



Backup e recovery di BlueXP per le VM

NetApp Solutions

NetApp
April 26, 2024

Sommario

Backup e recovery di BlueXP per le VM 1

 Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM..... 1

Backup e recovery di BlueXP per le VM

Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM

Autore: Josh Powell - NetApp Solutions Engineering

Panoramica

La strategia di backup 3-2-1 è un metodo di protezione dei dati accettato dal settore, che offre un approccio completo alla protezione dei dati importanti. Questa strategia è affidabile e garantisce che, anche in caso di incidenti imprevisti, vi sia ancora una copia dei dati disponibili.

La strategia si articola in tre regole fondamentali:

1. Conservare almeno tre copie dei dati. In questo modo, anche se una copia viene smarrita o danneggiata, sono ancora disponibili almeno due copie rimanenti.
2. Memorizzare due copie di backup su diversi supporti o dispositivi di archiviazione. La diversificazione dei supporti storage contribuisce a proteggerli da guasti specifici dei dispositivi o dei supporti. Se un dispositivo viene danneggiato o un tipo di supporto si guasta, l'altra copia di backup rimane inalterata.
3. Infine, assicurarsi che almeno una copia di backup sia fuori sede. Lo storage offsite serve come protezione contro i disastri localizzati, come incendi o inondazioni, che potrebbero rendere le copie on-site inutilizzabili.

Questo documento di soluzione descrive una soluzione di backup 3-2-1 che utilizza il plug-in SnapCenter per VMware vSphere (SCV) per creare backup primari e secondari delle nostre macchine virtuali on-premise e backup e recovery BlueXP per le macchine virtuali per effettuare il backup di una copia dei nostri dati su cloud storage o StorageGRID.





Casi di utilizzo

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup e ripristino di macchine virtuali e datastore on-premise utilizzando il plug-in SnapCenter per VMware vSphere.
- Backup e ripristino di macchine virtuali e datastore on-premise, in hosting su cluster ONTAP e backup su storage a oggetti utilizzando backup e recovery di BlueXP per le macchine virtuali.

Storage NetApp ONTAP

ONTAP è la soluzione di storage leader del settore di NetApp che offre storage unificato con accesso a protocolli SAN o NAS. La strategia di backup 3-2-1 garantisce la protezione dei dati on-premise su più tipi di supporto, mentre NetApp offre piattaforme che vanno da flash ad alta velocità a supporti a costi inferiori.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
			
Hybrid flash storage	Capacity all-flash storage	Performance all-flash storage	All-flash SAN storage
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency	Refresh of hybrid flash, Tier 1 @ 2-4ms latency	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed
Backup / Low-cost DR	Tier 2 workloads VMware datastores		

Per ulteriori informazioni su tutti i prodotti hardware della piattaforma NetApp, consulta l'articolo ["Storage NetApp"](#).

Plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter per VMware vSphere è un'offerta di protezione dei dati strettamente integrata con VMware vSphere e consente una facile gestione di backup e ripristini per le macchine virtuali. Come parte di questa soluzione, SnapMirror fornisce un metodo rapido e affidabile per creare una seconda copia di backup immutabile dei dati della macchina virtuale su un cluster di storage ONTAP secondario. Con questa architettura implementata, le operazioni di ripristino delle macchine virtuali possono essere avviate facilmente da posizioni di backup primarie o secondarie.

SCV viene installato come appliance virtuale linux utilizzando un file OVA. Il plug-in ora utilizza un plug-in remoto architettura. Il plug-in remoto viene eseguito al di fuori del server vCenter e viene ospitato sull'appliance virtuale SCV.

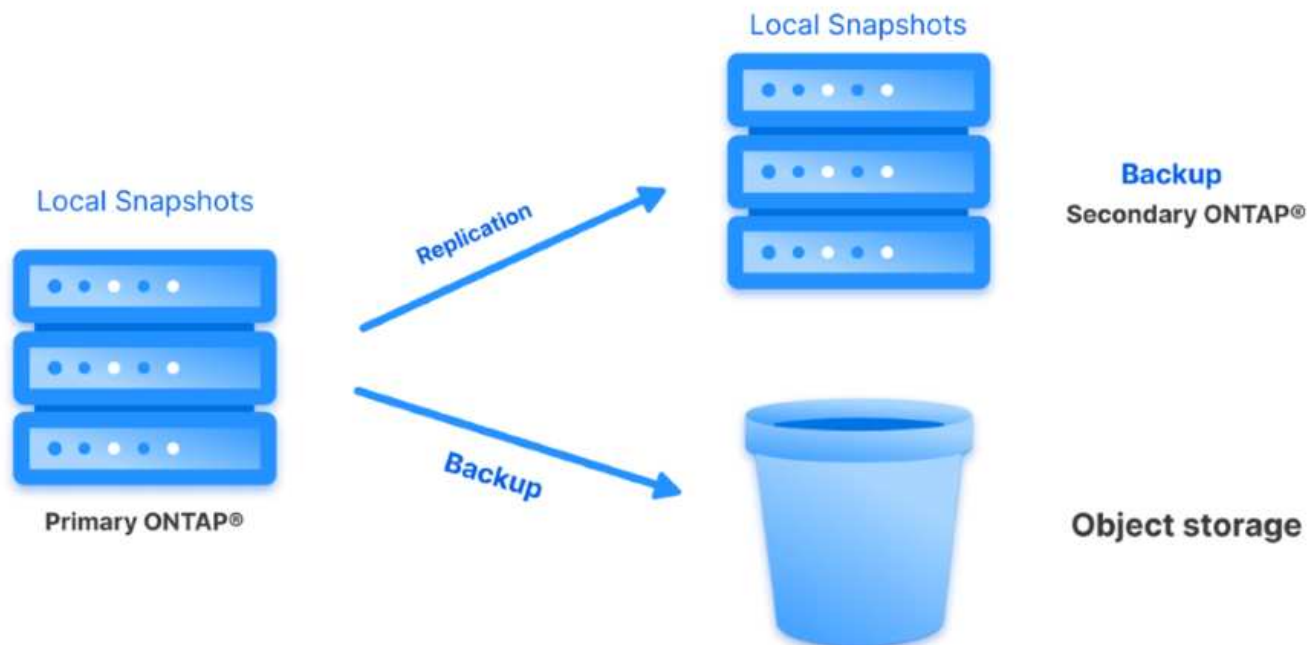
Per informazioni dettagliate sul distributore idraulico, fare riferimento a ["Plug-in SnapCenter per la documentazione di VMware vSphere"](#).

Backup e recovery di BlueXP per le macchine virtuali

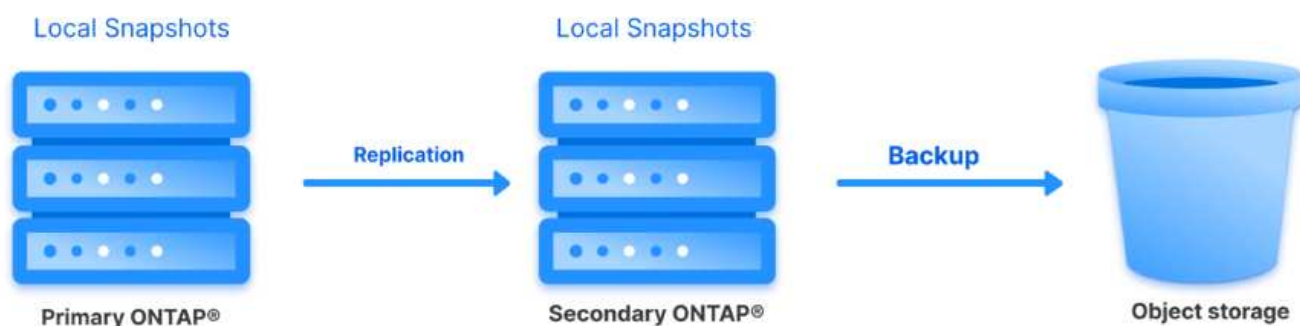
Il backup e recovery di BlueXP è uno strumento basato su cloud per la gestione dei dati che offre un singolo pannello di controllo per un'ampia gamma di operazioni di backup e recovery negli ambienti on-premise e cloud. Parte della suite di backup e recovery BlueXP di NetApp è una funzionalità che si integra con il plug-in SnapCenter per VMware vSphere (on-premise) per estendere una copia dei dati allo storage a oggetti nel cloud. In questo modo viene stabilita una terza copia dei dati fuori sede che provengono dai backup dello storage primario o secondario. Il backup e recovery di BlueXP semplifica la configurazione di policy dello storage che trasferiscono le copie dei dati da una di queste due posizioni on-premise.

La scelta tra backup primari e secondari come origine in BlueXP Backup and Recovery comporterà l'implementazione di una delle due topologie:

Topologia fan-out – quando un backup viene avviato dal plug-in SnapCenter per VMware vSphere, viene immediatamente creata una snapshot locale. SCV avvia quindi un'operazione SnapMirror che replica lo snapshot più recente nel cluster ONTAP secondario. In BlueXP Backup and Recovery, una policy specifica il cluster ONTAP primario come origine di una copia Snapshot dei dati da trasferire nello storage a oggetti nel cloud provider scelto.



Topologia a cascata – la creazione delle copie dei dati primari e secondari mediante SCV è identica alla topologia fan-out menzionata in precedenza. Tuttavia, questa volta viene creata una policy in BlueXP Backup and Recovery che specifica che il backup nello storage a oggetti avrà origine dal cluster ONTAP secondario.



Il backup e recovery di BlueXP può creare copie di backup degli snapshot ONTAP on-premise nello storage AWS Glacier, Azure Blob e GCP Archive.



AWS Glacier and Deep Glacier



Azure Blob Archive



GCP Archive Storage

Inoltre, puoi utilizzare NetApp StorageGRID come destinazione del backup dello storage a oggetti. Per ulteriori informazioni su StorageGRID, fare riferimento alla ["Landing page di StorageGRID"](#).

Panoramica sull'implementazione della soluzione

Questo elenco fornisce i passaggi di alto livello necessari per configurare questa soluzione ed eseguire operazioni di backup e ripristino da SCV e BlueXP - Backup e ripristino:

1. Configurare la relazione SnapMirror tra i cluster ONTAP da utilizzare per le copie di dati primarie e secondarie.
2. Configura il plug-in SnapCenter per VMware vSphere.
 - a. Aggiunta di sistemi storage
 - b. Creare policy di backup
 - c. Creare gruppi di risorse
 - d. Eseguire i primi processi di backup
3. Configura backup e recovery di BlueXP per le macchine virtuali
 - a. Aggiungi ambiente di lavoro
 - b. Scopri le appliance SCV e vCenter
 - c. Creare policy di backup
 - d. Attivare i backup
4. Ripristinare le macchine virtuali dallo storage primario e secondario utilizzando SCV.
5. Ripristina le macchine virtuali dallo storage a oggetti utilizzando il backup e ripristino di BlueXP.

