



Backup und Restore von Applikationsdaten

Cloud Backup

NetApp
December 15, 2022

This PDF was generated from <https://docs.netapp.com/de-de/cloud-manager-backup-restore/aws/concept-protect-app-data-to-cloud.html> on December 15, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

- Backup und Restore von Applikationsdaten. 1
 - Backup und Restore von On-Premises-Applikationsdaten 1
 - Backup und Restore von Cloud-nativen Applikationsdaten 14

Backup und Restore von Applikationsdaten

Backup und Restore von On-Premises-Applikationsdaten

Sichern Sie Ihre lokalen Applikationsdaten

Sie können Cloud Backup für Applikationen in BlueXP (früher Cloud Manager) und On-Premises-SnapCenter integrieren und so die applikationskonsistenten Snapshots aus lokalen ONTAP in die Cloud sichern. Bei Bedarf können Sie die Daten aus der Cloud auf lokalen SnapCenter Server wiederherstellen.

Sie können Backups von Oracle, Microsoft SQL und SAP HANA Applikationsdaten von lokalen ONTAP Systemen auf Amazon Web Services, Microsoft Azure, Google Cloud Platform und StorageGRID erstellen.



Sie sollten die SnapCenter-Software 4.6 oder höher verwenden.

Weitere Informationen zu Cloud-Backup für Applikationen finden Sie unter:

- ["Applikationsorientiertes Backup mit Cloud Backup und SnapCenter"](#)
- ["Podcast zum Thema Cloud Backup für Applikationen"](#)

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Applikationsdaten in Cloud-Services beginnen.

- ONTAP 9.8 oder höher
- BlueXP 3.9
- SnapCenter Server 4.6 oder höher Sie sollten SnapCenter Server 4.7 verwenden, wenn Sie die folgenden Funktionen nutzen möchten:
 - Sichern von Backups vor Ort aus sekundärem Storage
 - Schutz von SAP HANA Applikationen
 - Sichern Sie Oracle und SQL Applikationen auf VMware Umgebung
 - Mount-Backups
 - Backups deaktivieren
 - SnapCenter-Server nicht registrieren
- Mindestens ein Backup pro Applikation sollte auf dem SnapCenter-Server verfügbar sein
- Mindestens eine Tages-, Wochen- oder Monatsrichtlinie in SnapCenter ohne Etikett oder dieselbe Bezeichnung wie die der Cloud Backup for Applications-Richtlinie in BlueXP.



Cloud Backup für Applikationen unterstützt keinen Schutz von Applikationen, die sich auf SVMs befinden, die mit FQDN oder IP-Adresse hinzugefügt wurden.

Die folgende Abbildung zeigt die einzelnen Komponenten beim Backup in der Cloud und die Verbindungen, die zwischen ihnen vorbereitet werden müssen:



Die folgende Abbildung zeigt jede Komponente beim Backup in StorageGRID und die Verbindungen, die zwischen ihnen vorbereitet werden müssen:



Registrieren Sie den SnapCenter-Server

Nur ein Benutzer mit SnapCenterAdmin-Rolle kann den Host registrieren, auf dem SnapCenter Server 4.6 oder höher ausgeführt wird. Sie können mehrere SnapCenter-Server-Hosts registrieren.

Schritte

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

2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Server**.
3. Klicken Sie auf **SnapCenter-Server registrieren**.
4. Geben Sie folgende Details an:
 - a. Geben Sie im Feld SnapCenter-Server den FQDN oder die IP-Adresse des SnapCenter-Serverhosts an.
 - b. Geben Sie im Feld Port die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.

Sie sollten sicherstellen, dass der Port offen ist, damit die Kommunikation zwischen SnapCenter Server und Cloud Backup for Applications erfolgen kann.
 - c. Geben Sie im Feld Tags einen Standortnamen, einen Städtenamen oder einen benutzerdefinierten Namen an, mit dem der SnapCenter-Server markiert werden soll.

Die Tags sind durch Komma getrennt.
 - d. Geben Sie im Feld Benutzername und Kennwort die Anmeldeinformationen des Benutzers mit der Rolle SnapCenterAdmin an.
5. Klicken Sie Auf **Registrieren**.

Nach Ihrer Beendigung

Klicken Sie auf **Backup & Restore > Anwendungen**, um alle Anwendungen anzuzeigen, die mit dem registrierten SnapCenter Server-Host geschützt sind.

Standardmäßig werden die Anwendungen automatisch jeden Tag um Mitternacht erkannt. Sie können den Zeitplan so konfigurieren, dass die Anwendungen ermittelt werden.



Bei SQL Server-Datenbanken zeigt die Spalte Anwendungsname den Namen im Format *Application_Name (Instanzname)* an.

Folgende Applikationen und ihre Konfigurationen werden unterstützt:

- Oracle Datenbank:
 - Vollständige Backups (Daten + Protokoll) werden mit mindestens einem täglichen, wöchentlichen oder monatlichen Zeitplan erstellt
 - SAN, NFS, VMDK-SAN, VMDK-NFS UND RDM
- Microsoft SQL Server Datenbank:
 - Standalone, Failover-Cluster-Instanzen und Verfügbarkeitsgruppen
 - Vollständige Backups, die mit mindestens einem täglichen, wöchentlichen oder monatlichen Zeitplan erstellt wurden
 - SAN, VMDK-SAN, VMDK-NFS UND RDM
- SAP HANA Datenbank:
 - Einzelner Container 1.x
 - Mehrere Datenbank-Container 2.x
 - HANA System Replication (HSR)

Sie sollten mindestens ein Backup am primären und sekundären Standort haben. Sie können entscheiden, einen pro-aktiven Ausfall oder einen verzögerten Failover auf das sekundäre zu tun.

- Nicht-Daten-Volumes (NDV) Ressourcen wie HANA-Binärdateien, HANA Archiv-Log-Volume, HANA Shared Volume usw.

Die folgenden Datenbanken werden nicht angezeigt:

- Datenbanken ohne Backups
- Datenbanken mit nur bedarfsgerechter oder stündlicher Richtlinie
- Oracle-Datenbanken auf NVMe

Erstellen einer Richtlinie für das Backup von Applikationen

Sie können entweder eine der vordefinierten Richtlinien verwenden oder eine individuelle Richtlinie für das Backup der Applikationsdaten in der Cloud erstellen. Sie können Richtlinien erstellen, wenn Sie die vordefinierten Richtlinien nicht bearbeiten möchten.

