Backup e ripristino dei dati delle applicazioni on-premise

BlueXP backup and recovery

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/it-it/bluexp-backup-recovery/concept-protect-app-data-to-cloud.html on April 18, 2024. Always check docs.netapp.com for the latest.

Sommario

Backup e ripristino dei dati delle applicazioni on-premise

Proteggi i dati delle tue applicazioni on-premise

Il backup e ripristino BlueXP per le applicazioni offre funzionalità di protezione dei dati per snapshot coerenti con le applicazioni da ONTAP primario on-premise a cloud provider.

Puoi eseguire il backup di Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL, e PostgreSQL dai sistemi ONTAP on-premise ad Amazon Web Services, Microsoft Azure, Google Cloud Platform e StorageGRID.

Per ulteriori informazioni sul backup e ripristino BlueXP per le applicazioni, fare riferimento a:

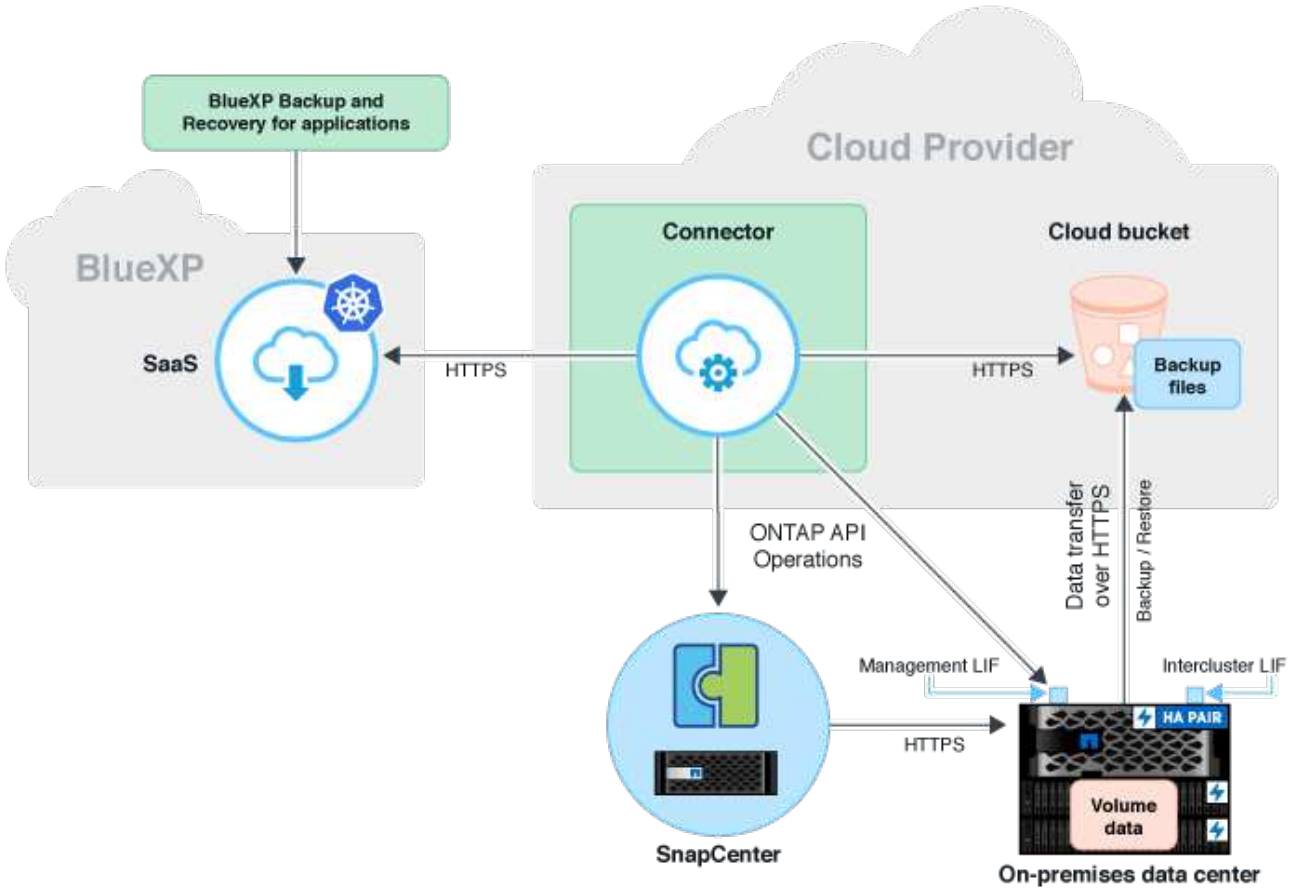
- "Backup integrato con l'applicazione con backup e ripristino BlueXP e SnapCenter"
- "Podcast su BlueXP backup e recovery per le applicazioni"

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei dati delle applicazioni nel cloud provider.

