



# **Backup und Wiederherstellung von Cloud-nativen Applikationsdaten**

BlueXP backup and recovery

NetApp  
April 18, 2024

# Inhalt

- Backup und Wiederherstellung von Cloud-nativen Applikationsdaten . . . . . 1
  - Sichern Sie Ihre Cloud-nativen Applikationsdaten . . . . . 1
  - Backup von Cloud-nativen Oracle-Datenbanken . . . . . 5
  - Backup von Cloud-nativen SAP HANA-Datenbanken . . . . . 18
  - Sichern Sie Cloud-native SQL Server-Datenbanken mit REST-APIs . . . . . 28
  - Stellen Sie Cloud-native Oracle-Datenbanken wieder her . . . . . 40
  - Wiederherstellung von Cloud-nativen SAP HANA-Datenbanken . . . . . 42
  - Stellen Sie die Microsoft SQL Server-Datenbank wieder her . . . . . 44
  - Klonen Cloud-nativer Oracle-Datenbanken . . . . . 47
  - Aktualisierung des SAP HANA-Zielsystems . . . . . 56
  - Management der Sicherung von Cloud-nativen Applikationsdaten . . . . . 57

# Backup und Wiederherstellung von Cloud-nativen Applikationsdaten

## Sichern Sie Ihre Cloud-nativen Applikationsdaten

BlueXP Backup und Recovery für Applikationen bietet applikationskonsistente Datensicherungsfunktionen für Applikationen, die auf NetApp Cloud Storage ausgeführt werden. BlueXP Backup und Recovery bietet effizienten, applikationskonsistenten und richtlinienbasierten Schutz für die folgenden Applikationen:

- Oracle Datenbanken, die sich auf Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP und Azure NetApp Files befinden
- SAP HANA-Systeme auf Azure NetApp Files
- Microsoft SQL Server-Datenbanken auf Amazon FSX für NetApp ONTAP

## Der Netapp Architektur Sind

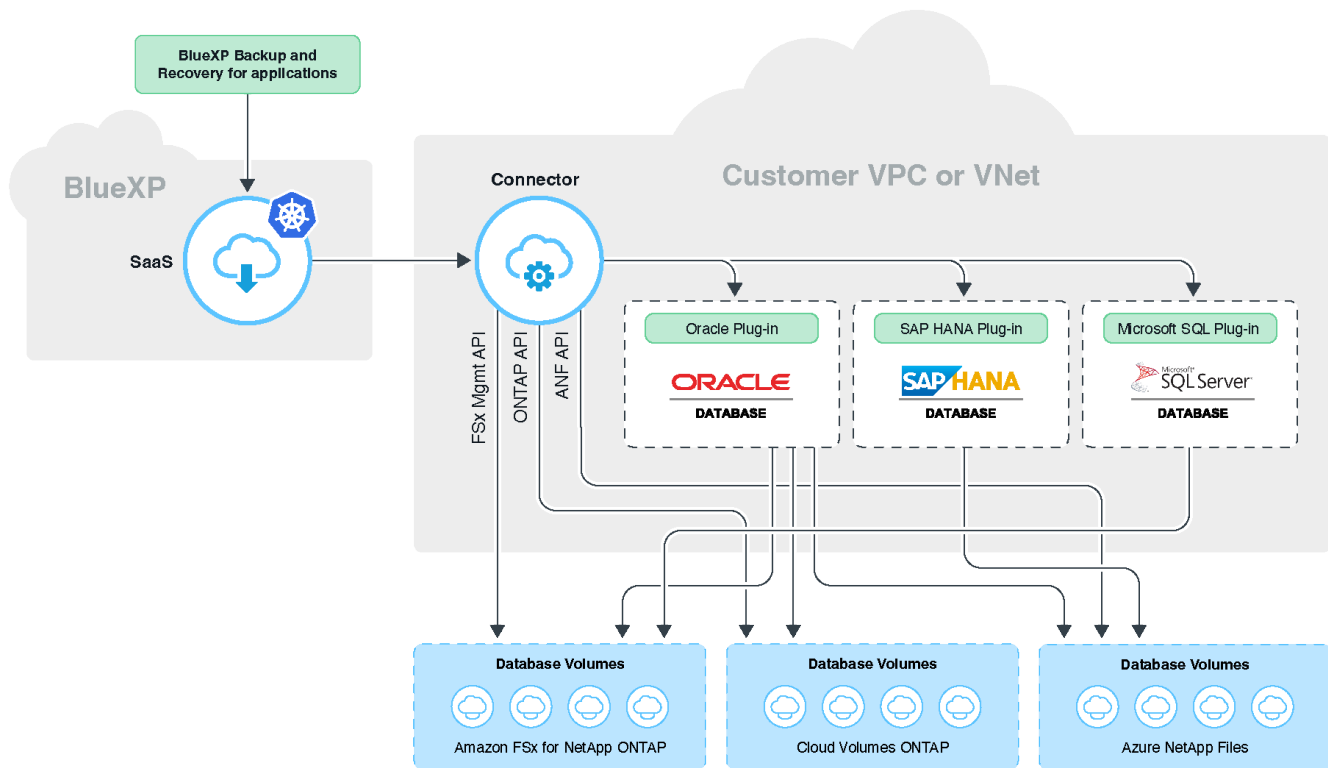
Die BlueXP Backup- und Recovery-Architektur für Applikationen umfasst die folgenden Komponenten:

- Das Backup und Recovery von BlueXP 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.

- Die BlueXP UI bietet Datensicherungsfunktionen für Applikationen und ist über die BlueXP UI zugänglich.
- BlueXP Connector ist eine Komponente, die in Ihrem Cloud-Netzwerk 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:



Bei vom Benutzer initiierten Anfragen kommuniziert die BlueXP UI mit der BlueXP SaaS. Dabei wird die Anforderung validiert, um dieselbe Verarbeitung zu erhalten. 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.



Die BlueXP SaaS-Infrastruktur ist robust gegenüber Ausfällen der Verfügbarkeitszonen innerhalb einer Region. Es unterstützt regionale Ausfälle durch Failover auf eine neue Region, und der Failover hat ungefähr zwei Stunden Ausfallzeit.

## Schutz von Oracle Datenbanken

### Funktionen

- Host hinzufügen und Plug-in implementieren

Plug-in kann über UI, Skript oder manuell implementiert werden.

- Automatische Erkennung von Oracle-Datenbanken

- Sichern von Oracle-Datenbanken auf Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP und Azure NetApp Files
  - 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. Sie können auch die Post-Skripte angeben, die nach einem erfolgreichen Backup ausgeführt werden, um den Snapshot in den sekundären Speicher zu kopieren.
- Backups von Oracle-Datenbanken auf Azure NetApp Files können mit Oracle RMAN katalogisiert werden
- Aufbewahrung von Backups anhand der Richtlinie
- Wiederherstellung von Oracle Datenbanken auf Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP und Azure NetApp Files
  - Wiederherstellen der vollständigen Oracle-Datenbank (Datendateien + Kontrolldatei) aus dem angegebenen Backup
  - Wiederherstellen der Oracle-Datenbank mit bis SCN, bis zu der Zeit, alle verfügbaren Protokolle und keine Recovery-Optionen
- Wiederherstellung von Oracle-Datenbanken auf Azure NetApp Files an einem alternativen Speicherort
- Klonen von Oracle-Datenbanken, die sich auf Amazon FSX für NetApp ONTAP und Cloud Volumes ONTAP auf Quell- oder alternativen Ziel-Hosts befinden
  - 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
- Aktualisieren Sie das Host-Plug-in

## 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-Adresse ausfällt oder Sie nicht auf die IP-Adresse zugreifen können, schlägt der Datenschutzbetrieb fehl.
- Die IP-Adressen der Netzwerkschnittstelle von Amazon FSX for NetApp ONTAP oder Cloud Volumes ONTAP müssen im BlueXP Konto und in der Region eindeutig sein.