Die vordefinierten Richtlinien sind:

Name Der Richtlinie	Etikett	Aufbewahrungswert
1 Jahr tägliche LTR	Täglich	366
5 Jahre tägliche LTR	Täglich	1830
7 Jahre wöchentlicher LTR	Wöchentlich	370
10 Jahre Monatliche LTR	Monatlich	120

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Klicken Sie im Dropdown-Menü Einstellungen auf **Richtlinien > Richtlinien erstellen**.
3. Geben Sie im Abschnitt Richtliniendetails den Richtliniennamen an.
4. Wählen Sie im Abschnitt Aufbewahrung einen Aufbewahrungstyp aus und geben Sie die Anzahl der zu behaltenden Backups an.
5. Wählen Sie Primary oder Secondary als Backup-Speicherquelle aus.
6. (Optional) Wenn Sie Backups nach einer bestimmten Anzahl von Tagen zur Kostenoptimierung vom Objektspeicher in den Archivspeicher verschieben möchten, aktivieren Sie das Kontrollkästchen **Tiering Backups in Archive**.

Sie können Backups nur dann von einem Objektspeicher in einen Archiv-Storage verschieben, wenn Sie ONTAP 9.10.1 oder höher und Amazon Web Services oder Azure als Cloud-Provider verwenden. Sie sollten die Zugriffsebene für den Archiv für jeden Cloud-Provider konfigurieren.

7. Klicken Sie Auf **Erstellen**.

Sie können die angepassten Richtlinien bearbeiten, kopieren und löschen.



Eine Richtlinie, die einer Anwendung zugeordnet ist, kann nicht bearbeitet oder gelöscht werden.

Sichern Sie On-Premises-Applikationsdaten in Amazon Web Services

Durch die Integration von Cloud Backup für Applikationen in BlueXP und On-Premises SnapCenter können Sie Backups der Applikationsdaten von ONTAP in Amazon Web Services erstellen.

Sie können eine oder mehrere Applikationen gleichzeitig mit einer einzigen Richtlinie in der Cloud sichern.



Sie können nur eine Anwendung gleichzeitig schützen, wenn Sie die BlueXP-GUI verwenden. Wenn SIE JEDOCH REST-APIs verwenden, können Sie mehrere Applikationen gleichzeitig sichern.

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Klicken Sie Auf **...** Entsprechend der Anwendung und klicken Sie auf **Backup aktivieren**.
3. Wählen Sie auf der Seite Richtlinie zuweisen die Richtlinie aus und klicken Sie auf **Weiter**.
4. Fügen Sie die Arbeitsumgebung hinzu.

Konfigurieren Sie den ONTAP-Cluster, der die SVM hostet, auf dem die Applikation ausgeführt wird. Nach dem Hinzufügen der Arbeitsumgebung für eine der Applikationen kann sie für alle anderen Applikationen in demselben ONTAP Cluster wiederverwendet werden.

- a. Wählen Sie die SVM aus und klicken Sie auf **Arbeitsumgebung hinzufügen**.
- b. Im Assistenten „Arbeitsumgebung hinzufügen“:
 - i. Geben Sie die IP-Adresse des ONTAP-Clusters an.
 - ii. Geben Sie die Admin-Anmeldedaten an.

Cloud Backup für Applikationen unterstützt nur Cluster-Administratoren.

- c. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.
5. Wählen Sie als Cloud-Provider * Amazon Web Services* aus.
 - a. Geben Sie den AWS Account an.
 - b. Geben Sie im Feld AWS Access Key den Schlüssel an.
 - c. Geben Sie im Feld AWS Secret Key das Passwort an.
 - d. Wählen Sie den Bereich aus, in dem Sie die Backups erstellen möchten.
 - e. Geben Sie den IP-Speicherplatz an.
 - f. Wählen Sie die Archivebene aus.

Es wird empfohlen, die Archivebene einzustellen, da dies eine einmalige Aktivität ist und Sie sie später nicht einrichten können.

6. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

Sichern Sie On-Premises-Applikationsdaten in StorageGRID

Durch die Integration von Cloud Backup für Applikationen in BlueXP und On-Premises-SnapCenter können Sie ein Backup der Applikationsdaten von ONTAP in StorageGRID erstellen.

Sie können eine oder mehrere Applikationen gleichzeitig mit einer einzigen Richtlinie in StorageGRID sichern.



Sie können nur eine Anwendung gleichzeitig schützen, wenn Sie die BlueXP-GUI verwenden. Wenn SIE JEDOC REST-APIs verwenden, können Sie mehrere Applikationen gleichzeitig sichern.

Was Sie brauchen

Beim Daten-Backup in StorageGRID muss am Standort ein Connector verfügbar sein. Sie müssen entweder einen neuen Konnektor installieren oder sicherstellen, dass sich der aktuell ausgewählte Connector auf der Prem befindet. Der Connector kann auf einer Website mit oder ohne Internetzugang installiert werden.

Weitere Informationen finden Sie unter ["Anschlüsse für StorageGRID erstellen"](#).

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Klicken Sie Auf **...** Entsprechend der Anwendung und klicken Sie auf **Backup aktivieren**.
3. Wählen Sie auf der Seite Richtlinie zuweisen die Richtlinie aus und klicken Sie auf **Weiter**.
4. Fügen Sie die Arbeitsumgebung hinzu.

Konfigurieren Sie den ONTAP-Cluster, der die SVM hostet, auf dem die Applikation ausgeführt wird. Nach dem Hinzufügen der Arbeitsumgebung für eine der Applikationen kann sie für alle anderen Applikationen in demselben ONTAP Cluster wiederverwendet werden.

- a. Wählen Sie die SVM aus und klicken Sie auf **Arbeitsumgebung hinzufügen**.
- b. Im Assistenten „Arbeitsumgebung hinzufügen“:
 - i. Geben Sie die IP-Adresse des ONTAP-Clusters an.
 - ii. Geben Sie die Admin-Anmeldedaten an.

Cloud Backup für Applikationen unterstützt nur Cluster-Administratoren.

- c. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.

5. Wählen Sie **StorageGRID**.

- a. Geben Sie den FQDN des StorageGRID-Servers und den Port an, auf dem der StorageGRID-Server ausgeführt wird.

