



# **Sichern von Daten nativer Cloud- Applikationen**

## **Cloud Backup**

NetApp  
January 06, 2023

# Inhaltsverzeichnis

- Sichern von Daten nativer Cloud-Applikationen. . . . . 1
  - Sichern Sie Ihre Daten aus Cloud-nativen Applikationen. . . . . 1
  - Backup von Cloud-nativen Applikationsdaten . . . . . 5
  - Stellen Sie Daten nativer Cloud-Applikationen wieder her. . . . . 12
  - Klonen Cloud-nativer Applikationsdaten . . . . . 14
  - Sicherung von Cloud-nativen Applikationsdaten managen . . . . . 22

# Sichern von Daten nativer Cloud-Applikationen

## Sichern Sie Ihre Daten aus Cloud-nativen Applikationen

Cloud Backup für Applikationen ist ein SaaS-basierter Service mit Datensicherungsfunktionen für Applikationen, die auf NetApp Cloud Storage ausgeführt werden. Cloud Backup für Anwendungen, die in BlueXP (ehemals Cloud Manager) aktiviert sind, bietet effizienten, applikationskonsistenten, richtlinienbasierten Schutz der folgenden Anwendungen:

- Oracle Datenbanken befinden sich auf Amazon FSX für NetApp ONTAP und Cloud Volumes ONTAP
- SAP HANA Systeme auf Azure NetApp Files (ANF)

### Der Netapp Architektur Sind

Die Architektur von Cloud Backup für Applikationen umfasst die folgenden Komponenten:

- Cloud Backup für Applikationen ist eine Reihe von Datensicherungsservices, die von NetApp als SaaS-Service gehostet werden und auf der BlueXP SaaS-Plattform basieren.

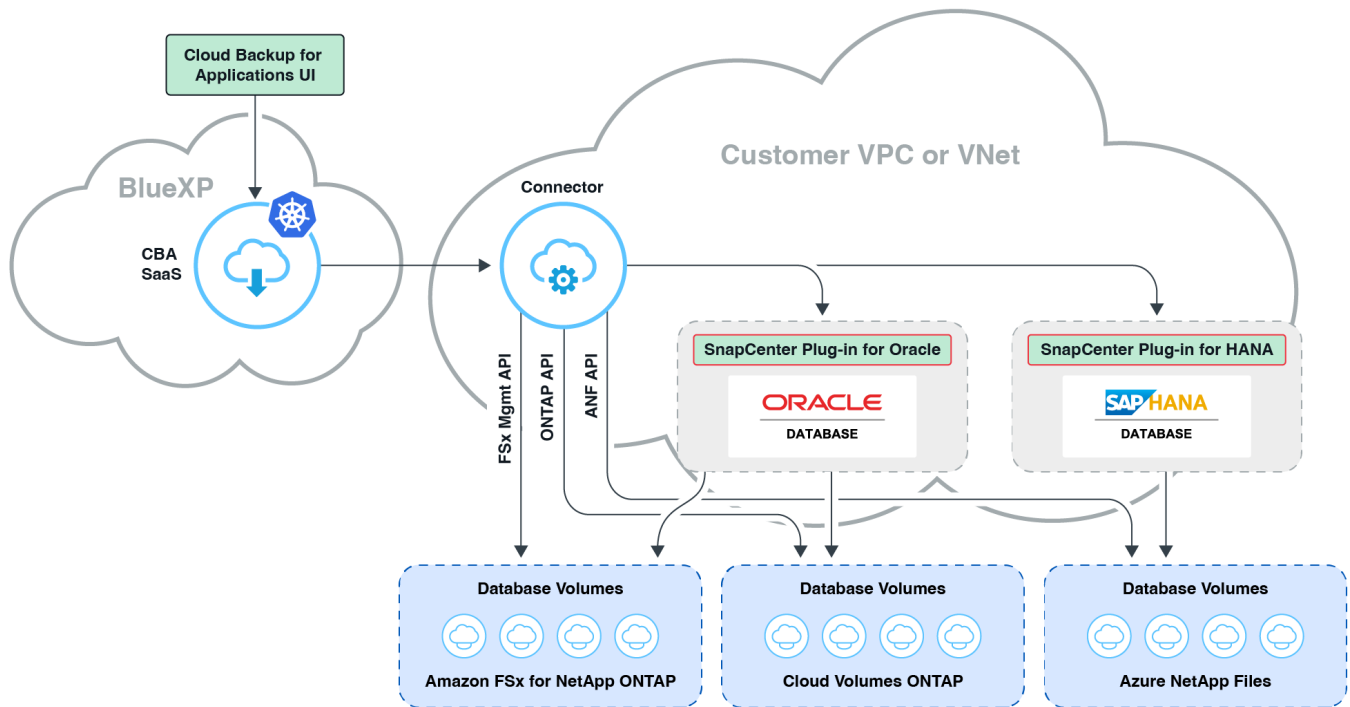
Die Datensicherungs-Workflows werden für Applikationen auf NetApp Cloud Storage orchestriert.

- Auf die Benutzeroberfläche von Cloud Backup für Applikationen kann über die Benutzeroberfläche von BlueXP zugegriffen werden.

Die Benutzeroberfläche von Cloud Backup für Applikationen bietet Datensicherungsfunktionen für Applikationen.

- BlueXP Connector ist eine Komponente, die im Cloud-Netzwerk des Benutzers ausgeführt wird und mit Storage-Systemen und applikationsspezifischen Plug-ins interagiert.
- Das applikationsspezifische Plug-in ist eine Komponente, die auf jedem Applikations-Host ausgeführt wird und mit den auf dem Host ausgeführten Datenbanken interagiert, während gleichzeitig Datensicherungsprozesse durchgeführt werden.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Für alle von Benutzern initiierten Anfragen kommuniziert die Benutzeroberfläche von Cloud Backup for Applications mit dem SaaS von BlueXP, das bei der Validierung der Anfrageprozesse identisch ist. Wenn die Anfrage einen Workflow wie Backup, Wiederherstellung oder Klon ausführen soll, initiiert der SaaS-Service den Workflow und leitet diesen bei Bedarf an den BlueXP Connector weiter. Der Connector kommuniziert dann im Rahmen der Ausführung der Workflow-Aufgaben mit dem Speichersystem und dem anwendungsspezifischen Plug-in.

