Backup von Cloud-nativen Applikationsdaten

Cloud Backup

NetApp
December 19, 2022

Inhaltsverzeichnis

Backup von Cloud-nativen Applikationsdaten

Backup Cloud-nativer Oracle Database

Zugriff auf BlueXP

Sollten Sie "melden Sie sich auf der NetApp BlueXP Website an", "Melden Sie sich bei BlueXP an", Und dann eine "NetApp Konto".

Konfigurieren Sie FSX für ONTAP

Sie sollten die Arbeitsumgebung FSX für ONTAP und den Connector erstellen.

Erstellung von FSX für ONTAP-Arbeitsumgebung

Sie sollten Amazon FSX für ONTAP-Arbeitsumgebungen erstellen, in denen Ihre Datenbanken gehostet werden. Weitere Informationen finden Sie unter "Erste Schritte mit Amazon FSX für ONTAP" Und "Erstellung und Management einer Amazon FSX für ONTAP Arbeitsumgebung".

Sie können NetApp FSX entweder mit BlueXP oder AWS erstellen. Falls Sie mit AWS erstellt haben, sollten Sie die FSX für ONTAP Systeme in BlueXP entdecken.

Einen Konnektor erstellen

Ein Account-Administrator muss einen Connector in AWS implementieren, der es BlueXP ermöglicht, Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu managen.

Weitere Informationen finden Sie unter "Erstellen eines Connectors in AWS aus BlueXP".

- Sie sollten denselben Konnektor verwenden, um sowohl FSX-Arbeitsumgebung als auch Oracle-Datenbanken zu verwalten.
- Wenn Sie über die FSX-Arbeitsumgebung und Oracle-Datenbanken in derselben VPC verfügen, können Sie den Connector in derselben VPC implementieren.
- Wenn Sie über die FSX-Arbeitsumgebung und Oracle-Datenbanken in verschiedenen VPCs verfügen:
  - Wenn auf FSX NAS-Workloads (NFS) konfiguriert sind, können Sie den Connector auf einem der VPCs erstellen.
  - Wenn nur SAN-Workloads konfiguriert sind und keine NAS- (NFS-) Workloads verwendet werden sollen, sollte der Connector in der VPC erstellt werden, über den das FSX-System erstellt wird.

> Für die Verwendung von NAS-Workloads (NFS) sollte ein Transit-Gateway zwischen der Oracle Database VPC und FSX VPC vorhanden sein. Auf die NFS-IP-Adresse, die eine unverankerte IP-Adresse ist, kann von einer anderen VPC nur über das Transit-Gateway zugegriffen werden. Wir können nicht auf die Floating IP-Adressen zugreifen, indem wir die VPCs Peering.

Klicken Sie nach dem Erstellen des Connectors auf **Storage** > **Canvas** > **Meine Arbeitsumgebung** > **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen, um die Arbeitsumgebung hinzuzufügen. Stellen Sie sicher, dass Konnektivität zwischen dem Connector und den Oracle-Datenbank-Hosts und der FSX-Arbeitsumgebung vorhanden ist. Der Anschluss sollte eine Verbindung zur Cluster-Management-IP-

Adresse der FSX-Arbeitsumgebung herstellen können.

Klicken Sie nach dem Erstellen des Connectors auf **Connector > Steckverbinder verwalten**; wählen Sie den Namen des Connectors aus, und kopieren Sie die Konnektor-ID.

Konfigurieren Sie Cloud Volumes ONTAP

Sie sollten die Cloud Volumes ONTAP-Arbeitsumgebung und den Connector erstellen.

Cloud Volumes ONTAP Arbeitsumgebung erstellen

Sie können vorhandene Cloud Volumes ONTAP-Systeme entdecken und zu BlueXP hinzufügen. Weitere Informationen finden Sie unter "Hinzufügen vorhandener Cloud Volumes ONTAP-Systeme zu BlueXP".

Einen Konnektor erstellen

Erste Schritte mit Cloud Volumes ONTAP für Ihre Cloud-Umgebung. Weitere Informationen finden Sie im Folgenden:

- "Schnellstart für Cloud Volumes ONTAP in AWS"
- "Schnellstart für Cloud Volumes ONTAP in Azure"
- "Schnellstart für Cloud Volumes ONTAP in Google Cloud"

Sie sollten denselben Konnektor verwenden, um sowohl die CVO-Arbeitsumgebung als auch Oracle-Datenbanken zu verwalten.

- Wenn die CVO Arbeitsumgebung und Oracle-Datenbanken im selben VPC oder vnet sind, können Sie den Connector in demselben VPC oder vnet implementieren.
- Wenn Sie über die CVO-Arbeitsumgebung und Oracle-Datenbanken in verschiedenen VPCs oder VNets verfügen, stellen Sie sicher, dass die VPCs oder VNets erreicht sind.

