S3-Zugriff auf eine SVM konfigurieren

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-config/create-svm-s3-task.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

S3-Zugriff auf eine SVM konfigurieren 1
Eine SVM für ONTAP S3 erstellen 1
Erstellen und Installieren eines CA-Zertifikats auf einer ONTAP S3-fähigen SVM 3
Die ONTAP S3 Service-Datenrichtlinie erstellen 6
Daten-LIFs für ONTAP S3 erstellen 7
Intercluster-LIFs für Remote FabricPool Tiering mit ONTAP S3 erstellen 10
ONTAP S3 Objektspeicher-Server erstellen 12

S3-Zugriff auf eine SVM konfigurieren

Eine SVM für ONTAP S3 erstellen

Obwohl S3 in einer SVM mit anderen Protokollen koexistieren kann, kann es sinnvoll sein, eine neue SVM zu erstellen, um den Namensraum und die Arbeitslast zu isolieren.

Über diese Aufgabe

Wenn Sie S3 Objektspeicher ausschließlich über eine SVM bereitstellen, benötigt der S3 Server keine DNS-Konfiguration. Wenn jedoch andere Protokolle verwendet werden, kann eine DNS-Konfiguration auf der SVM sinnvoll sein.

Wenn Sie den S3-Zugriff auf eine neue Storage-VM mithilfe des System Manager konfigurieren, werden Sie aufgefordert, Zertifikats- und Netzwerkinformationen einzugeben, und die Storage-VM sowie der S3-Objektspeicherserver werden in einem einzigen Vorgang erstellt.

Beispiel 1. Schritte

System Manager

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollqualifizierten Domänennamen (FQDN) einzugeben, den 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 Schnittstellenrolle Data einzugeben.

Wenn Sie ein von einer externen Zertifizierungsstelle signiertes Zertifikat verwenden, erfolgt während dieses Vorgangs eine Aufforderung zur Eingabe; alternativ besteht die Möglichkeit, ein systemgeneriertes Zertifikat zu verwenden.

1. S3 auf einer Storage-VM aktivieren.

   a. Eine neue Storage-VM hinzufügen: **Speicher > Storage-VMs** auswählen und dann auf **Hinzufügen** klicken.

      Falls es sich um ein neues System ohne vorhandene Storage-VMs handelt: **Dashboard > Protokolle konfigurieren** auswählen.

   Wenn Sie einen S3-Server zu einer bestehenden Storage-VM hinzufügen, auf **Speicher > Storage-VMs** klicken, eine Storage-VM auswählen, auf **Einstellungen** klicken und dann ⚙ unter **S3** klicken.

   a. **S3 aktivieren** auswählen und anschließend den S3-Servernamen eingeben.

   b. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.

   c. Die Netzwerkschnittstellen eingeben.

2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   - Der geheime Schlüssel wird nicht erneut angezeigt.

- Falls Sie die Zertifikatsinformationen erneut benötigen: **Speicher > Speicher-VMs** auswählen, die Speicher-VM auswählen und auf **Einstellungen** klicken.

CLI

1. Es sollte überprüft werden, ob S3 auf Ihrem Cluster lizenziert ist:

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

   Falls dies nicht der Fall ist, kontaktieren Sie Ihren Vertriebsmitarbeiter.

2. Eine 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>
   ```

   - Die UNIX-Einstellung für die `-rootvolume-security-style` Option verwenden.
   - Die Standardoption C.UTF-8 `-language` kann verwendet werden.
   - Die `ipspace` Einstellung ist optional.

3. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden:

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

   Das `Vserver Operational State`Feld muss den `running`Status anzeigen. Wenn es den `initializing`Status anzeigt, bedeutet dies, dass ein Zwischenvorgang wie die Erstellung des Root-Volumes fehlgeschlagen ist und die SVM gelöscht und neu erstellt werden muss.

Beispiele

Der folgende Befehl erstellt eine SVM für den Datenzugriff im IPspace ipspaceA:

```
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, das automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine Standard-Export-Richtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird. Standardmäßig wird das vsadmin-Benutzerkonto erstellt und befindet sich im `locked` Status. Die vsadmin-Rolle ist dem Standard-vsadmin-Benutzerkonto 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 eines CA-Zertifikats auf einer ONTAP S3-fähigen SVM

S3-Clients benötigen ein Zertifikat einer Zertifizierungsstelle (CA), um HTTPS-Datenverkehr an die S3-fähige SVM zu senden. CA-Zertifikate schaffen eine Vertrauensbeziehung zwischen Clientanwendungen und dem ONTAP Objektspeicher-Server. Ein CA-Zertifikat sollte auf ONTAP installiert werden, bevor es als Objektspeicher für Remote-Clients genutzt wird.

