



Backup e ripristino dei dati delle applicazioni native del cloud

BlueXP backup and recovery

NetApp
April 18, 2024

Sommario

- Backup e ripristino dei dati delle applicazioni native del cloud 1
 - Proteggi i dati delle tue applicazioni native del cloud 1
 - Eseguire il backup dei database Oracle nativi del cloud 5
 - Eseguire il backup dei database SAP HANA nativi del cloud 18
 - Eseguire il backup di database SQL Server nativi per il cloud utilizzando le API REST 27
 - Ripristinare i database Oracle nativi del cloud 39
 - Ripristinare i database SAP HANA nativi del cloud 41
 - Ripristinare il database Microsoft SQL Server 43
 - Clonare i database Oracle nativi del cloud 46
 - Aggiornare il sistema di destinazione SAP HANA 54
 - Gestire la protezione dei dati applicativi nativi del cloud 56

Backup e ripristino dei dati delle applicazioni native del cloud

Proteggi i dati delle tue applicazioni native del cloud

Il backup e ripristino BlueXP per le applicazioni offre funzionalità di protezione dei dati coerenti per le applicazioni eseguite sullo storage cloud NetApp. Il backup e ripristino BlueXP offre una protezione efficiente, coerente con l'applicazione e basata su policy delle seguenti applicazioni:

- Database Oracle residenti su Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP e Azure NetApp Files
- Sistemi SAP HANA che risiedono su Azure NetApp Files
- Database Microsoft SQL Server residenti in Amazon FSX per NetApp ONTAP

Architettura

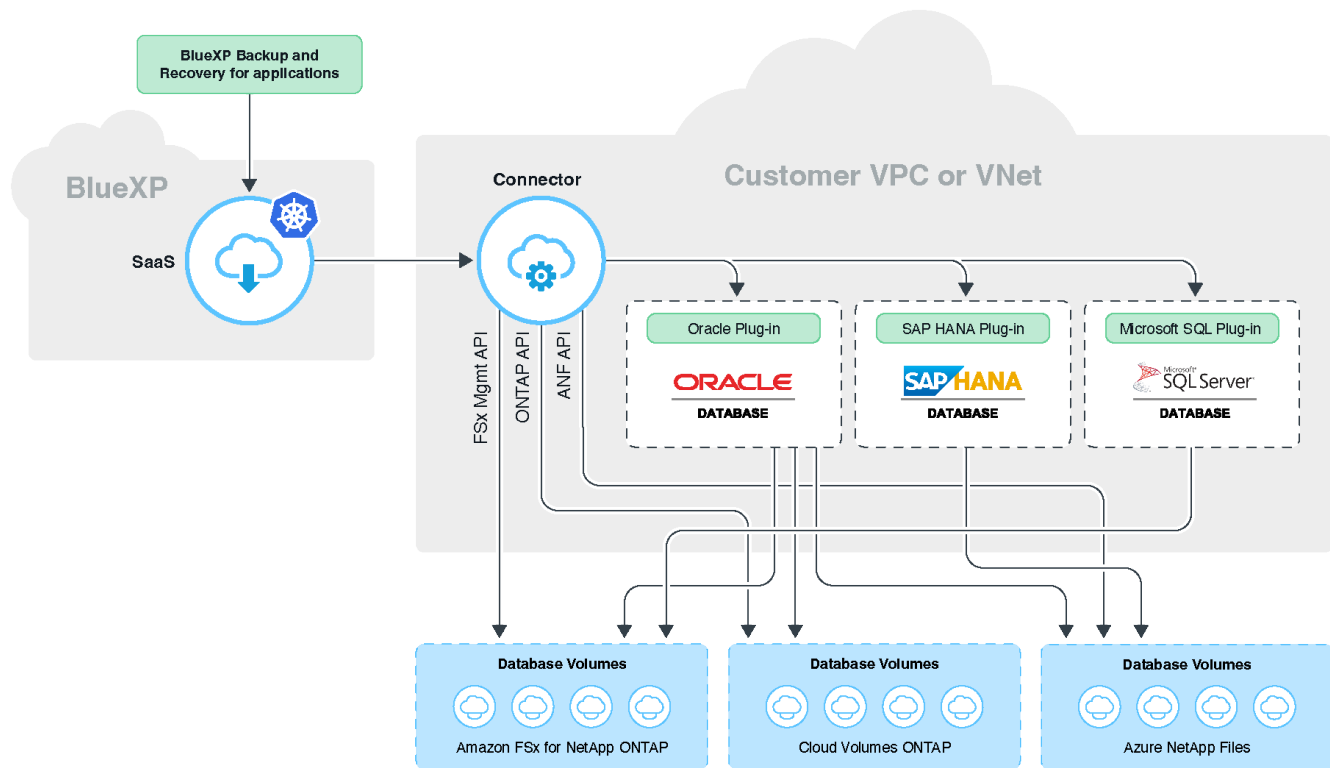
Il backup e ripristino BlueXP per l'architettura delle applicazioni include i seguenti componenti.

- Il backup e ripristino BlueXP è un insieme di servizi di protezione dei dati ospitati come servizio SaaS da NetApp e si basa sulla piattaforma BlueXP SaaS.

Orchestrano i flussi di lavoro per la protezione dei dati per le applicazioni che risiedono su NetApp Cloud Storage.

- L'interfaccia utente di BlueXP offre funzionalità di protezione dei dati per le applicazioni ed è accessibile dall'interfaccia utente di BlueXP.
- BlueXP Connector è un componente che viene eseguito nella rete cloud e interagisce con i sistemi storage e i plug-in specifici dell'applicazione.
- Il plug-in specifico dell'applicazione è un componente che viene eseguito su ciascun host dell'applicazione e interagisce con i database in esecuzione sull'host durante le operazioni di protezione dei dati.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



Per qualsiasi richiesta avviata dall'utente, l'interfaccia utente di BlueXP comunica con BlueXP SaaS che, dopo la convalida della richiesta, elabora lo stesso. Se la richiesta consiste nell'eseguire un flusso di lavoro, ad esempio un backup, un ripristino o un clone, il servizio SaaS avvia il flusso di lavoro e, se necessario, inoltra la chiamata a BlueXP Connector. Il connettore comunica quindi con il sistema di storage e il plug-in specifico dell'applicazione durante l'esecuzione delle attività del flusso di lavoro.

Il connettore può essere implementato nello stesso VPC o VNET delle applicazioni o in un altro. Se il connettore e le applicazioni si trovano su una rete diversa, è necessario stabilire una connettività di rete tra di essi.



Un singolo connettore BlueXP è in grado di comunicare con più sistemi storage e plug-in di applicazioni. Per gestire le applicazioni è necessario un unico connettore, purché vi sia connettività tra il connettore e gli host delle applicazioni.



L'infrastruttura BlueXP SaaS è resiliente ai guasti delle zone di disponibilità all'interno di una regione. Supporta i guasti regionali eseguendo il failover in una nuova regione e questo failover comporta un downtime di circa 2 ore.

Proteggere i database Oracle

Caratteristiche

- Aggiungere host e implementare il plug-in

È possibile implementare il plug-in utilizzando l'interfaccia utente, lo script o manualmente.

- Rilevamento automatico dei database Oracle

- Backup dei database Oracle che risiedono su Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP e Azure NetApp Files
 - Backup completo (dati + controllo + file di log di archiviazione)
 - Backup on-demand
 - Backup pianificato in base ai criteri definiti dal sistema o personalizzati

È possibile specificare diverse frequenze di pianificazione, ad esempio oraria, giornaliera, settimanale e mensile, nella policy. È inoltre possibile specificare gli script successivi che verranno eseguiti dopo il backup per copiare lo snapshot nello storage secondario.

- I backup dei database Oracle su Azure NetApp Files possono essere catalogati utilizzando Oracle RMAN
- Conservazione dei backup in base alla policy
- Ripristino dei database Oracle residenti su Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP e Azure NetApp Files
 - Ripristino del database Oracle completo (file di dati + file di controllo) dal backup specificato
 - Ripristino del database Oracle con fino a SCN, fino al momento, tutti i registri disponibili e nessuna opzione di ripristino
- Ripristino dei database Oracle su Azure NetApp Files in una posizione alternativa
- Clonazione di database Oracle residenti su Amazon FSX per NetApp ONTAP e Cloud Volumes ONTAP su host di destinazione di origine o alternativi
 - Clone di base con un click
 - Cloning avanzato con file di specifica del clone personalizzato
 - Il nome delle entità clonate può essere generato automaticamente o identico all'origine
 - Visualizzazione della gerarchia di cloni
 - Eliminazione dei database clonati
- Monitoraggio di backup, ripristino, clonazione e altri processi
- Visualizzazione del riepilogo della protezione sul dashboard
- Invio di avvisi tramite e-mail
- Aggiornare il plug-in host

Limitazioni

- Non supporta Oracle 11g
- Non supporta operazioni di montaggio, catalogo e verifica sui backup
- Non supporta Oracle su RAC e Data Guard
- Per Cloud Volumes ONTAP ha, viene utilizzato solo uno degli IP dell'interfaccia di rete. Se la connettività dell'IP non è disponibile o non è possibile accedere all'IP, le operazioni di protezione dei dati non vengono eseguite correttamente.
- Gli indirizzi IP dell'interfaccia di rete di Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP devono essere univoci nell'account e nella regione BlueXP.

Proteggere i database SAP HANA

Caratteristiche

- Aggiungere manualmente i sistemi SAP HANA
- Backup dei database SAP HANA
 - Backup on-demand (basato su file e copia Snapshot)
 - Backup pianificato in base ai criteri definiti dal sistema o personalizzati

È possibile specificare diverse frequenze di pianificazione, ad esempio oraria, giornaliera, settimanale e mensile, nella policy.

- Compatibile con HANA System Replication (HSR)
- Conservazione dei backup in base alla policy
- Ripristino del database SAP HANA completo dal backup specificato
- Backup e ripristino di volumi non dati HANA e volumi non dati globali
- Supporto Prescript e postscript utilizzando variabili ambientali per le operazioni di backup e ripristino
- Creazione di un piano d'azione per gli scenari di guasto utilizzando l'opzione pre-exit

Limitazioni

- Per la configurazione HSR, è supportato solo HSR a 2 nodi (1 primario e 1 secondario)
- La conservazione non viene attivata se il postscript non riesce durante l'operazione di ripristino

Proteggere il database di Microsoft SQL Server

Caratteristiche

- Aggiungere manualmente l'host e distribuire il plug-in
- Rilevare i database manualmente
- Eseguire il backup delle istanze di SQL Server che risiedono in Amazon FSX per NetApp ONTAP
 - Backup on-demand
 - Backup pianificato in base al criterio
 - Backup del registro dell'istanza di Microsoft SQL Server
- Ripristinare il database nella posizione originale

Limitazioni

- Il backup è supportato solo per le istanze di SQL Server
- La configurazione di istanza cluster di failover (FCI) non è supportata
- L'interfaccia utente di BlueXP non supporta operazioni specifiche del database SQL

Tutte le operazioni specifiche dei database Microsoft SQL Server vengono eseguite tramite API REST.

- Il ripristino in una posizione alternativa non è supportato

Eseguire il backup dei database Oracle nativi del cloud

Avvio rapido

Inizia subito seguendo questa procedura.

1

Verificare il supporto per la configurazione

- Sistema operativo:
 - RHEL 7.5 o versione successiva e 8.x.
 - OL 7.5 o versione successiva e 8.x
 - SLES 15 SP4
- Cloud storage NetApp:
 - Amazon FSX per NetApp ONTAP
 - Cloud Volumes ONTAP
 - Azure NetApp Files
- Layout dello storage:
 - NFS v3 e v4.1 (incluso DNFS)
 - iSCSI con ASM (ASMFD, ASMLib e ASMUdev)



Azure NetApp Files non supporta l'ambiente SAN.

- Layout dei database: Oracle Standard e Oracle Enterprise standalone (CDB e PDB legacy e multi-tenant)
- Versioni di database: 19c e 21c

2

Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a ["Iscriviti a BlueXP"](#).

3

Accedere a BlueXP

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a ["Accedere a BlueXP"](#).

4

Gestisci il tuo account BlueXP

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a ["Gestisci il tuo account BlueXP"](#).

Configurare FSX per ONTAP

Con BlueXP è necessario creare un ambiente di lavoro FSX per ONTAP per aggiungere

e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro FSX per ONTAP

È necessario creare FSX per ambienti di lavoro ONTAP in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a ["Inizia a utilizzare Amazon FSX per ONTAP"](#) e ["Creare e gestire un ambiente di lavoro Amazon FSX per ONTAP"](#).

È possibile creare l'ambiente di lavoro FSX per ONTAP utilizzando BlueXP o AWS. Se hai creato utilizzando AWS, dovresti scoprire FSX per i sistemi ONTAP in BlueXP.

Creare un connettore

Un account Admin deve creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a ["Creazione di un connettore in AWS da BlueXP"](#).

- È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro FSX per ONTAP che i database.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e dei database nello stesso cloud privato virtuale (VPC), è possibile implementare il connettore nello stesso VPC.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e di database in diversi VPC:
 - Se si dispone di carichi di lavoro NAS (NFS) configurati su FSX per ONTAP, è possibile creare il connettore su uno dei VPC.
 - Se si hanno solo carichi di lavoro SAN configurati e non si intende utilizzare carichi di lavoro NAS (NFS), è necessario creare il connettore nel VPC in cui viene creato il sistema FSX per ONTAP.



