Konfigurieren des S3-Zugriffs auf eine SVM

ONTAP 9

NetApp
September 12, 2024

Inhalt

Konfigurieren des S3-Zugriffs auf eine SVM

Erstellung einer SVM für S3

Obwohl S3 parallel zu anderen Protokollen in einer SVM unterstützt werden kann, sollten Sie möglicherweise eine neue SVM erstellen, um Namespace und Workload zu isolieren.

Über diese Aufgabe

Wenn Sie lediglich S3-Objekt-Storage über eine SVM bereitstellen, ist für den S3-Server keine DNS-Konfiguration erforderlich. Allerdings möchten Sie DNS möglicherweise auf der SVM konfigurieren, wenn andere Protokolle verwendet werden.

Wenn Sie mit System Manager S3-Zugriff auf eine neue Storage-VM konfigurieren, müssen Sie Zertifikat- und Netzwerkinformationen eingeben. Die Storage-VM und der S3-Objekt-Storage-Server werden in einem Vorgang erstellt.

Beispiel 1. Schritte

System Manager

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den die Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

Sie sollten darauf vorbereitet sein, IP-Adressen für die Schnittstellenrollendaten einzugeben.

Wenn Sie ein von einer externen Zertifizierungsstelle signiertes Zertifikat verwenden, werden Sie aufgefordert, es während dieses Verfahrens einzugeben. Sie haben auch die Möglichkeit, ein vom System generiertes Zertifikat zu verwenden.

1. Aktivieren Sie S3 auf einer Storage-VM.

   a. Fügen Sie eine neue Speicher-VM hinzu: Klicken Sie auf **Storage > Storage VMs** und dann auf **Hinzufügen**.

      Falls es sich um ein neues System ohne bereits vorhandene Storage-VMs handelt, klicken Sie auf **Dashboard > Protokolle konfigurieren**.

   Wenn Sie einen S3-Server zu einer vorhandenen Speicher-VM hinzufügen: Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **S3**.

   a. Klicken Sie auf **S3** aktivieren und geben Sie dann den S3-Servernamen ein.
   b. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.

   c. Geben Sie die Netzwerkschnittstellen ein.
2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   - Der Geheimschlüssel wird nicht mehr angezeigt.
   - Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Vergewissern Sie sich, dass S3 für Ihr Cluster lizenziert ist:

   ```
   system license show -package s3
   ```

   Falls nicht, wenden Sie sich an Ihren Vertriebsmitarbeiter.

2. SVM erstellen:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- Verwenden Sie die UNIX-Einstellung für den `-rootvolume-security-style` Option.
- Verwenden Sie die Standard-C.UTF-8 `-language` Option.
- Der `ipspace` Die Einstellung ist optional.

3. Konfiguration und Status der neu erstellten SVM überprüfen:

```
vserver show -vserver <svm_name>
```

Der `Vserver Operational State` Das Feld muss angezeigt werden `running` Bundesland. Wenn der angezeigt wird `initializing` Zustand: Einiger Zwischenvorgang wie z. B. die Erstellung des Root-Volumes ist fehlgeschlagen. Außerdem müssen Sie die SVM löschen und erneut erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace ipspace A erstellt:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde und dass sie automatisch gestartet wurde und sich in befindet `running` Bundesland. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird. Standardmäßig wird das vsadmin-Benutzerkonto erstellt und befindet sich in `locked` Bundesland. Die vsadmin-Rolle ist dem vsadmin-Standardbenutzerkonto zugewiesen.

```
cluster-1::> vserver show -vserver svm1.example.com
                                   Vserver: svm1.example.com
                              Vserver Type: data
                           Vserver Subtype: default
                              Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                               Root Volume: root_svm1
                                 Aggregate: aggr1
                                NIS Domain: -
                 Root Volume Security Style: unix
                                LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                   Comment:
                              Quota Policy: default
                List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                              IPspace Name: ipspaceA
```

Erstellen und installieren Sie ein CA-Zertifikat auf der SVM

Um den HTTPS-Datenverkehr von S3-Clients auf die S3-fähige SVM zu aktivieren, ist ein CA-Zertifikat erforderlich.

Über diese Aufgabe

Zwar ist es möglich, einen S3-Server so zu konfigurieren, dass nur HTTP verwendet wird. Clients können zwar auch ohne CA-Zertifikat konfiguriert werden, es empfiehlt sich jedoch, den HTTPS-Datenverkehr auf ONTAP S3-Servern mit einem CA-Zertifikat zu sichern.

Ein CA-Zertifikat ist nicht erforderlich für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Traffic nur über die Cluster LIFs erfolgt.

