Backup und Restore von On-Premises-Applikationsdaten

BlueXP backup and recovery

NetApp
April 18, 2024

Inhalt

Backup und Restore von On-Premises-Applikationsdaten

Sichern Sie Ihre lokalen Applikationsdaten

BlueXP Backup und Recovery für Applikationen bietet Datensicherungsfunktionen für applikationskonsistente Snapshots – von der primären On-Premises-ONTAP-Umgebung zum Cloud-Provider.

Backups von Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL, PostgreSQL-Applikationen werden von lokalen ONTAP Systemen über Amazon Web Services, Microsoft Azure, Google Cloud Platform und StorageGRID übertragen.

Weitere Informationen zu BlueXP Backup und Recovery für Applikationen finden Sie unter:

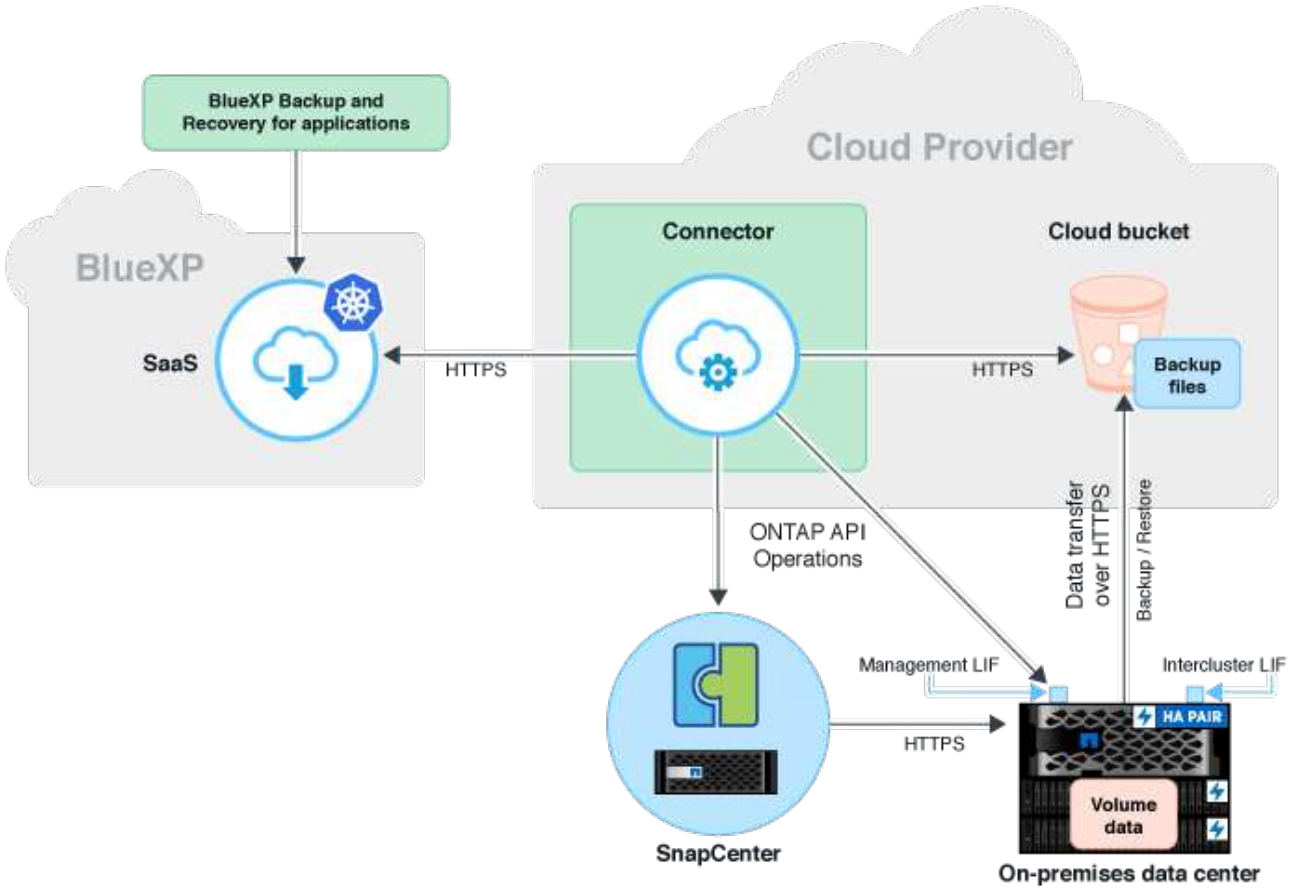
- "Applikationsspezifisches Backup mit BlueXP Backup und Recovery sowie SnapCenter"
- "Podcast zu BlueXP Backup und Recovery für Applikationen"

