



Backup und Restore von On-Premises- Applikationsdaten

Cloud Backup

NetApp
December 07, 2022

Inhaltsverzeichnis

- Backup und Restore von On-Premises-Applikationsdaten 1
 - Sichern Sie Ihre lokalen Applikationsdaten 1
 - Registrieren Sie den SnapCenter-Server. 2
 - Erstellen einer Richtlinie für das Backup von Applikationen 4
 - Sichern Sie On-Premises-Applikationsdaten in Amazon Web Services 5
 - Sichern Sie On-Premises-Applikationsdaten in Microsoft Azure 6
 - Sichern Sie On-Premises-Applikationsdaten auf der Google Cloud Platform 7
 - Sichern Sie On-Premises-Applikationsdaten in StorageGRID. 7
 - Management der Sicherung von Applikationen 9
 - Wiederherstellung von Applikationsdaten 12
 - Binden Sie Backups von Applikationen ein 15

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 Microsoft Azure

Durch die Integration von Cloud Backup für Applikationen in BlueXP und On-Premises-SnapCenter können Sie ein Backup der Applikationsdaten von ONTAP in Microsoft Azure 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 * Microsoft Azure* aus.
 - a. Geben Sie die Azure Abonnement-ID an.
 - b. Wählen Sie den Bereich aus, in dem Sie die Backups erstellen möchten.
 - c. Erstellen Sie entweder eine neue Ressourcengruppe oder verwenden Sie eine vorhandene Ressourcengruppe.
 - d. Geben Sie den IP-Speicherplatz an.
 - e. 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 auf der Google Cloud Platform

Durch die Integration von Cloud Backup für Anwendungen in BlueXP und On-Premises-SnapCenter können Sie Backups der Applikationsdaten von ONTAP auf der Google Cloud-Plattform 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 JEDOC 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 **Google Cloud Platform** als Cloud-Provider aus.
 - a. Wählen Sie das Google Cloud Projekt aus, in dem der Google Cloud Storage-Bucket für Backups erstellt werden soll.
 - b. Geben Sie im Feld Google Cloud Access Key den Schlüssel an.
 - c. Geben Sie im Feld Google Cloud 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.
 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"](#).

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.