# Schutz von SAP HANA Datenbanken

## 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

# Sicherung von Microsoft SQL Server Datenbanken

## Funktionen

- Host manuell hinzufügen und Plug-in bereitstellen
- Ermitteln Sie die Datenbanken manuell
- Erstellen Sie ein Backup von SQL Server Instanzen auf Amazon FSX for NetApp ONTAP
  - On-Demand-Backup
  - Geplantes Backup basierend auf der Richtlinie
  - Protokollsicherung der Microsoft SQL Server-Instanz
- Stellen Sie die Datenbank am ursprünglichen Speicherort wieder her

## Einschränkungen

- Backup wird nur für SQL Server-Instanzen unterstützt
- Die Konfiguration der Failover-Cluster-Instanz (FCI) wird nicht unterstützt
- Die BlueXP UI unterstützt keine für SQL-Datenbanken spezifischen Vorgänge

Alle für Microsoft SQL Server-Datenbanken spezifischen Vorgänge werden mithilfe von REST-APIs ausgeführt.

- Die Wiederherstellung an einem alternativen Speicherort wird nicht unterstützt

# 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_plug  
in_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.	-
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 <b>Upgrade Plug-in</b>.</p> <p>b. Führen Sie auf der Seite Konfiguration die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>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.</li> <li>Kopieren Sie den in der BlueXP UI angezeigten Text.</li> <li>Bearbeiten Sie die Datei <code>/etc/sudoers.d/snapcenter</code> auf dem Linux-Rechner und fügen Sie den kopierten Text ein.</li> <li>Aktivieren Sie in der BlueXP UI das Kontrollkästchen und klicken Sie auf <b>Upgrade</b>.</li> </ol>	<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 &lt;plugin_host&gt; --username &lt;host_user_name&gt; --sshkey &lt;host_ssh_key&gt; --pluginport &lt;plugin_port&gt; --sshport &lt;host_ssh_port&gt; --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 &lt;plugin_host&gt; --username &lt;host_user_name&gt; --sshkey &lt;host_ssh_key&gt; --pluginport &lt;plugin_port&gt; --sshport &lt;host_ssh_port&gt; --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 Tablespaces 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.
- (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"](#).

# Backup von Cloud-nativen SAP HANA-Datenbanken

## Schnellstart

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

1

### Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Betriebssystem:
  - RHEL 7.6 oder höher
  - RHEL 8.1 oder höher für SAP-HANA SPS07
  - SLES 12 SP5 oder höher und 15 SPX Plattformen zertifiziert von SAP HANA
- Azure NetApp Files, NetApp Cloud-Storage
- Storage-Layouts: Für Daten- und Log-Dateien unterstützt Azure nur NFSv4.1.
- Datenbank-Layout:
  - SAP HANA Multitenant Database Container (MDC) 2.0SPS5, 2.0SPS6, 2.0SPS7 mit einzelnen oder mehreren Mandanten

- SAP HANA Einzelhostsystem, SAP HANA Mehrfach-Hostsystem, HANA System Replication
- Plug-in für SAP HANA auf dem Datenbank-Host

**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 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 SAP HANA und fügen Sie Datenbank-Hosts hinzu

Sie sollten das SnapCenter-Plug-in für SAP HANA auf jedem der SAP HANA-Datenbank-Hosts installieren. Je nachdem, ob auf dem SAP HANA-Host eine auf SSH-Schlüssel basierende Authentifizierung aktiviert ist, können Sie eine der Methoden zur Installation des Plug-ins befolgen.

- Wenn SSH für den Datenbank-Host aktiviert ist, können Sie das Plug-in mithilfe der SSH-Option installieren. [Weitere Informationen ..](#)
- Wenn SSH deaktiviert ist, installieren Sie das Plug-in manuell. [Weitere Informationen ..](#)

### Voraussetzungen

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

- Vergewissern Sie sich, dass auf jedem der SAP HANA-Datenbank-Hosts Java 11 (64-Bit) oder OpenJDK installiert ist.
- Sie sollten die Arbeitsumgebung hinzugefügt und den Connector erstellt haben.
- Stellen Sie sicher, dass der Connector mit den SAP HANA-Datenbank-Hosts verbunden ist.

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.
- Sie sollten den SnapCenter-Benutzer erstellt und sudo für den Benutzer nicht-root (sudo) konfiguriert haben. Weitere Informationen finden Sie unter "[Konfigurieren Sie sudo für SnapCenter-Benutzer](#)".
- Sie sollten das SnapCenter-Plug-in für SAP HANA installiert haben, bevor Sie den Datenbank-Host hinzufügen.
- Beim Hinzufügen der SAP HANA-Datenbank-Hosts sollten Sie die HDB-Benutzerspeicherschlüssel hinzufügen. Der HDB Secure User Store-Schlüssel wird verwendet, um die Verbindungsinformationen der SAP HANA Datenbank-Hosts sicher auf dem Client zu speichern und HDBSQL-Client verwendet den sicheren User Store-Schlüssel für die Verbindung zum SAP HANA-Datenbank-Host.
- Für HANA System Replication (HSR) sollten Sie zum Schutz der HANA-Systeme sowohl primäre als auch sekundäre HANA-Systeme manuell registrieren.



Der Hostname muss der gleiche sein wie der Host, der in der HSR-Replikation verwendet wird.

- 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 SAP HANA Datenbank](#).

## Konfigurieren Sie sudo für SnapCenter-Benutzer

Erstellen Sie einen nicht-Root-Benutzer (sudo), um das Plug-in zu installieren.

### 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. Kopieren Sie den Inhalt von **sudoeer.txt** unter: `/var/lib/Docker/Volumes/Service-Manager-2_cloudmanager_scs_Cloud_Volume/_Data/€(sudo docker ps_grep -Po "Cloud Manager_scs_Cloud:.*? „/sed -e s/ *€/“ Cut -f2 -d“:“)/sc-linux-Host-Plugin`
4. Melden Sie sich über das root-Benutzerkonto beim SAP HANA-Systemhost an.
5. Konfigurieren Sie den sudo-Zugriff für den nicht-root-Benutzer, indem Sie den im Schritt 3 kopierten Text in die `/etc/sudoers.d/snapcenter`-Datei kopieren.

Ersetzen Sie in den Zeilen, die Sie der `/etc/sudoers.d/snapcenter`-Datei hinzugefügt haben, `<LINUXUSER>` durch den Benutzer nicht-root und `<USER_HOME_DIRECTORY>` durch `Home/<non-root-user>`.