- ONTAP 9.8 o versione successiva
- BlueXP
- Server SnapCenter 4.6 o versione successiva
  - Se si desidera utilizzare le seguenti funzionalità, si consiglia di utilizzare SnapCenter Server 4.7 o versioni successive:
    - Protezione dei backup dallo storage secondario on-premise
    - Proteggere le applicazioni SAP HANA
    - Proteggere le applicazioni Oracle e SQL presenti nell'ambiente VMware
    - Esportazione dello storage di un backup
    - Disattivare i backup
    - Annullare la registrazione del server SnapCenter
  - Utilizzare SnapCenter Server 4,9 o versioni successive se si desidera utilizzare le seguenti funzioni:
    - Montare i backup del database Oracle
    - Ripristinare lo storage alternativo
  - Se si desidera proteggere le applicazioni MongoDB, MySQL e PostgreSQL, è consigliabile utilizzare SnapCenter Server 4,9P1
- Nel server SnapCenter deve essere disponibile almeno un backup per applicazione
- Almeno una policy giornaliera, settimanale o mensile in SnapCenter senza etichetta o stessa etichetta della policy in BlueXP

L'immagine seguente mostra ogni componente durante il backup nel cloud e le connessioni che è necessario preparare tra di essi:



Registrare il server SnapCenter

Solo un utente con ruolo SnapCenterAdmin può registrare l'host su cui è in esecuzione SnapCenter Server 4.6 o versione successiva. È possibile registrare più host server SnapCenter in BlueXP.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Server SnapCenter**.
3. Fare clic su **Registra server SnapCenter**.
4. Specificare i seguenti dettagli:
   a. Nel campo Server SnapCenter, specificare l'FQDN o l'indirizzo IP dell'host server SnapCenter.
   b. Nel campo porta, specificare il numero di porta su cui è in esecuzione l'host del server SnapCenter.

      Assicurarsi che la porta sia aperta per consentire la comunicazione tra il server SnapCenter e BlueXP.

   c. Nel campo Tag, specificare il nome del sito, la città o qualsiasi nome personalizzato con cui si desidera contrassegnare il server SnapCenter.

      I tag sono separati da virgole.

d. Nel campo Nome utente e Password, specificare le credenziali dell'utente con ruolo SnapCenterAdmin.

5. Selezionare il connettore dall'elenco a discesa **Connector** (connettore).
6. Fare clic su **Registra**.

Al termine

Fare clic su **Backup e ripristino** > **applicazioni** per visualizzare tutte le applicazioni protette mediante l'host del server SnapCenter registrato. Per impostazione predefinita, le applicazioni vengono rilevate automaticamente ogni giorno a mezzanotte.

Le applicazioni supportate e le relative configurazioni sono:

- Database Oracle:
  - Backup completi (dati + log) creati con almeno una pianificazione giornaliera, settimanale o mensile
  - SAN, NFS, VMDK-SAN, VMDK-NFS E RDM
- Database Microsoft SQL Server:
  - Standalone, istanze di cluster di failover e gruppi di disponibilità
  - Backup completi creati con almeno una pianificazione giornaliera, settimanale o mensile
  - SAN, VMDK-SAN, VMDK-NFS E RDM
- Database SAP HANA:
  - Container singolo 1.x
  - Contenitore di database multipli 2.x
  - Replica di sistema HANA (HSR)

    È necessario disporre di almeno un backup su siti primari e secondari. È possibile decidere di eseguire un guasto proattivo o un failover rinviato al secondario.

  - Risorse NDV (non-data Volumes) come file binari HANA, volume di log di archiviazione HANA, volume condiviso HANA e così via
- MongoDB
- MySQL
- PostgreSQL

I seguenti database non vengono visualizzati:

- Database senza backup
- Database con policy solo on-demand o orarie
- Database Oracle residenti su NVMe

Creare un criterio per il backup delle applicazioni

È necessario creare una policy per eseguire il backup dei dati dell'applicazione nel cloud.

Prima di iniziare

- Se si desidera spostare i backup dall'archivio di oggetti allo storage di archiviazione, assicurarsi di utilizzare la versione di ONTAP richiesta.