Geben Sie die Details im Format FQDN:PORT ein.

- b. Geben Sie im Feld Zugriffsschlüssel den Schlüssel an.
- c. Geben Sie im Feld Geheimer Schlüssel das Passwort an.
- d. Geben Sie den IP-Speicherplatz an.

6. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

Management der Sicherung von Applikationen

Sie können den Schutz von Anwendungen verwalten, indem Sie verschiedene Vorgänge über die Benutzeroberfläche von BlueXP ausführen.

Anzeigen von Richtlinien

Sie können alle Richtlinien anzeigen. Wenn Sie die Details anzeigen, werden für jede dieser Richtlinien alle zugehörigen Anwendungen aufgelistet.

1. Klicken Sie auf **Backup und Recovery > Anwendungen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **Richtlinien**.
3. Klicken Sie auf **Details anzeigen** entsprechend der Richtlinie, deren Details Sie anzeigen möchten.

Die zugehörigen Anwendungen werden aufgelistet.



Eine Richtlinie, die einer Anwendung zugeordnet ist, kann nicht bearbeitet oder gelöscht werden.

Sie können sich auch SnapCenter-Richtlinien für die Cloud anzeigen lassen, indem Sie auf ausführen `Get-SmResources SnapCenter Cmdlet`: Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von `Get-Help Command_Name` abgerufen werden. Alternativ können Sie auch die verweisen "[SnapCenter Software Cmdlet Referenzhandbuch](#)".

Anzeigen von Backups in der Cloud

Sie können die Backups in der Cloud in der BlueXP UI anzeigen.

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



Die für die Auflistung der Backups benötigte Zeit hängt von dem standardmäßigen Replizierungsplan von ONTAP (maximal 1 Stunde) und BlueXP (maximal 6 Stunden) ab.

- Bei Oracle Datenbanken werden sowohl Daten- als auch Log-Backups, SCN-Nummer für jedes Backup, Enddatum für jedes Backup aufgeführt. Sie können nur das Daten-Backup auswählen und die Datenbank auf dem lokalen SnapCenter Server wiederherstellen.
- Bei Microsoft SQL Server-Datenbanken werden nur die vollständigen Backups und das Enddatum für jedes Backup aufgeführt. Sie können das Backup auswählen und die Datenbank auf dem lokalen SnapCenter Server wiederherstellen.
- Bei Microsoft SQL Server werden Backups nicht nur in den Datenbanken aufgeführt, unter denen diese Instanz steht.
- Bei SAP HANA Datenbanken werden nur die Daten-Backups und das Enddatum für jedes Backup aufgeführt. Sie können das Backup auswählen und Mount-Vorgang durchführen.



Die vor Aktivierung der Cloud-Sicherung erstellten Backups werden nicht zur Wiederherstellung aufgeführt.

Sie können diese Backups auch anzeigen, indem Sie die ausführen `Get-SmBackup SnapCenter Cmdlet`: Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von `Get-Help Command_Name` abgerufen werden. Alternativ können Sie auch die verweisen "[SnapCenter Software Cmdlet Referenzhandbuch](#)".

Datenbanklayout ändern

Wenn Volumes zur Datenbank hinzugefügt werden, kennzeichnet SnapCenter Server die Snapshots auf den neuen Volumes automatisch gemäß Richtlinie und Zeitplan. Diese neuen Volumes verfügen nicht über den Endpunkt des Objektspeichers, und Sie sollten die Aktualisierung durch die folgenden Schritte durchführen:

1. Klicken Sie auf **Backup und Recovery > Anwendungen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Server**.
3. Klicken Sie Auf **...** Entsprechend dem SnapCenter-Server, der die Anwendung hostet, und klicken Sie auf **Aktualisieren**.

Die neuen Volumes werden ermittelt.

4. Klicken Sie Auf **...** Entsprechend der Anwendung und klicken Sie auf **Refresh Protection**, um den Cloud-Schutz für das neue Volume zu aktivieren.

Wenn ein Storage-Volume nach der Konfiguration des Cloud-Service aus der Applikation entfernt wird, kennzeichnet SnapCenter Server für neue Backups nur die Snapshots, auf denen sich die Anwendung befindet. Wenn das entfernte Volume von anderen Anwendungen nicht verwendet wird, sollten Sie die Objektspeicherbeziehung manuell löschen. Wenn Sie den Anwendungsbestand aktualisieren, enthält dieser das aktuelle Speicherlayout der Anwendung.

Änderung der Richtlinie oder Ressourcengruppe

Wenn die SnapCenter-Richtlinie oder Ressourcengruppe geändert wird, müssen Sie den Schutz aktualisieren.

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

SnapCenter-Server nicht registrieren

1. Klicken Sie auf **Backup und Recovery > Anwendungen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Server**.
3. Klicken Sie Auf **...** Entsprechend dem SnapCenter-Server und klicken Sie auf **Registrierung aufheben**.

Überwachen Von Jobs

Für alle Cloud-Backup-Vorgänge werden Jobs erstellt. Sie können alle Jobs und alle Unteraufgaben, die als Teil jeder Aufgabe ausgeführt werden, überwachen.

1. Klicken Sie auf **Sicherung und Wiederherstellung > Jobüberwachung**.

Wenn Sie einen Vorgang starten, wird ein Fenster angezeigt, in dem Sie angeben, dass der Job gestartet wird. Sie können auf den Link klicken, um den Job zu überwachen.

2. Klicken Sie auf die primäre Aufgabe, um die Unteraufgaben und den Status der einzelnen Unteraufgaben anzuzeigen.

Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest

Wenn Sie ein Backup wiederherstellen oder mounten möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz festlegen.

Schritte

1. Klicken Sie in BlueXP UI auf **Storage > Leinwand > Meine Arbeitsumgebung > Arbeitsumgebung hinzufügen**.
2. Geben Sie die Details der primären Arbeitsumgebung an und klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Backup und Recovery > Volumes**.
4. Klicken Sie Auf **...** Entsprechend einem der Volumes und klicken Sie auf **Details**.
5. Klicken Sie Auf **...** Entsprechend der Sicherung und klicken Sie auf **Wiederherstellen**.
6. Wählen Sie im Assistenten die neu hinzugefügte primäre Arbeitsumgebung als Ziel aus.
7. Geben Sie den IP-Speicherplatz an.