Per utilizzare i carichi di lavoro NAS (NFS), è necessario disporre di un gateway di transito tra il VPC del database e Amazon VPC. È possibile accedere all'indirizzo IP NFS, che è un indirizzo IP mobile, da un altro VPC solo attraverso il gateway di transito. Non è possibile accedere agli indirizzi IP mobili eseguendo il peering dei VPC.

Dopo aver creato il connettore, fare clic su **Storage > Canvas > My Working Environments > Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni per aggiungere l'ambiente di lavoro. Assicurarsi che vi sia connettività dal connettore agli host del database Oracle e all'ambiente di lavoro FSX. Il connettore dovrebbe essere in grado di connettersi all'indirizzo IP di gestione del cluster dell'ambiente di lavoro FSX.

- Aggiungere l'ambiente di lavoro facendo clic su **Storage > Canvas > My Working Environments > Add Working Environment**.

Assicurarsi che vi sia connettività dal connettore agli host del database e all'ambiente di lavoro FSX per ONTAP. Il connettore deve connettersi all'indirizzo IP di gestione del cluster di FSX per l'ambiente di lavoro ONTAP.

- Copiare l'ID del connettore facendo clic su **Connector > Manage Connectors** (connettore > Gestisci connettori) e selezionando il nome del connettore.

Configurare Cloud Volumes ONTAP

Con BlueXP è necessario creare un ambiente di lavoro Cloud Volumes ONTAP per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore per il proprio ambiente cloud che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Cloud Volumes ONTAP

È possibile individuare e aggiungere sistemi Cloud Volumes ONTAP esistenti a BlueXP. Per ulteriori informazioni, fare riferimento a. ["Aggiunta di sistemi Cloud Volumes ONTAP esistenti a BlueXP"](#).

Creare un connettore

Puoi iniziare a utilizzare Cloud Volumes ONTAP per il tuo ambiente cloud in pochi passaggi. Per ulteriori informazioni, fare riferimento a una delle seguenti voci:

- ["Avvio rapido di Cloud Volumes ONTAP in AWS"](#)
- ["Avvio rapido di Cloud Volumes ONTAP in Azure"](#)
- ["Guida rapida per Cloud Volumes ONTAP in Google Cloud"](#)

È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro Cloud Volumes ONTAP che i database.

- Se l'ambiente di lavoro Cloud Volumes ONTAP e i database si trovano nello stesso cloud privato virtuale (VPC) o VNET, è possibile implementare il connettore nello stesso VPC o VNET.
- Se si dispone di un ambiente di lavoro Cloud Volumes ONTAP e di database in VPC o VNet diversi, assicurarsi che i VPC o VNet siano peering.

Configurare Azure NetApp Files

Con BlueXP è necessario creare un ambiente di lavoro Azure NetApp Files per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Azure NetApp Files

È necessario creare ambienti di lavoro Azure NetApp Files in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. ["Scopri di più su Azure NetApp Files"](#) e ["Creare un ambiente di lavoro Azure NetApp Files"](#).

Creare un connettore

Un amministratore di account BlueXP dovrebbe implementare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. ["Creare un connettore in Azure da BlueXP"](#).

- Assicurarsi che vi sia connettività tra il connettore e gli host del database.

- Se si dispone dell'ambiente di lavoro e dei database Azure NetApp Files nella stessa rete virtuale (VNET), è possibile implementare il connettore nella stessa rete virtuale.
- Se si dispone di un ambiente di lavoro Azure NetApp Files e di database in reti VNet diverse e si hanno carichi di lavoro NAS (NFS) configurati su Azure NetApp Files, è possibile creare il connettore su una delle reti VNet.

Dopo aver creato il connettore, aggiungere l'ambiente di lavoro facendo clic su **Storage > Canvas > My Working Environments > Add Working Environment**.

Installare il plug-in SnapCenter per Oracle e aggiungere host di database

È necessario installare il plug-in SnapCenter per Oracle su ciascuno degli host di database Oracle, aggiungere gli host di database e rilevare i database sull'host per assegnare criteri e creare backup.

- Se SSH è attivato per l'host del database, è possibile installare il plug-in utilizzando uno dei seguenti metodi:
 - Installare il plug-in e aggiungere l'host dall'interfaccia utente utilizzando l'opzione SSH. [Scopri di più](#).
 - Installare il plug-in utilizzando lo script e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale. [Scopri di più](#).
- Se SSH è disattivato, installare il plug-in manualmente e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale. [Scopri di più](#).

Prerequisiti

Prima di aggiungere l'host, assicurarsi che i prerequisiti siano soddisfatti.

- L'ambiente di lavoro e il connettore dovrebbero essere stati creati.
- Assicurarsi che il connettore sia collegato agli host del database Oracle.

Per informazioni su come risolvere il problema di connettività, fare riferimento a. ["Impossibile convalidare la connettività dall'host del connettore BlueXP all'host del database dell'applicazione"](#).

Quando il connettore viene perso o se è stato creato un nuovo connettore, è necessario associarlo alle risorse dell'applicazione esistenti. Per istruzioni sull'aggiornamento del connettore, vedere ["Aggiornare i dettagli del connettore"](#).

- Assicurarsi che l'utente BlueXP abbia il ruolo di "account Admin".
- Assicurarsi che l'account non root (sudo) sia presente sull'host dell'applicazione per le operazioni di protezione dei dati.
- Assicurarsi che Java 11 (64-bit) Oracle Java o OpenJDK sia installato su ciascuno degli host di database Oracle e che LA variabile JAVA_HOME sia impostata correttamente.
- Se viene eseguita l'installazione basata su SSH, assicurarsi che il connettore abbia attivato la comunicazione con la porta SSH (impostazione predefinita: 22).
- Assicurarsi che il connettore abbia la comunicazione abilitata alla porta plug-in (impostazione predefinita: 8145) per il funzionamento delle operazioni di protezione dei dati.
- Assicurarsi che sia installata la versione più recente del plug-in. Per aggiornare il plug-in, fare riferimento a. [Upgrade del plug-in SnapCenter per database Oracle](#).

Aggiungere host dall'interfaccia utente utilizzando l'opzione SSH

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.

Se è già stato aggiunto un host e si desidera aggiungere un altro host, fare clic su **applicazioni > Gestisci database > Aggiungi**, quindi passare al punto 5.

2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

Viene creato un account di servizio (*SnapCenter-account-<accountid>*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-<accountid>*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account > Gestisci account > membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina host details (Dettagli host), eseguire le seguenti operazioni:

- a. Selezionare **utilizzando SSH**.
- b. Specificare l'FQDN o l'indirizzo IP dell'host in cui si desidera installare il plug-in.

Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

- c. Specificare l'utente non root(sudo) che utilizza il pacchetto del plug-in da copiare sull'host.

L'utente root non è supportato.

- d. Specificare la porta SSH e il plug-in.

La porta SSH predefinita è 22 e la porta plug-in è 8145.

Dopo aver installato il plug-in, è possibile chiudere la porta SSH sull'host dell'applicazione. La porta SSH non è necessaria per le operazioni di protezione dei dati.

- a. Selezionare il connettore.
- b. (Facoltativo) se l'autenticazione senza chiave non è abilitata tra il connettore e l'host, specificare la chiave privata SSH che verrà utilizzata per comunicare con l'host.



La chiave privata SSH non viene memorizzata nell'applicazione e non viene utilizzata per altre operazioni.

- c. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:
 - a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
 - b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
 - c. Creare il file `/etc/sudoers.d/snapcenter` sulla macchina Linux e incollare il testo copiato.

d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.

7. Esaminare i dettagli e fare clic su **Scopri applicazioni**.

- Una volta installato il plug-in, viene avviata l'operazione di rilevamento.
- Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a [Configurare le credenziali del database Oracle](#).
- Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
- Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Aggiungere host dall'interfaccia utente utilizzando l'opzione manuale e installare il plug-in utilizzando lo script

Configurare l'autenticazione basata su chiave SSH per l'account utente non root dell'host Oracle ed eseguire i seguenti passaggi per installare il plug-in.

Prima di iniziare

Assicurarsi che la connessione SSH al connettore sia attivata.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

Viene creato un account di servizio (*SnapCenter-account-`<accountid>`*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-`<accountid>`*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account > Gestisci account > membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina host details (Dettagli host), eseguire le seguenti operazioni:
 - a. Selezionare **Manuale**.
 - b. Specificare l'FQDN o l'indirizzo IP dell'host in cui è installato il plug-in.

Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

- c. Specificare la porta del plug-in.

La porta predefinita è 8145.

- d. Specificare l'utente non root (sudo) che utilizza il pacchetto del plug-in da copiare sull'host.
 - e. Selezionare il connettore.
 - f. Selezionare la casella di controllo per confermare che il plug-in è installato sull'host.
 - g. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:

- a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
- b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.
- c. Creare il file `/etc/sudoers.d/snapcenter` sulla macchina Linux e incollare il testo copiato.
- d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.

7. Accedere a Connector VM.

8. Installare il plug-in utilizzando lo script fornito nel connettore.

```
sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

Se si utilizza un connettore meno recente, eseguire il seguente comando per installare il plug-in.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Nome	Descrizione	Obbligatorio	Predefinito
plugin_host	Specifica l'host Oracle	Sì	-
nome_utente_host	Specifica l'utente SnapCenter con privilegi SSH sull'host Oracle	Sì	-
host_ssh_key	Specifica la chiave SSH dell'utente SnapCenter e viene utilizzata per connettersi all'host Oracle	Sì	-
porta_plugin	Specifica la porta utilizzata dal plug-in	No	8145
host_ssh_port	Specifica la porta SSH sull'host Oracle	No	22

Ad esempio:

- ° `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`
- ° `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. Nell'interfaccia utente di BlueXP, esaminare i dettagli e fare clic su **Scopri applicazioni**.
 - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a. [Configurare le credenziali del database Oracle](#).
 - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
 - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Aggiungere host dall'interfaccia utente utilizzando l'opzione manuale e installare il plug-in manualmente

Se l'autenticazione basata su chiave SSH non è abilitata sull'host del database Oracle, attenersi alla seguente procedura manuale per installare il plug-in e aggiungere l'host dall'interfaccia utente utilizzando l'opzione manuale.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native** e fare clic su **Next**.

Viene creato un account di servizio (*SnapCenter-account-`<accountid>`*) con ruolo *sistema SnapCenter* per eseguire operazioni pianificate di protezione dei dati per tutti gli utenti di questo account. L'account del servizio (*SnapCenter-account-`<accountid>`*) viene utilizzato per eseguire le operazioni di backup pianificate. Non eliminare mai l'account del servizio. Per visualizzare l'account del servizio, fare clic su **account > Gestisci account > membri**.

4. Selezionare Oracle come tipo di applicazione.
5. Nella pagina **Dettagli host**, eseguire le seguenti operazioni:
 - a. Selezionare **Manuale**.
 - b. Specificare l'FQDN o l'indirizzo IP dell'host in cui è installato il plug-in.

Assicurarsi che il connettore sia in grado di comunicare con l'host del database utilizzando l'FQDN o l'indirizzo IP.

- c. Specificare la porta del plug-in.

La porta predefinita è 8145.

- d. Specificare l'utente sudo non-root (sudo) che utilizza il pacchetto del plug-in da copiare sull'host.
- e. Selezionare il connettore.
- f. Selezionare la casella di controllo per confermare che il plug-in è installato sull'host.
- g. Fare clic su **Avanti**.
6. Nella pagina di configurazione, eseguire le seguenti operazioni:
 - a. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle.
 - b. Copiare il testo visualizzato nell'interfaccia utente di BlueXP.

- c. Creare il file `/etc/sudoers.d/snapcenter` sulla macchina Linux e incollare il testo copiato.
 - d. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su **Avanti**.
7. Accedere a Connector VM.
 8. Scarica il binario del plug-in host Linux di SnapCenter.


```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

Il binario del plug-in è disponibile all'indirizzo: `cd /var/lib/docker/Volumes/service-manager[1]-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po "cloudmanager_scs_cloud:.?*"|sed -e/ */|cut -f2 -d":")/sc-linux-host-plugin`
 9. Copiare `snapcenter_linux_host_plugin_scs.bin` dal percorso sopra indicato al percorso `/home/<non root user>/.sc_netapp` per ciascuno degli host di database Oracle utilizzando metodi scp o altri metodi alternativi.
 10. Accedere all'host del database Oracle utilizzando l'account non root (sudo).
 11. Modificare la directory in `/home/<non root user>/.sc_netapp/` ed eseguire il seguente comando per abilitare le autorizzazioni di esecuzione per il file binario.


```
chmod +x snapcenter_linux_host_plugin_scs.bin
```
 12. Installare il plug-in Oracle come utente sudo SnapCenter.


```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```
 13. Copiare `certificate.pem` dal percorso `<base_mount_path>/client/certificate/` del connettore VM a `/var/opt/snapcenter/spl/etc/` sull'host plug-in.
 14. Andare a `/var/opt/snapcenter/spl/etc` ed eseguire il comando `keytool` per importare il file `certificate.pem`.


```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks -deststorepass snapcenter -noprompt
```
 15. Riavviare SPL: `systemctl restart spl`
 16. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.