Über diese Aufgabe

Obwohl es möglich ist, einen S3-Server so zu konfigurieren, dass er nur HTTP verwendet, und obwohl es möglich ist, Clients ohne CA-Zertifikatsanforderung zu konfigurieren, gilt es als bewährte Methode, den HTTPS-Datenverkehr zu ONTAP S3-Servern mit einem CA-Zertifikat abzusichern.

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

Die Anweisungen in diesem Verfahren erstellen und installieren ein selbstsigniertes ONTAP-Zertifikat. Obwohl ONTAP selbstsignierte Zertifikate generieren kann, wird die Verwendung signierter Zertifikate von einer

Drittanbieter-Zertifizierungsstelle als empfohlene Best Practice angesehen; weitere Informationen enthält die Administrator-Authentifizierungsdokumentation.

"Administratorauthentifizierung und RBAC"

Weitere Informationen zu `security certificate` und zusätzlichen Konfigurationsoptionen finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Ein selbstsigniertes digitales Zertifikat erstellen:

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

   Die `-type root-ca`Option erstellt und installiert ein selbstsigniertes digitales Zertifikat, das zum Signieren anderer Zertifikate dient, indem es als Zertifizierungsstelle (CA) fungiert.

   Die `-common-name`Option erstellt den Certificate Authority (CA)-Namen der SVM und wird beim Generieren des vollständigen Namens des Zertifikats verwendet.

   Die Standardzertifikatsgröße 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, sollte dieser für spätere Schritte in diesem Verfahren gespeichert werden.

   Weitere Informationen zu `security certificate create` finden sich in der "ONTAP-Befehlsreferenz".

2. Eine Zertifikatsignierungsanforderung generieren:

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

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

   Sie können bei Bedarf den Standort und weitere detaillierte Informationen zur SVM angeben.

   Der `-dns-name`Parameter wird häufig von Clients benötigt, um die Subject Alternate Name-Erweiterung anzugeben, die eine Liste von DNS-Namen bereitstellt.

   Der `-ipaddr`Parameter wird häufig von Clients benötigt, um die Subject Alternate Name-Erweiterung anzugeben, die eine Liste von IP-Adressen bereitstellt.

   Sie werden aufgefordert, eine Kopie Ihrer Zertifikatsanforderung und Ihres privaten Schlüssels für

zukünftige Referenz aufzubewahren.

Weitere Informationen zu `security certificate generate-csr` finden sich in der "ONTAP-Befehlsreferenz".

3. Der CSR wird mit SVM_CA signiert, um das Zertifikat des S3 Servers 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 den vorherigen Schritten verwendet haben:

   - `-ca` — der gebräuchliche Name der CA, den Sie in Schritt 1 eingegeben haben.
   - `-ca-serial` — die CA-Seriennummer aus Schritt 1. Wenn beispielsweise der Name des CA-Zertifikats svm1_ca_159D1587CE21E9D4_svm1_ca ist, ist die Seriennummer 159D1587CE21E9D4.

     Standardmäßig läuft das signierte Zertifikat nach 365 Tagen ab. Es kann ein anderer Wert ausgewählt und weitere Signaturdetails angegeben werden.

     Wenn Sie dazu aufgefordert werden, kopieren und geben Sie die in Schritt 2 gespeicherte Zertifikatsanforderungszeichenfolge ein.

   Ein signiertes Zertifikat wird angezeigt; dieses für die spätere Verwendung speichern.

4. Das signierte Zertifikat auf der S3-fähigen SVM installieren:

   `security certificate install -type server -vserver` *`svm_name`*

   Bei Aufforderung sind das Zertifikat und der private Schlüssel einzugeben.

   Sie haben die Möglichkeit, Zwischenzertifikate einzugeben, falls eine Zertifikatskette gewünscht ist.

   Wenn der private Schlüssel und das von der Zertifizierungsstelle signierte digitale Zertifikat angezeigt werden, sollten diese für eine spätere Referenz gespeichert werden.

5. Öffentliches Schlüsselzertifikat:

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

   Das öffentliche Schlüsselzertifikat für die spätere Client-seitige Konfiguration speichern.

   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
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "Sicherheitszertifikat signieren"

Die ONTAP S3 Service-Datenrichtlinie erstellen

Sie können Dienstrichtlinien für S3-Daten- und Verwaltungsdienste erstellen. Eine S3-Daten-Dienstrichtlinie ist erforderlich, um den S3-Datenverkehr auf LIFs zu ermöglichen.

Über diese Aufgabe

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

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

Obwohl für SVMs und LIFs mehrere Protokolle konfiguriert werden können, ist es eine Best Practice, dass S3 das einzige Protokoll bei der Bereitstellung von Objektdaten ist.

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. Erstellen einer Dienstdatenrichtlinie:

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

Die `data-core`- und `data-s3-server`-Dienste sind die einzigen, die für die Aktivierung von ONTAP S3 erforderlich sind, obwohl bei Bedarf weitere Dienste eingeschlossen werden können.