Konfigurieren Sie CA-Zertifikate

Wenn Sie CA-Zertifikate haben, sollten Sie die Stammzertifizierungszertifikate manuell auf den Verbindungscomputer kopieren.

Wenn Sie jedoch keine CA-Zertifikate besitzen, können Sie ohne die Konfiguration von CA-Zertifikaten fortfahren.

Schritte

1. Kopieren Sie das Zertifikat in das Volume, auf das über den Docker-Agent zugegriffen werden kann.

```
° cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir  
  sc_certs  
° chmod 777 sc_certs
```

2. Kopieren Sie die RootCA-Zertifikatdateien in den obigen Ordner auf dem Verbindungscomputer.

```
cp <path on connector>/<filename>  
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
```

3. Kopieren Sie die CRL-Datei in das Volume, auf das über den Docker-Agent zugegriffen werden kann.

```
° cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl  
° chmod 777 sc_crl
```

4. Kopieren Sie die CRL-Dateien in den obigen Ordner auf dem Verbindungscomputer.

```
cp <path on connector>/<filename>  
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_crl
```

5. Nachdem Sie die Zertifikate und CRL-Dateien kopiert haben, starten Sie den Service Cloud Backup for Apps neu.

```
° sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation:  
true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-
```

```
agent/config/config.yml
```

```
° sudo docker restart cloudmanager_snapcenter
```

Wiederherstellung von Applikationsdaten

Oracle Datenbank wiederherstellen

Die Oracle-Datenbank kann nur auf demselben SnapCenter-Serverhost, derselben SVM oder demselben Datenbank-Host wiederhergestellt werden. Bei einer RAC-Datenbank werden die Daten auf dem On-Premises-Node, an dem das Backup erstellt wurde, wiederhergestellt.



Die Wiederherstellung von sekundären Backups über primären Server wird unterstützt.

Es wird nur eine vollständige Datenbank mit Wiederherstellung der Kontrolldatei unterstützt. Wenn die Archivprotokolle nicht im AFS vorhanden sind, müssen Sie den Speicherort angeben, der die für die Wiederherstellung erforderlichen Archivprotokolle enthält.



Single File Restore (SFR) wird nicht unterstützt.

Was Sie brauchen

Wenn Sie ein Backup wiederherstellen möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz festlegen. Weitere Informationen finden Sie unter ["Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest"](#).

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** aus und wählen Sie aus der Dropdown-Liste **Oracle** aus.
3. Klicken Sie auf **Details anzeigen**, die der Datenbank entsprechen, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
4. Führen Sie auf der Seite Wiederherstellungstyp die folgenden Aktionen durch:
 - a. Wählen Sie **Datenbankstatus** aus, wenn Sie den Status der Datenbank in den Zustand ändern möchten, der für die Wiederherstellung und Wiederherstellung erforderlich ist.

Die verschiedenen Status einer Datenbank von höher bis niedriger sind offen, montiert, gestartet und heruntergefahren. Sie müssen dieses Kontrollkästchen aktivieren, wenn sich die Datenbank in einem höheren Zustand befindet, der Status jedoch in einen niedrigeren Zustand geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen. Wenn sich die Datenbank in einem niedrigeren Zustand befindet, aber der Status in einen höheren Zustand geändert werden muss, um den Wiederherstellungsvorgang auszuführen, wird der Datenbankstatus automatisch geändert, auch wenn Sie das Kontrollkästchen nicht aktivieren.

Wenn sich eine Datenbank im Status „offen“ befindet und die Datenbank für die Wiederherstellung im Status „angehängt“ befinden muss, wird der Datenbankzustand nur geändert, wenn Sie dieses Kontrollkästchen aktivieren.

- a. Wählen Sie **Kontrolldateien** aus, wenn Sie Steuerdatei zusammen mit der vollständigen Datenbank wiederherstellen möchten.
 - b. Wenn sich der Snapshot im Archiv-Speicher befindet, geben Sie die Priorität an, um Ihre Daten aus dem Archiv-Speicher wiederherzustellen.
5. Führen Sie auf der Seite „Recovery Scope“ die folgenden Schritte aus:
- a. Geben Sie den Recovery-Umfang an.

Sie suchen...	Tun Sie das...
Möchten Sie die letzte Transaktion wiederherstellen	Wählen Sie Alle Protokolle .
Wiederherstellen einer bestimmten Systemänderungsnummer (SCN)	Wählen Sie bis SCN (Systemänderungsnummer) .
Möchten Sie Daten zu einer bestimmten Zeit wiederherstellen	Wählen Sie Datum und Uhrzeit . Sie müssen Datum und Uhrzeit der Zeitzone des Datenbank-Hosts angeben.
Möchten Sie nicht wiederherstellen	Wählen Sie Keine Wiederherstellung .
Soll beliebige externe Archiv-Log-Speicherorte angeben	Wenn die Archivprotokolle nicht im AFS vorhanden sind, müssen Sie den Speicherort angeben, der die für die Wiederherstellung erforderlichen Archivprotokolle enthält.

- b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

In einem RAC-Setup wird nach der Wiederherstellung nur die RAC-Instanz geöffnet, die für die Wiederherstellung verwendet wird.

6. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

SQL Server Datenbank wiederherstellen

Sie können eine SQL Server-Datenbank auf demselben Host oder auf dem alternativen Host wiederherstellen. Das Recovery von Protokoll-Backups und das erneute Seeding von Verfügbarkeitsgruppen wird nicht unterstützt.



WICHTIG: Die Wiederherstellung von sekundären Backups über Primärsystem wird unterstützt.



Single File Restore (SFR) wird nicht unterstützt.


Was Sie brauchen

Wenn Sie ein Backup wiederherstellen möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz

festlegen. Weitere Informationen finden Sie unter ["Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest"](#).

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** aus und wählen Sie aus dem Dropdown-Menü **SQL** aus.
3. Klicken Sie auf **Details anzeigen**, um alle verfügbaren Backups anzuzeigen.
4. Wählen Sie das Backup aus und klicken Sie auf **Wiederherstellen**.
5. Wählen Sie den Speicherort aus, an dem die Datenbankdateien wiederhergestellt werden sollen.