```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/PluginService/Version --cert /config/client/certificate/certificate.pem --key /config/client/certificate/key.pem
```
 17. Nell'interfaccia utente di BlueXP, esaminare i dettagli e fare clic su **Scopri applicazioni**.
 - Al termine dell'operazione di rilevamento, vengono visualizzati tutti i database sull'host. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per attivare l'autenticazione del database. Per ulteriori informazioni, fare riferimento a [Configurare le credenziali del database Oracle](#).
 - Fare clic su **Impostazioni** e selezionare **host** per visualizzare tutti gli host.
 - Fare clic su **Impostazioni** e selezionare **Criteri** per visualizzare i criteri predefiniti. Esaminare le policy predefinite e modificarle per soddisfare i requisiti o creare una nuova policy.

Configurare le credenziali del database Oracle

È necessario configurare le credenziali del database utilizzate per eseguire operazioni di protezione dei dati sui database Oracle.

Fasi

1. Se l'autenticazione del sistema operativo per il database è disattivata, fare clic su **Configura** per modificare l'autenticazione del database.
2. Specificare il nome utente, la password e i dettagli della porta.

Se il database risiede in ASM, è necessario configurare anche le impostazioni ASM.

L'utente Oracle deve disporre dei privilegi sysdba e l'utente ASM deve disporre dei privilegi sysasm.

3. Fare clic su **Configura**.

Upgrade del plug-in SnapCenter per database Oracle

È necessario aggiornare il plug-in SnapCenter per Oracle per accedere alle nuove funzionalità e ai miglioramenti più recenti. È possibile eseguire l'aggiornamento dall'interfaccia utente di BlueXP o dalla riga di comando.

Prima di iniziare

- Assicurarsi che non vi siano operazioni in esecuzione sull'host.

Fasi

1. Fare clic su **Backup and Recovery > applicazioni > host**.
2. Verificare se l'aggiornamento del plug-in è disponibile per uno degli host controllando la colonna Stato generale.
3. Aggiornare il plug-in dall'interfaccia utente o utilizzando la riga di comando.

Eseguire l'aggiornamento utilizzando l'interfaccia utente	Eseguire l'aggiornamento utilizzando la riga di comando
<p>a. Fare clic su ... Corrispondente all'host e fare clic su Upgrade Plug-in.</p> <p>b. Nella pagina di configurazione, eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> i. Configurare l'accesso sudo per l'utente SnapCenter nell'host del database Oracle effettuando l'accesso alla macchina Linux che esegue il database Oracle. ii. Copiare il testo visualizzato nell'interfaccia utente di BlueXP. iii. Modificare il file <code>/etc/sudoers.d/snapcenter</code> sulla macchina Linux e incollare il testo copiato. iv. Nell'interfaccia utente di BlueXP, selezionare la casella di controllo e fare clic su Upgrade (Aggiorna). 	<p>a. Accedere a Connector VM.</p> <p>b. Eseguire il seguente script.</p> <pre>sudo /var/lib/docker/volumes/service- manager- 2_cloudmanager_scs_cloud_volume/_da ta/scripts/linux_plugin_copy_and_in stall.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade</pre> <p>Se si utilizza un connettore meno recente, eseguire il seguente comando per aggiornare il plug-in.</p> <pre>sudo /var/lib/docker/volumes/cloudmanage r_scs_cloud_volume/_data/scripts/li nux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade</pre>

Eseguire il backup dei database Oracle nativi del cloud

È possibile creare backup pianificati o on-demand assegnando un criterio predefinito o il criterio creato.

È inoltre possibile catalogare i backup del database Oracle utilizzando Oracle Recovery Manager (RMAN) se è stata attivata la catalogazione durante la creazione di una policy. La catalogazione (RMAN) è supportata solo per i database su Azure NetApp Files. I backup catalogati possono essere utilizzati in seguito per operazioni di ripristino a livello di blocco o tablespace point-in-time. Il database deve essere in stato montato o superiore per la catalogazione.

Creare policy per proteggere il database Oracle

È possibile creare policy se non si desidera modificare le policy predefinite.

Fasi

1. Nella pagina applicazioni, dall'elenco a discesa Impostazioni, selezionare **Criteri**.
2. Fare clic su **Crea policy**.
3. Specificare un nome di policy.

4. (Facoltativo) modificare il formato del nome del backup.
5. Specificare la pianificazione e i dettagli di conservazione.
6. Se hai selezionato *daily* e *settimanalmente* come programma e desideri attivare la catalogazione RMAN, seleziona **Catalog backup with Oracle Recovery Manager (RMAN)**.
7. (Facoltativo) inserire il percorso post-script e il valore di timeout per il post-script che verrà eseguito dopo il backup corretto, ad esempio la copia dello snapshot nello storage secondario.

In alternativa, è possibile specificare anche gli argomenti.

I post-script devono essere contenuti nel percorso `/var/opt/snapcenter/spl/scripts`.

Lo script post supporta un set di variabili di ambiente.

Variabile ambientale	Descrizione
SC_ORACLE_SID	Specifica il SID del database Oracle.
HOST_SC	Specifica il nome host del database
NOME_BACKUP_SC	Specifica il nome del backup. Il nome del backup dei dati e il nome del backup del registro vengono concatenati mediante delimitatori.
NOME_POLICY_BACKUP_SC	Specifica il nome del criterio utilizzato per creare il backup.
PERCORSO_COMPLETO_VOLUME_DATI_PRIMARI_SC	<p>Specifica i percorsi dei volumi di dati concatenati utilizzando "," come delimitatore. Per i volumi Azure NetApp Files, le informazioni vengono concatenate utilizzando "/"</p> <p>— /Subscriptions/{subscription_id}/resourceGroups/{resource_group}/provider/{provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumeame{}</p>
SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH	<p>Specifica i percorsi dei volumi del log di archiviazione concatenati utilizzando "," come delimitatore. Per i volumi Azure NetApp Files, le informazioni vengono concatenate utilizzando "/"</p> <p>— /Subscriptions/{subscription_id}/resourceGroups/{resource_group}/provider/{provider}/netAppAccounts/{anfaccount}/capacityPools/{Capacity_pool}/volumeame{}</p>

8. Fare clic su **Create** (Crea).


Configurare il repository del catalogo RMAN

È possibile configurare il database del catalogo di ripristino come repository del catalogo RMAN. Se non si configura il repository, per impostazione predefinita, il file di controllo del database di destinazione diventa il repository del catalogo RMAN.

Prima di iniziare

Registrare manualmente il database di destinazione con il database del catalogo RMAN.

Fasi

1. Nella pagina applicazioni, fare clic su  > **Visualizza dettagli**.
2. Nella sezione Database details (Dettagli database), fare clic su  Per configurare il repository del catalogo RMAN.
3. Specificare le credenziali per catalogare i backup con RMAN e il nome TNS (transparent Network substrate) del database di ripristino del catalogo.
4. Fare clic su **Configura**.

Creare un backup del database Oracle


È possibile assegnare un criterio predefinito o creare un criterio e assegnarlo al database. Una volta assegnato il criterio, i backup vengono creati in base alla pianificazione definita nel criterio.



Quando si creano diskgroup ASM su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP, assicurarsi che non vi siano volumi comuni tra i diskgroup. Ogni gruppo di dischi deve disporre di volumi dedicati.

Fasi

1. Nella pagina applicazioni, se il database non è protetto mediante criteri, fare clic su **Assegna policy**.

Se il database è protetto mediante uno o più criteri, è possibile assegnare ulteriori criteri facendo clic su  > **Assegna policy**.
2. Selezionare il criterio e fare clic su **Assegna**.

I backup verranno creati in base alla pianificazione definita nella policy. Se è stato abilitato il catalogo RMAN nella policy, il backup alla fine del workflow avvierà l'operazione di catalogazione come un lavoro separato. L'avanzamento della catalogazione è visibile da Job Monitor. Una volta completata la catalogazione, **Backup Details** mostrerà lo stato del catalogo per ciascun backup.




L'account del servizio (*SnapCenter-account-`<account_id>`*) viene utilizzato per eseguire le operazioni di backup pianificate.

Creazione di backup on-demand del database Oracle

Dopo aver assegnato il criterio, è possibile creare un backup on-demand dell'applicazione.

Fasi

1. Nella pagina applicazioni, fare clic su  Corrispondente all'applicazione e fare clic su **Backup on-Demand**.

2. Se all'applicazione sono assegnati più criteri, selezionare il criterio, il livello di conservazione e fare clic su **Create Backup** (Crea backup).

Se è stato abilitato il catalogo RMAN nella policy, il backup alla fine del workflow avvierà l'operazione di catalogazione come un lavoro separato. L'avanzamento della catalogazione è visibile da Job Monitor. Una volta completata la catalogazione, **Backup Details** mostrerà lo stato del catalogo per ciascun backup.

Limitazioni

- Non supporta snapshot di gruppi di coerenza per database Oracle che risiedono su più gruppi di dischi ASM con sovrapposizione di volumi FSX
- Se i database Oracle si trovano su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP e sono configurati su ASM, assicurarsi che i nomi SVM siano univoci nei sistemi FSX. Se si dispone dello stesso nome SVM nei sistemi FSX, il backup dei database Oracle che risiedono su tali SVM non è supportato.
- Dopo il ripristino di un database di grandi dimensioni (250 GB o superiore), se si esegue un backup online completo sullo stesso database, l'operazione potrebbe non riuscire e causare il seguente errore:
failed with status code 500, error
{\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create snapshot. Reason: Snapshot operation not allowed due to clones backed by snapshots. Try again after sometime.\"}}

Per informazioni su come risolvere questo problema, fare riferimento a: ["Operazione Snapshot non consentita a causa di cloni supportati da snapshot"](#).

Eseguire il backup dei database SAP HANA nativi del cloud

Avvio rapido

Inizia subito seguendo questa procedura.

1

Verificare il supporto per la configurazione

- Sistema operativo:
 - RHEL 7.6 o versione successiva
 - RHEL 8.1 o versione successiva per SAP-HANA SPS07
 - SLES 12 SP5 o versioni successive e 15 piattaforme SPX certificate da SAP HANA
- Storage cloud NetApp: Azure NetApp Files
- Layout dello storage: Per i file di dati e log, Azure supporta solo NFSv4.1.
- Layout del database:
 - SAP HANA Multitenant Database Container (MDC) 2.0SPS5, 2.0SPS6, 2.0SPS7 con tenant singoli o multipli
 - Sistema host singolo SAP HANA, sistema host multiplo SAP HANA, replica di sistema HANA
- Plug-in SAP HANA sull'host del database

2

Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a. "[Iscriviti a BlueXP](#)".

3

Accedere a BlueXP

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a. "[Accedere a BlueXP](#)".

4

Gestisci il tuo account BlueXP

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a. "[Gestisci il tuo account BlueXP](#)".

Configurare Azure NetApp Files

Con BlueXP è necessario creare un ambiente di lavoro Azure NetApp Files per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro Azure NetApp Files

È necessario creare ambienti di lavoro Azure NetApp Files in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. "[Scopri di più su Azure NetApp Files](#)" e. "[Creare un ambiente di lavoro Azure NetApp Files](#)".

Creare un connettore

Un amministratore di account BlueXP dovrebbe implementare un connettore in Azure che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. "[Creare un connettore in Azure da BlueXP](#)".

- Assicurarsi che vi sia connettività tra il connettore e gli host del database.
- Se si dispone dell'ambiente di lavoro e dei database Azure NetApp Files nella stessa rete virtuale (VNET), è possibile implementare il connettore nella stessa rete virtuale.
- Se si dispone di un ambiente di lavoro Azure NetApp Files e di database in reti VNet diverse e si hanno carichi di lavoro NAS (NFS) configurati su Azure NetApp Files, è possibile creare il connettore su una delle reti VNet.

Dopo aver creato il connettore, aggiungere l'ambiente di lavoro facendo clic su **Storage > Canvas > My Working Environments > Add Working Environment**.

Installare il plug-in SnapCenter per SAP HANA e aggiungere host di database

Installare il plug-in SnapCenter per SAP HANA su ciascuno degli host di database SAP HANA. A seconda che l'host SAP HANA disponga di un'autenticazione basata su chiave SSH abilitata, è possibile seguire uno dei metodi per installare il plug-in.

- Se SSH è attivato per l'host del database, è possibile installare il plug-in utilizzando l'opzione SSH. [Scopri di più.](#)
- Se SSH è disattivato, installare il plug-in manualmente. [Scopri di più.](#)

Prerequisiti

Prima di aggiungere l'host, assicurarsi che i prerequisiti siano soddisfatti.

- Assicurarsi che Java 11 (64 bit) Oracle Java o OpenJDK sia installato su ciascuno degli host di database SAP HANA.
- L'ambiente di lavoro dovrebbe essere stato aggiunto e il connettore dovrebbe essere stato creato.
- Assicurarsi che il connettore sia connesso agli host del database SAP HANA.

Per informazioni su come risolvere il problema di connettività, fare riferimento a. ["Impossibile convalidare la connettività dall'host del connettore BlueXP all'host del database dell'applicazione"](#).

Quando il connettore viene perso o se è stato creato un nuovo connettore, è necessario associarlo alle risorse dell'applicazione esistenti. Per istruzioni sull'aggiornamento del connettore, vedere ["Aggiornare i dettagli del connettore"](#).

- Assicurarsi che l'utente BlueXP abbia il ruolo di "account Admin".
- Si dovrebbe aver creato l'utente SnapCenter e configurato sudo per l'utente non root (sudo). Per ulteriori informazioni, fare riferimento a. ["Configurare sudo per l'utente SnapCenter."](#)
- Prima di aggiungere l'host di database, è necessario aver installato il plug-in SnapCenter per SAP HANA.
- Durante l'aggiunta degli host di database SAP HANA, è necessario aggiungere le chiavi dell'archivio utente HDB. La chiave di archivio utente sicura HDB viene utilizzata per memorizzare le informazioni di connessione degli host di database SAP HANA in modo sicuro sul client e il client HDBSQL utilizza la chiave di archivio utente sicura per connettersi all'host di database SAP HANA.
- Per la replica del sistema HANA (HSR), per proteggere i sistemi HANA, è necessario registrare manualmente i sistemi HANA primario e secondario.



Il nome host deve essere uguale a quello dell'host utilizzato nella replica HSR.

- Se viene eseguita l'installazione basata su SSH, assicurarsi che il connettore abbia attivato la comunicazione con la porta SSH (impostazione predefinita: 22).
- Assicurarsi che il connettore abbia la comunicazione abilitata alla porta plug-in (impostazione predefinita: 8145) per il funzionamento delle operazioni di protezione dei dati.
- Assicurarsi che sia installata la versione più recente del plug-in. Per aggiornare il plug-in, fare riferimento a. [Upgrade del plug-in SnapCenter per il database SAP HANA.](#)

Configurare sudo per l'utente SnapCenter

Creare un utente non root (sudo) per installare il plug-in.

Fasi

1. Accedere a Connector VM.
2. Scarica il binario del plug-in host Linux di SnapCenter.

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

3. Copiare il contenuto di **sudoer.txt** situato all'indirizzo: `/var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po "cloudmanager_scs_cloud:.*?"|sed -e/ */|cut -f2 -d":")/sc-linux-host-plugin`
4. Accedere all'host di sistema SAP HANA utilizzando l'account utente root.
5. Configurare l'accesso sudo per l'utente non root copiando il testo copiato nel passaggio 3 nel file `/etc/sudoers.d/snapcenter`.

Nelle righe aggiunte al file `/etc/sudoers.d/snapcenter`, sostituire `<LINUXUSER>` con l'utente non root e `<USER_HOME_DIRECTORY>` con `home/<non-root-user>`.

Installare il plug-in utilizzando lo script

Configurare l'autenticazione basata su chiave SSH per l'account utente non root dell'host SAP HANA ed eseguire i seguenti passaggi per installare il plug-in.

Prima di iniziare

Assicurarsi che la connessione SSH al connettore sia attivata.

Fasi

1. Accedere a Connector VM.
2. Installare il plug-in utilizzando lo script fornito nel connettore.


