Client-Zugriff auf S3-Objekt-Storage aktivieren

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Client-Zugriff auf S3-Objekt-Storage aktivieren

Aktivieren Sie ONTAP S3 Zugriff für Remote FabricPool Tiering

Damit ONTAP S3 als Cloud-Tier (Remote FabricPool Capacity) verwendet werden kann, muss der ONTAP S3-Administrator dem Remote-ONTAP-Cluster-Administrator Informationen über die S3-Serverkonfiguration bereitstellen.

Über diese Aufgabe

Die folgenden S3-Serverinformationen sind erforderlich, um FabricPool Cloud-Tiers zu konfigurieren:

- Servername (FQDN)
- Bucket-Name
- CA-Zertifikat
- Zugriffsschlüssel
- Passwort (geheimer Zugriffsschlüssel)

Darüber hinaus ist die folgende Netzwerkkonfiguration erforderlich:

- Der Hostname des Remote-ONTAP S3-Servers muss im für die Admin-SVM konfigurierten DNS-Server einen Eintrag enthalten, einschließlich des FQDN-Namens des S3-Servers und der IP-Adressen auf seinen LIFs.
- Intercluster LIFs müssen auf dem lokalen Cluster konfiguriert werden, obwohl Cluster-Peering nicht erforderlich ist.

In der FabricPool Dokumentation finden Sie Informationen zur Konfiguration von ONTAP S3 als Cloud-Tier.

"Managen von Storage-Tiers mit FabricPool"

Aktivieren Sie ONTAP S3-Zugriff für lokales FabricPool Tiering

Damit ONTAP S3 als lokale FabricPool-Kapazitäts-Tier verwendet werden kann, müssen Sie einen Objektspeicher basierend auf dem von Ihnen erstellten Bucket definieren und dann den Objektspeicher an ein Performance-Tier-Aggregat anhängen, um eine FabricPool zu erstellen.

Bevor Sie beginnen

Sie müssen über den ONTAP S3-Servernamen und einen Bucket-Namen verfügen, und der S3-Server muss mithilfe von Cluster-LIFs (mit der erstellt wurden `-vserver Cluster` Parameter).

Über diese Aufgabe

Die Objektspeicher-Konfiguration enthält Informationen zur lokalen Kapazitäts-Tier, einschließlich der S3-Server, Bucket-Namen und Authentifizierungsanforderungen.

Eine einmal erstellte Objekt-Storage-Konfiguration darf keinem anderen Objektspeicher oder Bucket

zugeordnet werden. Sie können mehrere Buckets für lokale Tiers erstellen, jedoch nicht mehrere Objektspeichern in einem einzelnen Bucket erstellen.

Für eine lokale Kapazitäts-Tier ist keine FabricPool-Lizenz erforderlich.

Schritte

1. Objektspeicher für die lokale Kapazitäts-Tier erstellen:

   `storage aggregate object-store config create -object-store-name` *`store_name`* `-ipspace Cluster -provider-type ONTAP_S3 -server` *`S3_server_name`* `-container -name` *`bucket_name`* `-access-key` *`access_key`* `-secret-password password`

   - Der `-container-name` Ist der von Ihnen erstellte S3-Bucket.
   - Der `-access-key` Parameter autorisiert Anfragen an den ONTAP S3-Server.
   - Der `-secret-password` Parameter (Secret Access Key) authentifiziert Anforderungen an den ONTAP S3-Server.
   - Sie können die einstellen `-is-certificate-validation-enabled` Parameter an `false` So deaktivieren Sie die Zertifikatprüfung für ONTAP S3.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Anzeigen und Überprüfen der Konfigurationsinformationen des Objektspeichers:

   `storage aggregate object-store config show`

3. Optional: Um zu sehen, wie viele Daten in einem Volume inaktiv sind, führen Sie die Schritte unter aus "Bestimmen der Menge an Daten in einem Volume, die inaktiv sind, mithilfe der inaktiven Datenberichterstellung".

   Wenn Sie feststellen möchten, wie viele Daten in einem Volume inaktiv sind, können Sie entscheiden, welches Aggregat für lokales FabricPool Tiering verwendet werden soll.

4. Verbinden Sie den Objektspeicher mit einem Aggregat:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Sie können das verwenden `allow-flexgroup` **`true`** Sie können Aggregate hinzufügen, die FlexGroup Volume-Komponenten enthalten.

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. Zeigen Sie die Objektspeicherinformationen an, und überprüfen Sie, ob der angeschlossene Objektspeicher verfügbar ist:

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

Aktivieren des Client-Zugriffs über eine S3-Applikation

Damit S3-Client-Applikationen auf den ONTAP S3-Server zugreifen können, muss der ONTAP S3-Administrator Konfigurationsinformationen für den S3-Benutzer bereitstellen.

Was Sie benötigen

Die S3-Client-App muss in der Lage sein, sich mithilfe der folgenden AWS-Signaturversionen am ONTAP S3-Server zu authentifizieren:

- Signaturversion 4, ONTAP 9.8 und höher
- Signatur Version 2, ONTAP 9.11.1 und höher

Andere Signaturversionen werden von ONTAP S3 nicht unterstützt.

Der ONTAP S3 Administrator muss S3 Benutzer erstellt und ihnen Zugriffsberechtigungen als einzelne Benutzer oder als Gruppenmitglied, in der Bucket-Richtlinie oder der Objekt-Storage-Server-Richtlinie gewährt haben.

Die S3-Client-App muss in der Lage sein, den ONTAP S3-Servernamen zu beheben. Dazu muss der ONTAP S3-Administrator den S3-Servernamen (FQDN) und die IP-Adressen für die LIFs des S3-Servers angeben.

Über diese Aufgabe

Um auf einen ONTAP S3-Bucket zuzugreifen, geben Benutzer in der S3-Client-Applikation Informationen ein, die der ONTAP S3-Administrator zur Verfügung stellt.

Ab ONTAP 9.9 unterstützt der ONTAP S3 Server die folgenden AWS-Client-Funktionen:

- Benutzerdefinierte Objekt-Metadaten

  Ein Satz von Schlüsselwert-Paaren kann Objekten als Metadaten zugewiesen werden, wenn sie mit PUT (oder POST) erstellt werden. Wenn ein GET/HEAD-Vorgang am Objekt ausgeführt wird, werden die benutzerdefinierten Metadaten zusammen mit den Systemmetadaten zurückgegeben.

- Objekt-Tagging

  Ein separater Satz von Schlüsselwert-Paaren kann als Tags für die Kategorisierung von Objekten zugewiesen werden. Im Gegensatz zu Metadaten werden Tags unabhängig vom Objekt mit REST-APIs erstellt und gelesen. Sie werden auch dann implementiert, wenn Objekte erstellt oder zu einem beliebigen Zeitpunkt danach erstellt werden.

Damit Clients Informationen zum Tagging abrufen und einfügen können, werden die Aktionen durchgeführt `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging` Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

Weitere Informationen finden Sie in der AWS S3-Dokumentation.

Schritte

1. Authentifizieren Sie die S3-Client-App mit dem ONTAP S3-Server, indem Sie den S3-Servernamen und das CA-Zertifikat eingeben.
2. Authentifizieren Sie einen Benutzer in der S3-Client-App, indem Sie die folgenden Informationen eingeben:
   - S3-Servername (FQDN) und Bucket-Name
   - Zugriffsschlüssel und geheimer Schlüssel des Benutzers