Der Connector kann in derselben VPC oder vnet wie die der Applikationen oder in einer anderen implementiert werden. Wenn sich der Connector und die Anwendungen in einem anderen Netzwerk befinden, sollten Sie eine Netzwerkverbindung zwischen ihnen herstellen.



Ein einziger BlueXP Connector kann mit mehreren Speichersystemen und mehreren Anwendungs-Plug-ins kommunizieren. Sie benötigen einen einzigen Connector, um Ihre Anwendungen zu verwalten, solange die Verbindung zwischen dem Connector und den Anwendungs-Hosts besteht.



Cloud Backup für Applikationen die SaaS-Infrastruktur ist gegen Ausfälle der Verfügbarkeitszonen innerhalb einer Region stabil. Es unterstützt regionale Ausfälle durch Failover auf eine neue Region, und der Failover hat ungefähr zwei Stunden Ausfallzeit.

## Schutz von Oracle Datenbank

### Unterstützte Konfigurationen

- Betriebssystem:
  - RHEL 7.5 oder höher und 8.x
  - L 7.5 oder höher und 8.x
- Storage-System:
  - Amazon FSX für ONTAP

- Cloud Volumes ONTAP
- Storage-Layouts:
  - NFS v3 und v4.1 (einschließlich dNFS)
  - iSCSI mit ASM (ASMFD, ASMLib und ASMUdev)
- Datenbank-Layouts: Oracle Standard und Oracle Enterprise Standalone (veraltete und mandantenfähige CDB und PDB)
- Datenbankversionen: 12cR2, 18c, 19c und 21c

## Funktionen

- Host hinzufügen und Plug-in implementieren

Sie können das Plug-in entweder manuell, mithilfe eines Skripts oder automatisch bereitstellen.

- Automatische Erkennung von Oracle-Datenbanken
- Backup von Oracle Datenbanken
  - Vollständiges Backup (Daten + Kontrolle + Archivprotokolldateien)
  - On-Demand-Backup
  - Ein geplantes Backup basiert auf den systemdefinierten oder benutzerdefinierten Richtlinien

Sie können verschiedene Planungsfrequenzen wie stündlich, täglich, wöchentlich und monatlich in der Richtlinie festlegen.

- Aufbewahrung von Backups anhand der Richtlinie
- Wiederherstellen der vollständigen Oracle-Datenbank (Datendateien + Kontrolldatei) aus dem angegebenen Backup
- Nur Datendateien wiederherstellen und nur Dateien aus dem angegebenen Backup steuern
- Wiederherstellen der Oracle-Datenbank mit bis SCN, bis zu der Zeit, alle verfügbaren Protokolle und keine Recovery-Optionen
- Klonen von Oracle Datenbanken auf Quell- oder alternativen Ziel-Hosts
  - Grundklonen mit einem Klick
  - Erweitertes Klonen mit einer benutzerdefinierten Klonspezifikationsdatei
  - Der Name der Kloneinheiten kann automatisch generiert oder mit der Quelle identisch sein
  - Anzeigen der Klonhierarchie
  - Geklonte Datenbanken werden gelöscht
- Monitoring von Backups, Restores, Klonen und anderen Aufgaben
- Anzeigen der Schutzzusammenfassung im Dashboard
- Senden von Benachrichtigungen per E-Mail

## Einschränkungen

- Bietet keine Unterstützung für Oracle 11g
- Unterstützt keine Mount-, Katalog- und Überprüfungsvorgänge für Backups
- Bietet keine Unterstützung für Oracle auf RAC und Data Guard

- Bei Cloud Volumes ONTAP HA wird nur eine der Netzwerk-Schnittstellen-IPs verwendet. Wenn die Verbindung der IP unterbrochen wird oder Sie nicht auf die IP zugreifen können, schlagen die Vorgänge fehl.
- Die IP-Adressen der Netzwerkschnittstellen von Amazon FSX für NetApp ONTAP oder Cloud Volumes ONTAP müssen im BlueXP Konto und in der Region eindeutig sein.

## Schutz von SAP HANA Datenbanken

### Unterstützte Konfigurationen

- Betriebssystem:
  - RHEL 7.5 oder höher, 8.x-Plattformen, von SAP HANA zertifiziert
  - SLES 12 SP5 oder höher und 15 SPX Plattformen zertifiziert von SAP HANA
- Storage-System Azure NetApp Files (ANF)
- Storage-Layouts: Azure unterstützt für Daten und Protokoll nur NFSv4.1.
- Datenbank-Layout:
  - Single Container Version 1.0SPS12
  - SAP HANA Multitenant Database Container (MDC) 2.0SPS4, 2.0SPS5, 2.0SPS6 mit einzelnen oder mehreren Mandanten
  - SAP HANA Einzelhostsystem, SAP HANA mehrere Hostsysteme (ohne Standby-Host), HANA System Replication
- Plug-in für SAP HANA auf dem Datenbank-Host

### Funktionen

- Manuelles Hinzufügen von SAP HANA-Systemen
- Backup von SAP HANA Datenbanken
  - On-Demand-Backup (dateibasiert und auf Snapshot Kopien)
  - Ein geplantes Backup basiert auf den systemdefinierten oder benutzerdefinierten Richtlinien  
  
 Sie können verschiedene Planungsfrequenzen wie stündlich, täglich, wöchentlich und monatlich in der Richtlinie festlegen.
  - HANA System Replication (HSR)-orientiert
- Aufbewahrung von Backups anhand der Richtlinie
- Wiederherstellung der vollständigen SAP HANA-Datenbank aus dem angegebenen Backup
- Sichern und Wiederherstellen von HANA-Volumes ohne Daten und globalen nicht-Daten-Volumes
- Unterstützung von Prescript und Postscript mithilfe von Umgebungsvariablen für Backup- und Restore-Vorgänge
- Erstellen eines Aktionsplans für Fehlerszenarien mit der Option vor dem Beenden