```
sudo bash /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

Se si utilizza un connettore meno recente, eseguire il seguente comando per installare il plug-in.

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

Nome	Descrizione	Obbligatorio	Predefinito
plugin_host	Specifica l'host SAP HANA	Sì	-
nome_utente_host	Specifica l'utente SnapCenter con privilegi SSH sull'host SAP HANA	Sì	-
host_ssh_key	Specifica la chiave SSH dell'utente SnapCenter e viene utilizzata per connettersi all'host SAP HANA	Sì	-
porta_plugin	Specifica la porta utilizzata dal plug-in	No	8145

Nome	Descrizione	Obbligatorio	Predefinito
host_ssh_port	Specifica la porta SSH sull'host SAP HANA	No	22

Ad esempio, ``sudo bash /var/lib/docker/Volumes/service-manager-2_cloud_manager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --Username SnapCenter --sshkey /keys/netapp-ssh.ppk``

Dopo aver installato il plug-in, è necessario [Aggiunta di host di database SAP HANA](#).

Installare il plug-in manualmente

Se l'autenticazione basata su chiave SSH non è abilitata sull'host HANA, attenersi alla procedura manuale riportata di seguito per installare il plug-in.

Fasi

1. Accedere a Connector VM.

2. Scarica il binario del plug-in host Linux di SnapCenter.

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

Il binario del plug-in è disponibile all'indirizzo: `cd /var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/$(sudo docker ps|grep -po "cloudmanager_scs_cloud:.?*"|sed -e/ */|cut -f2 -d":")/sc-linux-host-plugin`

3. Copiare `snapcenter_linux_host_plugin_scs.bin` dal percorso sopra indicato al percorso `/home/<non root user>/.sc_netapp` per ciascuno degli host di database SAP HANA utilizzando metodi SCP o altri metodi alternativi.

4. Accedere all'host del database SAP HANA utilizzando l'account non root (sudo).

5. Modificare la directory in `/home/<non root user>/.sc_netapp/` ed eseguire il seguente comando per abilitare le autorizzazioni di esecuzione per il file binario.

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

6. Installare il plug-in SAP HANA come utente sudo SnapCenter.

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```

7. Copiare `certificate.pem` dal percorso `<base_mount_path>/client/certificate/` del connettore VM a `/var/opt/snapcenter/spl/etc/` sull'host plug-in.

8. Passare a `/var/opt/snapcenter/spl/etc` ed eseguire il comando `keytool` per importare il certificato.

```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
-deststorepass snapcenter -noprompt
```

9. Riavviare SPL: `systemctl restart spl`

10. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.

```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
plug-in host>:<plug-in port>/PluginService/Version --cert
config/client/certificate/certificate.pem --key
/config/client/certificate/key.pem
```


Dopo aver installato il plug-in, è necessario [Aggiunta di host di database SAP HANA](#).

Upgrade del plug-in SnapCenter per il database SAP HANA

È necessario aggiornare il plug-in SnapCenter per il database SAP HANA per accedere alle nuove funzionalità e ai miglioramenti più recenti.

Prima di iniziare

- Assicurarsi che non vi siano operazioni in esecuzione sull'host.

Fasi

1. Configurare sudo per l'utente SnapCenter. Per ulteriori informazioni, vedere [Configurare sudo per l'utente SnapCenter](#).
2. Eseguire il seguente script.

```
/var/lib/docker/volumes/service-manager-  
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh  
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>  
--pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
```

Se si utilizza un connettore meno recente, eseguire il seguente comando per aggiornare il plug-in.

```
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>  
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>  
--upgrade
```

Aggiunta di host di database SAP HANA

È necessario aggiungere manualmente gli host di database SAP HANA per assegnare policy e creare backup. Il rilevamento automatico dell'host del database SAP HANA non è supportato.

Fasi

1. Nell'interfaccia utente **BlueXP**, selezionare **protezione > Backup e ripristino > applicazioni**.
2. Selezionare **trova applicazioni**.
3. Selezionare **Cloud Native > SAP HANA** e selezionare **Next**.
4. Nella pagina **applicazioni**, selezionare **Aggiungi sistema**.
5. Nella pagina **Dettagli sistema**, eseguire le seguenti operazioni:
 - a. Selezionare tipo di sistema come container di database multi-tenant o volumi non dati globali.
 - b. Inserire il nome del sistema SAP HANA.
 - c. Specificare il SID del sistema SAP HANA.
 - d. (Facoltativo) modificare l'utente OSDB.
 - e. Se il sistema HANA è configurato con la replica del sistema HANA, attivare **sistema di replica del sistema HANA (HSR)**.
 - f. Selezionare la casella di testo **HDB Secure User Store Keys** per aggiungere i dettagli dei tasti di memorizzazione utente.

Specificare il nome della chiave, i dettagli del sistema, il nome utente e la password e fare clic su **Aggiungi chiave**.

È possibile eliminare o modificare le chiavi dell'archivio utente.

6. Selezionare **Avanti**.

7. Nella pagina **Dettagli host**, effettuare le seguenti operazioni:

- a. Selezionare **Aggiungi nuovo host o Usa host esistente**.
- b. Selezionare **usando SSH o Manuale**.

Per Manuale, immettere il FQDN host o IP, connettore, Nome utente, porta SSH, porta plug-in, e, facoltativamente, aggiungere e convalidare la chiave privata SSH.

Per SSH, immettere il nome host FQDN o IP, Connector, Username e plug-in port.

- a. Selezionare **Avanti**.

8. Nella pagina **Configurazione host**, verificare se i requisiti di configurazione sono soddisfatti.

Selezionare le caselle di controllo per confermare.

9. Selezionare **Avanti**.

10. Nella pagina **Storage Footprint**, selezionare **Aggiungi archiviazione** ed eseguire le seguenti operazioni:

- a. Selezionare l'ambiente di lavoro e specificare l'account NetApp.

Dal riquadro di navigazione a sinistra, selezionare BlueXP **Canvas** per aggiungere un nuovo ambiente di lavoro.

- b. Selezionare i volumi richiesti.
- c. Selezionare **Aggiungi archiviazione**.

11. Controllare tutti i dettagli e selezionare **Aggiungi sistema**.

È possibile modificare o rimuovere i sistemi SAP HANA dall'interfaccia utente.


Prima di rimuovere il sistema SAP HANA, è necessario eliminare tutti i backup associati e rimuovere la protezione.

Aggiungere volumi non dati

Dopo aver aggiunto il sistema SAP HANA di tipo container di database multi-tenant, è possibile aggiungere i volumi non-Data del sistema HANA.

È possibile aggiungere queste risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database SAP HANA disponibili.

Fasi

1. Nell'interfaccia utente **BlueXP**, fare clic su **Protection > Backup and Recovery > Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native > SAP HANA** e fare clic su **Avanti**.
4. Nella pagina **applicazioni**, fare clic su  Corrispondente al sistema per cui si desidera aggiungere volumi

non dati e selezionare **Manage System** (Gestisci sistema) > **non-Data Volume** (Volume non dati).

Aggiungere volumi non dati globali

Dopo aver aggiunto il sistema SAP HANA di tipo container di database multi-tenant, puoi aggiungere i Global non-Data Volumes del sistema HANA.

Fasi

1. Nell'interfaccia utente **BlueXP**, fare clic su **Protection > Backup and Recovery > Applications**.
2. Fare clic su **Scopri applicazioni**.
3. Selezionare **Cloud Native > SAP HANA** e fare clic su **Avanti**.
4. Nella pagina **applicazioni**, fare clic su **Aggiungi sistema**.
5. Nella pagina **Dettagli sistema**, eseguire le seguenti operazioni:
 - a. Dal menu a discesa System Type (tipo di sistema), selezionare **Global non-Data Volume** (Volume non dati globale).
 - b. Inserire il nome del sistema SAP HANA.
6. . Nella pagina **Dettagli host**, effettuare le seguenti operazioni:
 - a. Specificare i SID associati al sistema SAP HANA.
 - b. Selezionare l'host del plug-in
 - c. Fare clic su **Avanti**.
 - d. Esaminare tutti i dettagli e fare clic su **Aggiungi sistema**.

Eseguire il backup dei database SAP HANA nativi del cloud

È possibile creare un backup assegnando un criterio predefinito o il criterio creato.

Creare una policy per proteggere il database SAP HANA

È possibile creare policy se non si desidera utilizzare o modificare le policy predefinite.

1. Nella pagina **applicazioni**, dall'elenco a discesa Impostazioni, selezionare **Criteri**.
2. Fare clic su **Crea policy**.
3. Specificare un nome di policy.
4. (Facoltativo) modificare il formato del nome della copia Snapshot.
5. Selezionare il tipo di policy.
6. Specificare la pianificazione e i dettagli di conservazione.
7. (Facoltativo) specificare gli script. ["Prescrizioni e post-script."](#)
8. Fare clic su **Create** (Crea).

Prescrizioni e post-script

Durante la creazione di un criterio, è possibile fornire prescrizioni, postscript e script di uscita. Questi script vengono eseguiti sull'host HANA durante l'operazione di protezione dei dati.

Il formato supportato per gli script è .sh, python script, perl script e così via.

Il prescript e il postscript devono essere registrati dall'amministratore host in /opt/NetApp/snapcenter/scc/etc/allowed_commands.config file.

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

Variabili ambientali

Per il flusso di lavoro di backup, le seguenti variabili ambientali sono disponibili come parte di Prespt e postscript.

Variabile ambientale	Descrizione
SID	L'identificatore di sistema del database HANA scelto per il ripristino
BackupName	Nome del backup scelto per l'operazione di ripristino
UserStoreKeyNames	Chiave userstore configurata per il database HANA
OSDBUser	Configurato OSDBUser per il database HANA
Nome criterio	Solo per backup pianificati
tipo_pianificazione	Solo per backup pianificati

Creare un backup del database SAP HANA

È possibile assegnare un criterio predefinito o creare un criterio e assegnarlo al database. Una volta assegnato il criterio, i backup vengono creati in base alla pianificazione definita nel criterio.

Prima di iniziare

Dovrebbero essere stati aggiunti gli host del database SAP HANA. ["Aggiunta di host di database SAP HANA"](#)

A proposito di questa attività

Per HANA System Replication (HSR), il processo di backup pianificato viene attivato solo per il sistema HANA primario e se il sistema esegue il failover verso il sistema HANA secondario, i programmi esistenti attivano un backup sul sistema HANA primario corrente. Se il criterio non viene assegnato al sistema HANA primario e secondario, dopo il failover, le pianificazioni non avranno esito positivo.

Se ai sistemi HSR vengono assegnati criteri diversi, il backup pianificato viene attivato per i sistemi HANA primario e secondario e il backup non viene eseguito per il sistema HANA secondario.

Fasi

1. Nella pagina applicazioni, se il database non è protetto mediante criteri, fare clic su **Assegna policy**.

Sebbene il database sia protetto mediante uno o più criteri, se necessario, è possibile continuare ad assegnare ulteriori criteri facendo clic su **...** > **Assegna policy**.

2. Selezionare il criterio e fare clic su **Assegna**.

I backup vengono creati in base alla pianificazione definita nel criterio.



