informazioni, fare riferimento alla "Aggiungere i siti del server vCenter".

Supporto archivio dati gruppo di risorse

In precedenza, era possibile creare gruppi di risorse solo per macchine virtuali. Con questa release, puoi creare un gruppo di risorse per datastore. Quando si crea un piano di replica e si crea un gruppo di risorse per tale piano, vengono elencate tutte le macchine virtuali in un datastore. Ciò è utile se si dispone di un numero elevato di macchine virtuali e si desidera raggrupparle per datastore.

È possibile creare un gruppo di risorse con un archivio dati 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 replica e si crea un gruppo di risorse all'interno del piano, è possibile visualizzare le macchine virtuali negli archivi dati.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Notifiche di prova gratuita o scadenza della licenza

Questa versione fornisce notifiche che la versione di prova gratuita scadrà tra 60 giorni per assicurarsi di avere il tempo di ottenere una licenza. Questa versione fornisce inoltre notifiche il giorno della scadenza della licenza.

Notifica degli aggiornamenti del servizio

Con questa versione, nella parte superiore viene visualizzato un banner per indicare che i servizi sono in fase di aggiornamento e che il servizio è in modalità di manutenzione. Il banner viene visualizzato quando il servizio è in fase di aggiornamento e scompare al termine dell'aggiornamento. Mentre è possibile continuare a lavorare nell'interfaccia utente mentre è in corso l'aggiornamento, non è possibile inoltrare nuovi lavori. I processi pianificati vengono eseguiti al termine dell'aggiornamento e il servizio torna alla modalità di produzione.

10 marzo 2025

Versione 4.2.1

Supporto proxy intelligente

Il connettore BlueXP supporta il proxy intelligente. Il proxy intelligente è un modo leggero, sicuro ed efficiente per connettere l'ambiente on-premise al servizio BlueXP . Fornisce una connessione sicura tra l'ambiente e il servizio BlueXP senza richiedere una VPN o un accesso diretto a Internet. Questa implementazione proxy ottimizzata alleggerisce il traffico API all'interno della rete locale.

Quando viene configurato un proxy, BlueXP disaster recovery tenta di comunicare direttamente con VMware o ONTAP e utilizza il proxy configurato in caso di errore della comunicazione diretta.

L'implementazione del proxy per il disaster recovery di BlueXP richiede la comunicazione della porta 443 tra il connettore e qualsiasi server vCenter e array ONTAP utilizzando un protocollo HTTPS. L'agente di disaster recovery BlueXP all'interno del connettore comunica direttamente con VMware vSphere, VC o ONTAP durante l'esecuzione di qualsiasi azione.

Per ulteriori informazioni sul proxy intelligente per il ripristino di emergenza BlueXP , vedere "Configura l'infrastruttura per il disaster recovery di BlueXP".

Per ulteriori informazioni sulla configurazione generale del proxy in BlueXP , vedere "Configurare un connettore per l'utilizzo di un server proxy".

Termina la prova gratuita in qualsiasi momento

È possibile interrompere la prova gratuita a qualsiasi dente o attendere la scadenza.

Vedere "Termina la prova gratuita".

19 febbraio 2025

Versione 4,2

Supporto di ASA R2 per macchine virtuali e datastore su storage VMFS

Questa versione di BlueXP Disaster Recovery fornisce supporto per ASA R2 per macchine virtuali e datastore sullo storage VMFS. In un sistema ASA R2, il software ONTAP supporta le funzionalità SAN essenziali, mentre rimuove le funzioni non supportate negli ambienti SAN.

Questa versione supporta le seguenti funzioni per ASA R2:

- Provisioning di gruppi di coerenza per lo storage primario (solo gruppo di coerenza flat, ovvero solo un livello senza struttura gerarchica)
- Operazioni di backup (gruppo di coerenza) inclusa l'automazione SnapMirror

Il supporto per ASA R2 nel disaster recovery di BlueXP utilizza ONTAP 9.16.1.

Mentre i datastore possono essere montati su un volume ONTAP o su un'unità storage ASA R2, un gruppo di risorse nel disaster recovery di BlueXP non può includere un datastore di ONTAP e un datastore di ASA R2. È possibile selezionare un datastore da ONTAP o da ASA R2 in un gruppo di risorse.

30 ottobre 2024

Creazione di report

Ora puoi generare e scaricare report per analizzare il tuo scenario. I report preprogettati riassumono i failover e i failback, mostrano i dettagli di replica su tutti i siti e mostrano i dettagli dei processi degli ultimi sette giorni.

Fare riferimento alla "Creare report di disaster recovery".

prova gratuita di 30 giorni

Ora puoi iscriverti a una prova gratuita di 30 giorni del disaster recovery di BlueXP . In precedenza, le versioni di prova gratuite erano per 90 giorni.

Fare riferimento alla "Impostare la licenza".

Disabilitare e abilitare i piani di replica

Una release precedente includeva aggiornamenti alla struttura di pianificazione dei test di failover, necessari per supportare le pianificazioni giornaliere e settimanali. Questo aggiornamento richiede la disattivazione e la riattivazione di tutti i piani di replica esistenti in modo da poter utilizzare le nuove pianificazioni dei test di failover giornalieri e settimanali. Questo è un requisito una tantum.

Ecco come:

1. Dal menu superiore, selezionare **piani di replica**.
2. Selezionare un piano e selezionare l'icona azioni per visualizzare il menu a discesa.
3. Selezionare **Disable** (Disattiva).
4. Dopo alcuni minuti, selezionare **Abilita**.

Mappatura delle cartelle

Quando si crea un piano di replica e si mappano le risorse di calcolo, è ora possibile mappare le cartelle in modo che le macchine virtuali vengano recuperate in una cartella specificata per il data center, il cluster e l'host.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Dettagli VM disponibili per failover, failback e test failover

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

Fare riferimento alla "Eseguire il failover delle applicazioni in un sito remoto".

Ritardo di avvio VM con sequenza di avvio ordinata

Quando si crea un piano di replica, è ora possibile impostare un ritardo di avvio per ciascuna VM del piano. In questo modo è possibile impostare una sequenza per l'avvio delle macchine virtuali per garantire che tutte le macchine virtuali con priorità 1 vengano eseguite prima dell'avvio delle macchine virtuali con priorità successiva.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Informazioni sul sistema operativo VM

Quando si crea un piano di replica, è ora possibile vedere il sistema operativo per ciascuna VM nel piano. Ciò è utile per decidere come raggruppare le VM in un gruppo di risorse.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Aliasing nome VM

Quando si crea un piano di replica, è ora possibile aggiungere un prefisso e un suffisso ai nomi delle macchine virtuali sul ripristino di emergenza SIT. Ciò consente di utilizzare un nome più descrittivo per le macchine virtuali nel piano.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Pulire le vecchie istantanee

Puoi eliminare snapshot non più necessarie oltre il numero di conservazione specificato. Gli snapshot possono accumularsi nel tempo quando si riduce il numero di conservazione degli snapshot, quindi è possibile rimuoverli per liberare spazio. È possibile eseguire questa operazione in qualsiasi momento on-demand o quando si elimina un piano di replica.

Per ulteriori informazioni, fare riferimento alla "Gestisci siti, gruppi di risorse, piani di replica, datastore e informazioni sulle macchine virtuali".

Riconciliare le istantanee

È ora possibile riconciliare gli snapshot non sincronizzati tra origine e destinazione. Questo può verificarsi se le snapshot vengono eliminate su una destinazione al di fuori del disaster recovery di BlueXP . Il servizio elimina automaticamente lo snapshot sulla sorgente ogni 24 ore. Tuttavia, è possibile eseguire questa operazione su richiesta. Questa funzione consente di garantire la coerenza delle istantanee in tutti i siti.

Per ulteriori informazioni, fare riferimento alla "Gestire i piani di replica".

20 settembre 2024

Supporto per datastore VMFS VMware on-premise e on-premise

Questa release include il supporto per le VM montate su datastore VMFS (Virtual Machine file System) di VMware vSphere per iSCSI e FC protetti nello storage on-premise. In precedenza, il servizio forniva un'anteprima *tecnologica* che supportava datastore VMFS per iSCSI e FC.

Di seguito sono riportate alcune considerazioni aggiuntive sui protocolli iSCSI e FC:

- Il supporto FC è per i protocolli front-end dei client, non per la replica.

- Il disaster recovery di BlueXP 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 macchine virtuali protette. Ad esempio, se l'origine utilizza un protocollo FC, la destinazione deve utilizzare anche FC.

2 agosto 2024

Supporto per datastore VMFS VMware on-premise e on-premise per FC

Questa release include un'anteprima *tecnologica* del supporto per le macchine virtuali montate su datastore VMFS (Virtual Machine file System) VMware vSphere per FC protetti nello storage on-premise. In precedenza, il servizio forniva un'anteprima tecnologica che supportava gli archivi dati VMFS per iSCSI.

NetApp non ti addebita alcun costo per la capacità dei workload in anteprima.

Annullamento del processo

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

Fare riferimento alla "Monitorare i lavori".

17 luglio 2024

Pianificazioni dei test di failover

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

Ecco come:

1. Dal menu superiore, selezionare **piani di replica**.
2. Selezionare un piano e selezionare l'icona azioni per visualizzare il menu a discesa.
3. Selezionare **Disable** (Disattiva).
4. Dopo alcuni minuti, selezionare **Abilita**.

Aggiornamenti del piano di replica

Questa versione include aggiornamenti ai dati del piano di replica, che risolve un problema di "istantanea non trovata". Ciò richiede la modifica del conteggio di conservazione in tutti i piani di replica a 1 e l'avvio di uno snapshot on-demand. Questo processo crea un nuovo backup e rimuove tutti i backup precedenti.

Ecco come:

1. Dal menu superiore, selezionare **piani di replica**.
2. Selezionare il piano di replica, fare clic sulla scheda **mappatura di failover** e fare clic sull'icona **Modifica** matita.
3. Fare clic sulla freccia **Datastores** per espanderla.

4. Annotare il valore del conteggio di conservazione nel piano di replica. Sarà necessario ripristinare questo valore originale al termine di questi passaggi.
5. Ridurre il conteggio a 1.
6. Avvia una snapshot on-demand. A tale scopo, nella pagina piano di replica, selezionare il piano, fare clic sull'icona azioni e selezionare **scatta istantanea adesso**.
7. Una volta completato correttamente il processo snapshot, aumentare il conteggio nel piano di replica riportandolo al valore originale annotato nel primo passo.
8. Ripetere questi passaggi per tutti i piani di replica esistenti.

5 luglio 2024

Questa release di disaster recovery di BlueXP include i seguenti aggiornamenti:

Supporto per AFF serie A.

Questa versione supporta le piattaforme hardware NetApp AFF serie A.

Supporto per datastore VMFS VMware on-premise e on-premise

Questa release include un'anteprima *tecnologica* del supporto per le macchine virtuali montate su datastore VMFS (Virtual Machine file System) VMware vSphere, protetti nello storage on-premise. Con questa release, il disaster recovery è supportato in un'anteprima tecnologica per i carichi di lavoro VMware on-premise nell'ambiente VMware on-premise con datastore VMFS.

NetApp non ti addebita alcun costo per la capacità dei workload in anteprima.

Aggiornamenti del piano di replica

Puoi aggiungere un piano di replica più facilmente filtrando le macchine virtuali in base all'archivio dati nella pagina applicazioni e selezionando ulteriori dettagli sulla destinazione nella pagina mappatura delle risorse. Fare riferimento alla "Creare un piano di replica".

Modificare i piani di replica

Con questa versione, la pagina mappature di failover è stata migliorata per una maggiore chiarezza.

Fare riferimento alla "Gestire i piani".

Modificare le VM

Con questa versione, il processo di modifica delle macchine virtuali nel piano includeva alcuni piccoli miglioramenti dell'interfaccia utente.

Fare riferimento alla "Gestire le VM".

Eseguire il failover degli aggiornamenti

Prima di avviare un failover, è ora possibile determinare lo stato delle macchine virtuali e se sono accese o spente. Il processo di failover ti consente ora di creare una snapshot o di sceglierne una.

Fare riferimento alla "Eseguire il failover delle applicazioni in un sito remoto".

Pianificazioni dei test di failover

È ora possibile modificare i test di failover e impostare pianificazioni giornaliere, settimanali e mensili per il test di failover.

Fare riferimento alla "Gestire i piani".

Aggiornamento delle informazioni sui prerequisiti

Le informazioni sui prerequisiti per il ripristino di emergenza di BlueXP sono state aggiornate.

Fare riferimento alla "Prerequisiti per il disaster recovery di BlueXP".

15 maggio 2024

Questa release di disaster recovery di BlueXP include i seguenti aggiornamenti:

Replica dei workload VMware da on-premise a on-premise

Questa funzione è ora disponibile come funzione di disponibilità generale. In precedenza, si trattava di un'anteprima tecnologica con funzionalità limitate.

Aggiornamenti delle licenze

Con il disaster recovery di BlueXP , puoi iscriverti a 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 ottieni dal tuo rappresentante di vendita NetApp o dal sito di supporto NetApp (NSS).

Per ulteriori informazioni sulla configurazione delle licenze per il disaster recovery di BlueXP, fare riferimento a. "Impostare la licenza".

"Scopri di più sul disaster recovery di BlueXP".

5 marzo 2024

Questa è la release General Availability del disaster recovery di BlueXP, che include i seguenti aggiornamenti.

Aggiornamenti delle licenze

Con il disaster recovery di BlueXP , puoi iscriverti a una versione di prova gratuita di 90 giorni o a Bring Your Own License (BYOL), che è un file di licenza NetApp (NLF) che ottieni dal tuo rappresentante di vendita NetApp Puoi utilizzare il numero di serie della licenza per attivare il BYOL nel Digital Wallet di BlueXP. Le spese per il disaster recovery di BlueXP si basano sulla capacità di provisioning dei datastore.

Per ulteriori informazioni sulla configurazione delle licenze per il disaster recovery di BlueXP, fare riferimento a. "Impostare la licenza".

Per informazioni dettagliate sulla gestione delle licenze per **tutti** i servizi BlueXP, fare riferimento a. "Gestisci le licenze per tutti i servizi BlueXP".

Modificare le pianificazioni

Con questa versione, è ora possibile impostare le pianificazioni per verificare la conformità e i test di failover in modo da garantire che funzionino correttamente in caso di necessità.

Per ulteriori informazioni, fare riferimento a. "Creare il piano di replica".

1 febbraio 2024

Questa release di anteprima del disaster recovery di BlueXP include i seguenti aggiornamenti:

Potenziamento della rete

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

- DHCP: Se si sceglie questa opzione, si forniscono le credenziali per la macchina virtuale.
- Static IP (IP statico): È possibile selezionare informazioni identiche o diverse dalla macchina virtuale di origine. Se si sceglie lo stesso come origine, non è necessario immettere le credenziali. D'altro canto, se si sceglie di utilizzare informazioni diverse dall'origine, è possibile fornire le credenziali, l'indirizzo IP, la maschera di sottorete, il DNS e le informazioni sul gateway.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Script personalizzati

Può ora essere incluso come processi successivi al failover. Grazie agli script personalizzati, puoi fare in modo che il disaster recovery di BlueXP esegua lo script dopo un processo di failover. Ad esempio, è possibile utilizzare uno script personalizzato per riprendere tutte le transazioni del database al termine del failover.

Per ulteriori informazioni, fare riferimento a. "Failover su un sito remoto".

Relazione di SnapMirror

È ora possibile creare una relazione SnapMirror durante lo sviluppo del piano di replica. In precedenza, era necessario creare una relazione al di fuori del disaster recovery di BlueXP.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Gruppi di coerenza

Quando crei un piano di replica, puoi includere macchine virtuali provenienti da diversi volumi e SVM diverse. Il disaster recovery di BlueXP crea una snapshot del gruppo di coerenza includendo tutti i volumi e aggiornando tutte le posizioni secondarie.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Opzione ritardo accensione VM

Quando si crea un piano di replica, è possibile aggiungere VM a un gruppo di risorse. Con gruppi di risorse, è possibile impostare un ritardo su ciascuna VM in modo che si accenda in una sequenza ritardata.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

Copie Snapshot coerenti con l'applicazione

È possibile specificare se creare copie Snapshot coerenti con l'applicazione. Il servizio disattiverà l'applicazione e quindi eseguirà un'istantanea per ottenere uno stato coerente dell'applicazione.

Per ulteriori informazioni, fare riferimento a. "Creare un piano di replica".

11 gennaio 2024

Questa release di anteprima del disaster recovery di BlueXP include i seguenti aggiornamenti:

Dashboard più rapidamente

Con questa versione, è possibile accedere più rapidamente alle informazioni presenti in altre pagine dal dashboard.

"Scopri di più sul disaster recovery di BlueXP".

20 ottobre 2023

Questa versione di anteprima del disaster recovery di BlueXP include i seguenti aggiornamenti.

Proteggere i carichi di lavoro VMware on-premise basati su NFS

Ora con il disaster recovery di BlueXP, puoi proteggere i tuoi carichi di lavoro VMware on-premise basati su NFS dai disastri in un altro ambiente VMware on-premise basato su NFS, oltre al cloud pubblico. Il disaster recovery di BlueXP orchestra il completamento dei piani di disaster recovery.

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

"Scopri di più sul disaster recovery di BlueXP".

27 settembre 2023

Questa release di anteprima del disaster recovery di BlueXP include i seguenti aggiornamenti:

Aggiornamenti dashboard

È ora possibile fare clic sulle opzioni del dashboard, semplificando la revisione rapida delle informazioni. Inoltre, la dashboard ora mostra lo stato di failover e migrazioni.

Fare riferimento a. "Visualizzare lo stato dei piani di disaster recovery sul Dashboard".

Aggiornamenti del piano di replica

- **RPO**: È ora possibile inserire l'obiettivo del punto di ripristino (RPO) e il conteggio della conservazione nella sezione datastore del piano di replica. Indica la quantità di dati che deve esistere non più vecchia dell'ora impostata. Se, ad esempio, viene impostato su 5 minuti, il sistema può perdere fino a 5 minuti di dati in caso di disastro, senza influire sulle esigenze business-critical.

  Fare riferimento a. "Creare un piano di replica".

- **Miglioramenti al networking**: Quando si esegue il mapping del networking tra le posizioni di origine e di destinazione nella sezione macchine virtuali del piano di replica, il disaster recovery di BlueXP ora offre due opzioni: DHCP o IP statico. In precedenza era supportato solo DHCP. Per gli indirizzi IP statici, configurare la subnet, il gateway e i server DNS. Inoltre, è ora possibile immettere le credenziali per le macchine virtuali.

Fare riferimento a. "Creare un piano di replica".

- **Modifica pianificazioni**: È ora possibile aggiornare le pianificazioni dei piani di replica.

  Fare riferimento a. "Gestione delle risorse".

- **Automazione di SnapMirror**: Durante la creazione del piano di replica in questa release, è possibile definire la relazione di SnapMirror tra volumi di origine e di destinazione in una delle seguenti configurazioni:
  - da 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 replica".

1 agosto 2023

Anteprima disaster recovery BlueXP

L'anteprima del disaster recovery di BlueXP è un servizio di disaster recovery basato sul cloud che automatizza i flussi di lavoro di disaster recovery. Inizialmente, con l'anteprima del disaster recovery di BlueXP, puoi proteggere i tuoi workload VMware on-premise basati su NFS che eseguono lo storage NetApp in VMware Cloud (VMC) su AWS con Amazon FSX per ONTAP.

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

"Scopri di più sul disaster recovery di BlueXP".

Questa versione include i seguenti aggiornamenti:

I gruppi di risorse si aggiornano per l'ordine di avvio

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

Verifica della replica

Dopo aver creato il piano di disaster recovery o di replica, identificare la ricorrenza nella procedura guidata e avviare una replica in un sito di disaster recovery, ogni 30 minuti il disaster recovery di BlueXP verifica l'effettiva esecuzione della replica in base al piano. È possibile monitorare l'avanzamento nella pagina monitoraggio processi. Fare riferimento alla "Replicare le applicazioni in un altro sito".

Il piano di replica mostra le pianificazioni del trasferimento degli RPO (Recovery Point Objective)

Quando si crea un piano di ripristino di emergenza o di replica, si selezionano le VM. In questa release, ora puoi vedere lo SnapMirror associato a ciascuno dei volumi associati al datastore o alla macchina virtuale.

Inoltre, puoi vedere le pianificazioni del trasferimento RPO associate alla pianificazione SnapMirror. RPO consente di determinare se la pianificazione del backup è sufficiente per il ripristino dopo un evento disastroso. Fare riferimento alla "Creare un piano di replica".

Aggiornamento di Job Monitor

La pagina Job Monitor ora include un'opzione Aggiorna che consente di ottenere uno stato aggiornato delle operazioni. Fare riferimento alla "Monitorare i processi di disaster recovery".

18 maggio 2023

Questa è la versione iniziale del disaster recovery di BlueXP.

Servizio di disaster recovery basato sul cloud

Il disaster recovery di BlueXP è un servizio di disaster recovery basato sul cloud che automatizza i flussi di lavoro di disaster recovery. Inizialmente, con l'anteprima del disaster recovery di BlueXP, puoi proteggere i tuoi workload VMware on-premise basati su NFS che eseguono lo storage NetApp in VMware Cloud (VMC) su AWS con Amazon FSX per ONTAP.

"Scopri di più sul disaster recovery di BlueXP".

Limitazioni nel ripristino di emergenza di BlueXP

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

Attendere il completamento del failback prima di eseguire il rilevamento

Al termine di un failover, non avviare manualmente il rilevamento sul vCenter di origine. Attendere il completamento del failback, quindi avviare il rilevamento sul vCenter di origine.

BlueXP potrebbe non scoprire Amazon FSX per NetApp ONTAP

A volte, BlueXP non rileva Amazon FSX per i cluster NetApp ONTAP. Ciò potrebbe essere dovuto al fatto che le credenziali di FSX non erano corrette.

Soluzione alternativa: Aggiungere il cluster Amazon FSX per NetApp ONTAP in BlueXP e aggiornare periodicamente il cluster per visualizzare eventuali modifiche.

Se devi rimuovere il cluster ONTAP FSX dal servizio di disaster recovery BlueXP, completa i seguenti passaggi:

1. Nel connettore BlueXP, usa le opzioni di connettività del tuo cloud provider, connettiti alla macchina virtuale Linux su cui è eseguito il connettore, riavvia il servizio "occm" usando l' `docker restart occm` comando.

   Fare riferimento a. "Gestire i connettori esistenti".

2. In BlueXP Canvas, Aggiungi nuovamente l'ambiente Amazon FSX per ONTAP e fornisci le credenziali FSX.

   Fare riferimento a. "Crea un file system Amazon FSX per NetApp ONTAP".

3. Dal disaster recovery di BlueXP, selezionare **Siti**, nella riga di vCenter selezionare l'opzione **azioni**  E dal menu azioni, selezionare **Aggiorna** per aggiornare la ricerca FSX in BlueXP Disaster Recovery.

   In questo modo viene riscoperto il datastore, le macchine virtuali e la relazione di destinazione.

Inizia subito

Scopri le funzionalità di disaster recovery di BlueXP per VMware

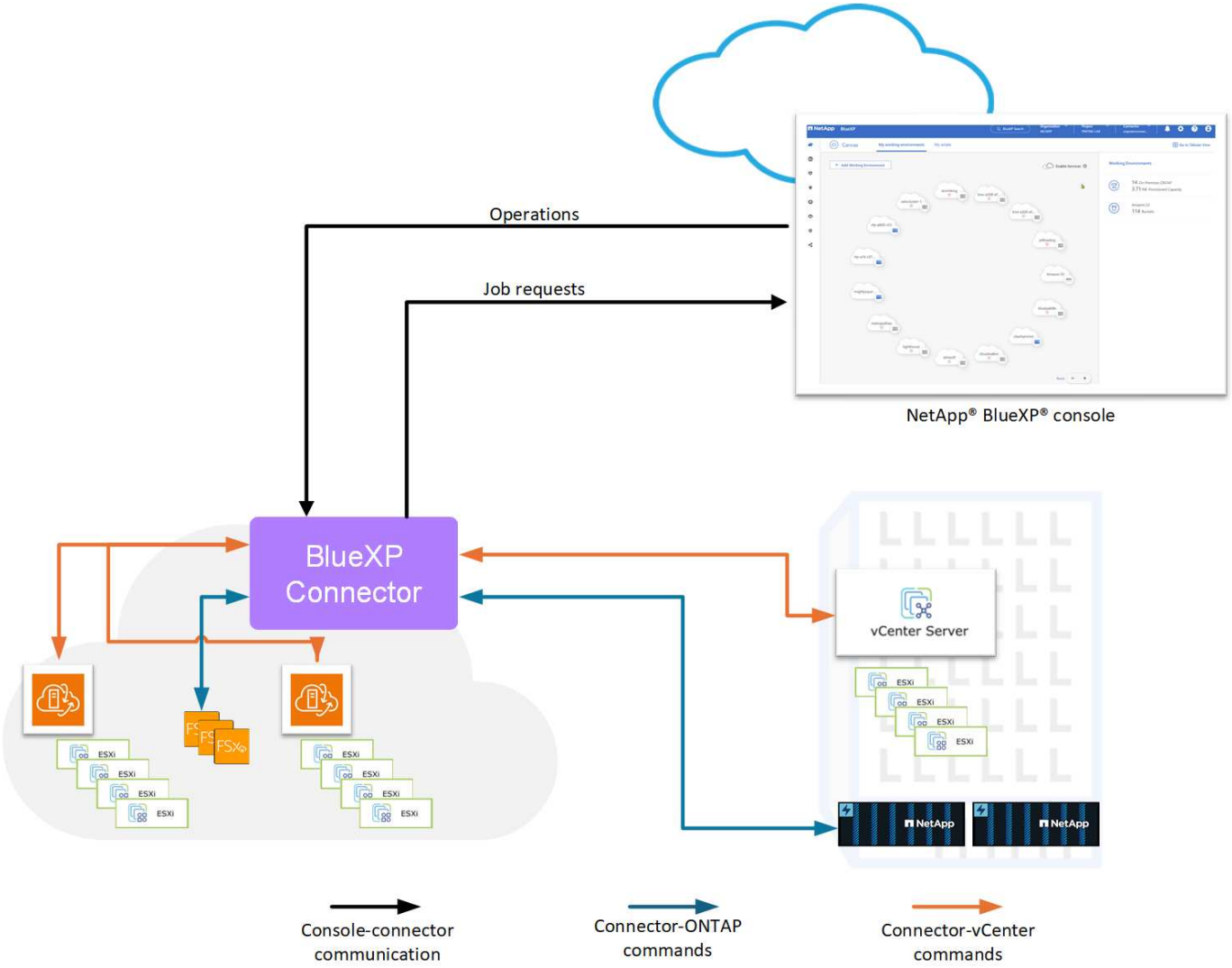
Il disaster recovery nel cloud rappresenta un modo conveniente e resiliente per proteggere i carichi di lavoro da fuori servizio del sito e eventi di corruzione dei dati. Con il disaster recovery di BlueXP per VMware, puoi replicare i carichi di lavoro di datastore o macchine virtuali VMware on-premise che eseguono lo storage ONTAP su un data center software-defined VMware in un cloud pubblico utilizzando il cloud storage NetApp o in un altro ambiente VMware on-premise con lo storage ONTAP come sito di disaster recovery.

Il disaster recovery di BlueXP è un servizio di disaster recovery basato sul cloud che automatizza i flussi di lavoro di disaster recovery. Grazie al servizio di disaster recovery BlueXP , puoi proteggere i tuoi carichi di lavoro on-premise basati su NFS e gli archivi dati VMFS (Virtual Machine file System) di VMware vSphere per iSCSI e FC che eseguono lo storage NetApp in uno dei seguenti modi:

- VMware Cloud (VMC) su AWS con Amazon FSX per NetApp ONTAP o.
- Un altro ambiente VMware on-premise basato su NFS con storage ONTAP

> QUESTA DOCUMENTAZIONE RIGUARDANTE AWS EVS VIENE FORNITA COME ANTEPRIMA TECNOLOGICA. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale. Per ulteriori informazioni, vedere "Introduzione del disaster recovery di BlueXP tramite Amazon Elastic VMware Service e Amazon FSx per NetApp ONTAP".

Il disaster recovery di BlueXP sfrutta la tecnologia ONTAP SnapMirror come trasporto di replica verso il sito di disaster recovery. Ciò offre la migliore efficienza dello storage del settore (compressione e deduplica) sui siti primari e secondari.



Vantaggi dell'utilizzo di BlueXP per il disaster recovery per VMware

Il disaster recovery di BlueXP offre i seguenti benefici:

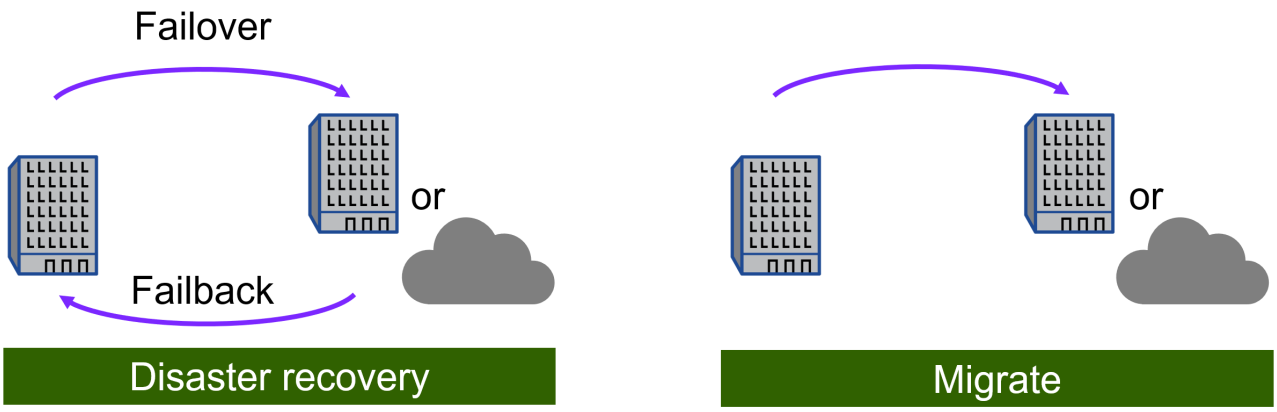
- Esperienza utente semplificata per il rilevamento e il recovery di vCenter delle applicazioni con più operazioni di recovery point-in-time
- Total cost of ownership inferiore con costi operativi ridotti e capacità di creare e regolare piani di disaster recovery con risorse minime
- Disponibilità del disaster recovery costante con test di failover virtuale che non interrompono le operazioni
- Time-to-value più veloce grazie alle modifiche dinamiche dell'ambiente IT e alla capacità di gestirlo nei piani di disaster recovery

Cosa puoi fare con il disaster recovery BlueXP per VMware

Il disaster recovery di BlueXP ti fornisce l'utilizzo completo di diverse tecnologie NetApp per raggiungere i seguenti obiettivi:

- Replica le app VMware sul sito di produzione on-premise in un sito remoto di disaster recovery nel cloud o on-premise utilizzando la replica SnapMirror.
- Eseguire la migrazione dei carichi di lavoro VMware dal sito originale a un altro sito.

- Eseguire un test di failover; le macchine virtuali vengono create temporaneamente. Il disaster recovery di BlueXP crea un nuovo volume FlexClone dalla snapshot selezionata e un datastore temporaneo di backup del volume FlexClone viene mappato agli host ESXi. Questo processo non consuma capacità fisica aggiuntiva nello storage ONTAP on-premise o in FSX per lo storage NetApp ONTAP 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, effettua il failover on-demand nel sito di disaster recovery, che può essere VMware Cloud su AWS con Amazon FSX per NetApp ONTAP o un ambiente VMware on-premise con ONTAP.
- Una volta risolto il disastro, è possibile eseguire il failback on-demand dal sito di disaster recovery al sito primario. *Raggruppare le macchine virtuali o i datastore in gruppi di risorse logiche per una gestione efficiente.



La configurazione del server vSphere viene eseguita al di fuori del disaster recovery BlueXP in vSphere Server.

Costo

NetApp non ti addebita i costi per l'utilizzo della versione di prova del disaster recovery di BlueXP.

È possibile utilizzare il servizio di disaster recovery di BlueXP con una licenza NetApp o con un piano annuale basato su abbonamento tramite Amazon Web Services.

Alcune versioni includono un'anteprima tecnologica. NetApp non ti addebita alcun costo per la capacità dei workload in anteprima. Per informazioni sulle anteprime delle tecnologie più recenti, vedere "Novità del disaster recovery BlueXP" .

Licensing

È possibile utilizzare i seguenti tipi di licenza:

- Iscriviti per una prova gratuita di 30 giorni.
- Acquista un abbonamento pay-as-you-go (PAYGO) a **servizi intelligenti NetApp** con il marketplace di Amazon Web Services (AWS).
- BYOL (Bring Your Own License), ovvero un file di licenza NetApp (NLF) ottenuto dal rappresentante

vendite NetApp Puoi utilizzare il numero di serie della licenza per attivare il BYOL nel Digital Wallet di BlueXP.

Le licenze per tutti i servizi BlueXP sono gestite dal servizio di Digital Wallet di BlueXP. Dopo aver configurato il BYOL, puoi vedere una licenza attiva per il servizio nel Digital Wallet di BlueXP.

> Le spese per il disaster recovery di BlueXP si basano sulla capacità utilizzata degli archivi dati sul sito di origine quando vi è almeno una macchina virtuale con un piano di replica. La capacità di un datastore in failover non è inclusa nella capacità consentita. Per un BYOL, se i dati superano la capacità consentita, le operazioni del servizio sono limitate fino a quando non ottieni una licenza di capacità aggiuntiva o esegui l'upgrade della licenza nel Digital Wallet di BlueXP.

Per ulteriori informazioni sulla configurazione delle licenze per il disaster recovery di BlueXP, fare riferimento a. "Configura le licenze di disaster recovery di BlueXP".

prova gratuita di 30 giorni

Puoi provare il disaster recovery di BlueXP utilizzando una prova gratuita di 30 giorni.

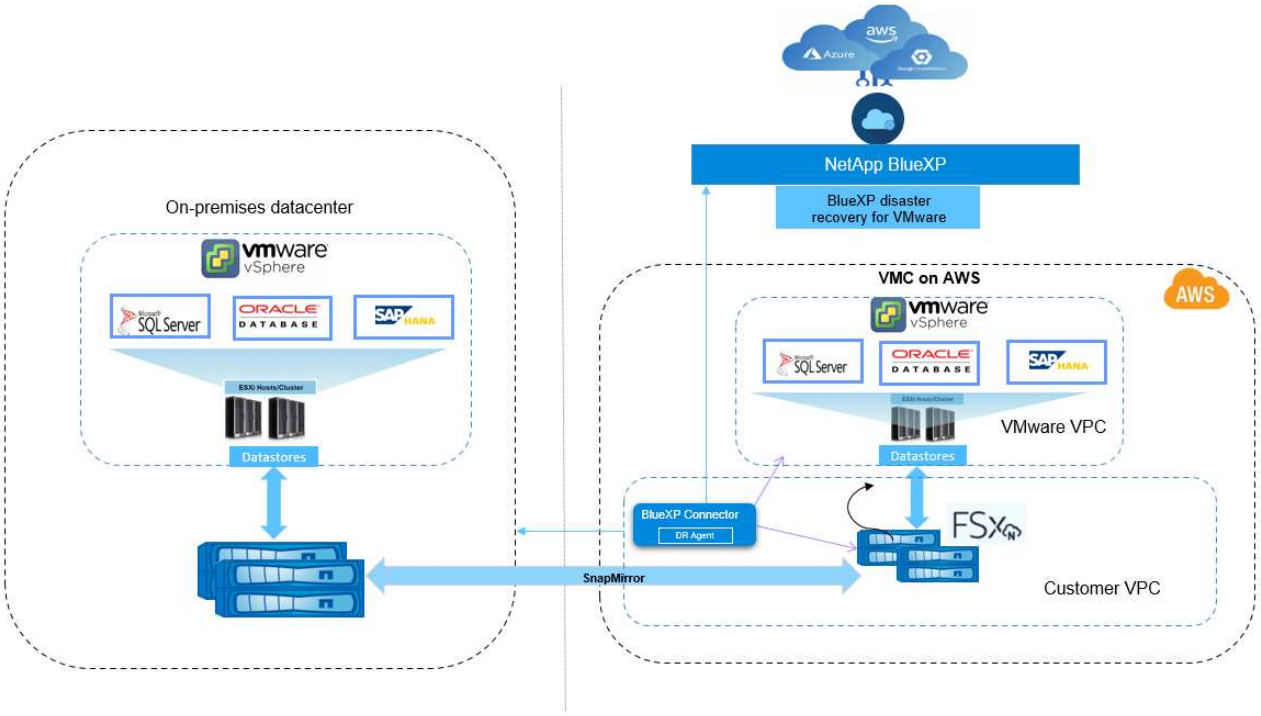
Per continuare dopo la prova di 30 giorni, devi ottenere un abbonamento Pay-as-you-go (PAYGO) dal tuo cloud provider o acquistare una licenza BYOL da NetApp.

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

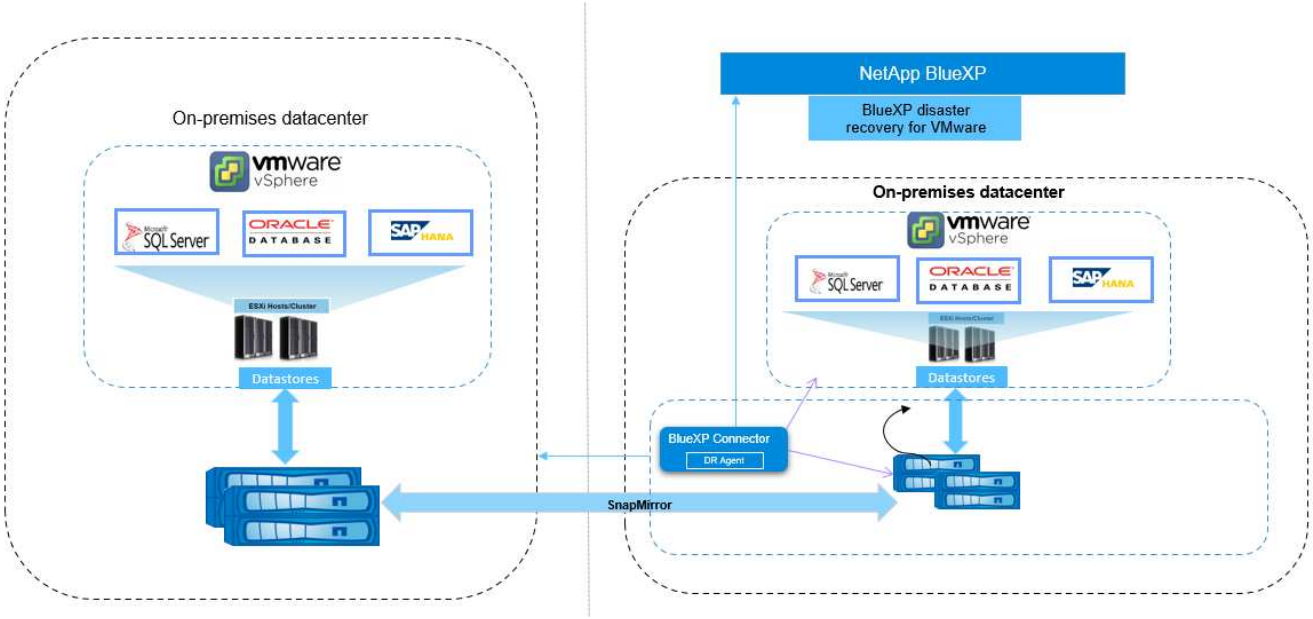
Come funziona il disaster recovery di BlueXP

Il disaster recovery di BlueXP può ripristinare i workload replicati da un sito on-premise su Amazon FSX per ONTAP o in un altro sito on-premise. Questo servizio automatizza il ripristino dal livello di SnapMirror, tramite la registrazione della macchina virtuale al Virtual Machine Cloud (VMC) e alle mappature di rete direttamente sulla piattaforma di sicurezza e virtualizzazione della rete di VMware, NSX-T. Questa funzione è inclusa in tutti gli ambienti Virtual Machine Cloud.

Il disaster recovery di BlueXP sfrutta la tecnologia ONTAP SnapMirror, che offre una replica altamente efficiente e mantiene l'efficienza delle snapshot nelle operazioni incrementali e senza fine di ONTAP. La replica SnapMirror garantisce che le copie snapshot coerenti con l'applicazione siano sempre sincronizzate e i dati siano utilizzabili subito dopo un failover.



Il diagramma seguente mostra l'architettura dei piani di disaster recovery da on-premise a on-premise.



In caso di disastro, questo servizio aiuta a ripristinare macchine virtuali nell'altro ambiente VMware o VMC on-premise suddividendo le relazioni SnapMirror e rendendo attivo il sito di destinazione.

- Il servizio consente inoltre di eseguire il failback delle macchine virtuali nel percorso di origine.
- È possibile verificare il processo di failover del disaster recovery senza interrompere le macchine virtuali originali. Il test ripristina le macchine virtuali in una rete isolata creando un FlexClone del volume.
- Per il processo di failover o di test del failover, è possibile scegliere l'ultimo (predefinito) o lo snapshot selezionato da cui ripristinare la macchina virtuale.

Termini e condizioni per il disaster recovery di BlueXP

È possibile trarre vantaggio dalla comprensione di alcuni termini relativi al disaster recovery.

- **Sito**: Un contenitore logico generalmente associato a un data center fisico o a un cloud provider.
- **Gruppo di risorse**: Un contenitore logico che consente di gestire più VM come una singola unità.
- **Piano di replica**: Un insieme di regole sulla frequenza dei backup e sulla gestione degli eventi di failover. I piani vengono assegnati a uno o più gruppi di risorse.

Prerequisiti per il disaster recovery di BlueXP

Prima di utilizzare il disaster recovery di BlueXP, assicurati che il tuo ambiente soddisfi i requisiti di storage ONTAP, cluster VMware vCenter e BlueXP.

Prerequisiti per lo storage ONTAP

Questi prerequisiti si applicano alle istanze ONTAP o Amazon FSX per NetApp ONTAP.

- I cluster di origine e di destinazione devono avere una relazione peer.
- La SVM che ospiterà i volumi di disaster recovery deve esistere nel cluster di destinazione.
- La SVM di origine e la SVM di destinazione devono avere una relazione di peer.

> I volumi di disaster recovery nella SVM o nelle SVM di destinazione non devono essere creati in anticipo. Il disaster recovery di BlueXP creerà i volumi di destinazione in base alle esigenze per il piano di replica.

- Se si esegue la distribuzione con Amazon FSX per NetApp ONTAP, si applica il seguente prerequisito:
  - Un'istanza di Amazon FSX per NetApp ONTAP per l'hosting di datastore DR VMware deve esistere nel VPC. Fare riferimento alla documentazione di Amazon FSX per ONTAP all'indirizzo "introduzione".

Prerequisiti dei cluster VMware vCenter

Questi prerequisiti si applicano sia ai cluster vCenter on-premise che al Software-Defined Data Center (SDDC) di VMware Cloud per AWS.

- Tutti i cluster VMware che vuoi gestire il disaster recovery di BlueXP devono essere ospitati su ONTAP Volumes.
- Tutti i datastore VMware da gestire con il disaster recovery di BlueXP 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 questi prerequisiti.
  - In VMware Cloud Console, utilizzare i ruoli di servizio Administrator e NSX Cloud Administrator. Utilizzare anche il proprietario dell'organizzazione per il ruolo Organizzazione. Fare riferimento alla "Utilizzo della documentazione relativa a VMware Cloud Foundations with AWS FSX for NetApp ONTAP".

- Link all'istanza di VMware Cloud SDDC con Amazon FSX per NetApp ONTAP. Fare riferimento alla "Integrazione di VMware Cloud su AWS con Amazon FSX per NetApp ONTAP".

Prerequisiti di BlueXP

Inizia a utilizzare BlueXP

Se non l'avete già fatto, "Registrati a BlueXP e crea un'organizzazione"

Raccolta delle credenziali per ONTAP e VMware

- Le credenziali di Amazon FSX per ONTAP e AWS devono essere aggiunte all'ambiente di lavoro all'interno del progetto BlueXP che verrà utilizzato per gestire il disaster recovery di BlueXP .
- Il disaster recovery di BlueXP richiede le credenziali vCenter. Inserisci le credenziali vCenter quando Aggiungi un sito nel disaster recovery di BlueXP.

  Per un elenco dei privilegi vCenter necessari, fare riferimento a "Privilegi vCenter necessari per il disaster recovery di BlueXP". Per istruzioni su come aggiungere un sito, fare riferimento a "Aggiungere un sito".

Crea un connettore BlueXP

È necessario configurare un connettore BlueXP in BlueXP. Quando utilizzi il connettore BlueXP, includerà le funzionalità appropriate per il servizio di disaster recovery.

- Il disaster recovery di BlueXP funziona solo con l'implementazione di connettori in modalità standard. Vedere "Guida introduttiva di BlueXP in modalità standard".
- Assicurarsi che sia il vCenter di origine che quello di destinazione utilizzino lo stesso BlueXP Connector.
- Tipo di connettore BlueXP richiesto:
  - **Disaster recovery da on-premise a on-premise**: Installare il connettore BlueXP on-premise nel sito di disaster recovery. Fare riferimento alla "Installazione e configurazione di un connettore on-premise".
  - **Da on-premise ad AWS**: Installa il connettore BlueXP per AWS nel VPC AWS. Fare riferimento alla "Opzioni di installazione del connettore in AWS".

    Utilizza il connettore BlueXP on-premise per quanto riguarda da on-premise a on-premise. Per gli ambienti on-premise in AWS, utilizza BlueXP AWS Connector, che ha accesso a vCenter on-premise di origine e a vCenter on-premise di destinazione.

  - Il connettore BlueXP installato deve essere in grado di accedere a qualsiasi cluster VMware gestito dal disaster recovery BlueXP.
- Tutti gli array ONTAP da gestire mediante il disaster recovery di BlueXP devono essere aggiunti a qualsiasi ambiente di lavoro all'interno del progetto BlueXP che verrà utilizzato per gestire il disaster recovery di BlueXP .

  Vedere "Scopri i cluster ONTAP on-premise".
- Per informazioni sulla configurazione di un proxy intelligente per il ripristino di emergenza BlueXP , vedere "Configura l'infrastruttura per il disaster recovery di BlueXP".

Prerequisiti dei carichi di lavoro

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

- Verificare che gli strumenti VMware (o Open VM) siano in esecuzione sulle VM che verranno protette.
- Per le macchine virtuali Windows che eseguono Microsoft SQL Server o Oracle Database o entrambi, i database devono avere i VSS Writer abilitati.
- Per i database Oracle in esecuzione su un sistema operativo Linux, l'autenticazione utente del sistema operativo deve essere abilitata per il ruolo SYSDBA del database Oracle.

Avvio rapido del disaster recovery di BlueXP

Di seguito è riportata una panoramica dei passaggi necessari per iniziare con il disaster recovery di BlueXP. I collegamenti all'interno di ogni passaggio consentono di accedere a una pagina che fornisce ulteriori dettagli.

1 **Esaminare i prerequisiti**

"Assicurati che il tuo ambiente soddisfi questi requisiti".

2 **Configurare il servizio di disaster recovery BlueXP**

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

3 **Quali sono le prossime novità?**

Dopo aver configurato il servizio, ecco cosa fare in seguito.