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass eine unterstützte Konfiguration vorhanden ist, bevor Sie mit dem Backup von Applikationsdaten beim Cloud-Provider beginnen.

- ONTAP 9.8 oder höher
- BlueXP
- SnapCenter Server 4.6 oder höher
  - Sie sollten SnapCenter Server 4.7 oder höher verwenden, wenn Sie die folgenden Funktionen verwenden möchten:
    - Sichern Sie Backups aus lokalem sekundären Storage
    - Sicherung von SAP HANA Applikationen
    - Sichern von Oracle- und SQL-Applikationen in VMware-Umgebungen
    - Speicherexport eines Backups
    - Backups deaktivieren
    - SnapCenter-Server nicht registrieren
  - Sie sollten SnapCenter Server 4.9 oder höher verwenden, wenn Sie die folgenden Funktionen verwenden möchten:
    - Mounten Sie die Backups der Oracle Datenbank
    - Stellen Sie die Daten auf dem alternativen Speicher wieder her
  - Wenn Sie MongoDB-, MySQL- und PostgreSQL-Applikationen schützen möchten, sollten Sie SnapCenter Server 4.9P1 verwenden
- Mindestens ein Backup pro Applikation sollte auf dem SnapCenter-Server verfügbar sein
- Mindestens eine tägliche, wöchentliche oder monatliche Police in SnapCenter ohne Etikett oder Etikett mit der Richtlinie in BlueXP

Die folgende Abbildung zeigt die einzelnen Komponenten beim Backup in der Cloud 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 in BlueXP 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-Host ausgeführt wird.

      Stellen Sie sicher, dass der Port offen ist, damit die Kommunikation zwischen SnapCenter Server und BlueXP stattfinden 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. Wählen Sie den Konnektor aus der Dropdown-Liste **Connector** aus.
6. Klicken Sie Auf **Registrieren**.

Nachdem Sie fertig sind

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.

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.
- MongoDB
- MySQL
- PostgreSQL

Folgende 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

Erstellen Sie eine Richtlinie für Backups von Applikationsdaten in der Cloud.

Bevor Sie beginnen

- Wenn Sie Backups vom Objektspeicher auf den Archiv-Storage verschieben möchten, stellen Sie sicher, dass Sie die erforderliche ONTAP-Version verwenden.
  - Wenn Sie Amazon Web Services verwenden, sollten Sie ONTAP 9.10.1 oder höher verwenden
  - Wenn Sie Microsoft Azure verwenden, sollten Sie ONTAP 9.10.1 oder höher verwenden
  - Wenn Sie Google Cloud nutzen, sollten Sie ONTAP 9.12.1 oder höher verwenden
  - Wenn Sie StorageGRID verwenden, sollten Sie ONTAP 9.12.1 oder höher verwenden
- Sie sollten die Zugriffsebene für den Archiv für jeden Cloud-Provider konfigurieren.

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**.
7. Klicken Sie Auf **Erstellen**.

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

Sichern Sie On-Premises-Applikationsdaten in Amazon Web Services

Führen Sie ein paar Schritte durch, um die Anwendungsdaten von ONTAP auf Amazon Web Services zu sichern.