L'account del servizio (*SnapCenter-account-`<account_id>`*) viene utilizzato per eseguire le operazioni di backup pianificate.

Creazione di backup on-demand del database SAP HANA

Dopo aver assegnato il criterio, è possibile creare un backup on-demand dell'applicazione.

Fasi

1. Nella pagina **applicazioni**, fare clic su **...** Corrispondente all'applicazione e fare clic su **Backup on-Demand**.
2. Selezionare il tipo di backup on-demand.
3. Per il backup basato su policy, selezionare il criterio, il livello di conservazione e fare clic su **Create Backup** (Crea backup).
4. Per una volta, selezionare Snapshot copy based (basato su copia Snapshot) o file based (basato su file), attenersi alla seguente procedura:
 - a. Selezionare il valore di conservazione e specificare il nome del backup.
 - b. (Facoltativo) specificare gli script e il percorso per gli script.

Per ulteriori informazioni, vedere "[Prescritture e postscript](#)"

- c. Fare clic su **Create Backup** (Crea backup).

Eseguire il backup di database SQL Server nativi per il cloud utilizzando le API REST

Avvio rapido

Inizia subito seguendo questa procedura.



Verificare il supporto per la configurazione

- Sistema operativo:
 - Windows 2016
 - Windows 2019
 - Windows 2022
- Cloud storage NetApp: Amazon FSX per NetApp ONTAP
- Layout dello storage: SAN (iSCSI)

La configurazione NAS non è supportata.

- Versioni database:
 - Microsoft SQL Server 2016
 - Microsoft SQL Server 2019
 - Microsoft SQL Server 2022
- Configurazione database:
 - Standalone

2

Iscriviti a BlueXP

BlueXP è accessibile da una console basata su web. Una volta iniziato a utilizzare BlueXP, il primo passo consiste nell'iscriversi utilizzando le credenziali del sito di supporto NetApp o creando un login cloud NetApp. Per ulteriori informazioni, fare riferimento a. "[Iscriviti a BlueXP](#)".

3

Accedere a BlueXP

Dopo aver effettuato la registrazione a BlueXP, è possibile accedere dalla console basata sul Web. Per ulteriori informazioni, fare riferimento a. "[Accedere a BlueXP](#)".

4

Gestisci il tuo account BlueXP

Puoi amministrare il tuo account gestendo utenti, account di servizio, aree di lavoro e connettori. Per ulteriori informazioni, fare riferimento a. "[Gestisci il tuo account BlueXP](#)".

Configurare FSX per ONTAP

Con BlueXP è necessario creare un ambiente di lavoro FSX per ONTAP per aggiungere e gestire volumi e servizi dati aggiuntivi. È inoltre necessario creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del proprio ambiente di cloud pubblico.

Creare un ambiente di lavoro FSX per ONTAP

È necessario creare FSX per ambienti di lavoro ONTAP in cui sono ospitati i database. Per ulteriori informazioni, fare riferimento a. "[Inizia a utilizzare Amazon FSX per ONTAP](#)" e. "[Creare e gestire un ambiente di lavoro Amazon FSX per ONTAP](#)".

È possibile creare l'ambiente di lavoro FSX per ONTAP utilizzando BlueXP o AWS. Se hai creato utilizzando AWS, dovresti scoprire FSX per i sistemi ONTAP in BlueXP.

Creare un connettore

Un account Admin deve creare un connettore in AWS che consenta a BlueXP di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni, fare riferimento a. "[Creazione di un connettore in AWS da BlueXP](#)".

- È necessario utilizzare lo stesso connettore per gestire sia l'ambiente di lavoro FSX per ONTAP che i database.

- Se si dispone dell'ambiente di lavoro FSX per ONTAP e dei database nello stesso cloud privato virtuale (VPC), è possibile implementare il connettore nello stesso VPC.
- Se si dispone dell'ambiente di lavoro FSX per ONTAP e di database in diversi VPC:
 - Se si dispone di carichi di lavoro NAS (NFS) configurati su FSX per ONTAP, è possibile creare il connettore su uno dei VPC.
 - Se si hanno solo carichi di lavoro SAN configurati e non si intende utilizzare carichi di lavoro NAS (NFS), è necessario creare il connettore nel VPC in cui viene creato il sistema FSX per ONTAP.



Per utilizzare i carichi di lavoro NAS (NFS), è necessario disporre di un gateway di transito tra il VPC del database e Amazon VPC. È possibile accedere all'indirizzo IP NFS, che è un indirizzo IP mobile, da un altro VPC solo attraverso il gateway di transito. Non è possibile accedere agli indirizzi IP mobili eseguendo il peering dei VPC.

Dopo aver creato il connettore, fare clic su **Storage > Canvas > My Working Environments > Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni per aggiungere l'ambiente di lavoro. Assicurarsi che vi sia connettività dal connettore agli host del database Oracle e all'ambiente di lavoro FSX. Il connettore dovrebbe essere in grado di connettersi all'indirizzo IP di gestione del cluster dell'ambiente di lavoro FSX.

- Aggiungere l'ambiente di lavoro facendo clic su **Storage > Canvas > My Working Environments > Add Working Environment**.

Assicurarsi che vi sia connettività dal connettore agli host del database e all'ambiente di lavoro FSX per ONTAP. Il connettore deve connettersi all'indirizzo IP di gestione del cluster di FSX per l'ambiente di lavoro ONTAP.

- Copiare l'ID del connettore facendo clic su **Connector > Manage Connectors** (connettore > Gestisci connettori) e selezionando il nome del connettore.

Installare il plug-in SnapCenter per SQL Server e aggiungere host di database

È necessario installare il plug-in di SnapCenter per SQL Server su ciascuno degli host del database SQL, aggiungere gli host del database, rilevare le istanze del database e configurare le credenziali per le istanze del database.

Installare il plug-in SnapCenter per SQL Server

È necessario scaricare il plug-in **snapcenter_service_Windows_host_plugin.exe** e quindi eseguire il comando silent installer per installare il plug-in sull'host del database.

Prima di iniziare

- È necessario verificare che siano soddisfatti i seguenti prerequisiti.
 - È installato .Net 4.7.2
 - Viene installato PowerShell 4,0
 - È disponibile uno spazio minimo su disco di 5 GB
 - È disponibile una dimensione minima di 4 GB di RAM
- È necessario eseguire l'API per completare l'assunzione del cliente. Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Tenant%20Registration/createTenant>

Fasi

1. Scaricare il plug-in eseguendo l'API dall'host del connettore.

```
docker exec -it cloudmanager_scs_cloud curl  
'http://127.0.0.1/api/v2/pluginpackage/windows'
```

La posizione del file è `/var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/<agent_version>/sc-Windows-host-plugin/snapcenter_service_Windows_host_plugin.exe`.
2. Copiare `snapcenter_service_Windows_host_plugin.exe` dal connettore a ciascuno degli host del database MSSQL Server utilizzando SCP o altri metodi alternativi.
3. Installare il plug-in.

```
"C://<install_folder>/snapcenter_service_Windows_host_plugin.exe"/silent/debuglog  
"C://<install_folder>/ha_Suite_Silent_Install_SCSQL_FRESH.log" /log"C://install_folder/"  
BI_SNAPCENTER_PORT=8145 ISFeatureInstall=SCSQL'
```
4. Copiare il certificato autofirmato da `/var/lib/docker/Volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/client/certificate/certificate.pem` negli host del database di MSSQL Server.

È inoltre possibile generare un certificato autofirmato o un certificato CA firmato se non si utilizza quello predefinito.
5. Convertire il certificato dal formato `.pem` al formato `.crt` nell'host del connettore.

```
'openssl x509 -outform der -in certificate.pem -out certificate.crt'
```
6. Fare doppio clic sul certificato per aggiungerlo all'archivio **Personal e Trusted Root Certification Authority**.

Aggiungere l'host del database SQL Server

È necessario aggiungere l'host del database MSSQL utilizzando l'FQDN host.

```
"POST snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts"
```

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/Host%20Management/AddHosts>

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
addr	stringa	Vero
id_connettore	stringa	Vero
plugin_type	stringa	Vero
metodo_installazione	stringa	Vero

Nome	Tipo	Obbligatorio
porta_plugin	numero	Vero
nome utente	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Visualizzare gli host del database SQL Server aggiunti

È possibile eseguire questa API per visualizzare tutti gli host di database SQL Server aggiunti.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/GetHosts>

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```
{
  "num_records": 1,
  "total_records": 1,
  "records": [
    {
      "id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
      "addr": "scspa2722211001.rtp.openenglab.netapp.com",
      "status": "Running",
      "connector_id": "fBf8Iwbp4BscBfD02qBwWm6I03gGAesRclients",
      "plugin_port": 8145,
      "plugins": [
        {
          "type": "mssql"
        }
      ],
      "os_type": "windows",
      "platform": "onprem",
      "username": "administrator",
      "operating_mode": "production"
    }
  ],
  "_links": {
    "next": {}
  }
}
```

Rilevare le istanze del database

È possibile eseguire questa API e immettere l'ID host per rilevare tutte le istanze MSSQL.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/MSSQLInstancesDiscoveryRequest>

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametro

Nome	Tipo	Obbligatorio
host_id	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Visualizzare le istanze del database rilevate

È possibile eseguire questa API per visualizzare tutte le istanze del database rilevate.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/GetMSSQLInstancesRequest>

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```
{
  "num_records": 2,
  "total_records": 2,
  "records": [
    {
      "id": "953e66de-10d9-4fd9-bdf2-bf4b0eaabfd7",
      "name": "scspa2722211001\\\\NAMEDINSTANCE1",
      "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
      "status": "Running",
      "auth_mode": 0,
      "version": "",
      "is_clustered": false,
      "is_credentials_configured": false,
      "protection_mode": ""
    },
    {
      "id": "18e1b586-4c89-45bd-99c8-26268def787c",
      "name": "scspa2722211001",
      "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
      "status": "Stopped",
      "auth_mode": 0,
      "version": "",
      "is_clustered": false,
      "is_credentials_configured": false,
      "protection_mode": ""
    }
  ],
  "_links": {
    "next": {}
  }
}
```

Configurare le credenziali dell'istanza del database

È possibile eseguire questa API per convalidare e impostare le credenziali per le istanze del database.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/ConfigureCredentialRequest>

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametro

Nome	Tipo	Obbligatorio
host_id	stringa	Vero
id_istanza	stringa	Vero
nome utente	stringa	Vero
password	stringa	Vero
auth_mode	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Eseguire il backup di database Microsoft SQL Server nativi per il cloud

È possibile creare backup pianificati o su richiesta assegnando i criteri creati.

Creare un criterio di backup

È possibile eseguire questa API per creare il criterio di backup.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies"

Per ulteriori informazioni, fare riferimento a: https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService_CreateMSSQLBackupPolicy

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
nome	stringa	Vero
tipo_backup	stringa	Vero
copia_solo_backup	stringa	Falso
è_definito_sistema	stringa	Falso
formato_nome_backup	stringa	Vero
tipo_pianificazione	stringa	Vero
ora_inizio	numero	Vero
hours_interval	numero	Vero
minuti_intervallo	numero	Vero
retention_type	stringa	Vero
retention_count	numero	Vero
ora_fine	numero	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 201.

Esempio:

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  }
}
```

Assegnare il criterio all'istanza del database SQL

È possibile eseguire questa API per assegnare i criteri all'istanza del database SQL.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/{id}/policy-assignment"

Dove *id* è l'ID istanza MSSQL ottenuto eseguendo l'API dell'istanza del database Discover. Per ulteriori informazioni, fare riferimento a. ["Rilevare le istanze del database"](#).

Array di ID è l'input qui. Ad esempio:

```
[  
  "c9f3e68d-1f9c-44dc-b9af-72a9dfc54320"  
]
```

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/MSSQL%20Policy%20Assignment/PostMSSQLInstanceAssignPolicyRequest>

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{  
  "job": {  
    "_links": {  
      "self": {  
        "href": "/api/resourcelink"  
      }  
    },  
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"  
  }  
}
```

Crea un backup su richiesta

Puoi eseguire questa API per creare un backup on-demand.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/MSSQL%20Backups/CreateMSSQLBackupRequest>

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
id	stringa	Vero
 <p>Questo è l'ID dell'istanza del database MSSQL.</p>		
tipo_risorsa	stringa	Vero
policy_id	stringa	Vero
tipo_pianificazione	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Visualizzare i backup

È possibile eseguire queste API per visualizzare l'elenco di tutti i backup e per visualizzare i dettagli di un particolare backup.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups"

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups/{id}"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/MSSQL%20Backups/MSSQLGetBackupsRequest>

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:


```
{
  "total_records": 1,
  "num_records": 1,
  "records": [
    {
      "backup_id": "602d7796-8074-43fc-a178-eee8c78566ac",
      "resource_id": "a779578d-cf78-46f3-923d-b9223255938c",
      "backup_name":
"Hourly_policy2_scspa2722211001_NAMEDINSTANCE1_2023_08_08_07_02_01_81269_0",
      "policy_name": "policy2",
      "schedule_type": "Hourly",
      "start_time": "2023-08-08T07:02:10.203Z",
      "end_time": "0001-01-01T00:00:00Z",
      "backup_status": "success",
      "backup_type": "FullBackup"
    }
  ],
  "_links": {
    "next": {}
  }
}
```

Ripristinare i database Oracle nativi del cloud

Ripristinare i database Oracle nativi del cloud nella posizione originale


In caso di perdita di dati, è possibile ripristinare i file di dati, i file di controllo o entrambi nella posizione originale e quindi ripristinare il database.