- "Aggiungi i siti vCenter al disaster recovery di BlueXP".
- "Creare il primo gruppo di risorse".
- "Creare il primo piano di replica".
- "Replicare le applicazioni in un altro sito".
- "Eseguire il failover delle applicazioni in un sito remoto".
- "Eseguire il failback delle applicazioni nel sito di origine".
- "Gestire siti, gruppi di risorse e piani di replica".
- "Monitorare le operazioni di disaster recovery".

Configura l'infrastruttura per il disaster recovery di BlueXP

Per utilizzare il disaster recovery di BlueXP, esegui alcuni passaggi per configurarlo sia in Amazon Web Services (AWS) che in BlueXP.

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

Preparati al disaster recovery con BlueXP per la protezione on-premise

Assicurati che siano soddisfatti i seguenti requisiti prima di impostare il disaster recovery BlueXP per la protezione on-premise-premise:

- Storage ONTAP
  - Assicurarsi di disporre delle credenziali ONTAP.
  - Creare o verificare il sito di disaster recovery.
  - Crea o verifica la tua ONTAP SVM di destinazione.
  - Verifica che le SVM ONTAP di origine e destinazione siano sottoposte a peering.
- Cluster vCenter
  - Assicurarsi che le macchine virtuali da proteggere siano ospitate su datastore NFS (utilizzando volumi NFS ONTAP) o datastore VMFS (utilizzando LUN iSCSI NetApp).
  - Revisione "VCenter Privileges" richiesta per BlueXP DR.
  - Creare un account utente per il disaster recovery (non l'account amministratore vCenter predefinito) e assegnare vCenter Privileges all'account.

Supporto proxy intelligente

Il connettore BlueXP supporta il proxy intelligente. Il proxy intelligente è un modo leggero, sicuro ed efficiente per connettere l'ambiente on-premise al servizio BlueXP . Fornisce una connessione sicura tra l'ambiente e il servizio BlueXP senza richiedere una VPN o un accesso diretto a Internet. Questa implementazione proxy ottimizzata alleggerisce il traffico API all'interno della rete locale.

Quando viene configurato un proxy, BlueXP disaster recovery tenta di comunicare direttamente con VMware o ONTAP e utilizza il proxy configurato in caso di errore della comunicazione diretta.

L'implementazione del proxy per il disaster recovery di BlueXP richiede la comunicazione della porta 443 tra il connettore e qualsiasi server vCenter e array ONTAP utilizzando un protocollo HTTPS. L'agente di disaster recovery BlueXP all'interno del connettore comunica direttamente con VMware vSphere, VC o ONTAP durante l'esecuzione di qualsiasi azione.

Per ulteriori informazioni sulla configurazione generale del proxy in BlueXP , vedere "Configurare un connettore per l'utilizzo di un server proxy".

Preparati al disaster recovery di BlueXP per la protezione on-premise nel cloud con AWS

Per configurare il disaster recovery BlueXP per la protezione on-premise nel cloud utilizzando AWS, devi impostare quanto segue:

- Configura AWS FSX per NetApp ONTAP
- Configura VMware Cloud su AWS SDDC

Configura AWS FSX per NetApp ONTAP

- Crea un file system Amazon FSX per NetApp ONTAP.
  - Esegui il provisioning e configura FSX per ONTAP. Amazon FSX per NetApp ONTAP è un servizio completamente gestito che offre un file storage altamente affidabile, scalabile, dalle performance elevate e ricco di funzionalità, costruito sul file system NetApp ONTAP.

    - Seguire i passaggi in "Report tecnico 4938: Monta Amazon FSX ONTAP come datastore NFS con VMware Cloud su AWS" e per eseguire il provisioning e "Avvio rapido di Amazon FSX per NetApp ONTAP" configurare FSX per ONTAP.
- Aggiungi Amazon FSX per ONTAP all'ambiente di lavoro e Aggiungi le credenziali AWS per FSX per ONTAP.
- Crea o verifica la tua SVM ONTAP di destinazione in un'istanza di AWS FSX per ONTAP.
- Configura la replica tra il cluster ONTAP on-premise di origine e l'istanza di FSX per ONTAP in BlueXP .

Per i passi dettagliati, fare riferimento alla "Come impostare un ambiente di lavoro FSX per ONTAP" .

Configura VMware Cloud su AWS SDDC

"VMware Cloud su AWS" Offre un'esperienza nativa del cloud per i 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), il networking software-defined NSX-T, lo storage software-defined vSAN e uno o più host ESXi che forniscono risorse di calcolo e storage ai carichi di lavoro.

Per configurare un ambiente VMware Cloud su AWS, attenersi alla procedura descritta in "Implementare e configurare l'ambiente di virtualizzazione su AWS". è possibile utilizzare Un cluster pilota anche per il ripristino di emergenza.

Accedi al disaster recovery di BlueXP

USA NetApp BlueXP per accedere al servizio di disaster recovery di BlueXP.

Per accedere a BlueXP, puoi utilizzare le credenziali del sito di supporto NetApp oppure iscriverti per un login cloud NetApp utilizzando la tua email e una password. "Scopri di più sull'accesso".

Attività specifiche richiedono ruoli utente BlueXP specifici. "Scopri di più sui ruoli utente e sulle autorizzazioni nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

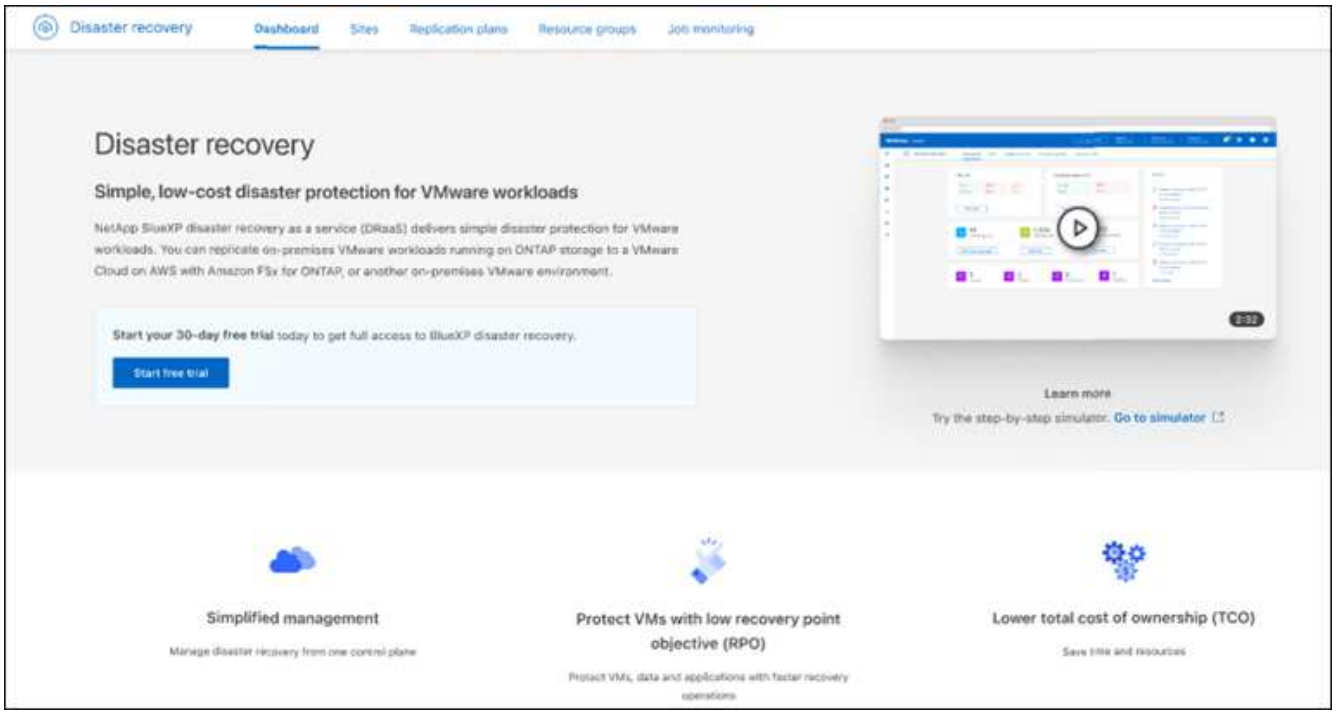
Fasi

1. Aprire un browser Web e accedere a. "Console BlueXP".

   Viene visualizzata la pagina di accesso a NetApp BlueXP.

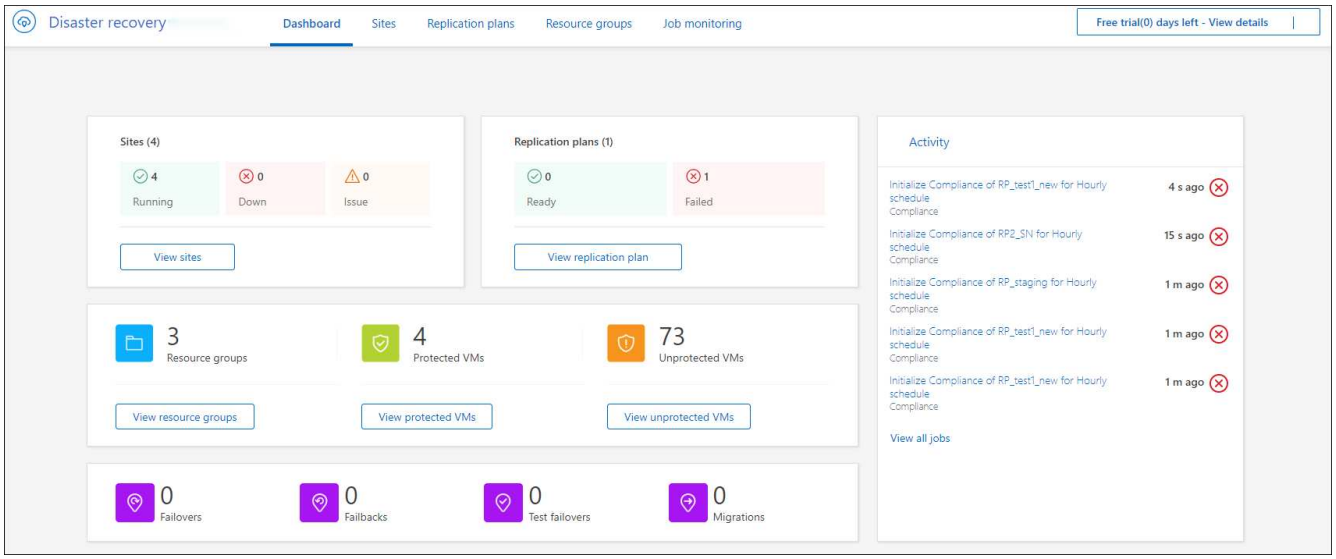
2. Accedere a BlueXP.
3. Dal menu di navigazione a sinistra di BlueXP, selezionare **protezione** > **Disaster Recovery**.

   Se questa è la prima volta che accedi a questo servizio, viene visualizzata la pagina di destinazione ed è possibile registrarsi per una prova gratuita.



In caso contrario, verrà visualizzata la dashboard di disaster recovery di BlueXP.

- Se non hai ancora aggiunto un connettore BlueXP, dovrai aggiungere un connettore. Per aggiungere un connettore, fare riferimento a. "Scopri di più sui connettori".
- Se sei un utente BlueXP con un connettore esistente, quando selezioni "Disaster Recovery", viene visualizzato un messaggio relativo alla registrazione.
- Se si sta già utilizzando il servizio, quando si seleziona "Disaster Recovery" viene visualizzato il dashboard.



Imposta le licenze per il disaster recovery di BlueXP

Grazie al disaster recovery di BlueXP, puoi utilizzare diversi piani di licenza, tra cui una versione di prova gratuita, un'iscrizione pay-as-you-go o il modello Bring Your Own License.

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

È possibile utilizzare i seguenti tipi di licenza:

- Iscriviti per una prova gratuita di 30 giorni.
- Acquista un abbonamento pay-as-you-go (PAYGO) a **NetApp Intelligent Services** con Amazon Web Services (AWS) Marketplace.
- BYOL (Bring Your Own License), ovvero un file di licenza NetApp (NLF) ottenuto dal rappresentante vendite NetApp Puoi utilizzare il numero di serie della licenza per attivare il BYOL nel Digital Wallet di BlueXP.

> Le spese per il disaster recovery di BlueXP si basano sulla capacità utilizzata degli archivi dati sul sito di origine quando vi è almeno una macchina virtuale con un piano di replica. La capacità di un datastore in failover non è inclusa nella capacità consentita. Per un BYOL, se i dati superano la capacità consentita, le operazioni del servizio sono limitate fino a quando non ottieni una licenza di capacità aggiuntiva o esegui l'upgrade della licenza nel Digital Wallet di BlueXP.

"Ulteriori informazioni sul Digital Wallet".

Al termine della prova gratuita o alla scadenza della licenza, è comunque possibile effettuare le seguenti operazioni nel servizio:

- Puoi visualizzare qualsiasi risorsa, ad esempio un carico di lavoro o un piano di replica.
- Eliminare qualsiasi risorsa, ad esempio un carico di lavoro o un piano di replica.
- Eseguire tutte le operazioni pianificate create durante il periodo di prova o sotto la licenza.

Provalo con una prova gratuita di 30 giorni

Puoi provare il disaster recovery di BlueXP utilizzando una prova gratuita di 30 giorni.

> Durante la prova non vengono applicati limiti di capacità.

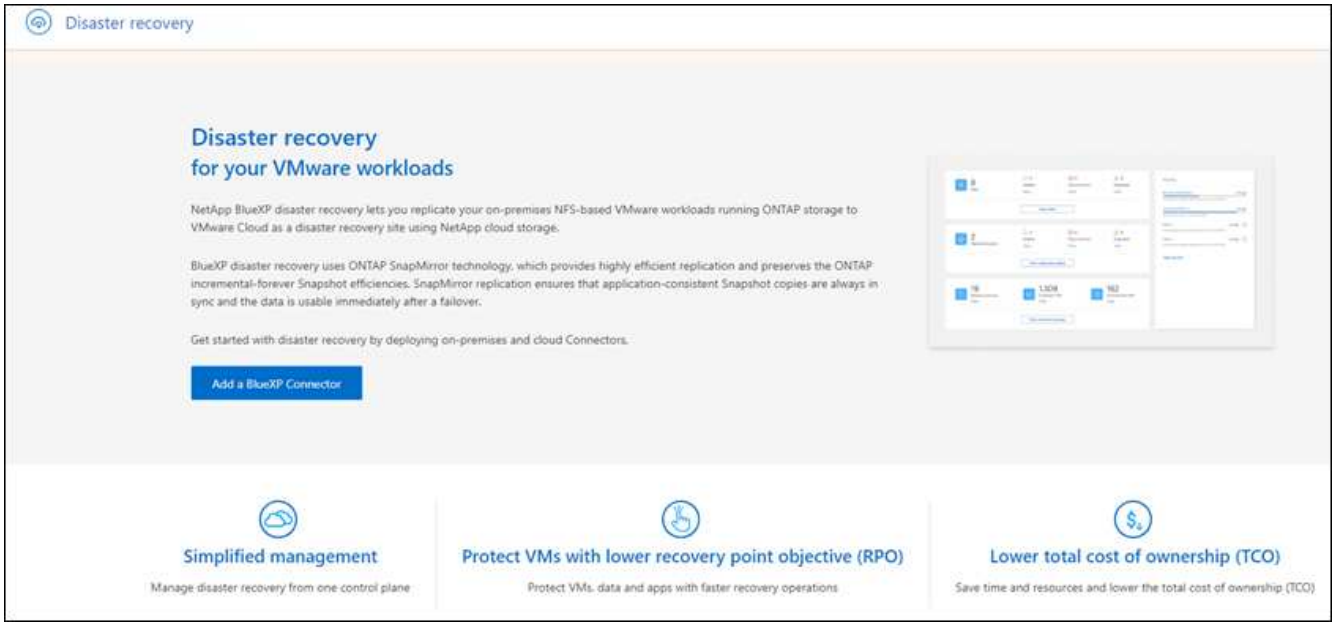
Per continuare dopo la prova, dovrai acquistare una licenza BYOL o un abbonamento PAYGO AWS. Puoi ottenere una licenza in qualsiasi momento e non ti verrà addebitato alcun costo fino al termine della prova.

Durante la prova, si dispone di tutte le funzionalità.

Fasi

1. Accedere a. "Console BlueXP".
2. Accedere a BlueXP.
3. Dal menu di navigazione a sinistra di BlueXP, selezionare **protezione** > **Disaster Recovery**.

   Se è la prima volta che accedi a questo servizio, viene visualizzata la pagina iniziale.



4. Se non è già stato aggiunto un connettore per altri servizi, aggiungerne uno.

   Per aggiungere un connettore, fare riferimento a. "Scopri di più sui connettori".

5. Dopo aver configurato un connettore, nella landing page di disaster recovery di BlueXP, il pulsante per aggiungere un connettore diventa un pulsante per iniziare una prova gratuita. Selezionare **Avvia prova gratuita**.
6. Iniziare con l'aggiunta di vCenter.

   Per ulteriori informazioni, vedere "Aggiungere siti vCenter".

Al termine della prova, iscriviti attraverso AWS Marketplace

Al termine della prova gratuita, puoi acquistare una licenza da NetApp o abbonarti a **NetApp Intelligent Services** tramite AWS Marketplace. Questa procedura offre una panoramica di alto livello su come iscriversi direttamente in AWS Marketplace.

Fasi

1. Nel disaster recovery di BlueXP, viene visualizzato un messaggio che informa che la prova gratuita sta per scadere. Nel messaggio, selezionare **Sottoscrivi o acquista una licenza**.
2. Seleziona **Iscriviti in AWS Marketplace**.
3. USA il marketplace AWS per abbonarti a **servizi intelligenti di NetApp** e **disaster recovery di BlueXP** .
4. Quando torni al disaster recovery di BlueXP, un messaggio indica che sei iscritto.

   Puoi visualizzare i dettagli dell'abbonamento nel portafoglio digitale di BlueXP . "Scopri di più sulla gestione delle iscrizioni con il Digital Wallet".

Al termine della prova, acquista una licenza BYOL tramite NetApp

Al termine della prova, è possibile acquistare una licenza tramite il proprio rappresentante NetApp

Se porti la tua licenza BYOL, il setup include l'acquisto della licenza, il reperimento del file di licenza NetApp e

l’aggiunta della licenza al Digital Wallet di BlueXP.

Aggiungi la licenza al portafoglio digitale BlueXP * dopo aver acquistato la licenza di disaster recovery BlueXP dal rappresentante di vendita NetApp, puoi gestire la licenza nel portafoglio digitale.

"Scopri come aggiungere licenze con il Digital Wallet".

Aggiorna la tua licenza BlueXP alla scadenza

Se il termine in licenza si avvicina alla data di scadenza o se la capacità concessa in licenza sta raggiungendo il limite, riceverai una notifica nell’interfaccia utente di disaster recovery di BlueXP. Puoi aggiornare la licenza di disaster recovery di BlueXP prima che scada, in modo che non si verifichino interruzioni nella capacità di accesso ai dati sottoposti a scansione.

Questo messaggio viene visualizzato anche nel Digital Wallet di BlueXP e in "Notifiche".

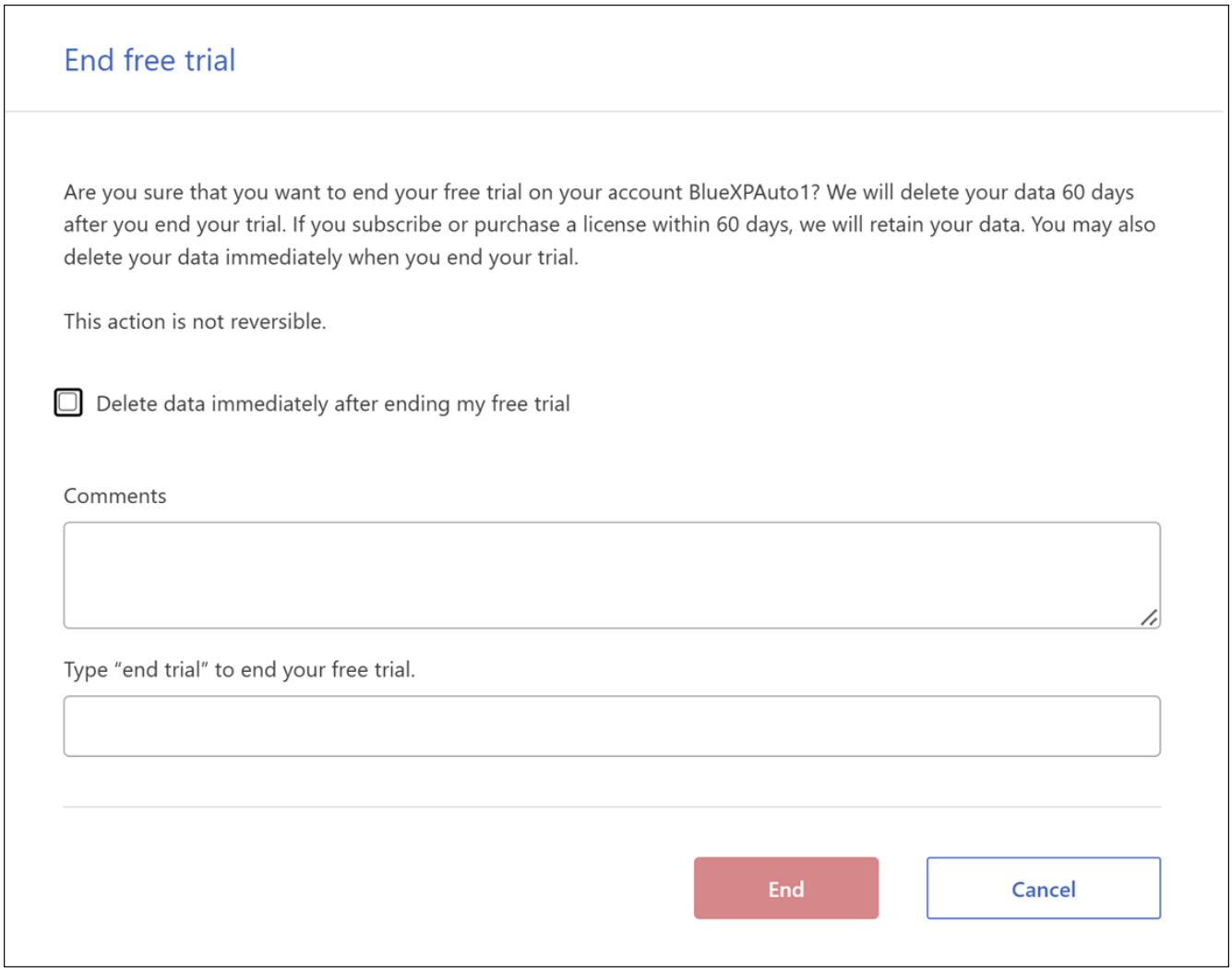
"Ulteriori informazioni sull’aggiornamento delle licenze con il portafoglio digitale".

Termina la prova gratuita

È possibile interrompere la prova gratuita in qualsiasi momento o attendere la scadenza.

Fasi

1. Nel disaster recovery di BlueXP, in alto a destra, seleziona **prova gratuita - Visualizza dettagli**.
2. Nell’elenco a discesa, selezionare **fine prova gratuita**.



3. Se si desidera eliminare tutti i dati, selezionare **Elimina dati immediatamente dopo aver terminato la prova gratuita**.

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

   Se si termina la prova gratuita, non si è chiesto di eliminare i dati e non si acquista una licenza o un abbonamento, il ripristino d’emergenza BlueXP elimina tutti i dati 60 giorni dopo la fine della prova gratuita.

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

Domande frequenti sul disaster recovery di BlueXP

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Che cos’è l’URL di disaster recovery di BlueXP?
Per l’URL, in un browser, immettere: "https://console.bluexp.netapp.com/" Per accedere alla console BlueXP.

È necessaria una licenza per utilizzare il disaster recovery di BlueXP?
Per un accesso completo è necessaria una licenza di disaster recovery BlueXP. Tuttavia, è possibile provarlo con la versione di prova gratuita.

Per ulteriori informazioni sulla configurazione delle licenze per il disaster recovery di BlueXP, fare riferimento a. "Configura le licenze di disaster recovery di BlueXP".

Come si accede al disaster recovery di BlueXP ? Il disaster recovery di BlueXP non richiede alcuna abilitazione. L'opzione di disaster recovery viene visualizzata automaticamente nella navigazione a sinistra di BlueXP.

USA il disaster recovery di BlueXP

USA la panoramica sul disaster recovery di BlueXP

Il disaster recovery di BlueXP ti permette di raggiungere i seguenti obiettivi:

- "Visualizzare lo stato dei piani di disaster recovery".
- "Aggiungere siti vCenter".
- "Creare gruppi di risorse per organizzare insieme le VM"
- "Creare un piano di disaster recovery".
- "Replica delle applicazioni VMware" Sul tuo sito primario in un sito remoto di disaster recovery nel cloud usando la replica SnapMirror.
- "Migrazione delle applicazioni VMware" sul sito primario in un altro sito.
- "Verificare il failover" senza interrompere le macchine virtuali originali.
- In caso di disastro, "eseguire il failover del sito primario" Verso VMware Cloud su AWS con FSX per NetApp ONTAP.
- Dopo la risoluzione del disastro, "failback" dal sito di disaster recovery a quello primario.
- "Monitorare le operazioni di disaster recovery" Nella pagina monitoraggio processi.

Visualizza lo stato di integrità dei tuoi piani di disaster recovery BlueXP sulla Dashboard

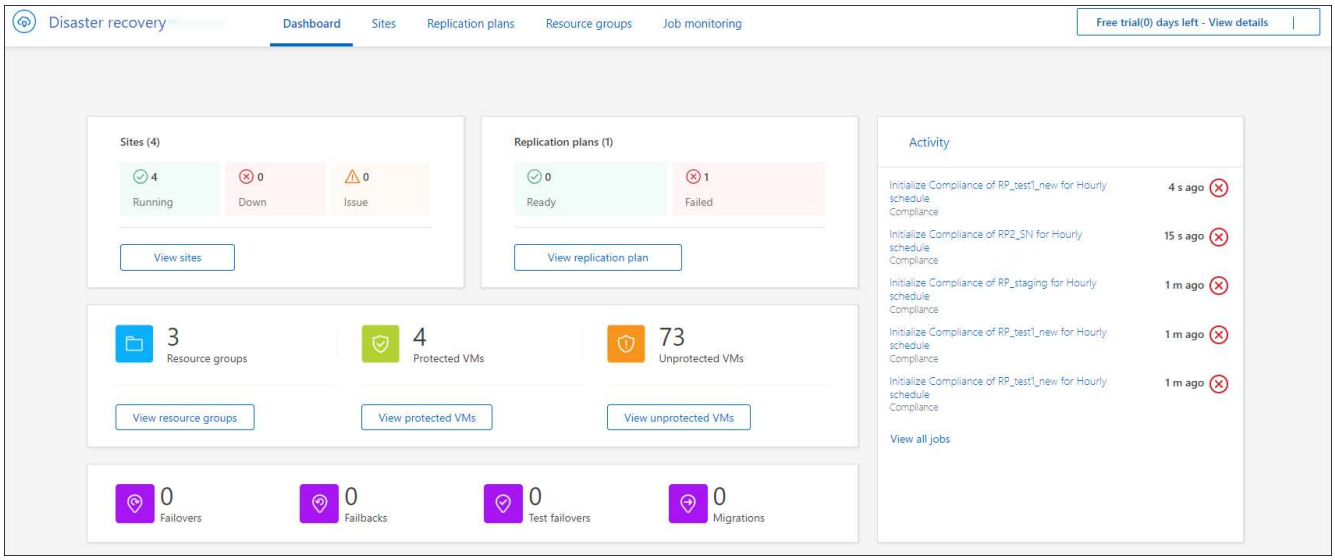
Usando la dashboard di disaster recovery di BlueXP, puoi determinare lo stato di salute dei siti di disaster recovery e dei piani di replica. È possibile stabilire rapidamente quali siti e piani sono sani, scollegati o degradati.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Amministratore del ripristino di emergenza, Amministratore dell'applicazione di ripristino di emergenza o Ruolo di visualizzatore del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore del disaster recovery di BlueXP, selezionare **Dashboard**.



3. Esaminare le seguenti informazioni sul dashboard:
   - **Siti**: Visualizza la salute dei tuoi siti. Un sito può avere uno dei seguenti stati:
     - **In esecuzione**: VCenter è connesso, funzionante e in esecuzione.
     - **Down**: 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, selezionare **Visualizza tutto** per uno stato o **Visualizza siti** per visualizzarli tutti.
   - **Piani di replica**: Consente di visualizzare lo stato di salute dei piani. Un piano può avere uno dei seguenti stati:
     - **Pronto**
     - **Non riuscito**

       Per rivedere i dettagli del piano di replica, selezionare **Visualizza tutto** per uno stato o **Visualizza piani di replica** per visualizzarli tutti.
   - **Gruppi di risorse**: Consente di visualizzare lo stato dei 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, selezionare il collegamento **Visualizza** sotto ciascuno.
   - Il numero di failover, failover di test e migrazioni. Ad esempio, se sono stati creati due piani e sono stati migrati verso le destinazioni, il numero di migrazioni viene visualizzato come "2".
4. Controllare tutte le operazioni nel riquadro attività. Per visualizzare tutte le operazioni in Job Monitor, selezionare **Visualizza tutti i lavori**.

Aggiungere vCenter a un sito nel ripristino di emergenza di BlueXP

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 in BlueXP .

Assicurarsi che sia il vCenter di origine che quello di destinazione utilizzino lo stesso BlueXP Connector.

Una volta aggiunti i vCenter, il disaster recovery di BlueXP esegue un rilevamento approfondito degli ambienti vCenter, inclusi cluster vCenter, host ESXi, datastore, impronta ecologica dello storage, dettagli delle macchine virtuali, repliche SnapMirror e reti di macchine virtuali.

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti oppure Amministratore del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Se nelle release precedenti sono stati aggiunti vCenter e si desidera personalizzare la pianificazione del rilevamento, è necessario modificare il sito del server vCenter e impostare la pianificazione.

Il disaster recovery di BlueXP esegue il rilevamento ogni 24 ore. Dopo aver configurato un sito, è possibile modificare vCenter in un secondo momento per personalizzare la pianificazione di rilevamento che soddisfa le proprie esigenze. Ad esempio, se si dispone di un numero elevato di macchine virtuali, è possibile impostare la pianificazione del rilevamento in modo che venga eseguita ogni 23 ore e 59 minuti. Se si dispone di un numero limitato di macchine virtuali, è possibile impostare la pianificazione del rilevamento in modo che venga eseguita ogni 12 ore. L'intervallo minimo è di 30 minuti e il massimo è di 24 ore.

Per ottenere le informazioni più aggiornate sull'ambiente in uso, è necessario innanzitutto effettuare alcune ricerche manuali. Successivamente, è possibile impostare l'esecuzione automatica della pianificazione.

Le macchine virtuali appena aggiunte o eliminate vengono riconosciute nel successivo rilevamento pianificato o durante un rilevamento manuale immediato.

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

- Pronti
- Failback confermata
- Verifica failover confermata

Fasi

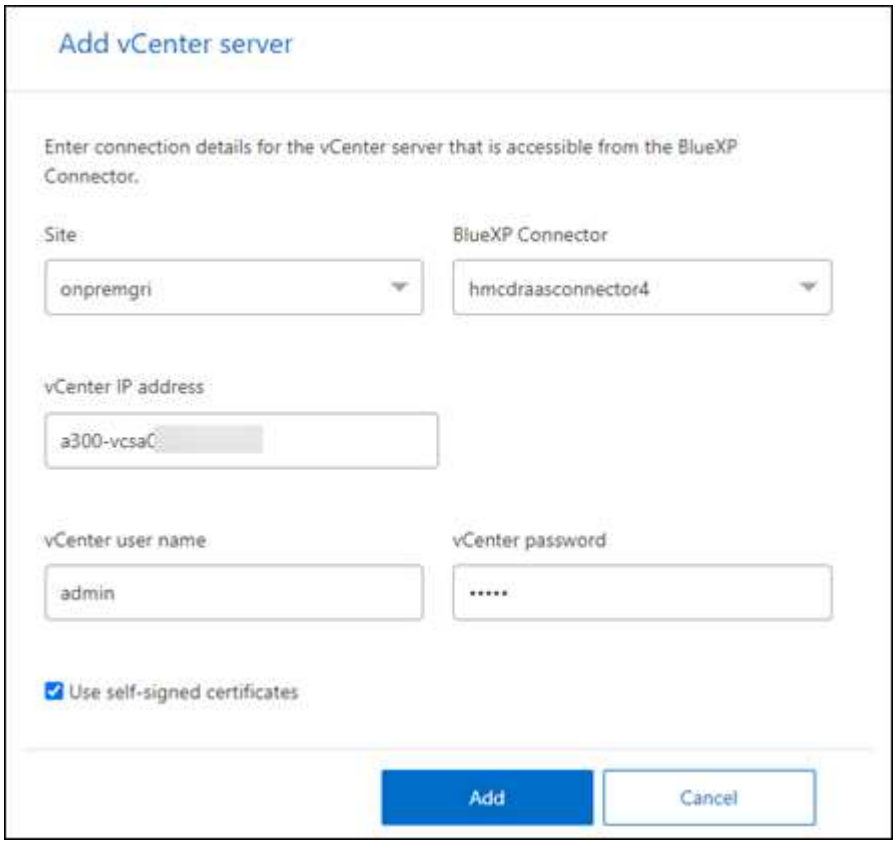
1. Accedere a BlueXP e dal menu di navigazione a sinistra selezionare **protezione** > **Disaster Recovery**.

   Ti atterrai alla pagina della dashboard di disaster recovery di BlueXP. Quando si inizia con il servizio, è necessario aggiungere le informazioni vCenter. Successivamente, il Dashboard visualizza i dati relativi ai siti e ai piani di replica.

   Vengono visualizzati campi diversi a seconda del tipo di sito che si sta aggiungendo.

2. **Fonte**: Selezionare **Scopri i server vCenter** per inserire le informazioni sul sito vCenter di origine.

   Se alcuni siti vCenter esistono già e si desidera aggiungerne altri, dal menu in alto, selezionare **Sites** (Siti), quindi selezionare **Add** (Aggiungi).



   - Aggiungi un sito, seleziona il connettore BlueXP e fornisci credenziali vCenter.
   - (Valido solo per i siti on-premise) per accettare certificati autofirmati per il vCenter di origine, selezionare la casella.

     I certificati autofirmati non sono protetti come gli altri certificati. Se vCenter è **NON** configurato con certificati di autorità di certificazione (CA), selezionare questa casella; in caso contrario, la connessione a vCenter non funzionerà.

3. Selezionare **Aggiungi**.

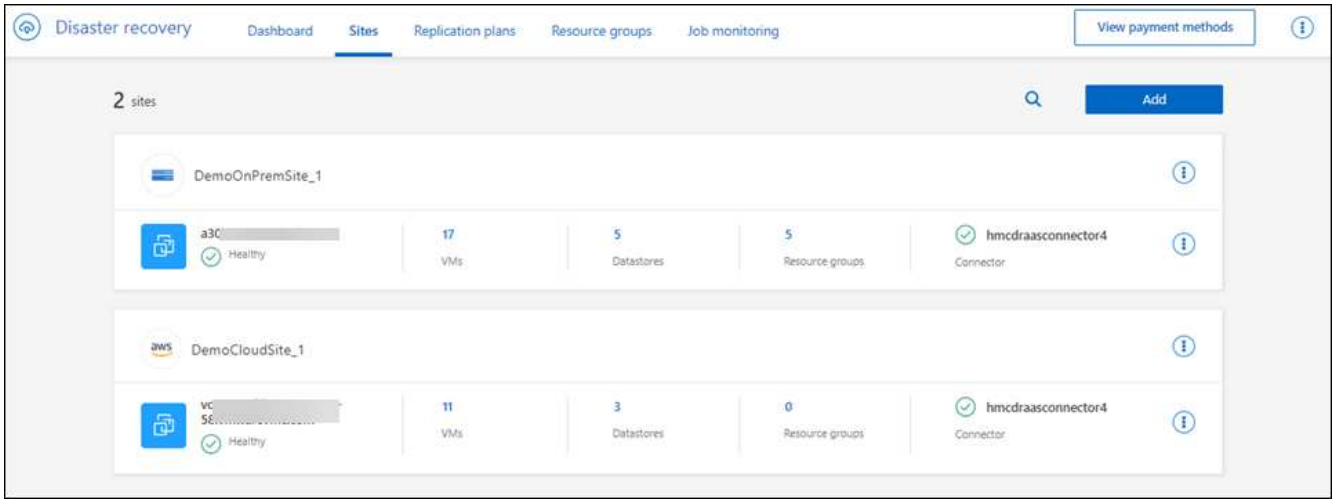
   Successivamente, verrà aggiunto un vCenter di destinazione.

4. **Destinazione**:

   a. Scegliere il sito di destinazione e la posizione. Se la destinazione è cloud, selezionare **AWS**.
      - (Si applica solo ai siti cloud) **token API**: Immettere il token API per autorizzare l'accesso al servizio per l'organizzazione. Creare il token API fornendo ruoli di organizzazione e servizio specifici.
      - (Applicabile solo ai siti cloud) **Long Organization ID**: Immettere l'ID univoco per l'organizzazione. È possibile identificare questo ID facendo clic sul nome utente nella sezione account della console BlueXP .

   b. Selezionare **Aggiungi**.

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



5. Per visualizzare lo stato di avanzamento dell'operazione, dal menu superiore, selezionare **monitoraggio processi**.

Aggiungere la mappatura della subnet per un sito vCenter

Gestire gli indirizzi IP in caso di failover in un nuovo modo utilizzando la mappatura delle subnet, che consente di aggiungere sottoreti per ogni vCenter. In tal caso, definire IPv4 CIDR, il gateway predefinito e il DNS per ogni rete virtuale.

In caso di failover, BlueXP Disaster Recovery determina l'indirizzo IP appropriato di ogni vNIC guardando il CIDR fornito per la rete virtuale mappata e la utilizza per derivare il nuovo indirizzo IP.

Ad esempio:

- Rete a = 10,1.1.0/24
- Rete B = 192.168.1.0/24

VM1 dispone di una vNIC (10,1.1,50) collegata a NetworkA. NetworkA viene mappato su NetworkB nelle impostazioni del piano di replica.

In caso di failover, il disaster recovery di BlueXP sostituisce la parte Network dell'indirizzo IP originale (10,1.1) e mantiene l'indirizzo host (.50) dell'indirizzo IP originale (10,1.1,50). Per VM1, BlueXP 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.

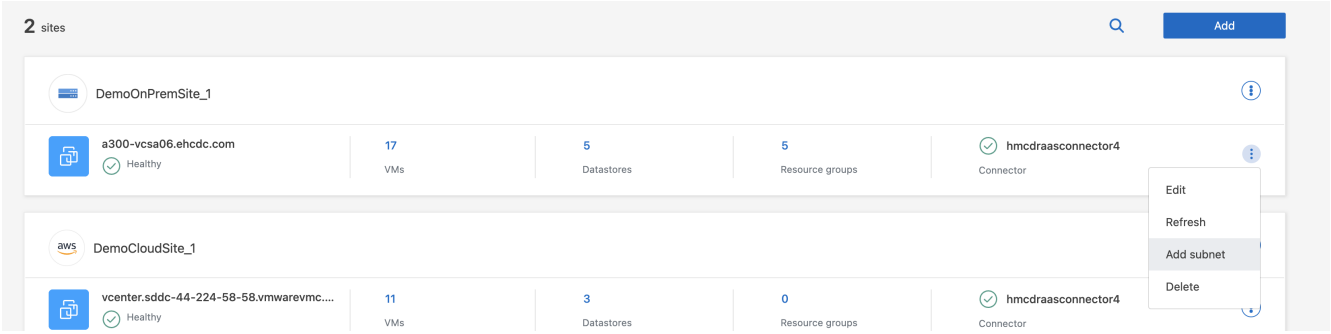
Riassumendo, l'indirizzo dell'host rimane lo stesso, mentre l'indirizzo di rete viene sostituito con quello configurato nella mappatura della subnet del sito. Ciò consente di gestire più facilmente la riassegnazione degli indirizzi IP al momento del failover, specialmente se si devono gestire centinaia di reti e migliaia di macchine virtuali.

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

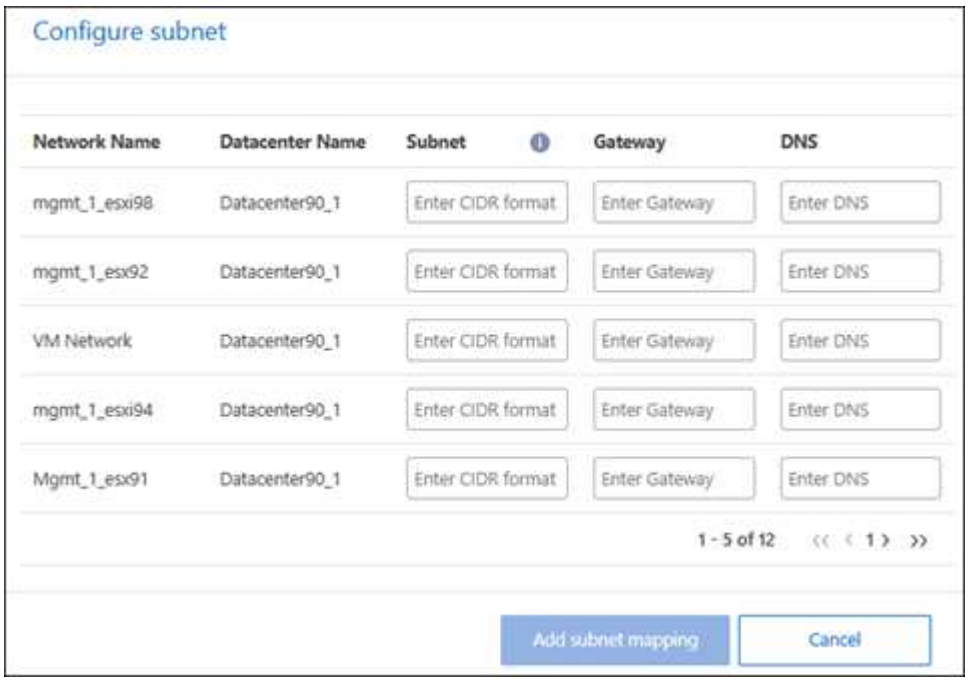
- Innanzitutto, aggiungere la mappatura della subnet per ogni sito vCenter.
- In secondo luogo, nel piano di replica, indicare che si desidera utilizzare la mappatura della subnet.

Fasi

1. Dal menu di ripristino di emergenza BlueXP , selezionare **Siti**.
2. Dall'icona azioni a destra, selezionare **Aggiungi subnet**.



Viene visualizzata la pagina Configure subnet (Configura subnet):



3. Nella pagina Configure subnet (Configura subnet), inserire le seguenti informazioni:
   a. Subnet: Inserire IPv4 CIDR 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 maschera di rete. Il numero è costituito da un indirizzo IP con il numero dopo "/" che 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: Inserire il gateway predefinito per la subnet.
   c. DNS: Inserire il DNS della subnet.
4. Selezionare **Aggiungi mappatura subnet**.

Selezionare la mappatura della subnet per un piano di replica

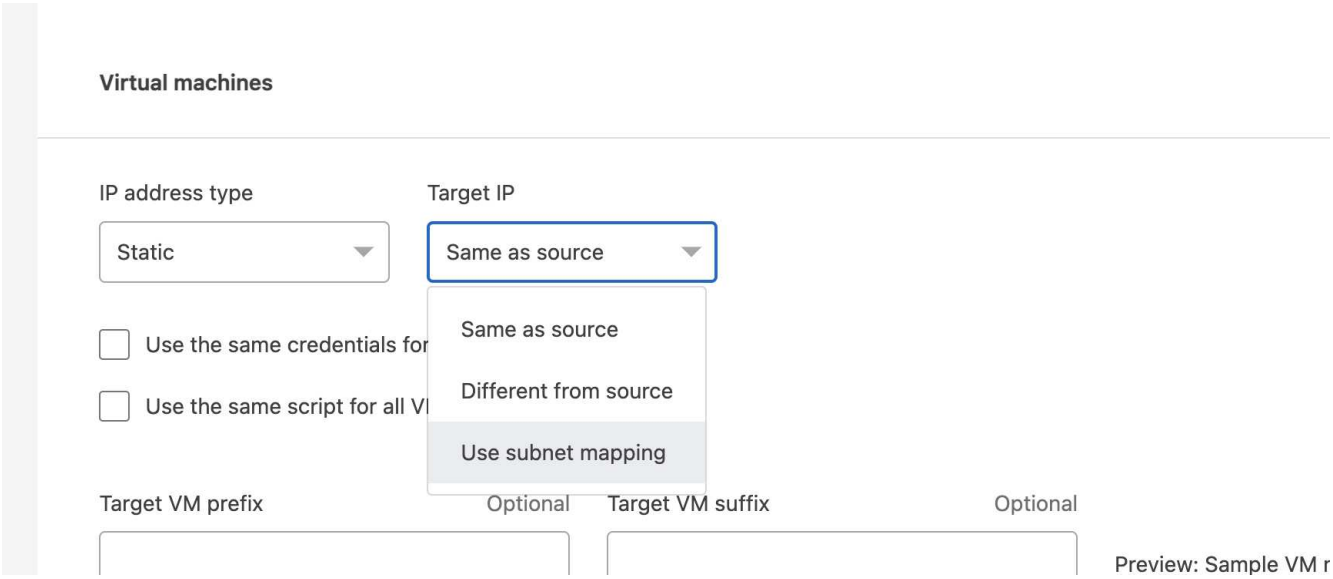
Quando si crea un piano di replica, è possibile selezionare la mappatura della subnet per il piano di replica.

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

- Innanzitutto, aggiungere la mappatura della subnet per ogni sito vCenter.
- In secondo luogo, nel piano di replica, indicare che si desidera utilizzare la mappatura della subnet.

Fasi

1. Dal menu superiore del disaster recovery di BlueXP, selezionare **piani di replica**.
2. Selezionare **Aggiungi** per aggiungere un piano di replica.
3. Completare i campi nel modo usuale aggiungendo i server vCenter, selezionando i gruppi di risorse o le applicazioni e completando le mappature.
4. Nella pagina piano di replica > mappatura delle risorse, selezionare la sezione **macchine virtuali**.