- Se utilizzi i servizi Web Amazon, dovresti utilizzare ONTAP 9.10.1 o versione successiva
- Se si utilizza Microsoft Azure, è necessario utilizzare ONTAP 9.10.1 o versione successiva
- Se utilizzi Google Cloud, dovresti utilizzare ONTAP 9.12.1 o versione successiva
- Se si utilizza StorageGRID, si consiglia di utilizzare ONTAP 9.12.1 o versione successiva

- È necessario configurare il Tier di accesso all'archivio per ciascun provider di cloud.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Dal menu a discesa Impostazioni, fare clic su **Criteri** > **Crea policy**.
3. Nella sezione Dettagli policy, specificare il nome del policy.
4. Nella sezione conservazione, selezionare uno dei tipi di conservazione e specificare il numero di backup da conservare.
5. Selezionare Primary (principale) o Secondary (secondario) come origine dello storage di backup.
6. (Facoltativo) se si desidera spostare i backup dall'archivio di oggetti allo storage di archiviazione dopo un certo numero di giorni per l'ottimizzazione dei costi, selezionare la casella di controllo **Tier backups to Archival**.
7. Fare clic su **Create** (Crea).

Non è possibile modificare o eliminare un criterio associato a un'applicazione.

Eseguire il backup dei dati delle applicazioni on-premise su Amazon Web Services

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP a Amazon Web Services.

BlueXP supporta il blocco dei dati e la protezione dal ransomware. Se il cluster ONTAP è in esecuzione su ONTAP 9.11.1 o versione successiva e non hai configurato lo storage di archivio, puoi proteggere i backup dalla sovrascrittura, dall'eliminazione e dalle minacce ransomware.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (Avanti).
4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.

Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

c. Fare clic su **Aggiungi ambiente di lavoro**.

5. Selezionare **Amazon Web Services** come provider cloud.
   a. Specificare l'account AWS.
   b. Nel campo AWS Access Key (chiave di accesso AWS), specificare la chiave.
   c. Nel campo AWS Secret Key (chiave segreta AWS), specificare la password.
   d. Selezionare la regione in cui si desidera creare i backup.
   e. Specificare lo spazio IP.
   f. Selezionare il livello di archiviazione se è stato configurato lo spazio di archiviazione nel criterio.

      Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Configurare il blocco dei dati e la protezione dal ransomware.
7. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei dati delle applicazioni on-premise su Microsoft Azure

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP a Microsoft Azure.

BlueXP supporta il blocco dei dati e la protezione dal ransomware. Se il cluster ONTAP è in esecuzione su ONTAP 9.12.1 o versione successiva e non hai configurato lo storage di archivio, puoi proteggere i backup dalla sovrascrittura, dall'eliminazione e dalle minacce ransomware.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (Avanti).
4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.

         Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

   c. Fare clic su **Aggiungi ambiente di lavoro**.
5. Selezionare **Microsoft Azure** come cloud provider.

a. Specificare l'ID dell'abbonamento Azure.
b. Selezionare la regione in cui si desidera creare i backup.
c. Creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente.
d. Specificare lo spazio IP.
e. Selezionare il livello di archiviazione se è stato configurato lo spazio di archiviazione nel criterio.

   Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Configurare il blocco dei dati e la protezione dal ransomware.
7. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei dati delle applicazioni on-premise su Google Cloud Platform

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP alla piattaforma cloud Google.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (Avanti).
4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.

      Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

   c. Fare clic su **Aggiungi ambiente di lavoro**.
5. Selezionare **Google Cloud Platform** come provider di cloud.
   a. Seleziona il progetto Google Cloud in cui desideri creare il bucket di storage Google Cloud per i backup.
   b. Nel campo Google Cloud Access Key, specificare la chiave.
   c. Nel campo Google Cloud Secret Key, specificare la password.
   d. Selezionare la regione in cui si desidera creare i backup.
   e. Specificare lo spazio IP.
   f. Selezionare il livello di archiviazione.

Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Eseguire il backup dei dati delle applicazioni on-premise su StorageGRID

Completare alcuni passaggi per eseguire il backup dei dati delle applicazioni da ONTAP a StorageGRID.

BlueXP supporta il blocco dei dati e la protezione dal ransomware. Se il cluster ONTAP è in esecuzione su ONTAP 9.11.1 o versione successiva, i sistemi StorageGRID sono 11.6.0.3 o versione successiva e se non hai configurato lo storage di archivio, puoi proteggere i backup da sovrascrittura, eliminazione e minacce ransomware.

Prima di iniziare

Quando si esegue il backup dei dati su StorageGRID, è necessario che sia disponibile un connettore on-premise. Sarà necessario installare un nuovo connettore o assicurarsi che il connettore attualmente selezionato risieda on-premise. Il connettore può essere installato in un sito con o senza accesso a Internet.