Fügen Sie Host hinzu und erkennen Sie Oracle Datenbanken

Sie sollten den Host hinzufügen und die Datenbanken auf dem Host erkennen, um Richtlinien zuzuweisen und Backups zu erstellen. Sie können den Host entweder manuell hinzufügen, wenn Sie das Plug-in bereits bereitgestellt haben, oder den Host über SSH hinzufügen.

Voraussetzungen

Bevor Sie den Host hinzufügen, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie sollten die Arbeitsumgebung und den Connector erstellt haben.
- Stellen Sie sicher, dass der Connector mit der Arbeitsumgebung und den Oracle-Datenbank-Hosts verbunden ist.
- Stellen Sie sicher, dass der BlueXP-Benutzer über die Rolle „Account Admin“ verfügt.
- Stellen Sie sicher, dass entweder Java 11 (64-Bit) Oracle Java oder OpenJDK auf jedem der Oracle-Datenbank-Hosts installiert ist und die JAVA_HOME-Variable entsprechend eingestellt ist.
- Sie sollten den nicht-Root-Benutzer erstellt haben. Weitere Informationen finden Sie unter Konfigurieren

Sie einen nicht-Root-Benutzer.

- Wenn Sie den Host manuell hinzufügen möchten, sollten Sie zuerst das Plug-in implementieren. Sie können das Plug-in entweder implementieren Manuell Oder Verwenden des Skripts.

  Sie sollten das Plug-in auf jedem der Oracle Datenbank-Hosts bereitstellen.

Konfigurieren Sie einen nicht-Root-Benutzer

Sie sollten einen nicht-Root-Benutzer für die Bereitstellung des Plug-ins konfigurieren.

Schritte

1. Melden Sie sich bei der Connector-VM an.
2. Laden Sie die SnapCenter Linux Host Plug-in-Binärdatei herunter.
   `sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'`
3. Ermitteln Sie den Mount-Pfad für die Basis.
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`
4. Kopieren Sie die Zeilen 1 bis 16 aus der Datei **oracle_checksum_scs.txt** unter ***base_Mount_PATH /Version*/sc-linux-Host-Plugin/**.
5. Melden Sie sich beim Oracle-Datenbank-Host an, und führen Sie die folgenden Schritte aus:
   a. Erstellen Sie das nicht-Root-Benutzerkonto, das private Schlüsselpaar und weisen Sie die Berechtigungen zu. Weitere Informationen finden Sie unter "Erstellen Sie ein Benutzerkonto".
   b. Fügen Sie die Zeilen, die Sie in Schritt 4 mit dem Dienstprogramm visudo Linux in die Datei */etc/sudoers* kopiert haben, ein.

      Ersetzen Sie in den obigen Zeilen den <LINUXUSER> durch den nicht-Root-Benutzer, den Sie erstellt haben, und speichern Sie die Datei im visudo-Dienstprogramm.

Stellen Sie das Plug-in manuell bereit

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Host nicht aktiviert ist, sollten Sie die folgenden manuellen Schritte durchführen, um das Plug-in bereitzustellen.

Schritte

1. Melden Sie sich bei der Connector-VM an.
2. Laden Sie die SnapCenter Linux Host Plug-in-Binärdatei herunter.
   `sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'`
3. Ermitteln Sie den Mount-Pfad für die Basis.
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`
4. Den Binärpfad des heruntergeladenen Plug-ins abrufen.
   `sudo ls <base_mount_path> $(sudo docker ps|grep -Po "cloudmanager_scs_cloud:.*? "|sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host-plugin/snapcenter_linux_host_plugin_scs.bin`

5. Kopieren Sie *snapcenter_linux_Host_Plugin_scs.bin* auf jeden der Oracle-Datenbank-Hosts, entweder mit scp oder anderen alternativen Methoden.

   Das *snapcenter_linux_Host_Plugin_scs.bin* sollte an einen Speicherort kopiert werden, auf den der nicht-Root-Benutzer zugreifen kann.

