



Backup von Cloud-nativen Oracle-Datenbanken

BlueXP backup and recovery

NetApp
April 18, 2024

This PDF was generated from <https://docs.netapp.com/de-de/bluexp-backup-recovery/task-quick-start-oracle.html> on April 18, 2024. Always check docs.netapp.com for the latest.

Inhalt

- Backup von Cloud-nativen Oracle-Datenbanken 1
 - Schnellstart 1
 - Konfigurieren Sie FSX für ONTAP 2
 - Konfigurieren Sie Cloud Volumes ONTAP 3
 - Konfigurieren Sie Azure NetApp Files 3
 - Installieren Sie das SnapCenter Plug-in für Oracle und fügen Sie Datenbank-Hosts hinzu 4
 - Backup von Cloud-nativen Oracle-Datenbanken 11

Backup von Cloud-nativen Oracle-Datenbanken

Schnellstart

Führen Sie die folgenden Schritte aus, um schnell zu beginnen:

1

Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Betriebssystem:
 - RHEL 7.5 oder höher und 8.x
 - L 7.5 oder höher und 8.x
 - SLES 15 SP4
- NetApp Cloud-Storage:
 - Amazon FSX für NetApp ONTAP
 - Cloud Volumes ONTAP
 - Azure NetApp Dateien
- Storage-Layouts:
 - NFS v3 und v4.1 (einschließlich dNFS)
 - iSCSI mit ASM (ASMFD, ASMLib und ASMUdev)



Azure NetApp Files unterstützt keine SAN-Umgebung.

- Datenbank-Layouts: Oracle Standard und Oracle Enterprise Standalone (veraltete und mandantenfähige CDB und PDB)
- Datenbankversionen: 19c und 21c

2

Melden Sie sich bei BlueXP an

Der Zugriff auf BlueXP erfolgt über eine webbasierte Konsole. Wenn Sie mit BlueXP starten, müssen Sie sich zunächst mit Ihren vorhandenen Zugangsdaten auf der NetApp Support Website anmelden oder ein NetApp Cloud-Login erstellen. Weitere Informationen finden Sie unter ["Melden Sie sich bei BlueXP an"](#).

3

Melden Sie sich bei BlueXP an

Nachdem Sie sich bei BlueXP angemeldet haben, können Sie sich über die webbasierte Konsole anmelden. Weitere Informationen finden Sie unter ["Melden Sie sich bei BlueXP an"](#).

4

Managen Sie Ihr BlueXP Konto

Sie können Ihr Konto verwalten, indem Sie Benutzer, Servicekonten, Arbeitsbereiche und Connectors verwalten. Weitere Informationen finden Sie unter ["Managen Sie Ihr BlueXP Konto"](#).

Konfigurieren Sie FSX für ONTAP

Mit BlueXP sollten Sie eine Arbeitsumgebung FSX for ONTAP erstellen, um Volumes und zusätzliche Datenservices hinzuzufügen und zu managen. Sie sollten auch einen Connector in AWS erstellen, mit dem BlueXP Ressourcen und Prozesse in der Public Cloud-Umgebung des Kunden managen kann.

Erstellung von FSX für ONTAP-Arbeitsumgebung

Sie sollten die 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"](#).

Die Arbeitsumgebung FSX for ONTAP lässt sich 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 Kontoadministrator muss einen Connector in AWS erstellen, mit dem BlueXP Ressourcen und Prozesse in der Public Cloud-Umgebung des Kunden managen kann.

Weitere Informationen finden Sie unter ["Erstellen eines Connectors in AWS aus BlueXP"](#).

- Sie sollten denselben Konnektor verwenden, um sowohl FSX für ONTAP Arbeitsumgebungen als auch Datenbanken zu verwalten.
- Wenn die Arbeitsumgebung FSX for ONTAP und Datenbanken in derselben Virtual Private Cloud (VPC) liegen, können Sie den Connector in derselben VPC implementieren.
- Wenn Sie die FSX for ONTAP Arbeitsumgebung und Datenbanken in verschiedenen VPCs haben:
 - Wenn Sie NAS (NFS) Workloads auf FSX für ONTAP konfiguriert haben, können Sie den Connector auf einem der vPCs erstellen.
 - Wenn Sie nur SAN-Workloads konfiguriert haben und keine NAS (NFS)-Workloads verwenden möchten, sollten Sie den Connector in der VPC erstellen, wo das FSX für ONTAP-System erstellt wird.