## Installieren Sie das Plug-in mithilfe des Skripts

Konfigurieren Sie die SSH-Schlüsselauthentifizierung für das nicht-root-Benutzerkonto des SAP HANA-Hosts und führen Sie die folgenden Schritte zur Installation des Plug-ins aus.

### Bevor Sie beginnen

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

### Schritte

1. Melden Sie sich bei Connector VM an.
2. Installieren Sie das Plug-in mit dem im Connector bereitgestellten Skript.  

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

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 SAP HANA-Host an	Ja.	-

Name	Beschreibung	Obligatorisch	Standard
Host_User_Name	Gibt den SnapCenter-Benutzer mit SSH-Berechtigungen auf dem SAP HANA-Host an	Ja.	-
Host_ssh_Key	Gibt den SSH-Schlüssel des SnapCenter-Benutzers an und wird zur Verbindung mit dem SAP HANA-Host verwendet	Ja.	-
Plugin_Port	Gibt den vom Plug-in verwendeten Port an	Nein	8145
Host_ssh_Port	Gibt den SSH-Port auf dem SAP HANA-Host an	Nein	22

Beispiel: ``sudo bash /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``

Nach der Installation des Plug-ins sollten Sie dies tun [Fügen Sie SAP HANA Datenbank-Hosts hinzu](#).

### Installieren Sie das Plug-in manuell

Wenn die SSH-Schlüsselauthentifizierung auf dem HANA-Host nicht aktiviert ist, sollten Sie die folgenden manuellen Schritte ausführen, um das Plug-in zu installieren.

#### Schritte

1. Melden Sie sich bei 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'
```

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

3. Kopieren Sie `snapcenter_linux_Host_Plugin_scs.bin` von dem obigen Pfad zu `/Home/<non root user>/.sc_netapp` Pfad für jeden der SAP HANA Datenbank Hosts entweder mit scp oder anderen alternativen Methoden.
4. Melden Sie sich über das nicht-Root-Konto (sudo) beim SAP HANA-Datenbank-Host an.
5. 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
```
6. Installieren Sie das SAP HANA-Plug-in als sudo-SnapCenter-Benutzer.



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

7. 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.
8. Navigieren Sie zu */var/opt/snapcenter/spl/etc* und führen Sie den keytool-Befehl aus, um das Zertifikat zu importieren.  

```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks  
-deststorepass snapcenter -noprompt
```
9. SPL neu starten: 

```
systemctl restart spl
```
10. 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
```

Nach der Installation des Plug-ins sollten Sie dies tun [Fügen Sie SAP HANA Datenbank-Hosts hinzu](#).

## Upgrade des SnapCenter Plug-in für SAP HANA Datenbank

Sie sollten das SnapCenter-Plug-in für SAP HANA-Datenbank aktualisieren, um auf die neuesten Funktionen und Verbesserungen zugreifen zu können.

### Bevor Sie beginnen

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

### Schritte

1. Konfigurieren Sie sudo für SnapCenter-Benutzer. Weitere Informationen finden Sie unter [Konfigurieren Sie sudo für SnapCenter-Benutzer](#).
2. Führen Sie das folgende Skript aus.  

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

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

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

## Fügen Sie SAP HANA Datenbank-Hosts hinzu

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

### Schritte

1. Wählen Sie in der **BlueXP**-Benutzeroberfläche **Schutz > Sicherung und Wiederherstellung >**

**Anwendungen** aus.

2. Wählen Sie **Anwendungen Entdecken**.
3. Wählen Sie **Cloud Native > SAP HANA** und dann **Next**.
4. Wählen Sie auf der Seite **Anwendungen** die Option **System hinzufügen** aus.
5. Führen Sie auf der Seite **Systemdetails** die folgenden Aktionen durch:
  - a. Wählen Sie den Systemtyp als mandantenfähiger Datenbank-Container oder als globale nicht-Daten-Volumes aus.
  - b. Geben Sie den SAP HANA-Systemnamen ein.
  - c. Geben Sie die SID des SAP HANA-Systems an.
  - d. (Optional) OSDB-Benutzer ändern.
  - e. Wenn HANA-System mit HANA System Replication konfiguriert ist, aktivieren Sie **HANA System Replication (HSR) System**.
  - f. Wählen Sie das Textfeld **HDB Secure User Store Keys** aus, um Details zum Benutzerspeicher hinzuzufügen.

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

Sie können die Benutzerspeicherschlüssel löschen oder ändern.

6. Wählen Sie **Weiter**.
7. Führen Sie auf der Seite **Host Details** die folgenden Aktionen durch:
  - a. Wählen Sie **Neuen Host hinzufügen** oder **vorhandenen Host verwenden**.
  - b. Wählen Sie **mit SSH** oder **manuell** aus.

Geben Sie für Manual den Host-FQDN oder IP, Connector, Username, SSH-Port, Plug-in-Port, und fügen Sie optional den privaten SSH-Schlüssel hinzu und validieren Sie diesen.

Geben Sie für SSH den Host-FQDN oder die IP-Adresse, den Connector, den Benutzernamen und den Plug-in-Port ein.

- a. Wählen Sie **Weiter**.
8. Überprüfen Sie auf der Seite **Host Configuration**, ob die Konfigurationsanforderungen erfüllt sind.

Aktivieren Sie zur Bestätigung die Kontrollkästchen.

9. Wählen Sie **Weiter**.

10. Wählen Sie auf der Seite **Storage Footprint** die Option **Add Storage** aus, und führen Sie die folgenden Schritte aus:
  - a. Wählen Sie die Arbeitsumgebung aus und geben Sie den NetApp Account an.

Wählen Sie im linken Navigationsbereich BlueXP **Canvas** aus, um eine neue Arbeitsumgebung hinzuzufügen.
  - b. Wählen Sie die erforderlichen Volumes aus.
  - c. Wählen Sie **Speicher Hinzufügen**.

11. Überprüfen Sie alle Details und wählen Sie **System hinzufügen**.

Sie können die SAP HANA-Systeme von der Benutzeroberfläche ändern oder entfernen.

Bevor Sie das SAP HANA-System entfernen, sollten Sie alle zugehörigen Backups löschen und den Schutz entfernen.

#### Hinzufügen Von Nicht-Daten-Volumes

Nach dem Hinzufügen des mandantenfähigen Datenbank-Containers vom Typ SAP HANA-System können Sie die nicht-Daten-Volumes des HANA-Systems hinzufügen.

Diese Ressourcen können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge durchzuführen, nachdem die verfügbaren SAP HANA Datenbanken ermittelt wurden.

#### Schritte

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

#### Hinzufügen Von Globalen, Nicht Datenbasierten Volumes

Nach dem Hinzufügen des mandantenfähigen Datenbank-Containers vom Typ SAP HANA-System können Sie die globalen nicht-Daten-Volumes des HANA-Systems hinzufügen.

#### Schritte

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

## Backup von Cloud-nativen SAP HANA-Datenbanken

Sie können ein Backup erstellen, indem Sie eine vordefinierte Richtlinie oder die erstellte

Richtlinie zuweisen.

## Richtlinie erstellen, um die SAP HANA-Datenbank zu sichern

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

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

### Vorschriften und Postskripte

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

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

Das Prescript und das Postscript sollten vom Hostadministrator registriert werden  
/opt/NetApp/snapcenter/scc/etc/allowed\_commands.config Datei:

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

### Umgebungsvariablen

Für den Backup-Workflow stehen die folgenden Umgebungsvariablen als Teil von prescript und postscript zur Verfügung.

Umgebungsvariable	Beschreibung
SID	Die Systemkennung der zur Wiederherstellung ausgewählten HANA-Datenbank
BackupName	Für den Wiederherstellungsvorgang ausgewählte Sicherungsname
UserStoreKeyNames	Konfigurierter Benutzerspeicherschlüssel für die HANA-Datenbank

Umgebungsvariable	Beschreibung
OSDBUser	OSDBUser für die HANA-Datenbank konfiguriert
PolicyName	Nur für geplante Backups
Schedule_TYPE	Nur für geplante Backups

## Backup der SAP HANA Datenbank erstellen

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

### Bevor Sie beginnen

Sie sollten die SAP HANA Datenbank-Hosts hinzugefügt haben. "[Fügen Sie SAP HANA Datenbank-Hosts hinzu](#)"

### Über diese Aufgabe

Für HANA System Replication (HSR) wird der geplante Backup-Job nur für das primäre HANA-System ausgelöst. Wenn das System auf das sekundäre HANA-System übergeht, werden durch die vorhandenen Zeitpläne ein Backup auf dem aktuellen primären HANA-System ausgelöst. Wenn die Richtlinie nicht sowohl dem primären als auch dem sekundären HANA-System zugewiesen ist, schlägt nach einem Failover der Zeitplan fehl.

Wenn den HSR-Systemen unterschiedliche Richtlinien zugewiesen werden, schlagen die geplanten Backup-Trigger sowohl für die primären als auch für sekundäre HANA-Systeme und das Backup für das sekundäre HANA-System fehl.

### Schritte

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

Obwohl die Datenbank mit einer oder mehreren Richtlinien geschützt ist, können Sie bei Bedarf weitere Richtlinien zuweisen, indem Sie auf klicken **... > Richtlinie Zuweisen**.

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

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



Das Servicekonto (*SnapCenter-Account-`<account_id>`*) wird für die geplanten Backup-Vorgänge verwendet.

## On-Demand-Backup der SAP HANA-Datenbank erstellen

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

### Schritte

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

Weitere Informationen finden Sie unter ["Verordnungen und Postskripte"](#)
  - c. Klicken Sie Auf **Backup Erstellen**.

## Sichern Sie Cloud-native SQL Server-Datenbanken mit REST-APIs

### Schnellstart

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

1

#### Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Betriebssystem:
  - Windows 2016
  - Windows 2019
  - Windows 2022
- NetApp Cloud-Storage Amazon FSX für NetApp ONTAP
- Storage-Layouts: SAN (iSCSI)

NAS-Konfiguration wird nicht unterstützt.

- Datenbankversionen:
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2022
- Datenbankkonfiguration:
  - Standalone

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.

## Installieren Sie das SnapCenter-Plug-in für SQL Server, und fügen Sie Datenbank-Hosts hinzu

Sie sollten das SnapCenter-Plug-in für SQL Server auf jedem der SQL-Datenbankhosts installieren, die Datenbank-Hosts hinzufügen, die Datenbankinstanzen ermitteln und die Anmeldeinformationen für die Datenbankinstanzen konfigurieren.

### Installieren Sie das SnapCenter-Plug-in für SQL Server

Sie sollten das Plug-in **snapcenter\_Service\_Windows\_Host\_Plugin.exe** herunterladen und dann den Befehl des automatischen Installers ausführen, um das Plug-in auf dem Datenbank-Host zu installieren.

#### Bevor Sie beginnen

- Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.
  - .Net 4.7.2 ist installiert
  - PowerShell 4.0 ist installiert
  - Mindestens 5 GB Festplattenspeicher ist verfügbar
  - Mindestens RAM-Größe von 4 GB ist verfügbar
- Sie sollten die API ausführen, um die Kundenanordnung abzuschließen. Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Tenant%20Registration/createTenant>

#### Schritte

1. Laden Sie das Plug-in herunter, indem Sie die API vom Connector-Host ausführen.

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

Der Speicherort der Datei ist */var/lib/Docker/Volumes/Service-Manager-2\_Cloudmanager\_scs\_Cloud\_Volume/\_Data/<agent\_version>/sc-Windows-Host-Plugin/snapcenter\_Service\_Windows\_Host\_Plugin.exe*.

2. Kopieren Sie *snapcenter\_Service\_Windows\_Host\_Plugin.exe* vom Konnektor auf jeden der MSSQL Server Datenbank-Hosts entweder mit scp oder anderen alternativen Methoden.
3. Installieren Sie das Plug-in.  
„C://<install\_folder>/snapcenter\_Service\_Windows\_Host\_Plugin.exe“/silent/debuglog