Option	Beschreibung
Stellen Sie die Datenbank auf demselben Host wieder her, auf dem das Backup erstellt wurde	Wählen Sie diese Option aus, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Backups erstellt werden.
Wiederherstellung der Datenbank auf einem alternativen Host	<p>Wählen Sie diese Option aus, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem Backups erstellt werden.</p> <p>Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen ein (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an.</p> <div><p>Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateierweiterung der ursprünglichen Datenbankdatei identisch sein.</p></div> <p>Wenn die Option Datenbank auf alternativen Host wiederherstellen nicht auf der Seite „Bereich wiederherstellen“ angezeigt wird, löschen Sie den Browser-Cache.</p>

6. Wenn sich der Snapshot im Archiv-Speicher befindet, geben Sie die Priorität an, um Ihre Daten aus dem Archiv-Speicher wiederherzustellen.
7. Wählen Sie auf der Seite **Pre Restore Options** eine der folgenden Optionen aus:
 - Wählen Sie **Überschreiben Sie die Datenbank mit demselben Namen während der Wiederherstellung** aus, um die Datenbank mit dem gleichen Namen wiederherzustellen.
 - Wählen Sie **SQL-Datenbankreplikationseinstellungen beibehalten** aus, um die Datenbank wiederherzustellen und die vorhandenen Replikationseinstellungen beizubehalten.
8. Wählen Sie auf der Seite **Optionen zur Wiederherstellung nach der Wiederherstellung** den Datenbankstatus für die Wiederherstellung weiterer Transaktionsprotokolle aus, eine der folgenden Optionen aus:

- Wählen Sie **Operational, aber nicht verfügbar** aus, wenn Sie jetzt alle notwendigen Backups wiederherstellen.

Dies ist das Standardverhalten, das die Datenbank durch ein Rollback der nicht gesicherten Transaktionen einsatzbereit macht. Sie können erst dann weitere Transaktionsprotokolle wiederherstellen, wenn Sie ein Backup erstellen.

- Wählen Sie * nicht betriebsbereit, aber verfügbar* aus, um die Datenbank nicht betriebsbereit zu lassen, ohne die nicht gesicherten Transaktionen zurückzurollen.

Zusätzliche Transaktions-Logs können wiederhergestellt werden. Sie können die Datenbank erst verwenden, wenn sie wiederhergestellt ist.

- Wählen Sie **schreibgeschützter Modus und verfügbar**, um die Datenbank im schreibgeschützten Modus zu belassen.

Mit dieser Option werden nicht gesicherte Transaktionen rückgängig gemacht, die nicht rückgängig gemachte Aktionen werden jedoch in einer Standby-Datei gespeichert, sodass Recovery-Effekte rückgängig gemacht werden können.

Wenn die Option „Verzeichnis aufheben“ aktiviert ist, werden mehr Transaktionsprotokolle wiederhergestellt. Wenn der Wiederherstellungsvorgang für das Transaktionsprotokoll nicht erfolgreich ist, können die Änderungen zurückgesetzt werden. Die SQL Server-Dokumentation enthält weitere Informationen.

9. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

Binden Sie Backups von Applikationen ein

SnapCenter unterstützt die Wiederherstellung von Oracle und HANA Backups auf einem alternativen Host nicht. Damit können Sie mit Cloud Backup für Anwendungen die Oracle- und HANA-Backups auf den angegebenen Host mounten.

Was Sie brauchen

Wenn Sie ein Backup mounten möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz festlegen. Weitere Informationen finden Sie unter ["Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest"](#).

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz > Sicherung und Wiederherstellung > Anwendungen**.
2. Wählen Sie im Feld Filtern nach die Option **Typ** aus und wählen Sie im Dropdown-Menü die Option **SAP HANA** oder **Oracle** aus.
3. Klicken Sie Auf **...** Entsprechend der geschützten Anwendung und wählen Sie **Details anzeigen**.
4. Klicken Sie Auf **...** Entsprechend der Sicherung und wählen Sie **Mount**.
 - a. Geben Sie eine der folgenden Optionen an:
 - i. Geben Sie in der NAS-Umgebung den FQDN oder die IP-Adresse des Hosts an, auf den aus dem Objektspeicher wiederhergestellte alternative Volumes exportiert werden sollen.
 - ii. Geben Sie in der SAN-Umgebung die Initiatoren des Hosts an, denen aus dem Objektspeicher wiederhergestellte LUNs eines alternativen Volumes zugeordnet werden sollen.

- b. Geben Sie das Suffix an, das dem alternativen Volume-Namen hinzugefügt wird.
- c. Wenn sich der Snapshot im Archiv-Storage befindet, geben Sie die Priorität an, um Ihre Daten aus dem Archiv-Storage abzurufen.
- d. Klicken Sie Auf **Mount**.

Dieser Vorgang bindet nur den Storage auf dem angegebenen Host ein. Sie sollten das Dateisystem manuell mounten und die Datenbank aufrufen. Nach Nutzung des alternativen Volumes kann der Storage-Administrator das Volume aus dem ONTAP-Cluster löschen.

Weitere Informationen zum Einrichten der SAP HANA-Datenbank finden Sie unter: ["TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"](#).

Backup und Restore von Cloud-nativen Applikationsdaten

Sichern Sie Ihre Daten aus Cloud-nativen Applikationen

Cloud Backup für Applikationen ist ein SaaS-basierter Service mit Datensicherungsfunktionen für Applikationen, die auf NetApp Cloud Storage ausgeführt werden. Cloud Backup für Applikationen innerhalb von NetApp BlueXP (früher Cloud Manager) bietet effiziente, applikationskonsistente, richtlinienbasierte Backups und Restores von Oracle Datenbanken auf Amazon FSX für NetApp ONTAP.