Für die Nutzung von NAS-Workloads (NFS) sollten Sie über ein Transit-Gateway zwischen der Datenbank VPC und Amazon VPC verfügen. 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 **Speicher > Leinwand > Meine Arbeitsumgebung > Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen, um die Arbeitsumgebung hinzuzufügen. Stellen Sie sicher, dass eine Verbindung zwischen dem Connector und den Oracle-Datenbank-Hosts und der FSX-Arbeitsumgebung besteht. Der Connector sollte in der Lage sein, eine Verbindung zur Cluster-Management-IP-Adresse der FSX Arbeitsumgebung herzustellen.

- Fügen Sie die Arbeitsumgebung hinzu, indem Sie auf **Speicher > Leinwand > Meine Arbeitsumgebung > Arbeitsumgebung hinzufügen** klicken.

Stellen Sie sicher, dass eine Verbindung zwischen dem Connector und den Datenbank-Hosts und der Arbeitsumgebung von FSX for ONTAP besteht. Der Connector sollte eine Verbindung zur Cluster-

Management-IP-Adresse der Arbeitsumgebung FSX für ONTAP herstellen.

- Kopieren Sie die Connector-ID, indem Sie auf **Connector > Connectors verwalten** klicken und den Connector-Namen auswählen.

Konfigurieren Sie Cloud Volumes ONTAP

Mit BlueXP sollten Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen, um Volumes und zusätzliche Datenservices hinzuzufügen und zu managen. Sie sollten auch einen Connector für Ihre Cloud-Umgebung erstellen, mit dem BlueXP Ressourcen und Prozesse in der Public Cloud-Umgebung managen kann.

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 in einer der folgenden Links:

- ["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 Cloud Volumes ONTAP-Arbeitsumgebungen als auch Datenbanken zu verwalten.

- Wenn sich die Arbeitsumgebung von Cloud Volumes ONTAP und Datenbanken in derselben virtuellen Private Cloud (VPC) oder vnet befinden, können Sie den Connector in derselben VPC oder vnet implementieren.
- Wenn Sie die Cloud Volumes ONTAP-Arbeitsumgebung und Datenbanken in verschiedenen VPCs oder VNets haben, stellen Sie sicher, dass die VPCs oder VNets peered sind.

Konfigurieren Sie Azure NetApp Files

Mit BlueXP sollten Sie eine Azure NetApp Files Arbeitsumgebung erstellen, um Volumes und zusätzliche Datenservices hinzuzufügen und zu managen. Sie sollten auch einen Connector in Azure erstellen, mit dem BlueXP Ressourcen und Prozesse in der Public Cloud-Umgebung des Kunden managen kann.

Azure NetApp Files Arbeitsumgebung erstellen

Sie sollten Azure NetApp Files-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 BlueXP Account-Administrator sollte einen Connector in Azure implementieren, der BlueXP ermöglicht, Ressourcen und Prozesse in der Public Cloud-Umgebung zu managen.

Weitere Informationen finden Sie unter ["Erstellen Sie einen Connector in Azure von BlueXP"](#).

- Stellen Sie sicher, dass eine Verbindung zwischen dem Connector und den Datenbank-Hosts besteht.
- Wenn sich die Azure NetApp Files-Arbeitsumgebung und -Datenbanken im gleichen virtuellen Netzwerk (vnet) befinden, können Sie den Connector im gleichen vnet bereitstellen.
- Wenn Sie die Arbeitsumgebung von Azure NetApp Files und Datenbanken in verschiedenen VNets haben und NAS (NFS) Workloads auf Azure NetApp Files konfiguriert haben, können Sie den Connector auf einem der VNets erstellen.