6. Melden Sie sich mit dem nicht-Root-Benutzerkonto beim Oracle-Datenbank-Host an, und führen Sie den folgenden Befehl aus, um Berechtigungen für die Binärdatei auszuführen.
   `chmod +x snapcenter_linux_host_plugin_scs.bin`
7. Stellen Sie das Oracle Plug-in als sudo-Benutzer ohne Root-Benutzer bereit.
   `./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-user>`
8. Kopieren Sie *Certificate.p12* von *<base_Mount_PATH>/Client/Certificate/* Pfad der Connector-VM auf den Plug-in-Host zu */var/opt/snapcenter/spl/etc/*.
9. Navigieren Sie zu */var/opt/snapcenter/spl/etc* und führen Sie den keytool-Befehl aus, um das Zertifikat zu importieren.
   ```
   keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12
   -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter
   -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
   ```
10. SPL neu starten: `systemctl restart spl`

Stellen Sie das Plug-in mithilfe von Skripten bereit

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Host für den nicht-Root-Benutzer aktiviert ist, können Sie die folgenden Schritte durchführen, um das Plug-in bereitzustellen. Bevor Sie die Schritte durchführen, stellen Sie sicher, dass die SSH-Verbindung zum Connector aktiviert ist.

Schritte

1. Melden Sie sich bei der Connector-VM an.
2. Ermitteln Sie den Mount-Pfad für die Basis.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
   docker volume inspect | grep Mountpoint
   ```
3. Stellen Sie das Plug-in mithilfe des im Konnektor enthaltenen Hilfsskripts bereit.
   ```
   sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host
   <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port>
   --pluginport <plugin_port> --installdir <install_dir>
   ```
   - Host_Name ist der Name des Oracle-Hosts, und dies ist ein obligatorischer Parameter.
   - ssh_Key_file ist der SSH-Schlüssel des nicht-root-Benutzers und wird für die Verbindung zum Oracle-Host verwendet. Dies ist ein obligatorischer Parameter.
   - User_Name: Nicht-Root-Benutzer mit SSH-Berechtigungen auf dem Oracle-Host und dies ist ein optionaler Parameter. Der Standardwert ist ec2-user.
   - ssh_Port: SSH-Port auf dem Oracle-Host und dies ist ein optionaler Parameter. Der Standardwert ist 22
   - Plugin_Port: Port verwendet vom Plug-in und dies ist ein optionaler Parameter. Der Standardwert ist 8145
   - Install_dir: Verzeichnis, in dem das Plug-in bereitgestellt wird und dies ein optionaler Parameter ist. Standardwert ist /opt.

Beispiel:

```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/oracle_plugin_copy_and_install.sh
--host xxx.xx.x.x --sshkey /keys/netapp-ssh.ppk
```

Fügen Sie Host hinzu

Fügen Sie den Host hinzu und ermitteln Sie die Oracle Datenbanken.

Schritte

1. Klicken Sie in der BlueXP-Benutzeroberfläche auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Klicken Sie Auf Anwendungen Ermitteln.
3. Wählen Sie **Cloud Native** und klicken Sie auf **Next**.

   Ein Servicekonto mit der Rolle *SnapCenter System* wird erstellt, um für alle Benutzer dieses Kontos geplante Datensicherungsvorgänge durchzuführen.

   - Klicken Sie auf **Konto** > **Konto verwalten** > **Mitglieder**, um das Servicekonto anzuzeigen.

   Das Service-Konto (*SnapCenter-Account-<accountid>*) wird für die Ausführung der geplanten Backup-Vorgänge verwendet. Sie sollten das Dienstkonto niemals löschen.

4. Führen Sie auf der Seite Host hinzufügen einen der folgenden Schritte aus:

Sie suchen…	Tun Sie das…
Beide Plug-ins implementiert haben Manuell Oder Verwenden des Skripts	a. Wählen Sie **Manuell**. b. Geben Sie den FQDN oder die IP-Adresse des Hosts an, auf dem das Plug-in bereitgestellt wird. Stellen Sie sicher, dass der Connector mit dem FQDN oder der IP-Adresse mit dem Datenbank-Host kommunizieren kann. c. Geben Sie den Plug-in-Port an. Standardport ist 8145. d. Wählen Sie den Anschluss aus. e. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass das Plug-in auf dem Host installiert ist f. Klicken Sie Auf **Anwendungen Entdecken**.

Sie suchen…	Tun Sie das…
Das Plug-in automatisch bereitstellen möchten	a. Wählen Sie **über SSH**. b. Geben Sie die FQDN- oder IP-Adresse des Hosts an, auf dem Sie das Plug-in installieren möchten. c. Geben Sie den Benutzernamen an (Nicht-Root-Benutzer) Mit dem das Plug-in-Paket auf den Host kopiert wird. d. Geben Sie SSH und Plug-in-Port an. Der standardmäßige SSH-Port ist 22 und der Plug-in-Port 8145. Nach der Installation des Plug-ins können Sie den SSH-Port auf dem Anwendungshost schließen. Der SSH-Port ist für andere Plug-in-Vorgänge nicht erforderlich. e. Wählen Sie den Anschluss aus. f. (Optional) Wenn die Authentifizierung ohne Schlüssel zwischen dem Connector und dem Host nicht aktiviert ist, müssen Sie den privaten SSH-Schlüssel angeben, der für die Kommunikation mit dem Host verwendet wird. Der private SSH-Schlüssel wird nicht an jedem Ort in der Applikation gespeichert und wird nicht für andere Vorgänge verwendet. g. Klicken Sie Auf **Weiter**.

- Zeigt alle Datenbanken auf dem Host an. Wenn die Betriebssystemauthentifizierung für die Datenbank deaktiviert ist, sollten Sie die Datenbankauthentifizierung konfigurieren, indem Sie auf **Configure** klicken. Weitere Informationen finden Sie unter Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank.
- Klicken Sie auf **Einstellungen** und wählen Sie **Hosts**, um alle Hosts anzuzeigen. Klicken Sie auf **Entfernen**, um einen Datenbank-Host zu entfernen.

  Der Filter zum Anzeigen eines bestimmten Hosts funktioniert nicht. Wenn Sie im Filter einen Hostnamen angeben, werden alle Hosts angezeigt.

- Klicken Sie auf **Einstellungen** und wählen Sie **Richtlinien**, um die vordefinierten Richtlinien anzuzeigen. Überprüfen Sie die vordefinierten Richtlinien, und wenn Sie möchten, können Sie sie entweder bearbeiten, um Ihre Anforderung zu erfüllen, oder erstellen Sie eine neue Richtlinie.

Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank

Sie sollten Anmeldedaten konfigurieren, die für Datensicherungsvorgänge in Oracle-Datenbanken verwendet werden.

Schritte

1. Wenn die Betriebssystemauthentifizierung für die Datenbank deaktiviert ist, sollten Sie die Datenbankauthentifizierung konfigurieren, indem Sie auf **Configure** klicken.
2. Geben Sie den Benutzernamen, das Kennwort und die Anschlussdetails an.

   Wenn sich die Datenbank auf ASM befindet, sollten Sie auch die ASM-Einstellungen konfigurieren.

   Der Oracle-Benutzer sollte über sysdba-Berechtigungen verfügen, und ASM-Benutzer sollten sysmasm-Berechtigungen haben.
3. Klicken Sie Auf **Konfigurieren**.

Backup Cloud-nativer Oracle Database

Sie sollten entweder eine vordefinierte Richtlinie oder die von Ihnen erstellte Richtlinie zuweisen und anschließend ein Backup erstellen.

Erstellen Sie eine Richtlinie zum Schutz von Oracle Datenbanken

Sie können Richtlinien erstellen, wenn Sie die vordefinierten Richtlinien nicht bearbeiten möchten.

Schritte

1. Wählen Sie auf der Seite Anwendungen aus der Dropdown-Liste Einstellungen die Option **Richtlinien** aus.
2. Klicken Sie auf **Create Policy**.
3. Geben Sie einen Richtliniennamen an.
4. (Optional) Bearbeiten Sie das Format des Backup-Namens.
5. Geben Sie den Zeitplan und die Aufbewahrungsdetails an.
6. Klicken Sie Auf **Erstellen**.

Erstellen Sie ein Backup der Oracle Database

Sie können entweder eine vordefinierte Richtlinie zuweisen oder eine Richtlinie erstellen und sie dann der Datenbank zuweisen. Sobald die Richtlinie zugewiesen ist, werden die Backups gemäß dem in der Richtlinie definierten Zeitplan erstellt.

Stellen Sie für Oracle beim Erstellen von ASM-Festplattengruppen sicher, dass es keine gemeinsamen Volumes über Festplattengruppen hinweg gibt. Jede Festplattengruppe benötigt dedizierte Volumes.

Schritte

1. Wenn die Datenbank nicht mit einer Richtlinie geschützt ist, klicken Sie auf der Seite Anwendungen auf **Richtlinie zuweisen**.

Wenn die Datenbank mit einer oder mehreren Richtlinien geschützt ist, können Sie durch Klicken auf weitere Richtlinien zuweisen ••• > **Richtlinie Zuweisen**.

2. Wählen Sie die Richtlinie aus und klicken Sie auf **Zuweisen**.

   Die Backups werden gemäß dem in der Richtlinie definierten Zeitplan erstellt.

   Das Servicekonto (*SnapCenter-Account-<Account_id>*) wird zur Ausführung der geplanten Backup-Vorgänge verwendet.

Erstellen eines On-Demand-Backups der Oracle Datenbank

Nach der Zuweisung der Richtlinie können Sie ein On-Demand-Backup der Applikation erstellen.

Schritte

1. Klicken Sie auf der Seite Anwendungen auf ••• Entsprechend der Anwendung und klicken Sie auf **On-Demand Backup**.
2. Wenn der Anwendung mehrere Richtlinien zugewiesen werden, wählen Sie die Richtlinie, den Aufbewahrungswert aus und klicken Sie dann auf **Backup erstellen**.

Weitere Informationen

Nach dem Wiederherstellen einer großen Datenbank (250 GB oder mehr), wenn Sie ein vollständiges Online-Backup in derselben Datenbank durchführen, kann der Vorgang mit dem folgenden Fehler fehlschlagen:

```
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.
```

Informationen zur Behebung dieses Problems finden Sie unter: "Der Snapshot-Vorgang ist aufgrund von durch Snapshots gesicherten Klonen nicht zulässig".

Einschränkungen

- Bietet keine Unterstützung für Online-Daten oder lediglich für Backup-Protokollierung
- Keine Unterstützung von Offline-Backups
- Unterstützt keine Sicherung der Oracle-Datenbank, die sich auf rekursiven Bereitstellungspunkten befindet
- Unterstützt keine Snapshots von Konsistenzgruppen für Oracle Datenbanken, die sich auf mehreren ASM-Festplattengruppen mit Überschneidungen von FSX Volumes befinden
- Wenn Ihre Oracle-Datenbanken auf ASM konfiguriert sind, stellen Sie sicher, dass Ihre SVM-Namen für die FSX-Systeme eindeutig sind. Wenn Sie in den FSX-Systemen denselben SVM-Namen haben, werden Backups der auf diesen SVMs befindlichen Oracle Datenbanken nicht unterstützt.

Backup der nativen Cloud-SAP HANA-Datenbank

Zugriff auf BlueXP

Sollten Sie "melden Sie sich auf der NetApp BlueXP Website an", "Melden Sie sich bei

BlueXP an", Und dann eine "NetApp Konto".

Konfigurieren Sie Azure NetApp Files

Sie sollten die Azure NetApp Files-Arbeitsumgebung und den Connector erstellen.

Azure NetApp Files Arbeitsumgebung erstellen

Sie sollten Azure NetApp Files (ANF)-Arbeitsumgebungen erstellen, in denen Ihre Datenbanken gehostet werden. Weitere Informationen finden Sie unter "Weitere Informationen zu Azure NetApp Files" Und "Schaffung einer Azure NetApp Files-Arbeitsumgebung".

Einen Konnektor erstellen

Ein Account-Administrator muss einen Connector in ANF implementieren, der es BlueXP ermöglicht, Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu managen.

Sie können die neue Connector_id nicht von der UI aktualisieren.

Weitere Informationen finden Sie unter "Erstellen Sie einen Connector in Azure von BlueXP".

Implementieren des SnapCenter-Plug-ins für SAP HANA

Das SnapCenter Plug-in für SAP HANA sollte auf jedem der SAP HANA Datenbank-Hosts implementiert werden. Je nachdem, ob auf dem SAP HANA-Host eine SSH-Schlüsselauthentifizierung aktiviert ist, können Sie eine der Methoden zur Bereitstellung des Plug-ins befolgen.

Vergewissern Sie sich, dass auf jedem der SAP HANA-Datenbank-Hosts Java 11 (64-Bit) oder OpenJDK installiert ist.

Konfigurieren Sie einen nicht-Root-Benutzer

Sie sollten einen nicht-Root-Benutzer erstellen, um das Plug-in bereitzustellen.

Schritte

1. Melden Sie sich bei der Connector-VM an.
2. Laden Sie die Linux-Host-Plug-in-Binärdatei herunter.
   `sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'`
3. Ermitteln Sie den Mount-Pfad für die Basis.
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`
4. Kopieren Sie Zeilen 1 bis 16 aus dem `oracle_checksum_scs.txt` Datei befindet sich unter `base_mount_path/version/sc-linux-host-plugin/`
5. Melden Sie sich beim SAP HANA Datenbank-Host an, und führen Sie die folgenden Schritte aus:
   a. Erstellen Sie das nicht-Root-Benutzerkonto, das private Schlüsselpaar und weisen Sie die Berechtigungen zu.

b. Fügen Sie die Zeilen ein, die Sie in Schritt 4 in die kopiert haben `/etc/sudoers` Datei mit dem Dienstprogramm visudo Linux.

   Ersetzen Sie in den obigen Zeilen den <LINUXUSER> durch den nicht-Root-Benutzer, den Sie im Visuod-Dienstprogramm erstellt und gespeichert haben.

Stellen Sie das Plug-in manuell bereit

Wenn die SSH-Schlüsselauthentifizierung auf dem HANA-Host nicht aktiviert ist, sollten Sie zur Bereitstellung des Plug-ins die folgenden manuellen Schritte durchführen.

Schritte

1. Melden Sie sich bei der Connector-VM an.
2. Laden Sie die Linux-Host-Plug-in-Binärdatei herunter.
   `# sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'`
3. Ermitteln Sie den Mount-Pfad für die Basis.
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`
4. Den Binärpfad des heruntergeladenen Plug-ins abrufen.
   `sudo ls <base_mount_path> $(sudo docker ps|grep -Po "cloudmanager_scs_cloud:.*? "|sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host-plugin/snapcenter_linux_host_plugin_scs.bin`