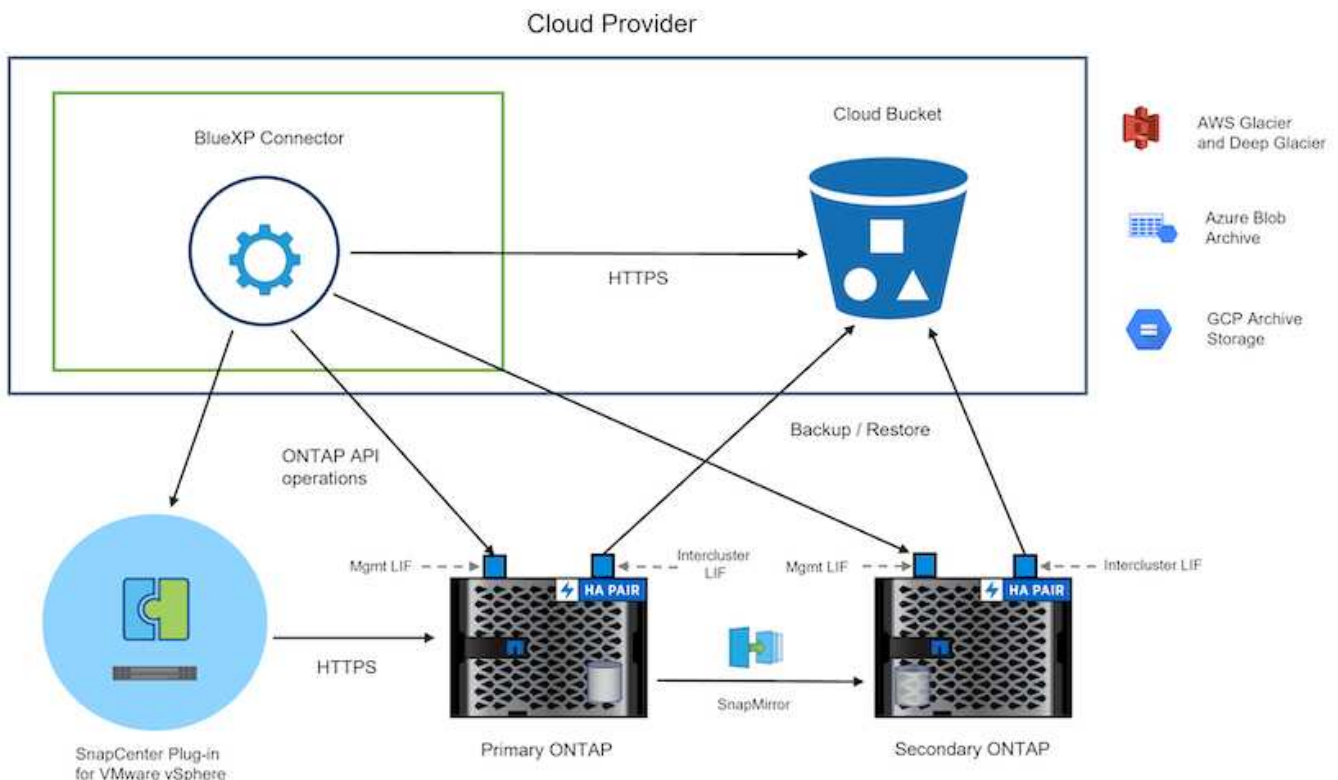
Prerequisiti

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware vSphere e situate negli archivi dati NFS ospitati da NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano configurati e pronti per l'uso:

1. Cluster di storage ONTAP con datastore NFS o VMFS connessi a VMware vSphere. Sono supportati datastore NFS e VMFS. Per questa soluzione sono stati utilizzati datastore NFS.
2. Cluster di storage ONTAP secondario con relazioni SnapMirror stabilite per volumi usati per datastore NFS.
3. Connettore BlueXP installato per il cloud provider utilizzato per i backup dello storage a oggetti.
4. Le macchine virtuali di cui eseguire il backup si trovano su datastore NFS che si trovano sul cluster di storage ONTAP primario.
5. Connettività di rete tra il connettore BlueXP e le interfacce di gestione del cluster di storage ONTAP on-premise.
6. Connettività di rete tra il connettore BlueXP e la macchina virtuale di un'appliance SCV on-premise e tra il connettore BlueXP e vCenter.
7. Connettività di rete tra le LIF ONTAP on-premise e il servizio di storage a oggetti.
8. DNS configurato per l'SVM di gestione su cluster di storage ONTAP primari e secondari. Per ulteriori informazioni, fare riferimento a. ["Configurare il DNS per la risoluzione del nome host"](#).

Architettura di alto livello

Il test/convalida di questa soluzione è stato eseguito in un laboratorio che potrebbe corrispondere o meno all'ambiente di implementazione finale.



Implementazione della soluzione

Questa soluzione fornisce istruzioni dettagliate per l'implementazione e la convalida di una soluzione che utilizza il plug-in SnapCenter per VMware vSphere, oltre al backup e al recovery di BlueXP, per eseguire backup e recovery di macchine virtuali Windows e Linux all'interno di un cluster VMware vSphere situato in un data center on-premise. Le macchine virtuali di questo setup sono memorizzate su datastore NFS ospitati da un cluster di storage ONTAP A300. Inoltre, un cluster di storage ONTAP A300 separato funge da destinazione secondaria per i volumi replicati mediante SnapMirror. Inoltre, lo storage a oggetti ospitato su Amazon Web Services e Azure Blob è stato utilizzato come destinazione per una terza copia dei dati.

Ci occuperemo della creazione di relazioni SnapMirror per copie secondarie dei nostri backup gestiti da SCV e della configurazione dei lavori di backup nel backup e ripristino di SCV e BlueXP.

Per informazioni dettagliate sul plug-in SnapCenter per VMware vSphere, consultare la ["Plug-in SnapCenter per la documentazione di VMware vSphere"](#).

Per informazioni dettagliate sul backup e recovery di BlueXP, consulta la ["Documentazione di backup e ripristino BlueXP"](#).

Stabilire relazioni di SnapMirror tra cluster ONTAP

Il plug-in SnapCenter per VMware vSphere utilizza la tecnologia ONTAP SnapMirror per gestire il trasporto delle copie SnapMirror e/o SnapVault secondarie in un cluster ONTAP secondario.

Le policy di backup dei distributori idraulici possono utilizzare relazioni SnapMirror o SnapVault. La differenza principale consiste nel fatto che quando si utilizza l'opzione SnapMirror, la pianificazione della conservazione configurata per i backup nella policy sarà la stessa nelle posizioni principale e secondaria. SnapVault è progettato per l'archiviazione e, quando si utilizza questa opzione, è possibile stabilire una pianificazione della conservazione separata con la relazione di SnapMirror per le copie Snapshot sul cluster di storage ONTAP secondario.

La configurazione delle relazioni di SnapMirror può essere effettuata in BlueXP, dove molti dei passaggi sono automatizzati, o può essere fatta con System Manager e l'interfaccia a riga di comando di ONTAP. Tutti questi metodi sono discussi di seguito.

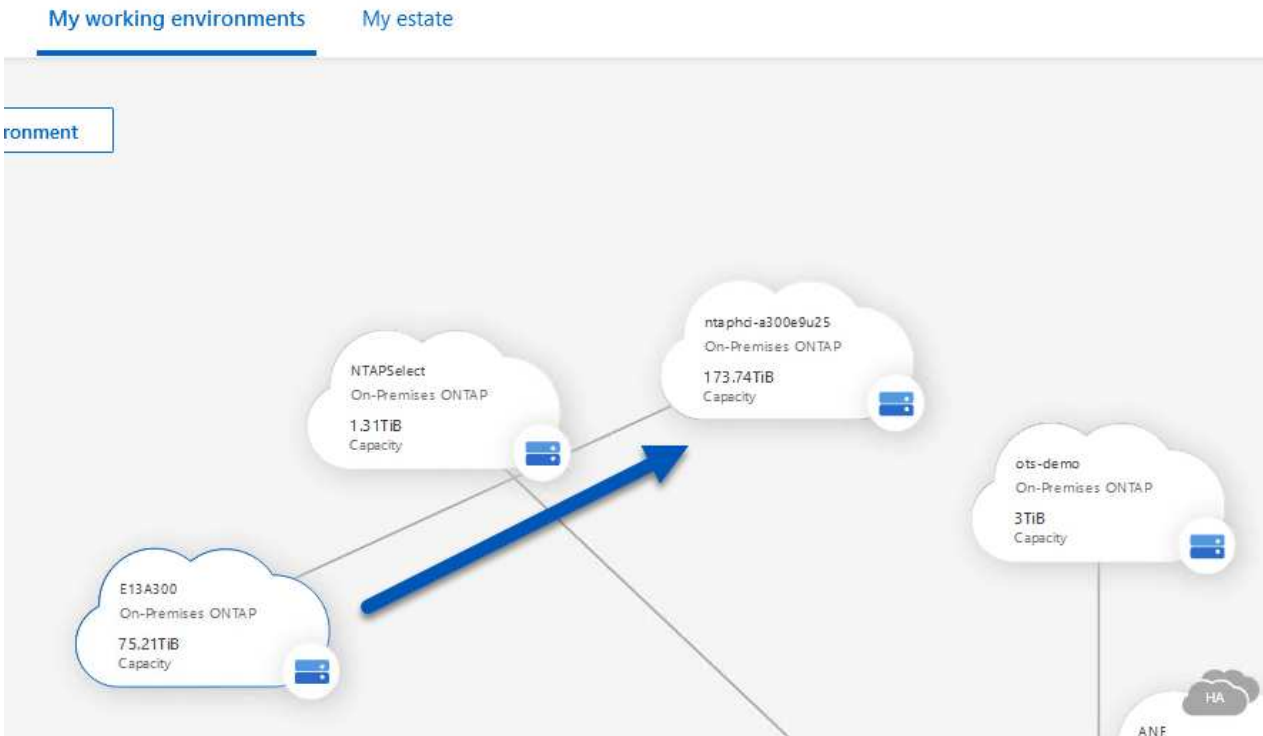
Stabilisci relazioni di SnapMirror con BlueXP

Dalla console web BlueXP devi completare i seguenti passaggi:

Configurazione della replica per sistemi di storage ONTAP primari e secondari

Iniziare accedendo alla console web BlueXP e navigando in Canvas.

1. Trascinare e rilasciare il sistema di storage ONTAP di origine (primario) nel sistema di storage ONTAP di destinazione (secondario).



2. Dal menu visualizzato, selezionare **Replica**.



3. Nella pagina **impostazione peering di destinazione**, selezionare le LIF Intercluster di destinazione da utilizzare per la connessione tra sistemi storage.

Select the destination LIFs you would like to use for cluster peering setup.
Replication requires an initial connection between the two working environments which is called a cluster peer relationship.
For more information about LIF selections, see Cloud Manager documentation.





