Backup und Restore von Cloud-nativen Applikationsdaten

Cloud Backup

NetApp
November 16, 2022

Inhaltsverzeichnis

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.

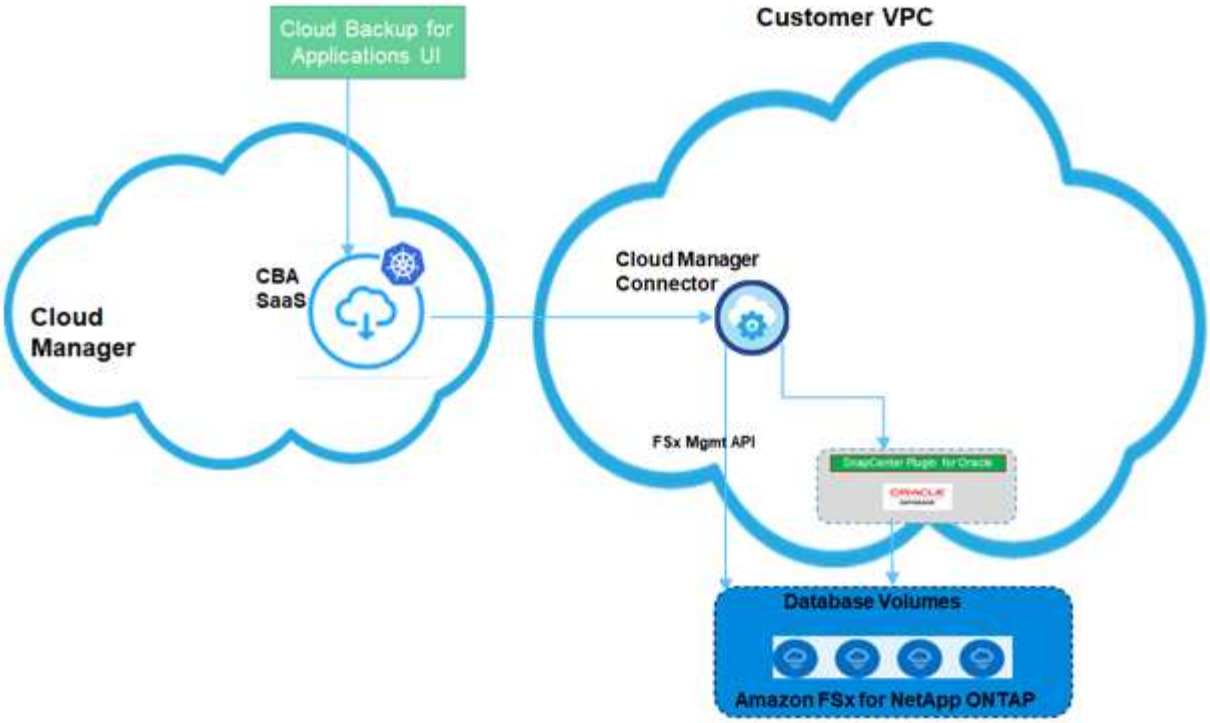
  Die Datensicherungs-Workflows werden für Applikationen auf NetApp Cloud Storage orchestriert.

- 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 -srcalias 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 Oracle database credentials.
   - 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 sysmasm-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:
   a. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher */var/opt/snapcenter/spl/etc*.
   b. Erstellen Sie das PKCS12-Format des Zertifikats, das sowohl ein Zertifikat als auch einen Schlüssel mit dem Alias *splkeystore* hat.
   c. Fügen Sie das CA-Zertifikat hinzu.
   `keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore -destalias splkeystore -noprompt`
   d. Überprüfen Sie die Zertifikate.
   `keytool -list -v -keystore keystore.jks`
   e. SPL neu starten: `systemctl restart spl`
2. Führen Sie die folgenden Schritte auf dem Konnektor aus:
   a. Melden Sie sich beim Connector als nicht-Root-Benutzer an.
   b. Kopieren Sie die gesamte Kette der CA-Zertifikate auf das persistente Volume unter *<base_Mount_PATH>/Server*.

      Erstellen Sie den Serverordner, falls er nicht vorhanden ist.
   c. Verbinden Sie sich mit dem cloudmanager_scs_Cloud und ändern Sie den **enableCACert** in *config.yml* an **true**.
   `sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert: false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-cloud/config/config.yml`
   d. Starten Sie den Cloud-Manager_scs_Cloud-Container neu.
   `sudo docker restart cloudmanager_scs_cloud`

Zugriff auf REST-APIs

ES sind DIE REST-APIs zum Schutz der Applikationen in der Cloud verfügbar "Hier".

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

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

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

Sie suchen…	Tun Sie das…
Möchten nur die Datendateien wiederherstellen	Wählen Sie **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

Markeninformationen