### Einschränkungen

- Bei HSR-Konfiguration wird nur HSR mit 2 Nodes unterstützt (1 primäre und 1 sekundäre).
- Die Aufbewahrung wird nicht ausgelöst, wenn das Postscript während der Wiederherstellung ausfällt

# 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 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

optionalen 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 ist ein optionaler Parameter. 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
```

## 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`

### 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 <a href="#">Manuell</a> Oder <a href="#">Verwenden des Skripts</a>	<ol style="list-style-type: none"><li>a. Wählen Sie <b>Manuell</b>.</li><li>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.</li><li>c. Geben Sie den Plug-in-Port an.  Standardport ist 8145.</li><li>d. Wählen Sie den Anschluss aus.</li><li>e. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass das Plug-in auf dem Host installiert ist</li><li>f. Klicken Sie Auf <b>Anwendungen Entdecken</b>.</li></ol>

Sie suchen...	Tun Sie das...
Das Plug-in automatisch bereitstellen möchten	<p>a. Wählen Sie <b>über SSH</b>.</p> <p>b. Geben Sie die FQDN- oder IP-Adresse des Hosts an, auf dem Sie das Plug-in installieren möchten.</p> <p>c. Geben Sie den Benutzernamen an (<b>Nicht-Root-Benutzer</b>) Mit dem das Plug-in-Paket auf den Host kopiert wird.</p> <p>d. Geben Sie SSH und Plug-in-Port an.</p> <p>Der standardmäßige SSH-Port ist 22 und der Plug-in-Port 8145.</p> <p>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.</p> <p>e. Wählen Sie den Anschluss aus.</p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Der private SSH-Schlüssel wird nicht an jedem Ort in der Applikation gespeichert und wird nicht für andere Vorgänge verwendet.</p> </div> <p>g. Klicken Sie Auf <b>Weiter</b>.</p>

- 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.

## Stellen Sie Daten nativer Cloud-Applikationen wieder her

### Wiederherstellung nativer Oracle Datenbank in der Cloud

Im Falle eines Datenverlustes können Sie die Datendateien, Kontrolldateien oder beides wiederherstellen. Anschließend können Sie die Datenbank wiederherstellen.

## Was Sie brauchen

Wenn sich die Oracle 21c-Datenbank im STARTZUSTAND befindet, schlägt der Wiederherstellungsvorgang fehl. Sie sollten Folgendes ausführen, um die Datenbank erfolgreich wiederherzustellen.

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

## Schritte

1. Klicken Sie Auf **...** Entsprechend der Datenbank, die Sie wiederherstellen möchten, und klicken Sie auf **Details anzeigen**.
2. Klicken Sie Auf **...** Entsprechend der Datensicherung, die Sie für die Wiederherstellung verwenden möchten, und klicken Sie auf **Restore**.
3. Führen Sie im Abschnitt „Umfang wiederherstellen“ die folgenden Aktionen durch:

Sie suchen...	Tun Sie das...
Möchten nur die Datendateien wiederherstellen	Wählen Sie <b>Alle Datendateien</b> .
Möchten nur die Kontrolldateien wiederherstellen	Wählen Sie <b>Steuerdateien</b>
Kunden möchten sowohl Datendateien als auch Kontrolldateien wiederherstellen	Wählen Sie <b>Alle Datendateien</b> und <b>Kontrolldateien</b> aus.



Die Wiederherstellung von Datendateien mit Kontrolldateien oder nur Kontrolldateien wird für iSCSI im ASM-Layout nicht unterstützt.

Sie können auch das Kontrollkästchen **in-Place-Wiederherstellung erzwingen** aktivieren.

Wenn das SnapCenter Plug-in für Oracle im SAN-Layout fremde Dateien als Oracle-Datendateien auf der ASM-Festplattengruppe findet, wird die connect and Copy Restore-Methode durchgeführt. Die Fremddateien können eine oder mehrere der folgenden Typen sein:

- Parameter
- Passwort
- Archivprotokoll
- Online-Protokoll
- ASM-Parameterdatei.

Die Option **Kraft in-Place Restore** überschreibt die fremden Dateien von Typ-Parameter, Passwort und Archivprotokoll. Sie sollten das neueste Backup verwenden, wenn die Option **in-Place Restore erzwingen** ausgewählt ist.

4. Führen Sie im Abschnitt „Recovery Scope“ die folgenden Schritte aus:

Sie suchen...	Tun Sie das...
Möchten Sie die letzte Transaktion wiederherstellen	Wählen Sie <b>Alle Protokolle</b> .

Sie suchen...	Tun Sie das...
Wiederherstellen einer bestimmten Systemänderungsnummer (SCN)	Wählen Sie <b>bis Systemänderungsnummer</b> und geben Sie das SCN an.
Sie möchten ein Recovery zu einem bestimmten Datum und einer bestimmten Zeit durchführen	Wählen Sie <b>Datum und Uhrzeit</b> .
Möchten Sie nicht wiederherstellen	Wählen Sie <b>Keine Wiederherstellung</b> .

Für den ausgewählten Wiederherstellungsbereich können Sie im Feld **Archiv Log Files Locations** optional den Speicherort angeben, der die für die Wiederherstellung erforderlichen Archivprotokolle enthält.

Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung im LESE-SCHREIB-Modus öffnen möchten.

5. Klicken Sie auf **Weiter** und prüfen Sie die Details.

6. Klicken Sie Auf **Wiederherstellen**.

### Einschränkungen

- Keine Unterstützung für granulare Restores, beispielsweise beim Wiederherstellen von Tabellen und PDBs
- Sowohl in-Place als auch connect-and-copy Wiederherstellungsmethoden werden verwendet, wenn einige Festplattengruppen fremde Dateien enthalten. Die Verwendung beider Methoden zur gleichen Zeit zur Wiederherstellung wird jedoch nicht unterstützt und der Wiederherstellungsvorgang schlägt fehl. Die Datenbank wird im Status „angehängt“ belassen und Sie müssen die Datenbank manuell in den Status „Öffnen“ versetzen.

Aufgrund eines bekannten Problems wird die Fehlermeldung aufgrund von Fremddateien nicht auf der Jobseite in der UI angezeigt. Prüfen Sie die Connector-Protokolle, wenn während der Phase der SAN-Vorabwiederherstellung ein Fehler auftritt, um die Ursache des Problems zu ermitteln.

## Klonen Cloud-nativer Applikationsdaten

### Klonen Cloud-nativer Oracle Datenbank

#### Klonkonzepte und -Anforderungen

Sie können eine Oracle-Datenbank mit dem Backup der Datenbank entweder auf dem Quelldatenbank-Host oder auf einem alternativen Host klonen. Sie können das Backup aus primären Storage-Systemen klonen.

Vor dem Klonen der Datenbank sollten Sie die Klonkonzepte verstehen und sicherstellen, dass alle Anforderungen erfüllt werden.

#### Anforderungen für das Klonen einer Oracle Datenbank

Bevor Sie eine Oracle-Datenbank klonen, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie sollten eine Sicherung der Datenbank erstellt haben. Damit der Klonvorgang erfolgreich abgeschlossen



wurde, sollten Sie die Online-Daten und das Backup-Protokoll erstellt haben.