BlueXP unterstützt Datensperrung und Ransomware-Schutz. Wenn der ONTAP Cluster unter ONTAP 9.11.1 oder höher ausgeführt wird und Sie den Archiv-Storage nicht konfiguriert haben, können Sie die Backups vor dem Überschreiben, Löschen und Ransomware-Bedrohungen schützen.

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 die Cluster-Management-LIF, die BlueXP ermitteln soll. 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 der Cluster-Management-LIF an.
   ii. Geben Sie die Anmeldedaten des ONTAP-Cluster-Benutzers an.

   BlueXP Backup und Recovery für Applikationen unterstützen 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 den Archiv-Tier aus, wenn Sie in der Richtlinie Archivspeicher konfiguriert haben.

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

6. Konfigurieren Sie die Datensperrung und den Ransomware-Schutz.
7. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

Sichern Sie On-Premises-Applikationsdaten in Microsoft Azure

Führen Sie ein paar Schritte durch, um die Applikationsdaten von ONTAP auf Microsoft Azure zu sichern.

BlueXP unterstützt Datensperrung und Ransomware-Schutz. Wenn der ONTAP Cluster unter ONTAP 9.12.1 oder höher ausgeführt wird und Sie den Archiv-Storage nicht konfiguriert haben, können Sie die Backups vor dem Überschreiben, Löschen und Ransomware-Bedrohungen schützen.

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 die Cluster-Management-LIF, die BlueXP ermitteln soll. 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 der Cluster-Management-LIF an.
   ii. Geben Sie die Anmeldedaten des ONTAP-Cluster-Benutzers an.

      BlueXP Backup und Recovery für Applikationen unterstützen 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 den Archiv-Tier aus, wenn Sie in der Richtlinie Archivspeicher konfiguriert haben.

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

6. Konfigurieren Sie die Datensperrung und den Ransomware-Schutz.
7. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

Sichern Sie On-Premises-Applikationsdaten auf der Google Cloud Platform

Führen Sie ein paar Schritte durch, um das Backup der Applikationsdaten von ONTAP auf der Google Cloud Platform zu 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 die Cluster-Management-LIF, die BlueXP ermitteln soll. 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 der Cluster-Management-LIF an.
      ii. Geben Sie die Anmeldedaten des ONTAP-Cluster-Benutzers an.

         BlueXP Backup und Recovery für Applikationen unterstützen 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.
   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

Führen Sie ein paar Schritte durch, um die Applikationsdaten von ONTAP auf StorageGRID zu sichern.

BlueXP unterstützt Datensperrung und Ransomware-Schutz. Wenn der ONTAP Cluster unter ONTAP 9.11.1 oder höher ausgeführt wird, sind die StorageGRID Systeme 11.6.0.3 oder höher. Wenn Sie keinen Archiv-Storage konfiguriert haben, können Sie die Backups vor dem Überschreiben, Löschen und Ransomware-Bedrohungen schützen.

Bevor Sie beginnen

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 die Cluster-Management-LIF, die BlueXP ermitteln soll. 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 der Cluster-Management-LIF an.
      ii. Geben Sie die Anmeldedaten des ONTAP-Cluster-Benutzers an.

BlueXP Backup und Recovery für Applikationen unterstützen 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.
   e. Geben Sie den Archiv-Tier an, wenn Sie in der Richtlinie Archivspeicher konfiguriert haben.

Wenn Sie die Option…	Führen Sie folgende Schritte durch…
AWS	i. Wählen Sie entweder die StorageGRID aus der Dropdown-Liste aus, oder fügen Sie den StorageGRID-Cluster hinzu. ii. Geben Sie den AWS Account an. iii. Geben Sie im Feld AWS Access Key den Schlüssel an. iv. Geben Sie im Feld AWS Secret Key das Passwort an. v. Wählen Sie den Bereich aus, in dem Sie die Backups erstellen möchten. vi. Klicken Sie Auf **Speichern**.
Azure	i. Wählen Sie im Dropdown-Menü den StorageGRID-Cluster aus, oder fügen Sie den Cluster hinzu. ii. Geben Sie die Azure Abonnement-ID an. iii. Wählen Sie den Bereich aus, in dem Sie die Backups erstellen möchten. iv. Erstellen Sie entweder eine neue Ressourcengruppe oder verwenden Sie eine vorhandene Ressourcengruppe. v. Klicken Sie Auf **Speichern**.