Per ulteriori informazioni, vedere "Creare connettori per StorageGRID".

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Activate Backup** (attiva backup).
3. Nella pagina Assign Policy (Assegna policy), selezionare il criterio e fare clic su **Next** (Avanti).
4. Aggiungere l'ambiente di lavoro.

   Configurare la LIF di gestione del cluster che BlueXP deve rilevare. Dopo aver aggiunto l'ambiente di lavoro per una delle applicazioni, è possibile riutilizzarlo per tutte le altre applicazioni che risiedono sullo stesso cluster ONTAP.

   a. Selezionare la SVM e fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
   b. Nella procedura guidata Aggiungi ambiente di lavoro:
      i. Specificare l'indirizzo IP della LIF di gestione del cluster.
      ii. Specificare le credenziali dell'utente del cluster ONTAP.

      Il backup e ripristino BlueXP per le applicazioni supporta solo l'amministratore del cluster.

   c. Fare clic su **Aggiungi ambiente di lavoro**.
5. Selezionare **StorageGRID**.
   a. Specificare l'FQDN del server StorageGRID e la porta su cui viene eseguito il server StorageGRID.

      Inserire i dettagli nel formato FQDN:PORT.

   b. Nel campo Access Key (chiave di accesso), specificare la chiave.
   c. Nel campo Secret Key (chiave segreta), specificare la password.

d. Specificare lo spazio IP.

e. Specificare il livello di archiviazione se è stato configurato lo spazio di archiviazione nel criterio.

Se si seleziona…	Eseguire le seguenti operazioni…
AWS	i. Selezionare il StorageGRID dal menu a discesa o aggiungere il cluster StorageGRID. ii. Specificare l'account AWS. iii. Nel campo AWS Access Key (chiave di accesso AWS), specificare la chiave. iv. Nel campo AWS Secret Key (chiave segreta AWS), specificare la password. v. Selezionare la regione in cui si desidera creare i backup. vi. Fare clic su **Save** (Salva).
Azure	i. Selezionare il cluster StorageGRID dal menu a discesa o aggiungere il cluster. ii. Specificare l'ID dell'abbonamento Azure. iii. Selezionare la regione in cui si desidera creare i backup. iv. Creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente. v. Fare clic su **Save** (Salva).

Si consiglia di impostare il livello di archiviazione perché si tratta di un'attività una tantum e non sarà possibile configurarla in un secondo momento.

6. Configurare il blocco dei dati e la protezione dal ransomware.
7. Esaminare i dettagli e fare clic su **Activate Backup** (attiva backup).

Gestire la protezione delle applicazioni

È possibile gestire la protezione delle applicazioni visualizzando i criteri, visualizzando i backup, visualizzando le modifiche al layout del database, ai criteri e al gruppo di risorse e monitorando tutte le operazioni dall'interfaccia utente di BlueXP.

Visualizzare le policy

È possibile visualizzare tutte le policy. Per ciascuno di questi criteri, quando si visualizzano i dettagli vengono elencate tutte le applicazioni associate.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Criteri**.

3. Fare clic su **View Details** (Visualizza dettagli) corrispondente alla policy di cui si desidera visualizzare i dettagli.

   Vengono elencate le applicazioni associate.

   Non è possibile modificare o eliminare un criterio associato a un'applicazione.

È inoltre possibile visualizzare le policy SnapCenter estese nel cloud eseguendo `Get-SmResources` Cmdlet in SnapCenter.
Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help command name.

Visualizza i backup sul cloud

È possibile visualizzare i backup sul cloud nell'interfaccia utente di BlueXP.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **View Details** (Visualizza dettagli).

   Il tempo necessario per l'elenco dei backup dipende dalla pianificazione di replica predefinita di ONTAP.

- Per i database Oracle, vengono elencati sia i backup dei dati che dei log, il numero di modifica del sistema (SCN) per ciascun backup e la data di fine di ciascun backup. È possibile selezionare solo il backup dei dati e ripristinare il database nella posizione originale. È possibile montare il backup dei dati e il backup dei log in una posizione alternativa.
- Per i database Microsoft SQL Server, vengono elencati solo i backup completi e la data di fine di ciascun backup. È possibile selezionare il backup e ripristinare il database nella posizione originale o alternativa.
- Per l'istanza di Microsoft SQL Server, vengono elencati i backup dei database in tale istanza.
- Per i database SAP HANA, vengono elencati solo i backup dei dati e la data di fine di ciascun backup. È possibile selezionare il backup ed eseguire l'esportazione dello storage su un determinato host.
- Per MongoDB, MySQL e PostgreSQL, sono elencati solo i backup dei dati e la data finale di ciascun backup. È possibile selezionare il backup ed eseguire l'esportazione dello storage su un determinato host.