Weitere Informationen zu `network interface service-policy create` finden sich in der "ONTAP-Befehlsreferenz".

Daten-LIFs für ONTAP S3 erstellen

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

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Wenn geplant ist, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für ein LIF zuzuweisen, muss das Subnetz bereits existieren.

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

  Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

- Die LIF-Servicerichtlinie muss bereits existieren.
- Als Best Practice sollten LIFs, die für den Datenzugriff (data-s3-server) verwendet werden, und LIFs, die für Verwaltungsoperationen (management-https) verwendet werden, getrennt sein. Beide Dienste sollten nicht auf demselben LIF aktiviert sein.
- DNS-Einträge sollten nur die IP-Adressen der LIFs enthalten, denen ein data-s3-server zugeordnet ist. Wenn im DNS-Eintrag IP-Adressen anderer LIFs angegeben sind, können ONTAP S3-Anfragen von anderen Servern bearbeitet werden, was zu unerwarteten Antworten oder Datenverlust führen kann.

Über diese Aufgabe

- Sowohl IPv4- als auch IPv6-LIFs können auf demselben Netzwerkport erstellt werden.
- Wenn Sie eine große Anzahl von LIFs in Ihrem Cluster haben, kann die vom Cluster unterstützte LIF-Kapazität mit dem `network interface capacity show` Befehl und die von jedem Knoten unterstützte LIF-Kapazität mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsstufe) überprüft werden.

  Weitere Informationen zu `network interface capacity show` und `network interface capacity details show` finden sich in der "ONTAP-Befehlsreferenz".

- Wenn Sie Remote-FabricPool-Kapazitäts-(Cloud)-Tiering aktivieren, müssen Sie auch Intercluster-LIFs konfigurieren.

Schritte

1. Eine 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 Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".

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

- `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option ermöglichen.
- Wird ein Subnetz zur Bereitstellung der IP-Adresse und der Netzwerkmaske verwendet, wird, falls das Subnetz mit einem Gateway definiert wurde, beim Erstellen eines LIF mit diesem Subnetz automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt.
- Wenn Sie IP-Adressen manuell zuweisen (ohne Verwendung eines Subnetzes), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, falls sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Weitere Informationen zu `network route create` und zum Erstellen einer statischen Route innerhalb einer SVM finden sich im "ONTAP-Befehlsreferenz".
- Für die `-firewall-policy` Option sollte derselbe Standardwert `data` wie für die LIF-Rolle verwendet werden.

  Bei Bedarf kann später eine benutzerdefinierte Firewall-Richtlinie erstellt und hinzugefügt werden.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für LIFs konfigurieren".

- `-auto-revert`Hiermit kann festgelegt werden, ob ein Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen einer Netzwerkverbindung automatisch auf seinen Heimatknoten zurückkehrt. Die Standardeinstellung ist `false, sie kann jedoch je nach Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf `false` gesetzt werden.
- Die `-service-policy` Option legt die von Ihnen erstellte Daten- und Verwaltungsdienstrichtlinie sowie alle weiteren benötigten Richtlinien fest.

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

   a. Mit dem `network ndp prefix show` Befehl lässt sich die Liste der auf verschiedenen Schnittstellen gelernten RA-Präfixe anzeigen.

      Der `network ndp prefix show` Befehl ist auf der Stufe „Erweiterte Berechtigungen“ verfügbar.

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

      `prefix` ist das Präfix, das auf verschiedenen Schnittstellen gelernt wird.

   Zur Ableitung des `id`wird eine zufällige 64-Bit-Hexadezimalzahl gewählt.

3. Es kann mit dem `network interface show` Befehl überprüft werden, ob die LIF erfolgreich erstellt

wurde.

4. Es sollte überprüft werden, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Der folgende Befehl zeigt, wie ein S3-Daten-LIF erstellt wird, dem die `my-S3-policy` Dienstrichtlinie zugewiesen ist:

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

Der folgende Befehl zeigt alle LIFs in cluster-1 an. Die Data LIFs datalif1 und datalif3 sind mit IPv4-Adressen konfiguriert, und datalif4 ist 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.
```

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"
- "network ndp prefix show"

Intercluster-LIFs für Remote FabricPool Tiering mit ONTAP S3 erstellen

Wenn Sie die Remote FabricPool Kapazitäts-Tiering (Cloud) mit ONTAP S3 aktivieren, müssen Intercluster-LIFs konfiguriert werden. Intercluster-LIFs können auf Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden. Dadurch wird die Anzahl der für die Intercluster-Vernetzung benötigten Ports reduziert.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Die LIF-Servicerichtlinie muss bereits existieren.

Über diese Aufgabe

Intercluster LIFs sind weder für das lokale FabricPool Tiering noch für die Bereitstellung externer S3-Anwendungen erforderlich.

Schritte

1. Die Ports im Cluster werden aufgelistet:

   ```
   network port show
   ```

   Das folgende Beispiel zeigt die Netzwerkanschlüsse in `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
```

Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

2. Intercluster-LIFs auf dem 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`*

   Das folgende Beispiel erstellt Intercluster-LIFs `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
```

   Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, 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. Es sollte sichergestellt werden, dass die Intercluster-LIFs redundant sind:

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

   Das folgende Beispiel zeigt, dass die Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` auf dem `e0c` Port auf den `e0d` Port übergehen.