Der Netapp Architektur Sind

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

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

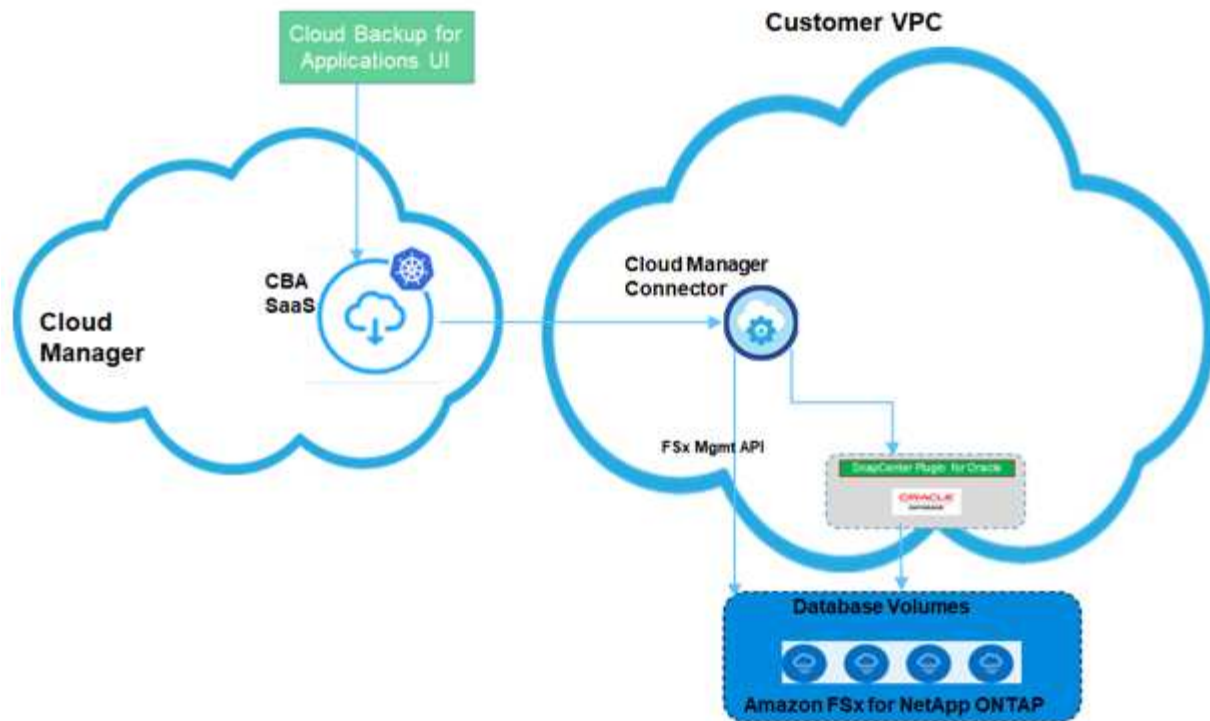
Die Datensicherungs-Workflows werden für Applikationen auf NetApp Cloud Storage orchestriert.

- Die Benutzeroberfläche von Cloud Backup für Applikationen ist in die Benutzeroberfläche von BlueXP integriert.

Die Benutzeroberfläche von Cloud Backup für Applikationen bietet diverse Storage- und Datenmanagement-Funktionen.

- BlueXP Connector ist eine Komponente von BlueXP, die in Ihrem Cloud-Netzwerk ausgeführt wird und mit Amazon FSX Storage-Dateisystemen und dem SnapCenter-Plug-in für Oracle interagiert, die auf Oracle-Datenbank-Hosts ausgeführt werden.
- Das SnapCenter Plug-in für Oracle ist eine Komponente, die auf jedem Oracle Datenbank-Host ausgeführt wird und mit den auf dem Host ausgeführten Oracle Datenbanken interagiert, während gleichzeitig Datensicherungsprozesse durchgeführt werden.

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



Für alle von Benutzern initiierten Anfragen kommuniziert die Benutzeroberfläche von Cloud Backup for Applications mit dem SaaS von BlueXP, das bei der Validierung der Anfrageprozesse identisch ist. Wenn die Anforderung einen Workflow wie Backup oder Wiederherstellung ausführen soll, initiiert der SaaS-Service den Workflow und leitet den Anruf an den BlueXP Connector weiter. Der Connector kommuniziert dann mit Amazon FSx für NetApp ONTAP und das SnapCenter Plug-in für Oracle, um die Workflow-Aufgaben auszuführen.

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



Die Infrastruktur von Cloud Backup für Applikationen kann Ausfälle der Verfügbarkeitszone innerhalb einer Region nicht kompensieren. Jetzt werden regionale Ausfälle unterstützt, indem ein Failover auf eine neue Region durchgeführt wird, was mit etwa zwei Stunden Ausfallzeit verbunden ist.

Unterstützte Konfigurationen

- Betriebssystem:
 - RHEL 7.5 oder höher und 8.x
 - L 7.5 oder höher und 8.x
- Storage-System Amazon FSX für ONTAP
- Storage-Layouts: NFS v3 und v4.1 (dNFS wird unterstützt) und iSCSI mit ASM (ASMFD, ASMLib und ASMUdev)
- Applikationen: Oracle Standard und Oracle Enterprise – Standalone (alt und mandantenfähig – CDB und PDB)
- Oracle Versionen: 12cR2, 18c und 19c

Funktionen

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

Sie können verschiedene Planungsfrequenzen wie stündlich, täglich, wöchentlich und monatlich in der Richtlinie festlegen.
- Aufbewahrung von Backups anhand der Richtlinie
- Wiederherstellen der vollständigen Oracle-Datenbank (Datendateien + Kontrolldatei) aus dem angegebenen Backup
- Nur Datendateien wiederherstellen und nur Dateien aus dem angegebenen Backup steuern
- Wiederherstellen der Oracle-Datenbank mit bis SCN, bis zu der Zeit, alle verfügbaren Protokolle und keine Recovery-Optionen
- Überwachung von Backups und anderen Aufgaben
- Anzeigen der Schutzzusammenfassung im Dashboard
- Senden von Benachrichtigungen per E-Mail