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

6. Konfigurieren Sie die Datensperrung und den Ransomware-Schutz.
7. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

Management der Sicherung von Applikationen

Sie können den Schutz von Applikationen managen, indem Sie Richtlinien anzeigen, Backups anzeigen, die Änderungen am Datenbank-Layout, an Richtlinien und Ressourcengruppen anzeigen und alle Vorgänge über die BlueXP UI überwachen.

Anzeigen von Richtlinien

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

Schritte

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` Cmdlet in SnapCenter:
Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können, und deren Beschreibungen können durch Ausführen des Befehls Get-Help abgerufen werden.

Anzeigen von Backups in der Cloud

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

Schritte

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 von Backups benötigte Zeit hängt von dem Standardreplizierungszeitplan von ONTAP ab.

- Für Oracle-Datenbanken werden sowohl Daten- als auch Protokollsicherungen, Systemänderungsnummer (SCN) für jedes Backup, Enddatum für jedes Backup aufgeführt. Sie können nur die Datensicherung auswählen und die Datenbank am ursprünglichen Speicherort wiederherstellen. Sie können das Daten-Backup mounten und Backup protokollieren an einem alternativen Speicherort.
- 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 an ihrem ursprünglichen oder alternativen Speicherort wiederherstellen.
- Für eine Instanz von Microsoft SQL Server werden Backups der Datenbanken unter dieser Instanz aufgeführt.
- Bei SAP HANA Datenbanken werden nur die Daten-Backups und das Enddatum für jedes Backup aufgeführt. Sie können das Backup auswählen und den Speicherexport auf einem bestimmten Host

durchführen.

- Für MongoDB, MySQL und PostgreSQL werden nur die Daten-Backups und das Enddatum jedes Backups aufgelistet. Sie können das Backup auswählen und den Speicherexport auf einem bestimmten Host 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` Cmdlet in SnapCenter: Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können, und deren Beschreibungen können durch Ausführen des Befehls Get-Help abgerufen werden.

Deaktivieren Sie die Sicherung

Sie können alle Backups, die in den Objektspeicher verschoben werden, sowohl aus SnapCenter als auch aus dem Objektspeicher löschen.

Schritte

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

   Standardmäßig ist das Kontrollkästchen aktiviert, und es löscht alle Backups, die sowohl aus SnapCenter als auch aus dem Objektspeicher in den Objektspeicher verschoben werden.

   Wenn Sie das Kontrollkästchen deaktivieren, werden die Backups nur im Objektspeicher beibehalten, aber diese Backups können nicht für die Wiederherstellung auf Applikationsebene verwendet werden. Wenn Sie später das Backup für diese Anwendung aktivieren, werden die im Objektspeicher aufbewahrten Backups nicht zur Wiederherstellung aufgeführt.

3. Klicken Sie Auf **Sicherung Deaktivieren**.

Datenbanklayout ändern

Wenn zur Datenbank Volumes hinzugefügt werden, kennzeichnet SnapCenter Server die Snapshots auf den neuen Volumes automatisch gemäß der Richtlinie und dem Zeitplan. Diese neuen Volumes verfügen nicht über den Objektspeicher-Endpunkt, und Sie sollten die Volumes aktualisieren, indem Sie die folgenden Schritte ausführen:

Schritte

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 der Anwendung nach der Konfiguration des Cloud-Providers ein Speicher-Volume hinzugefügt wird, kennzeichnet SnapCenter Server die Snapshots für neue Backups, auf denen sich die Anwendung befindet.

- Sie sollten die Beziehung zum Objektspeicher manuell löschen, wenn das entfernte Volume nicht von anderen Applikationen verwendet wird.
- 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, sollten Sie die Sicherungsbeziehung aktualisieren.