Fügen Sie nach dem Erstellen des Connectors die Arbeitsumgebung hinzu, indem Sie auf **Speicher > Leinwand > Meine Arbeitsumgebung > Arbeitsumgebung hinzufügen** klicken.

Installieren Sie das SnapCenter Plug-in für Oracle und fügen Sie Datenbank-Hosts hinzu

Sie sollten das SnapCenter-Plug-in für Oracle auf jedem der Oracle-Datenbank-Hosts installieren, die Datenbank-Hosts hinzufügen und die Datenbanken auf dem Host ermitteln, um Richtlinien zuzuweisen und Backups zu erstellen.

- Wenn SSH für den Datenbank-Host aktiviert ist, können Sie das Plug-in mithilfe einer der folgenden Methoden installieren:
 - Installieren Sie das Plug-in, und fügen Sie den Host über die Benutzeroberfläche mithilfe der SSH-Option hinzu. [Weitere Informationen ..](#)
 - Installieren Sie das Plug-in mithilfe des Skripts und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu. [Weitere Informationen ..](#)
- Wenn SSH deaktiviert ist, installieren Sie das Plug-in manuell und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu. [Weitere Informationen ..](#)

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 über eine Verbindung zu den Oracle-Datenbank-Hosts verfügt.

Informationen zur Behebung des Verbindungsproblem finden Sie unter ["Fehler beim Validieren der Verbindung vom BlueXP Connector-Host zum Applikationsdatenbank-Host"](#).

Wenn der Connector verloren geht oder Sie einen neuen Connector erstellt haben, sollten Sie den Connector den vorhandenen Anwendungsressourcen zuordnen. Anweisungen zum Aktualisieren des Connectors finden Sie unter ["Aktualisieren Sie die Verbindungsdetails"](#).

- Stellen Sie sicher, dass der BlueXP-Benutzer über die Rolle „Account Admin“ verfügt.
- Stellen Sie sicher, dass das nicht-Root-Konto (sudo) für Datenschutzvorgänge auf dem Anwendungshost vorhanden ist.

- 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.
- Stellen Sie sicher, dass für den Connector die Kommunikation zum SSH-Port aktiviert ist (Standard: 22), wenn eine SSH-basierte Installation durchgeführt wird.
- Stellen Sie sicher, dass der Connector die Kommunikation für den Plug-in-Port aktiviert hat (Standard: 8145), damit die Datenschutzvorgänge funktionieren.
- Stellen Sie sicher, dass die neueste Version des Plug-ins installiert ist. Informationen zum Aktualisieren des Plug-ins finden Sie unter [Upgrade des SnapCenter Plug-in für Oracle Database](#).

Fügen Sie den Host über die Benutzeroberfläche mithilfe der SSH-Option hinzu

Schritte

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

Wenn Sie bereits einen Host hinzugefügt haben und einen weiteren Host hinzufügen möchten, klicken Sie auf **Anwendungen > Datenbanken verwalten > Hinzufügen** und fahren Sie dann mit Schritt 5 fort.

2. Klicken Sie Auf **Anwendungen Entdecken**.
3. Wählen Sie **Cloud Native** und klicken Sie auf **Next**.

Ein Servicekonto (*SnapCenter-Account-`<accountid>`*) mit der Rolle *SnapCenter System* wird erstellt, um geplante Datensicherungsvorgänge für alle Benutzer in diesem Konto durchzuführen. Das Servicekonto (*SnapCenter-Account-`<accountid>`*) wird für die geplanten Backup-Vorgänge verwendet. Sie sollten das Dienstkonto niemals löschen. Sie können das Service-Konto anzeigen, indem Sie auf **Konto > Konto verwalten > Mitglieder** klicken.

4. Wählen Sie Oracle als Anwendungstyp aus.
5. Führen Sie auf der Seite Host-Details folgende Schritte aus:

- a. Wählen Sie **über SSH**.
- b. Geben Sie die FQDN- oder IP-Adresse des Hosts an, auf dem Sie das Plug-in installieren möchten.

