SVM への S3 アクセスを設定する

ONTAP 9

NetApp
September 12, 2024

目次

SVM への S3 アクセスを設定する . . . 1
S3 用の SVM を作成します . . . 1
CA 証明書を作成して SVM にインストールします . . . 4
S3 サービスデータポリシーを作成する . . . 7
データ LIF を作成します。 . . . 7
リモートの FabricPool 階層化用にクラスタ間 LIF を作成する . . . 10
S3 オブジェクトストアサーバを作成します . . . 13

SVM への S3 アクセスを設定する

S3 用の SVM を作成します

S3はSVM内で他のプロトコルと共存できますが、新しいSVMを作成してネームスペースとワークロードを分離することもできます。

このタスクについて

SVMからS3オブジェクトストレージのみを提供する場合は、S3サーバでDNS設定を行う必要はありません。ただし、他のプロトコルを使用する場合は、 SVM に DNS を設定できます。

System Managerを使用して新しいStorage VMへのS3アクセスを設定すると、証明書とネットワークの情報を入力するように求められ、Storage VMとS3オブジェクトストレージサーバは一度に作成されます。

例 **1.** 手順

System Manager の略

S3サーバ名を完全修飾ドメイン名（FQDN）として入力できるようにして、クライアントがS3アクセスに使用できるようにしておく必要があります。S3サーバのFQDNの先頭をバケット名にすることはできません。

インターフェイスロールデータ用のIPアドレスを入力する準備をしておく必要があります。

外部 CA 署名証明書を使用している場合は、この手順中に証明書の入力を求められます。システムで生成された証明書を使用することもできます。

1. Storage VM で S3 を有効にします。

   a. 新しいStorage VMを追加します。[* Storage（ストレージ）]>[Storage VMs]をクリックし、[* Add（追加）]をクリックします。

      既存のStorage VMがない新しいシステムの場合は、*ダッシュボード>プロトコルの設定*をクリックします。

   既存のStorage VMにS3サーバを追加する場合は、**[**ストレージ**]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、 S3 *の下をクリックし ます。

   a. Enable S3 * をクリックし、 S3 Server Name を入力します。
   b. 証明書のタイプを選択します。

      システムで生成された証明書と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。

   c. ネットワークインターフェイスを入力してください。

2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。
   - シークレットキーは今後表示されません。
   - 証明書情報が再度必要な場合は、[*ストレージ]、[Storage VMs]の順にクリックし、Storage VMを選択して、[*設定]をクリックします。

CLI の使用

1. クラスタ上で S3 のライセンスが有効であることを確認します。

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

   表示されない場合は、営業担当者にお問い合わせください。

2. SVM を作成します。

```
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>
```

- にUNIX設定を使用します `-rootvolume-security-style` オプション
- デフォルトのC.UTF-8を使用します `-language` オプション
- 。 `ipspace` 設定はオプションです。

3. 新しく作成した SVM の設定とステータスを確認します。

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

。 `Vserver Operational State` フィールドにはを表示する必要があります `running` 状態。が表示された場合 `initializing` 状態にすると、ルートボリュームの作成などの中間処理が失敗したため、SVMを削除して再作成する必要があります。

例

次のコマンドは、データアクセス用の SVM を IPspace ipspaceA 内に作成します。

```
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
```

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されてに追加されたことを示しています `running` 状態。ルートボリュームには、ルールを含まないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。デフォルトでは、vsadminユーザアカウントが作成され、に配置されます `locked` 状態。vsadmin ロールがデフォルトの vsadmin ユーザアカウントに割り当てられます。

```
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
```

CA 証明書を作成して SVM にインストールします

S3 クライアントから S3 対応 SVM への HTTPS トラフィックを有効にするには、認証局（ CA ）証明書が必要です。

このタスクについて

HTTP のみを使用するように S3 サーバを設定することは可能ですが、 CA 証明書が不要なクライアントを設定することも可能です。ただし、 ONTAP S3 サーバへの HTTPS トラフィックを CA 証明書を使用して保護することを推奨します。

IP トラフィックがクラスタ LIF のみを経由するローカル階層化の場合、 CA 証明書は必要ありません。

この手順に記載されている手順では、 ONTAP 自己署名証明書を作成してインストールします。サードパーティベンダーの CA 証明書もサポートされています。詳細については、管理者認証のドキュメントを参照してください。

"管理者認証と RBAC"

を参照してください `security certificate` 追加の設定オプションのマニュアルページ

手順

1. 自己署名デジタル証明書を作成します。

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

   。 `-type root-ca` オプションは、認証局（CA）として機能して他の証明書に署名するための自己署名デジタル証明書を作成してインストールします。

   。 `-common-name` オプションを指定すると、SVMの認証局（CA）名が作成され、証明書の完全な名前を生成するときに使用されます。

   デフォルトの証明書サイズは 2048 ビットです。

   例

   ```
   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
   ```

   生成された証明書の名前が表示されたら、この手順の以降の手順で名前を保存してください。

2. 証明書署名要求を生成します。

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

   。 `-common-name` 署名要求のパラメータには、S3サーバ名（FQDN）を指定する必要があります。

   必要に応じて、 SVM の場所やその他の詳細情報を指定できます。

   今後の参照用に、証明書要求と秘密鍵のコピーを保管するように求められます。

3. SVM_CA を使用して CSR に署名し、 S3 サーバの証明書を生成します。

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

   前の手順で使用したコマンドオプションを入力します。

   - `-ca` --ステップ1で入力したCAの共通名。
   - `-ca-serial` --ステップ1のCAシリアル番号。たとえば、 CA 証明書の名前が svm1_ca_159D1587CE21E9D4_svm1_ca の場合、シリアル番号は 159D1587CE21E9D4 です。