Schritte

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

SnapCenter-Server nicht registrieren

Schritte

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**.

   Standardmäßig ist das Kontrollkästchen aktiviert, und es löscht alle Backups, die sowohl aus SnapCenter als auch aus dem Objektspeicher in den Objektspeicher verschoben werden.

   Wenn Sie das Kontrollkästchen deaktivieren, werden die Backups nur im Objektspeicher beibehalten, aber diese Backups können nicht für die Wiederherstellung auf Applikationsebene verwendet werden. Wenn Sie später das Backup für diese Anwendung aktivieren, werden die im Objektspeicher aufbewahrten Backups nicht zur Wiederherstellung aufgeführt.

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.

Schritte

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.

Konfigurieren Sie CA-Zertifikate

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

Konfigurieren Sie ein von SnapCenter CA signiertes Zertifikat in BlueXP Connector

Sie sollten ein von SnapCenter CA signiertes Zertifikat in BlueXP Connector konfigurieren, damit der Connector das SnapCenter Zertifikat überprüfen kann.

Bevor Sie beginnen

Führen Sie den folgenden Befehl im BlueXP Connector aus, um *<base_mount_path>* zu erhalten:
```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Schritte

1. Melden Sie sich beim Connector an.
   ```
   cd <base_mount_path> mkdir -p server/certificate
   ```
2. Kopieren Sie die Stammzertifizierungsstelle und die Zwischendateien der Zertifizierungsstelle in das Verzeichnis *<base_mount_path>/Server/Certificate*.

   Die CA-Dateien sollten im Pem-Format vorliegen.
3. Wenn Sie CRL-Dateien haben, führen Sie die folgenden Schritte aus:
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Kopieren Sie die CRL-Dateien in das Verzeichnis *<base_mount_path>/Server/crl*.
4. Stellen Sie eine Verbindung zum Cloudmanager_snapcenter her und ändern Sie das enableCACert in config.yml auf true.
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert:
   false/enableCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. Starten Sie den Cloudmanager_snapcenter Container neu.
   ```
   sudo docker restart cloudmanager_snapcenter
   ```

Konfigurieren Sie ein CA-signiertes Zertifikat für BlueXP Connector

Wenn in SnapCenter 2-Wege-SSL aktiviert ist, sollten Sie die folgenden Schritte auf dem Connector durchführen, um das CA-Zertifikat als Clientzertifikat zu verwenden, wenn der Connector eine Verbindung mit dem SnapCenter herstellt.

Bevor Sie beginnen

Sie sollten den folgenden Befehl ausführen, um *<base_mount_path>* zu erhalten:
```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Schritte

1. Melden Sie sich beim Connector an.
   ```
   cd <base_mount_path> mkdir -p client/certificate
   ```
2. Kopieren Sie das CA-signierte Zertifikat und die Schlüsseldatei in das *<base_mount_path>/Client/Certificate* im Connector.

   Der Dateiname sollte Certificate.pem und key.pem sein. Das Zertifikat.pem sollte die gesamte Kette der Zertifikate wie Zwischenzertifikat und Root CA haben.
3. Erstellen Sie das PKCS12-Format des Zertifikats mit dem Namen Certificate.p12 und behalten Sie

<base_Mount_path>/Client/Certificate.