<input type="checkbox"/> CVO_InterCluster_B ntaphci-a300-02 : a0a-3510 172.21.254.212/24 up	<input type="checkbox"/> CVO_InterCluster_A ntaphci-a300-01 : a0a-3510 172.21.254.211/24 up	<input type="checkbox"/> zoneb-n1 ntaphci-a300-01 : a0a-3484 172.21.228.21/24 up	<input type="checkbox"/> zoneb-n2 ntaphci-a300-02 : a0a-3484 172.21.228.22/24 up	<input checked="" type="checkbox"/> intercluster_node_1 ntaphci-a300-01 : a0a-181 10.61.181.193/24 up	<input checked="" type="checkbox"/> intercluster_node_2 ntaphci-a300-01 : a0a-181 10.61.181.194/24 up
--	--	---	---	---	---

4. Nella pagina **Destination Volume Name** (Nome volume di destinazione), selezionare innanzitutto il volume di origine, quindi compilare il nome del volume di destinazione e selezionare la SVM e l'aggregato di destinazione. Fare clic su **Avanti** per continuare.

Select the volume that you want to replicate

E13A300

288 Volumes

 CDM01 ONLINE INFO Storage VM Name: FS02 Tiering Policy: None Volume Type: RW CAPACITY 206 GB Allocated 53.72 MB Disk Used	 Data ONLINE INFO Storage VM Name: FS02 Tiering Policy: None Volume Type: RW CAPACITY 512 GB Allocated 0 GB Disk Used
 Demo ONLINE INFO Storage VM Name: zonea Tiering Policy: None Volume Type: RW CAPACITY 250 GB Allocated 1.79 GB Disk Used	 Demo02_01 ONLINE INFO Storage VM Name: Demo Tiering Policy: None Volume Type: RW CAPACITY 500 GB Allocated 34.75 MB Disk Used

Destination Volume Name

Destination Volume Name

Demo_copy

Destination Storage VM

EHC_NFS

Destination Aggregate

EHCaggr01

5. Scegliere la velocità di trasferimento massima alla quale eseguire la replica.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.


- ☒ Limited to: MB/s
- ☐ Unlimited (recommended for DR only machines)

6. Scegliere il criterio che determinerà il programma di conservazione per i backup secondari. Questo criterio può essere creato in anticipo (vedere il processo manuale riportato di seguito nel passaggio **Crea un criterio di conservazione snapshot**) o può essere modificato in seguito, se lo si desidera.

[↑ Previous Step](#)


Default Policies

Additional Policies


 CloudBackupService-1674046623282

Original Policy Name: CloudBackupService-1674046623282

Creates a SnapVault relationship which replicates Snapshot copies with the following labels to the destination volume:
hourly (12), daily (15), weekly (4)
(# of retained Snapshot copies in parenthesis)

 CloudBackupService-1674047424679

Custom Policy - No Comment

[More info](#)
 CloudBackupService-1674047718637

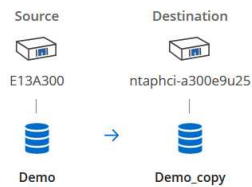
Custom Policy - No Comment

[More info](#)

7. Infine, esaminare tutte le informazioni e fare clic sul pulsante **Go** (Vai) per avviare il processo di configurazione della replica.

[↑ Previous Step](#)

Review your selection and start the replication process



Source Volume Allocated Size: 250 GB

Source Volume Used Size: 1.79 GB

Source Thin Provisioning: Yes

Destination Volume Allocated Size: 250 GB

Destination Thin Provisioning: No

Destination Aggregate: EHCaggr01

Destination Storage VM: EHC_NFS

Max Transfer Rate: 100 MB/s

SnapMirror Policy: Mirror

Replication Schedule: One-time copy

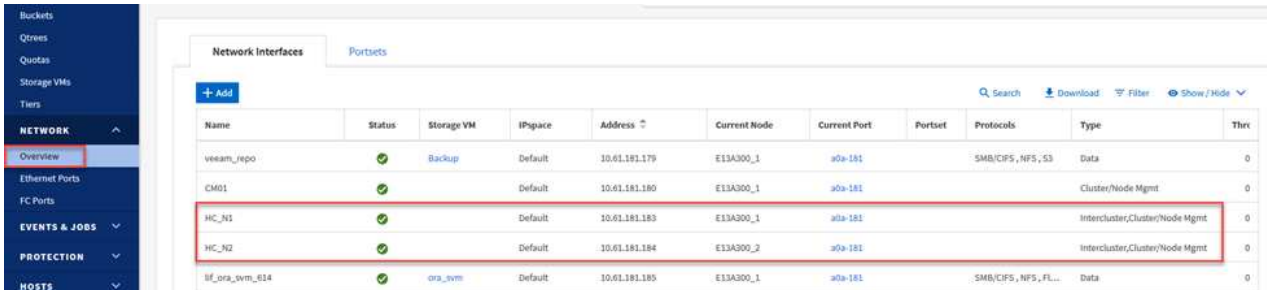
Stabilire relazioni di SnapMirror con System Manager e la CLI di ONTAP

Tutti i passaggi necessari per stabilire le relazioni SnapMirror possono essere eseguiti con System Manager o la CLI di ONTAP. La sezione seguente fornisce informazioni dettagliate su entrambi i metodi:

Registrare le interfacce logiche Intercluster di origine e destinazione

Per i cluster ONTAP di origine e di destinazione, puoi recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

1. In Gestore di sistema di ONTAP, accedere alla pagina Panoramica di rete e recuperare gli indirizzi IP di tipo: Intercluster configurati per comunicare con il VPC di AWS su cui è installato FSX.



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thr
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster, Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster, Cluster/Node Mgmt	0
bf_ora_vvm_614	✓	ora_vvm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. Per recuperare gli indirizzi IP di Intercluster utilizzando l'interfaccia CLI, eseguire il seguente comando:

```
ONTAP-Dest::> network interface show -role intercluster
```

Stabilisci il peering dei cluster tra i cluster ONTAP

Per stabilire il peering del cluster tra i cluster ONTAP, è necessario confermare una passphrase univoca inserita nel cluster ONTAP di avvio nell'altro cluster peer.

1. Impostare il peering sul cluster ONTAP di destinazione utilizzando l'`cluster peer create` comando. Quando richiesto, immettere una passphrase univoca da utilizzare in seguito nel cluster di origine per completare il processo di creazione.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addr  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

2. Nel cluster di origine, è possibile stabilire la relazione peer del cluster utilizzando Gestore di sistema di ONTAP o l'interfaccia CLI. Da Gestore di sistema di ONTAP, accedere a protezione > Panoramica e selezionare cluster peer.

ONTAP System Manager

DASHBOARD

STORAGE

- Overview
- Volumes
- LUNs
- Consistency Groups
- NVMe Namespaces
- Shares
- Buckets
- Qtrees
- Quotas
- Storage VMs
- Tiers

NETWORK

- Overview
- Ethernet Ports
- FC Ports

EVENTS & JOBS

PROTECTION

- Overview**
- Relationships

HOSTS

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Mediator ?

Not configured.

Configure

Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. Nella finestra di dialogo Peer Cluster, inserire le informazioni richieste:
 - a. Immettere la passphrase utilizzata per stabilire la relazione del cluster peer nel cluster ONTAP di destinazione.

- b. Selezionare **Yes** per stabilire una relazione crittografata.
- c. Inserire l'indirizzo IP intercluster LIF del cluster ONTAP di destinazione.
- d. Fare clic su **Initiate Cluster peering** (Avvia peering cluster) per completare il processo.

Peer Cluster ✕

Local

STORAGE VM PERMISSIONS

All storage VMs (incl... ✕)

Storage VMs created in the future also will be given permissions.

Remote

PASSPHRASE ?

.....

It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?

Yes

No

To generate passphrase, [Launch Remote Cluster](#)

Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

4

Initiate Cluster Peering

Cancel

4. Verificare lo stato della relazione di peer del cluster dal cluster ONTAP di destinazione con il seguente comando:

```
ONTAP-Dest::> cluster peer show
```

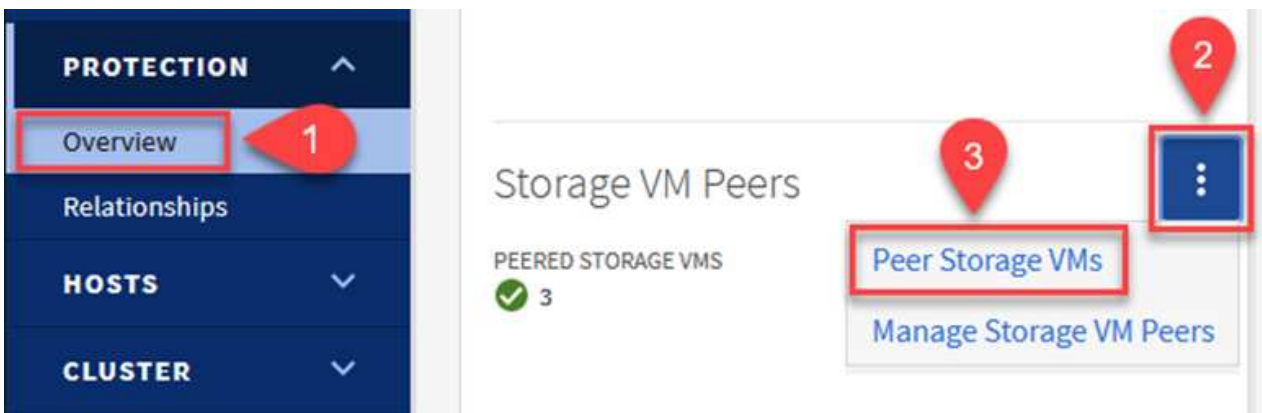

Stabilire una relazione di peering SVM

Il passaggio successivo consiste nell'impostare una relazione SVM tra le macchine virtuali dello storage di destinazione e di origine che contengono i volumi che si trovano nelle relazioni di SnapMirror.