I backup creati prima di attivare la protezione cloud non sono elencati per il ripristino.

È inoltre possibile visualizzare questi backup eseguendo il `Get-SmBackup` Cmdlet in SnapCenter.
Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help command name.

Disattivare il backup

È possibile eliminare tutti i backup spostati nell'archivio di oggetti da SnapCenter e dall'archivio di oggetti.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su Disattiva backup.

Per impostazione predefinita, la casella di controllo è selezionata ed elimina tutti i backup spostati nell'archivio di oggetti da SnapCenter e dall'archivio di oggetti.

Se si deseleziona la casella di controllo, i backup vengono conservati solo nell'archivio di oggetti, ma non possono essere utilizzati per il ripristino a livello di applicazione. Successivamente, quando si attiva il backup per questa applicazione, i backup conservati nell'archivio di oggetti non vengono elencati per il ripristino.

3. Fare clic su **Disattiva backup**.

Modifica del layout del database

Quando i volumi vengono aggiunti al database, il server SnapCenter assegna automaticamente le etichette agli snapshot sui nuovi volumi in base alla policy e alla pianificazione. Questi nuovi volumi non avranno l'endpoint dell'archivio di oggetti ed è necessario aggiornare i volumi eseguendo i seguenti passaggi:

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Server SnapCenter**.
3. Fare clic su ••• Corrispondente al server SnapCenter che ospita l'applicazione e fare clic su **Aggiorna**.

   I nuovi volumi vengono scoperti.

4. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Refresh Protection** per attivare la protezione cloud per il nuovo volume.
   - Se un volume di storage viene aggiunto all'applicazione dopo la configurazione del provider cloud, il server SnapCenter etichetterà le snapshot per i nuovi backup su cui risiede l'applicazione.
   - È necessario eliminare manualmente la relazione dell'archivio di oggetti se il volume rimosso non viene utilizzato da altre applicazioni.
   - Se si aggiorna l'inventario delle applicazioni, esso conterrà il layout di storage corrente dell'applicazione.

Modifica di policy o gruppi di risorse

In caso di modifica del criterio SnapCenter o del gruppo di risorse, è necessario aggiornare la relazione di protezione.

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Fare clic su ••• Corrispondente all'applicazione e fare clic su **Refresh Protection** (Aggiorna protezione).

Annullare la registrazione del server SnapCenter

Fasi

1. Fare clic su **Backup and Recovery** > **applicazioni**.
2. Nell'elenco a discesa **Impostazioni**, fare clic su **Server SnapCenter**.
3. Fare clic su ••• Corrispondente al server SnapCenter e fare clic su **Annulla registrazione**.

   Per impostazione predefinita, la casella di controllo è selezionata ed elimina tutti i backup spostati nell'archivio di oggetti da SnapCenter e dall'archivio di oggetti.

Se si deseleziona la casella di controllo, i backup vengono conservati solo nell'archivio di oggetti, ma non possono essere utilizzati per il ripristino a livello di applicazione. Successivamente, quando si attiva il backup per questa applicazione, i backup conservati nell'archivio di oggetti non vengono elencati per il ripristino.

Monitorare i lavori

I job vengono creati per tutte le operazioni di Cloud Backup. È possibile monitorare tutti i lavori e tutte le sottoattività eseguite come parte di ciascuna attività.

Fasi

1. Fare clic su **Backup and Recovery** > **Job Monitoring**.

   Quando si avvia un'operazione, viene visualizzata una finestra che indica che il processo è stato avviato. È possibile fare clic sul collegamento per monitorare il lavoro.

2. Fare clic sull'attività principale per visualizzare le attività secondarie e lo stato di ciascuna di queste attività secondarie.

Configurare i certificati CA

È possibile configurare il certificato firmato dalla CA se si desidera includere ulteriore protezione nell'ambiente.

Configurare il certificato firmato dalla CA SnapCenter in BlueXP Connector

È necessario configurare il certificato firmato dalla CA SnapCenter in BlueXP Connector in modo che il connettore possa verificare il certificato di SnapCenter.

Prima di iniziare

Eseguire il seguente comando in BlueXP Connector per ottenere *<base_mount_path>*:

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Fasi

1. Accedere al connettore.
   ```
   cd <base_mount_path> mkdir -p server/certificate
   ```
2. Copiare i file CA principali e intermedi nella directory *<base_mount_path>/server/certificate*.

   I file CA devono essere in formato .pem.