- Im parameter `asm_diskstring` sollten Sie `AFD:*` konfigurieren, wenn Sie ASMFD verwenden oder `ORCL:*` konfigurieren, wenn Sie ASMLIB verwenden.
- Wenn Sie den Klon auf einem alternativen Host erstellen, sollte der alternative Host folgende Anforderungen erfüllen:
  - Das Plug-in sollte auf dem alternativen Host installiert sein.
  - Der Klon-Host sollte in der Lage sein, LUNs vom Storage zu entdecken, wenn Sie eine Datenbank klonen, die sich auf iSCSI SAN Storage befindet. Wenn Sie auf einem alternativen Host klonen, stellen Sie sicher, dass eine iSCSI-Sitzung zwischen dem Storage und dem alternativen Host hergestellt wird.
  - Wenn die Quelldatenbank eine ASM-Datenbank ist:
    - Die ASM-Instanz sollte auf dem Host ausgeführt werden, auf dem der Klon ausgeführt wird.
    - Die ASM-Festplattengruppe sollte vor dem Klonvorgang bereitgestellt werden, wenn Sie Archivprotokolldateien der geklonten Datenbank in eine dedizierte ASM-Festplattengruppe platzieren möchten.
    - Der Name der Datendiskgruppe kann konfiguriert werden, aber stellen Sie sicher, dass der Name nicht von einer anderen ASM-Festplattengruppe auf dem Host verwendet wird, auf dem der Klon ausgeführt wird.
    - Datendateien auf der ASM-Festplattengruppe werden als Teil des Klon-Workflows bereitgestellt.

### Einschränkungen beim Klonen

- Geplante Klone (Lifecycle Management für Klone) werden nicht unterstützt.
- Das Klonen einer geklonten Datenbank wird nicht unterstützt.
- Das Klonen von Datenbanken auf Qtree wird nicht unterstützt.
- Das Klonen von Backups für Archivprotokolle wird nicht unterstützt.
- Das Backup einer geklonten Datenbank wird nicht unterstützt.

### Klonmethoden

Sie können den Klon entweder mit der Basismethode oder mit der Klon-Spezifikations-Datei erstellen.

### Klonen mit einfacher Methode

Sie können den Klon mit den Standardkonfigurationen auf Basis der Quelldatenbank und des ausgewählten Backups erstellen.

- Die Datenbankparameter `Home` und der OS-Benutzer werden standardmäßig auf die Quelldatenbank gesetzt.
- Die Datendateipfade werden basierend auf dem ausgewählten Benennungsschema benannt.
- Die vor-, Post- und SQL-Anweisungen können nicht angegeben werden.
- Die Recovery-Option ist standardmäßig **bis Abbrechen** und es verwendet die Log-Backup mit dem Datenbank-Backup für die Wiederherstellung verbunden

### Klonen mit Spezifikationsdatei

Sie können die Konfigurationen in der Klon-Spezifikations-Datei definieren und sie zum Klonen der Datenbank verwenden. Sie können die Spezifikationsdatei herunterladen, an Ihre Anforderung anpassen und

anschließend die Datei hochladen. ["Weitere Informationen ."](#)

Die verschiedenen Parameter, die in der Spezifikations-Datei definiert sind und die geändert werden können, sind wie folgt:

Parameter	Beschreibung
Control_Dateien	<p>Speicherort der Kontrolldateien für die Klondatenbank</p> <p>Die Anzahl der Kontrolldateien wird mit der Quelldatenbank identisch sein. Wenn Sie den Pfad der Steuerdatei überschreiben möchten, können Sie einen anderen Pfad für die Steuerdatei angeben. Auf dem Host sollte das Dateisystem oder die ASM-Festplattengruppe vorhanden sein.</p>
Redo_Logs	<p>Standort, Größe, Anzahl der Wiederherstellungsprotokolle.</p> <p>Zum Klonen der Datenbank sind mindestens zwei Wiederherstellungsprotokolle erforderlich. Wenn Sie den Pfad der Redo-Log-Datei überschreiben möchten, können Sie den Pfad der Redo-Log-Datei auf ein anderes Dateisystem als die der Quelldatenbank anpassen. das Dateisystem oder die ASM-Diskgruppe sollte auf dem Host vorhanden sein.</p>
oracle_Version	Oracle-Version auf dem Ziel-Host.
oracle_Home	Oracle Home auf dem Ziel-Host:
Enable_Archive_log_Mode	Steuert den Archivprotokollmodus für die Klondatenbank
Datenbankparameter	Datenbankparameter für die geklonte Datenbank
sql_Anweisungen	Die SQL-Anweisungen, die nach dem Klonen auf der Datenbank ausgeführt werden sollen
os_user_Detail	Oracle OS Benutzer auf der Zielklondatenbank
Datenbankport	Port, der für die Kommunikation mit der Datenbank verwendet wird, wenn die OS-Authentifizierung auf dem Host deaktiviert ist.
asm_Port	Port, der für die Kommunikation mit der ASM-Datenbank verwendet wird, wenn Anmeldedaten in der Eingabe zum Erstellen eines Klons angegeben sind.

Parameter	Beschreibung
skip_Recovery	Führt keinen Wiederherstellungsvorgang aus.
Bis_scn	Stellt die Datenbank bis zur angegebenen Systemänderungsnummer (scn) wieder her.
„Bis_Zeit“	<p>Stellt die Datenbank bis zum angegebenen Datum und der angegebenen Zeit wieder her.</p> <p>Das akzeptierte Format lautet <i>mm/TT/JJJJ hh:mm:ss</i>.</p>
Bis_Abbrechen	<p>Stellen Sie die Wiederherstellung wieder her, indem Sie das Log-Backup mounten, das für das Klonen ausgewählt wurde.</p> <p>Die geklonte Datenbank wird wiederhergestellt, bis die fehlende oder beschädigte Protokolldatei vorliegt.</p>
Log_Paths	Weitere Standorte für Archivprotokolle, die für das Recovery der geklonten Datenbank verwendet werden sollen.
Source_Location	Speicherort der Diskgruppe oder des Bereitstellungspunkts auf dem Quell-Datenbank-Host.
Clone_Location	Speicherort der Diskgruppe oder des Mount-Punkts, der auf dem Zielhost erstellt werden muss, der dem Quellspeicherort entspricht.
Location_type	<p>Es kann entweder ASM_Diskgroup oder Mountpoint sein.</p> <p>Die Werte werden beim Herunterladen der Datei automatisch ausgefüllt. Sie sollten diesen Parameter nicht bearbeiten.</p>
Pre_Script	Skript, das auf dem Zielhost ausgeführt werden soll, bevor der Klon erstellt wird.
Post_Script	Skript, das auf dem Zielhost ausgeführt werden soll, nachdem der Klon erstellt wurde.
Pfad	<p>Absoluter Pfad des Skripts auf dem Klon-Host.</p> <p>Sie sollten das Skript entweder in <i>/var/opt/snapcenter/spl/scripts</i> oder in einem beliebigen Ordner in diesem Pfad speichern.</p>

Parameter	Beschreibung
Zeitüberschreitung	Die für das auf dem Zielhost ausgeführte Skript festgelegte Zeitüberschreitung.
Argumente	Für die Skripte angegebene Argumente.

## Benennungsschema für Klone

Clone Benennungsschema definiert den Speicherort der Mount-Punkte und den Namen der Festplattengruppen der geklonten Datenbank. Sie können entweder **identisch** oder **automatisch generiert** wählen.

### Identisches Benennungsschema

Wenn Sie das Namensschema für den Klon als **identisch** auswählen, wird der Speicherort der Mount-Punkte und der Name der Diskgroups der geklonten Datenbank mit der Quelldatenbank identisch sein.

Wenn der Mount-Punkt der Quelldatenbank beispielsweise */netapp\_sourceb/Data\_1 , +DATA1\_DG* ist, bleibt der Mount-Punkt für die geklonte Datenbank sowohl für NFS als auch für ASM auf SAN gleich.