1. Dal cluster FSX di origine, utilizzare il seguente comando dalla CLI per creare la relazione peer SVM:

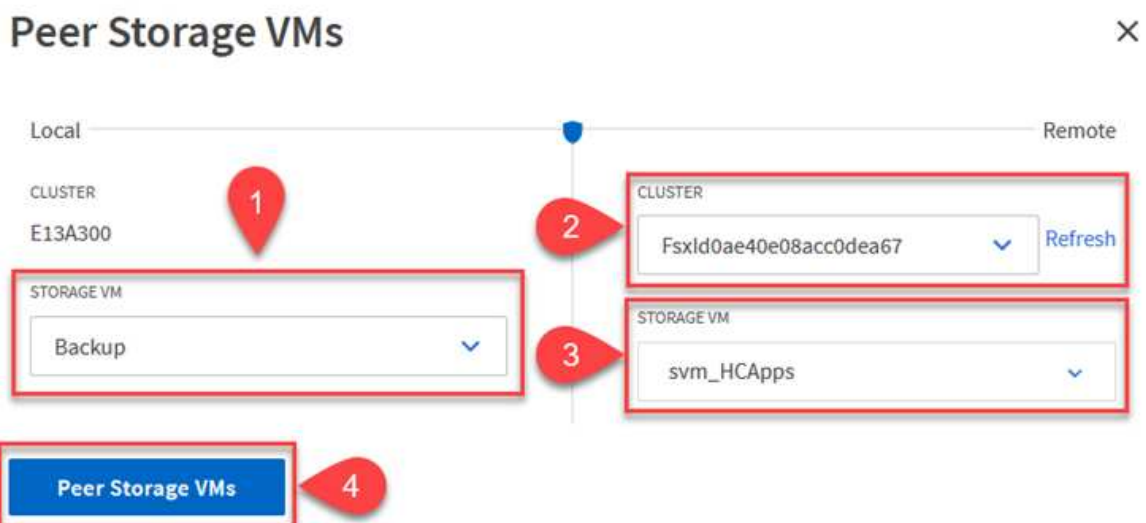
```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Dal cluster ONTAP di origine, accettare la relazione di peering con Gestore di sistema ONTAP o CLI.
3. Da Gestore di sistema ONTAP, andare a protezione > Panoramica e selezionare le VM di storage peer in peer di macchine virtuali di storage.



4. Nella finestra di dialogo Peer Storage VM, compilare i campi obbligatori:

- La VM di storage di origine
- Il cluster di destinazione
- La VM di storage di destinazione



5. Fare clic su Peer Storage VM per completare il processo di peering SVM.

Creare un criterio di conservazione delle snapshot

SnapCenter gestisce le pianificazioni di conservazione per i backup che esistono come copie Snapshot sul sistema di storage primario. Questo viene stabilito quando si crea un criterio in SnapCenter. SnapCenter non gestisce le policy di conservazione per i backup conservati nei sistemi di storage secondari. Questi criteri vengono gestiti separatamente attraverso un criterio SnapMirror creato nel cluster FSX secondario e associato ai volumi di destinazione che si trovano in una relazione SnapMirror con il volume di origine.

Quando si crea un criterio SnapCenter, è possibile specificare un'etichetta di criterio secondaria che viene aggiunta all'etichetta SnapMirror di ogni snapshot generato quando viene eseguito un backup SnapCenter.



Sullo storage secondario, queste etichette vengono associate alle regole dei criteri associate al volume di destinazione allo scopo di applicare la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutte le snapshot generate come parte di una policy utilizzata per i backup giornalieri del database SQL Server e dei volumi di log.

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label ⓘ

sql-daily

Error retry count

3 ⓘ

Per ulteriori informazioni sulla creazione di criteri SnapCenter per un database SQL Server, vedere ["Documentazione SnapCenter"](#).

È necessario innanzitutto creare un criterio SnapMirror con regole che determinano il numero di copie snapshot da conservare.

1. Creare il criterio SnapMirror sul cluster FSX.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy  
PolicyName -type mirror-vault -restart always
```

2. Aggiungere regole al criterio con le etichette SnapMirror che corrispondono alle etichette dei criteri secondari specificate nei criteri SnapCenter.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Il seguente script fornisce un esempio di regola che è possibile aggiungere a un criterio:

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



Creare regole aggiuntive per ciascuna etichetta SnapMirror e il numero di snapshot da conservare (periodo di conservazione).

Creare volumi di destinazione

Per creare un volume di destinazione su ONTAP che sarà destinatario di copie Snapshot dai volumi di origine, esegui il seguente comando sul cluster ONTAP di destinazione:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Creare le relazioni di SnapMirror tra i volumi di origine e di destinazione

Per creare una relazione di SnapMirror tra un volume di origine e di destinazione, esegui il seguente comando sul cluster ONTAP di destinazione:

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Inizializzare le relazioni di SnapMirror

Inizializzare la relazione SnapMirror. Questo processo avvia un nuovo snapshot generato dal volume di origine e lo copia nel volume di destinazione.

Per creare un volume, esegui il seguente comando sul cluster ONTAP di destinazione:

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Configurare il plug-in SnapCenter per VMware vSphere

Una volta installato, è possibile accedere al plug-in SnapCenter per VMware vSphere dall'interfaccia di gestione dell'appliance vCenter Server. SCV gestirà i backup degli archivi dati NFS montati sugli host ESXi e che contengono le macchine virtuali Windows e Linux.

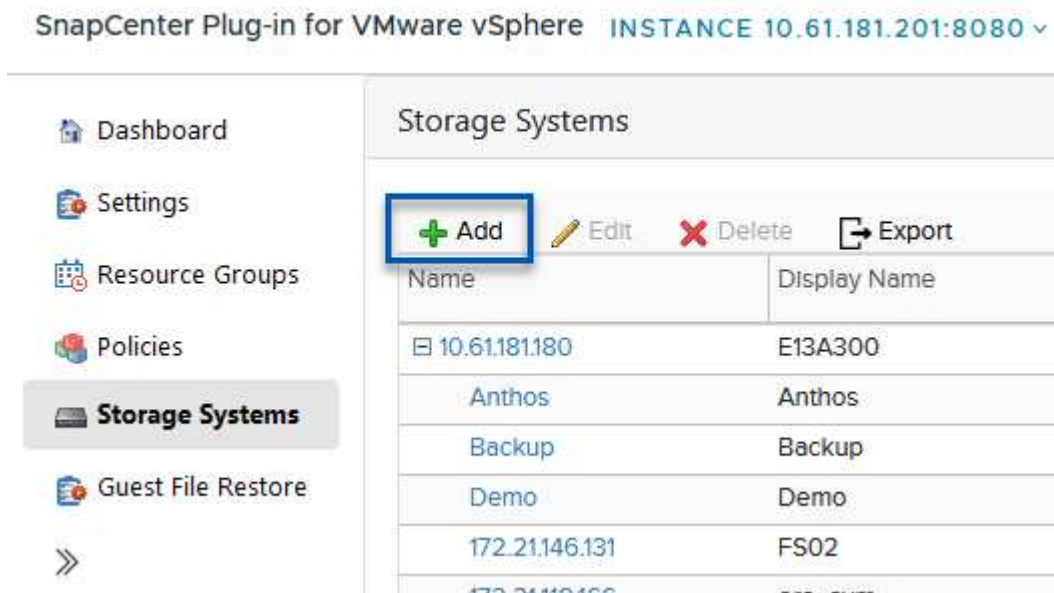
Esaminare "[Workflow di data Protection](#)" Sezione della documentazione del distributore idraulico per ulteriori informazioni sulle fasi di configurazione dei backup.

Per configurare backup di macchine virtuali e datastore, è necessario completare i seguenti passaggi dall'interfaccia del plug-in.

Sistemi storage Discovery ONTAP

Scopri i cluster di storage ONTAP da utilizzare per il backup primario e secondario.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **sistemi di archiviazione** nel menu a sinistra e fare clic sul pulsante **Aggiungi**.



2. Compilare le credenziali e il tipo di piattaforma per il sistema di storage ONTAP primario e fare clic su **Aggiungi**.

Add Storage System

Storage System	<input type="text" value="10.61.185.145"/>
Platform	<input type="text" value="All Flash FAS"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> <input type="text" value="Seconds"/>
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>
Event Management System(EMS) & AutoSupport Setting	
<input type="checkbox"/> Log Snapcenter server events to syslog	
<input type="checkbox"/> Send AutoSupport Notification for failed operation to storage system	

3. Ripetere questa procedura per il sistema di storage ONTAP secondario.

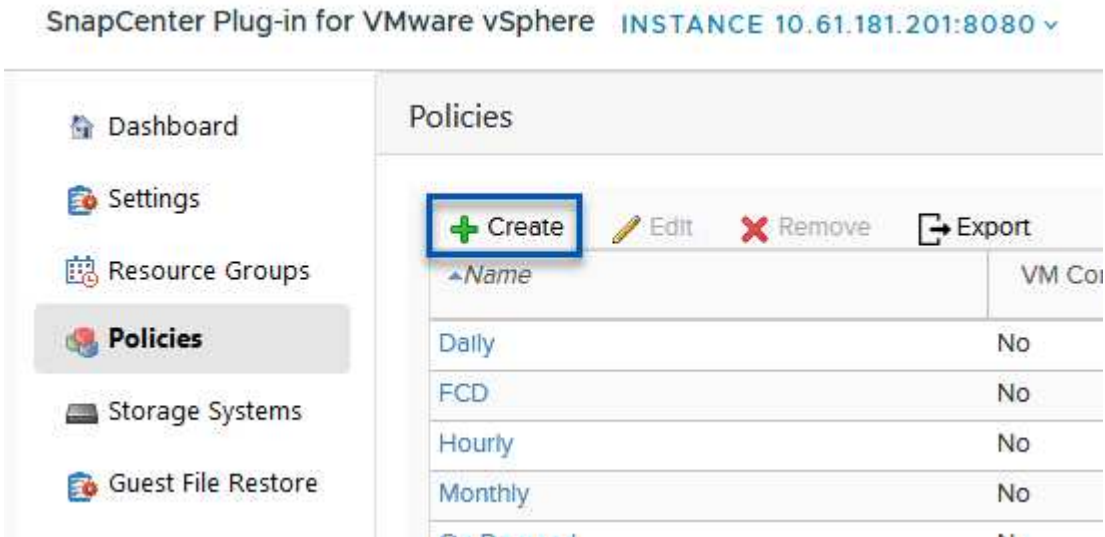
Creare le politiche di backup dei distributori idraulici

I criteri specificano il periodo di conservazione, la frequenza e le opzioni di replica per i backup gestiti da SCV.

Esaminare ["Creare policy di backup per macchine virtuali e datastore"](#) della documentazione per ulteriori informazioni.

Per creare i criteri di backup, attenersi alla seguente procedura:

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **Policies** nel menu a sinistra e fare clic sul pulsante **Create**.



2. Specificare un nome per il criterio, il periodo di conservazione, la frequenza e le opzioni di replica e l'etichetta dello snapshot.

New Backup Policy

Name	<input type="text" value="Daily"/>
Description	<input type="text" value="description"/>
Retention	<div>Days to keep <input type="text" value="30"/></div>
Frequency	<input type="text" value="Daily"/>
Replication	<div><input type="checkbox"/> Update SnapMirror after backup </div> <div><input checked="" type="checkbox"/> Update SnapVault after backup </div> <div>Snapshot label <input type="text" value="Daily"/></div>
Advanced	<div><input checked="" type="checkbox"/> VM consistency </div> <div><input type="checkbox"/> Include datastores with independent disks</div> <div>Scripts </div> <div><input type="text" value="Enter script path"/></div>



Quando si crea una policy nel plug-in di SnapCenter sono visualizzate le opzioni per SnapMirror e SnapVault. Scegliendo SnapMirror, il programma di conservazione specificato nella policy sarà lo stesso per gli snapshot primari e secondari. Scegliendo SnapVault, il programma di conservazione per la snapshot secondaria si baserà su una pianificazione separata implementata con la relazione di SnapMirror. Questa funzione è utile quando si desiderano periodi di conservazione più lunghi per backup secondari.