Die Anweisungen in diesem Verfahren erstellen und installieren ein selbstsigniertes ONTAP-Zertifikat. CA-Zertifikate von Drittanbietern werden ebenfalls unterstützt. Weitere Informationen finden Sie in der Dokumentation zur Administratorauthentifizierung.

"Administratorauthentifizierung und RBAC"

Siehe `security certificate` Man-Pages für weitere Konfigurationsoptionen.

Schritte

1. Erstellen eines selbstsignierten digitalen Zertifikats:

   `security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name`

   Der `-type root-ca` Option erstellt und installiert ein selbstsigniertes digitales Zertifikat, um andere Zertifikate zu signieren, indem es als Zertifizierungsstelle fungiert.

   Der `-common-name` Option erstellt den Namen der Zertifizierungsstelle (CA) der SVM und wird verwendet, wenn der vollständige Name des Zertifikats generiert wird.

   Die standardmäßige Zertifikatsgröße beträgt 2048 Bit.

   Beispiel

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Wenn der generierte Name des Zertifikats angezeigt wird, speichern Sie ihn für die nachfolgenden Schritte.

2. Erzeugen einer Anfrage zum Signieren eines Zertifikats:

   `security certificate generate-csr -common-name s3_server_name [additional_options]`

   Der `-common-name` Der Parameter für die Signaturanforderung muss der S3-Servername (FQDN) sein.

   Gegebenenfalls können Sie den Speicherort und weitere detaillierte Informationen zur SVM angeben.

   Sie werden aufgefordert, eine Kopie Ihrer Zertifikatsanfrage und einen privaten Schlüssel für zukünftige Referenz aufzubewahren.

3. Signieren Sie die CSR mit SVM_CA, um das S3-Server-Zertifikat zu generieren:

   `security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial ca_cert_serial_number [additional_options]`

   Geben Sie die Befehlsoptionen ein, die Sie in früheren Schritten verwendet haben:

   - `-ca` — der allgemeine Name der CA, die Sie in Schritt 1 eingegeben haben.
   - `-ca-serial` — die CA-Seriennummer von Schritt 1. Wenn der Name des CA-Zertifikats beispielsweise svm1_ca_159D1587CE21E9D4_svm1_ca lautet, lautet die Seriennummer 159D1587CE21E9D4.

     Standardmäßig läuft das signierte Zertifikat in 365 Tagen ab. Sie können einen anderen Wert auswählen und weitere Signierungsdetails angeben.

Wenn Sie dazu aufgefordert werden, kopieren Sie die Zeichenfolge für die Zertifikatanforderung, die Sie in Schritt 2 gespeichert haben, und geben Sie sie ein.

Es wird ein signiertes Zertifikat angezeigt und zur späteren Verwendung gespeichert.

4. Installieren Sie das signierte Zertifikat auf der S3-fähigen SVM:

   `security certificate install -type server -vserver svm_name`

   Geben Sie bei Aufforderung das Zertifikat und den privaten Schlüssel ein.

   Sie haben die Möglichkeit, Zwischenzertifikate einzugeben, wenn eine Zertifikatkette gewünscht wird.

   Wenn der private Schlüssel und das CA-signierte digitale Zertifikat angezeigt werden, speichern Sie sie für zukünftige Referenz.

5. Holen Sie sich das Zertifikat für den öffentlichen Schlüssel:

   `security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

   Speichern Sie das Zertifikat für den öffentlichen Schlüssel für eine spätere Client-seitige Konfiguration.

   Beispiel

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                         Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                     Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Erstellen einer S3-Service-Datenrichtlinie

Es können Service-Richtlinien für S3-Daten und Managementservices erstellt werden. Für die Aktivierung des S3-Datenverkehrs auf LIFs ist eine S3-Service-Datenrichtlinie erforderlich.

Über diese Aufgabe

Eine Datenrichtlinie für den S3-Service ist erforderlich, wenn Sie Daten-LIFs und Intercluster-LIFs verwenden. Wenn Sie Cluster-LIFs für den lokalen Tiering-Anwendungsfall verwenden, ist dies nicht erforderlich.

Wenn eine Service-Richtlinie für eine LIF angegeben wird, wird diese Richtlinie verwendet, um eine Standardrolle, Failover-Richtlinie und Datenprotokollliste für die LIF zu erstellen.

Obwohl mehrere Protokolle für SVMs und LIFs konfiguriert werden können, empfiehlt es sich, S3 als einziges Protokoll für die Bereitstellung von Objektdaten zu verwenden.