Einschränkungen

- Oracle Versionen 11g und 21c werden nicht unterstützt
- Mount-, Klon-, Katalog- und Verifizierungsvorgänge für Backups werden nicht unterstützt
- Bietet keine Unterstützung für Oracle auf RAC und Data Guard
- Backup-Einschränkungen:
 - Bietet keine Unterstützung für Online-Daten oder lediglich für Backup-Protokollierung
 - Keine Unterstützung von Offline-Backups
 - Unterstützt keine Sicherung der Oracle-Datenbank, die sich auf rekursiven Bereitstellungspunkten befindet
 - Unterstützt keine Snapshots von Konsistenzgruppen für Oracle Datenbanken, die sich auf mehreren ASM-Festplattengruppen mit Überschneidungen von FSX Volumes befinden
 - Wenn Ihre Oracle-Datenbanken auf ASM konfiguriert sind, stellen Sie sicher, dass Ihre SVM-Namen für die FSX-Systeme eindeutig sind. Wenn Sie in den FSX-Systemen denselben SVM-Namen haben, werden Backups der auf diesen SVMs befindlichen Oracle Datenbanken nicht unterstützt.
- Einschränkungen bei Wiederherstellungen:
 - Keine Unterstützung für granulare Restores, beispielsweise beim Wiederherstellen von Tabellen und PDBs
 - Unterstützt nur die in-Place-Wiederherstellung von Oracle-Datenbanken unter NAS- und SAN-Layouts
 - Unterstützt nicht die Wiederherstellung von Kontrolldatei nur oder Datendateien + Kontrolldatei von Oracle-Datenbanken auf SAN-Layouts
 - Im SAN-Layout schlägt der Wiederherstellungsvorgang fehl, wenn das SnapCenter Plug-in für Oracle andere fremde Dateien als Oracle-Datendateien auf der ASM-Festplattengruppe findet. Die

Fremddateien können eine oder mehrere der folgenden Typen sein:

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

Aktivieren Sie das Kontrollkästchen in-Place-Wiederherstellung erzwingen, um die fremden Dateien von Typ-Parameter, Passwort und Archivprotokoll zu überschreiben.



Wenn es andere Arten von Fremddateien gibt, schlägt der Wiederherstellungsvorgang fehl und die Datenbank kann nicht wiederhergestellt werden. Wenn Sie andere Arten von Fremddateien haben, sollten Sie sie löschen oder an einen anderen Speicherort verschieben, bevor Sie den Wiederherstellungsvorgang durchführen.

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

Voraussetzungen

Sie sollten Zugriff auf BlueXP haben, ein BlueXP-Konto erstellt, die Arbeitsumgebung und den Connector erstellt und das SnapCenter-Plug-in für Oracle bereitgestellt haben.

Zugriff auf BlueXP

Sollten Sie ["Melden Sie sich bei BlueXP an"](#), Und dann eine ["NetApp Konto"](#).

Erstellung von FSX für ONTAP-Arbeitsumgebung

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

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

Einen Konnektor erstellen

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

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

- Sie sollten denselben Konnektor verwenden, um sowohl FSX-Arbeitsumgebung als auch Oracle-Datenbanken zu verwalten.
- Wenn Sie über die FSX-Arbeitsumgebung und Oracle-Datenbanken in derselben VPC verfügen, können Sie den Connector in derselben VPC implementieren.
- Wenn Sie über die FSX-Arbeitsumgebung und Oracle-Datenbanken in verschiedenen VPCs verfügen:

- Wenn auf FSX NAS-Workloads (NFS) konfiguriert sind, können Sie den Connector auf einem der VPCs erstellen.
- Wenn nur SAN-Workloads konfiguriert sind und keine NAS- (NFS-) Workloads verwendet werden sollen, sollte der Connector in der VPC erstellt werden, über den das FSX-System erstellt wird.



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

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



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

Implementieren Sie das SnapCenter Plug-in für Oracle

Sie sollten das SnapCenter Plug-in für Oracle auf jedem der Oracle Datenbank-Hosts bereitstellen. Je nachdem, ob auf dem Oracle-Host die SSH-Schlüsselauthentifizierung aktiviert ist, können Sie eine der Methoden zur Bereitstellung des Plug-ins befolgen.



Stellen Sie sicher, DASS JAVA 8 auf jedem der Oracle-Datenbank-Hosts installiert ist und die JAVA_HOME-Variable entsprechend eingestellt ist.

Plug-in-Implementierung mit SSH-schlüsselbasierter Authentifizierung

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Host aktiviert ist, können Sie zum Bereitstellen des Plug-ins die folgenden Schritte durchführen. Bevor Sie die Schritte durchführen, stellen Sie sicher, dass die SSH-Verbindung zum Connector aktiviert ist.

1. Melden Sie sich bei der Connector-VM als nicht-Root-Benutzer an.

2. Ermitteln Sie den Mount-Pfad für die Basis.

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

3. Plug-in implementieren

```
sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host
<host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port>
--pluginport <plugin_port> --installdir <install_dir>
```

- Host_Name ist der Name des Oracle-Hosts, und dies ist ein obligatorischer Parameter.
- ssh_Key_file ist SSH-Schlüssel, der für die Verbindung zum Oracle-Host verwendet wird und dies ist ein obligatorischer Parameter.
- User_Name: Benutzer mit SSH-Berechtigungen auf dem Oracle-Host und dies ist ein optionaler Parameter. Der Standardwert ist ec2-user.

- `ssh_Port`: SSH-Port auf dem Oracle-Host und dies ist ein optionaler Parameter. Der Standardwert ist 22
- `Plugin_Port`: Port verwendet vom Plug-in und dies ist ein optionaler Parameter. Der Standardwert ist 8145
- `Install_dir`: Verzeichnis, in dem das Plug-in bereitgestellt wird und dies ein optionaler Parameter ist. Standardwert ist `/opt`.

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

Manuelle Implementierung des Plug-ins

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

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

Backup von Cloud-nativen Applikationsdaten

Erkennen Sie die Anwendungen

Sie sollten die Datenbanken auf dem Host erkennen, um Richtlinien zuzuweisen und Backups zu erstellen.

Was Sie brauchen

- Sie sollten die FSX für die Arbeitsumgebung ONTAP und den Connector erstellt haben.
- Stellen Sie sicher, dass der Connector mit dem FSX für die ONTAP-Arbeitsumgebung und den Oracle-Datenbank-Hosts verbunden ist.
- Stellen Sie sicher, dass der BlueXP-Benutzer über die Rolle „Account Admin“ verfügt.
- Sie sollten das SnapCenter Plug-in für Oracle implementiert haben. "[Weitere Informationen](#) .".