     デフォルトでは、署名済み証明書の有効期限は 365 日です。別の値を選択し、他の署名の詳細を指定できます。

     プロンプトが表示されたら、手順 2 で保存した証明書要求文字列をコピーして入力します。

署名済み証明書が表示されます。あとで使用できるように保存しておきます。

4. S3 対応 SVM に署名済み証明書をインストールします。

   `security certificate install -type server -vserver svm_name`

   プロンプトが表示されたら、証明書と秘密鍵を入力します。

   証明書チェーンが必要な場合は、中間証明書を入力できます。

   秘密鍵と CA 署名デジタル証明書が表示されたら、あとで参照できるように保存します。

5. 公開鍵証明書を取得します。

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

   公開鍵証明書を保存しておき、以降のクライアント側の設定に使用します。

   例

```
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
```

S3 サービスデータポリシーを作成する

S3 のデータサービスと管理サービスのサービスポリシーを作成できます。LIF 上の S3 データトラフィックを有効にするには、 S3 サービスデータポリシーが必要です。

このタスクについて

データ LIF とクラスタ間 LIF を使用する場合は、 S3 サービスデータポリシーが必要です。ローカル階層化のユースケースにクラスタ LIF を使用している場合は必要ありません。

LIF にサービスポリシーを指定すると、そのポリシーを使用して LIF のデフォルトロール、フェイルオーバーポリシー、データプロトコルのリストが作成されます。

SVM と LIF には複数のプロトコルを設定できますが、オブジェクトデータを提供する際には S3 だけを使用することを推奨します。

手順

1. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

2. サービスデータポリシーを作成します。

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

   。 `data-core` および `data-s3-server` ONTAP S3を有効にするために必要なサービスはサービスだけですが、必要に応じて他のサービスも含めることができます。

データ LIF を作成します。

新しい SVM を作成した場合、 S3 アクセス用に作成する専用の LIF はデータ LIF です。

作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります `up` ステータス。
- サブネット名を使用して LIF の IP アドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF サービスポリシーがすでに存在している必要があります。
- ベストプラクティスとして、データアクセスに使用するLIF（data-s3-server）と管理処理に使用するLIF（management-https）を別 々 に配置することを推奨します。同じLIFで両方のサービスを有効にしないでください。
- DNSレコードには、data-s3-serverが関連付けられているLIFのIPアドレスだけを含める必要があります。他のLIFのIPアドレスがDNSレコードに指定されていると、ONTAP S3要求が他のサーバから処理され、予期しない応答が返される可能性があります。

このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- クラスタ内のLIFの数が多い場合は、を使用して、クラスタでサポートされるLIFの容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。
- リモートの FabricPool 容量（クラウド）階層化を有効にする場合は、クラスタ間 LIF も設定する必要があります。

手順

1. LIF を作成します。

   `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` は、の実行時にLIFが戻るノードです `network interface revert` LIFに対してコマンドを実行します。

     を使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert` オプション

   - `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
   - でIPアドレスを指定できます `-address` および `-netmask` オプションを選択するか、を使用してサブネットからの割り当てを有効にします `-subnet_name` オプション
   - サブネットを使用して IP アドレスとネットワークマスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用して LIF を作成するときにゲートウェイへのデフォルトルートが SVM に自動的に追加されます。
   - サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合にゲートウェイへのデフォルトルートの設定が必要になることがあります。。 `network route create` のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
   - をクリックします `-firewall-policy` オプションで、同じデフォルトを使用します `data` をLIFのロールとして使用します。

     必要に応じて、カスタムファイアウォールポリシーをあとから作成して追加できます。

     > ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシーに置き換えられました。詳細については、を参照してください "LIF のファイアウォールポリシーを設定します"。

   - `-auto-revert` 起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルト設定はです `false`に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。
   - 。 `-service-policy` optionは、作成したデータサービスポリシーと管理サービスポリシー、およびその他の必要なポリシーを指定します。

2. でIPv6アドレスを割り当てる場合 `-address` オプション：

   a. を使用します `network ndp prefix show` さまざまなインターフェイスで学習されたRAプレフィックスのリストを表示するコマンド。

      。 `network ndp prefix show` コマンドはadvanced権限レベルで使用できます。

   b. の形式を使用します `prefix:id` IPv6アドレスを手動で作成します。

      `prefix` は、さまざまなインターフェイスで学習されたプレフィックスです。

   を導出するため `id` で、ランダムな64ビット16進数を選択します。

3. を使用して、LIFが正常に作成されたことを確認します `network interface show` コマンドを実行します

4. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドは、に割り当てられたS3データLIFを作成する方法を示しています `my-S3-policy` サービスポリシー：