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Service-Datenrichtlinie erstellen:

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   Der `data-core` Und `data-s3-server` Services sind die einzigen erforderlich, die für die Aktivierung von ONTAP S3 erforderlich sind, andere Services können jedoch bei Bedarf eingebunden werden.

Erstellung von Daten-LIFs

Wenn Sie eine neue SVM erstellt haben, sollten die dedizierten LIFs, die Sie für S3-Zugriff erstellen, Daten-LIFs sein.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerk-Port muss für den Administrator konfiguriert worden sein `up` Status:
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

  Subnetze enthalten einen Pool mit IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem erstellt `network subnet create` Befehl.

- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.
- Als Best Practice sollten LIFs, die für den Datenzugriff verwendet werden (Daten-s3-Server), und für Managementaufgaben verwendete LIFs (Management-https) getrennt sein. Beide Services sollten nicht auf derselben logischen Schnittstelle aktiviert werden.
- DNS-Einträge sollten nur IP-Adressen der LIFs haben, denen der Daten-s3-Server zugeordnet ist. Wenn IP-Adressen anderer LIFs im DNS-Datensatz angegeben werden, können ONTAP S3-Anfragen von anderen Servern bedient werden, was zu unerwarteten Antworten führt.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie eine große Anzahl von LIFs im Cluster besitzen, können Sie die im Cluster unterstützte LIF-Kapazität mithilfe der überprüfen `network interface capacity show` Befehl und die LIF-Kapazität, die auf jedem Node mithilfe von unterstützt wird `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene).
- Wenn Sie das Cloud-Tiering (Remote FabricPool Capacity) aktivieren, müssen Sie auch LIFs für Intercluster konfigurieren.

Schritte

1. LIF erstellen:

   ```
   network interface create -vserver svm_name -lif lif_name -service-policy
   service_policy_names -home-node node_name -home-port port_name {-address
   IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
   data -auto-revert {true|false}
   ```

- `-home-node` Ist der Node, den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.

  Sie können auch angeben, ob die LIF automatisch auf den Home-Node und den Home-Port mit zurückgesetzt werden soll `-auto-revert` Option.

- `-home-port` Ist der physische oder logische Port, an den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.
- Sie können eine IP-Adresse mit dem angeben `-address` Und `-netmask` Optionen, oder Sie aktivieren die Zuweisung von einem Subnetz mit dem `-subnet_name` Option.
- Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Der `network route create` Die man-Page enthält Informationen zum Erstellen einer statischen Route in einer SVM.
- Für das `-firewall-policy` Wählen Sie die gleiche Standardeinstellung aus `data` Die LIF-Rolle.

  Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- `-auto-revert` Ermöglicht Ihnen, anzugeben, ob eine Daten-LIF automatisch auf den Home-Node zurückgesetzt wird. Dies kann unter Umständen wie „Startvorgang“, ändert den Status der Management-Datenbank oder wenn die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Aber Sie können es auf einstellen `false` Abhängig von Netzwerkmanagement-Richtlinien in Ihrer Umgebung.
- Der `-service-policy` Option gibt die von Ihnen erstellte Daten- und Management-Services-Richtlinie sowie alle weiteren Richtlinien an, die Sie benötigen.

2. Wenn Sie im eine IPv6-Adresse zuweisen möchten `-address` Option:

   a. Verwenden Sie die `network ndp prefix show` Befehl zum Anzeigen der Liste der RA-Präfixe, die auf verschiedenen Schnittstellen gelernt wurden.

      Der `network ndp prefix show` Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

   b. Verwenden Sie das Format `prefix:id` Um die IPv6-Adresse manuell zu erstellen.

      `prefix` Ist das Präfix auf verschiedenen Schnittstellen gelernt.

   Für die Ableitung der `id`, Wählen Sie eine zufällige 64-Bit-Hexadezimalzahl aus.

3. Überprüfen Sie, ob das LIF erfolgreich mit dem erstellt wurde `network interface show` Befehl.
4. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Mit dem folgenden Befehl wird gezeigt, wie eine S3-Daten-LIF erstellt wird, die dem zugewiesen ist `my-S3-policy` Service-Richtlinie:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird mit einer IPv6-Adresse konfiguriert:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Erstellen von Intercluster LIFs für Remote FabricPool Tiering

Wenn Sie Cloud-Tiering (Remote FabricPool Capacity) mit ONTAP S3 aktivieren, müssen Sie Intercluster LIFs konfigurieren. Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerk-Port muss für den Administrator konfiguriert

worden sein `up` Status:

- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.