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

4. Stellen Sie eine Verbindung zum Cloudmanager_snapcenter her und ändern Sie sendCACert in config.yml auf true.
```
sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
false/sendCACert: true/g' /opt/netapp/cloudmanager-
snapcenter/config/config.yml
```
5. Starten Sie den Cloudmanager_snapcenter Container neu.
```
sudo docker restart cloudmanager_snapcenter
```
6. Führen Sie die folgenden Schritte auf dem SnapCenter durch, um das vom Konnektor gesendete Zertifikat zu validieren.
   a. Melden Sie sich beim Host des SnapCenter Servers an.
   b. Klicken Sie Auf **Start** > **Suche Starten**.
   c. Geben sie mmc ein und drücken Sie **Enter**.
   d. Klicken Sie Auf **Ja**.
   e. Klicken Sie im Menü Datei auf **Snap-in hinzufügen/entfernen**.
   f. Klicken Sie auf **Zertifikate** > **Hinzufügen** > **Computerkonto** > **Weiter**.
   g. Klicken Sie auf **lokaler Computer** > **Fertig stellen**.
   h. Wenn Sie keine weiteren Snap-ins zur Konsole hinzufügen möchten, klicken Sie auf **OK**.
   i. Doppelklicken Sie in der Konsolenstruktur auf **Zertifikate**.
   j. Klicken Sie mit der rechten Maustaste auf den Store **Trusted Root Certification Authorities**.
   k. Klicken Sie auf **Import**, um die Zertifikate zu importieren und befolgen Sie die Schritte im **Zertifikatimport-Assistenten**.

Wiederherstellung von lokalen Applikationsdaten

Oracle Datenbank wiederherstellen

Sie können Oracle Datenbanken entweder am ursprünglichen Speicherort oder an einem alternativen Speicherort wiederherstellen. Bei einer RAC-Datenbank werden die Daten auf dem lokalen Knoten wiederhergestellt, auf dem das Backup erstellt wurde.

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.

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. Geben Sie auf der Seite Wiederherstellungsoptionen den Speicherort an, an dem Sie die Datenbankdateien wiederherstellen möchten.

Sie suchen…	Tun Sie das…
Sie möchten den ursprünglichen Speicherort wiederherstellen	a. Wählen Sie **auf ursprünglichen Speicherort zurücksetzen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Klicken Sie Auf **Weiter**. d. 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. ◦ Wenn die Datenbank einen höheren Status aufweist, der Status jedoch in einen niedrigeren Status geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen, müssen Sie dieses Kontrollkästchen aktivieren. ◦ 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. e. Geben Sie den Recovery-Umfang an. ◦ Wählen Sie **Alle Protokolle**, wenn Sie die letzte Transaktion wiederherstellen möchten. ◦ Wählen Sie **bis SCN (System Change Number)**, wenn Sie eine Wiederherstellung auf eine bestimmte SCN durchführen möchten. ◦ Wählen Sie **Datum und Uhrzeit** aus, wenn Sie eine bestimmte Zeit und Daten wiederherstellen möchten. Sie müssen Datum und Uhrzeit der Zeitzone des Datenbank-Hosts angeben.
	Wählen Sie **Keine Wiederherstellung**,

Sie suchen…	Tun Sie das…
Sie möchten vorübergehend in einem anderen Speicher wiederherstellen und dann die wiederhergestellten Dateien an den ursprünglichen Speicherort kopieren	a. Wählen Sie **auf ursprünglichen Speicherort zurücksetzen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Wählen Sie **Speicherort ändern**. Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt. d. Klicken Sie Auf **Weiter**. e. Geben Sie auf der Seite Speicherzuordnung die Details zum alternativen Speicherort an, an dem die vom Objektspeicher wiederhergestellten Daten vorübergehend gespeichert werden. Wenn Sie ein lokales ONTAP-System auswählen und die Cluster-Verbindung zum Objektspeicher nicht konfiguriert haben, werden Sie aufgefordert, weitere Informationen zum Objektspeicher zu erhalten. f. Klicken Sie Auf **Weiter**. g. 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. ◦ Wenn die Datenbank einen höheren Status aufweist, der Status jedoch in einen niedrigeren Status geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen, müssen Sie dieses Kontrollkästchen aktivieren. ◦ 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