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

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

6. Continuare con la creazione del piano di replica.

Modificare il sito del server vCenter e personalizzare la pianificazione del rilevamento

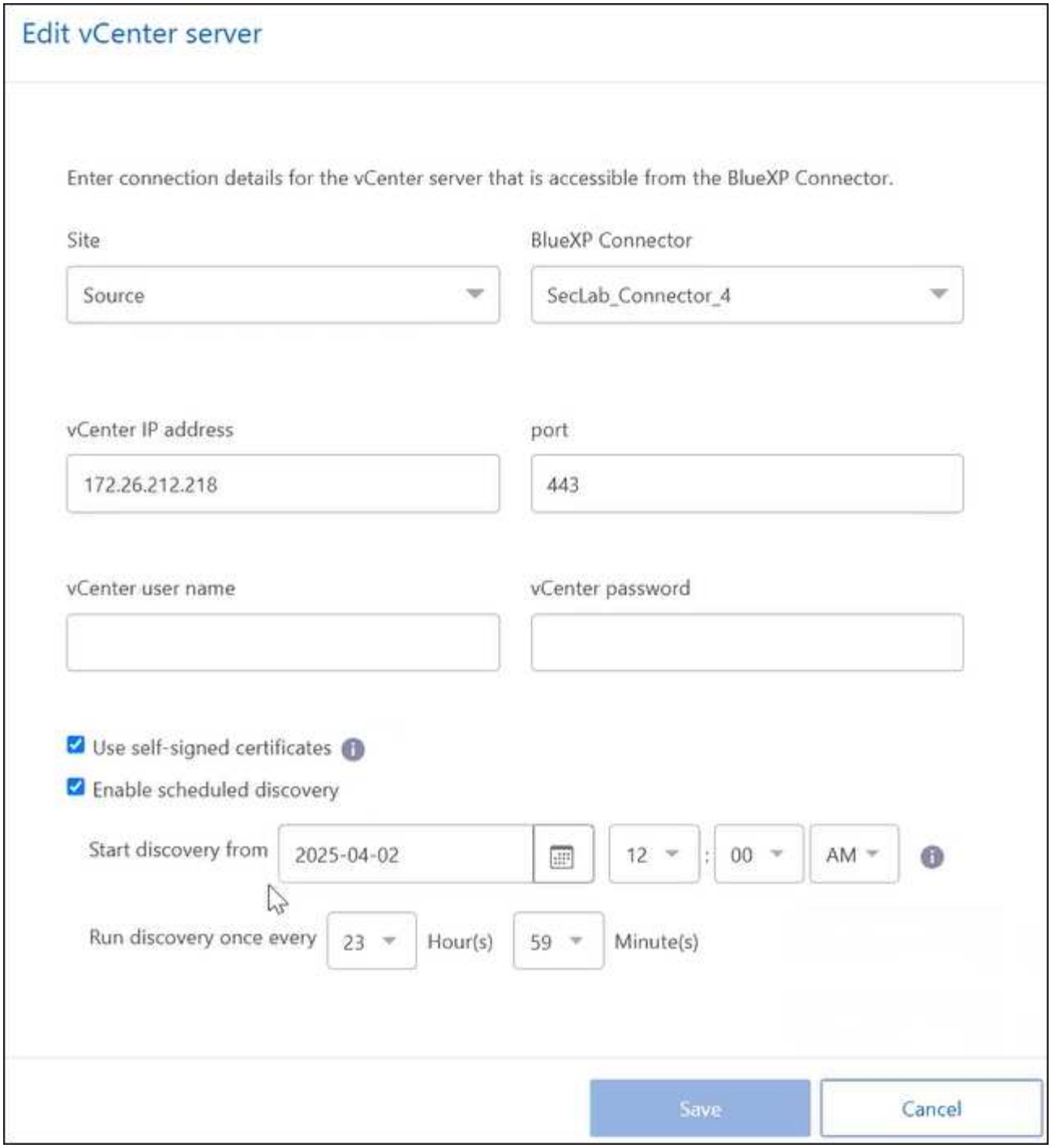
È possibile modificare il sito del server vCenter per personalizzare la pianificazione del rilevamento. Ad esempio, se si dispone di un numero elevato di macchine virtuali, è possibile impostare la pianificazione del rilevamento in modo che venga eseguita ogni 23 ore e 59 minuti. Se si dispone di un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

Se nelle release precedenti sono stati aggiunti vCenter e si desidera personalizzare la pianificazione del rilevamento, è necessario modificare il sito del server vCenter e impostare la pianificazione.

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

Fasi

1. Dal menu di ripristino di emergenza di BlueXP , selezionare **Siti**.
2. Selezionare il sito che si desidera modificare.
3. Selezionare l'icona azioni  a destra e selezionare **Modifica**.
4. Nella pagina Modifica server vCenter, modificare i campi in base alle esigenze.
5. Per personalizzare la pianificazione della ricerca, selezionare la casella **Abilita ricerca pianificata** e selezionare la data e l'intervallo di tempo desiderati.



6. Selezionare **Salva**.

Aggiornare la ricerca manualmente

È possibile aggiornare la ricerca manualmente in qualsiasi momento. Ciò è utile se sono state aggiunte o rimosse macchine virtuali e si desidera aggiornare le informazioni in BlueXP Disaster Recovery.

Fasi

1. Dal menu di ripristino di emergenza di BlueXP , selezionare **Siti**.
2. Selezionare il sito che si desidera aggiornare.
3.

Selezionare l'icona azioni  a destra e selezionare **Aggiorna**.

Crea un gruppo di risorse per organizzare insieme le VM nel ripristino di emergenza di BlueXP

Una volta aggiunti siti vCenter, potresti voler creare gruppi di risorse che raggruppano le macchine virtuali in base alle macchine virtuali o ai datastore. I gruppi di risorse consentono di organizzare una serie di macchine virtuali dipendenti in gruppi logici che soddisfano le proprie esigenze. Ad esempio, è possibile raggruppare le macchine virtuali associate a un'applicazione oppure raggruppare le applicazioni con livelli simili. Come altro esempio, i gruppi potrebbero contenere ordini di avvio ritardati che possono essere eseguiti al momento del ripristino.

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Puoi raggruppare macchine virtuali in maniera autonoma o macchine virtuali in datastore.

È possibile creare gruppi di risorse utilizzando i seguenti metodi:

- Dalla scheda gruppi di risorse
- Durante la creazione di un piano di disaster recovery o di *replica*. Se si dispone di molte macchine virtuali 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 replica".

Ogni gruppo di risorse può includere una o più macchine virtuali o datastore. Le macchine virtuali si accenderanno in base alla sequenza in cui vengono incluse nel piano di replica. È possibile modificare l'ordine trascinando le macchine virtuali o gli archivi dati 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 macchine virtuali o datastore che includono macchine virtuali correlate a livello operativo e che devono essere protette come una singola unità.

Ad esempio, un'applicazione point-of-sale potrebbe essere costituita da diverse macchine virtuali che ospitano database, diverse macchine virtuali che ospitano la gestione delle regole della logica aziendale e diverse macchine virtuali che fungono da storefront basato su webserver. Gestire la disponibilità dell'intera applicazione con un singolo processo di protezione può essere vantaggioso collocare queste VM in un singolo gruppo di risorse.

Con i gruppi di risorse impostati, è possibile applicare le regole del piano di replica per l'ordine di avvio corretto della VM, la connessione di rete e altro ancora per garantire il ripristino corretto di tutte le VM richieste per l'applicazione.

Come funziona?

Il disaster recovery di BlueXP protegge le macchine virtuali replicando i volumi ONTAP sottostanti e i LUN che

ospitano le macchine virtuali nel gruppo di risorse. A tale scopo, il sistema esegue una query in vCenter per individuare il nome di ciascun datastore che ospita le macchine virtuali in un gruppo di risorse. Il disaster recovery di BlueXP identifica quindi il volume ONTAP di origine o la LUN che ospita quel datastore. Tutta la protezione viene eseguita a livello di volume ONTAP utilizzando la replica SnapMirror.

Se le VM nel gruppo di risorse sono ospitate in diversi datastore, il disaster recovery di BlueXP utilizza uno dei seguenti metodi per creare una snapshot coerente con i dati dei volumi ONTAP o delle LUN.

Posizione relativa dei volumi FlexVol	**Processo di replica Snapshot**
Archivi dati multipli - volumi FlexVol nella **stessa SVM**	• Gruppo di coerenza ONTAP creato • Istantanee del gruppo di coerenza acquisite • Esecuzione della replica SnapMirror con ambito di volume
Archivi di dati multipli - volumi FlexVol in **più SVM**	• API ONTAP: `cg_start`. Consente di chiudere tutti i volumi in modo da creare snapshot e avviare snapshot con ambito di volume di tutti i volumi dei gruppi di risorse. • API ONTAP: `cg_end`. Riprende l'i/o su tutti i volumi e consente la replica SnapMirror con ambito di volume dopo la creazione di snapshot.

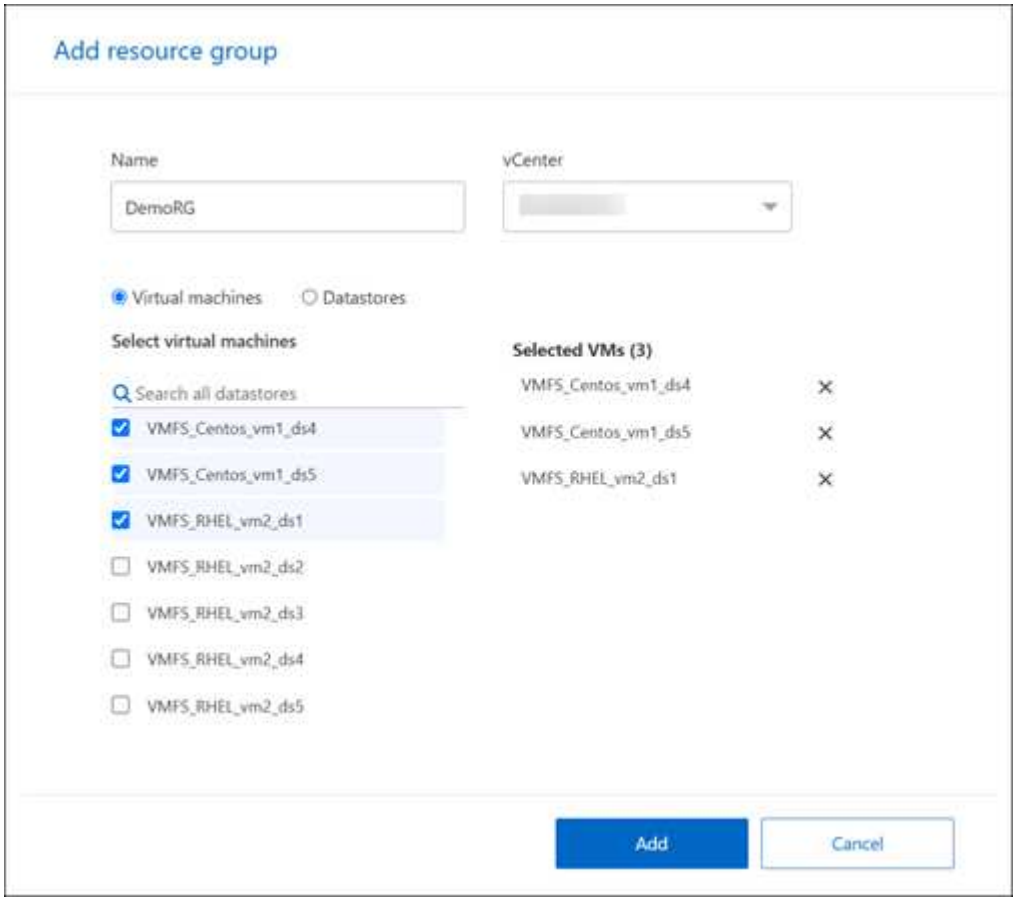
Quando si creano gruppi di risorse, considerare i seguenti aspetti:

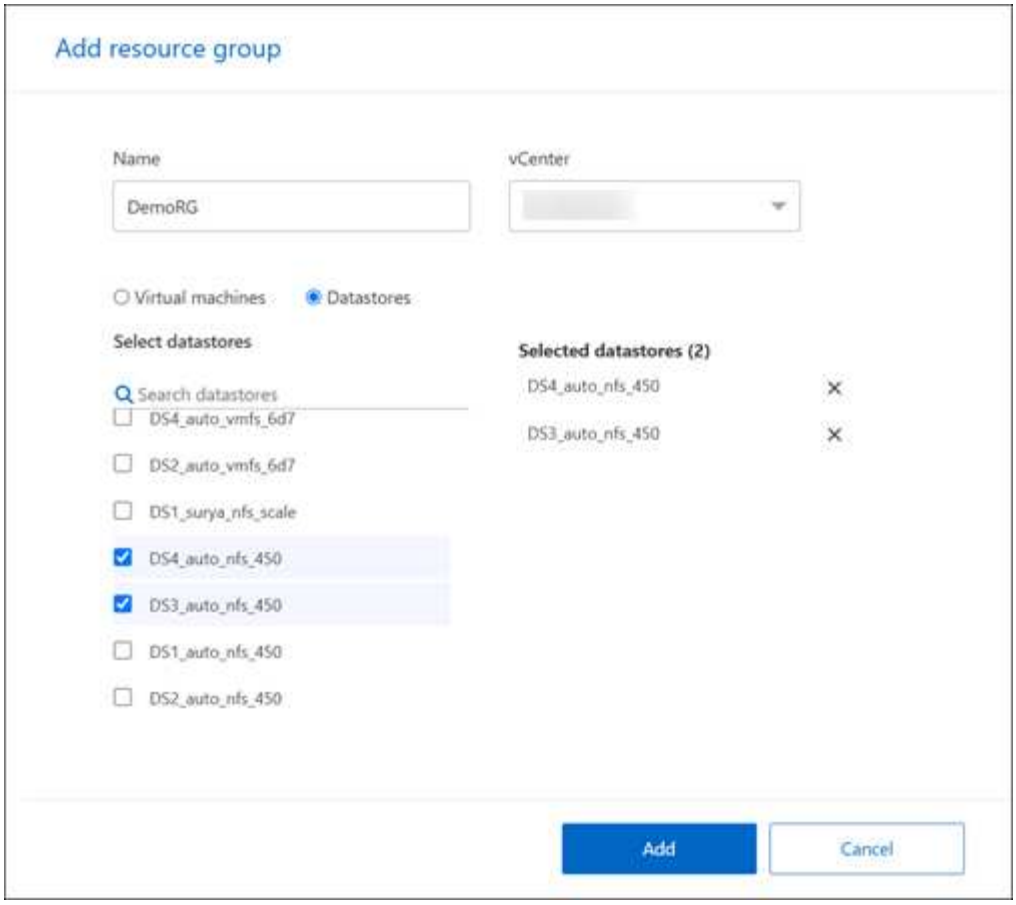
- Prima di aggiungere datastore ai gruppi di risorse, avviare prima un rilevamento manuale o un rilevamento pianificato delle macchine virtuali. In questo modo si garantisce che le VM vengano rilevate ed elencate nel gruppo di risorse. Se non si attiva una ricerca manuale, le VM potrebbero non essere elencate nel gruppo di risorse.
- Assicurarsi che nel datastore sia presente almeno una macchina virtuale. Se nel datastore non sono presenti macchine virtuali, il datastore non verrà rilevato.
- Un singolo datastore non deve ospitare macchine virtuali protette da più di un piano di replica.
- Non ospitare macchine virtuali protette e non protette nello stesso datastore. Se le macchine virtuali protette e non protette sono ospitate nello stesso datastore, possono verificarsi i seguenti problemi:
  - Poiché il disaster recovery di BlueXP utilizza SnapMirror e il sistema replica interi ONTAP Volume, la capacità utilizzata di quel volume viene utilizzata per prendere in considerazione la licenza. In questo caso, lo spazio del volume occupato dalle macchine virtuali protette e non protette sarebbe incluso in questo calcolo.
  - Se il gruppo di risorse e i datastore associati devono essere sottoposti a failover nel sito di disaster recovery, qualsiasi macchina virtuale non protetta (macchine virtuali non appartenenti al gruppo di risorse ma ospitate nel volume ONTAP) non esisterà più sul sito di origine dal processo di failover, con conseguente guasto di macchine virtuali non protette nel sito di origine. Inoltre, il disaster recovery di BlueXP non avvierà le macchine virtuali non protette sul sito vCenter di failover.
- Per avere una VM protetta, deve essere inclusa in un gruppo di risorse.

BEST PRACTICE: Organizzare le macchine virtuali prima di implementare il disaster recovery di BlueXP per ridurre al minimo la "proliferazione dei datastore". Posiziona le macchine virtuali che richiedono protezione su un sottoinsieme di datastore e posiziona le macchine virtuali che non verranno protette in un altro sottoinsieme di datastore. Assicurarsi che le macchine virtuali di un determinato datastore non siano protette da piani di replica diversi.

Fasi

1. Dal menu disaster recovery di BlueXP , selezionare **gruppi di risorse**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il gruppo di risorse.
4. Selezionare il cluster vCenter di origine in cui si trovano le VM.
5. Selezionare **macchine virtuali** o **Datastores** a seconda della modalità di ricerca.
6. Selezionare la scheda **Aggiungi gruppi di risorse**. Il sistema elenca tutti i datastore o le macchine virtuali nel cluster vCenter selezionato. Se è stato selezionato **Datastores**, il sistema elenca tutti gli archivi dati nel cluster vCenter selezionato. Se si seleziona **macchine virtuali**, il sistema elenca tutte le macchine virtuali nel cluster vCenter selezionato.
7. Sul lato sinistro della pagina Aggiungi gruppi di risorse, selezionare le macchine virtuali che si desidera proteggere.





8. Facoltativamente, modificare l'ordine delle VM a destra trascinando ciascuna VM verso l'alto o verso il basso nell'elenco. Le VM si accenderanno in base alla sequenza in cui vengono incluse.
9. Selezionare **Aggiungi**.

Creare un piano di replicazione nel ripristino di emergenza di BlueXP

Una volta aggiunti i siti vCenter, sarai pronto a creare un disaster recovery o un *piano di replica*. 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 macchine virtuali (VM) associate a un'applicazione o raggruppare applicazioni con livelli simili.

Tali piani sono a volte chiamati *blueprint*.

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

È possibile creare un piano di replica e modificare le pianificazioni per la conformità e il test.

Puoi proteggere più VM su datastore multipli. Il disaster recovery di BlueXP crea gruppi di coerenza ONTAP

per tutti i volumi ONTAP che ospitano datastore di macchine virtuali protetti.

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

- Pronti
- Failback confermata
- Verifica failover confermata

Creare il piano

Una procedura guidata consente di eseguire le seguenti operazioni:

- Seleziona i server vCenter.
- Seleziona le macchine virtuali o gli archivi dati che desideri replicare e assegnare gruppi di risorse.
- Mappare la modalità di mappatura delle risorse dall'ambiente di origine alla destinazione.
- Identificare la ricorrenza, eseguire uno script ospitato da guest, impostare l'ordine di avvio e selezionare l'obiettivo del punto di ripristino.
- Rivedere il piano.

Quando si crea il piano, è necessario attenersi alle seguenti linee guida:

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

Prima di iniziare

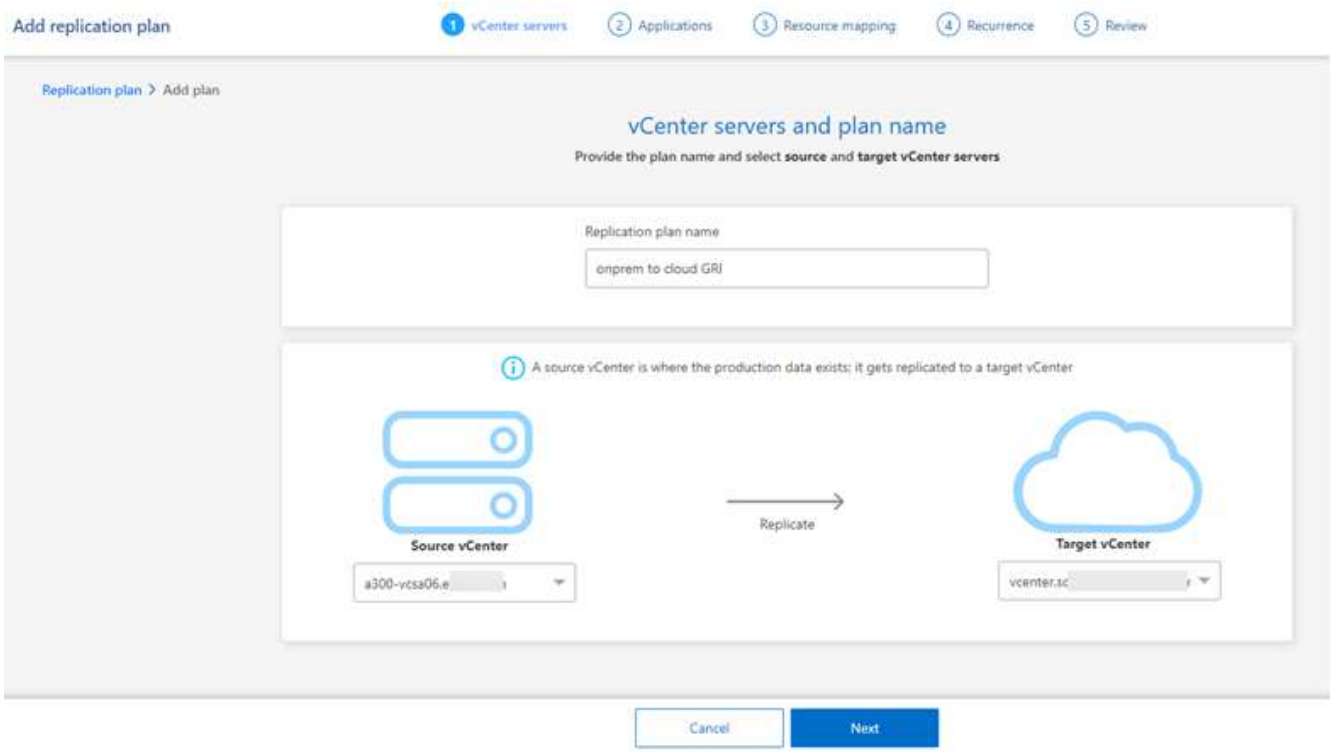
Per creare una relazione di SnapMirror in questo servizio, il cluster e il relativo peering SVM dovrebbero essere già stati impostati al di fuori del disaster recovery di BlueXP.

Seleziona i server vCenter

Prima di tutto, seleziona il vCenter di origine e poi il vCenter di destinazione.

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu principale di ripristino di emergenza di BlueXP , selezionare **piani di replica** e selezionare **Aggiungi**. In alternativa, se si sta appena iniziando a utilizzare il servizio, nel Dashboard selezionare **Aggiungi piano di replica**.



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

Selezionare le applicazioni da replicare e assegnare gruppi di risorse

La fase successiva consiste nel raggruppare le VM o i datastore richiesti in gruppi di risorse funzionali. I gruppi di risorse consentono di proteggere un set di macchine virtuali o datastore con una snapshot comune.

Quando selezioni le applicazioni nel piano di replica, puoi vedere il sistema operativo per ogni macchina virtuale o datastore nel piano. Che è utile per decidere come raggruppare macchine virtuali o datastore in un gruppo di risorse.

Ogni gruppo di risorse può includere una o più macchine virtuali o datastore.

Quando si creano gruppi di risorse, considerare i seguenti aspetti:

- Prima di aggiungere datastore ai gruppi di risorse, avviare prima un rilevamento manuale o un rilevamento pianificato delle macchine virtuali. In questo modo si garantisce che le VM vengano rilevate ed elencate nel gruppo di risorse. Se non si attiva una ricerca manuale, le VM potrebbero non essere elencate nel gruppo di risorse.
- Assicurarsi che nel datastore sia presente almeno una macchina virtuale. Se nel datastore non sono presenti macchine virtuali, il datastore non verrà rilevato.
- Un singolo datastore non deve ospitare macchine virtuali protette da più di un piano di replica.
- Non ospitare macchine virtuali protette e non protette nello stesso datastore. Se le macchine virtuali protette e non protette sono ospitate nello stesso datastore, possono verificarsi i seguenti problemi:
  - Poiché il disaster recovery di BlueXP utilizza SnapMirror e il sistema replica interi ONTAP Volume, la capacità utilizzata di quel volume viene utilizzata per prendere in considerazione la licenza. In questo

caso, lo spazio del volume occupato dalle macchine virtuali protette e non protette sarebbe incluso in questo calcolo.

- Se il gruppo di risorse e i datastore associati devono essere sottoposti a failover nel sito di disaster recovery, qualsiasi macchina virtuale non protetta (macchine virtuali non appartenenti al gruppo di risorse ma ospitate nel volume ONTAP) non esisterà più sul sito di origine dal processo di failover, con conseguente guasto di macchine virtuali non protette nel sito di origine. Inoltre, il disaster recovery di BlueXP non avvierà le macchine virtuali non protette sul sito vCenter di failover.

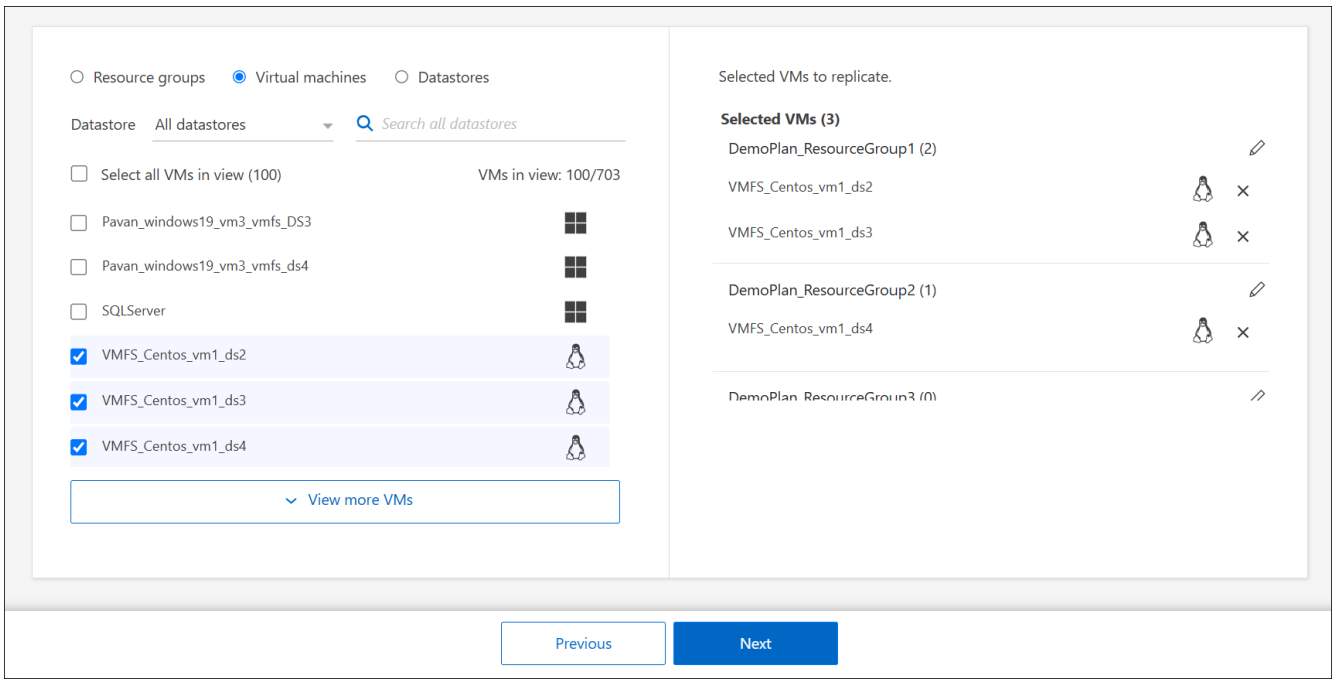
- Per avere una VM protetta, deve essere inclusa in un gruppo di risorse.

BEST PRACTICE: Organizzare le macchine virtuali prima di implementare il disaster recovery di BlueXP per ridurre al minimo la "proliferazione dei datastore". Posiziona le macchine virtuali che richiedono protezione su un sottoinsieme di datastore e posiziona le macchine virtuali che non verranno protette in un altro sottoinsieme di datastore. Utilizza la protezione basata su datastore per garantire la protezione delle macchine virtuali di un datastore specifico.

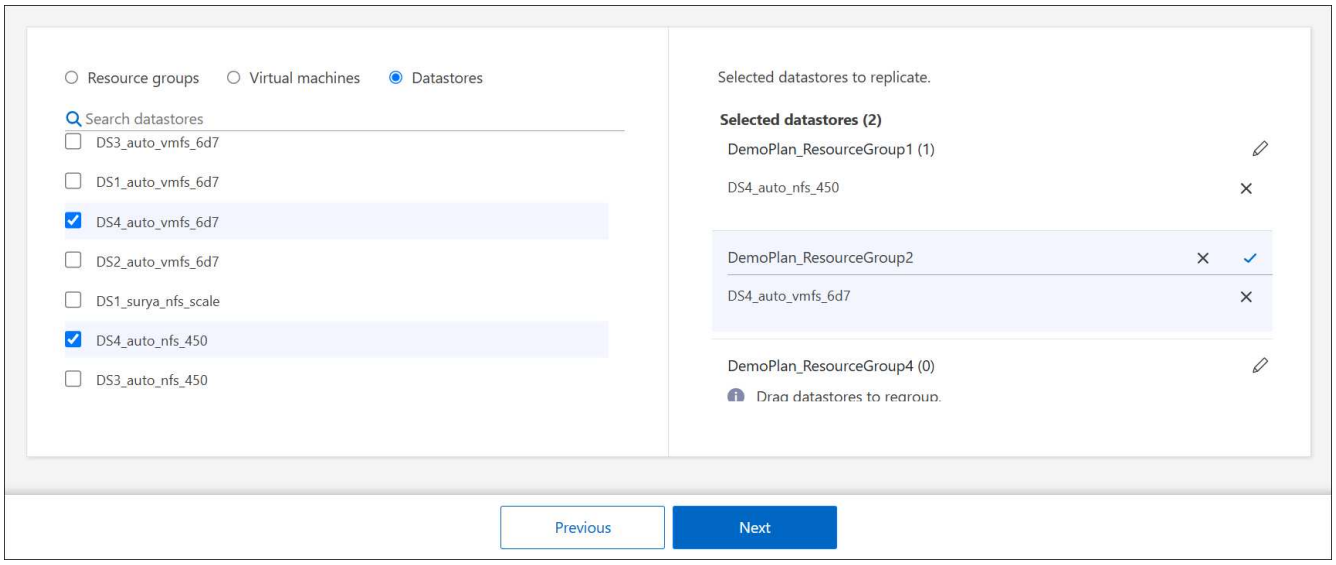
Fasi

1. Selezionare **macchine virtuali** o **archivi dati**.
2. È possibile cercare una macchina virtuale o un datastore specifici per nome.
3. Sul lato sinistro della pagina applicazioni, selezionare le macchine virtuali o gli archivi dati che si desidera proteggere e assegnare al gruppo selezionato.

   La risorsa selezionata viene aggiunta automaticamente 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, eseguire una delle seguenti operazioni:
   - Per modificare il nome del gruppo, fare clic sull'icona **Modifica** del gruppo .
   - Per rimuovere una risorsa da un gruppo, selezionare **X** accanto alla risorsa.
   - Per spostare una risorsa in un gruppo diverso, trascinarla e rilasciarla nel nuovo gruppo.

> Per spostare un datastore in un gruppo di risorse diverso, deselezionare l'archivio dati indesiderato e inviare il piano di replica. Quindi, creare o modificare l'altro piano di replica e riselezionare l'archivio dati.

5. Selezionare **Avanti**.

Mappare le risorse di origine alla destinazione

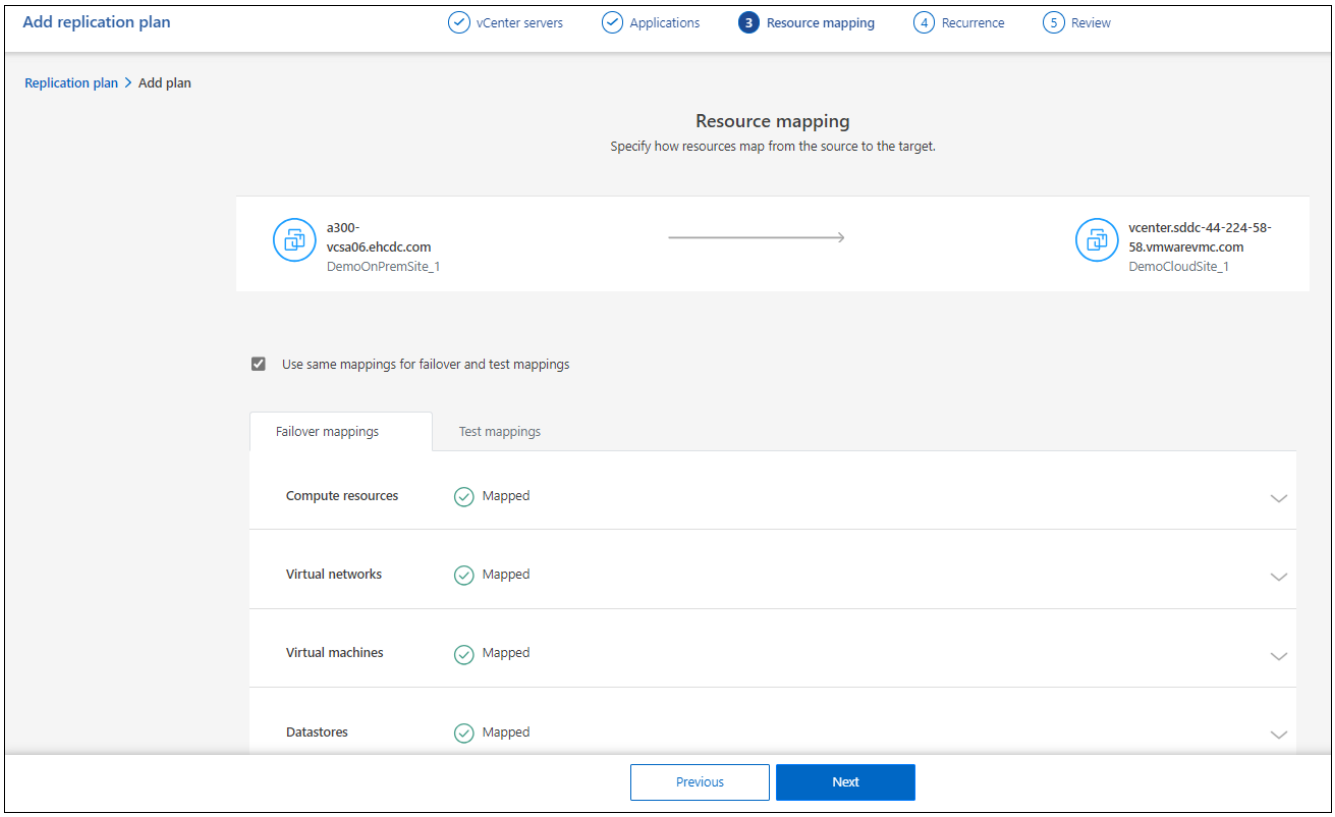
Nel passaggio mappatura risorse, specificare il modo in cui le risorse dell'ambiente di origine devono essere mappate alla destinazione. Quando si crea un piano di replica, è possibile impostare un ritardo di avvio e un ordine per ciascuna VM del piano. In questo modo è possibile impostare una sequenza di avvio delle VM.

Prima di iniziare

Per creare una relazione di SnapMirror in questo servizio, il cluster e il relativo peering SVM dovrebbero essere già stati impostati al di fuori del disaster recovery di BlueXP.

Fasi

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



2. Nella scheda Mapping di failover, selezionare la freccia verso il basso a destra di ciascuna risorsa e mappare le risorse in ciascuna.

Risorse mappa > risorse di calcolo

Selezionare la freccia giù accanto a **Compute resources** (Calcola risorse).

- **Datacenter di origine e destinazione**
- **Cluster di destinazione**
- **Host di destinazione** (opzionale): Dopo aver selezionato il cluster, è possibile impostare queste informazioni.

Se un vCenter ha un DRS (Distributed Resource Scheduler) configurato per gestire più host in un cluster, non è necessario selezionare un host. Se si seleziona un host, il disaster recovery di BlueXP posizionerà tutte le VM sull'host selezionato. * **Cartella VM di destinazione** (opzionale): Creare una nuova cartella principale per memorizzare le VM selezionate.

Risorse mappa > reti virtuali

Nella scheda mappature di failover, selezionare la freccia verso il basso accanto a **reti virtuali**. Selezionare la LAN virtuale di origine e la LAN virtuale di destinazione.

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

Risorse mappa > macchine virtuali

Nella scheda Mapping di failover, selezionare la freccia verso il basso accanto a **macchine virtuali**.

Viene mappato il valore predefinito per le macchine virtuali. La mappatura predefinita utilizza le stesse impostazioni utilizzate dalle macchine virtuali nell'ambiente di produzione (stesso indirizzo IP, subnet mask e gateway).

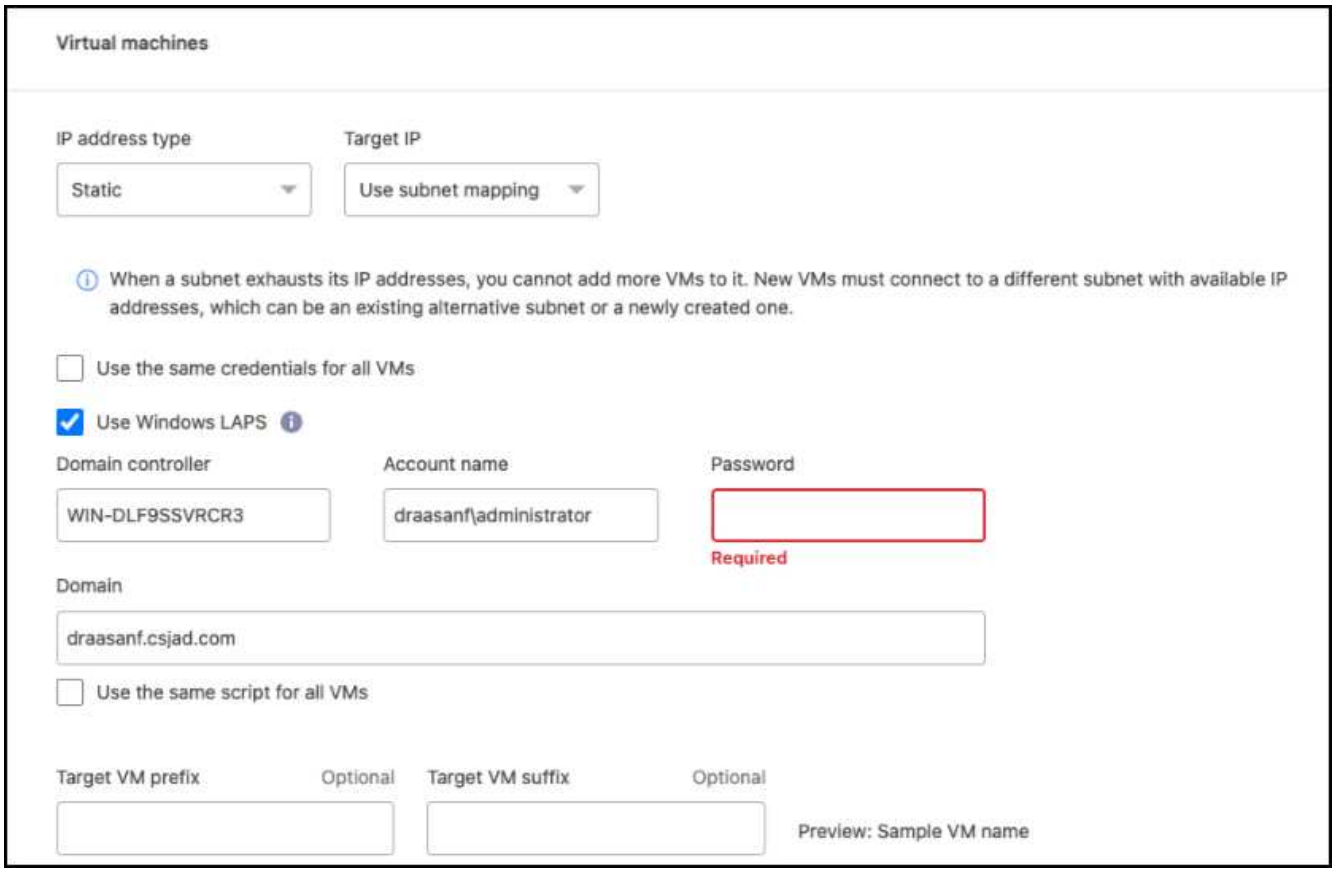
Se si apportano modifiche rispetto alle impostazioni predefinite, è necessario modificare il campo IP di destinazione in "diverso dall'origine".

Se si modificano le impostazioni in "diverso dall'origine", è necessario fornire le credenziali del sistema operativo guest della VM.

In questa sezione potrebbero essere visualizzati campi diversi a seconda della selezione effettuata.

- **Tipo di indirizzo IP**: Riconfigurare la configurazione delle VM in modo che corrisponda ai requisiti della rete virtuale di destinazione. Il disaster recovery di BlueXP 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 macchine virtuali ottengano informazioni sulla configurazione di rete da un server DHCP. Se si sceglie questa opzione, è necessario fornire solo le credenziali per la macchina virtuale.
  - **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, diversa dall'origine o mappatura della subnet. Se si sceglie lo stesso come origine, non è necessario immettere le credenziali. D'altro canto, se si sceglie di utilizzare informazioni diverse dall'origine, è possibile fornire le credenziali, l'indirizzo IP della macchina virtuale, la subnet mask, il DNS e le informazioni del gateway. Le credenziali del sistema operativo guest delle VM devono essere fornite a livello globale o a ciascun livello di VM.

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



- Nel campo **IP di destinazione**, seleziona una delle seguenti opzioni:
  - **Come la fonte**
  - **Diverso dalla fonte**
  - **Mappatura subnet**: selezionare questa opzione se si desidera mappare la subnet di origine a una subnet di destinazione diversa. È possibile selezionare la subnet di origine e quindi quella di destinazione. Questa opzione è utile quando si desidera modificare l'indirizzo IP della VM nell'ambiente di destinazione.

> L'utilizzo del mapping delle subnet è un processo facoltativo in due fasi: innanzitutto, aggiungere il mapping delle subnet per ciascun sito vCenter nella scheda Siti. In secondo luogo, nel piano di replica, indicare che si desidera utilizzare la mappatura della subnet.

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

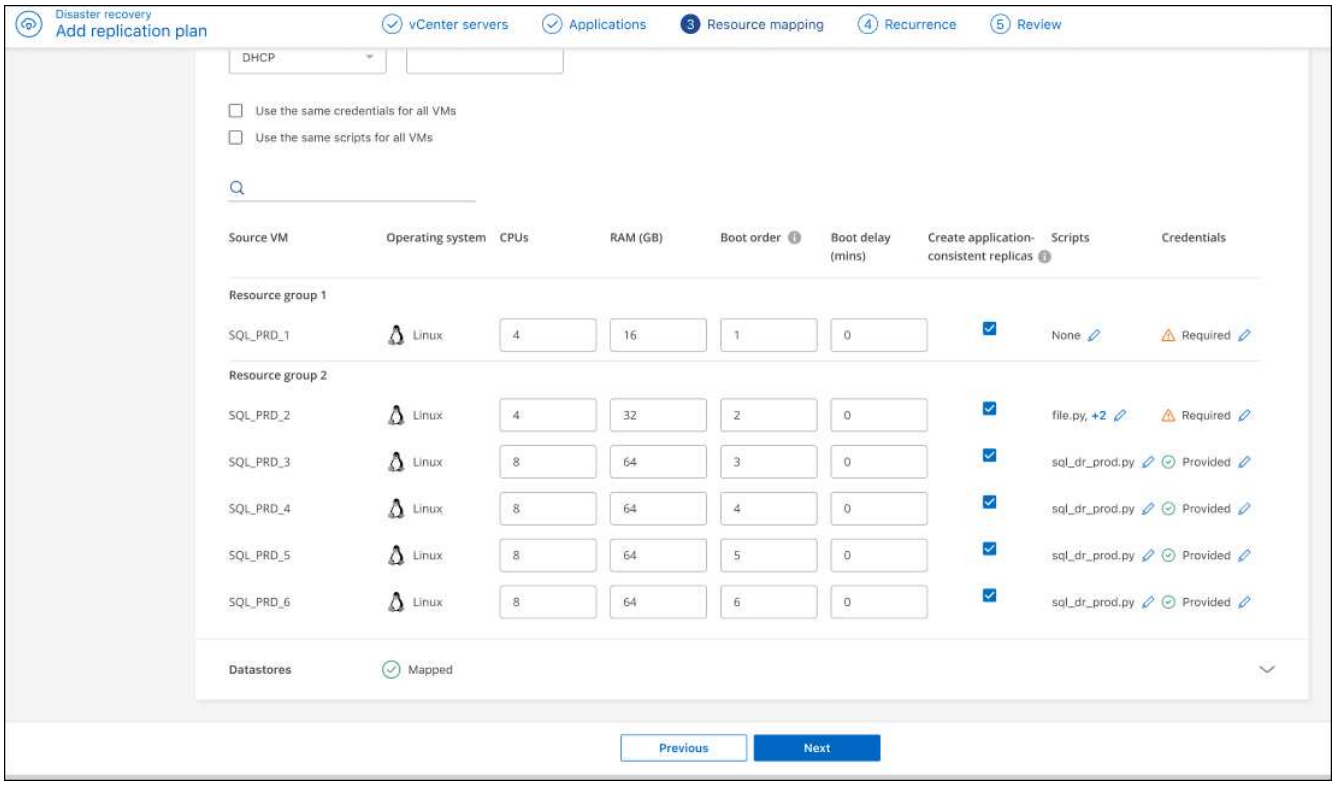
- **Utilizza Windows LAPS**: se si utilizza Windows Local Administrator Password Solution (Windows LAPS), selezionare questa casella. Questa opzione è disponibile solo se è stata selezionata l'opzione **IP statico**. Selezionando questa casella, non è necessario fornire una password per ciascuna macchina virtuale. È sufficiente fornire i dettagli del controller di dominio.

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

- **Scripts**: È possibile includere script personalizzati in formato .sh, .bat o .ps1 come processi di post-failover. Grazie agli script personalizzati, puoi fare in modo che il disaster recovery di BlueXP esegua lo

script dopo un processo di failover. Ad esempio, è possibile utilizzare uno script personalizzato per riprendere tutte le transazioni del database al termine del failover.

- **Prefisso e suffisso VM di destinazione**: Nei dettagli delle macchine virtuali è possibile aggiungere un prefisso e un suffisso al nome VM.
- **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.



- **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 macchine virtuali si avviano insieme in parallelo; tuttavia, è possibile apportare modifiche in questa fase. Questa operazione è utile per garantire che tutte le macchine virtuali con priorità 1 vengano eseguite prima dell'avvio delle macchine virtuali con priorità successiva.

  Tutte le macchine virtuali con lo stesso numero di ordine di avvio verranno avviate in parallelo.

  - Avvio sequenziale: Assegnare a ciascuna macchina virtuale un numero univoco per avviare nell'ordine assegnato, ad esempio 1,2,3,4,5.
  - Avvio simultaneo: Assegnare lo stesso numero a tutte le macchine virtuali per avviarle contemporaneamente, ad esempio 1,1,1,1,2,2,3,4,4.
- **Boot Delay**: Regola il ritardo in minuti dell'azione di avvio.