Über diese Aufgabe

Intercluster LIFs sind für das lokale Fabric Pool Tiering oder für die Bereitstellung externer S3-Applikationen nicht erforderlich.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Im folgenden Beispiel werden die Netzwerkports in angezeigt `cluster01`:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Intercluster-LIFs auf der System-SVM erstellen:

   `network interface create -vserver Cluster -lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

   Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

   `network interface show –service-policy default-intercluster -failover`

   Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf dem `e0c` Ein Failover des Ports zum erfolgt `e0d` Port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Erstellen Sie den S3-Objektspeicher-Server

Der ONTAP Objektspeicher-Server managt Daten als S3-Objekte, anstatt von Datei- oder Block-Storage, der von ONTAP NAS- und SAN-Servern bereitgestellt wird.

Bevor Sie beginnen

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den die Clients für den S3-Zugriff verwenden. Der FQDN darf nicht mit einem Bucket-Namen beginnen. Beim Zugriff auf Buckets im Virtual-Hosted-Stil wird der Servername als verwendet `mydomain.com`. `bucketname.mydomain.com`Beispiel: .

Sie sollten über ein selbstsigniertes CA-Zertifikat (erstellt in vorherigen Schritten) oder ein Zertifikat, das von einem externen CA-Anbieter signiert wurde. Ein CA-Zertifikat ist nicht erforderlich für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Traffic nur über die Cluster LIFs erfolgt.

Über diese Aufgabe

Wenn ein Objektspeicher-Server erstellt wird, wird ein Root-Benutzer mit UID 0 erstellt. Für diesen Root-Benutzer wird kein Zugriffsschlüssel oder geheimer Schlüssel generiert. Der ONTAP-Administrator muss den ausführen `object-store-server users regenerate-keys` Befehl zum Festlegen des Zugriffsschlüssels und des Geheimschlüssels für diesen Benutzer.

> Verwenden Sie als NetApp Best Practice diesen Root-Benutzer nicht. Alle Client-Anwendungen, die den Zugriffsschlüssel oder den geheimen Schlüssel des Root-Benutzers verwenden, haben vollständigen Zugriff auf alle Buckets und Objekte im Objektspeicher.

Siehe `vserver object-store-server` Man-Pages für zusätzliche Konfigurations- und Anzeigeoptionen.

Beispiel 2. Schritte

System Manager

Gehen Sie folgendermaßen vor, wenn Sie einer vorhandenen Storage-VM einen S3-Server hinzufügen. Informationen zum Hinzufügen eines S3-Servers zu einer neuen Storage-VM finden Sie unter "Erstellung einer Storage-SVM für S3".

Sie sollten darauf vorbereitet sein, IP-Adressen für die Schnittstellenrollendaten einzugeben.

1. Aktivieren von S3 auf einer vorhandenen Storage-VM
   a. Wählen Sie die Speicher-VM aus: Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **S3**.
   b. Klicken Sie auf **S3** aktivieren und geben Sie dann den S3-Servernamen ein.
   c. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.

   d. Geben Sie die Netzwerkschnittstellen ein.
2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   - Der Geheimschlüssel wird nicht mehr angezeigt.
   - Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Erstellen des S3-Servers:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   Sie können weitere Optionen beim Erstellen des S3-Servers oder zu einem späteren Zeitpunkt festlegen.

   - Beim Konfigurieren von lokalem Tiering kann der SVM-Name entweder ein Daten-SVM- oder ein System-SVM-(Cluster-)Name sein.
   - Der Zertifikatname sollte der Name des Serverzertifikats (Endbenutzer- oder Leaf-Zertifikat) und nicht das Server-CA-Zertifikat (Zwischen- oder Stammzertifizierungsstellenzertifikat) sein.
   - HTTPS ist standardmäßig an Port 443 aktiviert. Sie können die Portnummer mit dem ändern `-secure-listener-port` Option.

     Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die korrekte Integration mit SSL/TLS erforderlich. Ab ONTAP 9.15.1 wird TLS 1.3 auch für S3-Objektspeicher unterstützt.

   - HTTP ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wartet der Server an Port 80. Aktivieren Sie die Aktivierung mit dem `-is-http-enabled` Oder ändern Sie die Portnummer mit `-listener-port` Option.

Wenn HTTP aktiviert ist, werden die Anforderung und die Antworten im Klartext über das Netzwerk gesendet.

2. Vergewissern Sie sich, dass S3 konfiguriert ist:

```
vserver object-store-server show
```

Beispiel

Mit diesem Befehl werden die Konfigurationswerte aller Objektspeicher-Server überprüft:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```