- Konfigurationen wie Anzahl und Pfad von Kontrolldateien und Wiederherstellungsdateien werden mit der Quelle identisch sein.



Wenn sich die Redo-Logs oder Kontrolldateipfade auf den nicht-Daten-Volumes befinden, sollte der Benutzer die ASM-Festplattengruppe oder den Bereitstellungspunkt im Ziel-Host bereitgestellt haben.

- Oracle OS-Benutzer und die Oracle Version werden mit der Quelldatenbank identisch sein.
- Der Name des Klon-Storage Volumes hat das folgende Format:  
SourceVolNameSCS\_Clone\_CurrentTimeStampNumber.

Wenn der Volume-Name auf der Quelldatenbank beispielsweise *sourceVolName* lautet, lautet der geklonte Volume-Name *sourceVolNameSCS\_Clone\_1661420020304608825*.



Die *CurrentTimeStampNumber* bietet die Einzigartigkeit im Volumennamen.

### Automatisch generiertes Benennungsschema

Wenn Sie das Klon-Schema als **automatisch generiert** auswählen, wird der Speicherort der Mount-Punkte und der Name der Diskgroups der geklonten Datenbank mit einem Suffix angehängt. \* Wenn Sie die grundlegende Clone-Methode ausgewählt haben, ist das Suffix die **Clone-SID**. \* Wenn Sie die Methode der Spezifikatei ausgewählt haben, ist das Suffix **Suffix**, das beim Herunterladen der Klon-Spezifikations-Datei angegeben wurde.

Wenn zum Beispiel der Mount-Punkt der Quelldatenbank */netapp\_sourcedb/Data\_1* und der **Clone SID** oder der **Suffix HR** ist, dann ist der Mount-Punkt der geklonten Datenbank */netapp\_sourcedb/Data\_1\_HR*.

- Die Anzahl der Kontrolldateien und Wiederherstellungsprotokolle wird mit der Quelle identisch sein.
- Alle Redo-Log-Dateien und Kontrolldateien befinden sich auf einem der geklonten Datenmontagepunkte oder Daten-ASM-Festplattengruppen.

- Der Name des Klon-Storage Volumes hat das folgende Format:  
`SourceVolNameSCS_Clone_CurrentTimeStampNumber`.

Wenn der Volume-Name auf der Quelldatenbank beispielsweise *sourceVolName* lautet, lautet der geklonte Volume-Name *sourceVolNameSCS\_Clone\_1661420020304608825*.



Die *CurrentTimeStampNumber* bietet die Einzigartigkeit im Volumennamen.

- Das Format des NAS-Mount-Punkts ist *SourceNASMountPoint\_Suffix*.
- Das Format der ASM-Festplattengruppe ist *SourceDiskgroup\_Suffix*.



Wenn die Anzahl der Zeichen in der Clone-Festplattengruppe größer als 25 ist, hat sie *SC\_HashCode\_Suffix*.

### Datenbankparameter

Der Wert der folgenden Datenbankparameter entspricht unabhängig vom Namenskonvention des Klons dem der Quelldatenbank.

- `Log_Archive_Format`
- `Audit_Trail`
- `Prozessen`
- `pga_Aggregate_Target`
- `Remote_Login_passwordfile`
- `Undo_Tablespace`
- `Open_Cursors`
- `sga_Target`
- `db_Block_size`

Der Wert der folgenden Datenbankparameter wird mit einem Suffix basierend auf der Clone-SID angehängt.

- `Audit_file_dest = {sourceDatabase_parametervalue}_Suffix`
- `Log_Archive_dest_1 = {sourceDatabase_oraclehome}_Suffix`

### Unterstützte vordefinierte Umgebungsvariablen für das Klonen spezifischer Preskript und Postscript

Sie können die unterstützten vordefinierten Umgebungsvariablen verwenden, wenn Sie das Prescript und das Postscript beim Klonen einer Datenbank ausführen.

- `SC_ORIGINAL_SID` gibt die SID der Quelldatenbank an. Dieser Parameter wird für Anwendungs-Volumes ausgefüllt. Beispiel: NFSB32
- `SC_ORIGINAL_HOST` gibt den Namen des Quellhosts an. Dieser Parameter wird für Anwendungs-Volumes ausgefüllt. Beispiel: asmrac1.gdl.englab.netapp.com
- `SC_ORACLE_HOME` gibt den Pfad des Oracle-Home-Verzeichnisses der Zieldatenbank an. Beispiel: /Ora01/App/oracle/Product/18.1.0/db\_1
- `SC_BACKUP_NAME` gibt den Namen des Backups an. Dieser Parameter wird für Anwendungs-Volumes ausgefüllt. Beispiele:

- Wenn die Datenbank nicht im ARCHIVELOG-Modus ausgeführt wird:  
DATEN@RG2\_scspr2417819002\_07-20- 2021\_12.16.48.9267\_0\_LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird:  
DATEN@@RG2\_scspr2417819002\_07-20- 2021\_12.16.48.9267\_0 RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-21-2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-22-2021\_12.16.48.9267\_11\_11\_11\_1\_1
- SC\_ORIGINAL\_OS\_USER gibt den Betriebssystembesitzer der Quelldatenbank an. Beispiel: oracle
- SC\_ORIGINAL\_OS\_GROUP gibt die Betriebssystemgruppe der Quelldatenbank an. Beispiel: Oinstall
- SC\_TARGET\_SID“ gibt die SID der geklonten Datenbank an. Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert. Dieser Parameter wird für Anwendungs-Volumes ausgefüllt. Beispiel: Clonedb
- SC\_TARGET\_HOST gibt den Namen des Hosts an, auf dem die Datenbank geklont werden soll. Dieser Parameter wird für Anwendungs-Volumes ausgefüllt. Beispiel: asmrac1.gdl.englab.netapp.com
- SC\_TARGET\_OS\_USER gibt den Betriebssystembesitzer der geklonten Datenbank an. Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert. Beispiel: oracle
- SC\_TARGET\_OS\_GROUP gibt die Betriebssystemgruppe der geklonten Datenbank an. Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert. Beispiel: Oinstall
- SC\_TARGET\_DB\_PORT gibt den Datenbank-Port der geklonten Datenbank an. Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert. Beispiel: 1521

## Unterstützte Trennzeichen

- @ Wird verwendet, um Daten von seinem Datenbanknamen zu trennen und den Wert von seinem Schlüssel zu trennen. Beispiel: DATEN@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0\_LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- Wird verwendet, um die Daten zwischen zwei verschiedenen Entitäten für SC\_BACKUP\_NAME Parameter zu trennen. Beispiel: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0 LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- , Wird verwendet, um Satz von Variablen für den gleichen Schlüssel zu trennen. Beispiel: DATEN@RG2\_scspr2417819002\_07-20- 2021\_12.16.48.9267\_0 LOGBUCH@RG2\_scspr2417819002\_07-20- 2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-21-2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-22-2021\_12.16.48.9267\_1

## Klonen Cloud-nativer Oracle Datenbank

Sie können eine Oracle-Datenbank mit dem Backup der Datenbank entweder auf dem Quelldatenbank-Host oder auf einem alternativen Host klonen.

Sie können Datenbanken aus den folgenden Gründen klonen:

- Funktionen zu testen, die während der Applikationsentwicklungszyklen mit der aktuellen Datenbankstruktur und Inhalten implementiert werden müssen
- Um Data Warehouses mit Tools zur Datenextraktion und -Bearbeitung zu befüllen.
- Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden.

## Was Sie brauchen

Vor dem Klonen der Datenbank sollten Sie die Klonkonzepte verstehen und sicherstellen, dass alle


Anforderungen erfüllt werden. ["Weitere Informationen ."](#)