Sie suchen…	Tun Sie das…
Sie möchten an einem alternativen Speicherort wiederherstellen	a. Wählen Sie **an alternativen Speicherort wiederherstellen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Gehen Sie wie folgt vor, wenn Sie einen alternativen Speicher wiederherstellen möchten: i. Wählen Sie **Speicherort ändern**. Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt. ii. Klicken Sie Auf **Weiter**. iii. Geben Sie auf der Seite Speicherzuordnung die Details zum alternativen Speicherort an, an dem die Daten aus dem Objektspeicher wiederhergestellt werden müssen. d. Klicken Sie Auf **Weiter**. e. Wählen Sie auf der Seite Ziel-Host den Host aus, auf dem die Datenbank gemountet werden soll. i. (Optional) Geben Sie für NAS-Umgebungen den FQDN oder die IP-Adresse des Hosts an, auf den die aus dem Objektspeicher wiederhergestellten Volumes exportiert werden sollen. ii. (Optional) Geben Sie für die SAN-Umgebung die Initiatoren des Hosts an, denen LUNs der aus dem Objektspeicher wiederhergestellten Volumes zugeordnet werden sollen. f. Klicken Sie Auf **Weiter**.

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

Die Option **Restore to alternative location** hängt das ausgewählte Backup auf dem angegebenen Host an. Sie sollten die Datenbank manuell aufrufen.

Nach dem Mounten des Backups können Sie es erst wieder mounten, nachdem es abgehängt wurde. Sie können die Option **Unmount** von der Benutzeroberfläche aus verwenden, um das Backup zu entsperren.

Informationen zum Einrichten der Oracle-Datenbank finden Sie unter: "Knowledge Base-Artikel".

SQL Server Datenbank wiederherstellen

Sie können die SQL Server Datenbank entweder am ursprünglichen Speicherort oder an einem alternativen Speicherort wiederherstellen.

> Single File Restore (SFR), Recovery von Protokoll-Backups und erneutes Seeding von Verfügbarkeitsgruppen werden nicht unterstützt.

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. Geben Sie auf der Seite Wiederherstellungsoptionen den Speicherort an, an dem Sie die Datenbankdateien wiederherstellen möchten.

Sie suchen…	Tun Sie das…
Sie möchten den ursprünglichen Speicherort wiederherstellen	a. Wählen Sie **auf ursprünglichen Speicherort zurücksetzen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Klicken Sie Auf **Weiter**.
Sie möchten vorübergehend in einem anderen Speicher wiederherstellen und dann die wiederhergestellten Dateien an den ursprünglichen Speicherort kopieren	a. Wählen Sie **auf ursprünglichen Speicherort zurücksetzen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Wählen Sie **Speicherort ändern**. Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt. d. Klicken Sie Auf **Weiter**. e. Geben Sie auf der Seite Speicherzuordnung die Details zum alternativen Speicherort an, an dem die vom Objektspeicher wiederhergestellten Daten vorübergehend gespeichert werden. f. Klicken Sie Auf **Weiter**.

Sie suchen…	Tun Sie das…
Sie möchten an einem alternativen Speicherort wiederherstellen	a. Wählen Sie **an alternativen Speicherort wiederherstellen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Klicken Sie Auf **Weiter**. d. Wählen Sie auf der Seite Ziel-Host einen Hostnamen aus, geben Sie einen Datenbanknamen an (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an. Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateiendung der ursprünglichen Datenbankdatei identisch sein. e. Klicken Sie Auf **Weiter**.

Sie suchen…	Tun Sie das…
Sie möchten vorübergehend auf einem anderen Speicher wiederherstellen und die wiederhergestellten Dateien dann an einen anderen Speicherort kopieren	a. Wählen Sie **an alternativen Speicherort wiederherstellen**. b. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus. c. Wählen Sie **Speicherort ändern**. Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt. d. Klicken Sie Auf **Weiter**. e. Geben Sie auf der Seite Speicherzuordnung die Details zum alternativen Speicherort an, an dem die vom Objektspeicher wiederhergestellten Daten vorübergehend gespeichert werden. f. Klicken Sie Auf **Weiter**. g. Wählen Sie auf der Seite Ziel-Host einen Hostnamen aus, geben Sie einen Datenbanknamen an (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an. Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateiendung der ursprünglichen Datenbankdatei identisch sein. h. Klicken Sie Auf **Weiter**.

