Utilizzare NetApp Disaster Recovery con Amazon EVS

NetApp Disaster Recovery

NetApp
February 04, 2026

Sommario

Utilizzare NetApp Disaster Recovery con Amazon EVS . . . 1
- Introduzione di NetApp Disaster Recovery tramite Amazon Elastic VMware Service e Amazon FSx for NetApp ONTAP . . . 1
- Panoramica della soluzione NetApp Disaster Recovery tramite Amazon EVS e Amazon FSs per NetApp ONTAP . . . 1
- Installa l'agente NetApp Console per NetApp Disaster Recovery . . . 2
  - Installazione . . . 3
- Configurare NetApp Disaster Recovery per Amazon EVS . . . 3
  - Panoramica sulla configurazione NetApp Disaster Recovery per Amazon EVS . . . 3
  - Prerequisiti per Amazon EVS con NetApp Disaster Recovery . . . 3
  - Aggiungi array locali al sistema NetApp Console per Amazon EVS con NetApp Disaster Recovery . . . 4
  - Aggiungi il servizio NetApp Disaster Recovery al tuo account NetApp Console per Amazon EVS . . . 5
  - Aggiungere siti in NetApp Disaster Recovery per Amazon EVS . . . 7
  - Aggiungi cluster locali e Amazon EVS vCenter in NetApp Disaster Recovery . . . 8
- Creare piani di replicazione per Amazon EVS . . . 9
  - Creazione di piani di replica nella panoramica NetApp Disaster Recovery . . . 9
  - Creare un piano di replica: Passaggio 1: selezionare vCenter in NetApp Disaster Recovery . . . 9
  - Creare un piano di replica: Passaggio 2: selezionare le risorse VM in NetApp Disaster Recovery . . . 9
  - Creare un piano di replicazione: Passaggio 3 - Mappare le risorse in NetApp Disaster Recovery . . . 10
  - Creare un piano di replica: Passaggio 4 - Verificare le impostazioni in NetApp Disaster Recovery . . . 14
  - Verificare che tutto funzioni in NetApp Disaster Recovery . . . 15
- Eseguire operazioni di piano di replica con NetApp Disaster Recovery . . . 15
  - Failover . . . 15
  - Failover di prova . . . 16
  - Eseguire un controllo di conformità . . . 16
  - Aggiorna le risorse . . . 17
  - Migrare . . . 17
  - Scatta un'istantanea ora . . . 17
  - Disabilita o abilita il piano di replicazione . . . 18
  - Pulisci i vecchi snapshot . . . 18
  - Riconciliare gli snapshot . . . 18
  - Elimina piano di replicazione . . . 18
  - Modificare gli orari . . . 19

Utilizzare NetApp Disaster Recovery con Amazon EVS

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

I clienti dipendono sempre più dalle infrastrutture virtualizzate per i carichi di lavoro di elaborazione di produzione, come quelle basate su VMware vSphere. Poiché queste macchine virtuali (VM) sono diventate sempre più critiche per le loro attività, i clienti devono proteggerle dagli stessi tipi di disastri a cui sono soggette le loro risorse di elaborazione fisiche. Le soluzioni di disaster recovery (DR) attualmente offerte sono complesse, costose e richiedono molte risorse. NetApp, il più grande fornitore di storage utilizzato per infrastrutture virtualizzate, ha un interesse personale nel garantire che le VM dei suoi clienti siano protette allo stesso modo in cui proteggiamo i dati ospitati nello storage ONTAP di qualsiasi tipo. Per raggiungere questo obiettivo, NetApp ha creato il servizio NetApp Disaster Recovery .

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

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

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

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

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

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

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

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

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

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

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

Installa l'agente NetApp Console per NetApp Disaster Recovery

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

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

Installazione

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

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

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

Configurare NetApp Disaster Recovery per Amazon EVS

Panoramica sulla configurazione NetApp Disaster Recovery per Amazon EVS

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

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

Prerequisiti per Amazon EVS con NetApp Disaster Recovery

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

Prerequisiti

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

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

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

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

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

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

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

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

Devi fare quanto segue:

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

Aggiungere array di storage locali al sistema NetApp Console

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

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

   [Aggiungi sistema]

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

   [Aggiungi immagine di sistema]

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

   [Aggiungi immagine di sistema]

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

   [Aggiungi immagine di sistema]

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

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

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

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

   [Aggiungi immagine di sistema]

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

   [Aggiungi immagine di sistema]

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

   [Aggiungi immagine di sistema]

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.

   [Aggiungi immagine di sistema]

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

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

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

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

Tipi di licenza

Esistono due tipi principali di licenza:

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

Dimensiona le tue esigenze di capacità di disaster recovery

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

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

Passi

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

   Per esempio:

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

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

Aggiungere siti in NetApp Disaster Recovery per Amazon EVS

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

Devi creare quanto segue:

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

Crea siti on-premise

Creare un sito vCenter di produzione.