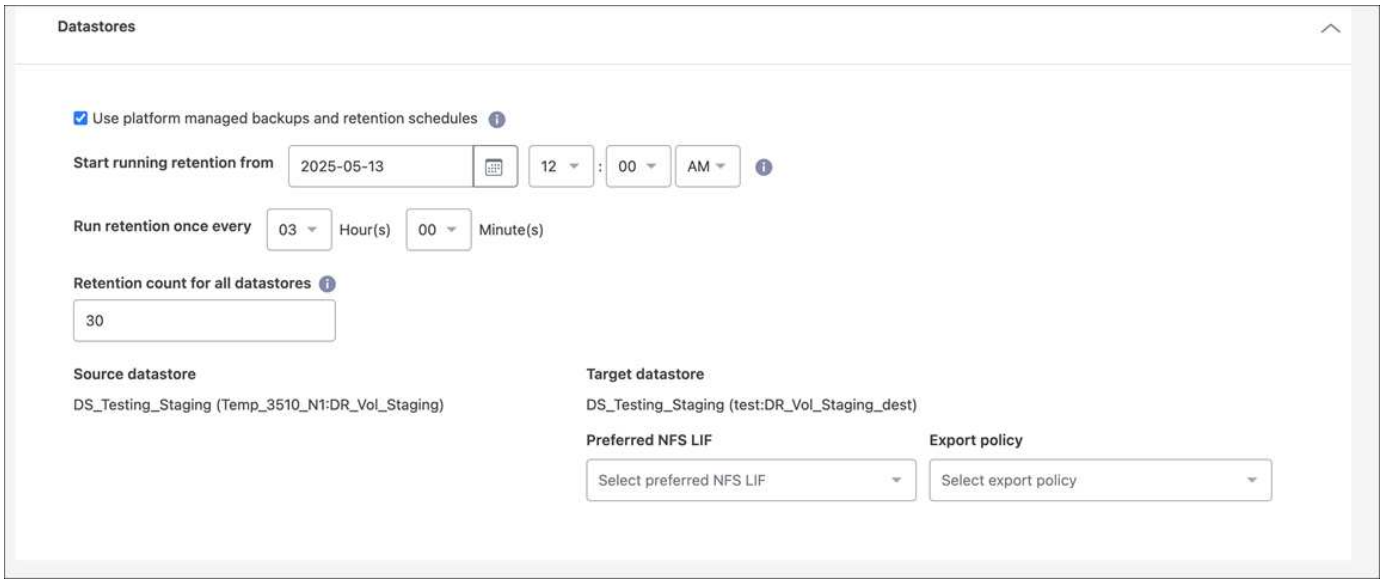
> Per ripristinare l'ordine di avvio predefinito, selezionare **Ripristina impostazioni VM predefinite**, quindi scegliere le impostazioni che si desidera ripristinare.

- **Crea repliche coerenti con l'applicazione**: Indica se creare copie snapshot coerenti con l'applicazione. Il servizio disattiverà l'applicazione, quindi acquisirà uno snapshot per ottenere uno stato coerente dell'applicazione. Questa funzionalità è supportata con Oracle in esecuzione su Windows e Linux e SQL Server in esecuzione su Windows.

Risorse mappa > sezione datastore

Selezionare la freccia verso il basso accanto a **Datastores**. In base alla selezione delle macchine virtuali, i mapping degli archivi dati vengono selezionati automaticamente.

Questa sezione potrebbe essere attivata o disattivata a seconda della selezione effettuata.



- **Utilizza backup gestiti dalla piattaforma e pianificazioni di conservazione**: Se si utilizza una soluzione di gestione delle istantanee esterna, selezionare questa casella. Il disaster recovery di BlueXP supporta l'utilizzo di soluzioni di gestione delle snapshot esterne, come lo scheduler nativo delle policy ONTAP SnapMirror o integrazioni di terze parti. Se ogni datastore (volume) nel piano di replica dispone già di una relazione SnapMirror che viene gestita altrove, puoi utilizzare tali snapshot come punti di recovery nel disaster recovery di BlueXP .

  Se selezionato, il ripristino di emergenza BlueXP non configura una pianificazione di backup. Tuttavia, è comunque necessario configurare un piano di conservazione, perché potrebbe essere ancora necessario creare snapshot per le operazioni di test, failover e failback.

  Dopo la configurazione, il servizio non acquisisce istantanee pianificate regolarmente, ma si affida all'entità esterna per acquisire e aggiornare tali istantanee.

- **Ora di inizio**: Immettere la data e l'ora in cui si desidera che i backup e la conservazione vengano eseguiti.
- **Intervallo di esecuzione**: Immettere l'intervallo di tempo in ore e minuti. Ad esempio, se si immette 1 ora, il servizio acquisirà un'istantanea ogni ora.
- **Conteggio di conservazione**: Immettere il numero di istantanee che si desidera conservare.
- **Datastore di origine e destinazione**: Se esistono più relazioni SnapMirror (fan-out), è possibile selezionare la destinazione da utilizzare. Se un volume ha già stabilito una relazione di SnapMirror, appariranno i datastore di origine e destinazione corrispondenti. Se un volume non ha una relazione SnapMirror, puoi crearlo subito selezionando un cluster di destinazione, selezionando una SVM di destinazione e fornendo un nome del volume. Il servizio crea la relazione tra volume e SnapMirror.

  Per creare una relazione di SnapMirror in questo servizio, il cluster e il relativo peering SVM dovrebbero essere già stati impostati al di fuori del disaster recovery di BlueXP.

  - Se le macchine virtuali provengono dallo stesso volume e dalla stessa SVM, il servizio esegue una

snapshot ONTAP standard e aggiorna le destinazioni secondarie.

- Se le macchine virtuali provengono da volumi diversi e dalla stessa SVM, il servizio crea uno snapshot del gruppo di coerenza includendo tutti i volumi e aggiornando le destinazioni secondarie.
- Se le VM provengono da volumi diversi e da SVM diverse, il servizio esegue una fase di avvio del gruppo di coerenza e applica la snapshot della fase includendo tutti i volumi nello stesso cluster o in un cluster diverso, quindi aggiorna le destinazioni secondarie.
- Durante il failover, è possibile selezionare uno snapshot qualsiasi. Se si seleziona la snapshot più recente, il servizio crea un backup on-demand, aggiorna la destinazione e utilizza tale snapshot per il failover.

Aggiungere mappature di failover di test

Fasi

1. Per impostare diverse mappature per l'ambiente di test, deselezionare la casella e selezionare la scheda **mappature di test**.
2. Passare attraverso ciascuna scheda come prima, ma questa volta per l'ambiente di test.

   Nella scheda Mapping test, le mappature macchine virtuali e archivi dati sono disattivate.

   In seguito, è possibile testare l'intero piano. In questo momento, si stanno impostando le mappature per l'ambiente di test.

Esaminare il piano di replica

Infine, dedicare qualche istante alla revisione del piano di replica.

È possibile disattivare o eliminare il piano di replica in un secondo momento.

Fasi

1. Esaminare le informazioni in ciascuna scheda: Dettagli del piano, mappatura di failover e VM.
2. Selezionare **Aggiungi piano**.

   Il piano viene aggiunto all'elenco dei piani.

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

È consigliabile impostare pianificazioni per verificare la conformità e i test di failover in modo da garantire che funzionino correttamente in caso di necessità.

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

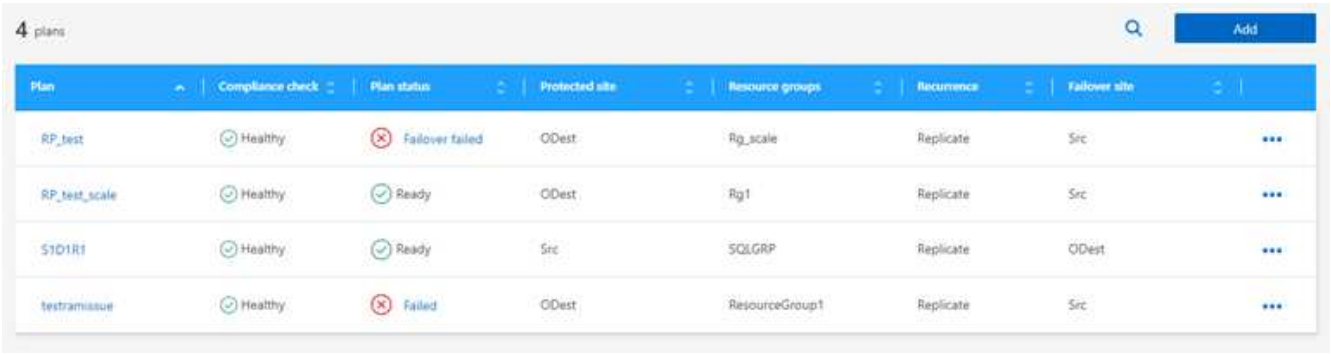
  Un failover di test crea un volume FlexClone, monta il datastore e sposta il carico di lavoro in quel datastore. Un'operazione di failover di test *non* influisce sui carichi di lavoro di produzione, sulla relazione

di SnapMirror utilizzata nel sito di test e sui carichi di lavoro protetti che devono continuare a funzionare normalmente.

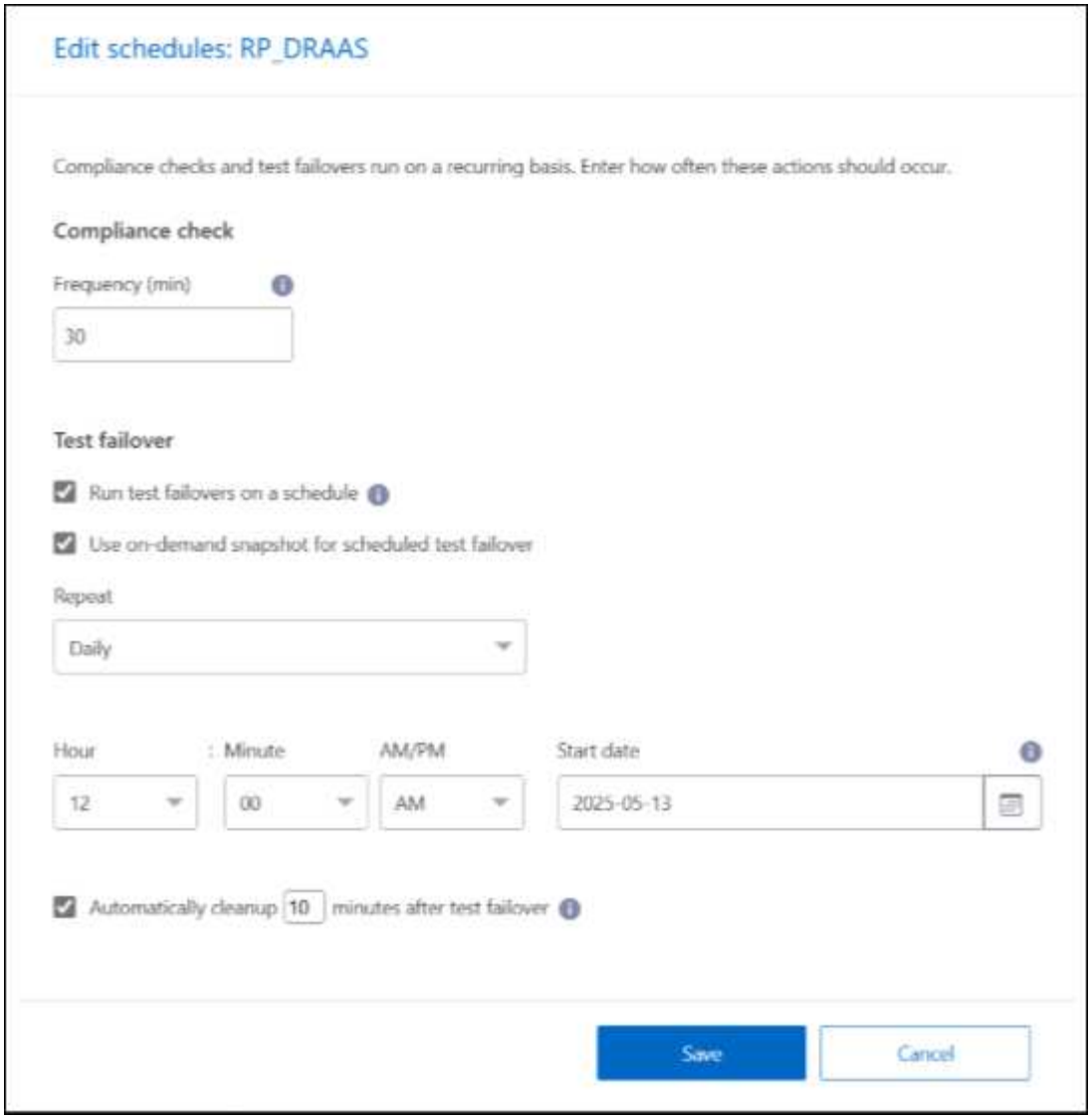
In base alla pianificazione, il test di failover viene eseguito e garantisce che i carichi di lavoro vengano spostati nella destinazione specificata dal piano di replica.

Fasi

1. Dal menu superiore del disaster recovery di BlueXP, selezionare **piani di replica**.



2. Selezionare **azioni** ••• E selezionare **Modifica pianificazioni**.
3. Inserisci con quale frequenza, in pochi minuti, vuoi che il disaster recovery di BlueXP verifichi la conformità ai test.
4. Per verificare che i test di failover siano integri, selezionare **Esegui failover in base a una pianificazione mensile**.
   a. Selezionare il giorno del mese e l'ora in cui si desidera eseguire i test.
   b. Immettere la data in formato aaaa-mm-gg quando si desidera avviare il test.



5. **Usa snapshot ondemand per il failover del test pianificato**: Per creare un nuovo snapshot prima di avviare il failover del test automatico, selezionare questa casella.
6. Per ripulire l'ambiente di test al termine del test di failover, selezionare **pulizia automatica dopo il failover di test** e immettere il numero di minuti che si desidera attendere prima dell'avvio della pulizia.

Questo processo disregistra le macchine virtuali temporanee dalla posizione di test, elimina il volume FlexClone creato e dismonta i datastore temporanei.

7. Selezionare **Salva**.

Replica le applicazioni su un altro sito con il ripristino di emergenza di BlueXP

Utilizzando il disaster recovery di BlueXP, puoi replicare le app VMware sul sito di origine in un sito remoto di disaster recovery nel cloud usando la replica SnapMirror.

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

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 il disaster recovery di BlueXP verifica l'effettivo svolgimento della replica secondo il piano. È possibile monitorare l'avanzamento nella pagina monitoraggio processi.

Prima di iniziare

Prima di avviare la replica, è necessario aver creato un piano di replica e selezionato per replicare le applicazioni. Quindi, nel menu azioni viene visualizzata l'opzione **Replica**.

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore, selezionare **piani di replica**.
3. Selezionare il piano di replica.
4. A destra, selezionare l'opzione **azioni** ••• E selezionare **Replica**.

Migrazione delle applicazioni su un altro sito con il ripristino di emergenza di BlueXP

Il disaster recovery di BlueXP ti permette di migrare le app VMware sul sito di origine in un altro sito.

Dopo aver creato il piano di replica, identificare la ricorrenza nella procedura guidata e avviare la migrazione, il disaster recovery di BlueXP verifica ogni 30 minuti che la migrazione avvenga effettivamente in base al piano. È possibile monitorare l'avanzamento nella pagina monitoraggio processi.

Prima di iniziare

Prima di iniziare la migrazione, è necessario aver creato un piano di replica e selezionato per migrare le applicazioni. Quindi, l'opzione **Migra** viene visualizzata nel menu azioni.

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore, selezionare **piani di replica**.
3. Selezionare il piano di replica.
4. A destra, selezionare l'opzione **azioni** ••• E selezionare **Migra**.

Eseguire il failover delle applicazioni su un sito remoto con il ripristino di emergenza BlueXP

In caso di disastro, esegui il failover del sito VMware on-premise primario in un altro sito VMware on-premise o in VMware Cloud on AWS. È possibile testare il processo di failover per garantire il successo quando necessario.

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Durante un failover viene utilizzata la copia snapshot SnapMirror più recente. In alternativa, puoi selezionare uno snapshot specifico da uno snapshot point-in-time, in base alla politica di conservazione di SnapMirror. L'opzione point-in-time può essere utile in caso di eventi di danneggiamento come il ransomware, in cui le repliche più recenti sono già compromesse o crittografate. Il disaster recovery di BlueXP mostra tutti i punti disponibili in tempo.

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:

- Guasto critico del sito di produzione nel quale il cluster vCenter o ONTAP di origine non è accessibile: Il disaster recovery di BlueXP ti consente di selezionare qualsiasi snapshot disponibile da ripristinare.
- L'ambiente di produzione è integro: È possibile "creare subito uno snapshot" o selezionare uno snapshot creato in precedenza.

Questa procedura interrompe il rapporto di replica, posiziona le macchine virtuali di origine di vCenter offline, registra i volumi come datastore in vCenter di disaster recovery, riavvia le macchine virtuali protette utilizzando le regole di failover del piano e consente la lettura/scrittura sul sito di destinazione.

Verificare il processo di failover

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

Durante un test di failover, le macchine virtuali vengono create temporaneamente. Il disaster recovery di BlueXP non mappa il volume di destinazione. Ma crea un nuovo volume FlexClone a partire dallo snapshot selezionato, mentre un datastore temporaneo di backup del volume FlexClone viene mappato agli host ESXi.

Questo processo non consuma capacità fisica aggiuntiva nello storage ONTAP on-premise o in FSX per lo storage NetApp ONTAP in AWS. Il volume di origine originale non viene modificato e i processi di replica possono continuare anche durante il ripristino di emergenza.

Al termine del test, è necessario reimpostare le macchine virtuali con l'opzione **Clean up test**. Sebbene questa opzione sia consigliata, non è necessaria.

Un'operazione di failover di test *non* influisce sui carichi di lavoro di produzione, sulla relazione di SnapMirror utilizzata nel sito di test e sui carichi di lavoro protetti che devono continuare a funzionare normalmente.

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore del disaster recovery di BlueXP, selezionare **piani di replica**.
3. Selezionare il piano di replica.
4. A destra, selezionare l'opzione **azioni** ••• E selezionare **Test failover**.
5. Nella pagina Test failover, immettere "Test failover" e selezionare **Test failover**.
6. Al termine del test, pulire l'ambiente di test.

Ripulire l’ambiente di test dopo un test di failover

Al termine del test di failover, è necessario ripulire l’ambiente di test. Questo processo rimuove le macchine virtuali temporanee dalla posizione di test, da FlexClone e dai datastore temporanei.

Fasi

1. Dal menu superiore del disaster recovery di BlueXP, selezionare **piani di replica**.
2. Selezionare il piano di replica.
3. A destra, selezionare l’opzione **azioni** ••• E selezionare **Clean up failover test**.
4. Nella pagina Test failover, immettere "Clean up failover" e selezionare **Clean up failover test**.

Esegui il failover del sito di origine su un sito di disaster recovery

In caso di disastro, potrai eseguire il failover on-demand del tuo sito VMware on-premise primario in un altro sito VMware on-premise o in VMware Cloud on AWS con FSX per NetApp ONTAP.

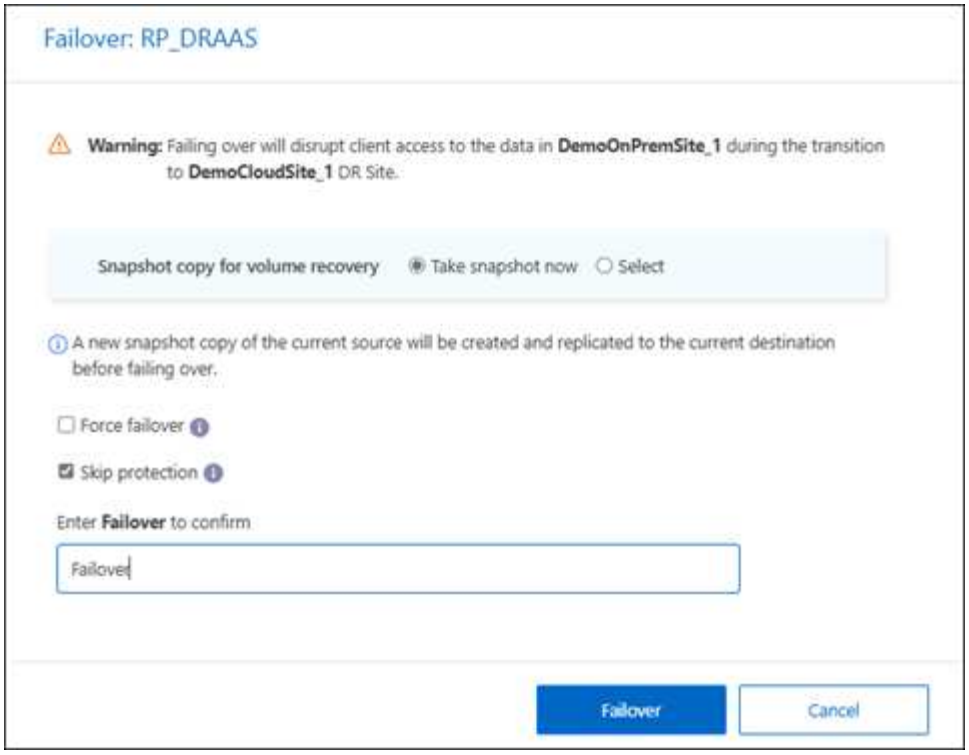
Il processo di failover comporta le seguenti operazioni:

- Se è stato selezionato l’ultimo snapshot, viene eseguito l’aggiornamento SnapMirror per replicare le ultime modifiche.
- Le macchine virtuali di origine sono spente.
- La relazione di SnapMirror viene interrotta e il volume di destinazione viene reso in lettura/scrittura.
- In base alla selezione dello snapshot, il file system attivo viene ripristinato allo snapshot specificato (ultimo o selezionato)
- I datastore vengono creati e montati sul cluster o sull’host VMware o VMC in base alle informazioni acquisite nel piano di replica.
- Le macchine virtuali di destinazione vengono registrate e attivate in base all’ordine acquisito nella pagina gruppi di risorse.
- Viene invertita la relazione di SnapMirror dalla macchina virtuale di destinazione a quella di origine.

Una volta avviato il 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 (carico di lavoro).

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore del disaster recovery di BlueXP, selezionare **piani di replica**.
3. Selezionare il piano di replica.
4. A destra, selezionare l’opzione **azioni** ••• E selezionare **failover**.



5. Nella pagina di failover, avviare uno snapshot ora o scegliere lo snapshot per il datastore da cui ripristinare. L'impostazione predefinita è l'ultima.

   Prima che si verifichi il failover, verrà acquisita e replicata una snapshot dell'origine corrente nella destinazione corrente.

6. Facoltativamente, selezionare **forza failover** se si desidera che il failover avvenga anche se viene rilevato un errore che normalmente impedirebbe il failover.
7. In alternativa, selezionare **Ignora protezione** se si desidera che il servizio non crei automaticamente una relazione di protezione SnapMirror inversa dopo il failover di un piano di replica. Questa funzione è utile se si desidera eseguire operazioni aggiuntive sul sito ripristinato prima di riportarlo online all'interno del disaster recovery di BlueXP .

   È possibile stabilire la protezione inversa selezionando **Proteggi risorse** dal menu azioni piano di replica. Questo tenta di creare una relazione di replica inversa per ogni volume nel piano. È possibile eseguire questo processo ripetutamente fino a quando non viene ripristinata la protezione. Una volta ripristinata la protezione, è possibile avviare un failback nel modo usuale.

8. Digitare "failover" nella casella.
9. Selezionare **failover**.
10. Per verificare l'avanzamento, nel menu superiore, selezionare **monitoraggio processi**.

Ripristina le applicazioni alla fonte originale con il ripristino di emergenza BlueXP

Dopo aver risolto un disastro, esegui il failback dal sito di disaster recovery al sito di origine per tornare alle normali operazioni. È possibile selezionare l'istantanea da cui

eseguire il ripristino.

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

In questo workflow, il disaster recovery di BlueXP replica (risincronizza) qualsiasi modifica alla macchina virtuale di origine prima di invertire la direzione della replica. Questo processo inizia da una relazione che ha completato il failover a una destinazione e prevede i seguenti passaggi:

- Sul sito di destinazione, le macchine virtuali vengono spente e non registrate e i volumi vengono dismontati.
- La relazione di SnapMirror nell'origine viene interrotta per renderla di lettura/scrittura.
- La relazione di SnapMirror viene risincronizzata per invertire la replica.
- Le macchine virtuali di origine sono accese e registrate e i volumi sono montati sull'origine.

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore del disaster recovery di BlueXP, selezionare **piani di replica**.
3. Selezionare il piano di replica.
4. A destra, selezionare l'opzione **azioni** ••• E selezionare **fail back**.
5. Immettere il nome del piano di replica per confermare e avviare il failback.
6. Scegliere lo snapshot per il datastore da cui eseguire il ripristino. L'impostazione predefinita è l'ultima.
7. Per verificare l'avanzamento, nel menu superiore, selezionare **monitoraggio processi**.

Gestisci siti, gruppi di risorse, piani di replica, datastore e informazioni sulle macchine virtuali con il disaster recovery di BlueXP

Puoi dare una rapida occhiata a tutte le risorse di disaster recovery di BlueXP o esaminarle singolarmente in dettaglio:

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

Le attività richiedono ruoli BlueXP diversi. Per maggiori dettagli, consulta la sezione **Ruolo BlueXP richiesto** in ogni attività.

"Scopri di più sui ruoli utente e sulle autorizzazioni nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Gestire i siti vCenter

Puoi modificare il nome del sito vCenter e il tipo di sito (on-premise o AWS).

Ruolo BlueXP obbligatorio Ruolo di amministratore dell'organizzazione, amministratore di cartelle o progetti o amministratore di ripristino di emergenza.

Fasi

1. Dal menu in alto, selezionare **Siti**.
2. Selezionare l'opzione **azioni**  A destra del nome vCenter e selezionare **Modifica**.
3. Modificare il nome e la posizione del sito vCenter.

Gestire i gruppi di risorse

Sebbene sia possibile aggiungere un gruppo di risorse come parte della creazione di un piano di replica, potrebbe essere più conveniente aggiungere i gruppi separatamente e in seguito utilizzare tali gruppi nel piano. Puoi creare gruppi di risorse per macchine virtuali o datastore.

Ruolo BlueXP obbligatorio 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 per 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 replica e si crea un gruppo di risorse all'interno del piano, è possibile visualizzare le macchine virtuali negli archivi dati.

È inoltre possibile modificare ed eliminare i gruppi di risorse.

Fasi

1. Dal menu superiore, selezionare **gruppi di risorse**.
2. Per aggiungere un gruppo di risorse, selezionare **Aggiungi gruppo**.
3. Per eseguire azioni con il gruppo di risorse, selezionare l'opzione **azioni** ••• A destra e selezionare una delle opzioni, ad esempio **Modifica gruppo di risorse** o **Elimina gruppo di risorse**.

Gestire i piani di replica

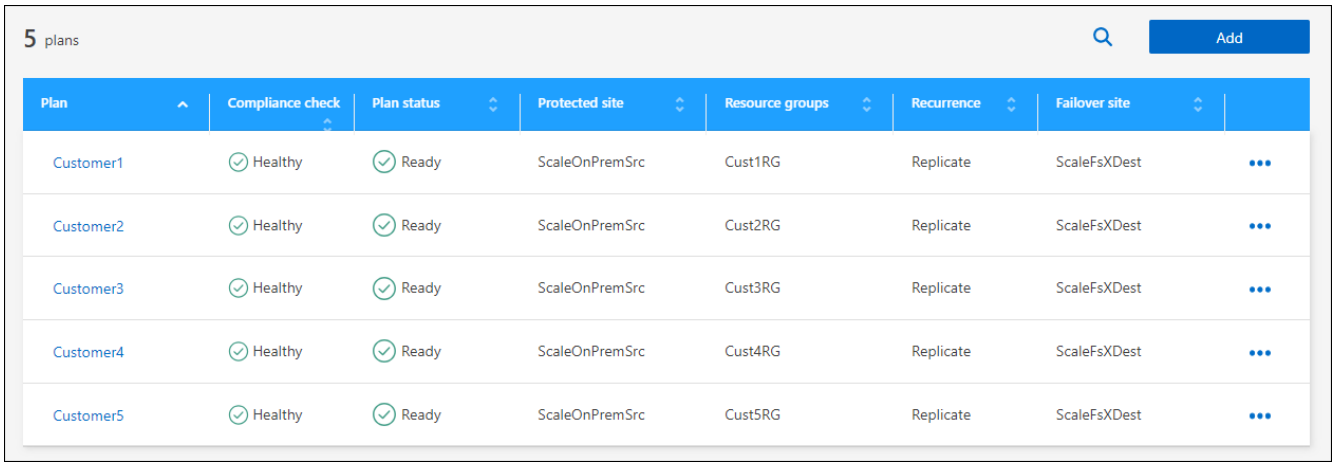
È possibile disattivare, attivare ed eliminare i piani di replica. È possibile modificare le pianificazioni.

Ruolo BlueXP obbligatorio 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 attivarlo in un secondo momento.
- Se il piano non è più necessario, è possibile eliminarlo.

Fasi

1. Dal menu superiore, selezionare **piani di replica**.



2. Per visualizzare i dettagli del piano, selezionare l'opzione **azioni** ••• E selezionare **Visualizza dettagli piano**.
3. Effettuare una delle seguenti operazioni:
   - Per modificare i dettagli del piano (modificare la ricorrenza), selezionare la scheda **Dettagli piano** e selezionare l'icona **Modifica** a destra.
   - Per modificare le mappature delle risorse, selezionare la scheda **mappatura failover** e selezionare l'icona **Modifica**.
   - Per aggiungere o modificare le macchine virtuali, selezionare la scheda **macchine virtuali** e selezionare l'opzione **Aggiungi macchine virtuali** o l'icona **Modifica**.
4. Tornare all'elenco dei piani selezionando "piani di replica" nelle breadcrumb in alto a sinistra.
5. Per eseguire azioni con il piano, dall'elenco dei piani di replica, selezionare l'opzione **azioni** ••• a destra del piano e selezionare una delle opzioni, come **Modifica pianificazioni**, **Test failover**, **fail over**, **fail back**, **Migrate**, **Take snapshot now**, **Clean up old snapshot**, **Disable**, **Enable** o **Delete**.
6. Per impostare o modificare una pianificazione di failover di test o impostare il controllo della frequenza di conformità, selezionare l'opzione **azioni** ••• a destra del piano e selezionare **Modifica pianificazioni**.
   a. Nella pagina Modifica pianificazioni, immettere la frequenza in minuti in cui si desidera che venga eseguito il controllo di conformità del failover.
   b. Selezionare **Esegui test failover in base a una pianificazione**.
   c. Nell'opzione Ripeti, selezionare la pianificazione giornaliera, settimanale o mensile.
   d. Selezionare **Salva**.

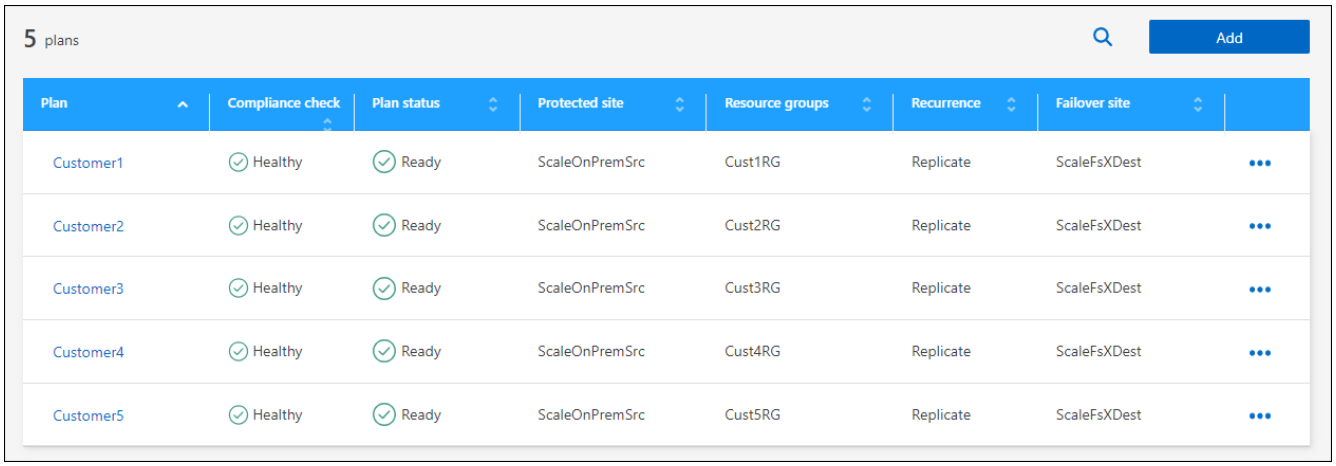
Riconciliare gli snapshot su richiesta

È possibile riconciliare le istantanee non sincronizzate tra l'origine e la destinazione. Questo può verificarsi se le snapshot vengono eliminate su una destinazione al di fuori del disaster recovery di BlueXP . Il servizio elimina automaticamente lo snapshot sulla sorgente ogni 24 ore. Tuttavia, è possibile eseguire questa operazione su richiesta. Questa funzione consente di garantire la coerenza delle istantanee in tutti i siti.

Ruolo BlueXP obbligatorio 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.

Fasi

1. Dal menu superiore, selezionare **piani di replica**.



2. Dall'elenco dei piani di replica, selezionare l'opzione **azioni** ••• a destra del piano e selezionare **Riconcilia istantanee**.
3. Esaminare le informazioni di riconciliazione.
4. Selezionare **Riconcilia**.

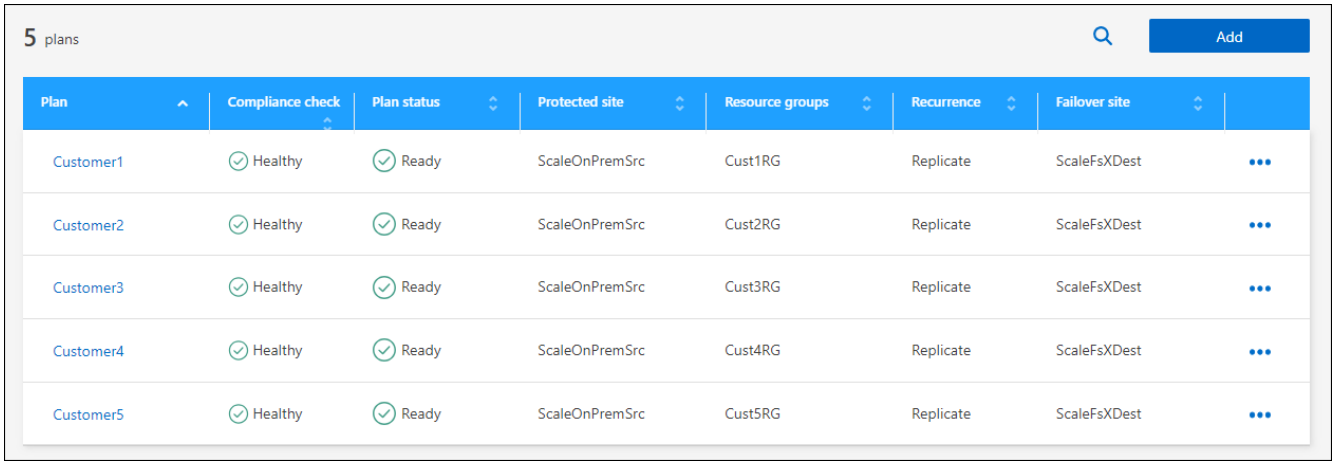
Eliminare un piano di replica

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

Ruolo BlueXP obbligatorio 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.

Fasi

1. Dal menu superiore, selezionare **piani di replica**.



2. Selezionare l'opzione **azioni** ••• a destra del piano e selezionare **Elimina**.
3. Selezionare se si desidera eliminare gli snapshot primari, secondari o solo i metadati creati dal piano.
4. Digitare "delete" per confermare l'eliminazione.
5. Selezionare **Delete** (Elimina).

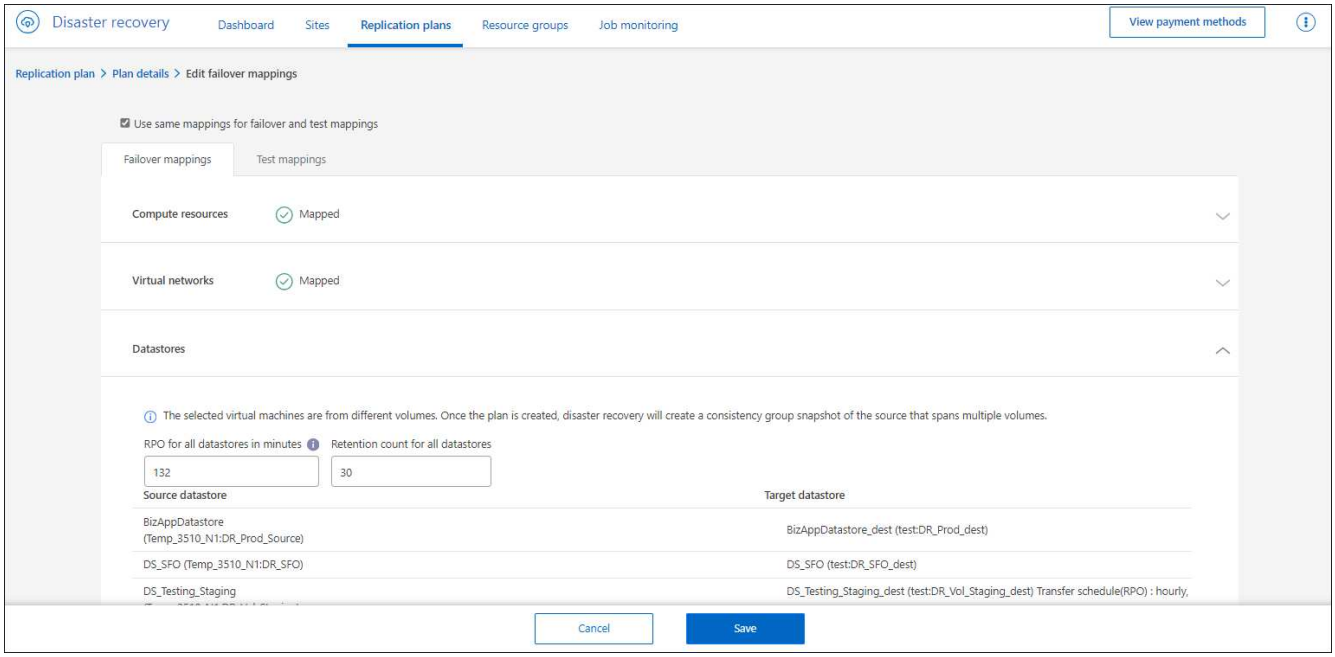
Modificare il numero di conservazione per le pianificazioni di failover

È possibile modificare il numero di datastore conservati.

Ruolo BlueXP obbligatorio 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.

Fasi

1. Dal menu superiore, selezionare **piani di replica**.
2. Selezionare il piano di replica, fare clic sulla scheda **mappatura di failover** e fare clic sull'icona **Modifica** matita.
3. Fare clic sulla freccia **Datastores** per espanderla.



4. Modificare il valore del conteggio di conservazione nel piano di replica.
5. Con il piano di replica selezionato, selezionare il menu azioni, selezionare *Pulisci snapshot precedenti" per rimuovere le istantanee precedenti sulla destinazione in modo che corrispondano al nuovo conteggio di conservazione.

Visualizzare informazioni sui datastore

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

Ruolo BlueXP obbligatorio 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 Ruolo di visualizzatore del ripristino di emergenza.

Fasi

1. Dal menu superiore, selezionare **Dashboard**.
2. Selezionare il vCenter nella riga del sito.
3. Selezionare **Datastores**.

4. Visualizzare le informazioni dei datastore.

Visualizzare le informazioni sulle macchine virtuali

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

Ruolo BlueXP obbligatorio 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 Ruolo di visualizzatore del ripristino di emergenza.

Fasi

1. Dal menu superiore, selezionare **Dashboard**.
2. Selezionare il vCenter nella riga del sito.
3. Selezionare **macchine virtuali**.
4. Visualizzare le informazioni sulle macchine virtuali.

Monitorare i processi di disaster recovery di BlueXP

È possibile monitorare tutti i processi di disaster recovery di BlueXP e verificarne l'avanzamento.

Visualizzare i lavori

Ruolo BlueXP obbligatorio Amministratore dell'organizzazione, Amministratore di cartelle o progetti, Amministratore del ripristino di emergenza, Amministratore dell'applicazione di ripristino di emergenza o Ruolo di visualizzatore del ripristino di emergenza.

"Scopri di più sui ruoli utente e sulle autorizzazioni nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore, selezionare **monitoraggio processi**.
3. Esaminare tutti i lavori relativi alle operazioni e controllare la data e lo stato.
4. Per visualizzare i dettagli di un determinato processo, selezionare la riga corrispondente.
5. Per aggiornare le informazioni, selezionare **Aggiorna**.

Annullare un lavoro

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

Ruolo BlueXP obbligatorio 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 nel BlueXP disaster recovery". "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Fasi

1. Dal nav sinistro di BlueXP, seleziona **protezione** > **Disaster Recovery**.
2. Dal menu superiore, selezionare **monitoraggio processi**.
3. Nella pagina monitoraggio lavoro, annotare l'ID del lavoro che si desidera annullare.

   Il lavoro deve essere in stato "in corso" o "in coda".

4. Nella colonna azioni, selezionare **Annulla lavoro**.

Crea report di ripristino di emergenza BlueXP

Esaminare i report di disaster recovery di BlueXP può aiutarti ad analizzare la tua preparazione al disaster recovery. I report preprogettati includono un riepilogo dei failover dei test, dei dettagli del piano di replica e dei dettagli dei processi 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 collegamento Download è valido per sei ore.

Fasi

1. Dal navigatore BlueXP sinistro, selezionare **protezione** > **Disaster Recovery** > **piani di replica**.
2. Nella parte superiore della pagina, selezionare **Crea rapporto**.
3. Selezionare il tipo di formato del file e il periodo di tempo negli ultimi 7 giorni.
4. Selezionare **Crea**.

   La visualizzazione del rapporto potrebbe richiedere alcuni minuti.

5. Per scaricare un report, selezionare **Scarica report** e selezionarlo nella cartella Download dell'amministratore.

Riferimento

Privilegi vCenter necessari per il disaster recovery di BlueXP

L'account vCenter deve disporre di un set minimo di privilegi vCenter per consentire al disaster recovery di BlueXP di eseguire i propri servizi, come registrazione e deregistrazione dei datastore, avvio e arresto delle macchine virtuali e riconfigurazione delle macchine virtuali (VM). Nella tabella seguente sono elencati tutti i privilegi necessari per il disaster recovery di BlueXP per interfacciarsi con un cluster vCenter.

Tipo	Nome privilegio	Descrizione
Datastore	Archivio dati. Configurare l'archivio dati	Utilizzare per configurare un datastore.
	Archivio dati. Rimuovere l'archivio dati	Utilizzare per rimuovere un datastore.
Macchina virtuale	Macchina virtuale.Configurazione.Modifica impostazioni	Consente di modificare le impostazioni generali della macchina virtuale.
	Macchina virtuale.Configurazione.Modifica delle impostazioni della periferica	Utilizzare per modificare le proprietà di una periferica esistente.
	Virtual machine.Configuration.Reload from path	Consente di modificare una patch di configurazione della macchina virtuale mantenendo l'identità della macchina virtuale. Soluzioni come VMware vCenter Site Recovery Manager utilizzano questa operazione per mantenere l'identificazione delle VM durante il failover e il failback.
	Macchina virtuale.Configurazione.Rinomina	Consente di rinominare una macchina virtuale o di modificare i nodi associati di una macchina virtuale.
	Virtual machine.Configuration.Reset informazioni guest	Consente di modificare le informazioni del sistema operativo guest per una VM.
	Macchina virtuale.Configurazione.Cambia memoria	Utilizzare per modificare la quantità di memoria allocata alla macchina virtuale.

Tipo	Nome privilegio	Descrizione
	Virtual machine.Configuration.Change CPU count (macchina virtuale.Configurazione.Modifica conteggio CPU)	Utilizzare per modificare il numero di CPU virtuali.
Guest macchina virtuale	Macchina virtuale. Operazioni per i clienti. Modifiche al funzionamento degli ospiti	Abilita le operazioni guest delle VM che implicano modifiche a un sistema operativo guest in una VM, come il trasferimento di un file alla VM.
Interazione macchina virtuale	Macchina virtuale.interazione.spegnimento	Utilizzare per spegnere una macchina virtuale accesa. Questa operazione disattiva il sistema operativo guest.
	Macchina virtuale.interazione.accensione	Utilizzare per accendere una macchina virtuale spenta e riprendere una macchina virtuale sospesa.
	Installazione di Virtual Machine.Interaction.VMware Tools	Utilizzare per montare e smontare il programma di installazione del CD di VMware Tools come CD-ROM per il sistema operativo guest.
Inventario macchine virtuali	Virtual machine.Inventory.Create new	Consente di creare una macchina virtuale e allocare le risorse per la sua esecuzione.
	Virtual machine.Inventory.Register	Consente di aggiungere una macchina virtuale esistente a un inventario vCenter Server o host.
	Macchina virtuale.inventario.Annulla registrazione	Consente di annullare la registrazione di una macchina virtuale da un inventario vCenter Server o host.
Stato macchina virtuale	Macchina virtuale. Gestione delle Snapshot. Crea snapshot	Consente di creare un'istantanea dallo stato corrente della VM.
	Macchina virtuale. Gestione delle Snapshot. Rimuovere l'istantanea	Consente di rimuovere un'istantanea dalla cronologia.
	Macchina virtuale. Gestione delle Snapshot. Ripristina istantanea	Utilizzare per impostare la macchina virtuale sullo stato in cui si trovava in un dato snapshot.

Accesso basato sui ruoli BlueXP disaster recovery alle funzionalità

Il BlueXP disaster recovery utilizza ruoli per gestire l'accesso di ciascun utente a specifiche funzionalità e azioni.

Il servizio utilizza i seguenti ruoli specifici per il BlueXP disaster recovery.

- **Amministratore del ripristino di emergenza**: esegue qualsiasi azione nel BlueXP disaster recovery.
- **Amministratore del failover del disaster recovery**: esegue azioni di failover e migrazione nel BlueXP 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 nel BlueXP disaster recovery, ma non può eseguire alcuna azione.

Questi ruoli sono specifici del BlueXP disaster recovery e non sono gli stessi dei ruoli della piattaforma utilizzati in BlueXP. Per informazioni dettagliate su tutti i ruoli della piattaforma BlueXP , vedere "La documentazione di installazione e amministrazione di BlueXP".

Nella tabella seguente sono indicate le azioni che ogni ruolo di BlueXP disaster recovery può eseguire.

Funzione e azione	Amministratore del ripristino di emergenza	Amministratore del failover del ripristino di emergenza	Amministratore dell'applicazione di ripristino di emergenza	Visualizzatore di ripristino di emergenza
Visualizza dashboard e tutte le schede	Sì	Sì	Sì	Sì
Inizia la prova gratuita	Sì	No	No	No
Avvia il rilevamento dei carichi di lavoro	Sì	No	No	No
Visualizza le informazioni sulla licenza	Sì	Sì	Sì	Sì
Attiva la licenza	Sì	No	Sì	No
Nella scheda Siti:				
Visualizza i siti	Sì	Sì	Sì	Sì
Aggiungere, modificare o eliminare siti	Sì	No	No	No
Nella scheda Piani di replicazione:				
Visualizza i piani di replicazione	Sì	Sì	Sì	Sì

Funzione e azione	Amministratore del ripristino di emergenza	Amministratore del failover del ripristino di emergenza	Amministratore dell'applicazione di ripristino di emergenza	Visualizzatore di ripristino di emergenza
Visualizza i dettagli del piano di replicazione	Sì	Sì	Sì	Sì
Creare o modificare piani di replicazione	Sì	Sì	Sì	No
Creare report	Sì	No	No	No
Visualizza istantanee	Sì	Sì	Sì	Sì
Eseguire test di failover	Sì	Sì	Sì	No
Eseguire failover	Sì	Sì	No	No
Eseguire failback	Sì	Sì	No	No
Eseguire migrazioni	Sì	Sì	No	No
Nella scheda Gruppi di risorse:				
Visualizza i gruppi di risorse	Sì	Sì	Sì	Sì
Crea, modifica o elimina gruppi di risorse	Sì	No	Sì	No
Nella scheda Monitoraggio lavori:				
Visualizzare i lavori	Sì	No	Sì	Sì
Annulla lavori	Sì	Sì	Sì	No

Utilizza il disaster recovery di BlueXP con Amazon EVS

Introduzione del disaster recovery di BlueXP tramite Amazon Elastic VMware Service e Amazon FSx per NetApp ONTAP

I clienti dipendono sempre di più dalle infrastrutture virtualizzate per i carichi di lavoro di elaborazione di produzione, come quelli basati 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 principale fornitore di storage per infrastrutture virtualizzate, ha un interesse personale nel garantire che le VM dei propri clienti siano protette allo stesso modo in cui proteggiamo i dati ospitati su storage

ONTAP di qualsiasi tipo. Per raggiungere questo obiettivo, NetApp ha creato il servizio di disaster recovery BlueXP.