```
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
```

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP S3 Objektspeicher-Server erstellen

Der ONTAP Objektspeicher-Server verwaltet Daten als S3-Objekte, im Gegensatz zum Datei- oder Blockspeicher, der von ONTAP NAS- und SAN-Servern bereitgestellt wird.

Bevor Sie beginnen

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollqualifizierten Domänennamen (FQDN) anzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN ist ab ONTAP 9.18.1 erforderlich. Der FQDN darf nicht mit einem Bucket-Namen beginnen. Beim Zugriff auf Buckets mit virtual-hosted-style wird der Servername als `mydomain.com` verwendet. Zum Beispiel `bucketname.mydomain.com`.

Sie benötigen ein selbstsigniertes CA-Zertifikat (das in den vorherigen Schritten erstellt wurde) oder ein von einem externen CA-Anbieter signiertes Zertifikat. Ein CA-Zertifikat ist für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Verkehr ausschließlich über Cluster-LIFs erfolgt, nicht erforderlich.

Über diese Aufgabe

Wenn ein Objektspeicherserver erstellt wird, wird ein Root-Benutzer mit der UID 0 angelegt. Für diesen Root-Benutzer werden kein Zugriffsschlüssel und kein geheimer Schlüssel generiert. Der ONTAP Administrator

muss den `object-store-server user regenerate-keys` Befehl ausführen, um den Zugriffsschlüssel und den geheimen Schlüssel für diesen Benutzer festzulegen.

> Als NetApp Best Practice sollte dieser Root-Benutzer nicht verwendet werden. Jede Clientanwendung, die den Zugriffsschlüssel oder den geheimen Schlüssel des Root-Benutzers verwendet, hat vollen Zugriff auf alle Buckets und Objekte im Objektspeicher.

Weitere Informationen zu `vserver object-store-server` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel 2. Schritte

System Manager

Verwenden Sie dieses Verfahren, wenn Sie einen S3-Server zu einer bestehenden Storage-VM hinzufügen. Um einen S3-Server zu einer neuen Storage-VM hinzuzufügen, siehe "Eine Storage-SVM für S3 erstellen".

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

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

      Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.

   d. Die Netzwerkschnittstellen eingeben.
2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   - Der geheime Schlüssel wird nicht erneut angezeigt.
   - Falls Sie die Zertifikatsinformationen erneut benötigen: **Speicher > Speicher-VMs** auswählen, die Speicher-VM auswählen und auf **Einstellungen** klicken.

CLI

1. Den S3-Server erstellen:

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

   Zusätzliche Optionen können beim Erstellen des S3-Servers oder jederzeit später angegeben werden.

   - Ab ONTAP 9.20.1 können Sie mit der Option `-default-bucket-size` die Größe von S3-Buckets festlegen, die ohne die Option `-size` erstellt werden. Diese Einstellung gilt für Buckets, die mit der ONTAP CLI, der ONTAP REST API oder der S3 API erstellt werden. Vorhandene Buckets werden dadurch nicht geändert.

     Nach dem Erstellen des S3-Servers lässt sich mit dem `vserver object-store-server modify`Befehl

über die `-default-bucket-size`Option die Standardgröße für neue Buckets ändern.

- Wenn lokales Tiering konfiguriert wird, kann der SVM-Name entweder ein Daten-SVM-Name oder ein System-SVM-Name (Cluster-Name) sein.
- Der Zertifikatsname sollte der Name des Serverzertifikats (Endbenutzer- oder Blattzertifikat) sein und nicht der Name des Server-CA-Zertifikats (Zwischen- oder Stammzertifizierungsstellenzertifikat).
- HTTPS ist standardmäßig auf Port 443 aktiviert. Die Portnummer kann mit der `-secure -listener-port` Option geändert werden.

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

- HTTP ist standardmäßig deaktiviert. Wenn aktiviert, hört der Server auf Port 80. HTTP kann mit der `-is-http-enabled` Option aktiviert oder die Portnummer mit der `-listener-port` Option geändert werden.

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

2. Es sollte überprüft werden, ob S3 konfiguriert ist:

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

Beispiel

Dieser Befehl überprüft die Konfigurationswerte aller Objektspeicherserver:

```
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
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.