5. Kopieren `snapcenter_linux_host_plugin_scs.bin` Auf jeden der SAP HANA-Datenbank-Hosts entweder mit scp oder anderen alternativen Methoden.
6. Führen Sie auf dem SAP HANA-Datenbank-Host den folgenden Befehl aus, um Berechtigungen für die Binärdatei auszuführen.
   `chmod +x snapcenter_linux_host_plugin_scs.bin`
7. Bereitstellen des SAP HANA-Plug-ins als sudo-Non-Root-Benutzer.`/snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root-user>`
8. Kopieren Auf dem Plug-in-Host.
   a. Navigieren Sie zu `/var/opt/snapcenter/spl/etc and execute the keytool command to import the certificate.
      `keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt`
   b. SPL neu starten: `systemctl restart spl`

Implementieren Sie das Plug-in mithilfe der SSH-Schlüsselauthentifizierung

Wenn die SSH-Schlüsselbasierte Authentifizierung auf dem HANA-Host aktiviert ist, können Sie zur Bereitstellung des Plug-ins die folgenden Schritte durchführen. Bevor Sie die Schritte durchführen, stellen Sie sicher, dass die SSH-Verbindung zum Connector aktiviert ist.

Schritte

1. Melden Sie sich bei der Connector-VM an.
2. Ermitteln Sie den Mount-Pfad für die Basis.
   ```
   # sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs
   sudo docker volume inspect | grep Mountpoint
   ```
3. Plug-in implementieren
   ```
   # sudo <base_mount_path>/scripts/hana_plugin_copy_and_install.sh --host
   <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port>
   --pluginport <plugin_port> --installdir <install_dir>
   ```
   - Host_Name ist der Name des HANA-Hosts, und dies ist ein obligatorischer Parameter.
   - ssh_Key_file ist der SSH-Schlüssel, der für die Verbindung zum HANA-Host verwendet wird, und dies ist ein obligatorischer Parameter.
   - User_Name: Benutzer mit SSH-Berechtigungen auf dem HANA-Host, und dies ist ein optionaler Parameter. Der Standardwert ist Azureuser.
   - ssh_Port: SSH-Port auf dem HANA-Host, und dies ist ein optionaler Parameter. Der Standardwert ist 22.
   - Plugin_Port: Port wird vom Plug-in verwendet, und dies ist ein optionaler Parameter. Der Standardwert ist 8145.
   - Install_dir: Verzeichnis, in dem das Plug-in bereitgestellt wird, und dies ist ein optionaler Parameter. Standardwert ist /opt.

Backup der nativen Cloud-SAP HANA-Datenbank

Bevor Sie ein Backup der SAP HANA-Datenbank erstellen, sollten Sie die SAP HANA-Datenbank-Hosts hinzufügen und entweder eine vordefinierte Richtlinie oder die von Ihnen erstellte Richtlinie zuweisen.

Fügen Sie SAP HANA Datenbank-Hosts hinzu

Sie sollten SAP HANA-Datenbank-Hosts manuell hinzufügen, um Richtlinien zuzuweisen und Backups zu erstellen. Die automatische Erkennung des SAP HANA-Datenbank-Hosts wird nicht unterstützt.

Was Sie brauchen

- Sie sollten die Arbeitsumgebung hinzugefügt und den Connector erstellt haben.
- Stellen Sie sicher, dass der Connector mit der Arbeitsumgebung verbunden ist
- Stellen Sie sicher, dass der BlueXP-Benutzer über die Rolle „Account Admin“ verfügt.
- Sie sollten das SnapCenter Plug-in für SAP HANA implementiert haben. "Weitere Informationen ."
- Beim Hinzufügen der SAP HANA-Datenbank-Hosts sollten Sie die HDB-Benutzerspeicherschlüssel hinzufügen. Der HDB Secure User Store-Schlüssel wird verwendet, um die Verbindungsinformationen der SAP HANA Datenbank-Hosts sicher auf dem Client zu speichern und HDBSQL-Client verwendet den sicheren User Store-Schlüssel für die Verbindung zum SAP HANA-Datenbank-Host.
- Für HANA System Replication (HSR) sollten Sie zum Schutz der HANA-Systeme sowohl primäre als auch sekundäre HANA-Systeme manuell registrieren.

Schritte

1. Klicken Sie in der Benutzeroberfläche **BlueXP** auf **Schutz** > **Sicherung und Wiederherstellung** >

Anwendungen.

2. Klicken Sie Auf **Anwendungen Entdecken**.
3. Wählen Sie **Cloud Native** > **SAP HANA** und klicken Sie auf **Next**.
4. Klicken Sie auf der Seite **Anwendungen** auf **System hinzufügen**.