3. Se si dispone di file CRL, attenersi alla seguente procedura:
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Copiare i file CRL nella directory *<base_mount_path>/server/crl*.
4. Connettersi a cloudmanager_snapcenter e modificare enableCACert in config.yml su true.
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert:
   false/enableCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. Riavviare il container Cloudmanager_snapcenter.
   ```
   sudo docker restart cloudmanager_snapcenter
   ```

Configurare il certificato firmato dalla CA per BlueXP Connector

Se il protocollo SSL bidirezionale è attivato in SnapCenter, attenersi alla seguente procedura sul connettore per utilizzare il certificato CA come certificato client quando il connettore si connette a SnapCenter.

Prima di iniziare

Eseguire il seguente comando per ottenere *<base_mount_path>*:

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Fasi

1. Accedere al connettore.
   ```
   cd <base_mount_path> mkdir -p client/certificate
   ```
2. Copiare il certificato e il file delle chiavi firmato dalla CA in *<base_mount_path>/client/certificate* nel connettore.

   Il nome del file deve essere certificate.pem e key.pem. Il file certificate.pem deve avere l'intera catena dei certificati, ad esempio CA intermedia e CA principale.

3. Creare il formato PKCS12 del certificato con il nome certificate.p12 e mantenere l'indirizzo *<base_mount_path>/client/certificate*.

   Esempio: openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12

4. Connettersi a cloudmanager_snapcenter e modificare sendCACert in config.yml su true.
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
   false/sendCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. Riavviare il container Cloudmanager_snapcenter.
   ```
   sudo docker restart cloudmanager_snapcenter
   ```
6. Per convalidare il certificato inviato dal connettore, eseguire le seguenti operazioni su SnapCenter.
   a. Accedere all'host del server SnapCenter.
   b. Fare clic su **Start** > **Avvia ricerca**.
   c. Digitare mmc e premere **Invio**.
   d. Fare clic su **Sì**.
   e. Nel menu file, fare clic su **Aggiungi/Rimuovi snap-in**.
   f. Fare clic su **certificati** > **Aggiungi** > **account computer** > **Avanti**.
   g. Fare clic su **computer locale** > **fine**.
   h. Se non si dispone di ulteriori snap-in da aggiungere alla console, fare clic su **OK**.
   i. Nella struttura della console, fare doppio clic su **certificati**.
   j. Fare clic con il pulsante destro del mouse sull'archivio **Trusted Root Certification Authorities**.
   k. Fare clic su **Import** (Importa) per importare i certificati e seguire la procedura descritta in **Certificate Import Wizard** (importazione guidata certificati).

Ripristinare i dati delle applicazioni on-premise

Ripristinare il database Oracle

È possibile ripristinare il database Oracle nella posizione originale o nella posizione alternativa. Per un database RAC, i dati vengono ripristinati nel nodo on-premise in cui è stato creato il backup.

È supportato solo il database completo con il ripristino del file di controllo. Se i log di archiviazione non sono presenti in AFS, specificare la posizione che contiene i log di archiviazione richiesti per il ripristino.

Single file Restore (SFR) non è supportato.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, selezionare il filtro **tipo** e dal menu a discesa selezionare **Oracle**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
4. Nella pagina delle opzioni di ripristino, specificare la posizione in cui si desidera ripristinare i file di database.

Se…	Eseguire questa operazione…
Ripristinare la posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Fare clic su **Avanti**. d. Selezionare **Database state** (Stato database) se si desidera modificare lo stato del database nello stato richiesto per eseguire le operazioni di ripristino e ripristino. I vari stati di un database, da quelli superiori a quelli inferiori, sono aperti, montati, avviati e arrestati. ◦ Se il database si trova in uno stato superiore ma lo stato deve essere modificato in uno stato inferiore per eseguire un'operazione di ripristino, selezionare questa casella di controllo. ◦ Se il database si trova in uno stato inferiore ma lo stato deve essere modificato in uno stato superiore per eseguire l'operazione di ripristino, lo stato del database viene modificato automaticamente anche se non si seleziona la casella di controllo. ◦ Se un database si trova in stato aperto e per il ripristino il database deve essere in stato montato, lo stato del database viene modificato solo se si seleziona questa casella di controllo. e. Specificare l'ambito del ripristino. ◦ Selezionare **All Logs** (tutti i registri) se si desidera ripristinare l'ultima transazione. ◦ Selezionare **fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico. ◦ Selezionare **Data e ora** se si desidera ripristinare dati e ore specifici. Specificare la data e l'ora del fuso orario dell'host del database. ◦ Selezionare **No recovery** se non si desidera eseguire il ripristino. f. Se i log di archiviazione non sono presenti nel file system attivo, specificare la posizione che contiene i log di archiviazione richiesti per il ripristino. Selezionare questa casella di controllo se si desidera aprire il database dopo il ripristino.