Stellen Sie sicher, dass der Connector mit dem Datenbankhost über den FQDN oder die IP-Adresse kommunizieren kann.

- c. Geben Sie den Benutzer non-root(sudo) an, mit dem das Plug-in-Paket auf den Host kopiert wird.

Root-Benutzer wird nicht unterstützt.

- 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 keine Datensicherungsvorgänge erforderlich.

- a. Wählen Sie den Anschluss aus.
- b. (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 an keiner beliebigen Stelle in der Anwendung gespeichert und nicht für andere Vorgänge verwendet.

- c. Klicken Sie Auf **Weiter**.
6. Führen Sie auf der Seite Konfiguration die folgenden Schritte aus:
 - a. Konfigurieren Sie den sudo-Zugriff für den SnapCenter-Benutzer im Oracle-Datenbank-Host, indem Sie sich bei dem Linux-Rechner anmelden, auf dem die Oracle-Datenbank ausgeführt wird.
 - b. Kopieren Sie den in der BlueXP UI angezeigten Text.
 - c. Erstellen Sie die Datei `/etc/sudoers.d/snapcenter` auf dem Linux-Rechner und fügen Sie den kopierten Text ein.
 - d. Aktivieren Sie in der BlueXP UI das Kontrollkästchen und klicken Sie auf **Weiter**.
7. Überprüfen Sie die Details und klicken Sie auf **Anwendungen entdecken**.
 - Nach der Installation des Plug-ins wird der Erkennungsvorgang gestartet.
 - Nach Abschluss des Ermittlungsvorgangs werden alle Datenbanken auf dem Host angezeigt. Wenn die OS-Authentifizierung für die Datenbank deaktiviert ist, klicken Sie auf **Configure**, um die Datenbankauthentifizierung zu aktivieren. 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 **Einstellungen** und wählen Sie **Richtlinien**, um die vordefinierten Richtlinien anzuzeigen. Überprüfen Sie die vordefinierten Richtlinien, und Sie können sie entweder nach Ihren Anforderungen bearbeiten oder eine neue Richtlinie erstellen.

Fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu, und installieren Sie das Plug-in mithilfe des Skripts

Konfigurieren Sie die auf SSH-Schlüsseln basierende Authentifizierung für das nicht-root-Benutzerkonto des Oracle-Hosts und führen Sie die folgenden Schritte durch, um das Plug-in zu installieren.

Bevor Sie beginnen

Stellen Sie sicher, dass die SSH-Verbindung zum Connector aktiviert ist.

Schritte

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

Ein Servicekonto (*SnapCenter-Account-`<accountid>`*) mit der Rolle *SnapCenter System* wird erstellt, um geplante Datensicherungsvorgänge für alle Benutzer in diesem Konto durchzuführen. Das Servicekonto (*SnapCenter-Account-`<accountid>`*) wird für die geplanten Backup-Vorgänge verwendet. Sie sollten das Dienstkonto niemals löschen. Sie können das Service-Konto anzeigen, indem Sie auf **Konto > Konto verwalten > Mitglieder** klicken.

4. Wählen Sie Oracle als Anwendungstyp aus.
5. Führen Sie auf der Seite Host-Details folgende Schritte aus:
 - a. Wählen Sie **Manuell**.

b. Geben Sie den FQDN oder die IP-Adresse des Hosts an, auf dem das Plug-in installiert ist.

Stellen Sie sicher, dass der Connector mit dem Datenbankhost über den FQDN oder die IP-Adresse kommunizieren kann.

c. Geben Sie den Plug-in-Port an.

Standardport ist 8145.

d. Geben Sie den nicht-Root-Benutzer (sudo) an, mit dem das Plug-in-Paket auf den Host kopiert wird.

e. Wählen Sie den Anschluss aus.

f. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass das Plug-in auf dem Host installiert ist.

g. Klicken Sie Auf **Weiter**.