```
„C://<install_folder>/HA_Suite_Silent_Install_SCSQL_FRESH.log“ /log„C://install_folder/“  
BI_SNAPCENTER_PORT=8145 ISFeatureInstall=SCSQL“
```

4. Kopieren Sie das selbstsignierte Zertifikat von `/var/lib/Docker/Volumes/Service-Manager-2_Cloudmanager_scs_Cloud_Volume/_Data/Client/Certificate/Certificate.pem` auf die MSSQL Server-Datenbank-Hosts.

Sie können auch ein selbstsigniertes Zertifikat oder ein CA-signiertes Zertifikat generieren, wenn Sie das Standardzertifikat nicht verwenden.

5. Konvertieren Sie das Zertifikat aus dem Pem-Format in das crt-Format im Connector-Host.  
'openssl x509 -outform der -in Certificate.pem -out Certificate.crt'
6. Doppelklicken Sie auf das Zertifikat, um es dem Speicher **Personal** und **Trusted Root Certification Authorities** hinzuzufügen.

## Fügen Sie den SQL Server-Datenbankhost hinzu

Sie sollten den MSSQL-Datenbank-Host mithilfe des Host-FQDN hinzufügen.

„NACH snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/AddHosts>

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

### Parameter

Name	Typ	Erforderlich
Adr.	Zeichenfolge	Richtig
Connector_id	Zeichenfolge	Richtig
Plug-in_TYPE	Zeichenfolge	Richtig
Install_Method	Zeichenfolge	Richtig
Plugin_Port	Nummer	Richtig
Benutzername	Zeichenfolge	Richtig

### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 202 angezeigt.

Beispiel:

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

### **Zeigen Sie die hinzugefügten SQL Server-Datenbank-Hosts an**

Sie können diese API ausführen, um alle hinzugefügten SQL Server-Datenbank-Hosts anzuzeigen.

'snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts' ERHALTEN

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/GetHosts>

### **Antwort**

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 200 angezeigt.

Beispiel:

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

## Ermitteln Sie die Datenbankinstanzen

Sie können diese API ausführen und die Host-ID eingeben, um alle MSSQL-Instanzen zu ermitteln.

„NACH [snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery](https://snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery)“

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/MSSQLInstancesDiscoveryRequest>

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

### Parameter

Name	Typ	Erforderlich
Host_id	Zeichenfolge	Richtig

### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 202 angezeigt.

Beispiel:

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

### Zeigen Sie die ermittelten Datenbankinstanzen an

Sie können diese API ausführen, um alle erkannten Datenbankinstanzen anzuzeigen.

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances' ERHALTEN

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/MSSQL%20Instances/GetMSSQLInstancesRequest>

### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 200 angezeigt.

Beispiel:

```

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

```

## Konfigurieren Sie die Anmeldeinformationen der Datenbankinstanz

Sie können diese API ausführen, um Anmeldeinformationen für die Datenbankinstanzen zu validieren und festzulegen.

„NACH [snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration](https://snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration)“

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/ConfigureCredentialRequest>

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

## Parameter

Name	Typ	Erforderlich
Host_id	Zeichenfolge	Richtig
Instanz-ids	Zeichenfolge	Richtig
Benutzername	Zeichenfolge	Richtig
Passwort	Zeichenfolge	Richtig
Auth_Mode	Zeichenfolge	Richtig

## Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 202 angezeigt.

Beispiel:

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

## Backup Cloud-nativer Microsoft SQL Server-Datenbanken

Sie können geplante oder On-Demand-Backups erstellen, indem Sie die von Ihnen erstellten Richtlinien zuweisen.

### Backup-Richtlinie erstellen

Sie können diese API ausführen, um die Sicherungsrichtlinie zu erstellen.

„NACH [snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies](https://snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies)“

Weitere Informationen finden Sie unter: [https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService\\_CreateMSSQLBackupPolicy](https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService_CreateMSSQLBackupPolicy)

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

## Parameter

Name	Typ	Erforderlich
Name	Zeichenfolge	Richtig
Backup_TYPE	Zeichenfolge	Richtig
Copy_only_Backup	Zeichenfolge	Falsch
Is_System_defined	Zeichenfolge	Falsch
Backup_Name_Format	Zeichenfolge	Richtig
Schedule_TYPE	Zeichenfolge	Richtig
Start_Time	Nummer	Richtig
Stundenintervall	Nummer	Richtig
Minuten_Intervall	Nummer	Richtig
Retention_type	Zeichenfolge	Richtig
Retention_count	Nummer	Richtig
Ende_Zeit	Nummer	Richtig

## Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 201 angezeigt.

Beispiel:

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

## Weisen Sie der SQL-Datenbankinstanz eine Richtlinie zu

Sie können diese API ausführen, um der SQL-Datenbankinstanz eine Richtlinie zuzuweisen.

„NACH snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/{id}/policy-assignment“

Wobei *id* die MSSQL-Instanz-ID ist, die durch Ausführen der Discover-Datenbankinstanz-API erhalten wird. Weitere Informationen finden Sie unter "[Ermitteln Sie die Datenbankinstanzen](#)".

Array von IDs ist hier der Eingang. Beispiel:

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

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Policy%20Assignment/PostMSSQLInstanceAssignPolicyRequest>

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

#### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 202 angezeigt.

Beispiel:

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

#### Erstellen Sie ein On-Demand-Backup

Sie können diese API ausführen, um ein On-Demand-Backup zu erstellen.


„NACH [snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups](https://snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups)“

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/CreateMSSQLBackupRequest>

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

#### Parameter



Name	Typ	Erforderlich
id	Zeichenfolge	Richtig
 Dies ist die ID der MSSQL-Datenbankinstanz.		
Resource_type	Zeichenfolge	Richtig
Richtlinien-id	Zeichenfolge	Richtig
Schedule_TYPE	Zeichenfolge	Richtig

#### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 202 angezeigt.

Beispiel:

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

#### Zeigen Sie die Backups an

Sie können diese APIs ausführen, um alle Backups aufzulisten und auch Details eines bestimmten Backups anzuzeigen.

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups' ERHALTEN

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups/{id}' ERHALTEN

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/MSSQL%20Backups/MSSQLGetBackupsRequest>

#### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 200 angezeigt.

Beispiel:

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

## Stellen Sie Cloud-native Oracle-Datenbanken wieder her

### Wiederherstellung von Cloud-nativen Oracle-Datenbanken am ursprünglichen Speicherort


Im Falle eines Datenverlustes können Sie die Datendateien, Kontrolldateien oder beides am ursprünglichen Speicherort wiederherstellen und dann die Datenbank wiederherstellen.

#### Bevor Sie beginnen

Wenn sich die Oracle 21c-Datenbank im STARTZUSTAND befindet, schlägt der Wiederherstellungsvorgang fehl. Sie sollten den folgenden Befehl 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  Der Datenbank, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
2. Wählen Sie den Wiederherstellungspunkt aus, an dem die Datenbank wiederhergestellt werden soll, und klicken Sie auf **an Originalspeicherort wiederherstellen**.
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.

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

Wenn das SnapCenter Plug-in für Oracle in Amazon FSX für NetApp ONTAP oder Cloud Volumes ONTAP SAN Layout andere fremde Dateien als Oracle-Datendateien auf der ASM-Festplattengruppe findet, wird die Wiederherstellungs- und Kopiermethode 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> .
Wiederherstellen einer bestimmten Systemänderungsnummer (SCN)	Wählen Sie <b>bis SCN</b> und geben Sie die 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**.

## Wiederherstellung von Cloud-nativen Oracle-Datenbanken an einem alternativen Speicherort

Im Falle eines Datenverlustes können Sie die Oracle Datenbank an einem alternativen Speicherort nur auf Azure NetApp Files wiederherstellen. Der alternative Speicherort kann sich auf einem anderen Host oder auf demselben Host befinden.

### Bevor Sie beginnen

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

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar  
/opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
```
- Stellen Sie sicher, dass die Oracle-Version auf dem alternativen Host mit der des ursprünglichen Hosts identisch ist.


### Über diese Aufgabe

Während des Wiederherstellungsvorgangs dürfen Sie die Konfigurationen mit Ausnahme der Oracle Startseite, des maximalen Volume-Durchsatzes, der Oracle SID und der Datenbankanmeldeinformationen nicht ändern.

Die vollständige Wiederherstellung ist standardmäßig mit *until Cancel* auf true aktiviert.

Der Archivprotokollmodus ist für die wiederhergestellte Datenbank standardmäßig deaktiviert. Sie können den Protokollmodus für die Archivierung aktivieren und bei Bedarf die Archivprotokolle auf dem NetApp Volume aufbewahren.

### Schritte

1. Klicken Sie Auf  Der Datenbank, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
2. Wählen Sie den Wiederherstellungspunkt aus, an dem die Datenbank wiederhergestellt werden soll, und klicken Sie auf **an alternativen Speicherort wiederherstellen > Weiter**.
3. Geben Sie auf der Seite Konfiguration die Details zum alternativen Speicherort, SID, Oracle\_Home, den Datenbankanmeldeinformationen und dem Speicherdurchsatz an.

Wenn die OS-Benutzerauthentifizierung deaktiviert ist, sollten Sie für die Datenbankanmeldeinformationen ein Kennwort angeben, mit dem der System-Benutzer eine Verbindung zur wiederhergestellten Datenbank auf demselben oder Zielhost herstellen kann.