Prima di iniziare

Se il database Oracle 21c è IN stato AVVIATO, l'operazione di ripristino non riesce. Eseguire il seguente comando per ripristinare correttamente il database.

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
/opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
```

Fasi

1. Fare clic su  Corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
2. Selezionare il punto di ripristino in cui ripristinare il database e fare clic su **Restore to original location** (Ripristina posizione originale).
3. Nella sezione ambito ripristino, eseguire le seguenti operazioni:

Se...	Eseguire questa operazione...
Ripristinare solo i file di dati	Selezionare tutti i file di dati .

Se...	Eseguire questa operazione...
Ripristinare solo i file di controllo	Selezionare file di controllo
Ripristinare sia i file di dati che i file di controllo	Selezionare tutti i file di dati e file di controllo.

È inoltre possibile selezionare la casella di controllo **Imponi ripristino in-place**.

Nel layout di Amazon FSX per NetApp ONTAP o SAN Cloud Volumes ONTAP, se il plug-in SnapCenter per Oracle trova file esterni diversi dai file di dati Oracle sul gruppo di dischi ASM, viene eseguito il metodo di ripristino connessione e copia. I file esterni possono essere di uno o più dei seguenti tipi:

- Parametro
- Password
- log di archiviazione
- log online
- File dei parametri ASM.

L'opzione **Imponi ripristino in-place** sovrascrive i file esterni di tipo parametro, password e log di archiviazione. Utilizzare il backup più recente quando è selezionata l'opzione **Force in-place restore** (forza ripristino in-place).

4. Nella sezione ambito ripristino, eseguire le seguenti operazioni:

Se...	Eseguire questa operazione...
Ripristinare l'ultima transazione	Selezionare tutti i registri.
Ripristinare un numero SCN (System Change Number) specifico	Selezionare fino a SCN e specificare il numero SCN.
Ripristinare una data e un'ora specifiche	Selezionare Data e ora.
Non si desidera eseguire il ripristino	Selezionare Nessun ripristino.

Per l'ambito di ripristino selezionato, nel campo **Archive Log Files Locations** (posizioni file registro archivio) è possibile specificare la posizione che contiene i registri di archiviazione richiesti per il ripristino.

Selezionare questa casella di controllo se si desidera aprire il database in modalità DI LETTURA/SCRITTURA dopo il ripristino.

5. Fare clic su **Avanti** e rivedere i dettagli.

6. Fare clic su **Restore** (Ripristina).

Ripristinare i database Oracle nativi del cloud in una posizione alternativa

In caso di perdita di dati, è possibile ripristinare il database Oracle in una posizione alternativa solo su Azure NetApp Files. La posizione alternativa può trovarsi su un host

diverso o sullo stesso host.

Prima di iniziare

- Se il database Oracle 21c è IN stato AVVIATO, l'operazione di ripristino non riesce. Eseguire il seguente comando per ripristinare correttamente il database.

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar  
/opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
```
- Assicurarsi che la versione di Oracle sull'host alternativo sia uguale a quella dell'host originale.

A proposito di questa attività

Durante l'avvio dell'operazione di ripristino, non è consentito modificare le configurazioni ad eccezione di Oracle home, throughput massimo del volume, SID Oracle e credenziali del database.

Il ripristino completo è attivato per impostazione predefinita con l'opzione *until CANCEL* impostata su true.

Per impostazione predefinita, la modalità di registro archivio è disattivata per il database ripristinato. Se necessario, è possibile attivare la modalità di registrazione dell'archivio e mantenere i registri di archiviazione sul volume NetApp.

Fasi

1. Fare clic su **...** Corrispondente al database che si desidera ripristinare e fare clic su **Restore** (Ripristina).
2. Selezionare il punto di ripristino in cui ripristinare il database e fare clic su **Restore to alternate location > Next**.
3. Nella pagina Configuration (Configurazione), specificare i dettagli relativi a posizione alternativa, SID, Oracle_Home, credenziali del database e throughput dello storage.

Per la credenziale del database, se l'autenticazione utente del sistema operativo è disattivata, è necessario fornire una password per consentire all'utente sys di connettersi al database ripristinato sullo stesso host o su quello di destinazione.

4. Fare clic su **Avanti**, rivedere i dettagli e fare clic su **Ripristina**.

L'avanzamento dell'operazione di ripristino può essere visualizzato nella pagina Job Monitor. Una volta completato il processo, fare clic su **Refresh Discovery** (Aggiorna rilevamento) per visualizzare il database ripristinato. Tuttavia, non è possibile proteggere il database ripristinato in una posizione alternativa.

Ripristinare i database SAP HANA nativi del cloud

In caso di perdita di dati, è possibile ripristinare i file di dati e non, quindi ripristinare il database.

Prima di iniziare

- Il sistema SAP HANA deve essere in stato di arresto.
- Se il sistema SAP HANA è attivo e in esecuzione, è possibile fornire una prescrizione per arrestare il sistema.

A proposito di questa attività

- Se si abilitano i backup ANF su un volume, viene eseguita l'operazione Single file SnapRestore.

- Per volumi non dati e volumi non dati globali, viene eseguita l'operazione di ripristino della connessione e della copia.
 - I valori QoS (Quality of Service) per le operazioni di connessione e ripristino delle copie vengono rilevati dai volumi di origine di volumi non dati o volumi non dati globali.



QoS è applicabile solo per pool di capacità di tipo "Manuale".

Fasi

1. Fare clic su [...](#) Corrispondente al database che si desidera ripristinare e fare clic su **View Details** (Visualizza dettagli).
2. Fare clic su [...](#) Corrispondente al backup dei dati che si desidera ripristinare e fare clic su **Restore** (Ripristina).
3. Nella pagina **Restore System**, inserire gli script. "[Prescrizioni e post-script.](#)"

Per il flusso di lavoro di ripristino, le seguenti variabili ambientali sono disponibili come parte di Prespt e postscript.

Variabile ambientale	Descrizione
SID	L'identificatore di sistema del database HANA scelto per il ripristino
BackupName	Nome del backup scelto per l'operazione di ripristino
UserStoreKeyNames	Chiave userstore configurata per il database HANA
OSDBUser	Configurato OSDBUser per il database HANA

4. Fare clic su **Restore** (Ripristina).

Cosa c'è di nuovo

Dopo il ripristino, ripristinare manualmente il sistema SAP HANA o fornire un postscript, che esegue il ripristino del sistema SAP HANA.

Ripristina volume non dati

A proposito di questa attività

Per l'operazione di connessione e ripristino delle copie, accedere al portale Microsoft Azure, selezionare il volume, fare clic su **Edit** e attivare **Hide snapshot path**.

Fasi

1. Nella pagina **applicazioni**, selezionare Volume non dati dalla casella a discesa.
2. Fare clic su [...](#) Corrispondente al backup che si desidera ripristinare e fare clic su **Restore** (Ripristina).

Ripristinare il volume globale non dati

A proposito di questa attività

Per l'operazione di connessione e ripristino delle copie, accedere al portale Microsoft Azure, selezionare il volume, fare clic su **Edit** e attivare **Hide snapshot path**.

Fasi

1. Nella pagina **applicazioni**, fare clic sul Global non-Data Volume che si desidera ripristinare.
2. Fare clic su **...** Corrispondente al volume non dati globale che si desidera ripristinare e fare clic su **Restore** (Ripristina).

Ripristinare il database Microsoft SQL Server

È possibile ripristinare il database Microsoft SQL Server sullo stesso host. È necessario prima ottenere l'elenco dei database e poi ripristinare il database.

Visualizzare l'elenco dei database

È possibile eseguire questa API per visualizzare l'elenco dei database.

"OTTIENI snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases"

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Databases/GetMSSQLDatabasesRequest>

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 200.

Esempio:

```

{
  "num_records": 3,
  "total_records": 3,
  "records": [
    {
      "id": "348901e5-aeaa-419f-88b1-80240de3b1fe",
      "name": "DB4",
      "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
      "size": 0.078125,
      "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
      "instance": "scspa2722211001\\NAMEDINSTANCE1",
      "db_status": "Normal",
      "db_access": "eUndefined",
      "db_type": "User",
      "recovery_mode": "Full"
    },
    {
      "id": "c79d33ab-7322-4ed6-92f5-51ad7a6944e0",
      "name": "DB5",
      "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
      "size": 0.078125,
      "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
      "instance": "scspa2722211001\\NAMEDINSTANCE1",
      "db_status": "Normal",
      "db_access": "eUndefined",
      "db_type": "User",
      "recovery_mode": "Full"
    },
    {
      "id": "40d6f35a-f4fb-48bc-8e0a-0ac93ddf0888",
      "name": "model",
      "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
      "size": 0.015625,
      "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
      "instance": "scspa2722211001\\NAMEDINSTANCE1",
      "db_status": "Normal",
      "db_access": "eUndefined",
      "db_type": "System",
      "recovery_mode": "Full"
    }
  ],
  "_links": {
    "next": {}
  }
}

```

Ripristinare e ripristinare il database MSSQL

È possibile eseguire questa API per ripristinare il database MSSQL.

"POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases/{id}/restore"

Dove *id* è l'ID del database MSSQL ottenuto eseguendo l'API del database di visualizzazione. Per ulteriori informazioni, fare riferimento a [Visualizzare l'elenco dei database](#).

Per ulteriori informazioni, fare riferimento a: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Database%20Restore/RestoreMSSQLDatabaseRequest>

Questa API crea un lavoro che può essere monitorato dalla scheda **Job Monitor** nell'interfaccia utente di BlueXP.

Parametri

Nome	Tipo	Obbligatorio
id_backup	stringa	Vero
sovrascrivi_database	bool	Vero
retain_replication_settings	bool	Falso
modalità_ripristino	stringa Le stringhe supportate da 3 sono <i>Operational</i> , <i>nonoperational</i> e <i>ReadOnly</i> .	Vero
annulla_directory_file	stringa	Vero
restore_type	stringa	Vero

Risposta

Se l'API viene eseguita correttamente, viene visualizzato il codice di risposta 202.

Esempio:

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

Clonare i database Oracle nativi del cloud

Clonare concetti e requisiti

È possibile clonare un database Oracle residente su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP utilizzando il backup del database sull'host del database di origine o su un host alternativo. È possibile clonare il backup dai sistemi di storage primari.

Prima di clonare il database, è necessario comprendere i concetti dei cloni e assicurarsi che tutti i requisiti siano soddisfatti.

Requisiti per la clonazione di un database Oracle

Prima di clonare un database Oracle, è necessario assicurarsi che i prerequisiti siano stati completati.

- Dovrebbe essere stato creato un backup del database. La creazione dei dati online e il backup dei log dovrebbero essere stati effettuati correttamente per consentire l'esecuzione dell'operazione di cloning.
- Nel parametro `asm_diskstring`, configurare:
 - `AFD:*` se si utilizza ASMFD
 - `ORCL:*` se si utilizza ASMLIB
 - `/Dev/<exact_device_location>` se si utilizza ASMUDEV
- Se si crea il clone su un host alternativo, l'host alternativo deve soddisfare i seguenti requisiti:
 - Il plug-in deve essere installato sull'host alternativo.
 - Il software Oracle deve essere installato sull'host alternativo.
 - L'host clone dovrebbe essere in grado di rilevare LUN dallo storage se si clonano database che risiedono su storage SAN iSCSI. Se si esegue la clonazione su un host alternativo, assicurarsi che sia stata stabilita una sessione iSCSI tra lo storage e l'host alternativo.
 - Se il database di origine è un database ASM:
 - L'istanza di ASM deve essere attiva e in esecuzione sull'host in cui verrà eseguito il clone.
 - Il provisioning del gruppo di dischi ASM deve essere eseguito prima dell'operazione di clonazione se si desidera inserire i file di log di archiviazione del database clonato in un gruppo di dischi ASM dedicato.

- Il nome del gruppo di dischi dati può essere configurato, ma assicurarsi che il nome non sia utilizzato da altri gruppi di dischi ASM sull'host in cui verrà eseguito il clone.
- I file di dati che risiedono sul gruppo di dischi ASM vengono forniti come parte del flusso di lavoro dei cloni.

Limitazioni

- La clonazione dei database residenti su Azure NetApp Files non è supportata.
- La clonazione dei database residenti su Qtree non è supportata.
- Il backup di un database clonato non è supportato.
- Se su Amazon FSX per NetApp ONTAP sono attivati backup automatici giornalieri, i volumi clonati su Amazon FSX per NetApp ONTAP non possono essere cancellati dall'interfaccia utente di BlueXP perché FSX avrebbe creato backup sui volumi clonati.
È necessario eliminare i volumi clonati dopo aver eliminato tutti i backup del volume dall'interfaccia utente FSX e quindi eliminare i cloni dall'interfaccia utente BlueXP utilizzando l'opzione force.

Metodi di clonazione

È possibile creare un clone utilizzando il metodo di base o il file di specifica del clone.

Clonare utilizzando il metodo di base

È possibile creare il clone con le configurazioni predefinite in base al database di origine e al backup selezionato.

- I parametri del database, home e utente del sistema operativo vengono impostati per impostazione predefinita sul database di origine.
- I percorsi dei file di dati vengono denominati in base allo schema di denominazione selezionato.
- Non è possibile specificare le istruzioni pre-script, post-script e SQL.
- Per impostazione predefinita, l'opzione di ripristino è **fino all'annullamento** e utilizza il backup del registro associato al backup dei dati per il ripristino

Clonare utilizzando il file delle specifiche

È possibile definire le configurazioni nel file di specifica del clone e utilizzarlo per clonare il database. È possibile scaricare il file delle specifiche, modificarlo in base alle proprie esigenze e quindi caricarlo. ["Scopri di più"](#).