6. Führen Sie auf der Seite Konfiguration die folgenden Schritte aus:

a. Konfigurieren Sie den sudo-Zugriff für den SnapCenter-Benutzer im Oracle-Datenbank-Host, indem Sie sich bei dem Linux-Rechner anmelden, auf dem die Oracle-Datenbank ausgeführt wird.

b. Kopieren Sie den in der BlueXP UI angezeigten Text.

c. Erstellen Sie die Datei `/etc/sudoers.d/snapcenter` auf dem Linux-Rechner und fügen Sie den kopierten Text ein.

d. Aktivieren Sie in der BlueXP UI das Kontrollkästchen und klicken Sie auf **Weiter**.

7. Melden Sie sich bei der Connector-VM an.

8. Installieren Sie das Plug-in mit dem im Connector bereitgestellten Skript.

```
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>
```

Wenn Sie einen älteren Connector verwenden, führen Sie den folgenden Befehl aus, um das Plug-in zu installieren.

```
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>
```

| Name | Beschreibung | Obligatorisch | Standard |
|----------------|--|---------------|----------|
| Plugin_Host | Gibt den Oracle-Host an | Ja. | - |
| Host_User_Name | Gibt den SnapCenter-Benutzer mit SSH-Berechtigungen auf dem Oracle-Host an | Ja. | - |
| Host_ssh_Key | Gibt den SSH-Schlüssel des SnapCenter-Benutzers an und wird zur Verbindung mit dem Oracle-Host verwendet | Ja. | - |

| Name | Beschreibung | Obligatorisch | Standard |
|---------------|--|---------------|----------|
| Plugin_Port | Gibt den vom Plug-in verwendeten Port an | Nein | 8145 |
| Host_ssh_Port | Gibt den SSH-Port auf dem Oracle-Host an | Nein | 22 |

Beispiel:

- `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. Überprüfen Sie in der BlueXP UI die Details, und klicken Sie auf **Anwendungen ermitteln**.

- Nach Abschluss des Ermittlungsvorgangs werden alle Datenbanken auf dem Host angezeigt. Wenn die OS-Authentifizierung für die Datenbank deaktiviert ist, klicken Sie auf **Configure**, um die Datenbankauthentifizierung zu aktivieren. 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 **Einstellungen** und wählen Sie **Richtlinien**, um die vordefinierten Richtlinien anzuzeigen. Überprüfen Sie die vordefinierten Richtlinien, und Sie können sie entweder nach Ihren Anforderungen bearbeiten oder eine neue Richtlinie erstellen.

Fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu, und installieren Sie das Plug-in manuell

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Datenbank-Host nicht aktiviert ist, sollten Sie die folgenden manuellen Schritte ausführen, um das Plug-in zu installieren und dann den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzuzufügen.

Schritte

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

Ein Servicekonto (*SnapCenter-Account-**<accountid>***) mit der Rolle *SnapCenter System* wird erstellt, um geplante Datensicherungsvorgänge für alle Benutzer in diesem Konto durchzuführen. Das Servicekonto (*SnapCenter-Account-**<accountid>***) wird für die geplanten Backup-Vorgänge verwendet. Sie sollten das Dienstkonto niemals löschen. Sie können das Service-Konto anzeigen, indem Sie auf **Konto > Konto verwalten > Mitglieder** klicken.

4. Wählen Sie Oracle als Anwendungstyp aus.
5. Führen Sie auf der Seite **Host Details** folgende Schritte aus:

- a. Wählen Sie **Manuell**.
- b. Geben Sie den FQDN oder die IP-Adresse des Hosts an, auf dem das Plug-in installiert ist.

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. Geben Sie den Benutzer `sudo non-root (sudo)` an, mit dem das Plug-in-Paket auf den Host kopiert wird.
- e. Wählen Sie den Anschluss aus.
- f. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass das Plug-in auf dem Host installiert ist.
- g. Klicken Sie Auf **Weiter**.