4. Klicken Sie auf **Weiter**, überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

Der Fortschritt des Wiederherstellungsvorgangs kann auf der Seite Job Monitor angezeigt werden. Klicken Sie nach Abschluss des Jobs auf **Ermittlung aktualisieren**, um die wiederhergestellte Datenbank anzuzeigen. Sie können jedoch die Datenbank, die an einem anderen Speicherort wiederhergestellt wird, nicht schützen.

## Wiederherstellung von Cloud-nativen SAP HANA-Datenbanken

Im Falle eines Datenverlustes können Sie die Daten und nicht-Datendateien wiederherstellen und dann die Datenbank wiederherstellen.

## Bevor Sie beginnen

- Das SAP HANA-System muss sich im Zustand „gestoppt“ befinden.
- Wenn das SAP HANA-System betriebsbereit ist, können Sie ein Vorscript bereitstellen, um das System anzuhalten.

## Über diese Aufgabe

- Wenn Sie die ANF-Backups auf einem Volume aktivieren, wird ein SnapRestore-Vorgang mit einer einzigen Datei ausgeführt.
- Für nicht-Daten-Volumes und globale nicht-Daten-Volumes wird der Wiederherstellungs- und Kopiervorgang durchgeführt.
  - Die QoS-Werte (Quality of Service) für den Verbindungs- und Kopiervorgang werden von den Quell-Volumes von nicht-Daten-Volumes oder globalen nicht-Daten-Volumes abgeholt.



QoS gilt nur für Kapazitäts-Pools des Typs „manuell“.

## 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 wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
3. Geben Sie auf der Seite **System wiederherstellen** die Skripte ein. "[Verordnungen und Postskripte](#)."

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

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

4. Klicken Sie Auf **Wiederherstellen**.

## Wie geht's weiter

Stellen Sie nach der Wiederherstellung das SAP HANA System manuell wieder her oder geben Sie ein Post-Script ein, das die Wiederherstellung des SAP HANA Systems durchführt.

## Nicht-Daten-Volume Wiederherstellen

### Über diese Aufgabe

Gehen Sie zum Verbinden und Kopieren von Dateien zum Microsoft Azure Portal, wählen Sie das Volume aus, klicken Sie auf **Bearbeiten** und aktivieren Sie **Snapshot-Pfad ausblenden**.

### Schritte

1. Wählen Sie auf der Seite **Anwendungen** aus dem Dropdown-Feld Non-Data Volume aus.
2. Klicken Sie Auf ... Entsprechend dem Backup, das Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.

## Globales Volume Ohne Daten Wiederherstellen

### Über diese Aufgabe

Gehen Sie zum Verbinden und Kopieren von Dateien zum Microsoft Azure Portal, wählen Sie das Volume aus, klicken Sie auf **Bearbeiten** und aktivieren Sie **Snapshot-Pfad ausblenden**.

### Schritte

1. Klicken Sie auf der Seite **Anwendungen** auf das globale nicht-Daten-Volume, das Sie wiederherstellen möchten.
2. Klicken Sie Auf ... Entsprechend dem globalen nicht-Daten-Volume, das Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.

## Stellen Sie die Microsoft SQL Server-Datenbank wieder her

Sie können die Microsoft SQL Server-Datenbank auf demselben Host wiederherstellen. Sie sollten zuerst eine Liste der Datenbanken erhalten und dann die Datenbank wiederherstellen.

### Liste der Datenbanken anzeigen

Sie können diese API ausführen, um die Liste der Datenbanken anzuzeigen.

'snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases' ERHALTEN

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Databases/GetMSSQLDatabasesRequest>

### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 200 angezeigt.

Beispiel:

```

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

```

## Stellen Sie die MSSQL-Datenbank wieder her

Sie können diese API ausführen, um die MSSQL-Datenbank wiederherzustellen.

„NACH `snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases/{id}/restore`“

Wobei *id* die MSSQL-Datenbank-ID ist, die durch Ausführen der View-Datenbank-API abgerufen wird. Weitere Informationen finden Sie unter [Liste der Datenbanken anzeigen](#).

Weitere Informationen finden Sie unter: <https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Database%20Restore/RestoreMSSQLDatabaseRequest>

Diese API erstellt einen Job, der über die Registerkarte **Job Monitor** in der BlueXP-Benutzeroberfläche verfolgt werden kann.

### Parameter

Name	Typ	Erforderlich
Backup_id	Zeichenfolge	Richtig
Overwrite_Database	bool	Richtig
Reased_Replication_settings	bool	Falsch
Recovery_Modus	Zeichenfolge  Die 3 unterstützten Strings sind <i>Operational</i> , <i>nicht Operational</i> und <i>ReadOnly</i> .	Richtig
Undo_File_Directory	Zeichenfolge	Richtig
Restore_type	Zeichenfolge	Richtig

### Antwort

Wenn die API erfolgreich ausgeführt wurde, wird der Antwortcode 202 angezeigt.

Beispiel:



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

## Klonen Cloud-nativer Oracle-Datenbanken

### Klonkonzepte und -Anforderungen

Sie können eine Oracle-Datenbank auf Amazon FSX for NetApp ONTAP oder Cloud Volumes ONTAP klonen, indem Sie das Backup der Datenbank entweder auf dem Quelldatenbankhost oder auf einem alternativen Host verwenden. 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 Folgendes konfigurieren:
  - `AFD:*` wenn Sie ASMFD verwenden
  - `ORCL:*` wenn Sie ASMLIB verwenden
  - `/Dev/<exact_device_location>`, wenn Sie ASMUDEV 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.
  - Oracle-Software sollte auf dem alternativen Host installiert werden.
  - 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

- Das Klonen von Datenbanken auf Azure NetApp Files wird nicht unterstützt.
- Das Klonen von Datenbanken auf Qtree wird nicht unterstützt.
- Das Backup einer geklonten Datenbank wird nicht unterstützt.
- Wenn tägliche automatische Backups auf Amazon FSX for NetApp ONTAP aktiviert sind, können die geklonten Volumes auf Amazon FSX for NetApp ONTAP nicht aus der BlueXP Benutzeroberfläche gelöscht werden, da FSX Backups auf den geklonten Volumes erstellt hätte. Sie sollten die geklonten Volumes löschen, nachdem Sie alle Backups für das Volume aus der FSX UI gelöscht haben, und dann die Klone aus der BlueXP UI mit der Force-Option löschen.

## 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 Daten-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 Klon angegeben sind.
skip_Recovery	Führt keinen Wiederherstellungsvorgang aus.
Bis_scn	Stellt die Datenbank bis zur angegebenen Systemänderungsnummer (scn) wieder her.

Parameter	Beschreibung
„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>
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 einfache Klonmethode ausgewählt haben, wird die Suffixe die **Clone SID** sein.
- Wenn Sie die Spezifikationsdateimethode ausgewählt haben, ist das Suffix das **Suffix**, das beim Herunterladen der Clone-Spezifikationsdatei 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-Datenbanken

Sie können eine Oracle-Datenbank auf Amazon FSX for NetApp ONTAP oder Cloud Volumes ONTAP klonen, indem Sie das Backup der Datenbank entweder auf dem Quelldatenbankhost oder auf einem alternativen Host verwenden.