Le etichette degli Snapshot sono utili per attuare policy con uno specifico periodo di conservazione per le copie SnapVault replicate nel cluster ONTAP secondario. Quando SCV viene utilizzato con il backup e ripristino di BlueXP, il campo dell'etichetta dell'istantanea deve essere vuoto oppure match l'etichetta specificata nel criterio di backup di BlueXP.

3. Ripetere la procedura per ogni criterio richiesto. Ad esempio, separare i criteri per i backup giornalieri, settimanali e mensili.

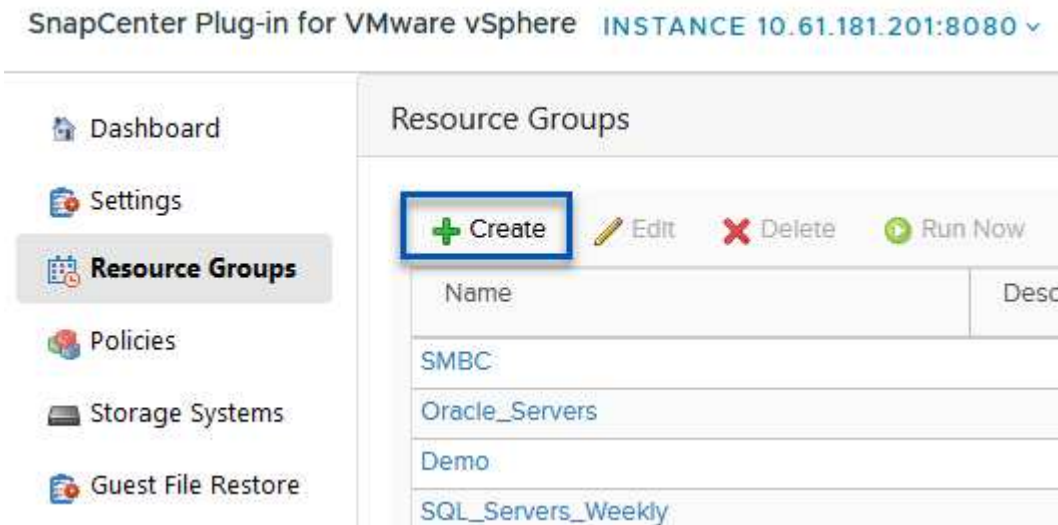
Creare gruppi di risorse

I gruppi di risorse contengono gli archivi dati e le macchine virtuali da includere in un processo di backup, insieme ai criteri e alla pianificazione di backup associati.

Esaminare ["Creare gruppi di risorse"](#) della documentazione per ulteriori informazioni.

Per creare gruppi di risorse, completare i seguenti passaggi.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **gruppi di risorse** nel menu a sinistra e fare clic sul pulsante **Crea**.



2. Nella procedura guidata Crea gruppo di risorse, immettere un nome e una descrizione per il gruppo, nonché le informazioni necessarie per ricevere le notifiche. Fare clic su **Avanti**
3. Nella pagina successiva selezionare i datastore e le macchine virtuali che si desidera includere nel processo di backup, quindi fare clic su **Avanti**.

Create Resource Group

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope:

Datastores

Datacenter:

Datastores
Virtual Machines
Tags
Folders

Entity name

Available entities

Demo
DemoDS
destination
esxi7-hc-01 Local
esxi7-hc-02 Local
esxi7-hc-03 Local
esxi7-hc-04 Local

Selected entities

NFS_SCV
NFS_WKLD



Hai la possibilità di selezionare macchine virtuali specifiche o interi datastore. Indipendentemente dal tipo di scelta effettuata, viene eseguito il backup dell'intero volume (e datastore) poiché il backup è il risultato di una snapshot del volume sottostante. Nella maggior parte dei casi, è più semplice scegliere l'intero datastore. Tuttavia, se si desidera limitare l'elenco delle VM disponibili durante il ripristino, è possibile scegliere solo un sottoinsieme di VM per il backup.

- Scegli le opzioni per l'estensione dei datastore per le macchine virtuali con VMDK che risiedono in più datastore e fai clic su **Avanti**.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

☒ Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

☐ Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

☐ Manually select the spanning datastores to be included

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.



Il backup e recovery di BlueXP non supporta al momento il backup di macchine virtuali con VMDK che coprono più datastore.

- Nella pagina successiva, selezionare i criteri da associare al gruppo di risorse e fare clic su **Avanti**.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

4. Policies

5. Schedules

6. Summary

+ Create

<input type="checkbox"/> Name	VM Consistent	Include independent di...	Schedule
<input checked="" type="checkbox"/> Daily	No	No	Daily
<input type="checkbox"/> FCD	No	Yes	On Demand Only
<input type="checkbox"/> Monthly	No	No	Monthly
<input type="checkbox"/> On Demand	No	No	On Demand Only
<input type="checkbox"/> Weekly	No	No	Weekly



Quando si esegue il backup di snapshot gestite da SCV su storage a oggetti utilizzando il backup e ripristino di BlueXP, ogni gruppo di risorse può essere associato solo a una singola policy.

- Selezionare una pianificazione che determinerà a quale ora verranno eseguiti i backup. Fare clic su **Avanti**.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

Daily



Type

Daily

Every

1

Day(s)

Starting

06/23/2023



At

07



00



PM



7. Infine, esaminare la pagina di riepilogo e poi **fine** per completare la creazione del gruppo di risorse.

Eseguire un processo di backup

In questa fase finale, eseguire un lavoro di backup e monitorarne l'avanzamento. Almeno un processo di backup deve essere completato correttamente in SCV prima di poter rilevare le risorse dal backup e ripristino di BlueXP.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **gruppi di risorse** nel menu a sinistra.
2. Per avviare un processo di backup, selezionare il gruppo di risorse desiderato e fare clic sul pulsante **Esegui ora**.

SnapCenter Plug-in for VMware vSphere **INSTANCE 10.61.181.201:8080** ▾

[Dashboard](#)
[Settings](#)
[Resource Groups](#)
[Policies](#)
[Storage Systems](#)
[Guest File Restore](#)
[»](#)

Resource Groups

[+ Create](#) [✎ Edit](#) [✖ Delete](#) **[▶ Run Now](#)** [⏸ Suspend](#)

Name	Description
Win01	
SMBC	
Oracle_Servers	
Demo	
SQL_Servers_Daily	
SQL_Servers_Weekly	

3. Per monitorare il processo di backup, accedere a **Dashboard** nel menu a sinistra. In **attività processo recenti** fare clic sul numero ID processo per monitorare l'avanzamento del processo.

Job Details : 2614

✓ Validate Retention Settings

✓ Quiescing Applications

✓ Retrieving Metadata

✓ Creating Snapshot copy

✓ Unquiescing Applications

✓ Registering Backup

✓ Backup Retention

✓ Clean Backup Cache

✓ Send EMS Messages

▶ (Job 2616)SnapVault Update

▶ Running, Start Time: 07/31/2023 07:24:40 PM.

CLOSE

DOWNLOAD JOB LOGS

Configura i backup sullo storage a oggetti nel backup e recovery di BlueXP

Per consentire a BlueXP di gestire l'infrastruttura dati in modo efficace, richiede la previa installazione di un connettore. Il connettore esegue le azioni necessarie per rilevare le risorse e gestire le operazioni sui dati.

Per ulteriori informazioni sul connettore BlueXP, fare riferimento a ["Scopri di più sui connettori"](#) Nella documentazione BlueXP.

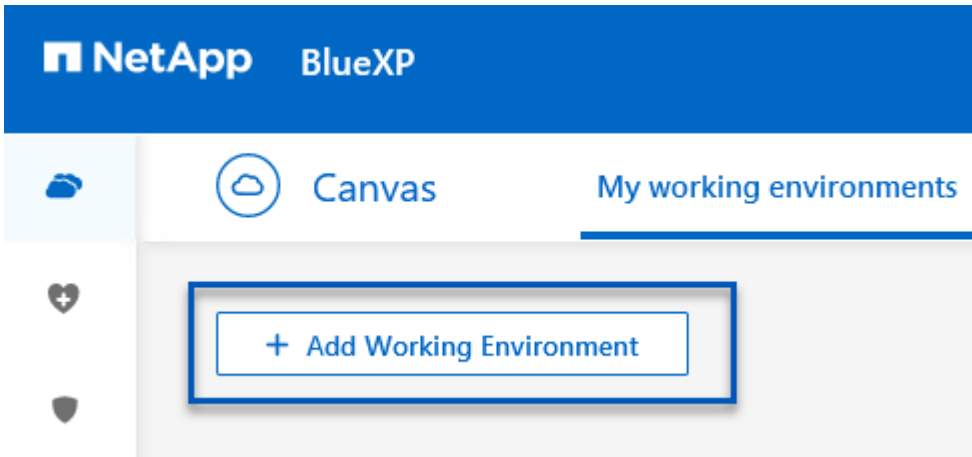
Una volta installato il connettore per il cloud provider utilizzato, una rappresentazione grafica dell'archivio oggetti sarà visibile da Canvas.

Per configurare il backup e ripristino BlueXP sui dati di backup gestiti da SCV on-premise, attenersi alla seguente procedura:

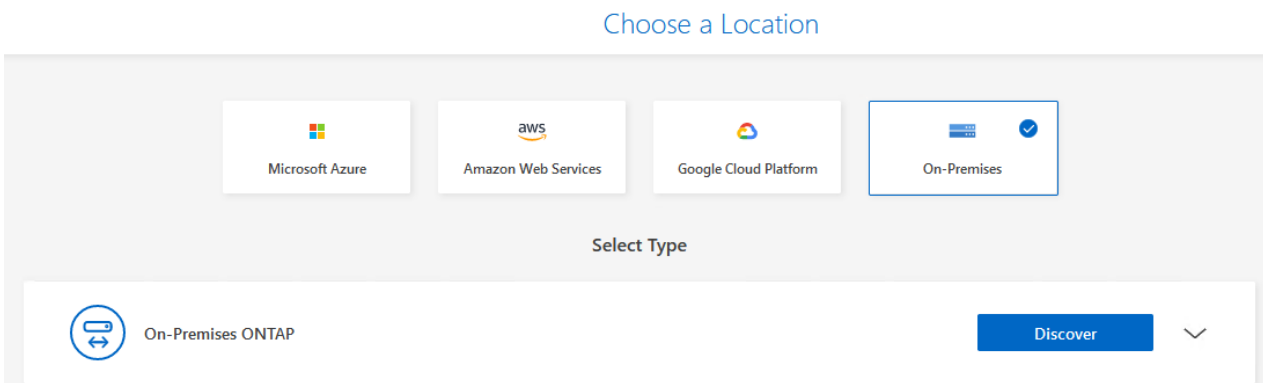
Aggiungere ambienti di lavoro al Canvas

Il primo passo è aggiungere i sistemi storage ONTAP on-premise ad BlueXP

1. Da Canvas selezionare **Aggiungi ambiente di lavoro** per iniziare.



2. Selezionare **on-Premises** (locale) dalla scelta delle località, quindi fare clic sul pulsante **Discover** (rileva).