6. Führen Sie auf der Seite Konfiguration die folgenden Schritte aus:

- a. Konfigurieren Sie den `sudo`-Zugriff für den SnapCenter-Benutzer im Oracle-Datenbank-Host, indem Sie sich bei dem Linux-Rechner anmelden, auf dem die Oracle-Datenbank ausgeführt wird.
- b. Kopieren Sie den in der BlueXP UI angezeigten Text.
- c. Erstellen Sie die Datei `/etc/sudoers.d/snapcenter` auf dem Linux-Rechner und fügen Sie den kopierten Text ein.
- d. Aktivieren Sie in der BlueXP UI das Kontrollkästchen und klicken Sie auf **Weiter**.

7. Melden Sie sich bei der Connector-VM an.

8. 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'
```

Die Plug-in-Binärdatei ist verfügbar unter: `cd /var/lib/Docker/Volumes/Service-Manager[1]-2_Cloudmanager_scs_Cloud_Volume/_Data/€(sudo docker ps grep -Po "Cloudmanager_scs_Cloud:.*?"/sed -e s/ *€/ / Cut -f2 -d".")/sc-linux-Host-Plugin`

9. Kopieren Sie `snapcenter_linux_Host_Plugin_scs.bin` von dem obigen Pfad zu `/Home/<non root user (sudo)>/sc_netapp` Pfad für jeden der Oracle-Datenbank-Hosts, entweder mit `scp` oder anderen alternativen Methoden.

10. Melden Sie sich über das nicht-Root-Konto (`sudo`) beim Oracle-Datenbank-Host an.

11. Ändern Sie das Verzeichnis in `/Home/<non root user>/sc_netapp/` und führen Sie den folgenden Befehl aus, um die Ausführungsberechtigungen für die Binärdatei zu aktivieren.

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

12. Installieren Sie das Oracle Plug-in als `sudo SnapCenter-Benutzer`.

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

13. Kopieren Sie `Certificate.pem` vom `<base_mount_path>/Client/Certificate/` Pfad der Konnektor-VM nach `/var/opt/snapcenter/spl/etc/` auf den Plug-in-Host.

14. Navigieren Sie zu `/var/opt/snapcenter/spl/etc` und führen Sie den Befehl `keytool` aus, um die Datei `Certificate.pem` zu importieren.

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

15. SPL neu starten: `systemctl restart spl`

16. Überprüfen Sie, ob das Plug-in über den Connector erreichbar ist, indem Sie den folgenden Befehl über den Connector ausführen.

```
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. Überprüfen Sie in der BlueXP UI die Details, und klicken Sie auf **Anwendungen ermitteln**.

- Nach Abschluss des Ermittlungsvorgangs werden alle Datenbanken auf dem Host angezeigt. Wenn die OS-Authentifizierung für die Datenbank deaktiviert ist, klicken Sie auf **Configure**, um die Datenbankauthentifizierung zu aktivieren. 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 **Einstellungen** und wählen Sie **Richtlinien**, um die vordefinierten Richtlinien anzuzeigen. Überprüfen Sie die vordefinierten Richtlinien, und Sie können sie entweder nach Ihren Anforderungen bearbeiten oder eine neue Richtlinie erstellen.

Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank

Sie sollten die Datenbankanmeldeinformationen konfigurieren, die zur Durchführung von Datensicherungsvorgängen in Oracle-Datenbanken verwendet werden.

Schritte

1. Wenn die OS-Authentifizierung für die Datenbank deaktiviert ist, klicken Sie auf **Configure**, um die Datenbankauthentifizierung zu ändern.
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 sysasm-Berechtigungen haben.

3. Klicken Sie Auf **Konfigurieren**.

Upgrade des SnapCenter Plug-in für Oracle Database

Sie sollten das SnapCenter-Plug-in für Oracle aktualisieren, um auf die neuesten Funktionen und Verbesserungen zugreifen zu können. Sie können ein Upgrade über die BlueXP UI oder über die Befehlszeile durchführen.

Bevor Sie beginnen

- Stellen Sie sicher, dass auf dem Host keine Vorgänge ausgeführt werden.