Se…	Eseguire questa operazione…
Ripristinare temporaneamente in un altro storage e copiare i file ripristinati nella posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. d. Fare clic su **Avanti**. e. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui i dati ripristinati dall'archivio di oggetti verranno memorizzati temporaneamente. Se si seleziona un sistema ONTAP on-premise e non si è configurata la connessione del cluster allo storage a oggetti, vengono richieste ulteriori informazioni relative all'archivio di oggetti. f. Fare clic su **Avanti**. g. Selezionare **Database state** (Stato database) se si desidera modificare lo stato del database nello stato richiesto per eseguire le operazioni di ripristino e ripristino. I vari stati di un database, da quelli superiori a quelli inferiori, sono aperti, montati, avviati e arrestati. ◦ Se il database si trova in uno stato superiore ma lo stato deve essere modificato in uno stato inferiore per eseguire un'operazione di ripristino, selezionare questa casella di controllo. ◦ Se il database si trova in uno stato inferiore ma lo stato deve essere modificato in uno stato superiore per eseguire l'operazione di ripristino, lo stato del database viene modificato automaticamente anche se non si seleziona la casella di controllo. ◦ Se un database si trova in stato aperto e per il ripristino il database deve essere in stato montato, lo stato del database viene modificato solo se si seleziona questa casella di controllo. Specificare l'ambito del ripristino. Selezionare **All Logs** (tutti i registri) se si

Se…	Eseguire questa operazione…
Ripristinare in una posizione alternativa	a. Selezionare **Ripristina in una posizione alternativa**. b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Se si desidera ripristinare lo storage alternativo, attenersi alla seguente procedura: i. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. ii. Fare clic su **Avanti**. iii. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui devono essere ripristinati i dati dell'archivio di oggetti. d. Fare clic su **Avanti**. e. Nella pagina Destination host (host di destinazione), selezionare l'host su cui verrà montato il database. i. (Facoltativo) per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti. ii. (Facoltativo) per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti. f. Fare clic su **Avanti**.

5. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

L'opzione **Restore to alternate location** (Ripristina in posizione alternativa) consente di montare il backup selezionato sull'host specificato. È necessario visualizzare manualmente il database.

Dopo aver montato il backup, non è possibile montarlo di nuovo fino a quando non viene smontato. È possibile utilizzare l'opzione **Unmount** dall'interfaccia utente per smontare il backup.

Per informazioni su come attivare il database Oracle, vedere "Articolo della Knowledge base".

Ripristinare il database di SQL Server

È possibile ripristinare il database di SQL Server nella posizione originale o nella posizione alternativa.

> Single file Restore (SFR), Recovery of log backups e reseed of Availability group non sono supportati.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, selezionare il filtro **tipo** e dal menu a discesa selezionare **SQL**.
3. Fare clic su **View Details** (Visualizza dettagli) per visualizzare tutti i backup disponibili.
4. Selezionare il backup e fare clic su **Restore** (Ripristina).
5. Nella pagina delle opzioni di ripristino, specificare la posizione in cui si desidera ripristinare i file di database.

Se…	Eseguire questa operazione…
Ripristinare la posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Fare clic su **Avanti**.
Ripristinare temporaneamente in un altro storage e copiare i file ripristinati nella posizione originale	a. Selezionare **Restore to original location** (Ripristina posizione originale). b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. d. Fare clic su **Avanti**. e. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui i dati ripristinati dall'archivio di oggetti verranno memorizzati temporaneamente. f. Fare clic su **Avanti**.

Se…	Eseguire questa operazione…
Ripristinare in una posizione alternativa	a. Selezionare **Ripristina in una posizione alternativa**. b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Fare clic su **Avanti**. d. Nella pagina host di destinazione, selezionare un nome host, specificare un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino. L'estensione del file fornita nel percorso alternativo deve essere uguale all'estensione del file di database originale. e. Fare clic su **Avanti**.

Se…	Eseguire questa operazione…
Ripristinare temporaneamente in un altro storage e copiare i file ripristinati nella posizione alternativa	a. Selezionare **Ripristina in una posizione alternativa**. b. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione. c. Selezionare **Modifica posizione di storage**. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. d. Fare clic su **Avanti**. e. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui i dati ripristinati dall'archivio di oggetti verranno memorizzati temporaneamente. f. Fare clic su **Avanti**. g. Nella pagina host di destinazione, selezionare un nome host, specificare un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino. L'estensione del file fornita nel percorso alternativo deve essere uguale all'estensione del file di database originale. h. Fare clic su **Avanti**.