> QUESTA DOCUMENTAZIONE RIGUARDANTE AMAZON EVS VIENE FORNITA COME ANTEPRIMA TECNOLOGICA. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale.

Una delle principali sfide di qualsiasi soluzione di disaster recovery è la gestione dei costi incrementali di acquisto, configurazione e manutenzione di risorse di elaborazione, rete e storage aggiuntive, necessarie solo per fornire un'infrastruttura di replica e ripristino per il disaster recovery. Un'opzione diffusa per la protezione delle risorse virtuali critiche on-premise è l'utilizzo di risorse virtuali ospitate nel cloud come infrastruttura di replica e ripristino per il disaster recovery. Amazon è un esempio di soluzione di questo tipo, in grado di fornire risorse convenienti e compatibili con le infrastrutture di VM ospitate su 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 software e agli strumenti VMware che già conosci, consentendo di integrare Amazon EVS vCenter come estensione della tua infrastruttura virtualizzata on-premise.

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 utilizzo di storage. In questi casi, l'integrazione di Amazon EVS con lo storage Amazon FSx for NetApp ONTAP (Amazon FSxN) può offrire una soluzione di storage più flessibile. Inoltre, quando si utilizzano soluzioni di storage NetApp ONTAP on-premise per ospitare l'infrastruttura VMware, l'utilizzo di Amazon EVS con FSx for ONTAP garantisce le migliori funzionalità di interoperabilità e protezione dei dati tra le infrastrutture on-premise e quelle ospitate nel cloud.

Per informazioni su Amazon FSX per NetApp ONTAP, vedere "Introduzione a Amazon FSX per NetApp ONTAP".

Panoramica della soluzione di disaster recovery di BlueXP tramite Amazon EVS e Amazon FSs per NetApp ONTAP

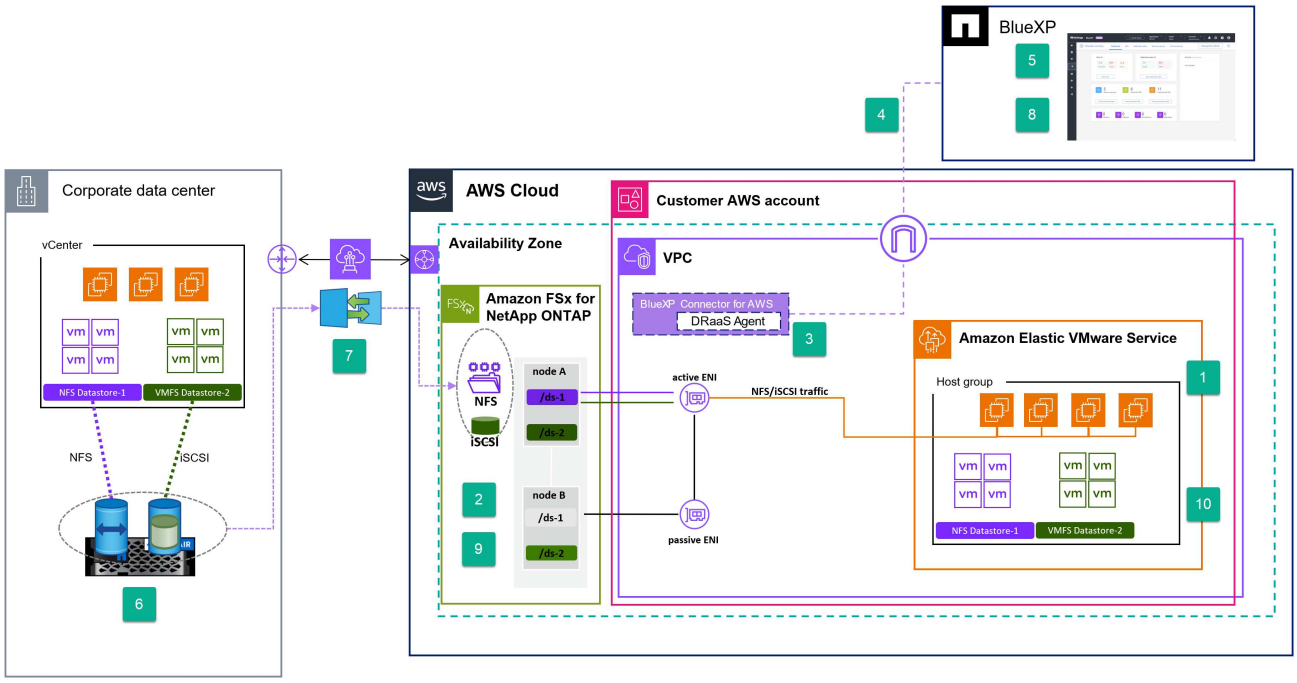
Il disaster recovery di BlueXP è un servizio a valore aggiunto ospitato nell'ambiente software-as-a-service di BlueXP, che si basa sull'architettura principale di BlueXP. Diversi componenti principali costituiscono il servizio di disaster recovery per la protezione VMware all'interno di BlueXP.

Per una panoramica completa della soluzione di disaster recovery BlueXP, vedere "Scopri le funzionalità di disaster recovery di BlueXP 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 per i datastore ospitati nello storage NetApp ONTAP.

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

Panoramica del disaster recovery di BlueXP tramite 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 for ONTAP viene distribuito nella stessa zona di disponibilità (AZ) 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 gateway AmazonTransit.
3. NetApp BlueXP Connector è installato nella tua VPC. BlueXP Connector ospita diversi servizi di gestione dei dati (chiamati agenti), incluso l'agente di disaster recovery BlueXP che gestisce il disaster recovery dell'infrastruttura VMware sia sui data center fisici locali che sulle risorse ospitate su Amazon AWS.
4. L'agente di disaster recovery di BlueXP comunica in modo sicuro con il servizio BlueXP ospitato nel cloud per ricevere attività e distribuirle alle istanze di storage vCenter e ONTAP appropriate, locali e ospitate su AWS.
5. È possibile creare un piano di replicazione utilizzando la console dell'interfaccia utente ospitata sul cloud di BlueXP, 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 replica determina quali datastore vCenter ospitano le VM protette e i volumi ONTAP che ospitano tali datastore. Se i volumi non sono ancora presenti sul cluster FSx for ONTAP, il disaster recovery di BlueXP li crea automaticamente.
7. Viene creata una relazione SnapMirror per ciascun volume ONTAP di origine identificato per ciascun volume ONTAP di destinazione ospitato su FSx for ONTAP e viene creato un programma di replicazione basato 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 console BlueXP e seleziona un backup da utilizzare come punto di ripristino.
9. L'agente di disaster recovery BlueXP attiva i volumi di protezione dei dati ospitati su 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 il connettore BlueXP per il ripristino di emergenza di BlueXP

Un connettore BlueXP è un software NetApp in esecuzione nel cloud o nella rete locale. Esegue le azioni necessarie a BlueXP per gestire l'infrastruttura dati. Il connettore interroga costantemente il software di disaster recovery BlueXP come livello di servizio per qualsiasi azione necessaria.

Per il servizio di disaster recovery di BlueXP, 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-premise. Sebbene il connettore possa essere installato in qualsiasi posizione di rete, per il disaster recovery di BlueXP consigliamo di installarlo nel sito di disaster recovery. Ciò garantisce che, in caso di guasto del sito primario, l'interfaccia utente della console cloud di BlueXP continui a comunicare con il connettore e possa orchestrare il processo di ripristino all'interno di tale sito di disaster recovery.

Per utilizzare il servizio, installare il Connettore in modalità standard. Per ulteriori informazioni sui tipi di installazione del Connettore, visitare "Scopri le modalità di distribuzione di BlueXP | Documentazione NetApp" .

Sebbene il Connettore sia fondamentale per l'utilizzo del servizio, la procedura di installazione dipende dalle esigenze e dalla configurazione di rete. Fornire istruzioni specifiche per l'installazione va oltre lo scopo di queste informazioni.

Il metodo più semplice per installare un connettore con Amazon AWS è utilizzare AWS Marketplace. Per dettagli sull'installazione del connettore tramite AWS Marketplace, consultare "Creare un connettore da AWS Marketplace | Documentazione NetApp" .

Configurare il disaster recovery di BlueXP per Amazon EVS

Panoramica sulla configurazione del disaster recovery di BlueXP per Amazon EVS

Dopo aver installato BlueXP Connector, è necessario integrare tutte le risorse di storage ONTAP e VMware vCenter che parteciperanno al processo di disaster recovery con BlueXP Disaster Recovery.

- "Prerequisiti per il disaster recovery di Amazon EVS con BlueXP"
- "Aggiungere array di archiviazione ONTAP al ripristino di emergenza di BlueXP"
- "Abilita il disaster recovery di BlueXP per Amazon EVS"
- "Aggiungere siti vCenter al ripristino di emergenza di BlueXP"
- "Aggiungere cluster vCenter al disaster recovery di BlueXP"

Prerequisiti per il disaster recovery di Amazon EVS con BlueXP

Prima di procedere alla configurazione del disaster recovery di Amazon EVS con BlueXP, è necessario assicurarsi che siano soddisfatti diversi prerequisiti.

Nello specifico, procedi come segue:

- Creare un account utente vCenter con i privilegi VMware specifici richiesti per il disaster recovery di BlueXP per eseguire le operazioni necessarie.

Si sconsiglia di utilizzare l'account amministratore predefinito "administrator@vsphere.com". invece consigliabile creare un account utente specifico per il disaster recovery di BlueXP su tutti i cluster vCenter che parteciperanno al processo di disaster recovery. Per un elenco dei privilegi specifici richiesti, consultare "Privilegi vCenter necessari per il disaster recovery di BlueXP" .

- Assicurarsi che tutti gli archivi dati vCenter che ospiteranno le VM protette dal disaster recovery di BlueXP siano posizionati su risorse di storage NetApp ONTAP.

  Il servizio supporta NFS e VMFS su iSCSI (e non FC) quando si utilizza Amazon FSx su NetApp ONTAP. Sebbene il servizio supporti FC, Amazon FSx per NetApp ONTAP non lo supporta.

- Assicurati che Amazon EVS vCenter sia connesso a un cluster di storage Amazon FSx for NetApp ONTAP.
- Assicurarsi che gli strumenti VMware 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. Ti consigliamo di utilizzare AWS Direct Connect, AWS Private Link o una VPN AWS Site-to-Site.

Aggiungi array locali all'ambiente di lavoro BlueXP per Amazon EVS con ripristino di emergenza BlueXP

Prima di utilizzare il disaster recovery di BlueXP, è necessario aggiungere istanze di archiviazione locali e ospitate nel cloud all'ambiente di lavoro BlueXP.

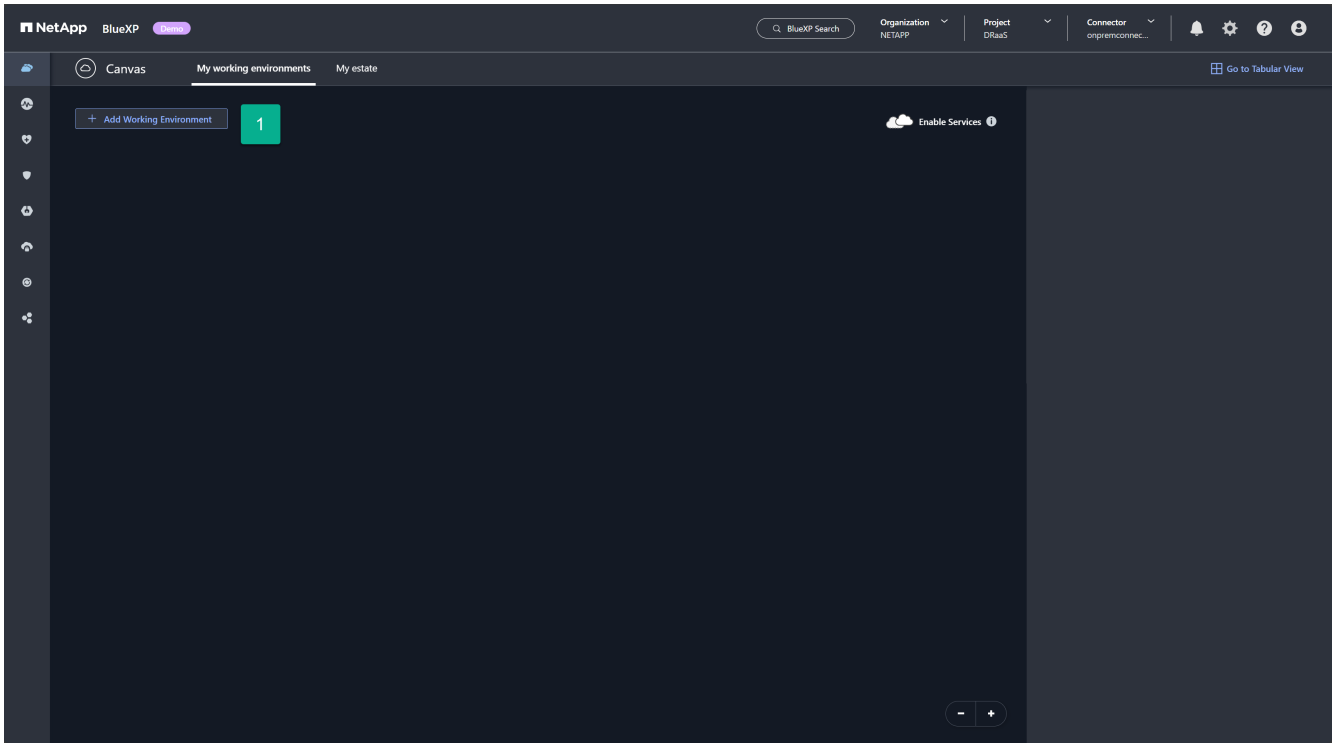
Devi fare quanto segue:

- Aggiungi array on-premise al tuo ambiente di lavoro BlueXP.
- Aggiungi istanze di Amazon FSx for NetApp ONTAP (FSx for ONTAP) al tuo ambiente di lavoro BlueXP.

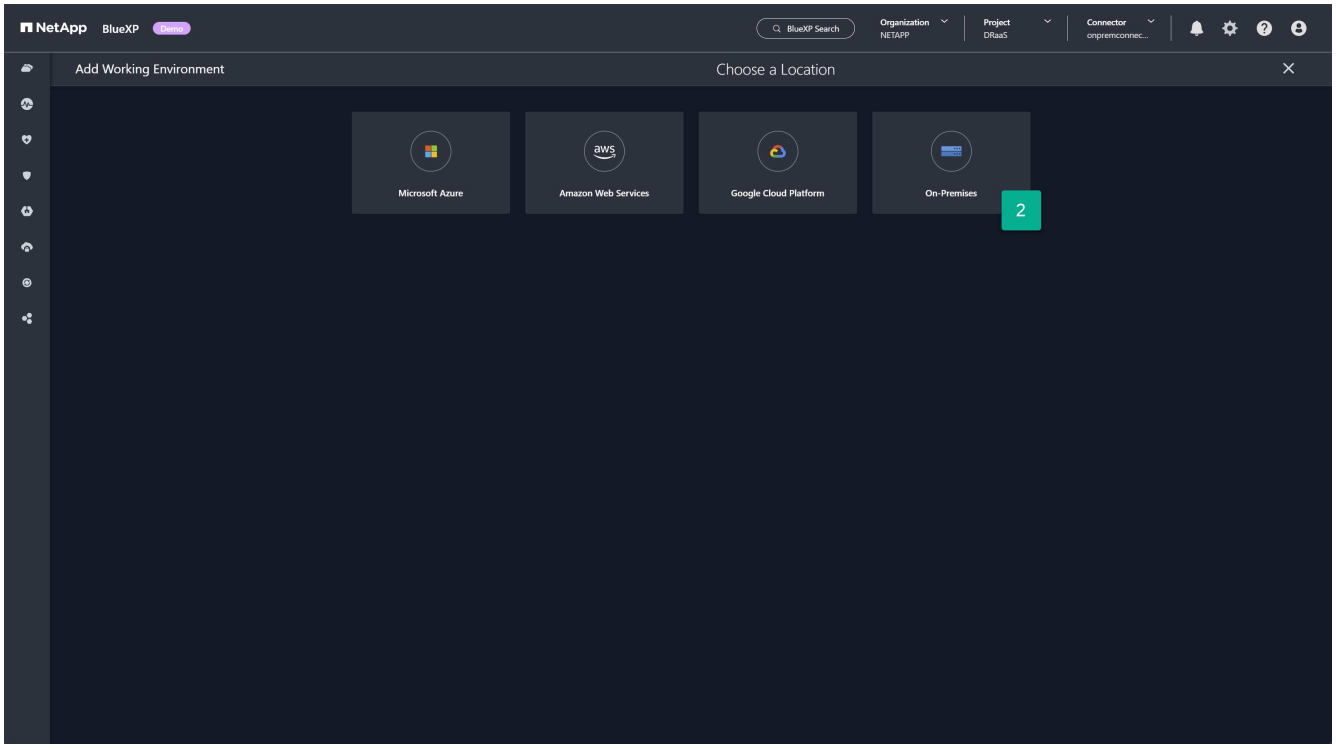
Aggiungere array di archiviazione locali all'ambiente di lavoro BlueXP

Aggiungi risorse di archiviazione ONTAP on-premise al tuo ambiente di lavoro BlueXP.

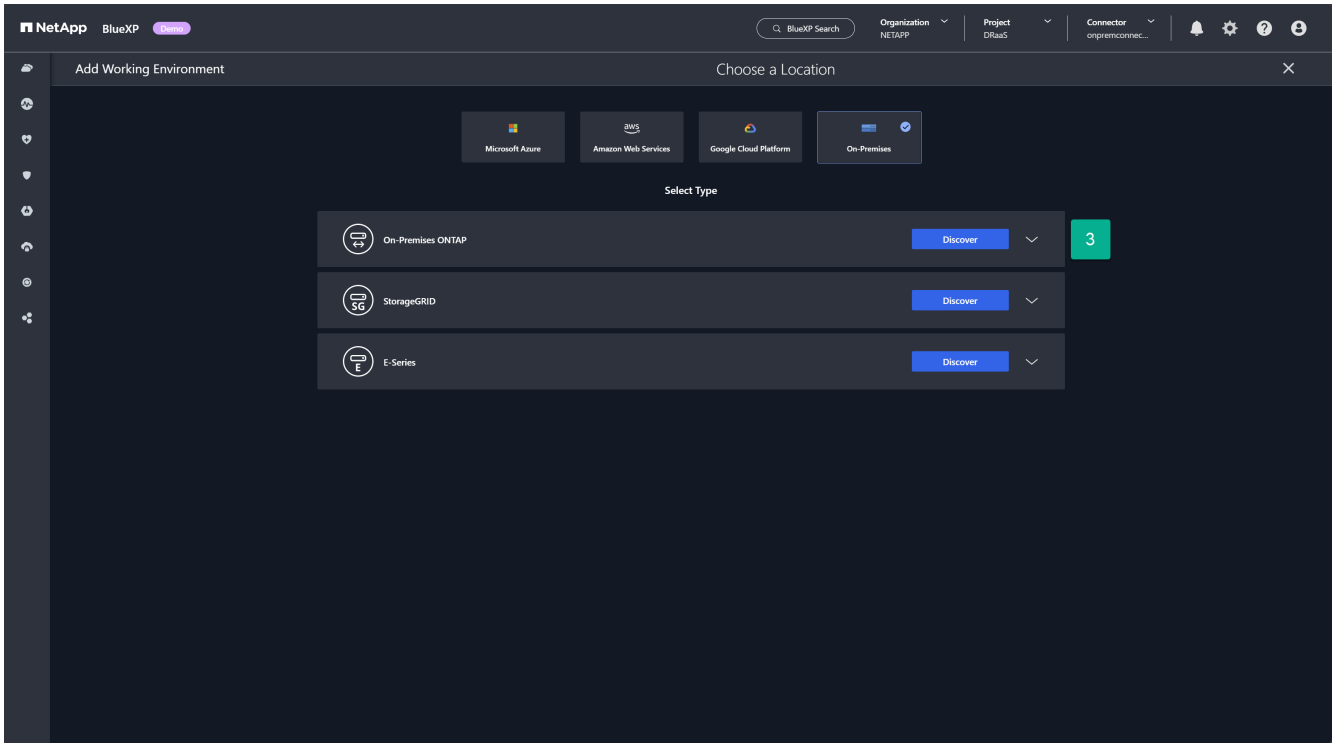
1. Da BlueXP Canvas, seleziona **Aggiungi ambiente di lavoro**.



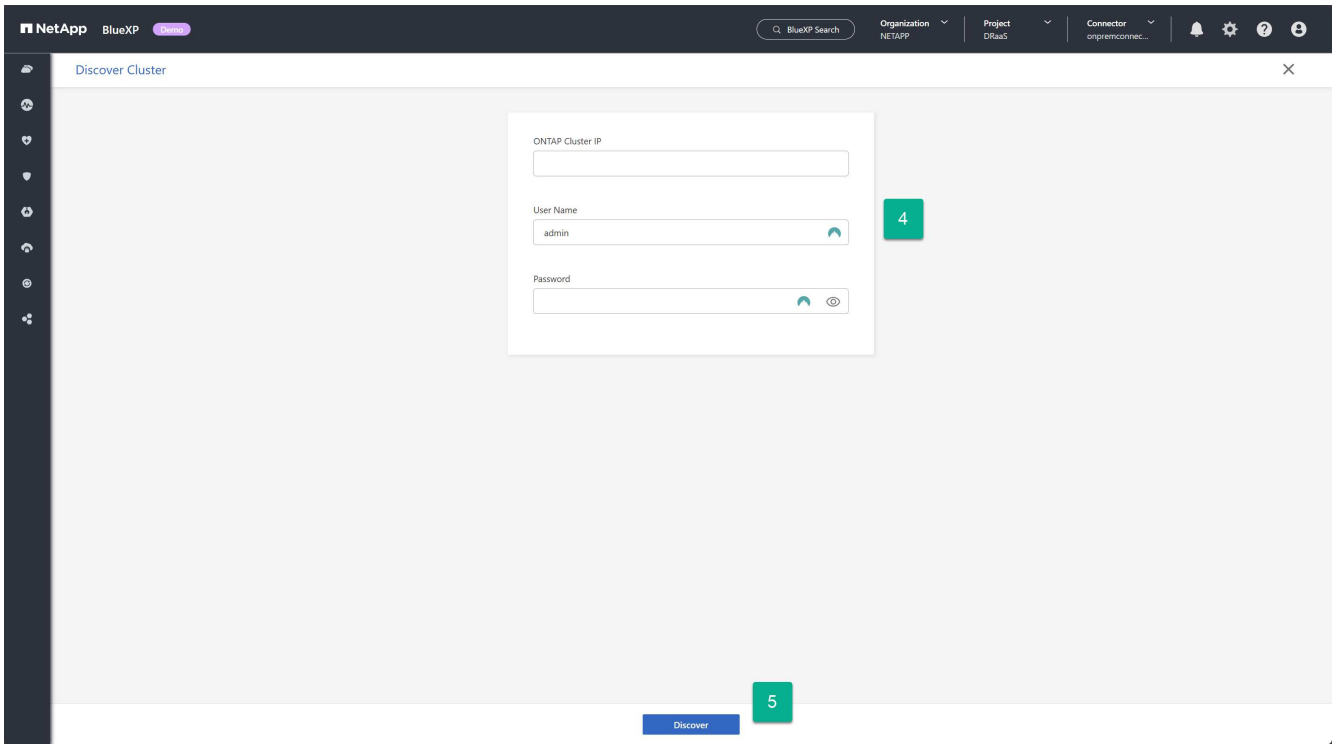
2. Nella pagina Aggiungi ambiente di lavoro, seleziona la scheda **In sede**.



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



4. Nella pagina Scopri cluster, immetti 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.

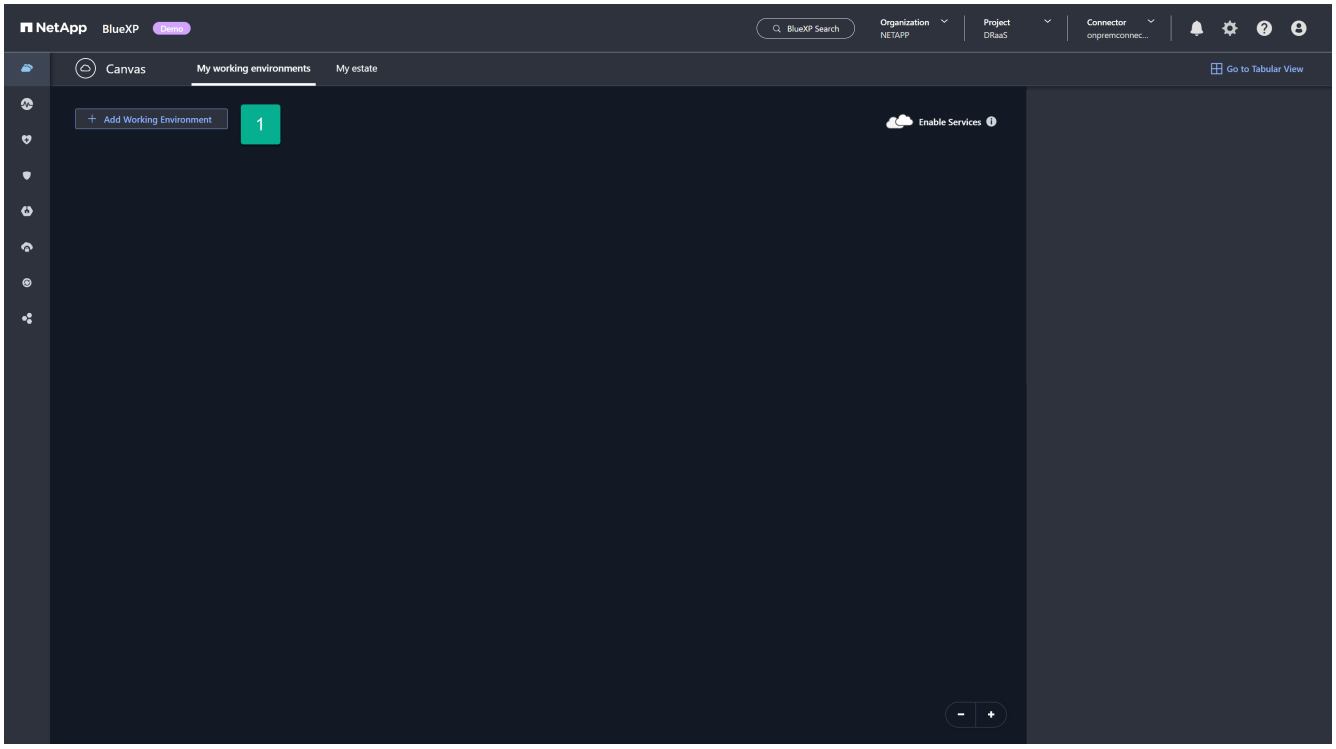


6. Ripetere i passaggi da 1 a 5 per ogni array ONTAP che ospiterà i datastore vCenter.

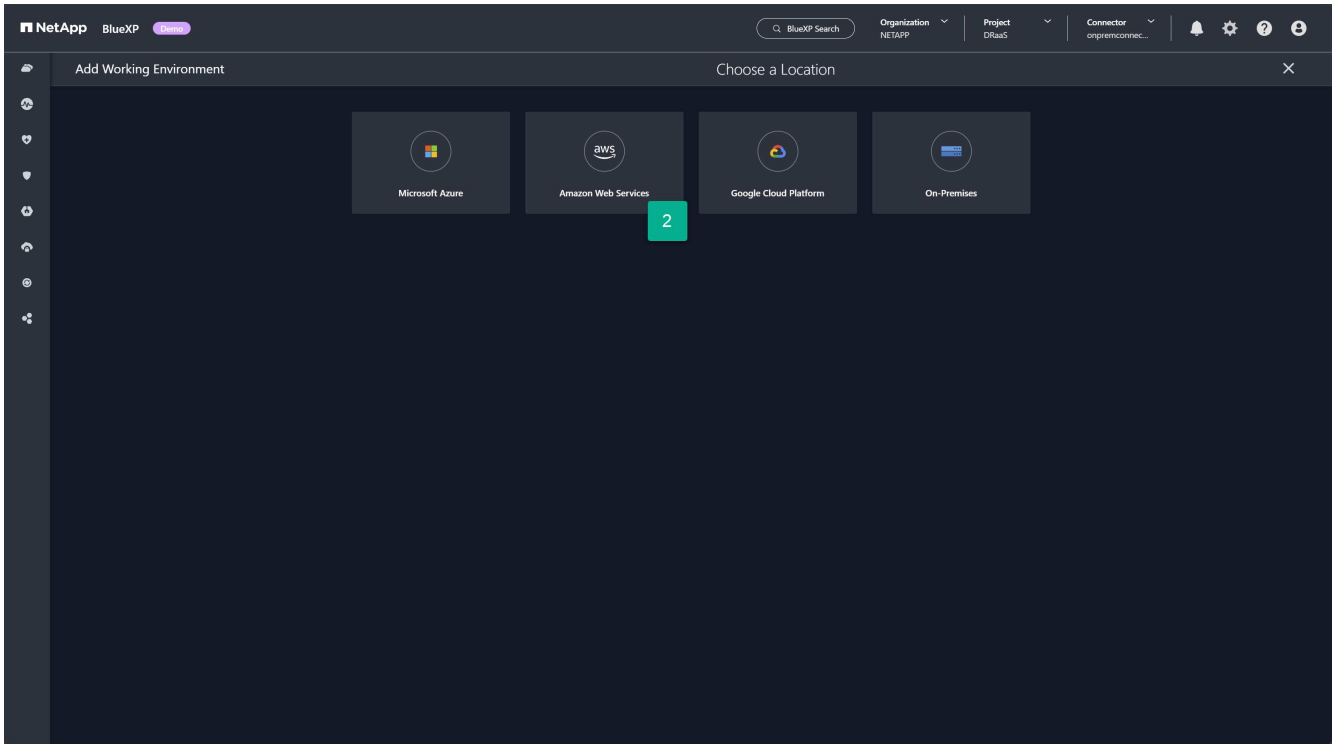
Aggiungere istanze di storage Amazon FSx per NetApp ONTAP all'ambiente di lavoro BlueXP

Successivamente, aggiungi risorse di storage Amazon FSx for NetApp ONTAP al tuo ambiente di lavoro BlueXP.

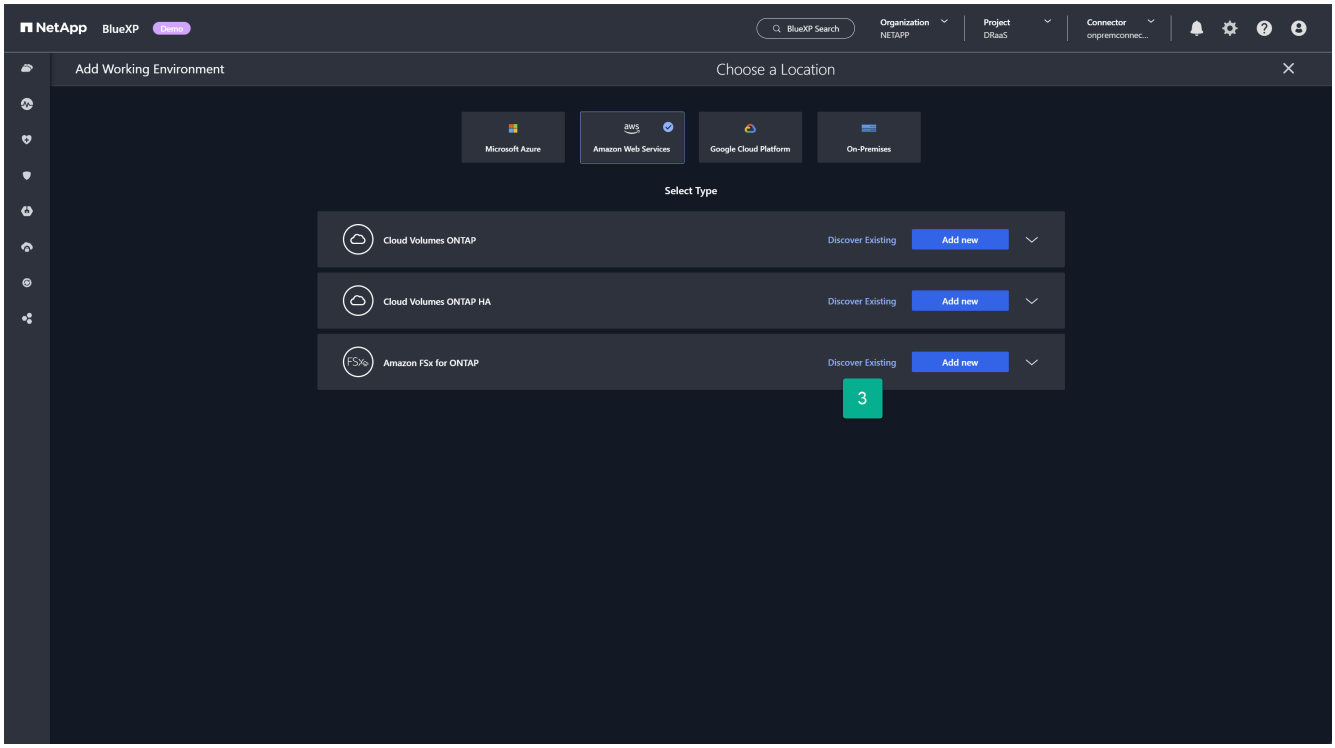
1. Da BlueXP Canvas, seleziona **Aggiungi ambiente di lavoro**.



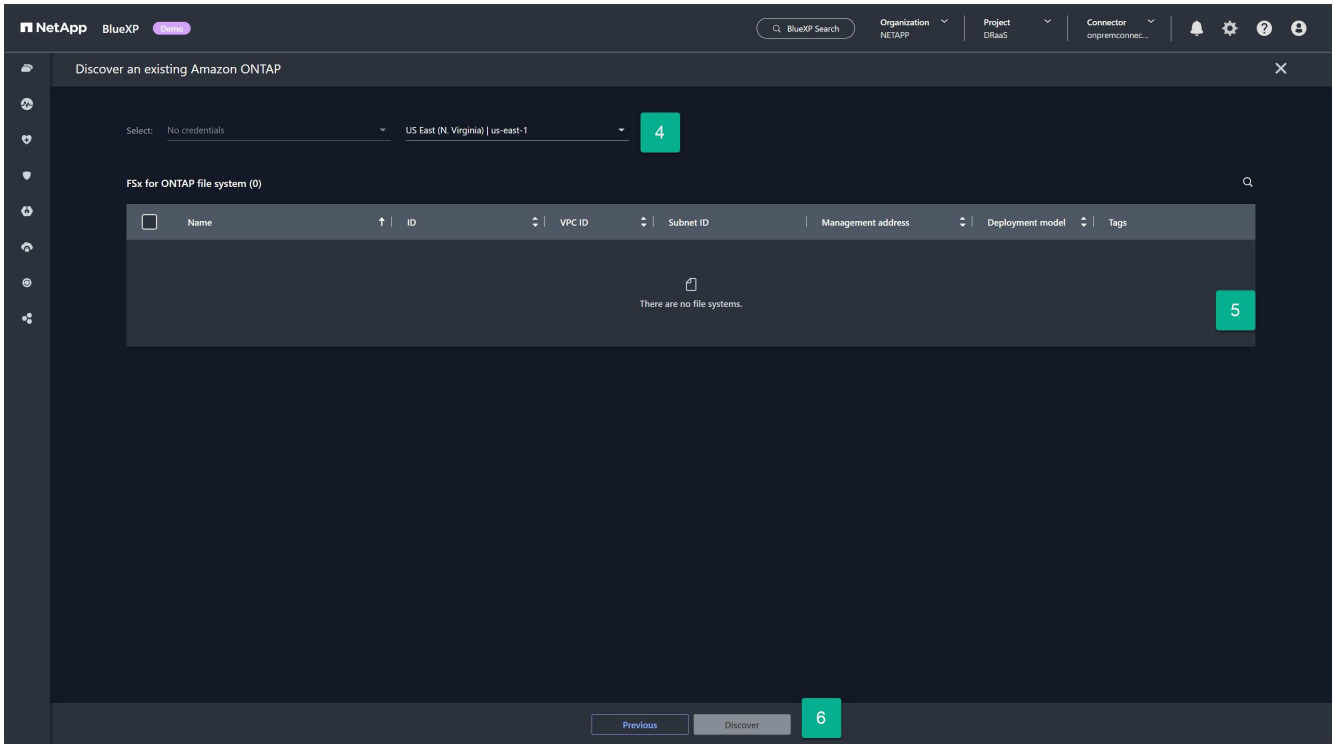
2. Dalla pagina Aggiungi ambiente di lavoro, seleziona la scheda **Amazon Web Services**.



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 di disaster recovery BlueXP al tuo account BlueXP per Amazon EVS

Il disaster recovery di BlueXP è un prodotto con licenza che deve essere acquistato prima di poter essere utilizzato. Esistono diversi tipi di licenza e diverse modalità di acquisto. Una licenza dà diritto a proteggere una quantità specifica di dati per un periodo di tempo specifico.

Per ulteriori informazioni sulle licenze di ripristino di emergenza di BlueXP, vedere "Imposta le licenze per il disaster recovery di BlueXP" .

Tipi di licenza

Esistono due tipi principali di licenza:

- NetApp offre un "licenza di prova di 30 giorni" che puoi utilizzare per valutare il disaster recovery di BlueXP utilizzando le tue risorse ONTAP e VMware. Questa licenza offre 30 giorni di utilizzo per una quantità illimitata di capacità protetta.
- Acquista una licenza di produzione se desideri la 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 ti consigliamo di acquistare la licenza **NetApp Intelligent Services** per il disaster recovery di BlueXP tramite Amazon AWS Marketplace. Per ulteriori informazioni sull'acquisto di una licenza tramite Amazon Marketplace, consulta "Iscriviti tramite AWS Marketplace" .

Dimensiona le tue esigenze di capacità di disaster recovery

Prima di acquistare la licenza, è necessario comprendere quanta capacità di storage ONTAP si desidera proteggere. Uno dei vantaggi dell'utilizzo dello storage NetApp ONTAP è l'elevata efficienza con cui NetApp archivia i dati. Tutti i dati archiviati in un volume ONTAP, come un datastore VMware che ospita VM, vengono archiviati in modo altamente efficiente. ONTAP utilizza di default tre tipi di efficienza di storage durante la scrittura dei dati su storage fisico: compattazione, deduplicazione e compressione. Il risultato finale è un'efficienza di storage 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.

Questo può essere vantaggioso perché il disaster recovery di BlueXP calcola la capacità ai fini della licenza dopo l'applicazione di tutte le efficienze di storage di ONTAP. Ad esempio, supponiamo di aver effettuato il provisioning di un datastore NFS da 100 terabyte (TiB) in 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 storage applicate automaticamente comportino un consumo di soli 33 TiB per tali VM (efficienza di storage 3:1). Il disaster recovery di BlueXP deve essere concesso in licenza solo per 33 TiB, non per 100 TiB. Questo può rappresentare un vantaggio significativo per il costo totale di proprietà della soluzione di disaster recovery rispetto ad altre soluzioni di disaster recovery.

Fasi

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 >.`

   Ad 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. Prendi nota del valore **Spazio Fisico Totale Utilizzato** per ciascun volume. Questo rappresenta la quantità di dati che BlueXP Disaster Recovery deve proteggere ed è il valore che utilizzerai per determinare la capacità necessaria per la licenza.

Aggiungere siti nel disaster recovery di BlueXP per Amazon EVS

Prima di proteggere l'infrastruttura VM, è necessario identificare quali cluster VMware vCenter ospitano le VM da proteggere e dove si trovano tali vCenter. Il primo passo consiste nel 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:

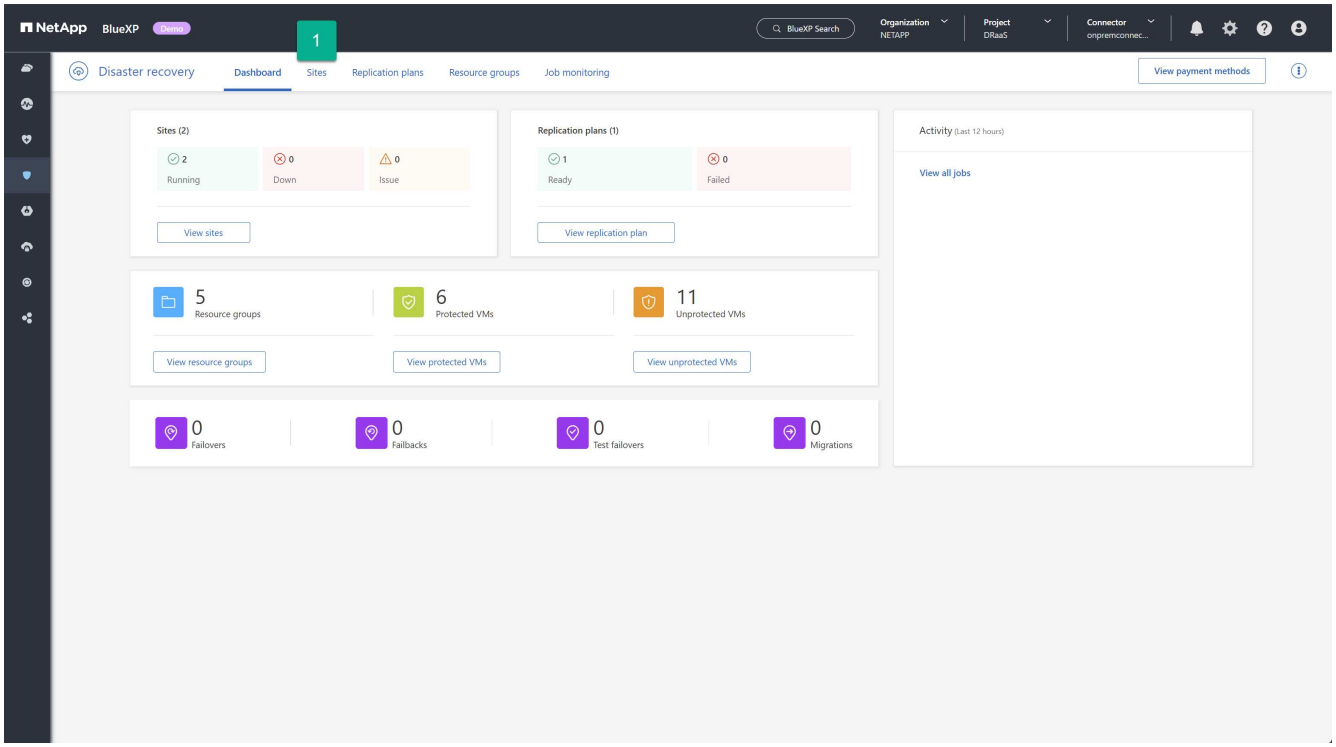
- Un sito che rappresenta ogni data center di produzione in cui risiedono i cluster vCenter di produzione
- Un sito per il tuo data center cloud Amazon EVS/Amazon FSx per NetApp ONTAP

Crea siti on-premise

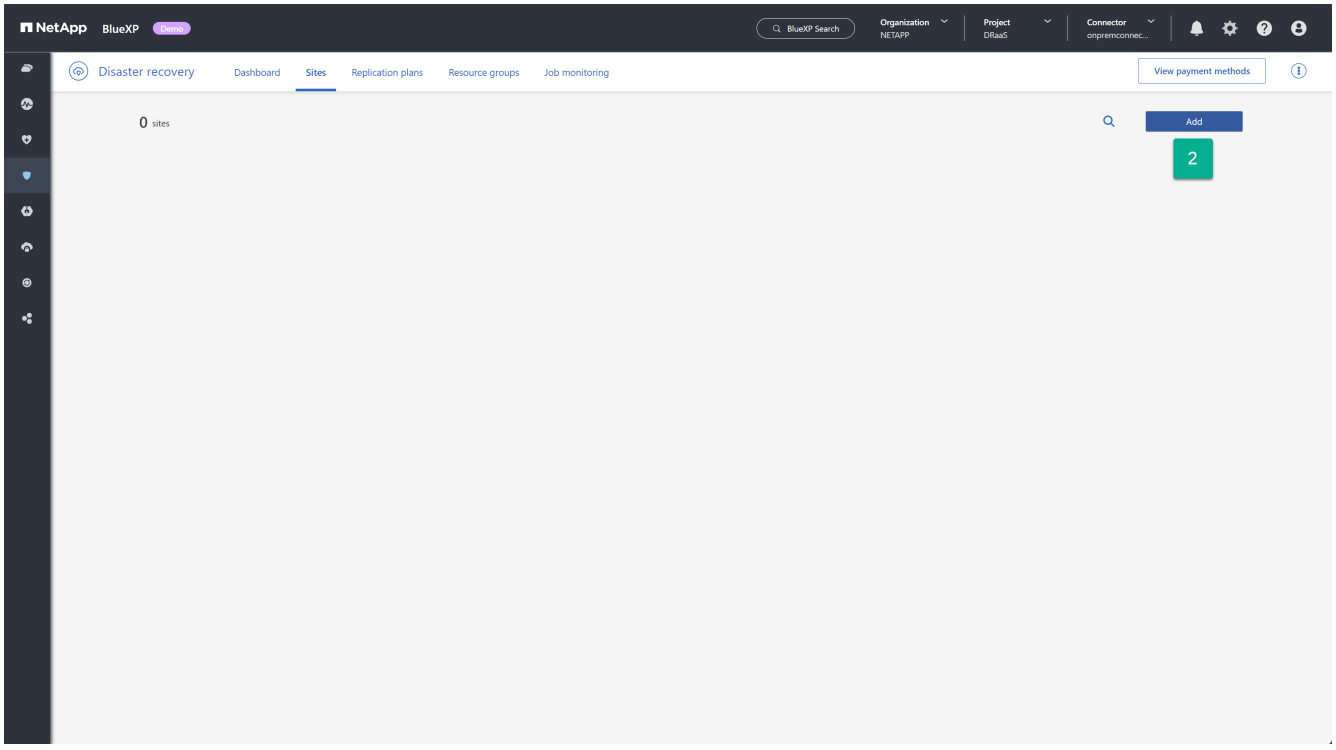
Creare un sito di produzione vCenter.