## Schritte

1. Klicken Sie Auf **...** Entsprechend der Datenbank, die Sie klonen möchten, und klicken Sie auf **Details anzeigen**.
2. Klicken Sie Auf **...** Entsprechend der Datensicherung und klicken Sie auf **Clone**.
3. Wählen Sie auf der Seite Klondetails eine der Klonoptionen aus.
4. Führen Sie je nach gewählter Option die folgenden Aktionen durch:

Wenn Sie ausgewählt haben...	Tun Sie das...
<b>Einfach</b>	<p>a. Wählen Sie den Klon-Host aus.</p> <p>Wenn Sie den Klon auf einem anderen Host erstellen möchten, wählen Sie den Host aus, der dieselbe Version von Oracle und dasselbe Betriebssystem wie der des Quelldatenbankhosts hat.</p> <p>b. Geben Sie die SID des Klons an.</p> <p>c. Wählen Sie das Benennungsschema für den Klon aus.</p> <p>Wenn die Datenbank zum Quell-Host geklont wird, wird das Benennungsschema automatisch generiert. Wenn die Datenbank auf einem alternativen Host geklont wird, ist das Benennungsschema von Klonen identisch.</p> <p>d. Geben Sie den Oracle Home Path an.</p> <p>e. (Optional) Geben Sie die Datenbankanmeldeinformationen an.</p> <ul style="list-style-type: none"><li>◦ Datenbank-Anmeldeinformationen: Wenn die OS-Benutzerauthentifizierung deaktiviert ist, sollten Sie ein Passwort für den sys-Benutzer angeben, um es auf dem Ziel-Host zu definieren.</li><li>◦ ASM-Anmeldedaten: Wenn die Authentifizierung des OS-Benutzers auf dem Zielhost deaktiviert ist, sollten Sie die Anmeldeinformationen eines sysasm-privilegierten Benutzers angeben, um eine Verbindung zur ASM-Instanz auf dem Zielhost herzustellen.</li></ul> <p>f. Klicken Sie Auf <b>Weiter</b>.</p> <p>g. Klicken Sie Auf <b>Clone</b>.</p>

Wenn Sie ausgewählt haben...	Tun Sie das...
<b>Spezifikations-Datei</b>	<p>a. Klicken Sie auf <b>Datei herunterladen</b>, um die Spezifikationsdatei herunterzuladen.</p> <p>b. Wählen Sie das Benennungsschema für den Klon aus.</p> <p>Wenn Sie <b>automatisch generiert</b> auswählen, sollten Sie das Suffix angeben.</p> <p>c. Bearbeiten Sie die Spezifikationsdatei gemäß der Anforderung und laden Sie sie hoch, indem Sie auf die Schaltfläche <b>Durchsuchen</b> klicken.</p> <p>d. Wählen Sie den Klon-Host aus.</p> <p>Wenn Sie den Klon auf einem anderen Host erstellen möchten, wählen Sie den Host aus, der dieselbe Version von Oracle und dasselbe Betriebssystem wie der des Quelldatenbankhosts hat.</p> <p>e. Geben Sie die SID des Klons an.</p> <p>f. (Optional) Geben Sie die Datenbankanmeldeinformationen an.</p> <ul style="list-style-type: none"> <li>◦ Datenbank-Anmeldeinformationen: Wenn die OS-Benutzerauthentifizierung deaktiviert ist, sollten Sie ein Passwort für den sys-Benutzer angeben, um es auf dem Ziel-Host zu definieren.</li> <li>◦ ASM-Anmeldedaten: Wenn die Authentifizierung des OS-Benutzers auf dem Zielhost deaktiviert ist, sollten Sie die Anmeldeinformationen eines sysasm-privilegierten Benutzers angeben, um eine Verbindung zur ASM-Instanz auf dem Zielhost herzustellen.</li> </ul> <p>g. Klicken Sie Auf <b>Weiter</b>.</p> <p>h. Klicken Sie Auf <b>Clone</b>.</p>

5. Klicken Sie Auf  Neben **Filter by** und wählen Sie **Clone-Optionen > Klone**, um die Klone anzuzeigen.

## Sicherung von Cloud-nativen Applikationsdaten managen

### Überwachen von Jobs

Sie können den Status der Jobs überwachen, die in Ihren Arbeitsumgebungen initiiert wurden. Auf diese Weise können Sie die Aufträge sehen, die erfolgreich abgeschlossen wurden, die derzeit in Bearbeitung sind und die, die nicht erfolgreich abgeschlossen wurden, damit Sie Probleme diagnostizieren und beheben können.



Sie können eine Liste aller Vorgänge und deren Status anzeigen. Jeder Vorgang oder Job hat eine eindeutige ID und einen Status. Der Status kann lauten:

- Erfolgreich
- In Bearbeitung
- Warteschlange
- Warnung
- Fehlgeschlagen

## Schritte

1. Klicken Sie auf **Backup und Recovery**.
2. Klicken Sie Auf **Jobüberwachung**

Sie können auf den Namen eines Jobs klicken, um die entsprechenden Details anzuzeigen. Wenn Sie nach einer bestimmten Stelle suchen, können Sie:

- Verwenden Sie die Zeitauswahl oben auf der Seite, um Jobs für einen bestimmten Zeitraum anzuzeigen
- Geben Sie einen Teil des Jobnamens in das Suchfeld ein
- Sortieren Sie die Ergebnisse mithilfe des Filters in jeder Spaltenüberschrift

## Audit-Daten

Wenn Sie entweder eine API direkt ausführen oder die Benutzeroberfläche verwenden, um den API-Aufruf an eine der extern exponierten APIs des Cloud Backup for Applications durchzuführen, werden die Anforderungsdetails wie Headern, Rolle, Anforderungskörper, Und API-Informationen werden in der BlueXP-Zeitleiste protokolliert und die Audit-Einträge werden für immer in der Zeitleiste gespeichert. Der Status und die Fehlerantwort des API-Aufrufs werden ebenfalls nach Abschluss des Vorgangs geprüft. Bei asynchronen API-Antworten wie Jobs wird auch die Job-id im Rahmen der Antwort protokolliert.

Cloud Backup for Applications protokolliert die Einträge wie Host-IP, Request Body, Operation Name, wer ausgelöst hat, einige Header, Und den Betriebsstatus der API.

## Zeigen Sie Backup-Details an

Sie können die Gesamtzahl der erstellten Backups, die Richtlinien zum Erstellen von Backups, die Datenbankversion und die Agenten-ID anzeigen.





1. Klicken Sie auf **Backup und Recovery > Anwendungen**.
2. Klicken Sie Auf **...** Entsprechend der Anwendung und klicken Sie auf **Details anzeigen**.



Die Agent-ID ist dem Konnektor zugeordnet. Wenn ein Connector, der bei der Registrierung des SAP HANA-Hosts verwendet wurde, nicht mehr vorhanden ist, schlagen die nachfolgenden Backups dieser Anwendung fehl, da die Agent-ID des neuen Connectors anders ist. Sie sollten die Konnektor-id im Host ändern.

## Klon löschen

Sie können einen Klon löschen, wenn Sie nicht mehr benötigen.

1. Klicken Sie Auf  Neben **Filtern nach** und wählen Sie **Clone-Optionen > Eltern klonen**.
2. Klicken Sie Auf  Entsprechend der Anwendung und klicken Sie auf **Details anzeigen**.
3. Klicken Sie auf der Seite Datenbankdetails auf  Neben **Filter by** und wählen Sie **Clone**.
4. Klicken Sie Auf  Entsprechend dem Klon, den Sie löschen möchten, und klicken Sie auf **Löschen**.
5. (Optional) Aktivieren Sie das Kontrollkästchen **Force delete**.

## Aktualisieren Sie die Connector-Details für den SAP HANA-Datenbank-Host

Wenn der Connector, der bei der Registrierung des Anwendungshosts verwendet wurde, nicht mehr existiert oder beschädigt ist, sollten Sie einen neuen Konnektor bereitstellen. Nach der Bereitstellung des neuen Connectors sollten Sie die **Connector-Update** API ausführen, um die Connector-Details für alle Hosts zu aktualisieren, die über den alten Konnektor registriert sind.