Schritte

1. Klicken Sie auf **Sicherung und Wiederherstellung > Anwendungen > Hosts**.
2. Überprüfen Sie, ob ein Plug-in-Upgrade für einen der Hosts verfügbar ist, indem Sie die Spalte Gesamtstatus überprüfen.
3. Aktualisieren Sie das Plug-in über die Benutzeroberfläche oder über die Befehlszeile.

| Upgrade über UI | Upgrade über Befehlszeile |
|---|---|
| <p>a. Klicken Sie Auf ... Dem Host entsprechend und klicken Sie auf Upgrade Plug-in.</p> <p>b. Führen Sie auf der Seite Konfiguration die folgenden Schritte aus:</p> <ol style="list-style-type: none"> Konfigurieren Sie den sudo-Zugriff für den SnapCenter-Benutzer im Oracle-Datenbank-Host, indem Sie sich bei dem Linux-Rechner anmelden, auf dem die Oracle-Datenbank ausgeführt wird. Kopieren Sie den in der BlueXP UI angezeigten Text. Bearbeiten Sie die Datei <code>/etc/sudoers.d/snapcenter</code> auf dem Linux-Rechner und fügen Sie den kopierten Text ein. Aktivieren Sie in der BlueXP UI das Kontrollkästchen und klicken Sie auf Upgrade. | <p>a. Melden Sie sich bei Connector VM an.</p> <p>b. Führen Sie das folgende Skript aus.</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>Wenn Sie einen älteren Connector verwenden, führen Sie den folgenden Befehl aus, um das Plug-in zu aktualisieren.</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> |

Backup von Cloud-nativen Oracle-Datenbanken

Sie können geplante oder On-Demand-Backups erstellen, indem Sie eine vordefinierte Richtlinie oder die von Ihnen erstellte Richtlinie zuweisen.

Sie können die Backups der Oracle-Datenbank auch mit Oracle Recovery Manager (RMAN) katalogisieren, wenn Sie die Katalogisierung beim Erstellen einer Richtlinie aktiviert haben. Die (RMAN) Katalogisierung wird nur für die Datenbanken auf Azure NetApp Files unterstützt. Die katalogisierten Backups können später für Wiederherstellungen auf Blockebene oder für zeitpunktgenaue Recovery-Vorgänge in Tablespace verwendet werden. Die Datenbank muss im gemounteten oder höheren Zustand für die Katalogisierung enthalten sein.

Erstellen einer Richtlinie zum Schutz der Oracle-Datenbank

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

Schritte

- Wählen Sie auf der Seite Anwendungen aus der Dropdown-Liste Einstellungen die Option **Richtlinien** aus.
- Klicken Sie auf **Create Policy**.
- Geben Sie einen Richtliniennamen an.

4. (Optional) Bearbeiten Sie das Format des Backup-Namens.
5. Geben Sie den Zeitplan und die Aufbewahrungsdetails an.
6. Wenn Sie *Daily* und *Weekly* als Zeitplan ausgewählt haben und RMAN-Katalogisierung aktivieren möchten, wählen Sie **Catalog Backup with Oracle Recovery Manager (RMAN)** aus.
7. (Optional) Geben Sie den Pfad und den Timeout-Wert für das Post-Skript ein, das nach dem erfolgreichen Backup ausgeführt wird, z. B. das Kopieren des Snapshots in den sekundären Speicher.

Optional können Sie auch die Argumente angeben.

Sie sollten die Post-Skripte im Pfad `/var/opt/snapcenter/spl/scripts` belassen.

Das Post-Skript unterstützt eine Reihe von Umgebungsvariablen.