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.

#### Bevor Sie beginnen


Sie sollten die Klonkonzepte kennen 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>◦ Datenbankanmeldeinformationen: Wenn die OS-Benutzerauthentifizierung deaktiviert ist, sollten Sie ein Kennwort für den sys-Benutzer angeben, mit dem eine Verbindung zur geklonten Datenbank auf demselben oder Zielhost hergestellt werden kann.</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> <div><p>Stellen Sie sicher, dass der Listener auf dem Zielhost ausgeführt wird.</p></div> <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>◦ Datenbankanmeldeinformationen: Wenn die OS-Benutzerauthentifizierung deaktiviert ist, sollten Sie ein Kennwort für den sys-Benutzer angeben, mit dem eine Verbindung zur geklonten Datenbank auf demselben oder Zielhost hergestellt werden kann.</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> <div style="display: flex; align-items: center; margin-top: 20px;">  <div> <p>Stellen Sie sicher, dass der Listener auf dem Zielhost ausgeführt wird.</p> </div> </div> <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.

# Aktualisierung des SAP HANA-Zielsystems

Sie können eine Aktualisierung eines SAP HANA-Zielsystems mit den Daten eines SAP HANA-Quellsystems durchführen. Damit können die aktuellen Produktionsdaten in einem Testsystem bereitgestellt werden. Mit BlueXP Backup und Recovery können Sie eine Snapshot Kopie von einem Quellsystem auswählen und auf Basis der Snapshot Kopie ein neues Azure NetApp Files Volume erstellen. Es sind Beispielskripte verfügbar, die die erforderlichen Vorgänge auf dem Datenbank-Host ausführen, um die SAP HANA-Datenbank wiederherzustellen.

## Bevor Sie beginnen

- Sie sollten das SAP HANA-Zielsystem installieren, bevor Sie die erste Aktualisierung ausführen.
- Die Quell- und Ziel-HANA-Systeme sollten Sie manuell zu BlueXP Backup und Recovery hinzufügen.
- Stellen Sie sicher, dass die SAP HANA-Datenbankversion auf dem Quell- und Zielsystem identisch ist.
- Sie sollten sich für die zu verwendenden Refresh-Skripte entschieden haben. Die Aktualisierungsskripts sind im technischen Bericht zur Lösung verfügbar.

### "Beispielskripte zur Automatisierung"

Sie können die Aktualisierungsskripts anpassen.

- Die folgenden Umgebungsvariablen stehen als Teil des Prescript und des Postscripts zur Verfügung:
  - GEKLONTE\_VOLUMES\_MOUNT\_PATH
  - <SOURCEVOLUME>\_DESTINATION
  - HANA\_DATABASE\_TYPE
  - TENANT\_DATABASE\_NAMES
- Sie müssen das Plug-in auf Version 3.0 aktualisieren.
- Die Mount-Pfade sollten sowohl auf den Quell- als auch auf den Ziel-SAP HANA-Systemen für das Datenvolume identisch sein.
- Stellen Sie vor dem ersten Aktualisierungsvorgang sicher, dass die Datei '/etc/fstab' keine Einträge für die Datenvolumes des SAP HANA-Zielsystems enthält.

## Über diese Aufgabe

- Die Systemaktualisierung wird nur für das Container-HANA-System mit mehreren Mandanten unterstützt.
- Die vorhandenen Richtlinien sind nach der Systemaktualisierung gültig.
- Die neuen erstellten Volumes werden die folgende Namenskonvention haben: <sourcevolumename>-<timestamp>
  - Zeitstempelformat: <year> <month> <day>-<hour> <minute> <second>

Wenn das Quell-Volume beispielsweise vol1 ist, lautet der aktualisierte Volume-Name vol1-20230109-184501



Das neue Volume wird im gleichen Kapazitäts-Pool wie das der Ziel-Volumes platziert.

- Der Verbindungspfad entspricht dem Volume-Namen.
- Die „maximale Durchsatzzahl“ für das neue Volume wird aus dem Volume des Zielsystems mit manuellen Quality of Service (QoS) Kapazitäts-Pools ausgewählt.  
Bei Auto-QoS-Kapazitätspools wird der Durchsatz durch die Kapazität des Quell-Volume definiert.
- Während der Systemaktualisierung werden das automatische Mounten und Unmounten der Volumes mithilfe von Workflows anstelle von Skripten durchgeführt.

## Schritte

1. Klicken Sie in der BlueXP-Benutzeroberfläche auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Klicken Sie auf der Seite **Anwendungen** auf **...** Symbol, um die Aktion auszuwählen, die dem System entspricht, das Sie aktualisieren möchten, und wählen Sie **Systemaktualisierung**.
3. Führen Sie auf der Seite **Systemaktualisierung** die folgenden Aktionen durch:
  - a. Wählen Sie das Quellsystem und die Snapshot Kopie aus.
  - b. (Optional) Geben Sie Exportadressen ein, von denen aus auf die neuen Volumes zugegriffen werden kann.
  - c. (Optional) Geben Sie den maximalen Speicherdurchsatz (MiBs) ein.
  - d. Geben Sie Prescript, Postscript und On Failure Script-Pfade ein. Das Skript bei einem Fehler wird nur ausgeführt, wenn die Systemaktualisierung fehlschlägt.
  - e. Klicken Sie Auf **Aktualisieren**.

# Management der Sicherung von Cloud-nativen Applikationsdaten

## 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.



Die geplanten Jobs werden auf der Seite BlueXP Job Monitor nach einer Verzögerung von maximal 5 Minuten nach Abschluss des Jobs aufgelistet.

Weitere Informationen finden Sie unter "[Überwachen Sie den Jobstatus](#)".

## Wartung von Oracle-Datenbank-Hosts

Ein Administrator kann die Datenbank-Hosts manuell in den Wartungsmodus versetzen, um Wartungsaufgaben auf den Hosts durchzuführen. Während des Upgrades werden die Hosts automatisch in den Wartungsmodus versetzt und nach dem Upgrade werden die Hosts automatisch in den Produktionsmodus geschaltet.



Wenn die Hosts in den Wartungsmodus versetzt werden, schlagen die On-Demand-Vorgänge fehl und die geplanten Jobs werden übersprungen.



Sie können nicht überprüfen, ob Jobs für die Ressourcen auf den Hosts ausgeführt werden, bevor Sie die Hosts in den Wartungsmodus versetzen.

## Schritte

1. Klicken Sie in der Benutzeroberfläche von BlueXP auf **Schutz > Backup und Recovery > Anwendungen**
2. Wählen Sie **Oracle** als Anwendungstyp aus.
3. Klicken Sie Auf **Einstellungen > Hosts**.
4. Führen Sie eine der folgenden Aktionen aus:

Sie suchen...	Tun Sie das...
Der Host soll in den Wartungsmodus versetzt werden	Klicken Sie Auf  Entsprechend dem Host und wählen Sie <b>Wartungsmodus aktivieren</b> .
Der Host soll aus dem Wartungsmodus versetzt werden	Klicken Sie Auf  Entsprechend dem Host, der gewartet wird, und wählen Sie <b>Wartungsmodus deaktivieren</b> .