Schritte

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

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

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



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

4. Geben Sie auf der Seite Hostdetails angeben die Details des Oracle-Datenbank-Hosts ein, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass das Plug-in auf dem Host installiert ist, und klicken Sie auf **Entdecken**.
 - Zeigt alle Datenbanken auf dem Host an. Wenn die Betriebssystemauthentifizierung für die Datenbank deaktiviert ist, sollten Sie die Datenbankauthentifizierung konfigurieren, indem Sie auf **Configure** klicken. Weitere Informationen finden Sie unter [Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank](#).
 - Klicken Sie auf **Anwendung verwalten**, wählen Sie **Hinzufügen**, um einen neuen Host hinzuzufügen, **Aktualisieren**, um neue Datenbanken zu entdecken, oder **Entfernen**, um einen Datenbank-Host zu entfernen.
 - Klicken Sie auf **Einstellungen** und wählen Sie **Richtlinien**, um die vordefinierten Richtlinien anzuzeigen. Überprüfen Sie die vordefinierten Richtlinien, und wenn Sie möchten, können Sie sie entweder bearbeiten, um Ihre Anforderung zu erfüllen, oder erstellen Sie eine neue Richtlinie.

Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank

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

Schritte

1. Wenn die Betriebssystemauthentifizierung für die Datenbank deaktiviert ist, sollten Sie die Datenbankauthentifizierung konfigurieren, indem Sie auf **Configure** klicken.

2. Geben Sie den Benutzernamen, das Kennwort und die Anschlussdetails entweder im Abschnitt Datenbankeinstellungen oder ASM-Einstellungen an.

Der Oracle-Benutzer sollte über sysdba-Berechtigungen verfügen, und ASM-Benutzer sollten sysasm-Berechtigungen haben.

3. Klicken Sie Auf **Konfigurieren**.

Erstellen einer Richtlinie

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

Schritte

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

Backup der Cloud-nativen Applikationsdaten

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. Sie können auch ein On-Demand-Backup erstellen.



Wenn Sie ASM-Festplattengruppen für Oracle erstellen, stellen Sie sicher, dass keine gemeinsamen Volumes in Festplattengruppen vorhanden sind. Jede Festplattengruppe benötigt dedizierte Volumes.

Schritte

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

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

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

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



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

Erstellen von On-Demand-Backups

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

Schritte

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

Weitere Informationen

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

```
failed with status code 500, error
{"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
snapshot. Reason: Snapshot operation not allowed due to clones backed by
snapshots. Try again after sometime.
```

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

Sicherung von Cloud-nativen Applikationsdaten managen

Überwachen von Jobs

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

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

- Erfolgreich
- In Bearbeitung
- Warteschlange
- Warnung
- Fehlgeschlagen

Schritte

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

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

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

Zeigen Sie Backup-Details an

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

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



Die Agent-ID ist dem Konnektor zugeordnet. Wenn ein Connector, der bei der Registrierung des Oracle-Datenbank-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 API **Connector-Update** ausführen, um die Agenten-ID zu ändern.

Aktualisieren Sie die Verbindungsdetails

Wenn ein Connector, der bei der Registrierung des Oracle-Datenbank-Hosts verwendet wurde, nicht mehr existiert oder in AWS beschädigt ist, sollten Sie einen neuen Konnektor bereitstellen. Nach der Bereitstellung des neuen Connectors sollten Sie die **Connector-Update** API ausführen, um die Connector-Details zu aktualisieren.

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

Nach dem Aktualisieren der Connector-Details sollten Sie eine Verbindung zum Oracle-Datenbank-Host herstellen und die folgenden Schritte durchführen:

1. Holen Sie die Plug-in-Informationen ab, die auf dem Oracle Database Host ausgeführt werden.
`rpm -qi netapp-snapcenter-plugin-oracle`
2. Deinstallieren Sie das Plug-in.
`sudo /opt/NetApp/snapcenter/spl/installation/plugins/uninstall`
3. Überprüfen Sie, ob das Plug-in erfolgreich deinstalliert wurde.
`rpm -qi netapp-snapcenter-plugin-oracle`

Nachdem Sie das Plug-in deinstalliert haben, können Sie das Plug-in bereitstellen. ["Weitere Informationen ."](#)

Konfigurieren Sie das Zertifikat der Zertifizierungsstelle

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

Konfigurieren Sie das Zertifikat einer Zertifizierungsstelle für die Authentifizierung des Clientzertifikats

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

Was Sie brauchen

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

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

Schritte

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

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

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

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

8. Importieren Sie die Stammzertifizierungsstelle und die Zwischenzertifikate.

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



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

9. SPL neu starten: `systemctl restart spl`

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

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

Was Sie brauchen

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

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

```
docker volume inspect | grep Mountpoint
```

Schritte

1. Führen Sie auf dem Plug-in-Host folgende Schritte durch:

- Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher `/var/opt/snapcenter/spl/etc`.
- Erstellen Sie das PKCS12-Format des Zertifikats, das sowohl ein Zertifikat als auch einen Schlüssel mit dem Alias `splkeystore` hat.

```
keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore -destalias splkeystore -noprompt
```
- Fügen Sie das CA-Zertifikat hinzu.

```
keytool -list -v -keystore keystore.jks
```
- Überprüfen Sie die Zertifikate.

```
keytool -list -v -keystore keystore.jks
```
- SPL neu starten: `systemctl restart spl`

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

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

Erstellen Sie den Serverordner, falls er nicht vorhanden ist.

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

```
sudo docker restart cloudmanager_scs_cloud
```

Zugriff auf REST-APIs

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

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

Stellen Sie Cloud-native Applikationsdaten wieder her

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

Schritte

- Klicken Sie Auf [...](#) Entsprechend der Datenbank, die Sie wiederherstellen möchten, und klicken Sie auf **Details anzeigen**.
- Klicken Sie Auf [...](#) Entsprechend der Datensicherung, die Sie für die Wiederherstellung verwenden

möchten, und klicken Sie auf **Restore**.

3. Führen Sie im Abschnitt „Umfang wiederherstellen“ die folgenden Aktionen durch:

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



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

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

Die Option **Kraft in-Place Restore** überschreibt die Datei spfile, Password file und Archivprotokolldateien aus der Diskgroup der Datendateien. 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 Alle Protokolle .
Wiederherstellen einer bestimmten Systemänderungsnummer (SCN)	Wählen Sie bis Systemänderungsnummer und geben Sie das SCN an.
Sie möchten ein Recovery zu einem bestimmten Datum und einer bestimmten Zeit durchführen	Wählen Sie Datum und Uhrzeit .
Möchten Sie nicht wiederherstellen	Wählen Sie Keine Wiederherstellung .

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**.

Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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