SVMへのS3アクセスの設定

ONTAP 9

NetApp
December 20, 2024

目次

SVMへのS3アクセスの設定

ONTAP S3用のSVMの作成

S3はSVM内で他のプロトコルと共存できますが、ネームスペースやワークロードを分離するために新しいSVMを作成することもできます。

タスクの内容

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サーバにDNS設定は必要ありません。ただし、他のプロトコルを使用する場合は、SVMにDNSを設定することもできます。

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情報を入力するように求められ、1回の処理でStorage VMとS3オブジェクトストレージサーバが作成されます。

例 **1.** 手順

System Manager

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。S3サーバのFQDNの1文字目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、この手順の実行中に入力するように求められます。また、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を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。

   c. ネットワークインターフェイスを入力します。

2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の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。

   - 今後シークレットキーは表示されません。
   - 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

1. クラスタでS3のライセンスが有効になっていることを確認します。

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

   サポートされていない場合は、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>
```

- オプションにはUNIX設定を使用し `-rootvolume-security-style`ます。
- デフォルトのC.UTF-8オプションを使用し `-language`ます。
- この `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`フィールドには状態が表示されている必要があり `running`ます。状態が表示された場合は `initializing`、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状態になっていることを示しています running。ルートボリュームには、ルールが含まれてい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、状態がになってい `locked`ます。vsadminロールは、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
```

ONTAP S3対応SVMにCA証明書を作成してインストールする

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。CA証明書を使用すると、クライアントアプリケーションとONTAPオブジェクトストアサーバの間に信頼された関係が作成されます。ONTAPをリモートクライアントからアクセス可能なオブジェクトストアとして使用する前に、CA証明書をインストールしておく必要があります。

タスクの内容

HTTPのみを使用するようにS3サーバを設定したり、CA証明書を必要とせずにクライアントを設定したりすることも可能ですが、ONTAP S3サーバへのHTTPSトラフィックをCA証明書で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では、CA証明書は必要ありません。

この手順では、ONTAP自己署名証明書を作成してインストールします。ONTAPでは自己署名証明書を生成できますが、サードパーティの認証局からの署名済み証明書を使用することを推奨します。詳細については、管理者の認証に関するドキュメントを参照してください。

"カンリシヤニンシヨウトRBAC"

その他の設定オプションについては、マニュアルページを参照して `security certificate`ください。

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`*

   オプションは `-type root-ca`、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。

   オプションを使用 `-common-name`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、以降の手順で使用するために保存しておきます。

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。

   あとで参照できるように、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。別の値を選択したり、他の署名の詳細を指定したりできます。

  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`

   クライアント側の設定用に公開鍵証明書を保存しておきます。

   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
```

ONTAP S3サービスデータポリシーを作成

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で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。

タスクの内容

データLIFとクラスタ間LIFを使用している場合は、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、および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の提供にはS3プロトコルのみ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`ONTAP S3を有効にするために必要なサービスはサービスと `data-s3-server`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。

ONTAP S3用のデータLIFの作成

新しいSVMを作成した場合は、S3アクセス専用のLIFとしてデータLIFを作成する必要があります。

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の管理 `up`ステータスがに設定されている必要があります。
- 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。コマンドを使用して作成し `network subnet create`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場合、ONTAP S3要求が他のサーバから処理され、予期しない応答やデータの損失が発生する可能性があります。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。
- 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、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

  オプションを使用して、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`。

- `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
- オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
- 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。
- IPアドレスを手動で（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、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。
- オプションには `-firewall-policy`、LIFのロールと同じデフォルトを使用し `data`ます。

  必要に応じて、あとからカスタムファイアウォールポリシーを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が廃止され、LIFのサービスポリシーに全面的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する"。

- `-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。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false`。
- オプションは、 `-service-policy`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. オプションでIPv6アドレスを割り当てる場合 `-address`は、次の手順を実行します。
   a. コマンドを使用して `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します。

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

   b. 形式を使用し `prefix:id`て、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。

   を生成するには `id`、ランダムな64ビット16進数を選択します。

3. コマンドを使用して、LIFが正常に作成されたことを確認します `network interface show`。
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	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

例

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

```
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とdatalif3のデータLIFにはIPv4アドレスを設定し、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.
```

ONTAP S3によるリモートFabricPool階層化用のクラスタ間LIFの作成

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。

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の管理 `up`ステータスがに設定されている必要がありま

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。

タスクの内容

クラスタ間LIFは、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 `cluster01`ます。

   ```
   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と `cluster01_icl02`を作成し `cluster01_icl01`ます。

```
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、インタークラスタLIFおよび `cluster01_icl02`ポート上の `e0c`ポートがそのポートにフェイルオーバーする `e0d`ことを示しています `cluster01_icl01`。

```
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
```

ONTAP S3オブジェクトストアサーバの作成

ONTAPオブジェクトストアサーバは、ONTAP NASサーバやSANサーバが提供するファイルストレージやブロックストレージとは対照的に、S3オブジェクトとしてデータを管理します。

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ベンダーによって署名され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では、CA証明書は必要ありません。

タスクの内容

オブジェクトストアサーバを作成すると、UIDが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やシークレットキーは生成されません。ONTAP管理者は、このユーザのアクセスキーとシークレットキーを設定するコマンドを実行する必要があります `object-store-server users regenerate-keys`。

> NetApp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には、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へのフルアクセスが付与されます。

その他の設定オプションおよび表示オプションについては、マニュアルページを参照して `vserver object-store-server`ください。

例 **2.** 手順

System Manager

この手順は、既存のStorage VMにS3サーバを追加する場合に使用します。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を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。

   d. ネットワークインターフェイスを入力します。
2. システム生成の証明書を選択した場合は、新しいStorage VMの作成を確認した時点で証明書の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。
   - 今後シークレットキーは表示されません。
   - 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

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]
   ```

   追加のオプションは、S3サーバの作成時または作成後いつでも指定できます。

   - 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ではデフォルトで有効になっています。ポート番号はオプションで変更できます `-secure-listener-port`。

     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。オプションを使用して有効にすることも、オプションを使用してポート番号を変更する `-listener-port`こともできます `-is-http-enabled`。

     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
```

著作権に関する情報

商標に関する情報