```
curl --location --request PATCH
'https://snapcenter.cloudmanager.cloud.netapp.com/api/saphana/hosts/connector/update' \
--header 'x-account-id: <CM account-id>' \
--header 'Authorization: Bearer token' \
--header 'Content-Type: application/json' \
--data-raw '{
"old_connector_id": "Old connector id that no longer exists",
"new_connector_id": "New connector Id"
}'
```

Connector-Details werden erfolgreich aktualisiert, wenn alle Hosts über ein SnapCenter-Plug-in für SAP HANA-Dienst installiert und ausgeführt werden und wenn sie alle über den neuen Konnektor erreichbar sind.

## Konfigurieren Sie das Zertifikat der Zertifizierungsstelle

Sie können ein Zertifikat mit Zertifizierungsstelle konfigurieren, wenn Sie zusätzliche Sicherheit in Ihre Umgebung aufnehmen möchten.

### Konfigurieren Sie das Zertifikat einer Zertifizierungsstelle für die Authentifizierung des Clientzertifikats

Der Anschluss verwendet ein selbstsigniertes Zertifikat, um mit dem Plug-in zu kommunizieren. Das selbstsignierte Zertifikat wird vom Installationsskript in den Schlüsselspeicher importiert. Sie können die folgenden Schritte durchführen, um das selbstsignierte Zertifikat durch CA-signiertes Zertifikat zu ersetzen.

### Was Sie brauchen

Sie können den folgenden Befehl ausführen, um **<base\_Mount\_path>** zu erhalten:

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

## Schritte

1. Melden Sie sich bei Connector an.
2. Löschen Sie alle vorhandenen Dateien unter `<base_Mount_PATH>/Client/Certificate` in der virtuellen Connector-Maschine.
3. Kopieren Sie das von der Zertifizierungsstelle signierte Zertifikat und die Schlüsseldatei in die virtuelle Konnektor-Maschine `<base_Mount_PATH>/Client/Certificate`.

Der Dateiname sollte `Certificate.pem` und `key.pem` sein. Das Zertifikat.pem sollte die gesamte Kette der Zertifikate wie Zwischenzertifikat und Root CA haben.

4. Erstellen Sie das PKCS12-Format des Zertifikats mit dem Namen `Certificate.p12` und behalten Sie `<base_Mount_path>/Client/Certificate`.
5. Kopieren Sie das `Certificate.p12` und die Zertifikate für alle Zwischenkatopie und Root-CA auf den Plug-in-Host unter `/var/opt/snapcenter/spl/etc/`.
6. Melden Sie sich beim Plug-in-Host an.

7. Navigieren Sie zu `/var/opt/snapcenter/spl/etc` und führen Sie den `keytool`-Befehl aus, um die Datei `Certificate.p12` zu importieren.

