



Backup Cloud-nativer Oracle Database

Cloud Backup

NetApp
March 15, 2023

Inhaltsverzeichnis

- Backup Cloud-nativer Oracle Database 1
- Zugriff auf BlueXP 1
- Konfigurieren Sie FSX für ONTAP 1
- Konfigurieren Sie Cloud Volumes ONTAP 2
- Implementieren Sie das SnapCenter Plug-in für Oracle und fügen Sie Datenbank-Hosts hinzu 2
- Backup Cloud-nativer Oracle Database 8

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.

Implementieren 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 bereitstellen, 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 implementieren:
 - Implementieren Sie das Plug-in, und fügen Sie die Host-Benutzeroberfläche mithilfe der SSH-Option hinzu. [Weitere Informationen ..](#)
 - Stellen Sie das Plug-in mithilfe des Skripts bereit, und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu. [und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu,Weitere Informationen ..](#)
- Wenn SSH deaktiviert ist, stellen Sie das Plug-in manuell bereit und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu. [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 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 SnapCenter-Benutzer erstellt und sudo für den SnapCenter-Benutzer konfiguriert haben. Weitere Informationen finden Sie unter [Konfigurieren Sie sudo für SnapCenter-Benutzer](#).
- Stellen Sie sicher, dass für den Connector die Kommunikation zum SSH-Port aktiviert ist (Standard: 22), wenn die SSH-basierte Bereitstellung verwendet wird.
- Stellen Sie sicher, dass die Kommunikation auf dem Connector für den Plug-in-Anschluss aktiviert ist (Standard: 8145), damit die Vorgänge funktionieren.

Konfigurieren Sie sudo für SnapCenter-Benutzer

Sie sollten einen SnapCenter-Benutzer erstellen und sudo für den Benutzer 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 SnapCenter-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 die <LINUXUSER> durch den SnapCenter-Benutzer, den Sie erstellt haben, und speichern Sie die Datei im visudo-Dienstprogramm.

Implementieren Sie das Plug-in und fügen Sie über die SSH-Option Host von der Benutzeroberfläche hinzu

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 die folgenden Schritte aus:

- Wählen Sie **über SSH**.
- Geben Sie die FQDN- oder IP-Adresse des Hosts an, auf dem Sie das Plug-in installieren möchten.
- Geben Sie den Benutzernamen an ([Sudo SnapCenter-Benutzer](#)) Mit dem das Plug-in-Paket auf den Host kopiert wird.
- 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.

- Wählen Sie den Anschluss aus.
- (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.

c. 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.

Stellen Sie das Plug-in mithilfe des Skripts bereit, und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Host für den SnapCenter-Benutzer aktiviert ist,

können Sie das Plug-in wie folgt bereitstellen: 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 SnapCenter-Benutzers, der zur Verbindung mit dem Oracle-Host verwendet wird. Dies ist ein obligatorischer Parameter.
- User_Name: SnapCenter-Benutzer mit SSH-Berechtigungen auf dem Oracle-Host. 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
```

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

5. Klicken Sie Auf Anwendungen Ermitteln.

6. 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.

7. Führen Sie auf der Seite Host hinzufügen die folgenden Schritte aus:

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**.

- 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.

Stellen Sie das Plug-in manuell bereit, und fügen Sie den Host über die Benutzeroberfläche mithilfe der manuellen Option hinzu

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

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 SnapCenter-Benutzer zugreifen kann.

6. Melden Sie sich über das SnapCenter-Benutzerkonto beim Oracle-Datenbank-Host an, und führen Sie den folgenden Befehl aus, um Ausführungsberechtigungen für die Binärdatei zu aktivieren.

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

7. Stellen Sie das Oracle-Plug-in als sudo SnapCenter-Benutzer bereit.

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<snapcenter-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`

11. 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>/getVersion --cert  
/config/client/certificate/certificate.pem --key  
/config/client/certificate/key.pem
```

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

13. Klicken Sie Auf Anwendungen Ermitteln.

14. 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.

15. Führen Sie auf der Seite Host hinzufügen die folgenden Schritte aus:

- 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**.

- 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 sysasm-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- \langle Account_id \rangle*) 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.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.