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

次のコマンドは、 cluster-1 内のすべての LIF を表示します。datalif1 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、 datalif4 には IPv6 アドレスを設定しています。

```
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.
```

リモートの **FabricPool** 階層化用にクラスタ間 **LIF** を作成する

ONTAP S3 を使用してリモートの FabricPool 容量（クラウド）階層化を有効にする場合は、クラスタ間 LIF を設定する必要があります。データネットワークと共有するポートにクラスタ間 LIF を設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります `up` ステータス。

- LIF サービスポリシーがすでに存在している必要があります。

このタスクについて

ローカルのファブリックプールの階層化や外部の S3 アプリケーションへの提供にクラスタ間 LIF は必要ありません。

手順

1. クラスタ内のポートの一覧を表示します。

   `network port show`

   次の例は、のネットワークポートを示しています `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. システム SVM にクラスタ間 LIF を作成します。

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

   次の例は、クラスタ間LIFを作成します `cluster01_icl01` および `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. クラスタ間 LIF が作成されたことを確認します。

   `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. クラスタ間 LIF が冗長構成になっていることを確認します。

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

   次の例は、クラスタ間LIFを示しています `cluster01_icl01` および `cluster01_icl02` をクリックします `e0c` ポートはにフェイルオーバーします `e0d` ポート：

```
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
```

S3 オブジェクトストアサーバを作成します

ONTAP オブジェクトストアサーバは、 ONTAP NAS サーバおよび SAN サーバが提供するファイルストレージまたはブロックストレージではなく、データを S3 オブジェクトとして管理します。

作業を開始する前に

クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。FQDNの1文字目をバケット名にすることはできません。仮想ホスト形式を使用してバケットにアクセスする場合は、サーバ名がとして使用されます `mydomain.com`。たとえば、 `bucketname.mydomain.com`です。

自己署名 CA 証明書（前の手順で作成）または外部 CA ベンダーが署名した証明書が必要です。IP トラフィックがクラスタ LIF のみを経由するローカル階層化の場合、 CA 証明書は必要ありません。

このタスクについて

オブジェクトストアサーバを作成すると、 UID 0 の root ユーザが作成されます。この root ユーザに対してアクセスキーもシークレットキーも生成されません。ONTAP 管理者はを実行する必要があります `object-store-server users regenerate-keys` コマンドを使用して、このユーザのアクセスキーとシークレットキーを設定します。

> ネットアップのベストプラクティスとして、この root ユーザは使用しないでください。root ユーザのアクセスキーまたはシークレットキーを使用するクライアントアプリケーションは、オブジェクトストア内のすべてのバケットとオブジェクトにフルアクセスできます。

を参照してください `vserver object-store-server` 追加の設定オプションおよび表示オプションのマニュアルページ

例 **2.** 手順

System Manager の略

既存のStorage VMにS3サーバを追加する場合は、この手順 を使用します。新しいStorage VMにS3サーバを追加する方法については、を参照してください "S3用のストレージSVMを作成します"。

インターフェイスロールデータ用のIPアドレスを入力する準備をしておく必要があります。

1. 既存のStorage VMでS3を有効にします。
   a. Storage VMを選択します。**[**ストレージ**]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[S3]*の下をクリックします ⚙ 。
   b. Enable S3 * をクリックし、 S3 Server Name を入力します。
   c. 証明書のタイプを選択します。

      システムで生成された証明書と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。

   d. ネットワークインターフェイスを入力してください。
2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。
   - シークレットキーは今後表示されません。
   - 証明書情報が再度必要な場合は、 [* ストレージ] 、 [Storage VMs] の順にクリックし、 Storage VM を選択して、 [* 設定] をクリックします。

CLI の使用

1. S3 サーバを作成します。

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

   S3 サーバの作成時またはあとからいつでも追加のオプションを指定できます。

   - ローカルの階層化を設定する場合は、SVM名にデータSVM名またはシステムSVM（クラスタ）名を指定できます。
   - 証明書名は、サーバCA証明書（中間またはルートCA証明書）ではなく、サーバ証明書（エンドユーザまたはリーフ証明書）の名前にする必要があります。
   - HTTPS は、ポート 443 でデフォルトで有効になっています。ポート番号はを使用して変更できます `-secure-listener-port` オプション

     HTTPSを有効にすると、SSL/TLSと正しく統合するためにCA証明書が必要になります。ONTAP 9.15.1以降では、S3オブジェクトストレージでTLS 1.3がサポートされます。

   - HTTPはデフォルトで無効になっています。有効にすると、サーバはポート80でリスンします。を使用して有効にできます `-is-http-enabled` オプションを選択するか、ポート番号を `-listener-port` オプション

     HTTPが有効な場合、要求と応答はクリアテキストでネットワーク経由で送信されます。

2. S3が設定されていることを確認します。

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

例

このコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。

```
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
```