## Audit-Daten

Wenn Sie eine API direkt ausführen oder die UI verwenden, um den API-Aufruf einer der extern offengelegten APIs des BlueXP Backup- und Recovery-Services für Applikationen zu machen, Angaben zu der Anforderung wie Header, Rolle, Anforderungskörper, Außerdem werden API-Informationen in der BlueXP Zeitachse protokolliert und die Audit-Einträge bleiben dauerhaft im Zeitplan. 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.

BlueXP Backup und Recovery für Applikationen protokollieren die Einträge wie Host-IP, Anfragekörper, Vorgangsname, der ausgelöst hat, einige Header, Und dem 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.

### Schritte

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. Weitere Informationen finden Sie unter [Aktualisieren Sie die Verbindungsdetails](#).

## Klon löschen

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

### Schritte

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 Verbindungsdetails

Sie sollten einen neuen Connector bereitstellen, wenn der Connector, der bei der Registrierung des Anwendungshosts verwendet wurde, nicht mehr existiert oder beschädigt ist. 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.

Führen Sie nach der Aktualisierung der Connector-Details für Oracle- oder SAP HANA-Hosts die folgenden Schritte aus, um sicherzustellen, dass die Connector-Details erfolgreich aktualisiert wurden.

### Schritte

1. Melden Sie sich bei der BlueXP Connector VM an und führen Sie folgende Schritte durch:
  - a. 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
```
  - b. 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
```
  - c. 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.
2. Melden Sie sich beim Plug-in-Host an und führen Sie die folgenden Schritte aus:
  - a. 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
```
  - b. SPL neu starten: `systemctl restart spl`
  - c. Führen Sie einen der folgenden Schritte aus:

Wenn Sie dabei sind...	Tun Sie das...
Oracle-Datenbank-Host	<ul style="list-style-type: none"> <li>i. Stellen Sie sicher, dass alle <a href="#">"Voraussetzungen"</a> Werden erfüllt.</li> <li>ii. Klicken Sie auf <b>Sicherung und Wiederherstellung &gt; Anwendungen</b></li> <li>iii. Klicken Sie Auf <b>...</b> Entsprechend der Anwendung und klicken Sie auf <b>Details anzeigen</b>.</li> <li>iv. Ändern Sie <b>Connector-ID</b>.</li> </ul>
SAP HANA Datenbank-Host	<ul style="list-style-type: none"> <li>i. Stellen Sie sicher, dass alle <a href="#">"Voraussetzungen"</a> Werden erfüllt.</li> <li>ii. Führen Sie den folgenden Befehl aus:</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>curl --location --request PATCH 'https://snapcenter.cloudmanager .cloud.netapp.com/api/saphana/ho sts/connector/update' \ --header 'x-account-id: &lt;CM account-id&gt;' \ --header 'Authorization: Bearer token' \ --header 'Content-Type: application/json' \ --data-raw '{ "old_connector_id": "Old connector id that no longer exists", "new_connector_id": "New connector Id"}</pre> </div> <p>Die Verbindungsdetails werden erfolgreich aktualisiert, wenn auf allen Hosts der SnapCenter-Plug-in für SAP HANA-Dienst installiert und ausgeführt wird und alle über den neuen Connector erreichbar sind.</p>

## Konfigurieren Sie das Zertifikat der Zertifizierungsstelle

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

## Konfigurieren Sie ein CA-signiertes Zertifikat für BlueXP Connector

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.

## Schritte

1. Führen Sie die folgenden Schritte auf dem Connector aus, um das CA-Zertifikat als Clientzertifikat zu verwenden, wenn der Connector eine Verbindung mit dem Plug-in herstellt.

- a. Melden Sie sich bei Connector an.
- b. Führen Sie den folgenden Befehl aus, um den `<base_mount_path>` zu erhalten:  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```
- c. Löschen Sie alle vorhandenen Dateien unter `<base_mount_path>/Client/Certificate` im Connector.
- d. Kopieren Sie das CA-signierte Zertifikat und die Schlüsseldatei in das `<base_mount_path>/Client/Certificate` im Connector.

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

- e. Erstellen Sie das PKCS12-Format des Zertifikats mit dem Namen Certificate.p12 und behalten Sie `<base_mount_path>/Client/Certificate`.

Beispiel: `openssl pkcs12 -inkey key.pem -in Certificate.pem -Export -out Certificate.p12`

2. Führen Sie die folgenden Schritte auf dem Plug-in-Host durch, um das vom Connector gesendete Zertifikat zu validieren.

- a. Melden Sie sich beim Plug-in-Host an.
- b. Kopieren Sie Certificate.pem und Zertifikate für alle zwischengeschalteten CA und die Stammzertifizierungsstelle vom Connector auf den Plug-in-Host unter `/var/opt/snapcenter/spl/etc/`.



Das Format der Zwischenzertifizierungsstelle und des Stammzertifizierungsstellenzertifikats sollte im crt-Format vorliegen.

- c. 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
```
- d. Importieren Sie die Stammzertifizierungsstelle und die Zwischenzertifikate.  

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



Das Certificate.crt bezieht sich auf die Zertifikate der Root-CA sowie der Zwischenzertifizierungsstelle.

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

## Konfigurieren Sie das CA-signierte Zertifikat für das Plug-in

Das CA-Zertifikat sollte denselben Namen haben wie in Cloud Backup für den Plug-in-Host registriert.

## Schritte

1. Führen Sie die folgenden Schritte auf dem Plug-in-Host durch, um das Plug-in mithilfe des CA-Zertifikats zu hosten.

- a. Navigieren Sie zu dem Ordner, der den Keystore `/var/opt/snapcenter/spl/etc` der SPL enthält.
- b. Erstellen Sie das PKCS12-Format des Zertifikats, das sowohl ein Zertifikat als auch einen Schlüssel mit dem Alias `splkeystore` hat.

Das Zertifikat.pem sollte die gesamte Kette der Zertifikate wie Zwischenzertifikat und Root CA haben.

Beispiel: `openssl pkcs12 -inkey key.pem -in Certificate.pem -Export -out Certificate.p12 -Name splkeystore`

- a. Fügen Sie das im obigen Schritt erstellte CA-Zertifikat hinzu.  

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

- b. Überprüfen Sie die Zertifikate.  

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

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

2. Führen Sie die folgenden Schritte am Anschluss aus, damit der Connector das Zertifikat des Plug-ins überprüfen kann.

- a. Melden Sie sich beim Connector als nicht-Root-Benutzer an.
- b. Führen Sie den folgenden Befehl aus, um den `<base_mount_path>` zu erhalten:  

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs  
sudo docker volume inspect | grep Mountpoint
```
- c. Kopieren Sie die Stammzertifizierungsstelle und die zwischengespeicherten CA-Dateien unter das Serververzeichnis.  

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

Die CA-Dateien sollten im pem-Format vorliegen.

- d. 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
```
- e. Starten Sie den `Cloud-Manager_scs_Cloud-Container` neu.  

```
sudo docker restart cloudmanager_scs_cloud
```

## Zugriff auf REST-APIs

Die REST-APIs zum Schutz der Applikationen in der Cloud sind verfügbar unter:  
<https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/>.

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 © 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, 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.