I diversi parametri definiti nel file delle specifiche e modificabili sono i seguenti:

Parametro	Descrizione
control_files	<p>Posizione dei file di controllo per il database clone.</p> <p>Il numero di file di controllo sarà lo stesso del database di origine. Se si desidera eseguire l'override del percorso del file di controllo, è possibile specificare un percorso diverso del file di controllo. Il file system o il gruppo di dischi ASM dovrebbe esistere sull'host.</p>

Parametro	Descrizione
redo_logs	<p>Posizione, dimensione, numero di gruppi di ripristino dei log di ripristino.</p> <p>Per clonare il database sono necessari almeno due gruppi di log di ripristino. Se si desidera eseguire l'override del percorso del file di log di ripristino, è possibile personalizzare il percorso del file di log di ripristino in un file system diverso da quello del database di origine. Il file system o il gruppo di dischi ASM dovrebbe esistere sull'host.</p>
versione_oracle	Versione di Oracle sull'host di destinazione.
oracle_home	Oracle home sull'host di destinazione.
enable_archive_log_mode	Controlla la modalità del log di archiviazione per il database clone
parametri_database	Parametri del database per il database clonato
istruzioni_sql	Le istruzioni SQL da eseguire sul database dopo la clonazione
os_user_detail	Utente del sistema operativo Oracle nel database dei cloni di destinazione
porta_database	Porta utilizzata per comunicare con il database se l'autenticazione del sistema operativo è disattivata sull'host.
porta_asm	Porta utilizzata per la comunicazione con il database ASM se le credenziali sono fornite nell'input create clone.
skip_recovery	Non esegue l'operazione di recovery.
fino a scn	Recupera il database fino al numero scn (System Change Number) specificato.
fino a ora	<p>Recupera il database fino alla data e all'ora specificate.</p> <p>Il formato accettato è <i>mm/gg/aaaa hh:mm:ss</i>.</p>

Parametro	Descrizione
until_cancel	<p>Effettua il ripristino montando il backup del log associato al backup dei dati selezionato per la clonazione.</p> <p>Il database clonato viene recuperato fino a quando il file di log non è mancante o corrotto.</p>
log_paths	Posizioni aggiuntive dei percorsi dei log di archiviazione da utilizzare per il ripristino del database clonato.
source_location	Posizione del gruppo di dischi o del punto di montaggio sull'host del database di origine.
clone_location	Posizione del gruppo di dischi o del punto di montaggio che deve essere creato sull'host di destinazione corrispondente alla posizione di origine.
location_type	<p>Può essere ASM_diskgroup o mountpoint.</p> <p>I valori vengono compilati automaticamente al momento del download del file. Non modificare questo parametro.</p>
pre_script	Script da eseguire sull'host di destinazione prima di creare il clone.
post_script	Script da eseguire sull'host di destinazione dopo la creazione del clone.
percorso	<p>Percorso assoluto dello script sull'host clone.</p> <p>Lo script deve essere memorizzato in /var/opt/snapcenter/spl/scripts o in qualsiasi cartella all'interno di questo percorso.</p>
timeout	Il tempo di timeout specificato per lo script in esecuzione sull'host di destinazione.
argomenti	Argomenti specificati per gli script.

Schema di naming dei cloni

Lo schema di naming dei cloni definisce la posizione dei punti di montaggio e il nome dei diskgroup del database clonato. È possibile selezionare **identico** o **generato automaticamente**.

Schema di denominazione identico

Se si seleziona lo schema di denominazione dei cloni come **identico**, la posizione dei punti di montaggio e il nome dei diskgroup del database clonato saranno gli stessi del database di origine.

Ad esempio, se il punto di montaggio del database di origine è `/netapp_sourcedb/data_1`, `+DATA1_DG`, per il database clonato il punto di montaggio rimane lo stesso sia per NFS che per ASM su SAN.

- Le configurazioni come il numero e il percorso dei file di controllo e dei file di ripristino saranno le stesse dell'origine.



Se i log di ripristino o i percorsi dei file di controllo si trovano nei volumi non dati, l'utente deve aver eseguito il provisioning del gruppo di dischi ASM o del punto di montaggio nell'host di destinazione.

- L'utente del sistema operativo Oracle e la versione di Oracle saranno le stesse del database di origine.
- Il nome del volume di storage clone avrà il seguente formato `sourceVolNameSCS_Clone_CurrentTimeStampNumber`.

Ad esempio, se il nome del volume nel database di origine è `sourceVolName`, il nome del volume clonato sarà `sourceVolNameSCS_Clone_1661420020304608825`.



Il campo `CurrentTimeStampNumber` fornisce l'univocità nel nome del volume.

Schema di naming generato automaticamente

Se si seleziona lo schema di cloning come **generato automaticamente**, alla posizione dei punti di montaggio e al nome dei diskgroup del database clonato verrà aggiunto un suffisso.

- Se è stato selezionato il metodo di clone di base, il suffisso sarà **Clone SID**.
- Se è stato selezionato il metodo del file delle specifiche, il suffisso sarà il suffisso **suffisso** specificato durante il download del file delle specifiche del clone.

Ad esempio, se il punto di montaggio del database di origine è `/netapp_sourcedb/data_1` e il **Clone SID** o il **suffisso** è `HR`, il punto di montaggio del database clonato sarà `/netapp_sourcedb/data_1_HR`.

- Il numero di file di controllo e di log di ripristino sarà uguale a quello dell'origine.
- Tutti i file di log di ripristino e i file di controllo si trovano su uno dei punti di montaggio dati clonati o su gruppi di dischi ASM di dati.
- Il nome del volume di storage clone avrà il seguente formato `sourceVolNameSCS_Clone_CurrentTimeStampNumber`.

Ad esempio, se il nome del volume nel database di origine è `sourceVolName`, il nome del volume clonato sarà `sourceVolNameSCS_Clone_1661420020304608825`.



Il campo `CurrentTimeStampNumber` fornisce l'univocità nel nome del volume.

- Il formato del punto di montaggio NAS sarà `SourceNASMountPoint_suffix`.
- Il formato del gruppo di dischi ASM sarà `SourceDiskgroup_suffix`.



Se il numero di caratteri nel gruppo di dischi clone è maggiore di 25, il numero di caratteri nel gruppo sarà *SC_hashCode_suffix*.

Parametri del database

Il valore dei seguenti parametri di database sarà uguale a quello del database di origine, indipendentemente dallo schema di denominazione dei cloni.

- log_archive_format
- audit_trail
- processi
- destinazione_aggregato_pga
- remote_login_passwordfile
- undo_tablespace
- open_cursors
- sga_target
- db_block_size

Al valore dei seguenti parametri di database viene aggiunto un suffisso basato sul SID clone.

- audit_file_dest = {sourcedatabase_parametervalue}_suffix
- log_archive_dest_1 = {sourcedatabase_oraclehome}_suffix

Variabili di ambiente predefinite supportate per il clone specifico prespt e postscript

È possibile utilizzare le variabili di ambiente predefinite supportate quando si eseguono prespt e postscript durante la clonazione di un database.

- SC_ORIGINAL_SID specifica il SID del database di origine. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: NFSB32
- SC_ORIGINAL_HOST specifica il nome dell'host di origine. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: asmrac1.gdl.englab.netapp.com
- SC_ORACLE_HOME specifica il percorso della home directory Oracle del database di destinazione. Esempio: /Ora01/app/oracle/product/18.1.0/db_1
- SC_BACKUP_NAME specifica il nome del backup. Questo parametro verrà popolato per i volumi dell'applicazione. Esempi:
 - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
 - Se il database è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_07 12.16.48.9267_22_2021
- SC_ORIGINAL_OS_USER specifica il proprietario del sistema operativo del database di origine. Esempio: oracle
- SC_ORIGINAL_OS_GROUP specifica il gruppo del sistema operativo del database di origine. Esempio: Oinstall

- **SC_TARGET_SID** specifica il SID del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: Clonedb
- **SC_TARGET_HOST** specifica il nome dell'host in cui verrà clonato il database. Questo parametro verrà popolato per i volumi dell'applicazione. Esempio: asmrac1.gdl.englab.netapp.com
- **SC_TARGET_OS_USER** specifica il proprietario del sistema operativo del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Esempio: oracle
- **SC_TARGET_OS_GROUP** specifica il gruppo di sistemi operativi del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Esempio: Oinstall
- **SC_TARGET_DB_PORT** specifica la porta del database clonato. Per il flusso di lavoro del clone PDB, il valore di questo parametro non sarà predefinito. Esempio: 1521

Delimitatori supportati

- **@** viene utilizzato per separare i dati dal nome del database e per separare il valore dalla chiave. Esempio: DATI@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- **|** viene utilizzato per separare i dati tra due entità diverse per il parametro **SC_BACKUP_NAME**. Esempio: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- **,** viene utilizzato per separare un insieme di variabili per la stessa chiave. Esempio: DATI@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_1, RG2_scspr2417819002_07-22-2021_12.16.48.9267_1

Clonare i database Oracle nativi del cloud

È possibile clonare un database Oracle residente su Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP utilizzando il backup del database sull'host del database di origine o su un host alternativo.

È possibile clonare i database per i seguenti motivi:


- Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto del database corrente durante i cicli di sviluppo dell'applicazione.
- Popolare i data warehouse utilizzando strumenti di estrazione e manipolazione dei dati.
- Per ripristinare i dati cancellati o modificati per errore.


Prima di iniziare

È necessario comprendere i concetti dei cloni e assicurarsi che tutti i requisiti siano soddisfatti. ["Scopri di più"](#).

Fasi

1. Fare clic su **...** Corrispondente al database che si desidera clonare e fare clic su **View Details** (Visualizza dettagli).
2. Fare clic su **...** Corrispondente al backup dei dati e fare clic su **Clone**.
3. Nella pagina Clone Details (Dettagli clone), selezionare una delle opzioni di clonazione.
4. A seconda dell'opzione selezionata, eseguire le seguenti operazioni:

Se si seleziona...	Eseguire questa operazione...
<p>Di base</p>	<p>a. Selezionare l'host clone.</p> <p>Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e del sistema operativo dell'host del database di origine.</p> <p>b. Specificare il SID del clone.</p> <p>c. Selezionare lo schema di denominazione dei cloni.</p> <p>Se il database viene clonato nell'host di origine, lo schema di denominazione dei cloni viene generato automaticamente. Se il database viene clonato in un host alternativo, lo schema di naming dei cloni sarà identico.</p> <p>d. Specificare il percorso principale Oracle.</p> <p>e. (Facoltativo) specificare le credenziali del database.</p> <ul style="list-style-type: none"> ◦ Credenziale del database: Se l'autenticazione utente del sistema operativo è disattivata, è necessario fornire una password per consentire all'utente sys di connettersi al database clonato sullo stesso host o su quello di destinazione. ◦ Credenziale ASM: Se l'autenticazione dell'utente del sistema operativo è disattivata sull'host di destinazione, è necessario fornire le credenziali dell'utente con privilegi sysasm per connettersi all'istanza ASM sull'host di destinazione. <div style="display: flex; align-items: center; margin-top: 20px;"> <div style="text-align: center; margin-right: 10px;">  </div> <div> <p>Assicurarsi che il listener sia attivo e in esecuzione sull'host di destinazione.</p> </div> </div> <p>f. Fare clic su Avanti.</p> <p>g. Fare clic su Clone.</p>

Se si seleziona...	Eseguire questa operazione...
File delle specifiche	<p>a. Fare clic su Download file per scaricare il file delle specifiche.</p> <p>b. Selezionare lo schema di denominazione dei cloni.</p> <p>Se si seleziona, generato automaticamente, specificare il suffisso.</p> <p>c. Modificare il file delle specifiche in base ai requisiti e caricarlo facendo clic sul pulsante Browse (Sfogliare).</p> <p>d. Selezionare l'host clone.</p> <p>Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e del sistema operativo dell'host del database di origine.</p> <p>e. Specificare il SID del clone.</p> <p>f. (Facoltativo) specificare le credenziali del database.</p> <ul style="list-style-type: none"> ◦ Credenziale del database: Se l'autenticazione utente del sistema operativo è disattivata, è necessario fornire una password per consentire all'utente sys di connettersi al database clonato sullo stesso host o su quello di destinazione. ◦ Credenziale ASM: Se l'autenticazione dell'utente del sistema operativo è disattivata sull'host di destinazione, è necessario fornire le credenziali dell'utente con privilegi sysasm per connettersi all'istanza ASM sull'host di destinazione. <div style="display: flex; align-items: center; margin-top: 20px;">  <div> <p>Assicurarsi che il listener sia attivo e in esecuzione sull'host di destinazione.</p> </div> </div> <p>g. Fare clic su Avanti.</p> <p>h. Fare clic su Clone.</p>

5. Fare clic su  Accanto a **Filtra per** e seleziona **Clona opzioni > cloni** per visualizzare i cloni.

Aggiornare il sistema di destinazione SAP HANA

È possibile eseguire un refresh di un sistema di destinazione SAP HANA con i dati di un

sistema di origine SAP HANA. Questo può essere utilizzato per fornire i dati di produzione correnti in un sistema di test. Il backup e recovery di BlueXP ti consente di selezionare una copia Snapshot da un sistema di origine e di creare un nuovo volume Azure NetApp Files basato sulla copia Snapshot. Sono disponibili script di esempio che consentono di eseguire le operazioni necessarie sull'host del database per ripristinare il database SAP HANA.