3. Compilare le credenziali per il sistema di archiviazione ONTAP e fare clic sul pulsante **Scopri** per aggiungere l'ambiente di lavoro.

ONTAP Cluster IP

10.61.181.180

User Name

admin

Password

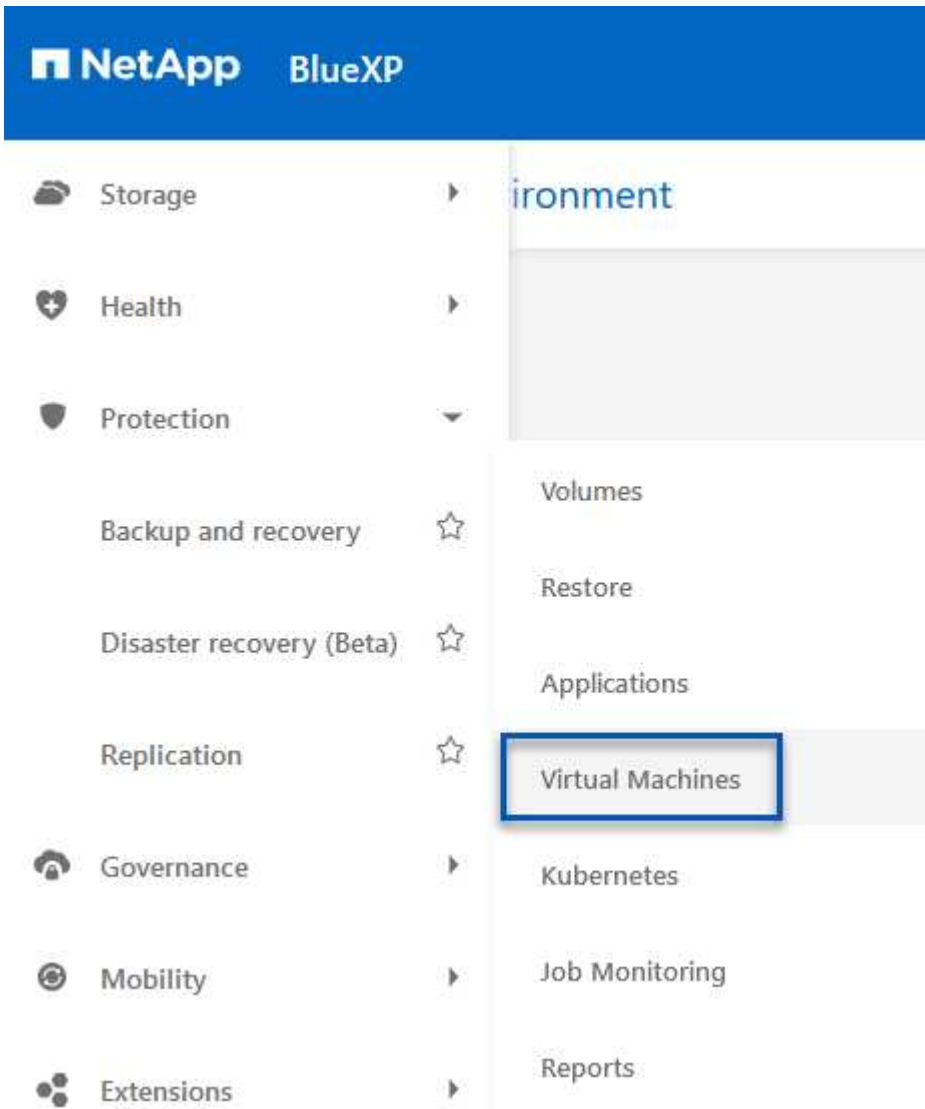
••••••••



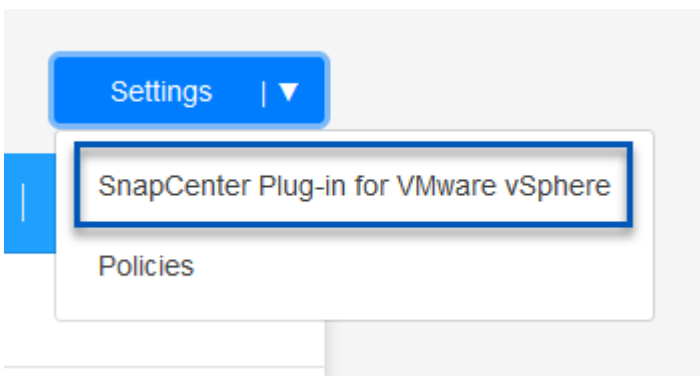
Scopri SCV appliance e vCenter on-premise

Per rilevare il datastore on-premise e le risorse delle macchine virtuali, Aggiungi le informazioni per il broker di dati SCV e le credenziali per l'appliance di gestione vCenter.

1. Dal menu a sinistra di BlueXP, selezionare **protezione > Backup e ripristino > macchine virtuali**



2. Dalla schermata principale macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare **Plug-in SnapCenter per VMware vSphere**.







3. Fare clic sul pulsante **Registra**, quindi immettere l'indirizzo IP e il numero di porta per l'appliance plug-in SnapCenter e il nome utente e la password per l'appliance di gestione vCenter. Fare clic sul pulsante **Registra** per avviare il processo di ricerca.

Register SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere	Username
<input type="text" value="10.61.181.201"/>	<input type="text" value="administrator@vsphere.local"/>
Port	Password
<input type="text" value="8144"/>	<input type="password" value="••••••••"/>

4. È possibile monitorare l'avanzamento dei lavori dalla scheda monitoraggio processi.

Job Name: Discover Virtual Resources from SnapCenter Plugin for VMWare vSphere
Job Id: 559167ba-8876-45db-9131-b918a165d0a1

			
Other Job Type	Jul 31 2023, 9:18:22 pm Start Time	Jul 31 2023, 9:18:26 pm End Time	Success Job Status

Sub-Jobs(2) Collapse All

Job Name	Job ID	Start Time	End Time	Duration
Discover Virtual Resources from SnapCenter Plu...	559167ba-8876-45db-...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:26 pm	4 Seconds
Discovering Virtual Resources	99446761-f997-4c80-8...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:24 pm	2 Seconds
Registering Datastores	b7ab4195-1ee5-40ff-9a...	Jul 31 2023, 9:18:24 pm	Jul 31 2023, 9:18:26 pm	2 Seconds

5. Una volta completato il rilevamento, sarà possibile visualizzare i datastore e le macchine virtuali in tutti gli apparecchi SCV rilevati.

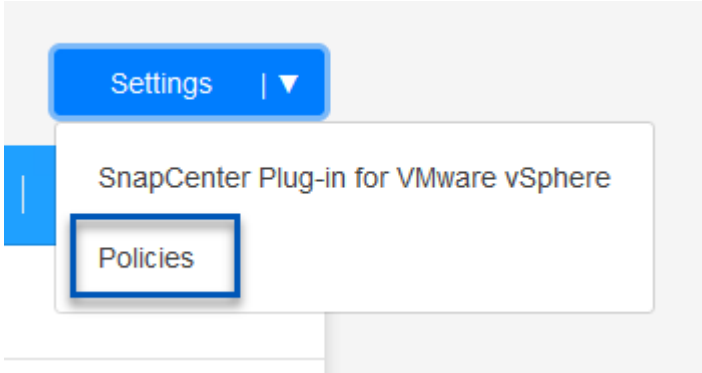
Immagine::bxp-scv-Hybrid-23.png[Visualizza risorse disponibili]

Crea policy di backup BlueXP

Nel backup e recovery di BlueXP per le macchine virtuali, crea policy per specificare il periodo di conservazione, l'origine di backup e la policy di archiviazione.

Per ulteriori informazioni sulla creazione dei criteri, consultare ["Creare una policy per il backup dei datastore"](#).

1. Dalla pagina principale di backup e ripristino di BlueXP per le macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare **Criteri**.



2. Fare clic su **Crea criterio** per accedere alla finestra **Crea criterio per il backup ibrido**.
 - a. Aggiungere un nome per il criterio
 - b. Selezionare il periodo di conservazione desiderato
 - c. Seleziona se i backup devono provenire dal sistema di storage ONTAP on-premise primario o secondario
 - d. In alternativa, è possibile specificare, dopo il periodo di tempo, il tiering dei backup nello storage di archivio, ottenendo ulteriori risparmi sui costi.

Create Policy for Hybrid Backup

Policy Details

Policy Name

Retention ⓘ

☒ Daily

Backups to retain

SnapMirror Label

☐ Weekly

Setup Retention Weekly

☐ Monthly

Setup Retention Monthly

Backup Source

☒ Primary
☐ Secondary

Archival Policy ⓘ

Backups reside in standard storage for frequently accessed data. Optionally, you can tier backups to archival storage for further cost optimization.

☐ Tier Backups to Archival

Archival After (Days)

Cancel

Create



L'etichetta SnapMirror immessa qui viene utilizzata per identificare i backup da applicare anche la policy. Il nome dell'etichetta deve corrispondere al nome dell'etichetta nella politica SCV in loco corrispondente.

- Fare clic su **Crea** per completare la creazione del criterio.

Effettuare il backup dei datastore su Amazon Web Services

L'ultima fase consiste nell'attivare la data Protection per i singoli datastore e le macchine virtuali. Segue una descrizione della modalità di attivazione dei backup in AWS.

Per ulteriori informazioni, fare riferimento a. "[Eseguire il backup dei datastore su Amazon Web Services](#)".

1. Dalla pagina principale di backup e recovery di BlueXP per le macchine virtuali, accedi al menu a discesa delle impostazioni per il datastore da sottoporre a backup e seleziona **attiva backup**.

6 Datastores

Filter By + VM View Settings

Datastore	Datastore Type	vCenter	Policy Name	Protection Status
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		Unprotected
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	Protected
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected

2. Assegnare il criterio da utilizzare per l'operazione di protezione dei dati e fare clic su **Avanti**.

1 Assign Policy **2 Add Working Environments** **3 Select Provider** **4 Configure Provider** **5 Review**

Assign Policy

21 Policies

	Policy Name	SnapMirror Label	Retention Count	Backup Source	Archival Policy
<input type="radio"/>	5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input checked="" type="radio"/>	5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input type="radio"/>	7 Year Weekly LTR	weekly	weekly : 370	Primary	Not Active

3. Nella pagina **Aggiungi ambienti di lavoro**, il datastore e l'ambiente di lavoro con un segno di spunta dovrebbero apparire se l'ambiente di lavoro è stato precedentemente rilevato. Se l'ambiente di lavoro non è stato rilevato in precedenza, è possibile aggiungerlo qui. Fare clic su **Avanti** per continuare.