Passi

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

   [Opzione siti]

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

   [Aggiungi opzione nell'opzione Siti]

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

   [Finestra di dialogo Crea sito]

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

Crea siti cloud Amazon

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

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

   [Opzione siti]

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

   [Aggiungi opzione nella pagina Siti]

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

   [Aggiungi finestra di dialogo]

Risultato

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

Aggiungi cluster locali e Amazon EVS vCenter in NetApp Disaster Recovery

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

Passaggi per aggiungere un vCenter a ciascun sito

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

   [Aggiungi l'opzione vCenter]

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

3. Selezionare **Aggiungi**.

   [Finestra di dialogo Aggiungi vCenter]

Creare piani di replicazione per Amazon EVS

Creazione di piani di replica nella panoramica NetApp Disaster Recovery

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

Per avviare il processo di creazione del piano di replicazione:

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

   [opzione piani di replicazione]

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

   [Schermata dei piani di replicazione]

Si apre la procedura guidata Crea piano di replica.

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

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

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

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

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

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

   [Crea un piano di replica, seleziona vCenter]

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

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

Selezionare le macchine virtuali da proteggere tramite NetApp Disaster Recovery.

Esistono diversi modi per selezionare le VM da proteggere:

- **Seleziona singole VM**: facendo clic sul pulsante **Macchine virtuali** è possibile selezionare le singole VM da proteggere. Quando selezioni ogni VM, il servizio la aggiunge a un gruppo di risorse predefinito situato sul lato destro dello schermo.
- **Seleziona gruppi di risorse creati in precedenza**: puoi creare gruppi di risorse personalizzati in anticipo utilizzando l'opzione Gruppo di risorse dal menu NetApp Disaster Recovery . Questo non è un requisito, poiché è possibile utilizzare gli altri due metodi per creare un gruppo di risorse come parte del processo del piano di replica. Per maggiori dettagli, vedere "Creare un piano di replicazione" .
- **Seleziona interi datastore vCenter**: se hai molte VM da proteggere con questo piano di replica, potrebbe non essere altrettanto efficiente selezionare singole VM. Poiché NetApp Disaster Recovery utilizza la replica SnapMirror basata sul volume per proteggere le VM, tutte le VM residenti in un datastore verranno replicate come parte del volume. Nella maggior parte dei casi, è necessario che NetApp Disaster Recovery protegga e riavvii tutte le VM presenti nel datastore. Utilizzare questa opzione per indicare al servizio di aggiungere all'elenco delle VM protette tutte le VM ospitate su un datastore selezionato.

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

Passaggi per accedere a questa pagina

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

   [Piano di replicazione, pagina Applicazioni]

Passaggi per selezionare il/i datastore/i:

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

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

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

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

È necessario mappare quattro tipi principali di informazioni:

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

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

- Le sezioni con l'icona di attenzione ([25,25]) richiedono di fornire informazioni sulla mappatura.
- La sezione contrassegnata con l'icona di spunta ([25,25]) sono stati mappati o hanno mappature predefinite. Esaminateli per assicurarvi che la configurazione attuale soddisfi i vostri requisiti.

Passaggi per accedere a questa pagina

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

   [Crea un piano di replicazione, pagina di mappatura delle risorse]

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

Mappatura delle risorse di calcolo

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

Passaggi per mappare le risorse di calcolo

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

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

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

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

   [Crea un piano di replicazione, calcola le risorse]

Mappare le risorse di rete virtuale

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

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

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

   [Creare un piano di replicazione, risorse di rete]

Definire le opzioni per la riconfigurazione della VM durante il failover

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

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

Riconfigurazione della rete

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

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

Dopo aver configurato le subnet, il mapping delle subnet utilizza lo stesso componente unità dell'indirizzo IP sia per la configurazione della VM di origine che di destinazione, ma sostituisce il componente subnet dell'indirizzo IP in base alle informazioni CIDR fornite. Questa funzionalità richiede inoltre che sia la rete virtuale di origine che quella di destinazione abbiano la stessa classe di indirizzo IP (la `/xx` componente del CIDR). Ciò garantisce che nel sito di destinazione siano disponibili indirizzi IP sufficienti per ospitare tutte le VM protette.

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

Apportare modifiche alla riconfigurazione delle impostazioni di rete

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

   [Creare un piano di replicazione, risorse di rete]

Riconfigurazione delle risorse di elaborazione della VM

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

Specificare eventuali modifiche alla configurazione della VM

1. (Facoltativo) Modificare il numero di CPU virtuali che ogni VM deve utilizzare. Questa operazione potrebbe essere necessaria se gli host del cluster vCenter DR non dispongono di tanti core CPU quanti ne ha il

cluster vCenter di origine.

2. (Facoltativo) Modificare la quantità di DRAM virtuale che ogni VM deve utilizzare. Questa operazione potrebbe essere necessaria se gli host del cluster vCenter DR non dispongono della stessa quantità di DRAM fisica degli host del cluster vCenter di origine.