Prima di iniziare

- Installare il sistema di destinazione SAP HANA prima di eseguire la prima operazione di refresh.
- Dovresti aggiungere manualmente i sistemi HANA di origine e destinazione nel backup e recovery di BlueXP.
- Assicurarsi che la versione del database SAP HANA sia la stessa sul sistema di origine e di destinazione.
- Si sarebbe dovuto decidere quali script di refresh utilizzare. Gli script di refresh sono disponibili nel report tecnico della soluzione.

"Script di esempio di automazione"

È possibile personalizzare gli script di refresh.

- Le seguenti variabili ambientali sono disponibili come parte di Prespt e postscript:
 - CLONED_VOLUMES_MOUNT_PATH
 - <SOURCEVOLUME>_DESTINATION
 - HANA_DATABASE_TYPE
 - TENANT_DATABASE_NAMES
- È necessario aggiornare il plug-in alla versione 3,0.
- I percorsi di montaggio devono essere identici per il volume di dati sui sistemi SAP HANA di origine e di destinazione.
- Prima della prima operazione di aggiornamento, assicurarsi che il file '/etc/fstab' non contenga voci per i volumi di dati del sistema SAP HANA di destinazione.

A proposito di questa attività

- L'aggiornamento del sistema è supportato solo per il sistema HANA di container di database multi-tenant.
- I criteri esistenti saranno validi dopo l'aggiornamento del sistema.
- I nuovi volumi creati avranno la seguente convenzione di denominazione: <sourcevolumename>-<timestamp>
 - Formato timestamp: <year> <month> <day>-<hour> <minute> <second>

Ad esempio, se il volume di origine è vol1, il nome del volume aggiornato sarà vol1-20230109-184501



Il nuovo volume verrà inserito nello stesso pool di capacità dei volumi di destinazione.

- Il percorso di giunzione sarà lo stesso del nome del volume.
- Il "numero massimo di throughput" per il nuovo volume viene prelevato dal volume del sistema di destinazione con pool di capacità manuali Quality of Service (QoS).

Per i pool di capacità QoS automatici, il throughput è definito dalla capacità del volume di origine.

- Durante l'aggiornamento del sistema, il montaggio e la disinstallazione automatici dei volumi vengono eseguiti utilizzando workflow e non script.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**.
2. Nella pagina **applicazioni**, fare clic su **...** Per selezionare l'azione corrispondente al sistema che si desidera aggiornare e selezionare **System Refresh** (Aggiorna sistema).
3. Nella pagina **System Refresh**, eseguire le seguenti operazioni:
 - a. Selezionare il sistema di origine e la copia Snapshot.
 - b. (Facoltativo) immettere gli indirizzi di esportazione da cui è possibile accedere ai nuovi volumi.
 - c. (Opzionale) immettere la massima velocità di trasmissione dello storage (MIB).
 - d. Immettere prescritti, postscript e i percorsi degli script di errore. Lo script on failure viene eseguito solo quando l'operazione di refresh del sistema non riesce.
 - e. Fare clic su **Aggiorna**.

Gestire la protezione dei dati applicativi nativi del cloud

Monitorare i lavori

È possibile monitorare lo stato dei lavori avviati negli ambienti di lavoro. In questo modo è possibile visualizzare i lavori completati correttamente, quelli in corso e quelli che non sono riusciti, in modo da poter diagnosticare e risolvere eventuali problemi.



I lavori pianificati verranno elencati nella pagina di monitoraggio dei lavori BlueXP dopo un ritardo di 5 minuti (massimo) dall'ora di completamento del lavoro.

Per ulteriori informazioni, fare riferimento a. "[Monitorare lo stato del lavoro](#)".

Manutenzione degli host di database Oracle

Un amministratore può mettere manualmente gli host del database in modalità di manutenzione per eseguire attività di manutenzione sugli host. Durante l'aggiornamento, gli host vengono automaticamente messi in modalità di manutenzione e, dopo l'aggiornamento, gli host vengono automaticamente trasferiti in modalità di produzione.

Quando gli host vengono messi in modalità di manutenzione, le operazioni on-demand non vengono eseguite e i processi pianificati vengono ignorati.





Non è possibile verificare se sono in esecuzione lavori per le risorse sugli host prima di mettere gli host in modalità di manutenzione.

Fasi

1. Nell'interfaccia utente di BlueXP, fare clic su **Protection > Backup and Recovery > Applications**
2. Selezionare **Oracle** come tipo di applicazione.
3. Fare clic su **Impostazioni > host**.

4. Eseguire una delle seguenti operazioni:

Se...	Eseguire questa operazione...
Impostare l'host in modalità di manutenzione	Fare clic su  Corrispondente all'host e selezionare Enable maintenance mode (attiva modalità di manutenzione).
Desidera portare l'host fuori dalla modalità di manutenzione	Fare clic su  Corrispondente all'host in manutenzione e selezionare Disable maintenance mode (Disattiva modalità di manutenzione).

Dati di audit


Quando si esegue direttamente un'API o si utilizza l'interfaccia utente per effettuare la chiamata API a una qualsiasi delle API esposte esternamente del backup e ripristino BlueXP per le applicazioni, la richiesta viene dettagliata come intestazioni, ruolo, corpo della richiesta, E le informazioni API verranno registrate nella tempistica di BlueXP e le voci di audit verranno conservate per sempre nella tempistica. Anche lo stato e la risposta agli errori della chiamata API vengono verificati dopo il completamento dell'operazione. Nel caso di risposte API asincrone come i job, l'id del job viene registrato anche come parte della risposta.

Il backup e ripristino BlueXP per le applicazioni registra le voci come host IP, corpo della richiesta, nome dell'operazione, chi ha attivato, alcune intestazioni, E lo stato operativo dell'API.

Visualizzare i dettagli del backup

È possibile visualizzare il numero totale di backup creati, i criteri utilizzati per la creazione dei backup, la versione del database e l'ID dell'agente.

Fasi

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






L'ID dell'agente è associato al connettore. Se un connettore utilizzato durante la registrazione dell'host SAP HANA non esiste più, i backup successivi dell'applicazione non avranno esito positivo perché l'ID dell'agente del nuovo connettore è diverso. Modificare l'id del connettore nell'host. Per ulteriori informazioni, vedere [Aggiornare i dettagli del connettore](#).

Elimina clone

Se non è più necessario, è possibile eliminare un clone.

Fasi

1. Fare clic su  Accanto a **Filtra per** e seleziona **Clona opzioni > Clona genitori**.
2. Fare clic su  Corrispondente all'applicazione e fare clic su **View Details** (Visualizza dettagli).
3. Nella pagina Database Details (Dettagli database), fare clic su  Accanto a **Filtra per** e selezionare **Clona**.

4. Fare clic su **...** Corrispondente al clone che si desidera eliminare e fare clic su **Delete** (Elimina).
5. (Facoltativo) selezionare la casella di controllo **forza eliminazione**.

Aggiornare i dettagli del connettore

Se il connettore utilizzato durante la registrazione dell'host dell'applicazione non esiste più o è danneggiato, è necessario implementare un nuovo connettore. Dopo aver implementato il nuovo connettore, eseguire l'API **Connector-update** per aggiornare i dettagli del connettore per tutti gli host registrati utilizzando il vecchio connettore.

Dopo aver aggiornato i dettagli del connettore per gli host Oracle o SAP HANA, eseguire le seguenti operazioni per assicurarsi che i dettagli del connettore siano stati aggiornati correttamente.

Fasi

1. Accedere a BlueXP Connector VM ed eseguire le seguenti operazioni:
 - a. Verificare che il plug-in sia raggiungibile dal connettore eseguendo il comando riportato di seguito dal connettore.


```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the plug-in host>:<plug-in port>/getVersion
--cert/config/client/certificate/certificate.pem
--key/config/client/certificate/key.pem
```
 - b. Ottenere il percorso di montaggio base.


```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs
sudo docker volume inspect | grep Mountpoint
```
 - c. Copiare certificate.pem dal percorso `<base_mount_path>/client/certificate/` del connettore VM a `/var/opt/snapcenter/spl/etc/` sull'host del plug-in.
2. Accedere all'host del plug-in ed eseguire le seguenti operazioni:
 - a. Passare a `/var/opt/snapcenter/spl/etc` ed eseguire il comando keytool per importare il file certificate.pem.


```
keytool -import -alias agentcert -file certificate.pem -keystore
keystore.jks -deststorepass snapcenter -noprompt
```
 - b. Riavviare SPL: `systemctl restart spl`
 - c. Eseguire una delle seguenti operazioni:

Se sei acceso...	Eseguire questa operazione...
Host del database Oracle	<ol style="list-style-type: none"> i. Assicurarsi che tutti i "prerequisiti" sono soddisfatti. ii. Fare clic su Backup and Recovery > applicazioni iii. Fare clic su ... Corrispondente all'applicazione e fare clic su View Details (Visualizza dettagli). iv. Modificare ID connettore.

Se sei acceso...	Eseguire questa operazione...
Host di database SAP HANA	<p>i. Assicurarsi che tutti i "prerequisiti" sono soddisfatti.</p> <p>ii. Eseguire il seguente comando:</p> <pre>curl --location --request PATCH 'https://snapcenter.cloudmanager .cloud.netapp.com/api/saphana/ho sts/connector/update' \ --header 'x-account-id: <CM account-id>' \ --header 'Authorization: Bearer token' \ --header 'Content-Type: application/json' \ --data-raw '{ "old_connector_id": "Old connector id that no longer exists", "new_connector_id": "New connector Id"}</pre> <p>I dettagli del connettore verranno aggiornati correttamente se tutti gli host hanno il plug-in SnapCenter per il servizio SAP HANA installato e in esecuzione e se sono tutti raggiungibili dal nuovo connettore.</p>

Configurare il certificato firmato dalla CA

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

Configurare il certificato firmato dalla CA per BlueXP Connector

Il connettore utilizza un certificato autofirmato per comunicare con il plug-in. Il certificato autofirmato viene importato nel keystore dallo script di installazione. Per sostituire il certificato autofirmato con il certificato firmato dalla CA, procedere come segue.

Fasi

1. Per utilizzare il certificato CA come certificato client quando il connettore si connette al plug-in, attenersi alla seguente procedura.
 - a. Accedere a Connector.
 - b. Eseguire il seguente comando per ottenere `<base_mount_path>`:

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

- c. Eliminare tutti i file esistenti che si trovano in `<base_mount_path>/client/certificate` nel connettore.
- d. 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.

- e. 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`

2. Per convalidare il certificato inviato dal connettore, eseguire le seguenti operazioni sull'host del plug-in.
 - a. Accedere all'host del plug-in.
 - b. Copiare il `certificate.pem` e i certificati per tutte le CA intermedie e root dal connettore all'host plug-in in `/var/opt/snapcenter/spl/etc/`.



Il formato della CA intermedia e del certificato della CA principale deve essere in formato `.crt`.

- c. Passare a `/var/opt/snapcenter/spl/etc` ed eseguire il comando `keytool` per importare il file `certificate.pem`.

```
keytool -import -alias agentcert -file certificate.pem -keystore
keystore.jks -deststorepass snapcenter -noprompt
```

- d. Importare la CA principale e i certificati intermedi.

```
keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter
-alias trustedca -file <certificate.crt>
```



Il `certificate.crt` fa riferimento ai certificati della CA principale e della CA intermedia.

- e. Riavviare SPL: `systemctl restart spl`

Configurare il certificato firmato dalla CA per il plug-in

Il certificato CA deve avere lo stesso nome registrato in Cloud Backup per l'host plug-in.

Fasi

1. Per ospitare il plug-in utilizzando il certificato CA, attenersi alla seguente procedura sull'host del plug-in.
 - a. Accedere alla cartella contenente il keystore della SPL `/var/opt/snapcenter/spl/etc`.
 - b. Creare il formato PKCS12 del certificato con certificato e chiave con alias `splkeystore`.

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

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

- a. Aggiungere il certificato CA creato nel passaggio precedente.

```
keytool -importkeystore -srckeystore certificate.p12 -srcstoretype pkcs12
-destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore
-destalias splkeystore -noprompt
```

- b. Verificare i certificati.

```
keytool -list -v -keystore keystore.jks
```

- c. Riavviare SPL: `systemctl restart spl`

2. Eseguire le seguenti operazioni sul connettore in modo che il connettore possa verificare il certificato del plug-in.

- a. Accedere al connettore come utente non root.

- b. Eseguire il seguente comando per ottenere `<base_mount_path>`:

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

- c. Copiare i file della CA principale e intermedia nella directory del server.

```
cd <base_mount_path>  
mkdir server
```

I file CA devono essere in formato pem.

- d. Connettersi a `cloud_scs_cloud` e modificare **enableCACert** in `config.yml` in **true**.

```
sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert:  
false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-  
cloud/config/config.yml
```

- e. Riavviare il container `cloud_scs_cloud`.

```
sudo docker restart cloudmanager_scs_cloud
```

Accedere alle API REST

Le API REST per proteggere le applicazioni nel cloud sono disponibili all'indirizzo:

<https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/>.

Per accedere alle API REST, è necessario ottenere il token utente con autenticazione federata. Per informazioni su come ottenere il token utente, fare riferimento a. "[Creare un token utente con autenticazione federata](#)".

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.