5. Führen Sie auf der Seite **Systemdetails** die folgenden Aktionen durch:

   a. Wählen Sie den Systemtyp als mandantenfähiger Datenbankcontainer oder einzelner Container aus.
   b. Geben Sie den SAP HANA-Systemnamen ein.
   c. Geben Sie die SID des SAP HANA-Systems an.
   d. (Optional) Geben Sie den HDBSQL OS-Benutzer an.
   e. Wählen Sie Plug-in-Host. (Optional) Wenn der Host nicht hinzugefügt wird oder Sie mehrere Hosts hinzufügen möchten, klicken Sie auf **Add Plug-in Host**.
   f. Wenn HANA-System mit HANA System Replication konfiguriert ist, aktivieren Sie **HANA System Replication (HSR) System**.
   g. Klicken Sie auf * HDB Secure User Store Keys* Textfeld, um Details zu den Benutzerspeicherschlüsseln hinzuzufügen.

      Geben Sie den Schlüsselnamen, die Systemdetails, den Benutzernamen und das Passwort an und klicken Sie auf **Schlüssel hinzufügen**.

   Sie können die Benutzerspeicherschlüssel löschen oder ändern.

6. Klicken Sie Auf **Weiter**.
7. Klicken Sie auf der Seite **Storage Footprint** auf **Speicher hinzufügen** und führen Sie Folgendes aus:
   a. Wählen Sie die Arbeitsumgebung aus und geben Sie den NetApp Account an.

      Gehen Sie zur Seite **Canvas**, um eine neue Arbeitsumgebung hinzuzufügen

   b. Wählen Sie die erforderlichen Volumes aus.
   c. Klicken Sie Auf **Speicher Hinzufügen**.
8. Überprüfen Sie alle Details und klicken Sie auf **System hinzufügen**.

Der Filter zum Anzeigen eines bestimmten Hosts funktioniert nicht. Wenn Sie im Filter einen Hostnamen angeben, werden alle Hosts angezeigt

Sie können SAP HANA-Systeme mithilfe DER REST-API ändern und entfernen. Vor dem Entfernen des HANA-Systems sollten Sie alle damit verbundenen Backups löschen und den Schutz entfernen.

Hinzufügen Von Nicht-Daten-Volumes

Nach dem Hinzufügen eines mandantenfähigen Datenbank-Containers oder eines einzelnen SAP HANA-Systems lassen sich die nicht-Daten-Volumes des HANA-Systems hinzufügen.

Schritte

1. Klicken Sie in der Benutzeroberfläche **BlueXP** auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.

2. Klicken Sie Auf **Anwendungen Entdecken**.
3. Wählen Sie **Cloud Native** > **SAP HANA** und klicken Sie auf **Next**.
4. Klicken Sie auf der Seite **Anwendungen** auf ••• Entsprechend dem System, für das Sie die nicht-Daten-Volumes hinzufügen möchten, und wählen Sie **System verwalten** > **nicht-Daten-Volume**.

Hinzufügen Von Globalen, Nicht Datenbasierten Volumes

Nach dem Hinzufügen eines mandantenfähigen Datenbank-Containers oder eines einzelnen SAP HANA-Systems lassen sich die globalen nicht-Data-Volumes des HANA-Systems hinzufügen.

Schritte

1. Klicken Sie in der Benutzeroberfläche **BlueXP** auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Klicken Sie Auf **Anwendungen Entdecken**.
3. Wählen Sie **Cloud Native** > **SAP HANA** und klicken Sie auf **Next**.
4. Klicken Sie auf der Seite **Anwendungen** auf **System hinzufügen**.
5. Führen Sie auf der Seite **Systemdetails** die folgenden Aktionen durch:
   a. Wählen Sie aus der Dropdown-Liste Systemtyp **globales Volume ohne Daten** aus.
   b. Geben Sie den SAP HANA-Systemnamen ein.
   c. Geben Sie die zugehörigen SIDs des SAP HANA-Systems an.
   d. Wählen Sie den Plug-in-Host aus

      (Optional) um mehrere Hosts hinzuzufügen, klicken Sie auf **Add Plug-in Host** und geben Sie den Hostnamen und Port an und klicken Sie auf **Add Host**.

   e. Klicken Sie Auf **Weiter**.
   f. Überprüfen Sie alle Details und klicken Sie auf **System hinzufügen**.

Vorschriften und Postskripte

Sie können Prescripts, Postskripte bereitstellen und Skripte beenden, während Sie eine Richtlinie erstellen. Diese Skripte werden auf dem HANA-Host während der Erstellung von Backups ausgeführt.

Das unterstützte Format für Skripte sind .sh, Python script, Perl script usw.

Das Prescript und das Postscript sollten vom Hostadministrator registriert werden `/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
```