   [Crea un piano di replicazione, risorse VM]

Ordine di avvio

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

Modificare le impostazioni dell'ordine di avvio

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

   [Crea piano di replicazione, ordine di avvio]

Operazioni personalizzate del sistema operativo guest

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

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

Modificare le operazioni personalizzate del sistema operativo guest di ogni VM

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

[Crea un piano di replicazione, operazioni personalizzate del sistema operativo guest]

Archivi dati cartografici

Il passaggio finale nella creazione di un piano di replicazione è identificare il modo in cui ONTAP dovrebbe

proteggere i datastore. Queste impostazioni definiscono l'obiettivo del punto di ripristino (RPO) dei piani di replica, quanti backup devono essere mantenuti e dove replicare i volumi ONTAP di hosting di ciascun datastore vCenter.

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

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

Per configurare la mappatura del datastore (volume)

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

   [Creare un piano di replicazione, mappatura del datastore]

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

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

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

Passi

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

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

   Revisione delle impostazioni del piano di replicazione[Revisione delle impostazioni del piano di replicazione]

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

Continua con"Verificare il piano di replicazione" .

Verificare che tutto funzioni in NetApp Disaster Recovery

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

Figura: Pagina dei piani di replicazione[Pagina dei piani di replicazione]

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

Nella pagina Piani di replicazione puoi vedere le seguenti informazioni:

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

Eseguire operazioni di piano di replica con NetApp Disaster Recovery

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

Failover

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

Il failover è un processo avviato manualmente.

Passaggi per accedere all'operazione di failover

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

Passaggi per eseguire un failover

1. Dalla pagina Piani di replica, seleziona l'opzione Azioni del piano di replica[Punti orizzontali per il menu Azioni] .
2. Selezionare **Fail over**.

   [Opzione di menu Failover]

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

   [Finestra di dialogo Failover]

Failover di prova

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

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

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

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

Passi

1. Selezionare l'opzione Azioni del piano di replicazione[Punti orizzontali per il menu Azioni] .
2. Selezionare **Test failover** dal menu.

   [Opzione di menu di failover di prova]

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**.

   [Finestra di dialogo di failover di prova]

Eseguire un controllo di conformità

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

Passi

1. Seleziona l'opzione *Azioni*[Icona del menu Azioni nel servizio NetApp Disaster Recovery] accanto al piano di replicazione.

2. Selezionare l'opzione **Esegui controllo di conformità** dal menu Azioni del piano di replicazione:

   [Opzione di menu Esegui controllo conformità]

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

Aggiorna le risorse

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

Ci sono due casi in cui è necessario un aggiornamento:

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

[Opzione di menu Aggiorna risorse] | *evs-rp-menu-refresh-resources.png*

Migrare

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

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

   [Opzione di menu Migra] | *evs-rp-menu-migrate.png*

3. Immettere le informazioni nella finestra di dialogo Migra.

Scatta un'istantanea ora

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

1. Seleziona l'opzione *Azioni*[Icona del menu Azioni nel servizio NetApp Disaster Recovery] 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:

   [Opzione di menu "Scatta istantanea ora"] | *evs-rp-menu-take-snapshot-now.png*

Disabilita o abilita il piano di replicazione

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

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

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

   [Opzione di menu Disabilita/Abilita] | *evs-rp-menu-disable-enable.png*

Pulisci i vecchi snapshot

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

1. Seleziona l'opzione *Azioni*[Icona del menu Azioni nel servizio NetApp Disaster Recovery] accanto al piano di replicazione.
2. Per rimuovere manualmente questi snapshot più vecchi, selezionare **Pulisci snapshot vecchi** dal menu Azioni del piano di replica.

   [Opzione di menu Pulisci vecchi snapshot] | *evs-rp-menu-cleanup-old-snapshots.png*

Riconciliare gli snapshot

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

1. Seleziona l'opzione *Azioni*[Icona del menu Azioni nel servizio NetApp Disaster Recovery] 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.

   [Opzione di menu Riconcilia snapshot] | *evs-rp-menu-reconcile-snapshots.png*

Elimina piano di replicazione

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

1. Seleziona l'opzione *Azioni*[Icona del menu Azioni nel servizio NetApp Disaster Recovery] accanto al piano di replicazione.
2. Per eliminare il piano di replicazione, selezionare **Elimina** dal menu contestuale del piano di replicazione.

   [Elimina l'opzione del menu] | *evs-rp-menu-delete.png*

Modificare gli orari

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

1. Seleziona l'opzione *Azioni*[Icona del menu Azioni nel servizio NetApp Disaster Recovery] accanto al piano di replicazione.
2. Per modificare queste pianificazioni per una di queste due operazioni, selezionare **Modifica pianificazioni** per il piano di replica.

   [Opzione di menu Modifica pianificazioni] | *evs-rp-menu-edit-schedules.png*

Modifica l'intervallo di controllo della conformità

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

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

[Programma di controllo della conformità] | *evs-rp-edit-compliance-check-schedule.png*

Pianificare failover di test automatizzati

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

Passaggi per pianificare i failover dei test

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

    [Modifica la pianificazione del failover del test] | *evs-rp-edit-schedule-test-failover.png*

Informazioni sul copyright

Informazioni sul marchio commerciale