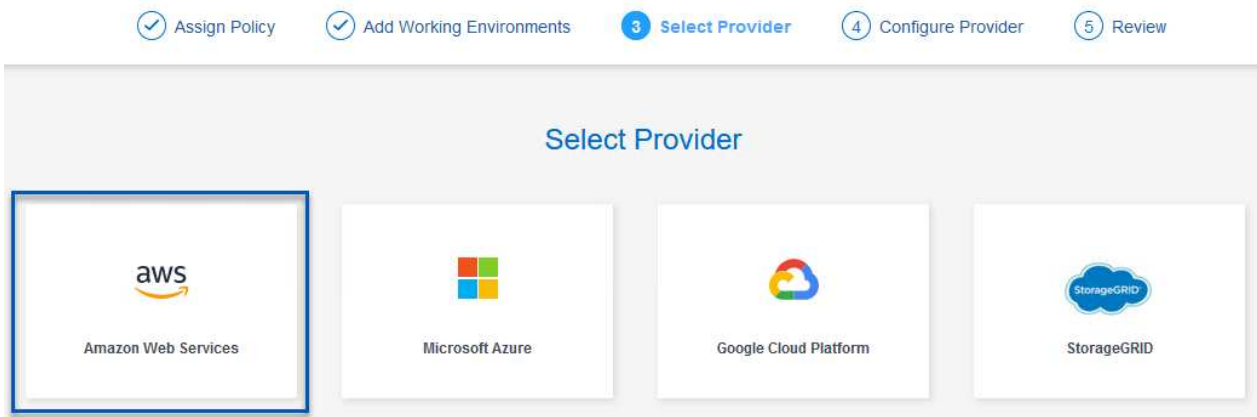
1 Assign Policy **2 Add Working Environments** **3 Select Provider** **4 Configure Provider** **5 Review**

Add Working Environments

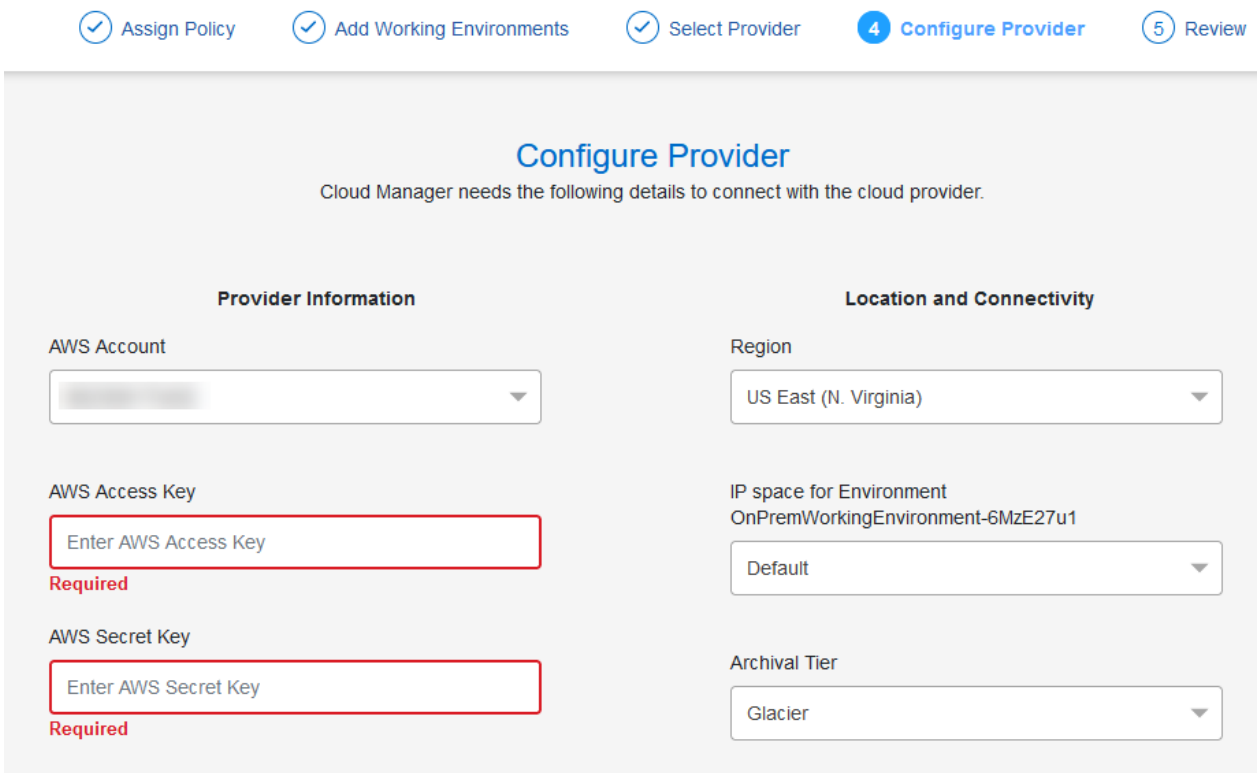
Provide ONTAP cluster (working environment) details that you want Cloud Manager to discover. Working environment details will appear for all volumes that reside on the same cluster. You will need to enter multiple working environments when volumes reside on different clusters.

SVM	Volume	Working Environment
EHC_NFS	NFS_SCV	OnPremWorkingEnvironment-6MzE27u1

4. Nella pagina **Select Provider** (Seleziona fornitore), fare clic su AWS, quindi sul pulsante **Next** (Avanti) per continuare.



5. Compila le informazioni sulle credenziali specifiche del provider per AWS, inclusi la chiave di accesso AWS e la chiave segreta, la regione e il Tier di archivio da utilizzare. Inoltre, seleziona lo spazio IP ONTAP per il sistema storage ONTAP on-premise. Fare clic su **Avanti**.



6. Infine, esaminare i dettagli del processo di backup e fare clic sul pulsante **attiva backup** per avviare la protezione dei dati del datastore.

Review

Policy	5 Year Daily LTR
SVM	EHC_NFS
Volumes	NFS_SCV
Working Environment	OnPremWorkingEnvironment-6MzE27u1
Backup Source	Primary
Cloud Service Provider	AWS
AWS Account	[REDACTED]
AWS Access Key	[REDACTED]
Region	US East (N. Virginia)
IP space	Default
Tier Backups to Archival	No

[Previous](#)[Activate Backup](#)

A questo punto il trasferimento dei dati potrebbe non iniziare immediatamente. Il backup e recovery di BlueXP analizza ogni ora le snapshot in sospeso e le trasferisce nello storage a oggetti.

Ripristino delle macchine virtuali in caso di perdita di dati

Garantire la protezione dei dati è solo un aspetto della protezione dati completa. Un aspetto altrettanto cruciale è la possibilità di ripristinare tempestivamente i dati da qualsiasi posizione in caso di perdita di dati o attacco ransomware. Questa funzionalità è fondamentale per mantenere operative di business perfette e soddisfare i recovery point objective.

NetApp offre una strategia 3-2-1 altamente adattabile, che offre un controllo customizzato sulle pianificazioni della conservazione nelle posizioni di storage primario, secondario e a oggetti. Questa strategia offre la flessibilità necessaria per personalizzare gli approcci di protezione dei dati in base a esigenze specifiche.

Questa sezione offre una panoramica del processo di ripristino dei dati dal plug-in SnapCenter per VMware vSphere e da backup e recovery BlueXP per le macchine virtuali.

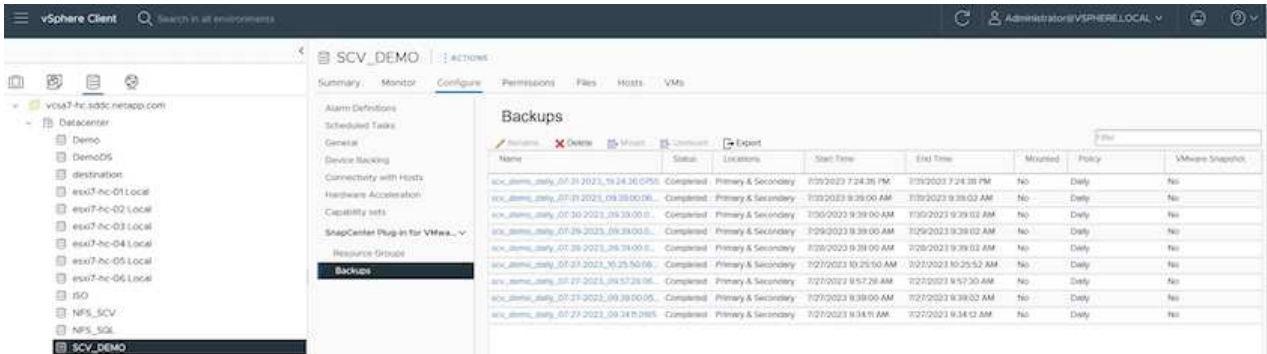
Ripristino di macchine virtuali dal plug-in SnapCenter per VMware vSphere

Per questa soluzione, le macchine virtuali sono state ripristinate in posizioni originali e alternative. Non tutti gli aspetti delle capacità di ripristino dei dati dei distributori idraulici saranno trattati in questa soluzione. Per informazioni dettagliate su tutto ciò che il distributore idraulico ha da offrire, fare riferimento alla "[Ripristinare le macchine virtuali dai backup](#)" nella documentazione del prodotto.