Fasi

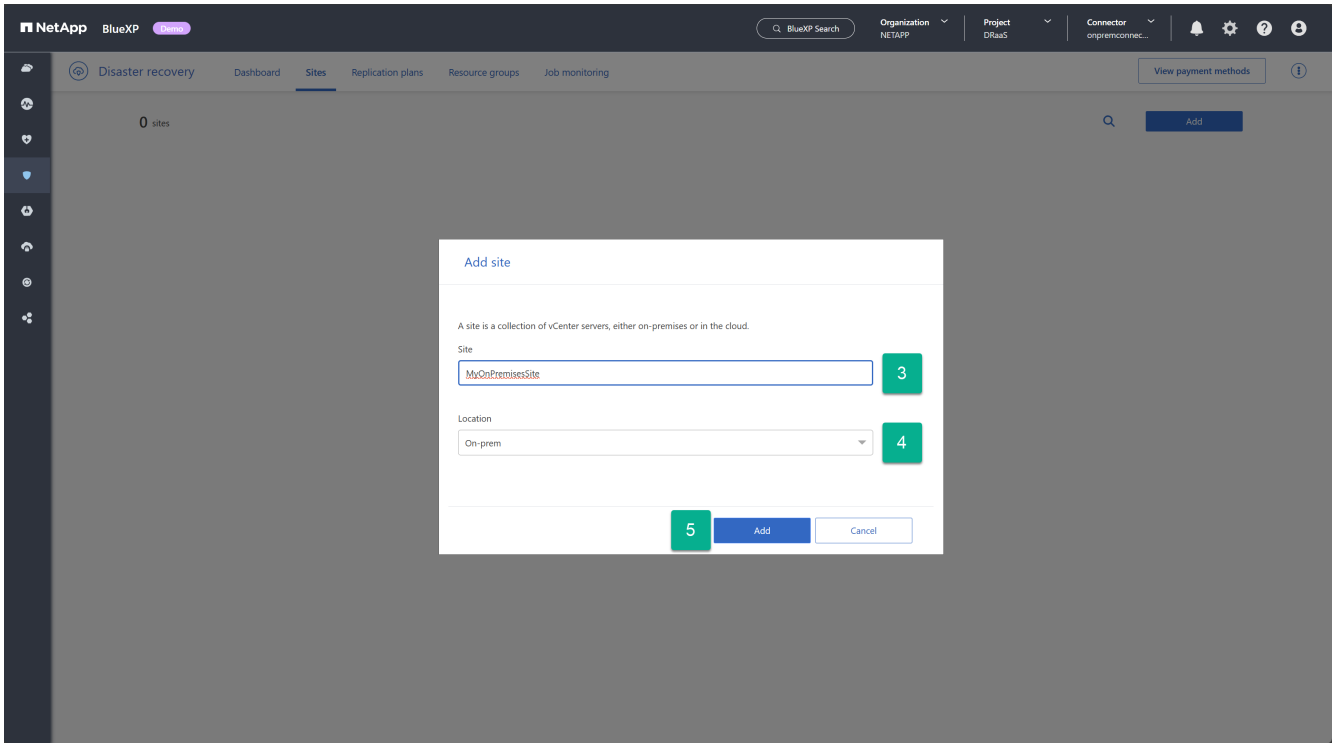
1. Dal menu di navigazione a sinistra di BlueXP, seleziona **Protezione** > **Disaster Recovery**.
2. Da qualsiasi pagina del disaster recovery di BlueXP, seleziona la scheda **Siti**.



3. Dalla scheda Siti, seleziona **Aggiungi**.



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

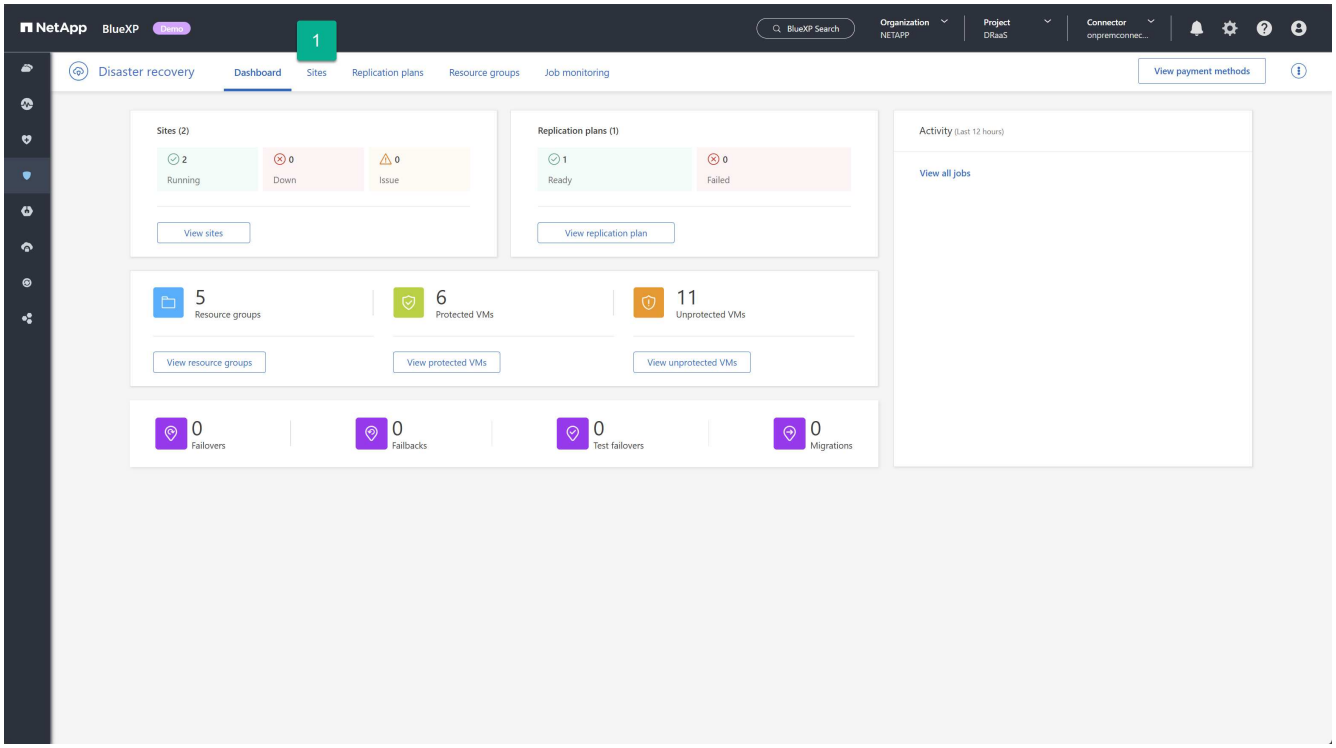


Se disponi di altri siti di produzione vCenter, puoi aggiungerli seguendo la stessa procedura.

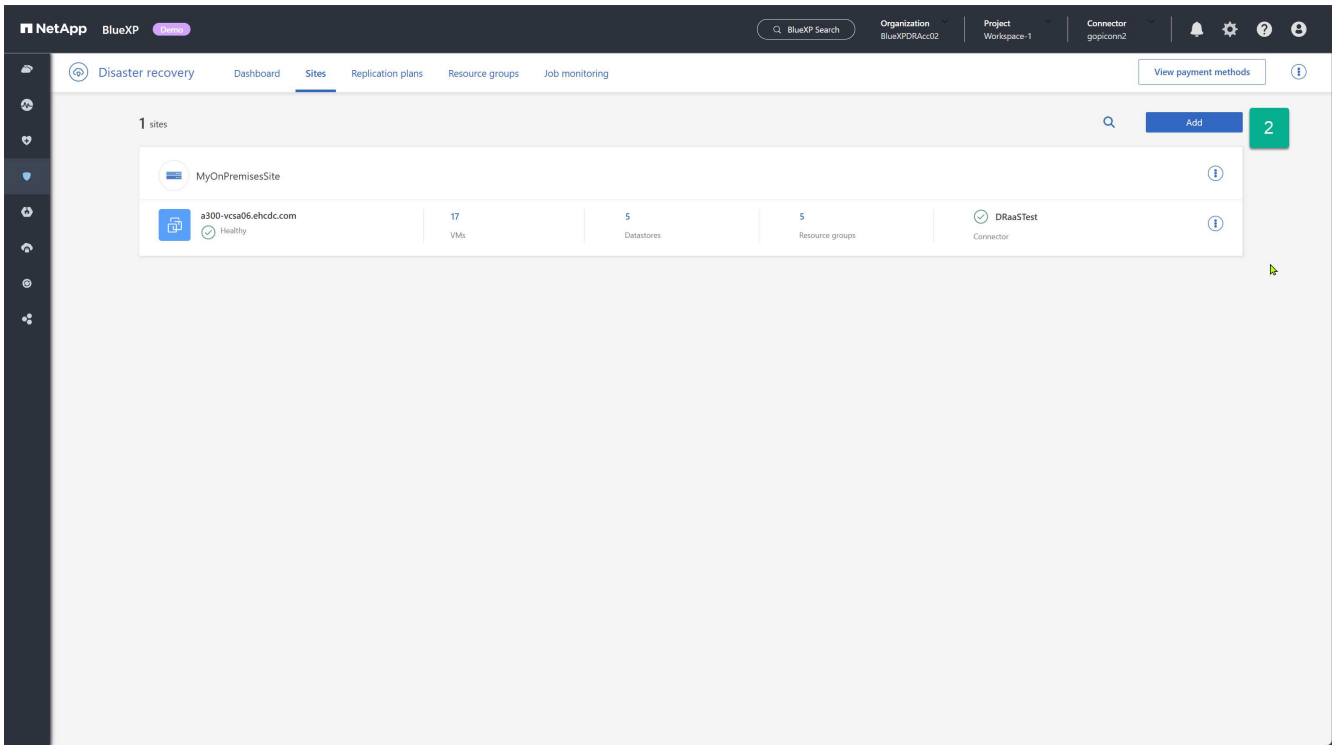
Crea siti cloud Amazon

Creare un sito DR per Amazon EVS utilizzando Amazon FSx per l'archiviazione NetApp ONTAP.

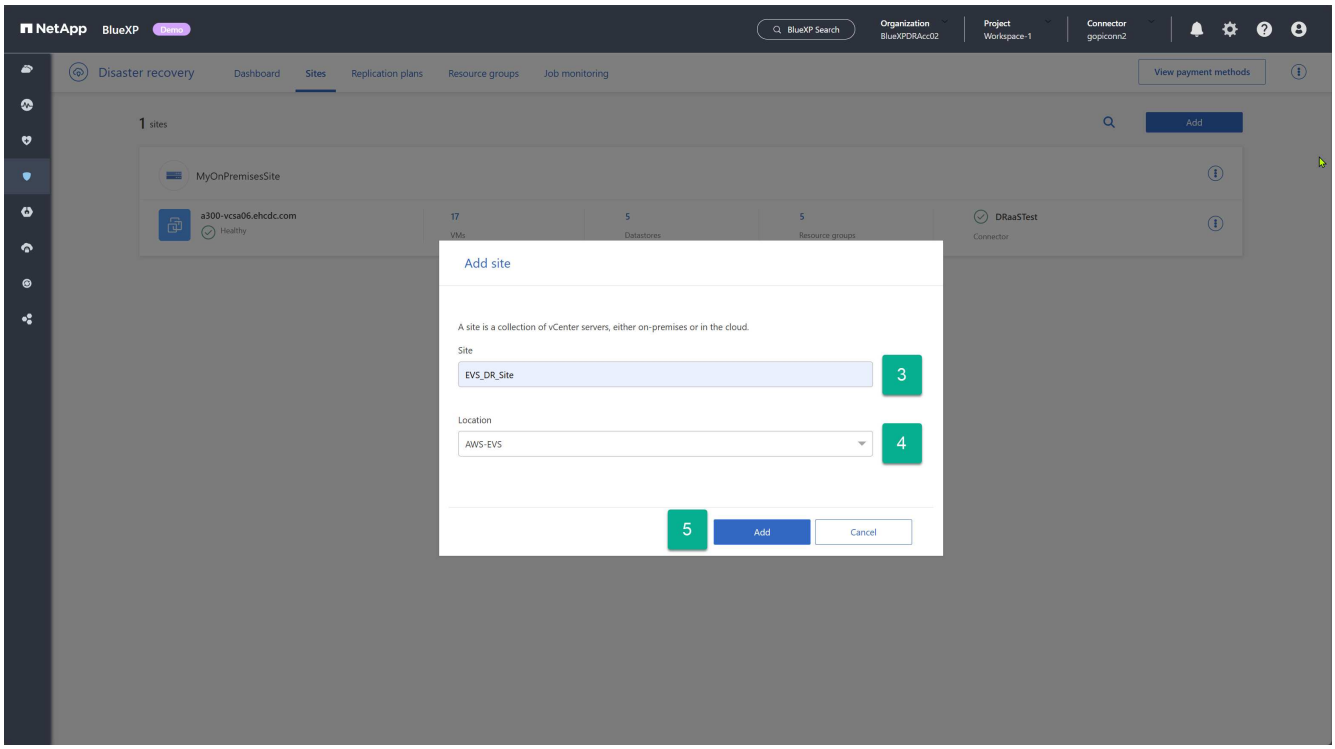
1. Da qualsiasi pagina del disaster recovery di BlueXP, seleziona la scheda **Siti**.



2. Dalla scheda 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

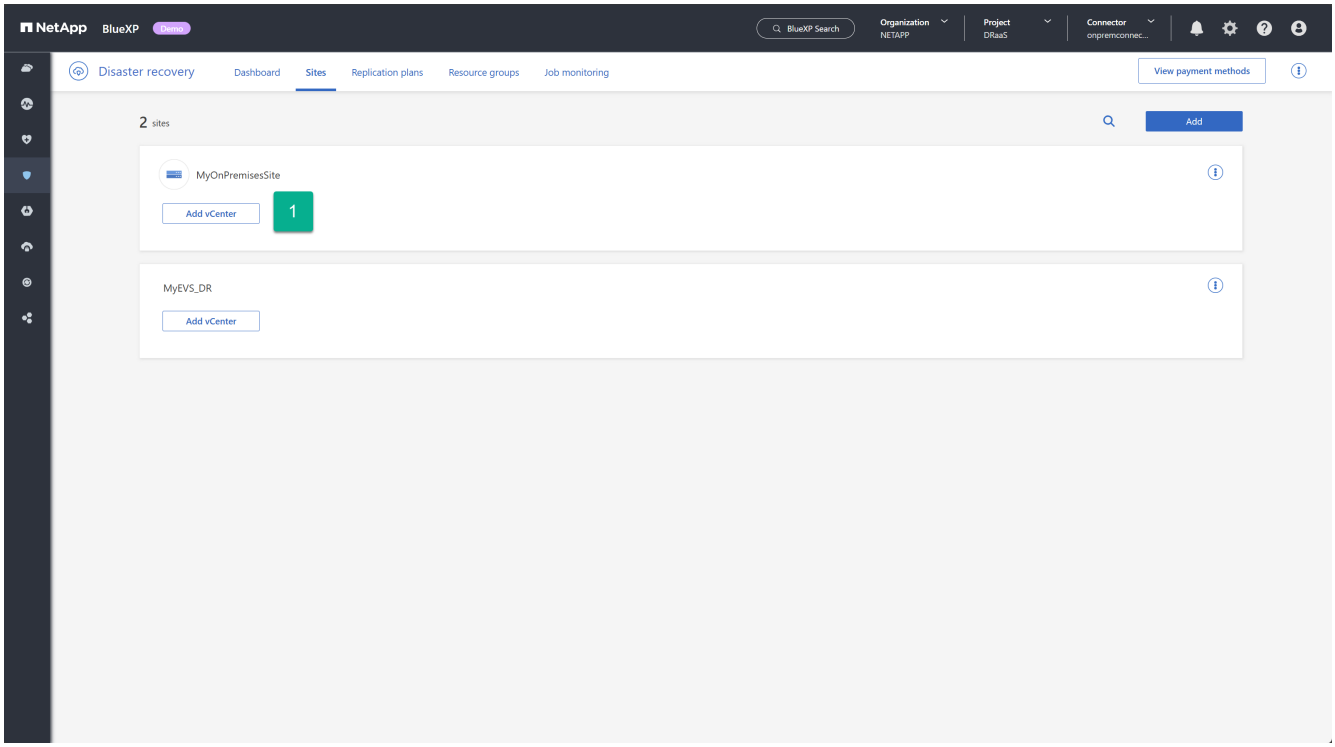
Ora hai creato un sito di produzione (sorgente) e un sito DR (destinazione).

Aggiungi cluster locali e Amazon EVS vCenter nel disaster recovery di BlueXP

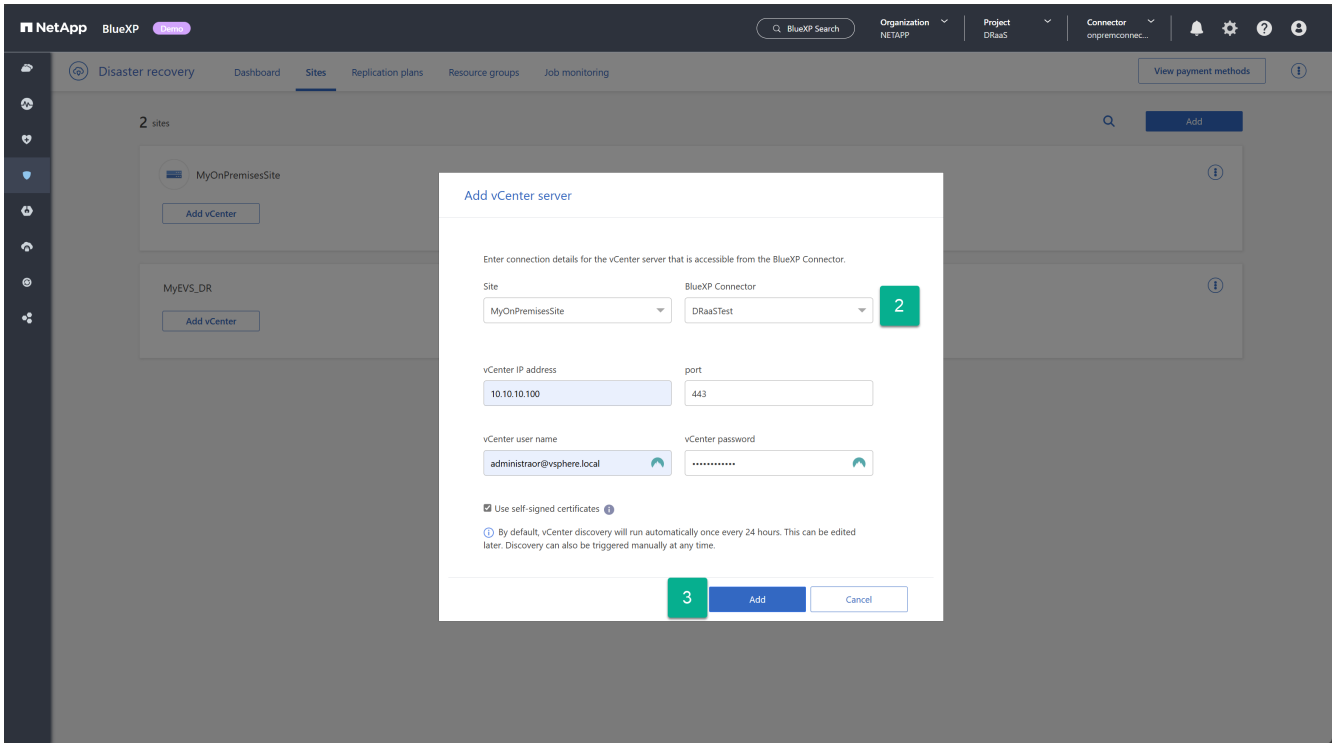
Una volta creati i siti, è ora possibile aggiungere i cluster vCenter a ciascun sito in BlueXP Disaster Recovery. Quando abbiamo creato ogni sito, abbiamo indicato ogni tipo di sito. Questo indica a BlueXP Disaster Recovery il tipo di accesso richiesto per i vCenter ospitati in ciascun tipo di sito. Uno dei vantaggi di Amazon EVS è che non esiste una reale differenziazione tra un vCenter Amazon EVS e un vCenter on-premise. Entrambi richiedono le stesse informazioni di connessione e autenticazione.

Passaggi per aggiungere un vCenter a ciascun sito

1. Dalla scheda **Siti**, seleziona **Aggiungi vCenter** per il sito desiderato.



2. Nella finestra di dialogo Aggiungi server vCenter, seleziona o fornisci le seguenti informazioni:
   a. Il connettore BlueXP ospitato nella tua AWS VPC.
   b. 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. Nome utente vCenter per l'account creato in precedenza che verrà utilizzato dal disaster recovery di BlueXP per gestire vCenter.
   e. Password vCenter per il nome utente fornito.
   f. Se la tua azienda utilizza un'autorità di certificazione (CA) esterna o il vCenter Endpoint Certificate Store per accedere ai tuoi vCenter, deseleziona la casella di controllo **Utilizza certificati autofirmati**. In caso contrario, lascia la casella selezionata.
3. Selezionare **Aggiungi**.



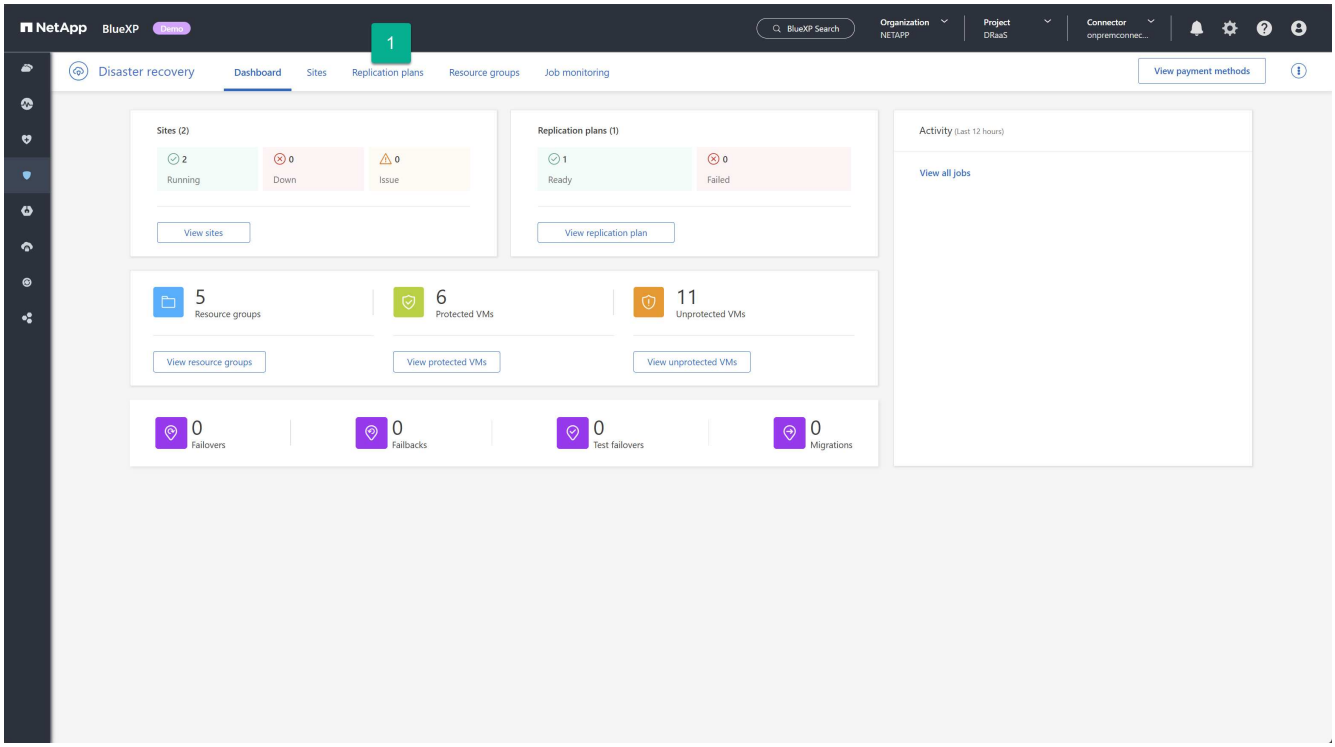
Creare piani di replicazione per Amazon EVS

Creazione di piani di replicazione nella panoramica del ripristino di emergenza di BlueXP

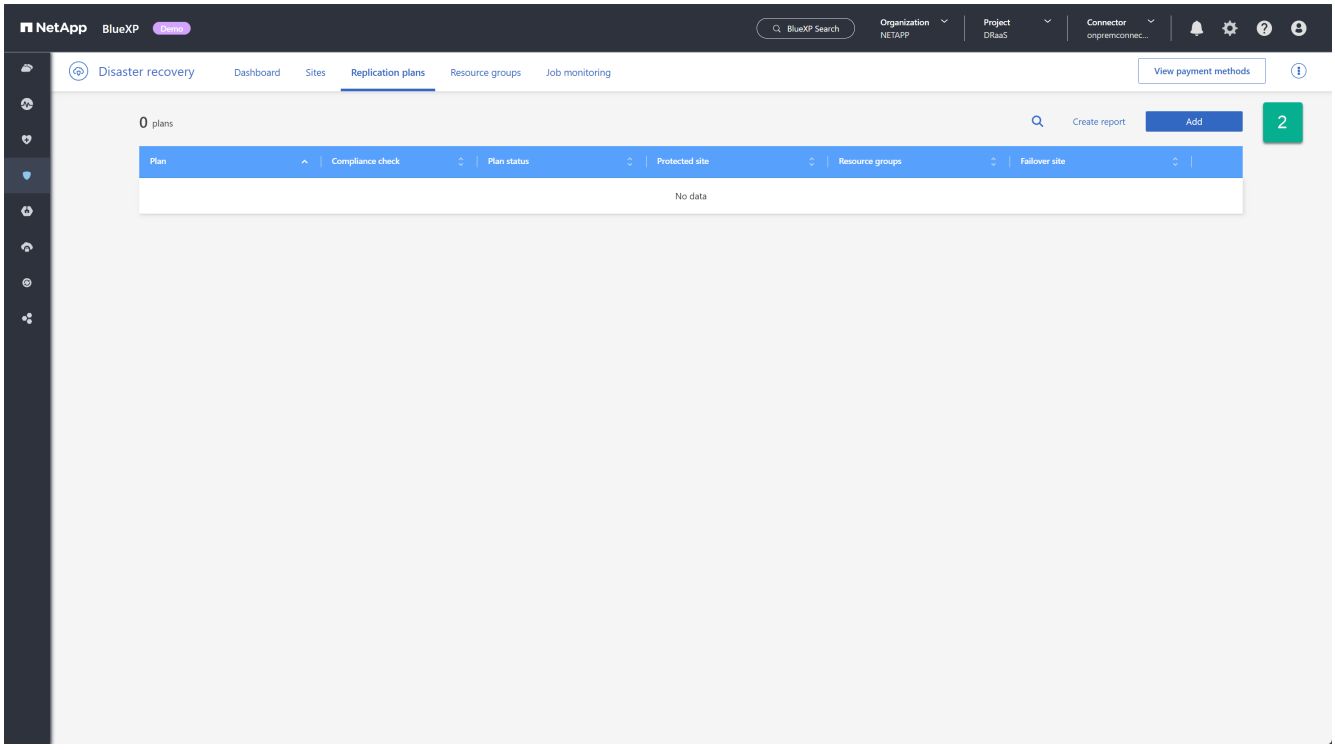
Dopo aver protetto i vCenter sul sito locale e aver configurato un sito Amazon EVS per utilizzare Amazon FSx for NetApp ONTAP da utilizzare come destinazione DR, è possibile creare un piano di replicazione (RP) per proteggere qualsiasi set di VM ospitate sul cluster vCenter all'interno del sito locale.

Per avviare il processo di creazione del piano di replicazione:

1. Da qualsiasi schermata di ripristino di emergenza di BlueXP, selezionare la scheda **Piani di replica**.



2. Nella schermata Piani di replicazione, seleziona **Aggiungi**.



Si apre la procedura guidata Crea piano di replica.

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

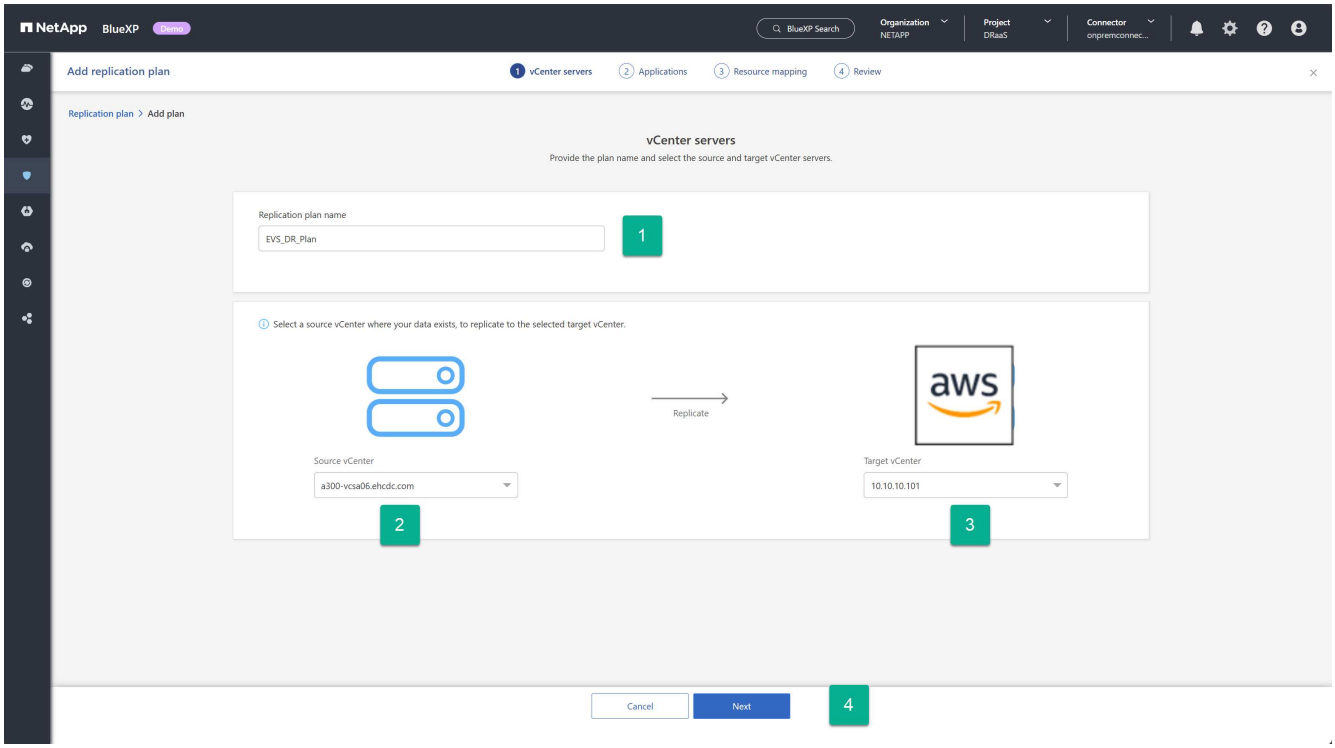
Creare un piano di replicazione: Passaggio 1: selezionare vCenter nel ripristino di emergenza di BlueXP

Per prima cosa, utilizzando il disaster recovery di BlueXP, 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 replicazione: Passaggio 2: selezionare le risorse della macchina virtuale nel ripristino di emergenza di BlueXP

Selezionare le macchine virtuali da proteggere tramite il ripristino di emergenza di BlueXP.

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. Selezionando ciascuna 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 la scheda Gruppo di risorse nella parte superiore dell'interfaccia utente di disaster recovery di

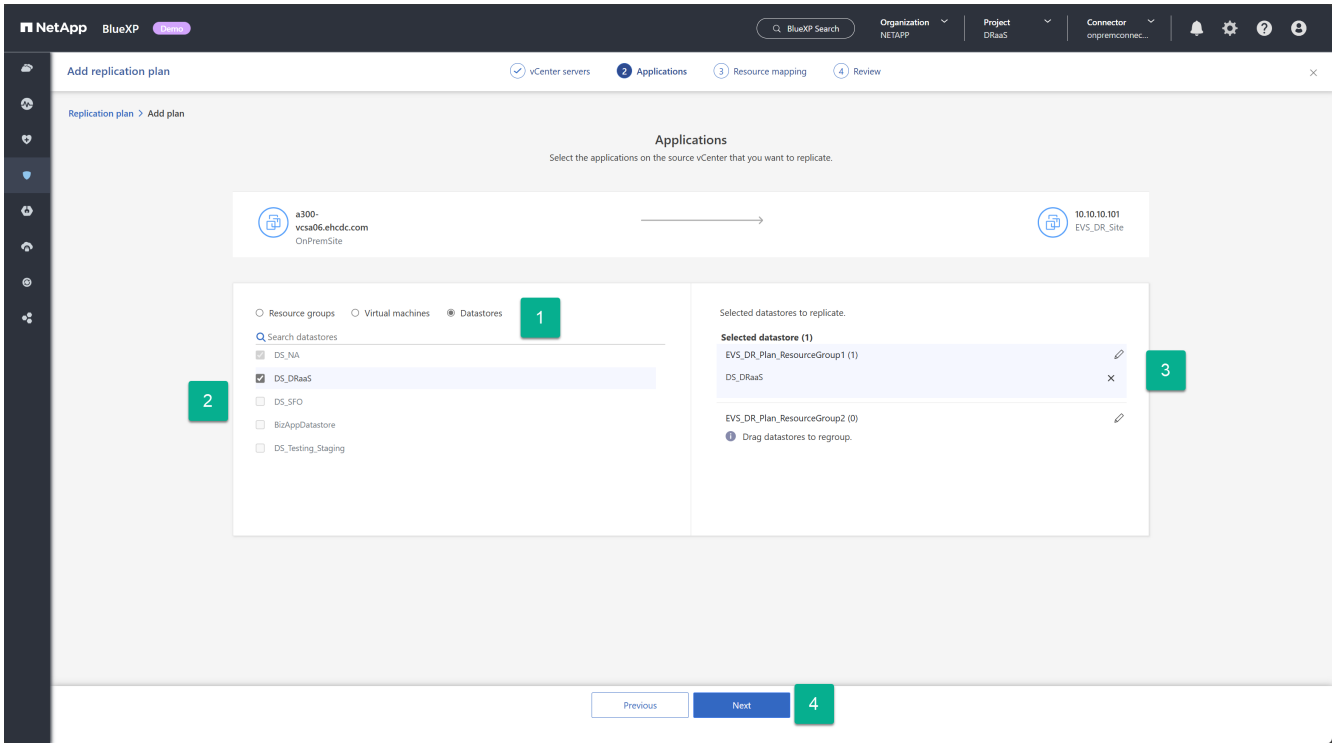
BlueXP. Questo non è obbligatorio, poiché puoi utilizzare gli altri due metodi per creare un gruppo di risorse come parte del processo di pianificazione della replica. Per ulteriori informazioni, vedere "Creare un piano di replica".

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

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 **Datastores**.
2. Seleziona le caselle di controllo accanto a ciascun datastore che desideri proteggere.
3. (Facoltativo) 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 nel ripristino di emergenza di BlueXP

Dopo aver ottenuto l'elenco delle VM che si desidera proteggere tramite il disaster recovery di BlueXP, 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:

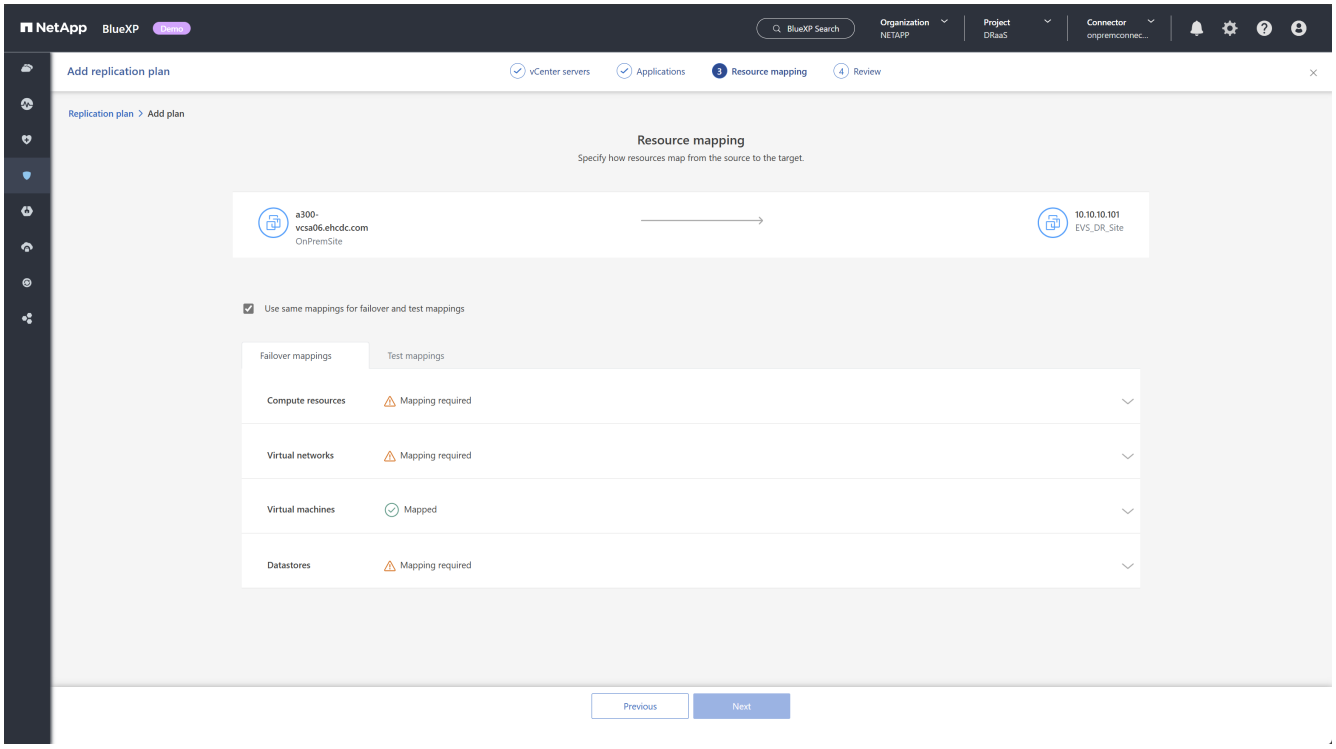
- Risorse di calcolo
- Reti virtuali
- Riconfigurazione della VM
- Mappatura del datastore

Ogni macchina virtuale richiede i primi tre tipi di informazioni. Il mapping del datastore è necessario per ogni datastore che ospita le macchine virtuali da proteggere.

- Le sezioni con l'icona di attenzione ( ) richiedono di fornire informazioni di mappatura.
- La sezione contrassegnata con l'icona di spunta ( ) sono stati mappati o hanno mappature predefinite. Esaminateli per assicurarvi che la configurazione corrente 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 richieste, selezionare la freccia rivolta verso il basso (**v**) accanto alla sezione.

Mappatura delle risorse di elaborazione

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.

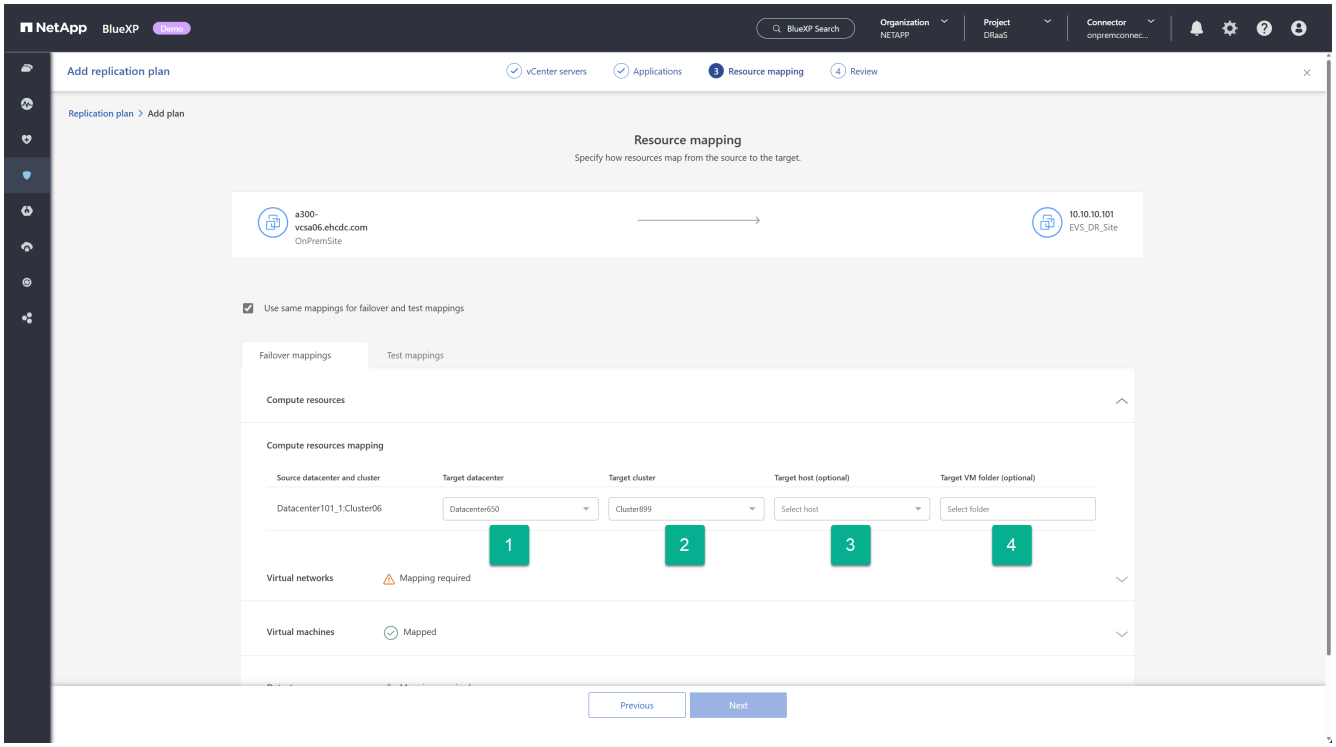
Passaggi per mappare le risorse di calcolo

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 il disaster recovery di BlueXP 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 esigenze e in base alle regole DRS configurate.

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

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



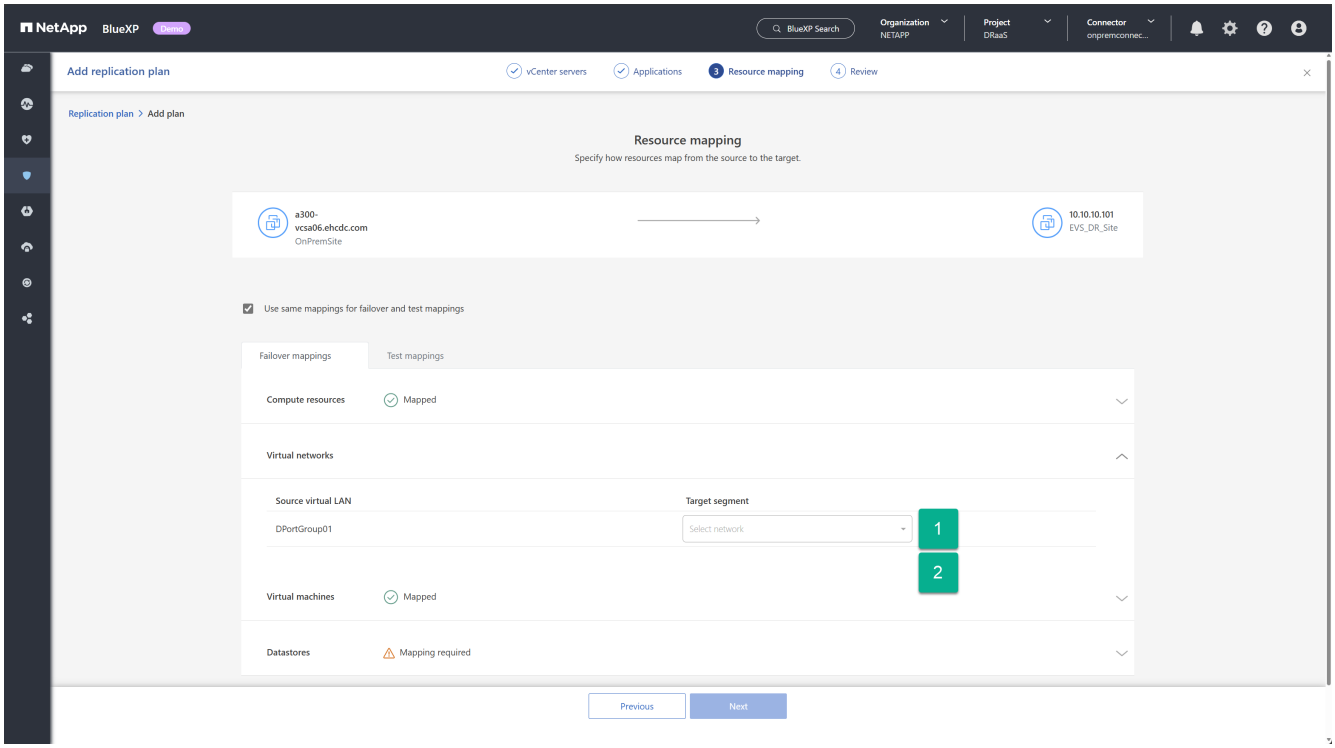
Mappare le risorse di rete virtuale

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 di DR, è necessario identificare a quali reti virtuali del sito di DR connettere queste VM. A tale scopo, è necessario mappare ciascuna rete virtuale nel sito on-premise a una rete associata nel sito di 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 ciascuna rete virtuale di origine elencata.



Definire le opzioni per la riconfigurazione della VM durante il failover

Ogni VM potrebbe richiedere modifiche per funzionare correttamente nel sito vCenter DR. La sezione Macchine virtuali consente di apportare le modifiche necessarie.

Per impostazione predefinita, il disaster recovery di BlueXP utilizza per ogni VM le stesse impostazioni utilizzate nel sito locale di origine. Questo 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. Ciò richiede la configurazione delle 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, è possibile 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.
- **Mapping subnet**: questa opzione riconfigura l'indirizzo IP di ciascuna VM in base alla configurazione CIDR della rete virtuale di destinazione. Per utilizzare questa funzionalità, assicurarsi che le reti virtuali di ogni vCenter dispongano di un'impostazione CIDR definita all'interno del servizio, come modificato nelle informazioni di vCenter nella scheda Siti.