```
keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12  
-destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter  
-deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
```

8. Importieren Sie die Stammzertifizierungsstelle und die Zwischenzertifikate.

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



Die `certfile.crt` bezieht sich auf die Zertifikate der Root CA sowie der Zwischenzertifizierungsstelle.

9. SPL neu starten: `systemctl restart spl`

## Konfigurieren Sie das CA-Zertifikat für das Server-Zertifikat des Plug-ins

Das CA-Zertifikat sollte den genauen Namen des Plug-in-Hosts haben, mit dem die virtuelle Connector-Maschine kommuniziert.

### Was Sie brauchen

Sie können den folgenden Befehl ausführen, um `<base_Mount_path>` zu erhalten:

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

## Schritte

1. Führen Sie auf dem Plug-in-Host folgende Schritte durch:
  - a. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher `/var/opt/snapcenter/spl/etc`.
  - b. Erstellen Sie das PKCS12-Format des Zertifikats, das sowohl ein Zertifikat als auch einen Schlüssel mit dem Alias `splkeystore` hat.
  - c. Fügen Sie das CA-Zertifikat hinzu.

```
keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype
```

```
pkcs12 -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore  
-destalias splkeystore -noprompt
```

- d. Überprüfen Sie die Zertifikate.

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

- e. SPL neu starten: `systemctl restart spl`

2. Führen Sie die folgenden Schritte auf dem Konnektor aus:

- a. Melden Sie sich beim Connector als nicht-Root-Benutzer an.
- b. Kopieren Sie die gesamte Kette der CA-Zertifikate auf das persistente Volume unter `<base_Mount_PATH>/Server`.

Erstellen Sie den Serverordner, falls er nicht vorhanden ist.

- c. Verbinden Sie sich mit dem `cloudmanager_scs_Cloud` und ändern Sie den **enableCACert** in `config.yml` an **true**.

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

- d. Starten Sie den Cloud-Manager\_scs\_Cloud-Container neu.

```
sudo docker restart cloudmanager_scs_cloud
```

## Zugriff auf REST-APIs

ES sind DIE REST-APIs zum Schutz der Applikationen in der Cloud verfügbar ["Hier"](#).

Sie sollten das Benutzer-Token mit gebündelter Authentifizierung erhalten, um auf DIE REST-APIs zuzugreifen. Informationen zum Abrufen des Benutzer-Tokens finden Sie unter ["Erstellen Sie ein Benutzer-Token mit gebündelter Authentifizierung"](#).

## Copyright-Informationen

Copyright © 2022 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, BEISPIELHAFTE 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.