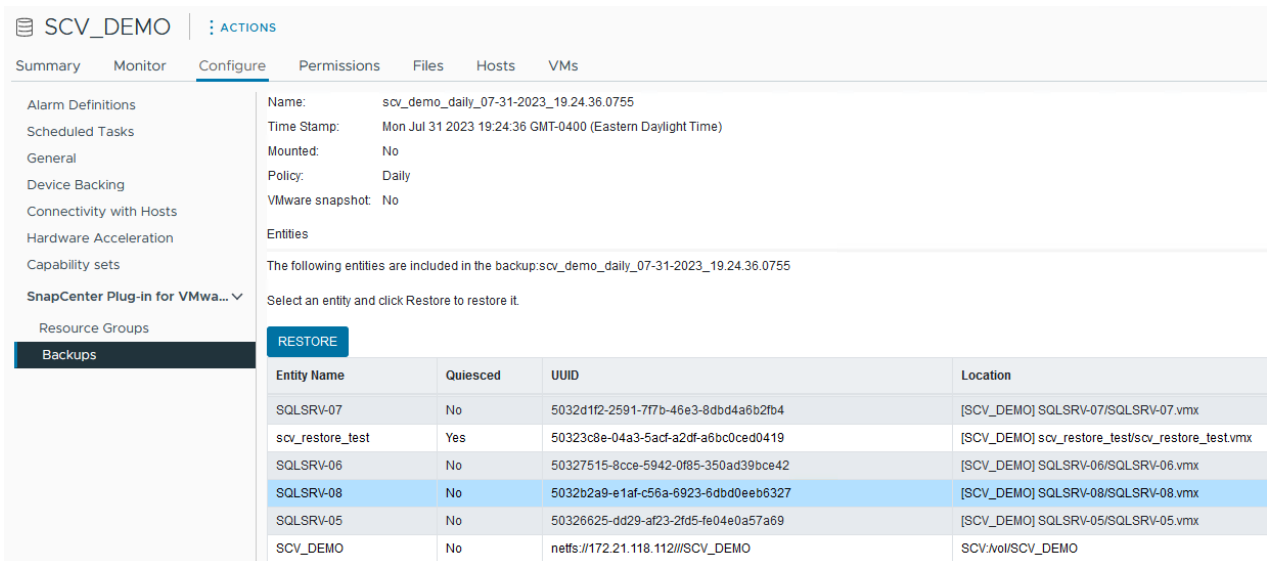
Ripristinare le macchine virtuali dal distributore idraulico

Completare i seguenti passaggi per ripristinare un ripristino di una macchina virtuale dallo storage primario o secondario.

1. Dal client vCenter, accedere a **inventario > archiviazione** e fare clic sul datastore che contiene le macchine virtuali che si desidera ripristinare.
2. Dalla scheda **Configure** fare clic su **backups** per accedere all'elenco dei backup disponibili.



- Fare clic su un backup per accedere all'elenco delle VM, quindi selezionare una VM da ripristinare. Fare clic su **Ripristina**.



4. Dalla procedura guidata di ripristino, selezionare per ripristinare l'intera macchina virtuale o un VMDK specifico. Seleziona per eseguire l'installazione nella posizione originale o in una posizione alternativa, fornisci il nome della macchina virtuale dopo il ripristino e il datastore di destinazione. Fare clic su **Avanti**.

Restore



✓ 1. Select scope

2. Select location

3. Summary

Restore scope

Entire virtual machine

Restart VM

☐

Restore Location

☐ Original Location

(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)

☒ Alternate Location

(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server

10.61.181.210

Destination ESXi host

esxi7-hc-04.sddc.netapp.com

Network

Management 181

VM name after restore

SQL_SRV_08_restored

Select Datastore:

NFS_SCV

BACK

NEXT

FINISH

CANCEL

5. Scegli di eseguire il backup dalla posizione dello storage primario o secondario.

Restore



✓ 1. Select scope

2. Select location

3. Summary

Destination datastore	Locations
SCV_DEMO	(Primary) SCV:SCV_DEMO
	(Primary) SCV:SCV_DEMO
	(Secondary) EHC_NFS:SCV_DEMO_dest

6. Infine, esaminare un riepilogo del processo di backup e fare clic su fine per avviare il processo di ripristino.

Ripristino di macchine virtuali dal backup e recovery di BlueXP per le macchine virtuali

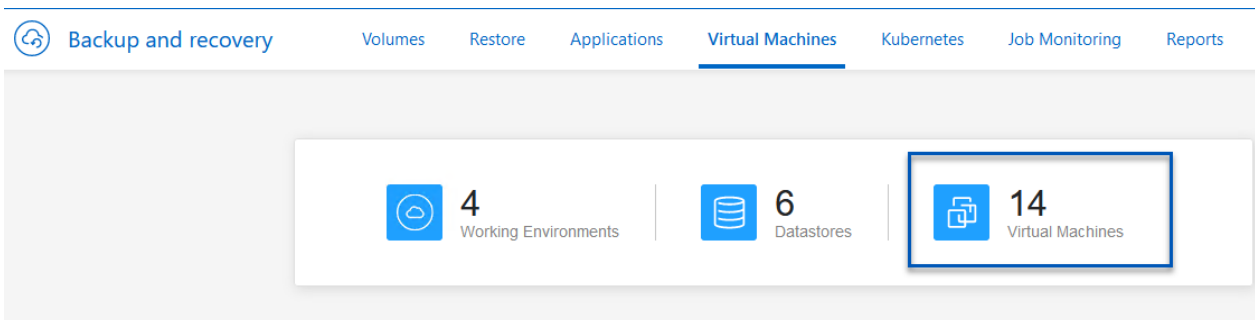
Il backup e recovery di BlueXP per le macchine virtuali consente di ripristinare le macchine virtuali nella loro posizione originale. È possibile accedere alle funzioni di ripristino dalla console web BlueXP.

Per ulteriori informazioni, fare riferimento a. ["Ripristinare i dati delle macchine virtuali dal cloud"](#).

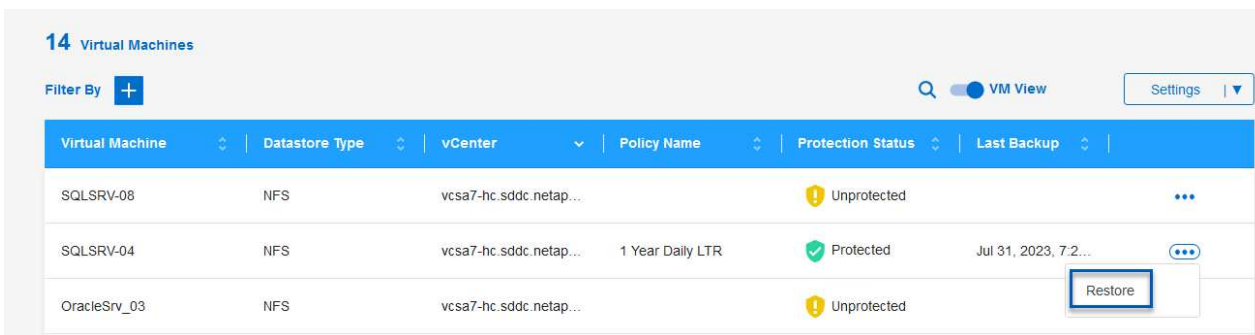
Ripristina le macchine virtuali dal backup e recovery di BlueXP

Per ripristinare una macchina virtuale dal backup e recovery di BlueXP, completa i seguenti passaggi.

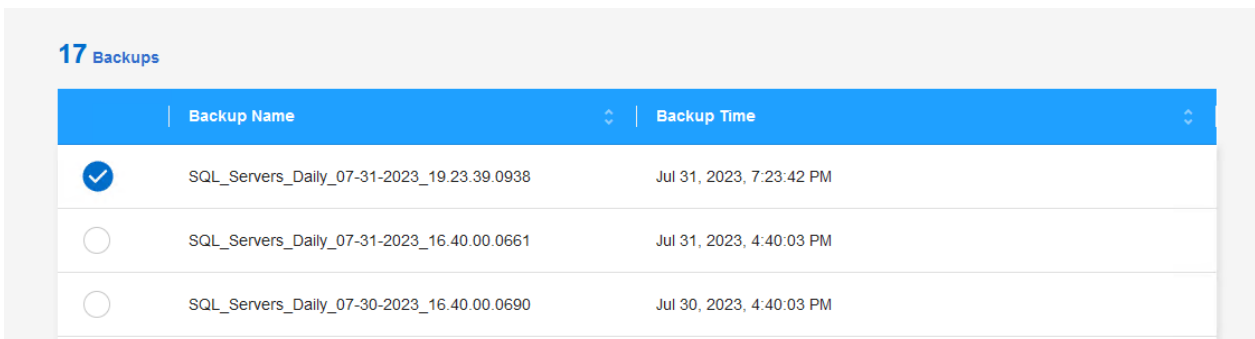
1. Accedere a **protezione > Backup e ripristino > macchine virtuali** e fare clic su macchine virtuali per visualizzare l'elenco delle macchine virtuali disponibili per il ripristino.



2. Accedere al menu a discesa delle impostazioni per la VM da ripristinare e selezionare



3. Selezionare il backup da cui eseguire il ripristino e fare clic su **Avanti**.



4. Esaminare un riepilogo del processo di backup e fare clic su **Ripristina** per avviare il processo di ripristino.
5. Monitorare l'avanzamento del processo di ripristino dalla scheda **monitoraggio processo**.

ery
Volumes
Restore
Applications
Virtual Machines
Kubernetes
Job Monitoring
Reports

restore 17 files from Cloud

Job Name: Restore 17 files from Cloud
 Job Id: ec567065-dcf4-4174-b7ef-b27e6620fdbf

Restore Files
Job Type

NFS_SQL
Restore Content

17 Files
Content Files

NFS_SQL
Restore to

In Progress
Job Status

Expand All

Restore Content

	ots-demo Working Environment Name	NAS_VOLS SVM Name	NFS_SQL Volume Name	SQL_Servers_Daily_07-31-2023_... Backup Name	Jul 31 2023, 7:24:03 pm Backup Time
--	--------------------------------------	----------------------	------------------------	---	--

Restore from

	AWS Provider	us-east-1 Region	982589175402 Account ID	netapp-backup-d56250b0-24ad... Bucket/Container Name
--	-----------------	---------------------	----------------------------	---

Conclusione

La strategia di backup 3-2-1, se implementata con il plug-in SnapCenter per backup e recovery di VMware vSphere e BlueXP per le macchine virtuali, offre una soluzione solida, affidabile e conveniente per la protezione dei dati. Questa strategia non solo garantisce ridondanza e accessibilità dei dati, ma offre anche la flessibilità di ripristinare i dati da qualsiasi posizione e da sistemi storage ONTAP on-premise e dallo storage a oggetti basato sul cloud.

Il caso di utilizzo presentato in questa documentazione si concentra sulle tecnologie comprovate di data Protection che evidenziano l'integrazione tra NetApp, VMware e i cloud provider leader. Il plug-in SnapCenter per VMware vSphere offre un'integrazione perfetta con VMware vSphere, consentendo una gestione efficiente e centralizzata delle operazioni di protezione dei dati. Questa integrazione semplifica i processi di backup e recovery per le macchine virtuali, consentendo operazioni di pianificazione, monitoraggio e ripristino flessibili all'interno dell'ecosistema VMware. Il backup e recovery di BlueXP per le macchine virtuali fornisce quello (1) in 3-2-1, fornendo backup sicuri e a corto di aria dei dati delle macchine virtuali sullo storage a oggetti basato sul cloud. L'interfaccia intuitiva e il flusso di lavoro logico offrono una piattaforma sicura per l'archiviazione a lungo termine dei dati critici.

Ulteriori informazioni

Per ulteriori informazioni sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- ["Plug-in SnapCenter per la documentazione di VMware vSphere"](#)
- ["Documentazione BlueXP"](#)

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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