| Umgebungsvariable | Beschreibung |
|---|---|
| SC_ORACLE_SID | Gibt die SID der Oracle-Datenbank an. |
| SC_HOST | Gibt den Hostnamen der Datenbank an |
| SC_BACKUP_NAME | Gibt den Namen des Backups an. Der Name der Datensicherung und der Name der Protokollsicherung werden mit Trennzeichen verkettet. |
| SC_BACKUP_POLICY_NAME | Gibt den Namen der Richtlinie an, die zum Erstellen des Backups verwendet wird. |
| SC_PRIMARY_DATA_VOLUME_FULL_PATH | Gibt die Pfade des Datenvolumes an, die mit „“ als Trennzeichen verbunden sind. Bei Azure NetApp Files-Volumes werden die Informationen mithilfe von „/“ verkettet. _/ /Abonnements/{subscription_id}/resourceGroups/{Resource_Group}/Providers/{Provider}/netAppAccounts/{anfacount}/capacityPools/{Capacity_Pool}/Volumes/{volumename}_ |
| SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH | Gibt die Volume-Pfade des Archivprotokolls an, die mit „“ als Trennzeichen verbunden sind. Bei Azure NetApp Files-Volumes werden die Informationen mithilfe von „/“ verkettet. _/ /Abonnements/{subscription_id}/resourceGroups/{Resource_Group}/Providers/{Provider}/netAppAccounts/{anfacount}/capacityPools/{Capacity_Pool}/Volumes/{volumename}_ |

8. Klicken Sie Auf **Erstellen**.


Konfigurieren Sie das RMAN-Katalog-Repository

Sie können die Datenbank des Wiederherstellungskatalogs als RMAN-Katalogrepository konfigurieren. Wenn Sie das Repository nicht konfigurieren, wird die Steuerdatei der Zieldatenbank standardmäßig zum RMAN-Katalog-Repository.

Bevor Sie beginnen

Sie sollten die Zieldatenbank manuell bei der RMAN-Katalogdatenbank registrieren.

Schritte

1. Klicken Sie auf der Seite Anwendungen auf **... > Details Anzeigen**.
2. Klicken Sie im Abschnitt Datenbankdetails auf  So konfigurieren Sie das RMAN-Katalog-Repository.
3. Geben Sie die Anmeldeinformationen zum Katalogisieren von Backups mit RMAN und den Namen des Transparent Network Substrat (TNS) der Katalogwiederherstellungsdatenbank an.
4. Klicken Sie Auf **Konfigurieren**.

Erstellen Sie ein Backup der Oracle Database

Sie können 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 beim Erstellen von ASM-Festplattengruppen auf Amazon FSX for NetApp ONTAP oder Cloud Volumes ONTAP sicher, dass es keine gemeinsamen Volumes in Festplattengruppen gibt. Jede Datenträgergruppe sollte über dedizierte Volumes verfügen.

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. Wenn Sie den RMAN-Katalog in der Richtlinie aktiviert haben, startet das Backup am Ende des Workflows den Katalogisierungsvorgang als separaten Job. Der Fortschritt der Katalogisierung kann vom Job Monitor aus gesehen werden. Nach erfolgreicher Katalogisierung zeigt **Backup Details** den Status des Katalogs für jedes Backup an.



Das Servicekonto (*SnapCenter-Account-`<account_id>`*) wird für die 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 sind, wählen Sie die Richtlinie, die Aufbewahrungsebene aus, und klicken Sie dann auf **Backup erstellen**.

Wenn Sie den RMAN-Katalog in der Richtlinie aktiviert haben, startet das Backup am Ende des Workflows den Katalogisierungsvorgang als separaten Job. Der Fortschritt der Katalogisierung kann vom Job Monitor aus gesehen werden. Nach erfolgreicher Katalogisierung zeigt **Backup Details** den Status des Katalogs für jedes Backup an.

Einschränkungen

- Unterstützt keine Snapshots von Konsistenzgruppen für Oracle Datenbanken, die sich auf mehreren ASM-Festplattengruppen mit Überschneidungen von FSX Volumes befinden
- Wenn sich Ihre Oracle-Datenbanken auf Amazon FSX for NetApp ONTAP oder Cloud Volumes ONTAP befinden und auf ASM konfiguriert sind, stellen Sie sicher, dass Ihre SVM-Namen in den FSX-Systemen eindeutig sind. Wenn Sie in den FSX-Systemen denselben SVM-Namen haben, werden Backups der auf diesen SVMs befindlichen Oracle Datenbanken nicht unterstützt.
- 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"](#).

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.