Umgebungsvariablen

Für den Wiederherstellungsworkflow stehen die folgenden Umgebungsvariablen als Teil von Prescript und Postscript zur Verfügung.

Umgebungsvariable	Beschreibung
SID	Die Systemkennung der zur Wiederherstellung ausgewählten HANA-Datenbank
BackupName	Für den Wiederherstellungsvorgang ausgewählte Sicherungsname
UserStoreKeyNames	Konfigurierter Benutzerspeicherschlüssel für die HANA-Datenbank
OSDBUser	OSDBUser für die HANA-Datenbank konfiguriert
PolicyName	Nur für geplante Backups
Schedule_TYPE	Nur für geplante Backups

Erstellen einer Richtlinie zum Schutz von SAP HANA Datenbanken

Sie können Richtlinien erstellen, wenn Sie die vordefinierten Richtlinien nicht verwenden oder bearbeiten möchten.

1. Wählen Sie auf der Seite **Anwendungen** aus der Dropdown-Liste Einstellungen die Option **Richtlinien** aus.
2. Klicken Sie auf **Create Policy**.
3. Geben Sie einen Richtliniennamen an.
4. (Optional) Bearbeiten Sie das Format des Namens der Snapshot Kopie.
5. Wählen Sie den Richtlinientyp aus.
6. Geben Sie den Zeitplan und die Aufbewahrungsdetails an.
7. (Optional) Geben Sie die Skripte an.
8. Klicken Sie Auf **Erstellen**.

Backup der SAP HANA Datenbank erstellen

Sie können entweder eine vordefinierte Richtlinie zuweisen oder eine Richtlinie erstellen und sie dann der Datenbank zuweisen. Sobald die Richtlinie zugewiesen ist, werden die Backups gemäß dem in der Richtlinie definierten Zeitplan erstellt.

Über diese Aufgabe

Bei HANA System Replication (HSR) wird der geplante Backup-Job nur für das primäre HANA-System ausgelöst und wenn das System auf das sekundäre HANA-System überfällt, werden die bestehenden Zeitpläne ein Backup auf dem aktuellen primären HANA-System auslösen. Wird die Richtlinie nicht sowohl dem HANA-System zugewiesen, so schlägt nach dem Failover die Planung fehl.

Wenn den HSR-Systemen unterschiedliche Richtlinien zugewiesen werden, wird das geplante Backup sowohl für die Systeme ausgelöst, als auch das Backup schlägt für das sekundäre HANA-System fehl.

Schritte

1. Wenn die Datenbank nicht mit einer Richtlinie geschützt ist, klicken Sie auf der Seite Anwendungen auf **Richtlinie zuweisen**.

   Wenn die Datenbank mit einer oder mehreren Richtlinien geschützt ist, können Sie durch Klicken auf weitere Richtlinien zuweisen ••• > **Richtlinie Zuweisen**.

2. Wählen Sie die Richtlinie aus und klicken Sie auf **Zuweisen**.

   Die Backups werden gemäß dem in der Richtlinie definierten Zeitplan erstellt.

   ⓘ Das Servicekonto (*SnapCenter-Account-<Account_id>*) wird zur Ausführung der geplanten Backup-Vorgänge verwendet.

On-Demand-Backup der SAP HANA-Datenbank erstellen

Nach der Zuweisung der Richtlinie können Sie ein On-Demand-Backup der Applikation erstellen.

Schritte

1. Klicken Sie auf der Seite **Anwendungen** auf ••• Entsprechend der Anwendung und klicken Sie auf **On-Demand Backup**.
2. Wählen Sie den Backup-Typ nach Bedarf aus.
3. Wählen Sie für eine Policy-basierte Sicherung die Policy, die Aufbewahrungsebene aus und klicken Sie dann auf **Backup erstellen**.
4. Führen Sie zunächst die folgenden Schritte aus:
   a. Wählen Sie den Aufbewahrungswert aus, und geben Sie den Backup-Namen an.
   b. (Optional) Geben Sie die Skripte und den Pfad für die Skripte an.
   c. Klicken Sie Auf **Backup Erstellen**.