6. Nell'opzione **Pre-Operations**, selezionare una delle seguenti opzioni:
   - Selezionare **sovrascrivere il database con lo stesso nome durante il ripristino** per ripristinare il database con lo stesso nome.
   - Selezionare **Mantieni impostazioni di replica del database SQL** per ripristinare il database e conservare le impostazioni di replica esistenti.
7. Nella sezione **Post-Operations**, per specificare lo stato del database per il ripristino di registri transazionali aggiuntivi, selezionare una delle seguenti opzioni:
   - Selezionare **operativo, ma non disponibile** se si stanno ripristinando tutti i backup necessari.

     Questo è il comportamento predefinito, che lascia il database pronto per l'uso eseguendo il rollback delle transazioni non assegnate. Non è possibile ripristinare ulteriori registri delle transazioni fino a quando non si crea un backup.
   - Selezionare **non operativo, ma disponibile** per lasciare il database non operativo senza eseguire il rollback delle transazioni non assegnate.

È possibile ripristinare ulteriori registri delle transazioni. Non è possibile utilizzare il database fino a quando non viene ripristinato.

- Selezionare **Read-only mode (modalità di sola lettura) e Available** (disponibile) per lasciare il database in modalità di sola lettura.

  Questa opzione annulla le transazioni non assegnate, ma salva le azioni non riuscite in un file di standby in modo che gli effetti di ripristino possano essere ripristinati.

Se l'opzione Undo directory (Annulla directory) è attivata, vengono ripristinati altri log delle transazioni. Se l'operazione di ripristino del log delle transazioni non riesce, è possibile eseguire il rollback delle modifiche. La documentazione di SQL Server contiene ulteriori informazioni.

8. Fare clic su **Avanti**.
9. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Ripristinare il database SAP HANA

È possibile ripristinare il database SAP HANA su qualsiasi host.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, selezionare il filtro **tipo** e dal menu a discesa selezionare **HANA**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
4. Nella pagina delle opzioni di ripristino, specificare una delle seguenti opzioni:
   a. Per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti.
   b. Per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti.
5. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione.
6. Se lo spazio disponibile sullo storage di origine non è sufficiente o se lo storage di origine non è disponibile, selezionare **Modifica ubicazione dello storage**.

   Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione.

7. Fare clic su **Avanti**.
8. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui verranno memorizzati i dati ripristinati dall'archivio di oggetti.
9. Fare clic su **Avanti**.
10. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Questa operazione esegue solo l'esportazione dello storage del backup selezionato sull'host specificato. Si consiglia di montare manualmente il file system e di visualizzare il database. Dopo aver utilizzato il volume, l'amministratore dello storage può eliminare il volume dal cluster ONTAP.

Per informazioni su come attivare il database SAP HANA, vedere "TR-4667: Panoramica del workflow di copia del sistema SAP con SnapCenter" e. "TR-4667: Panoramica del workflow dei cloni di sistema SAP con SnapCenter".

Ripristino dei database MongoDB, MySQL e PostgreSQL

È possibile ripristinare i database MongoDB, MySQL e PostgreSQL su qualsiasi host.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection** > **Backup and Recovery** > **Applications**.
2. Nel campo **Filtra per**, seleziona il filtro **tipo** e dal menu a discesa seleziona **MongoDB**, **MySQL** o **PostgreSQL**.
3. Fare clic su **View Details** (Visualizza dettagli) corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
4. Nella pagina delle opzioni di ripristino, specificare una delle seguenti opzioni:
   a. Per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti.
   b. Per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti.
5. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione.
6. Se lo spazio disponibile sullo storage di origine non è sufficiente o se lo storage di origine non è disponibile, selezionare **Modifica ubicazione dello storage**.

   Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione.
7. Fare clic su **Avanti**.
8. Nella pagina Storage mapping, specificare i dettagli della posizione di storage alternativa in cui verranno memorizzati i dati ripristinati dall'archivio di oggetti.
9. Fare clic su **Avanti**.
10. Esaminare i dettagli e fare clic su **Restore** (Ripristina).

Questa operazione esegue solo l'esportazione dello storage del backup selezionato sull'host specificato. Si consiglia di montare manualmente il file system e di visualizzare il database. Dopo aver utilizzato il volume, l'amministratore dello storage può eliminare il volume dal cluster ONTAP.

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.