6. Wählen Sie im Feld **Pre-Operations** 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.
7. Wählen Sie im Abschnitt **Post-Operations** eine der folgenden Optionen aus, um den Datenbankstatus für die Wiederherstellung zusätzlicher Transaktionsprotokolle festzulegen:
   - 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.

8. Klicken Sie Auf **Weiter**.
9. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

Wiederherstellung der SAP HANA Datenbank

Sie können die SAP HANA-Datenbank auf einem beliebigen Host wiederherstellen.

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** und wählen Sie aus der Dropdown-Liste **HANA** aus.
3. Klicken Sie auf **Details anzeigen**, die der Datenbank entsprechen, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
4. Geben Sie auf der Seite Wiederherstellungsoptionen eine der folgenden Optionen an:
   a. Geben Sie in der NAS-Umgebung den FQDN oder die IP-Adresse des Hosts an, auf den die aus dem Objektspeicher wiederhergestellten Volumes exportiert werden sollen.
   b. Geben Sie in der SAN-Umgebung die Initiatoren des Hosts an, dem die LUNs der aus dem Objektspeicher wiederhergestellten Volumes zugeordnet werden sollen.
5. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus.
6. Wenn nicht genügend Speicherplatz auf dem Quellspeicher vorhanden ist oder der Quellspeicher nicht verfügbar ist, wählen Sie **Speicherort ändern**.

   Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt.

7. Klicken Sie Auf **Weiter**.
8. Geben Sie auf der Seite Speicherzuordnung die Details zum alternativen Speicherort an, an dem die vom Objektspeicher wiederhergestellten Daten gespeichert werden.
9. Klicken Sie Auf **Weiter**.
10. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

Dieser Vorgang führt nur den Speicherexport des ausgewählten Backups auf dem angegebenen Host aus. Sie sollten das Dateisystem manuell mounten und die Datenbank aufrufen. Nach der Nutzung des Volumes kann der Speicheradministrator das Volume aus dem ONTAP-Cluster löschen.

Weitere Informationen zum Einrichten der SAP HANA-Datenbank finden Sie unter: "TR-4667: Überblick über den Workflow von SAP Systemkopien mit SnapCenter" Und "TR-4667: Überblick über den Workflow des SAP-Systemklons mit SnapCenter".

Stellen Sie MongoDB-, MySQL- und PostgreSQL-Datenbanken wieder her

Sie können MongoDB-, MySQL- und PostgreSQL-Datenbanken auf einem beliebigen Host wiederherstellen.

Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Wählen Sie im Feld **Filter by** den Filter **Type** aus und wählen Sie im Dropdown-Menü **MongoDB**, **MySQL** oder **PostgreSQL** aus.
3. Klicken Sie auf **Details anzeigen**, die der Datenbank entsprechen, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
4. Geben Sie auf der Seite Wiederherstellungsoptionen eine der folgenden Optionen an:
   a. Geben Sie in der NAS-Umgebung den FQDN oder die IP-Adresse des Hosts an, auf den die aus dem Objektspeicher wiederhergestellten Volumes exportiert werden sollen.
   b. Geben Sie in der SAN-Umgebung die Initiatoren des Hosts an, dem die LUNs der aus dem Objektspeicher wiederhergestellten Volumes zugeordnet werden sollen.
5. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus.
6. Wenn nicht genügend Speicherplatz auf dem Quellspeicher vorhanden ist oder der Quellspeicher nicht verfügbar ist, wählen Sie **Speicherort ändern**.

   Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt.
7. Klicken Sie Auf **Weiter**.
8. Geben Sie auf der Seite Speicherzuordnung die Details zum alternativen Speicherort an, an dem die vom Objektspeicher wiederhergestellten Daten gespeichert werden.
9. Klicken Sie Auf **Weiter**.
10. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

Dieser Vorgang führt nur den Speicherexport des ausgewählten Backups auf dem angegebenen Host aus. Sie sollten das Dateisystem manuell mounten und die Datenbank aufrufen. Nach der Nutzung des Volumes kann der Speicheradministrator das Volume aus dem ONTAP-Cluster löschen.