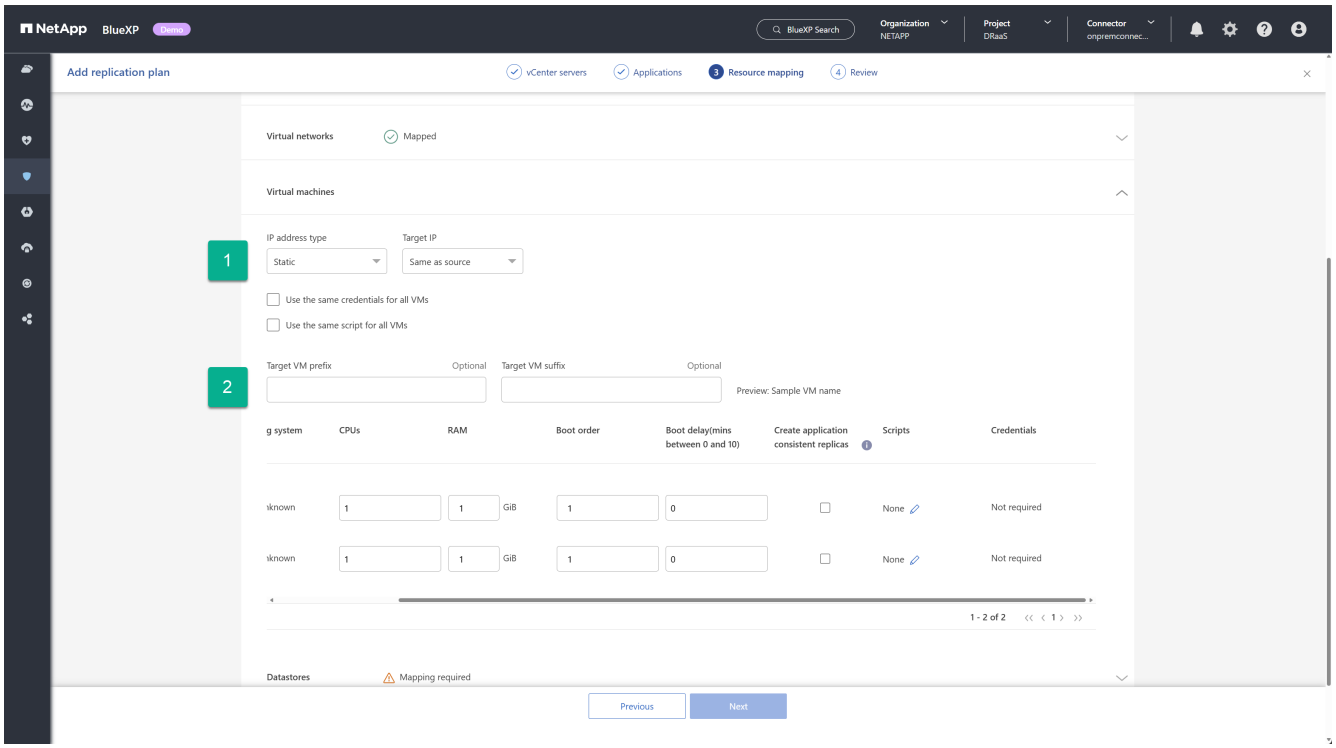
Dopo aver configurato le subnet, il mapping delle subnet utilizza lo stesso componente unitario dell'indirizzo IP per la configurazione della VM di origine e di destinazione, ma sostituisce il componente subnet dell'indirizzo

IP in base alle informazioni CIDR fornite. Questa funzionalità richiede inoltre che entrambe le reti virtuali di origine e 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, presupponiamo 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.

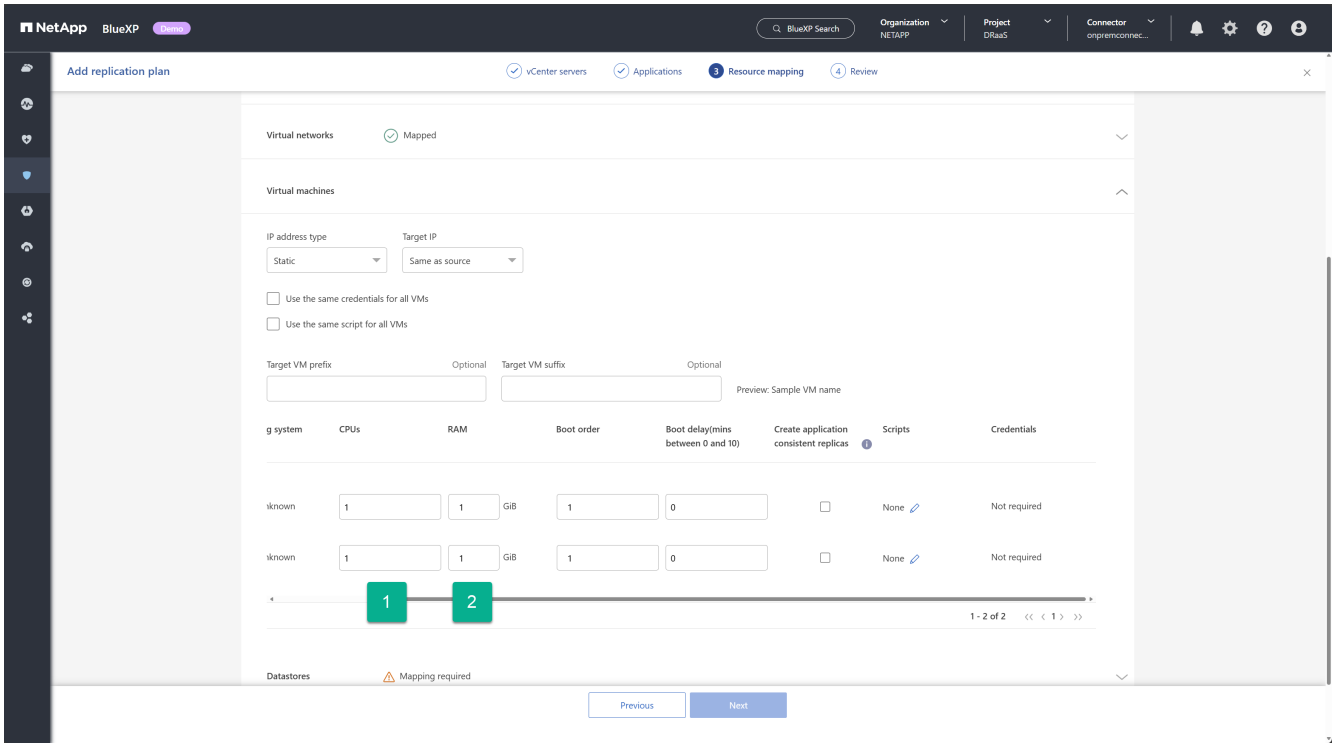


Riconfigurazione delle risorse di elaborazione della VM

Sono disponibili diverse opzioni per riconfigurare le risorse di elaborazione delle VM. Il disaster recovery di BlueXP 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) Modifica il numero di CPU virtuali che ogni VM deve utilizzare. Questo potrebbe essere necessario 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.

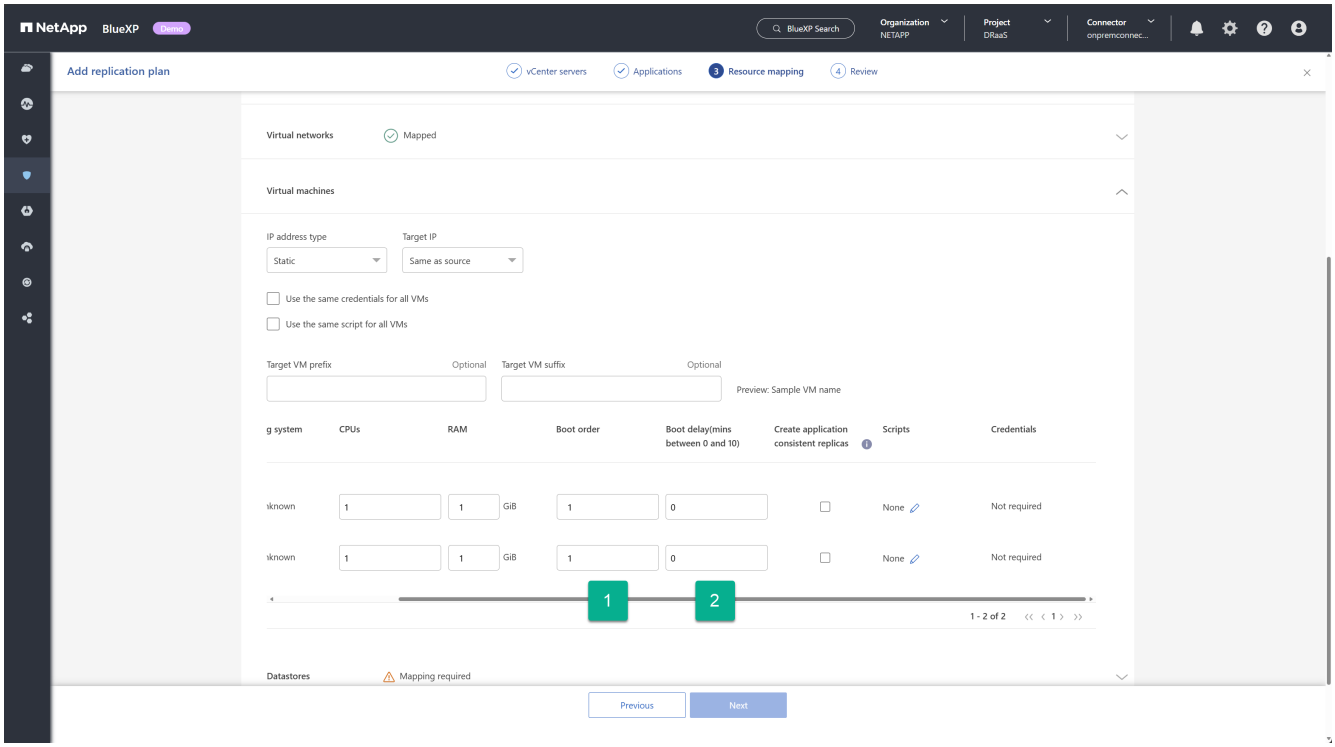


Ordine di avvio

Il disaster recovery di BlueXP supporta il riavvio ordinato delle VM in base a un campo relativo all'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 si avviano 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. Il disaster recovery di BlueXP tenta di riavviare in parallelo le VM con 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. Questo numero è espresso in minuti.



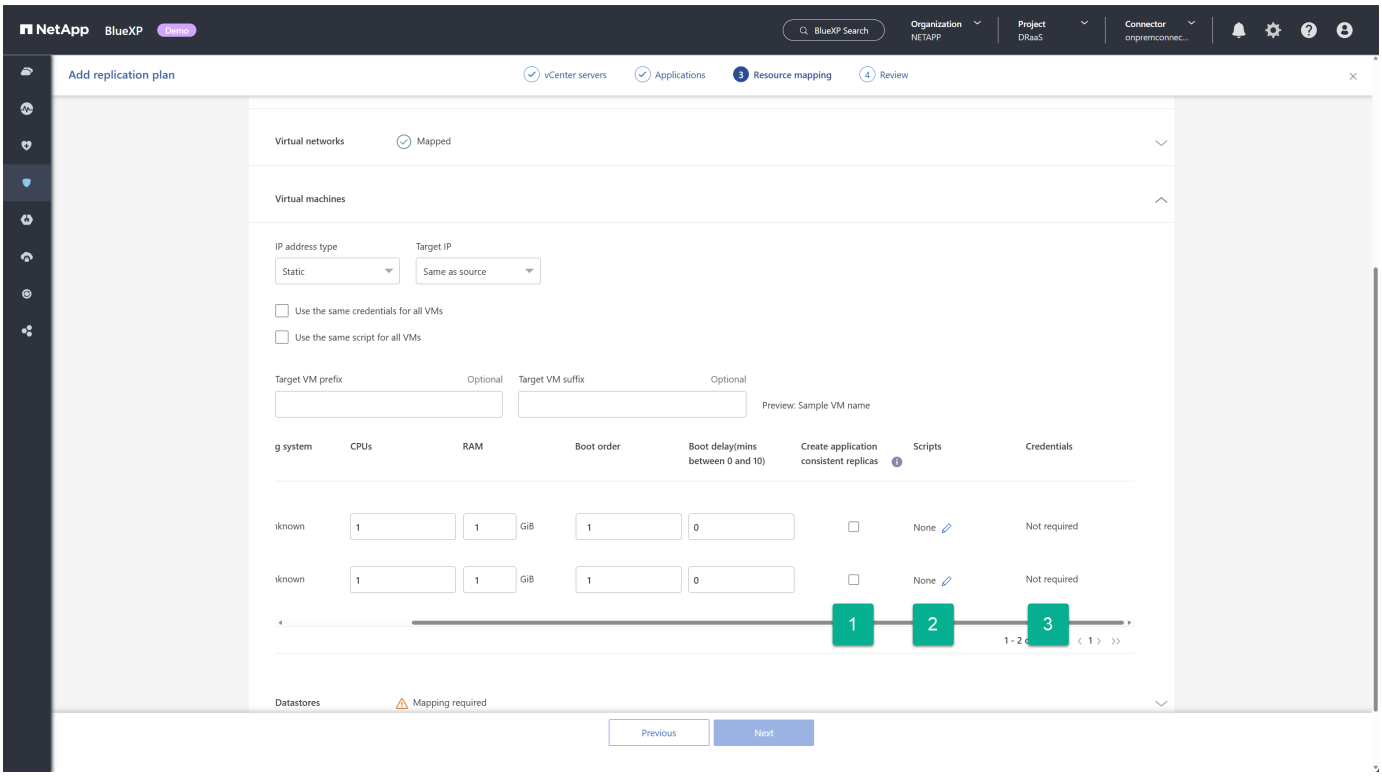
Operazioni personalizzate del sistema operativo guest

Il disaster recovery di BlueXP supporta l'esecuzione di alcune operazioni del sistema operativo guest per ogni VM:

- Il ripristino di emergenza di BlueXP può eseguire backup coerenti con l'applicazione delle VM che eseguono database Oracle e database Microsoft SQL Server.
- Il disaster recovery di BlueXP può eseguire script personalizzati adatti al sistema operativo guest per ciascuna VM. L'esecuzione di tali script richiede credenziali utente accettate dal sistema operativo guest, con privilegi sufficienti 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 durante il processo di avvio, carica uno script per tutte le VM. Per eseguire un singolo script in tutte le VM, seleziona la casella di controllo evidenziata e compila i campi.
3. Alcune modifiche alla configurazione richiedono credenziali utente con autorizzazioni adeguate per eseguire le operazioni. 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

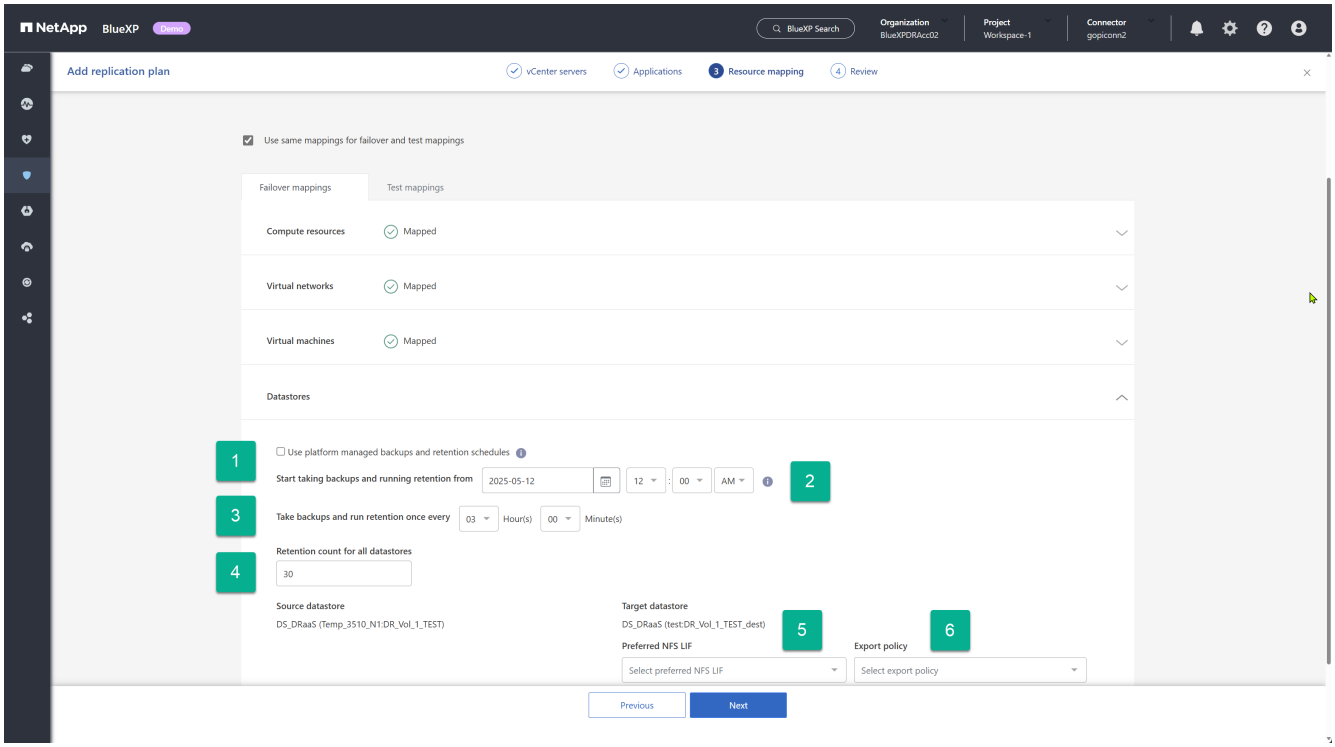
Il passaggio finale nella creazione di un piano di replica consiste nell'identificare come ONTAP debba proteggere i datastore. Queste impostazioni definiscono l'obiettivo del punto di ripristino (RPO) del piano di replica, il numero di backup da mantenere e dove replicare i volumi ONTAP di hosting di ciascun datastore vCenter.

Per impostazione predefinita, il disaster recovery di BlueXP 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 i LIF (interfacce logiche) dei dati e la policy di esportazione da utilizzare. Se non si specificano queste impostazioni, il disaster recovery di BlueXP utilizza tutti i LIF dei dati associati al protocollo appropriato (NFS, iSCSI o FC) e 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 il disaster recovery di BlueXP 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. Specifica quanti backup storici devono essere conservati. Il servizio mantiene lo stesso numero di backup sul cluster di storage di origine e di destinazione.
5. (Facoltativo) Selezionare un'interfaccia logica predefinita (LIF dati) per ciascun volume. Se non viene selezionata alcuna interfaccia logica, verranno configurati tutti i LIF dati nell'SVM di destinazione che supportano il protocollo di accesso al volume.
6. (Facoltativo) Selezionare una policy di esportazione per qualsiasi volume NFS. Se non selezionata, verrà utilizzata la policy di esportazione predefinita.



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

Creare un piano di replicazione: Passaggio 4 - Verificare le impostazioni nel ripristino di emergenza di BlueXP

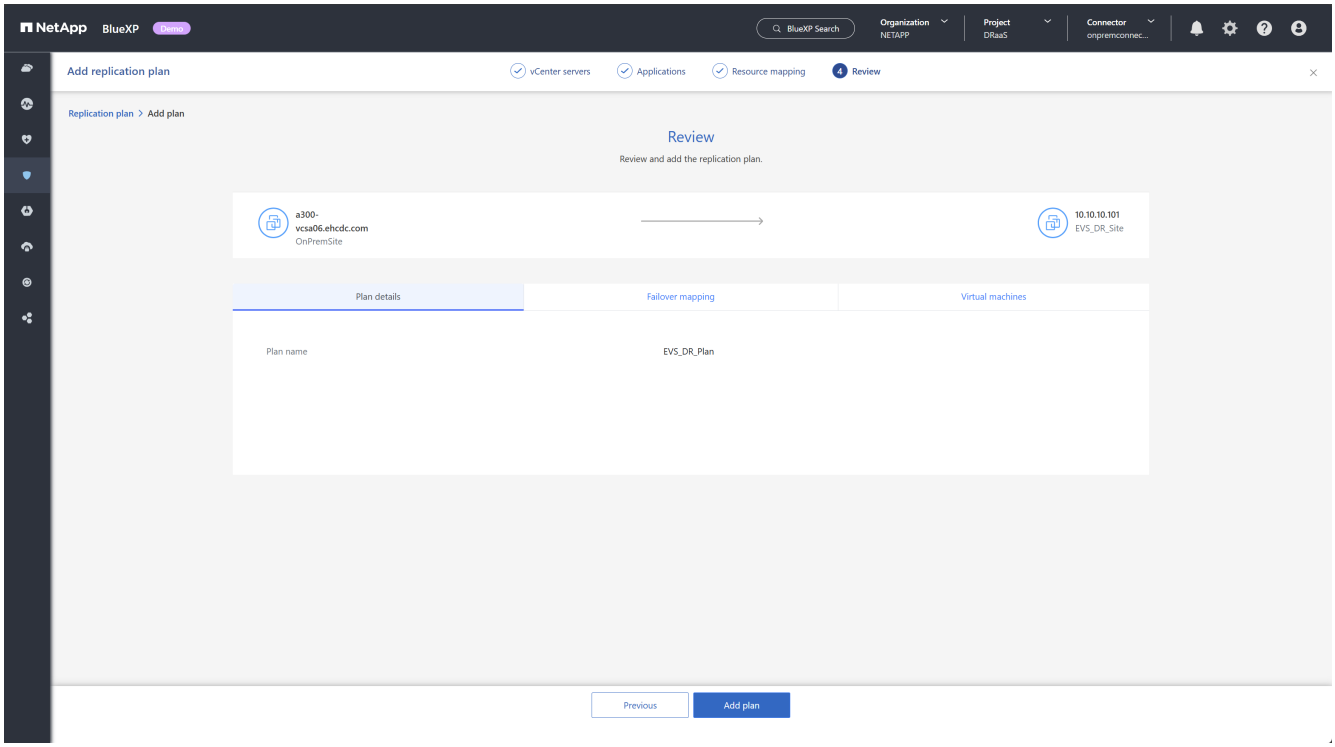
Dopo aver aggiunto le informazioni sul piano di replica nel ripristino di emergenza di BlueXP, verificare che le informazioni immesse siano corrette.

Fasi

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



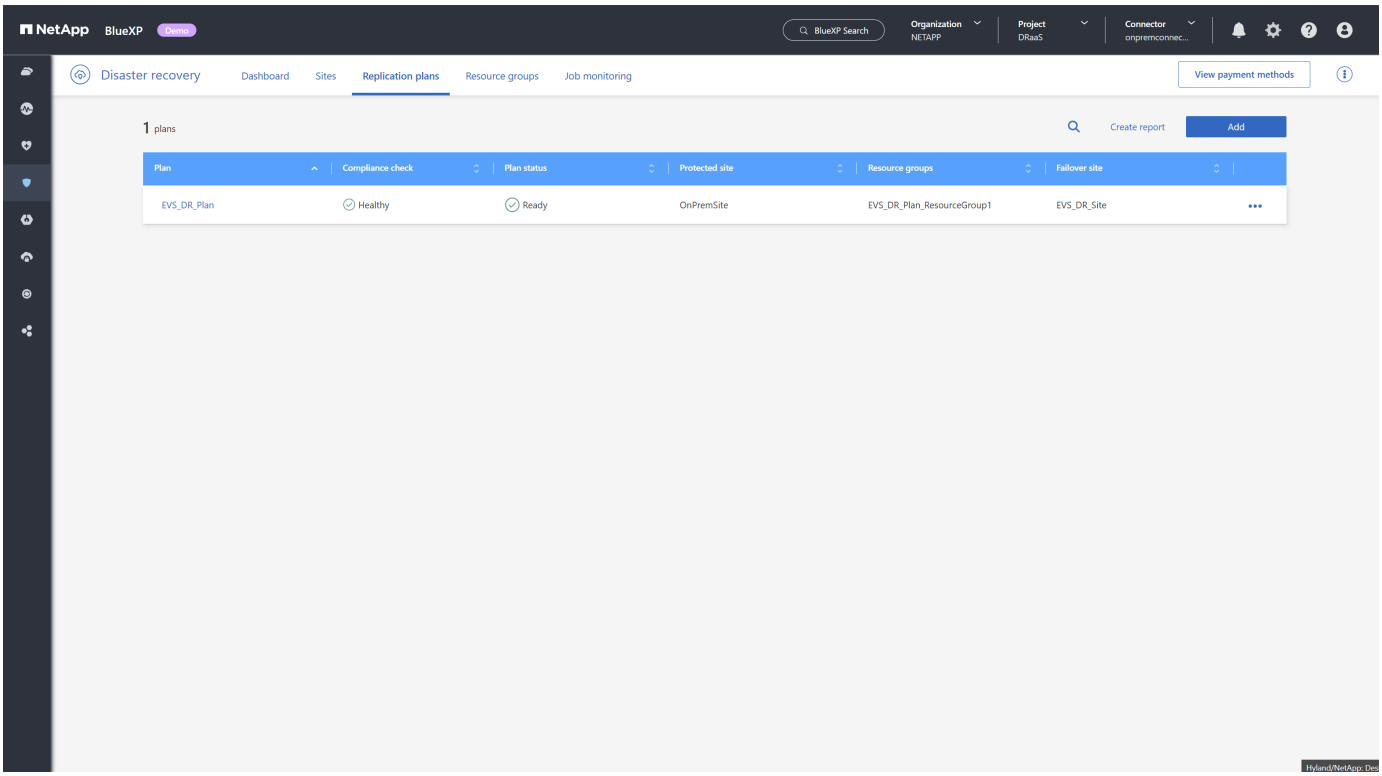
2. Quando sei sicuro che tutte le impostazioni siano corrette, seleziona **Aggiungi piano** nella parte inferiore dello schermo.

Continua con "Verificare il piano di replicazione" .

Verificare che tutto funzioni nel ripristino di emergenza di BlueXP

Dopo aver aggiunto il piano di replicazione nel disaster recovery di BlueXP, si torna alla pagina Piani di replicazione, dove è possibile visualizzare i piani di replicazione e il loro 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



Il disaster recovery di BlueXP esegue una serie di test per verificare che tutti i componenti (cluster ONTAP, cluster vCenter e VM) siano accessibili e in condizioni idonee affinché il servizio protegga le VM. Questo controllo, chiamato controllo di conformità, 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 replicazione
- Il nome del sito di failover (destinazione)

Eseguire operazioni di piano di replicazione con il ripristino di emergenza BlueXP

Utilizzare il disaster recovery di BlueXP con Amazon EVS e Amazon FSx per NetApp ONTAP per eseguire le seguenti operazioni: failover, failover di prova, aggiornamento delle risorse, migrazione, acquisizione di uno snapshot immediato, disabilitazione/abilitazione del piano di replica, pulizia di 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.

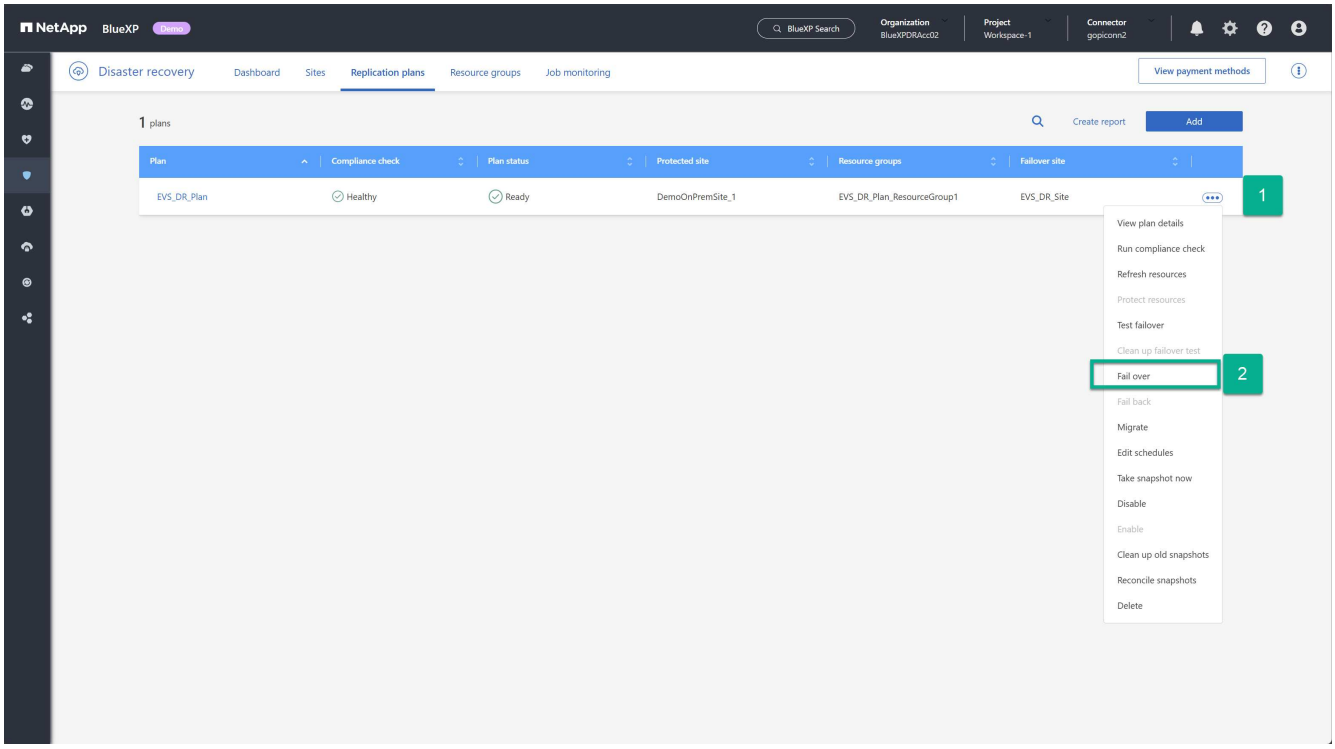
Il failover è un processo avviato manualmente.

Passaggi per accedere all'operazione di failover

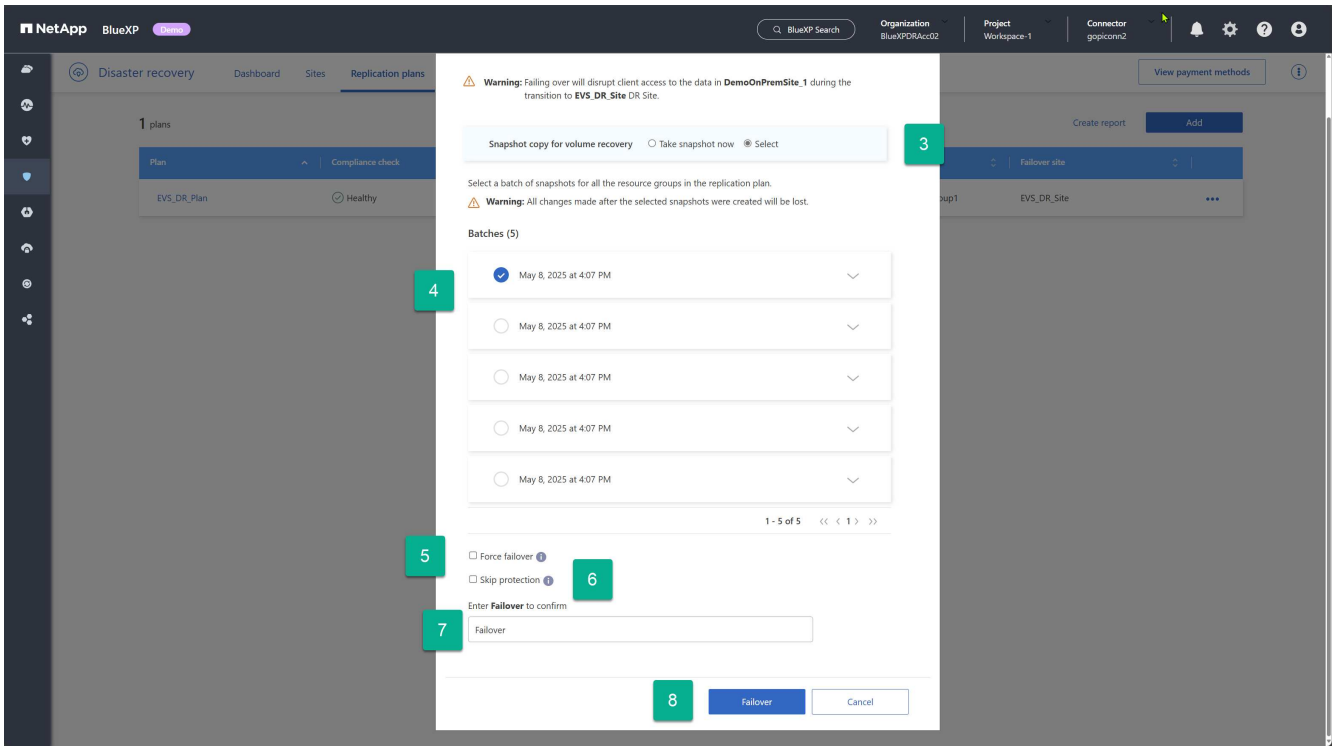
1. Dal menu di navigazione a sinistra di BlueXP, seleziona **Protezione** > **Disaster Recovery**.
2. Dal menu di ripristino di emergenza di BlueXP, selezionare **Piani di replica**.

Passaggi per eseguire un failover

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



3. Se il sito di produzione (protetto) non è accessibile, seleziona 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 il disaster recovery di BlueXP forzi il processo di failover indipendentemente dallo stato del piano di replica. Questa opzione dovrebbe essere utilizzata solo come ultima risorsa.
6. (Facoltativo) Selezionare se si desidera che il disaster recovery di BlueXP 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**.



Test del failover

Un test failover è simile a un failover, tranne che per due differenze.

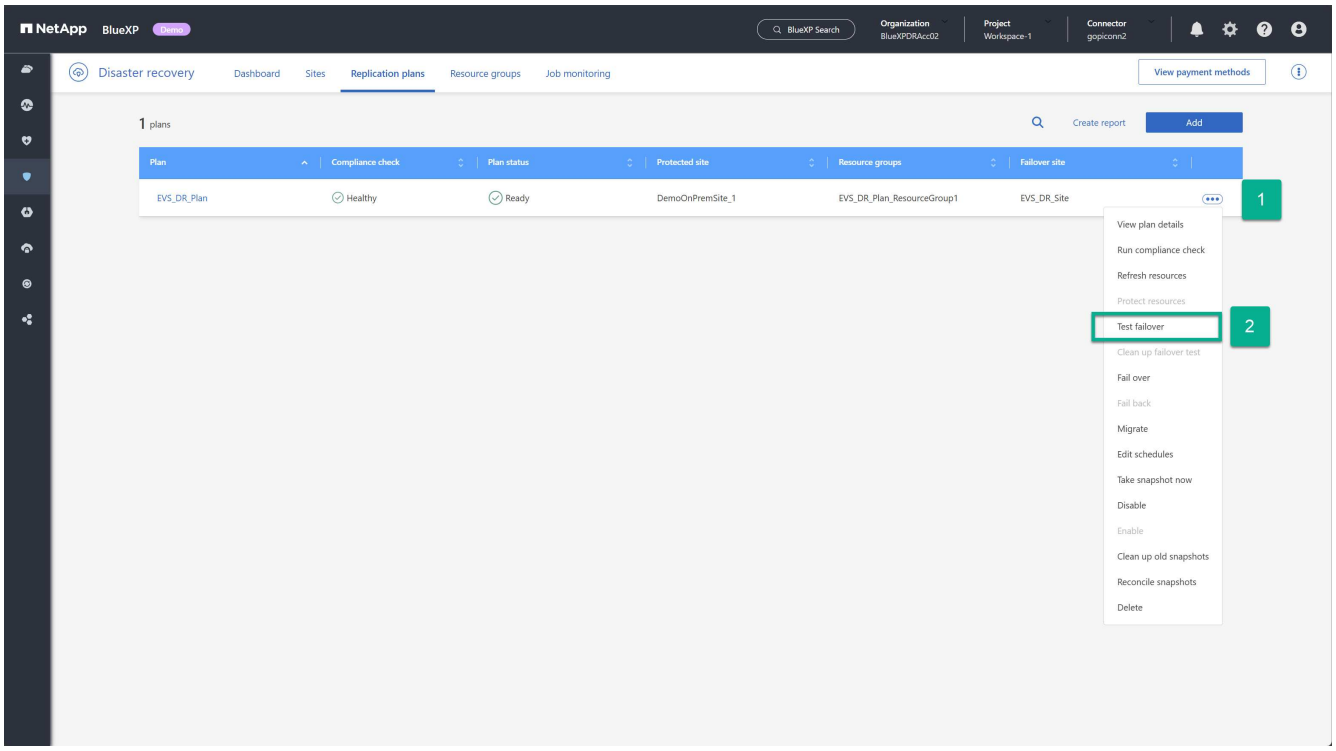
- Il sito di produzione è ancora attivo e tutte le VM funzionano ancora come previsto.
- Continua la protezione di disaster recovery di BlueXP per le VM di produzione.

Ciò si ottiene utilizzando volumi ONTAP FlexClone nativi nel sito di destinazione. Per ulteriori informazioni sul failover di test, vedere "Eseguire il failover delle applicazioni su un sito remoto | Documentazione NetApp" .

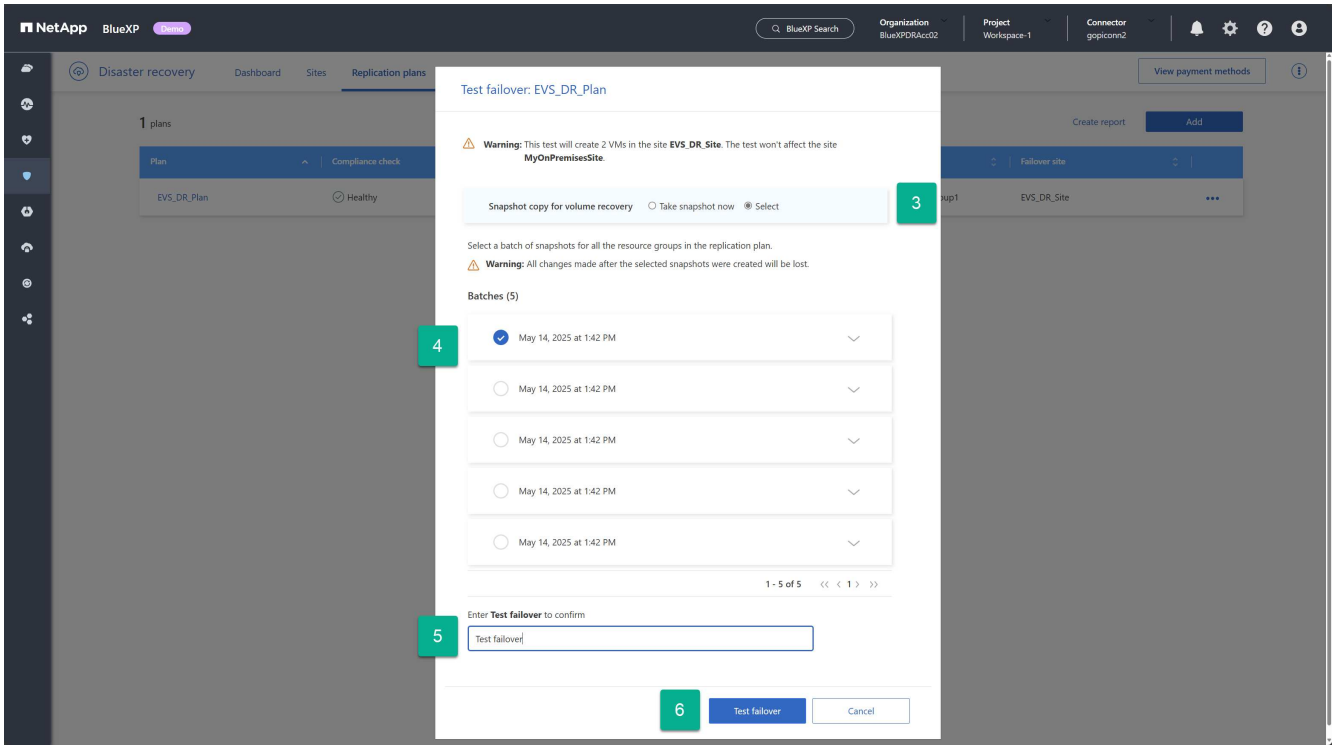
I passaggi per eseguire un failover di prova sono identici a quelli utilizzati per eseguire un failover reale, con la differenza che si utilizza l'operazione Failover di prova nel menu contestuale del piano di replica.

Fasi

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**.

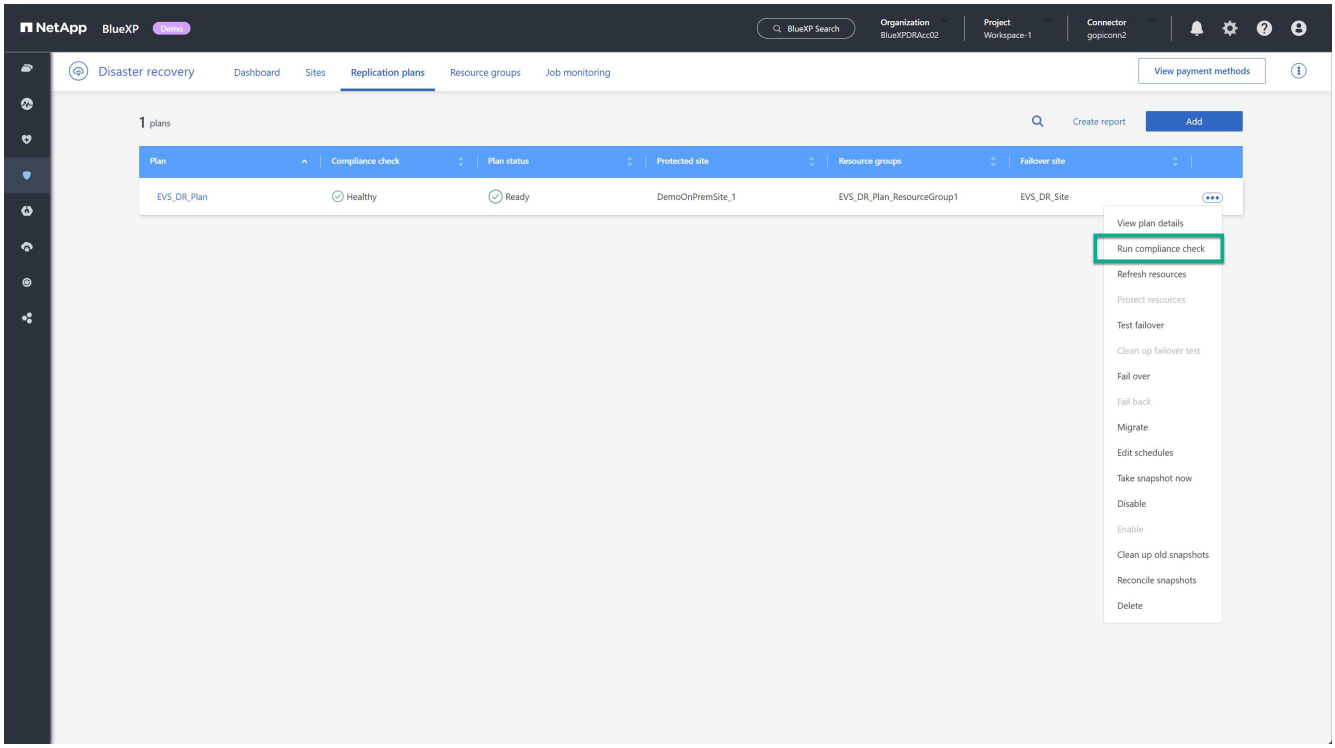


Eseguire un controllo di conformità

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

Fasi

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:



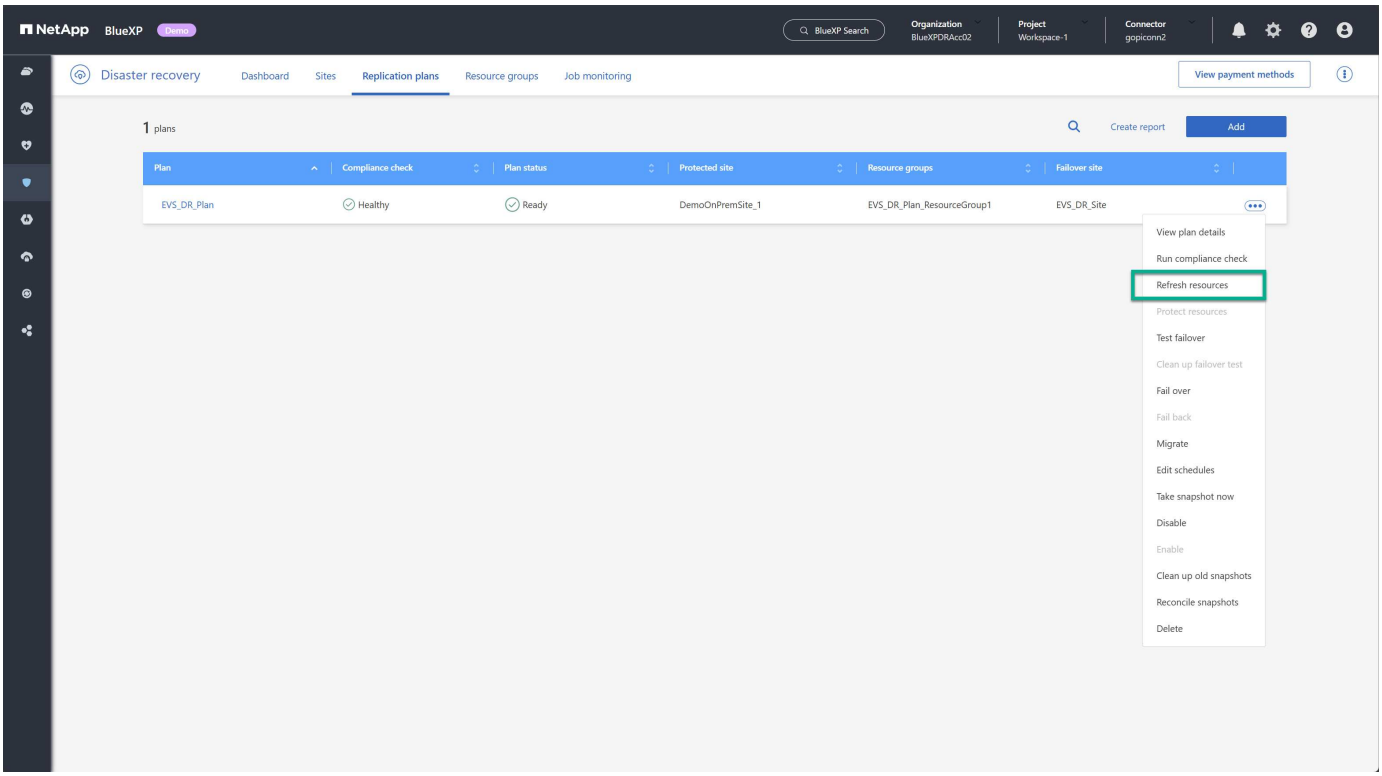
3. Per modificare la frequenza con cui il disaster recovery di BlueXP esegue automaticamente i controlli di conformità, selezionare l'opzione **Modifica pianificazioni** dal menu Azioni del piano di replica.

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 di disaster recovery BlueXP. Per impostazione predefinita, il servizio esegue questa operazione automaticamente 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:

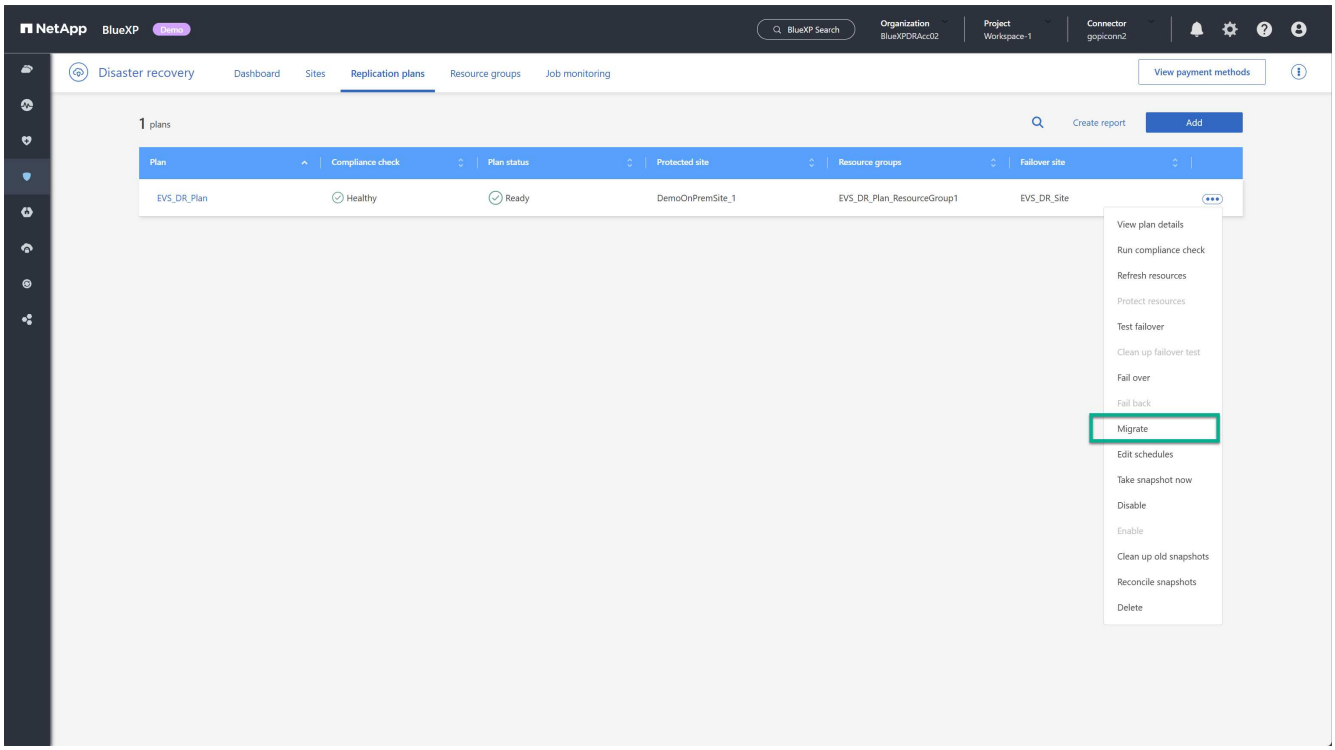
- Aggiornamento vCenter: esegui un aggiornamento vCenter ogni volta che le VM vengono aggiunte, eliminate o spostate da un cluster vCenter:
- Aggiornamento del piano di replica: esegue un aggiornamento del piano di replica ogni volta che una VM viene spostata tra datastore nello stesso cluster vCenter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



Migrare

Sebbene il disaster recovery di BlueXP sia utilizzato principalmente per casi d'uso di disaster recovery, può anche consentire spostamenti una tantum di un set di VM dal sito di origine a quello di destinazione. Questo potrebbe essere necessario per una migrazione coordinata al cloud o per prevenire 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, seleziona **Migra** dal menu Azioni del piano di replicazione:

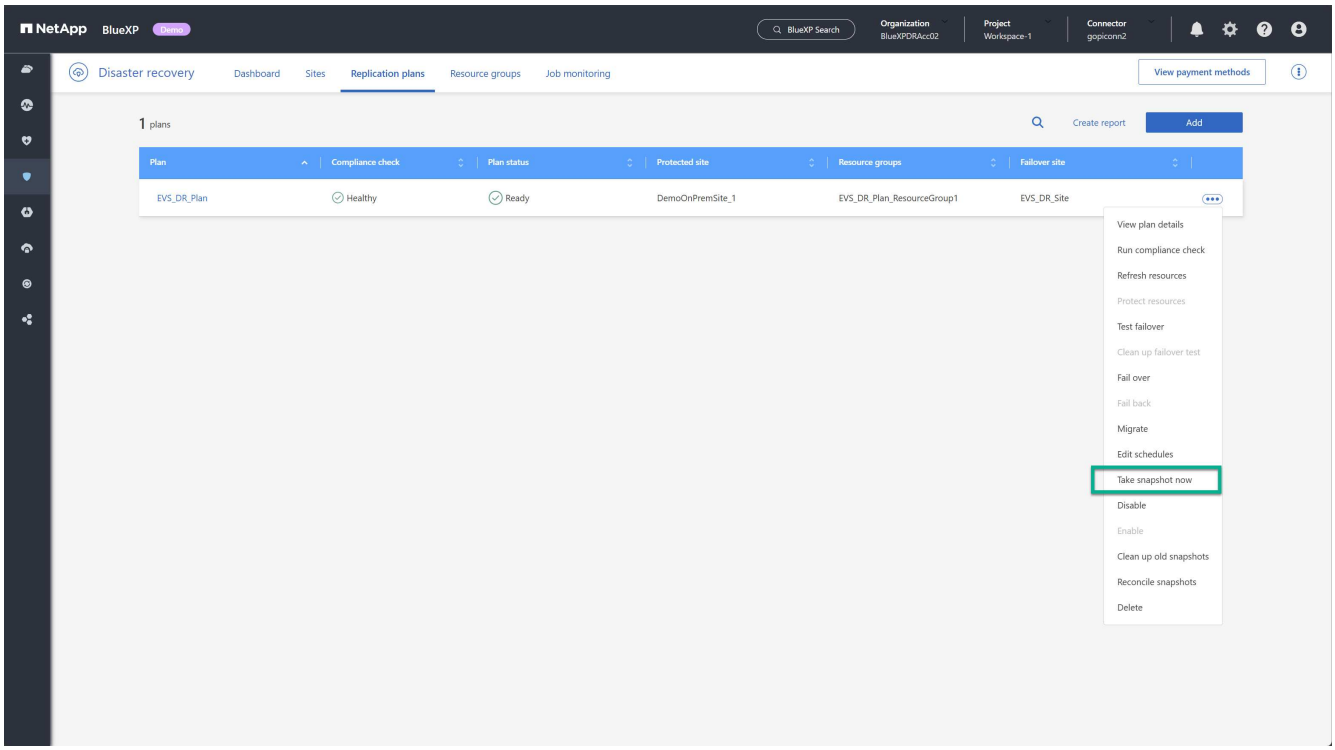


3. Immettere le informazioni nella finestra di dialogo Migra.

Scatta un'istantanea adesso

È possibile eseguire uno snapshot immediato del piano di replica in qualsiasi momento. Questo snapshot è incluso nelle considerazioni sul disaster recovery di BlueXP, definite 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:

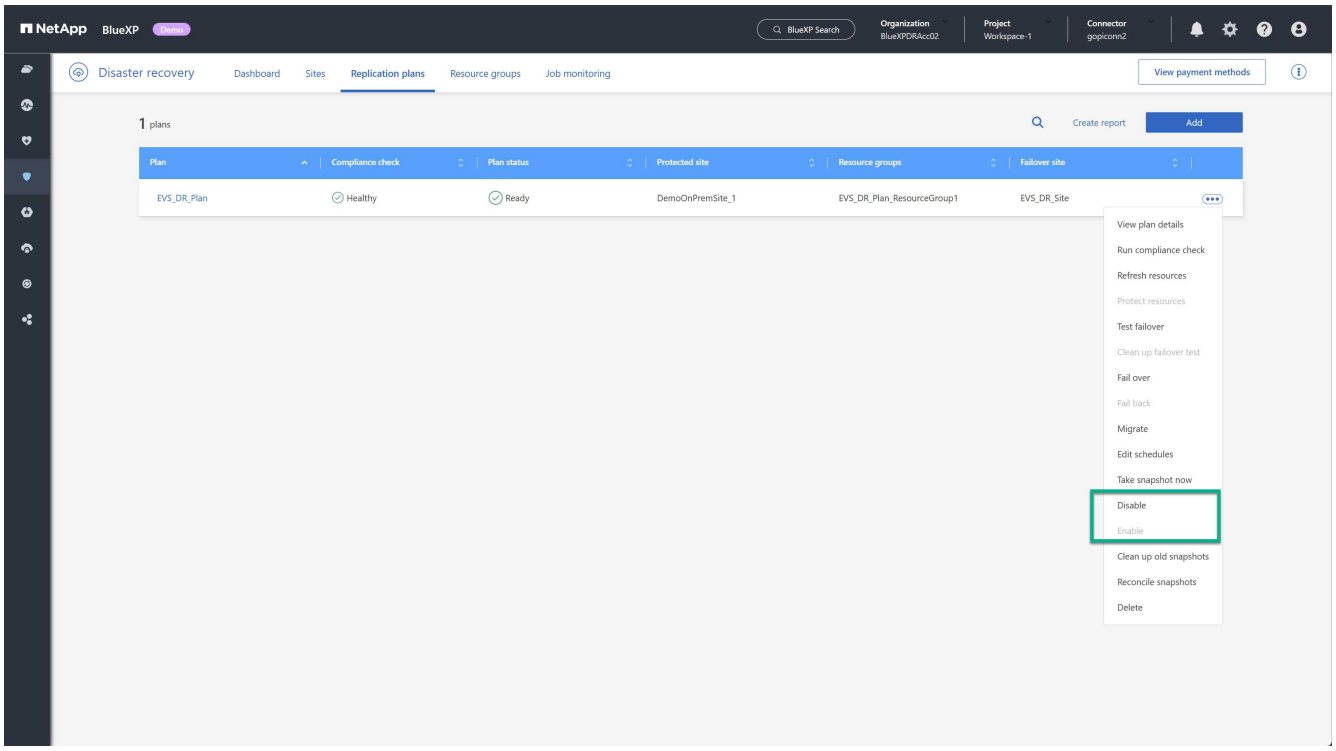


Disabilitare o abilitare il piano di replicazione

Potrebbe essere necessario interrompere temporaneamente il piano di replica per eseguire operazioni o interventi di manutenzione che potrebbero influire sul processo di replica. Il servizio fornisce un metodo per interrompere e riavviare 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.

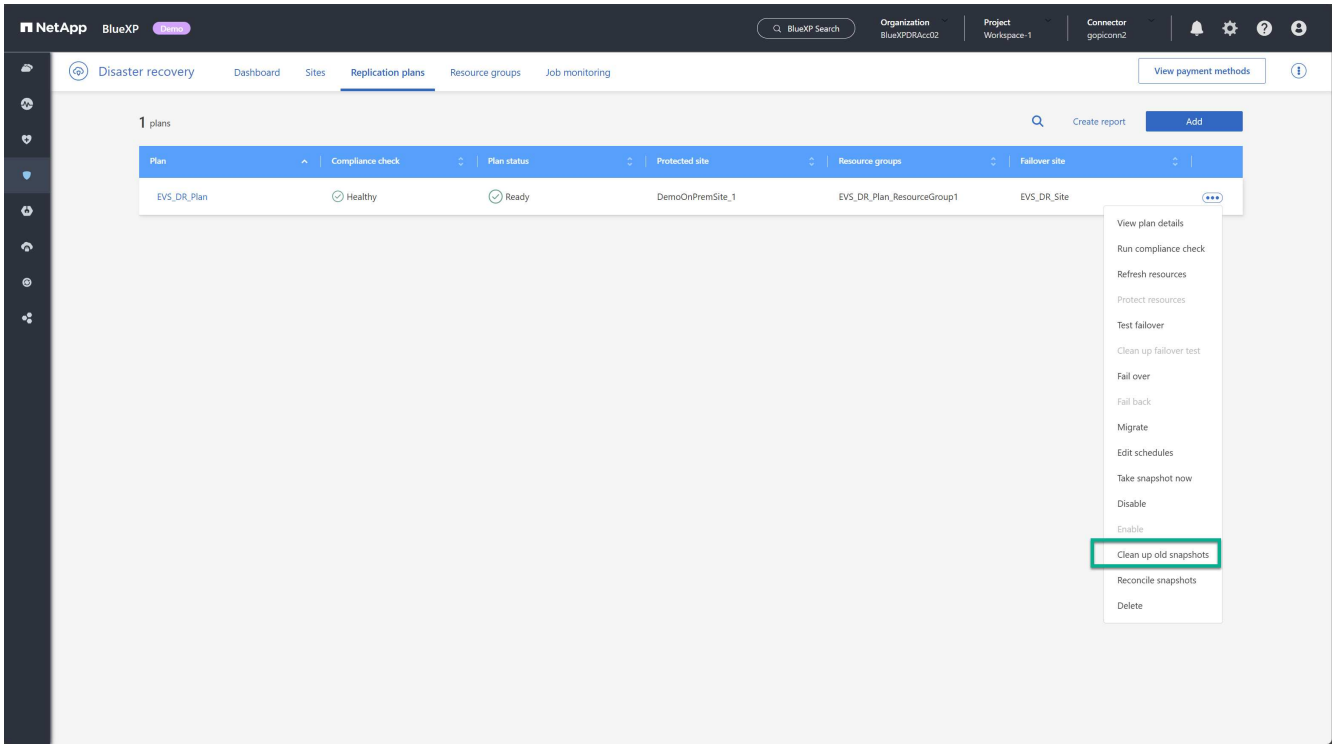
   Quando il piano di replica è attivo, il comando **Abilita** è disattivato. Quando il piano di replica è disattivato, il comando **Disabilita** è disattivato.



Pulire le vecchie istantanee

Potrebbe essere necessario ripulire gli snapshot più vecchi conservati sui siti di origine e di destinazione. Questo può accadere se il numero di snapshot conservati nel piano di replica viene modificato.

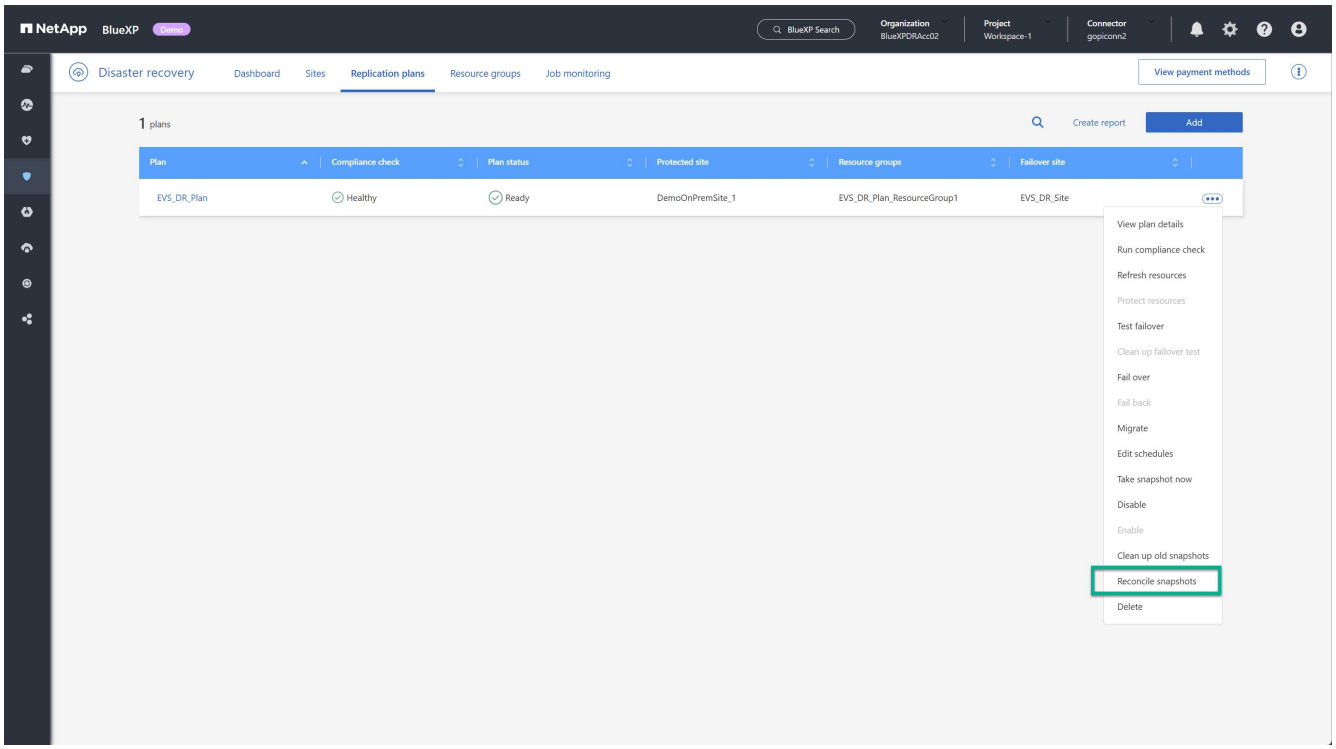
1. Seleziona l'opzione **Azioni** ••• accanto al piano di replicazione.
2. Per rimuovere manualmente questi vecchi snapshot, selezionare **Pulisci vecchi snapshot** dal menu Azioni del piano di replica.



Riconciliare le istantanee

Poiché il servizio orchestra gli snapshot dei volumi ONTAP, un amministratore dello storage ONTAP può eliminare direttamente gli snapshot utilizzando ONTAP System Manager, l'interfaccia a riga di comando ONTAP o le API REST di 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 funzione consente di garantire la coerenza delle istantanee in tutti i siti.

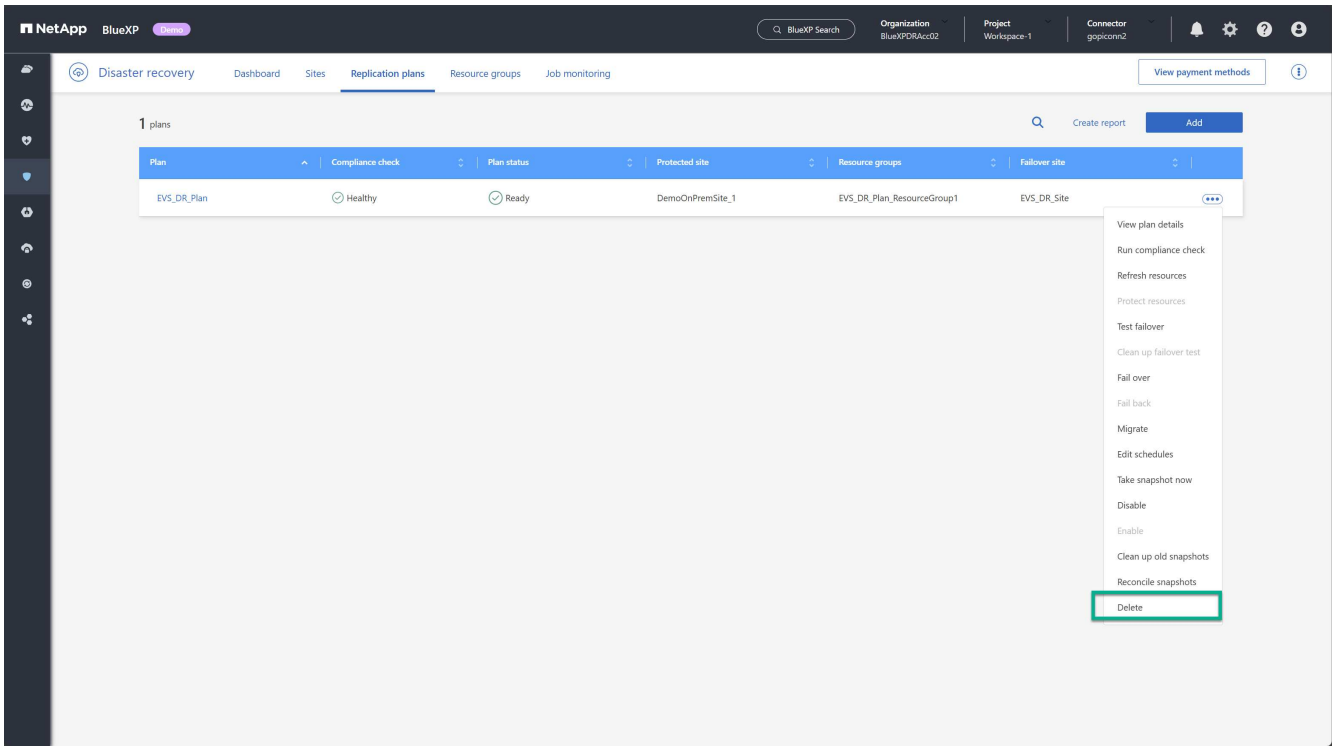
1. Seleziona l'opzione **Azioni** ••• accanto al piano di replicazione.
2. Per eliminare gli snapshot dal cluster di origine che non esistono nel cluster di destinazione, selezionare **Riconcilia snapshot** dal menu Azioni del piano di replica.



Elimina piano di replicazione

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

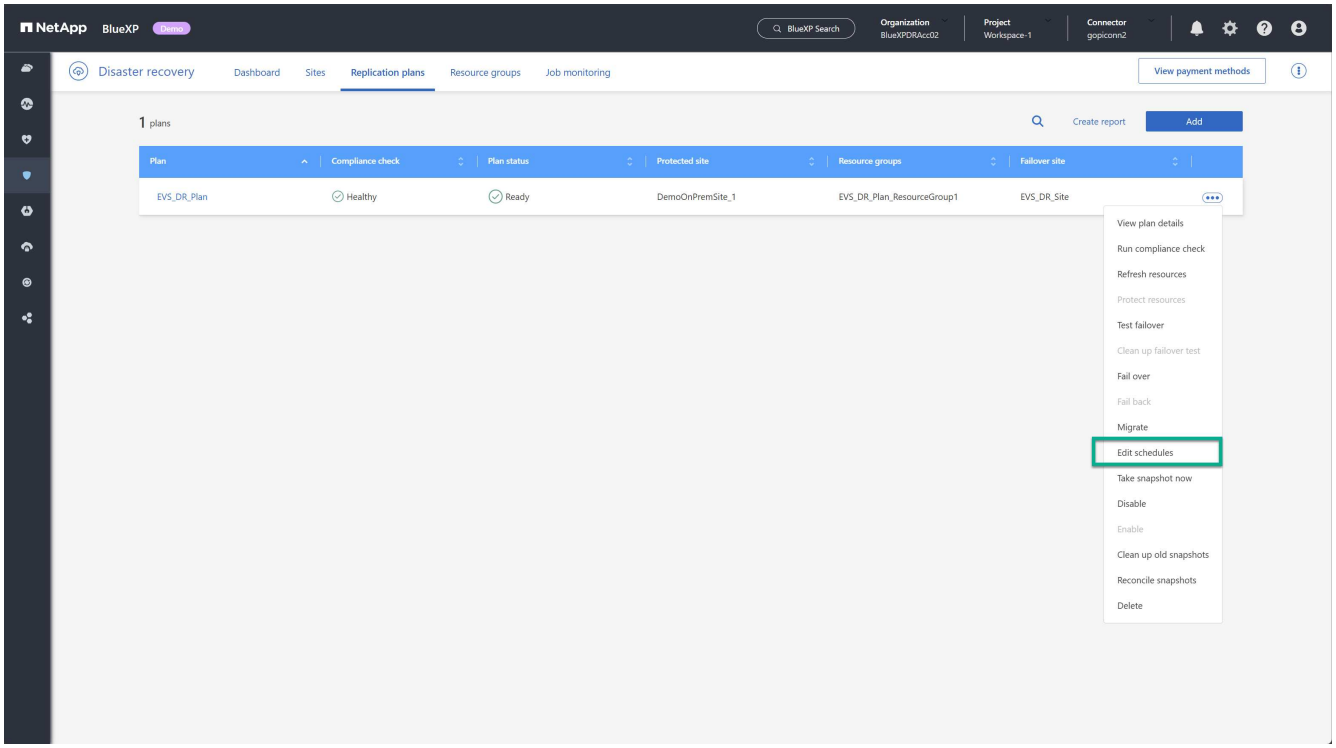
1. Seleziona l'opzione **Azioni** ••• accanto al piano di replicazione.
2. Per eliminare il piano di replicazione, selezionare **Elimina** dal menu contestuale del piano di replicazione.



Modificare le pianificazioni

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

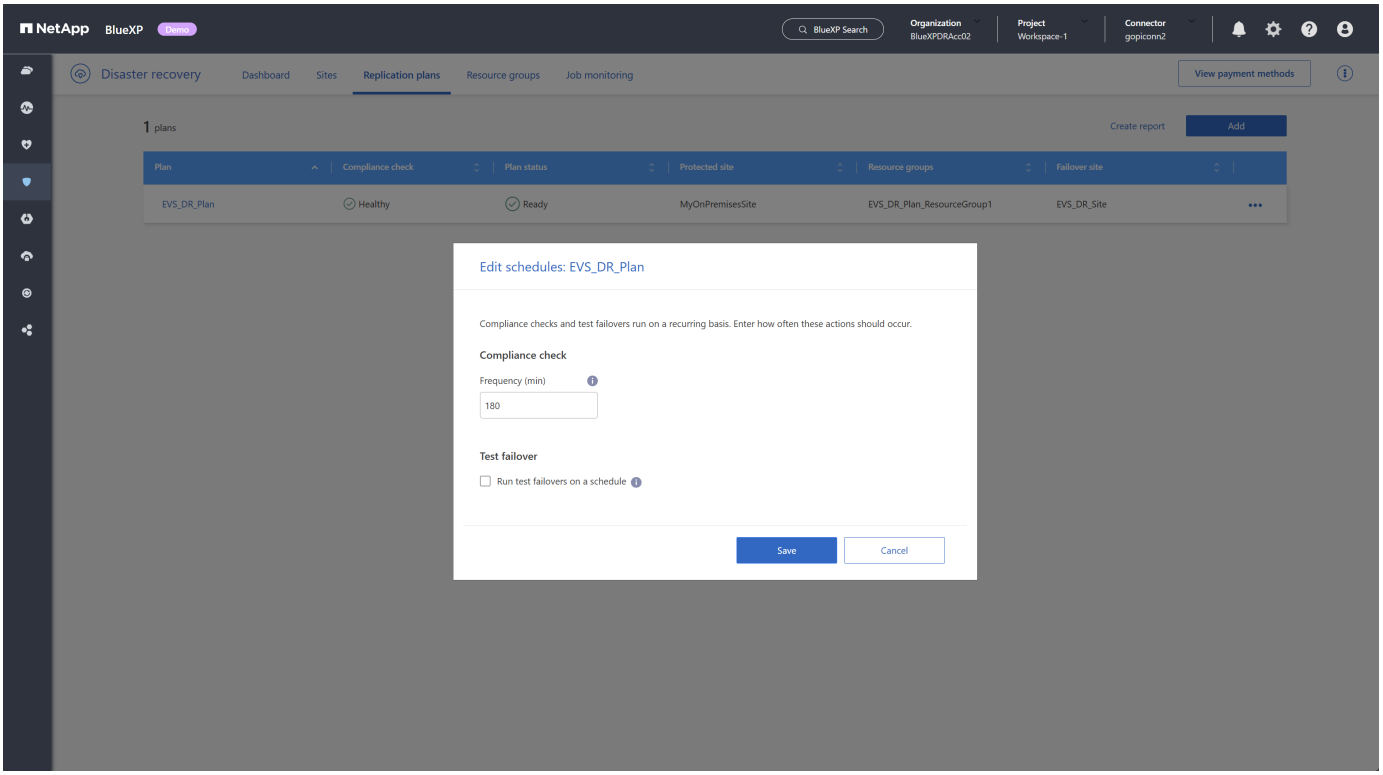
1. Seleziona l'opzione **Azioni** ••• accanto al piano di replicazione.
2. Per modificare le pianificazioni per una di queste due operazioni, selezionare **Modifica pianificazioni** per il piano di replica.



Modifica l'intervallo di controllo della conformità

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

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



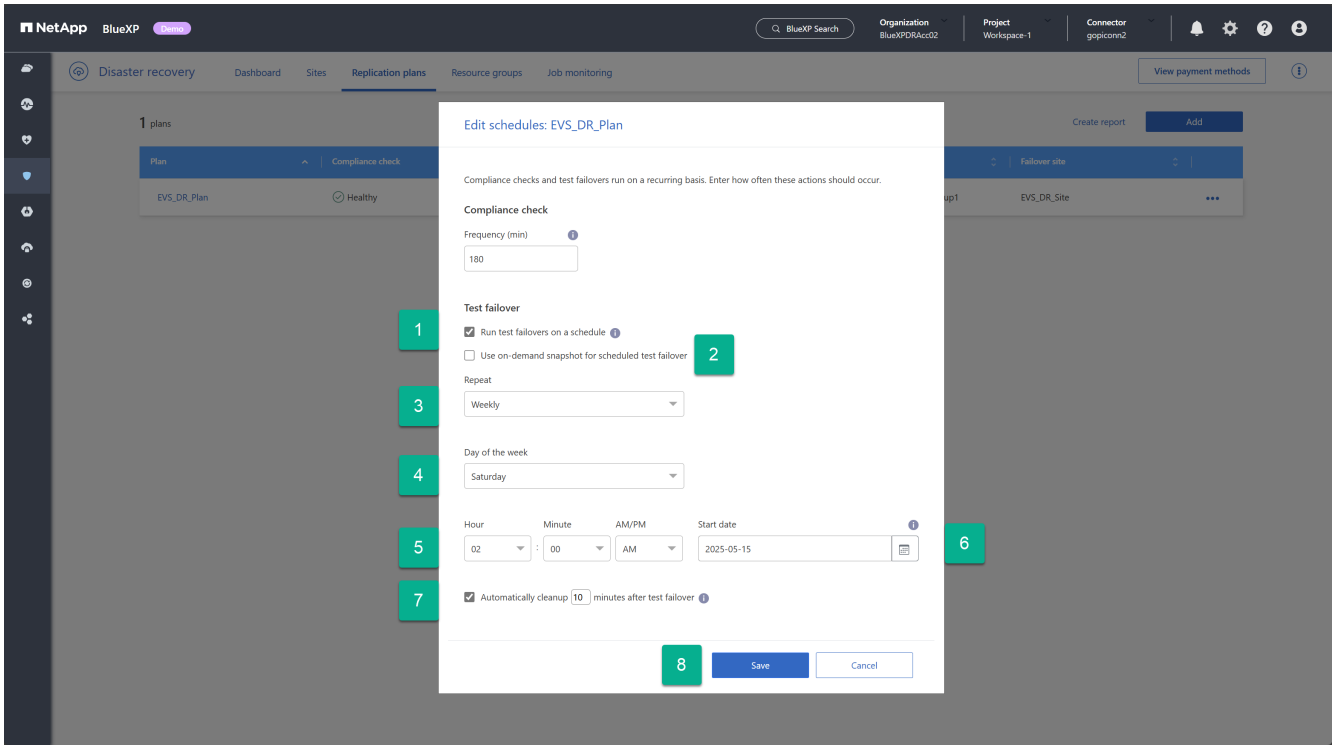
Pianificare failover di test automatizzati

I failover di test vengono eseguiti manualmente per impostazione predefinita. È possibile pianificare failover di test automatici, il che contribuisce a garantire che i piani di replica funzionino come previsto. Per ulteriori informazioni sul processo di failover di test, consultare "Verificare 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 **Utilizza 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 test di failover
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 sia in esecuzione prima che venga avviato il processo di pulizia.

10. Selezionare **Salva**.



Conoscenza e supporto

Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

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

Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione del numero di serie dell'account BlueXP (il numero di serie 960xxxxxxxx a 20 cifre si trova nella pagina risorse di supporto di BlueXP).

  Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

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

  Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

Registrare BlueXP per ricevere assistenza NetApp

Per registrarsi per ricevere assistenza e attivare i diritti di supporto, un utente dell'organizzazione (o account) BlueXP deve associare un account del sito di supporto NetApp al proprio login BlueXP . La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

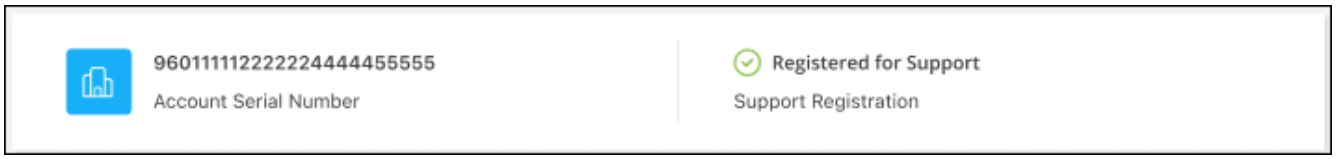
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

   La pagina **risorse** dovrebbe mostrare che l'organizzazione BlueXP è registrata per il supporto.



   Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che la tua organizzazione BlueXP non sia registrata per il supporto. Finché un utente dell'organizzazione ha seguito questi passaggi, l'organizzazione è stata registrata.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

Fasi

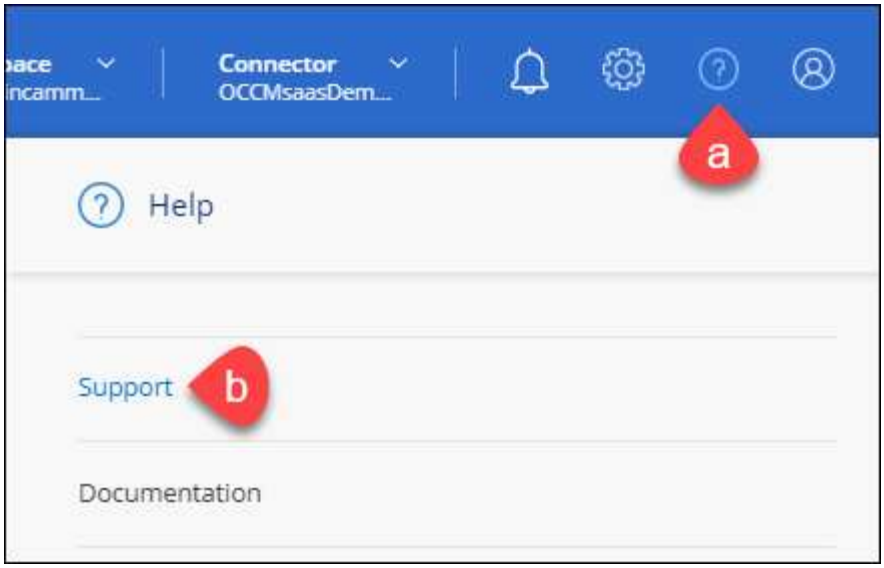
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto Cliente esistente con un account NSS.

Novità di NetApp

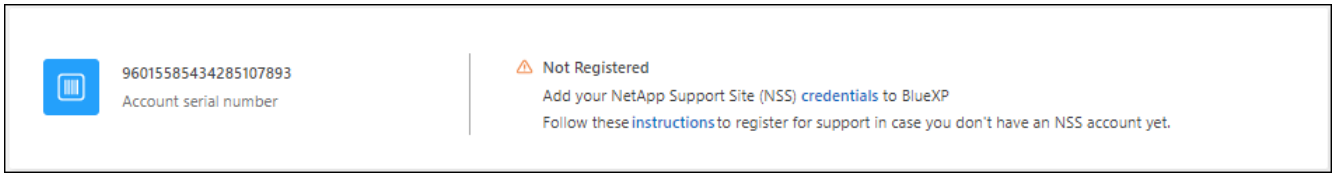
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare "Sito per la registrazione del supporto NetApp" E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

   Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

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

   La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

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

Al termine

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

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in Cliente esistente con un account NSS.

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

È necessario associare le credenziali del sito di supporto NetApp alla propria organizzazione BlueXP per abilitare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

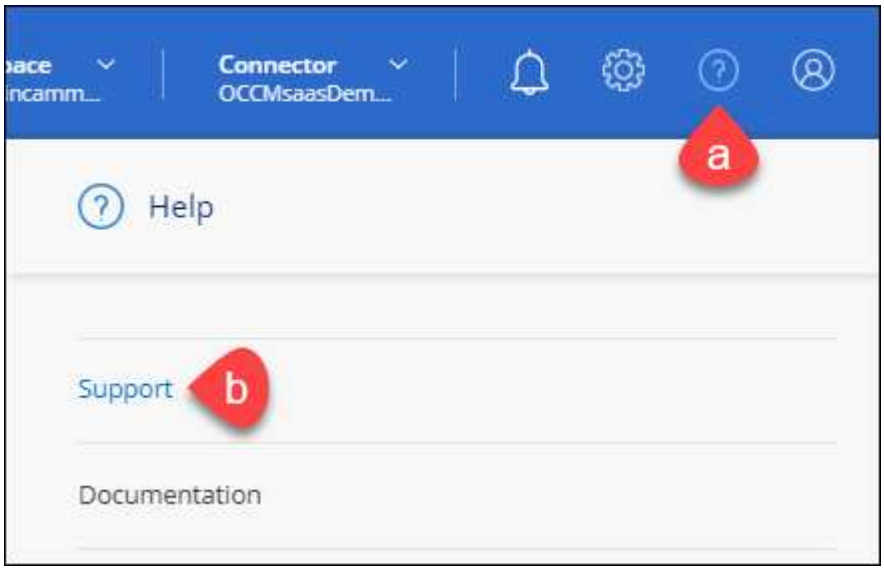
L'associazione delle credenziali NSS all'organizzazione BlueXP è diversa dall'account NSS associato a un accesso utente BlueXP .

Queste credenziali NSS sono associate all'ID organizzazione BlueXP specifico dell'utente. Gli utenti che appartengono all'organizzazione BlueXP possono accedere a queste credenziali da **supporto > Gestione NSS**.

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

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

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

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

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

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili ampie opzioni di supporto autonomo 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 file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

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

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

  Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- "Community"

  Unisciti alla community BlueXP 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 l'attivazione del supporto.

Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. "Scopri come gestire le credenziali associate all'accesso a BlueXP".
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:

   a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.

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

      - **Servizio**: Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
      - **Ambiente di lavoro**: Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

        L'elenco degli ambienti di lavoro rientra nell'ambito dell'organizzazione (o account), del progetto (o dell'area di lavoro) BlueXP e del connettore selezionato nell'intestazione superiore del servizio.

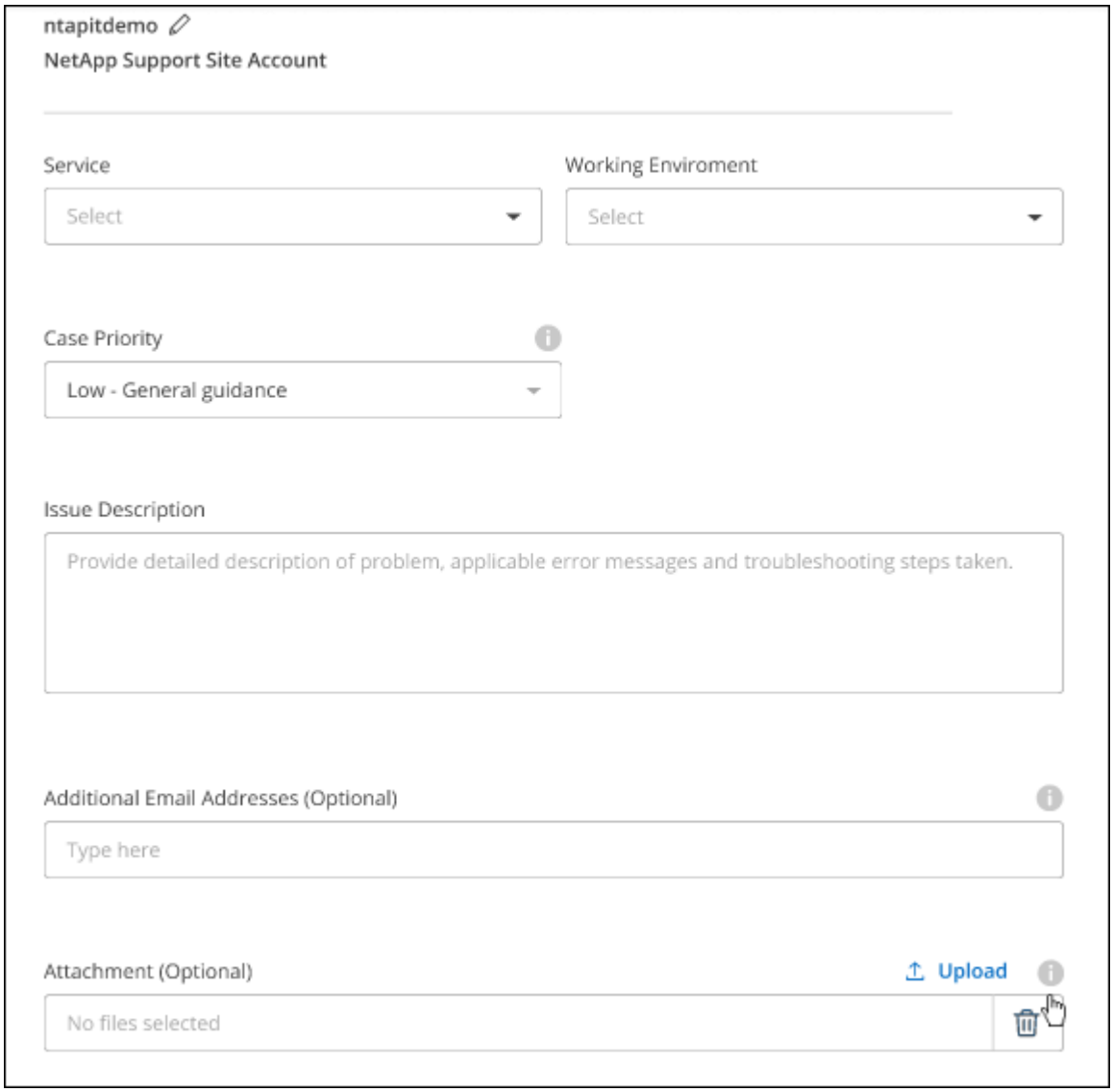
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.

      - **Descrizione del problema**: Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
      - **Indirizzi e-mail aggiuntivi**: Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale)**: 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.



Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare 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 per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo https://mysupport.netapp.com/site/help

Gestire i casi di supporto (anteprima)

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

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente 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 dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

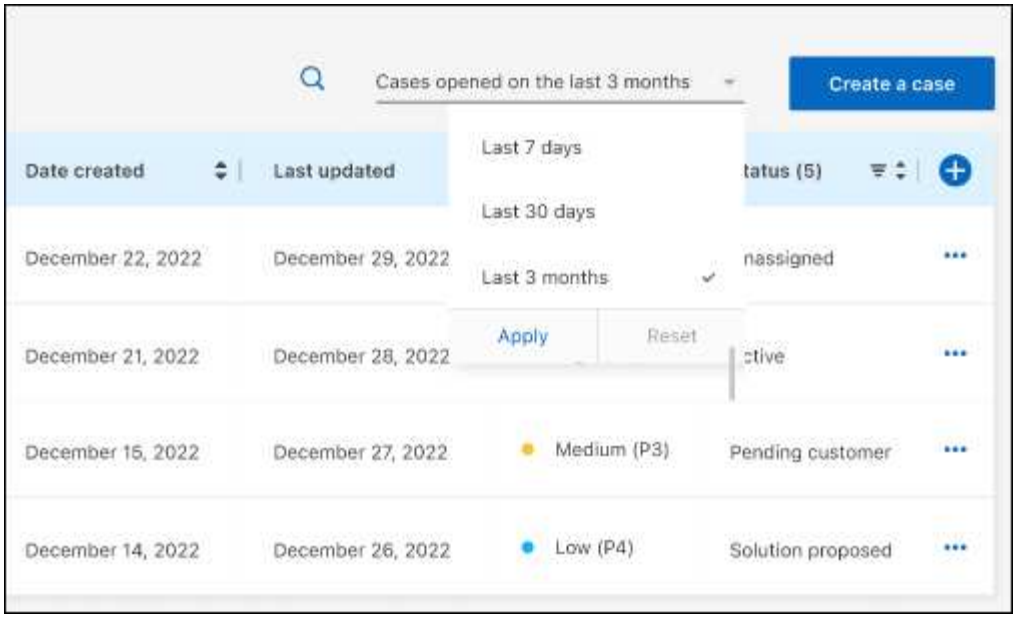
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  Per ulteriori informazioni, consulta la procedura riportata di seguito.
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

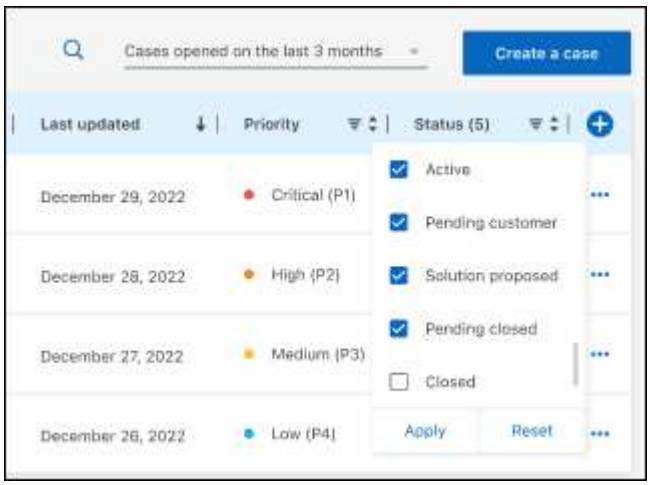
Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.

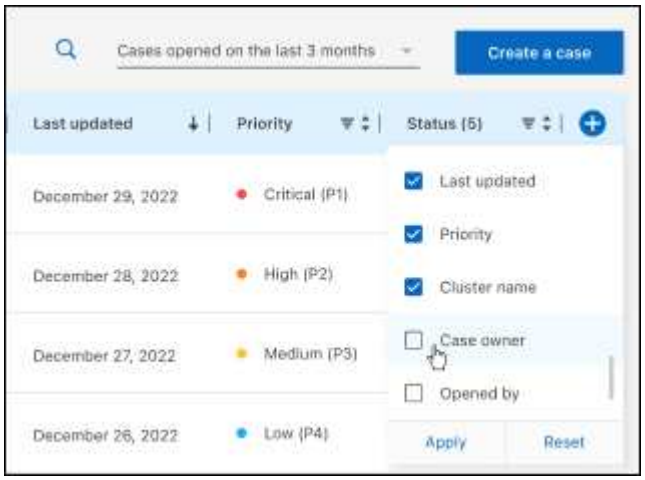
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
   - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.



- Modificare le colonne visualizzate nella tabella selezionando e quindi scegliere le colonne che si desidera visualizzare.

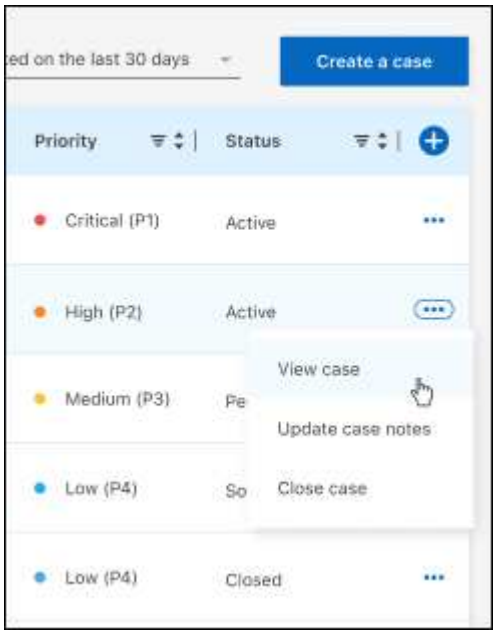


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

   - **Visualizza caso**: Visualizza tutti i dettagli relativi a un caso specifico.
   - **Aggiorna note sul caso**: Fornisci ulteriori dettagli sul problema oppure 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 l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

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

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero 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

Direttiva sulla privacy

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

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per il disaster recovery di BlueXP"