設定S3對SVM的存取

ONTAP 9

NetApp
February 12, 2026

目錄

設定S3對SVM的存取

為 ONTAP S3 建立 SVM

雖然S3可以與SVM中的其他傳輸協定共存、但您可能想要建立新的SVM來隔離命名空間和工作負載。

關於這項工作

如果您僅從SVM提供S3物件儲存設備、則S3伺服器不需要任何DNS組態。不過、如果使用其他通訊協定、您可能會想要在SVM上設定DNS。

當您使用System Manager設定S3存取新儲存VM時、系統會提示您輸入憑證和網路資訊、儲存VM和S3物件儲存伺服器會在單一作業中建立。

範例 **1.** 步驟

系統管理員

您應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將使用此名稱來存取S3。S3伺服器FQDN不得以儲存區名稱開頭。

您應準備好輸入介面角色資料的IP位址。

如果您使用的是外部CA簽署的憑證、系統會在此程序期間提示您輸入；您也可以選擇使用系統產生的憑證。

1. 在儲存VM上啟用S3。

   a. 新增儲存VM：按一下「儲存設備**>**儲存**VM**」、然後按一下「新增」。

      如果這是沒有現有儲存VM的新系統：請按一下*儀表板>設定傳輸協定*。

   如果您要將 S3 伺服器新增至現有的儲存 VM ：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * S2* 下的。

   a. 按一下「啟用**S2**」、然後輸入「S3伺服器名稱」。
   b. 選取憑證類型。

      無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。

   c. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 確認叢集上的S3已獲得授權：

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

   如果沒有、請聯絡您的銷售代表。

2. 建立SVM：

   ```
   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>
   ```

- 使用的 UNIX 設定 `-rootvolume-security-style` 選項。
- 使用預設的 C.UTF-8 `-language` 選項。
- 。 `ipspace` 設定為選用項目。

3. 驗證新建立的SVM的組態和狀態：

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

。 `Vserver Operational State` 欄位必須顯示 `running` 州/省。如果顯示 `initializing` 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會在IPspace ipspaceA中建立SVM以供資料存取：

```
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
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 `running` 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。根據預設、會建立 vsadmin 使用者帳戶、並位於中 `locked` 州/省。vsadmin角色會指派給預設的vsadmin使用者帳戶。

```
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
```

在啟用 ONTAP S3 的 SVM 上建立並安裝 CA 憑證

S3 用戶端需要憑證授權單位 (CA) 憑證才能將 HTTPS 流量傳送到啟用 S3 的 SVM。 CA 憑證在用戶端應用程式和ONTAP物件儲存伺服器之間建立信任關係。在將 ONTAP 用作遠端用戶端可存取的物件儲存之前，您應該在ONTAP上安裝 CA 憑證。

關於這項工作

雖然可以將S3伺服器設定為僅使用HTTP、而且雖然可以設定不需CA憑證的用戶端、但最佳做法是使用ONTAP CA憑證來保護HTTPS流量。

本機分層使用案例不需要CA憑證、因為IP流量只會流經叢集生命體。

本程序中的指示將建立並安裝ONTAP 一個自我簽署的驗證書。雖然 ONTAP 可以產生自我簽署的憑證，但建議最佳做法是使用協力廠商憑證授權單位所簽署的憑證；如需詳細資訊，請參閱系統管理員驗證文件。

"系統管理員驗證與RBAC"

如"指令參考資料ONTAP"需更多資訊及其他組態選項的詳細 `security certificate`資訊，請參閱。

步驟

1. 建立自我簽署的數位憑證：

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

   。 `-type root-ca` 選項會建立及安裝自我簽署的數位憑證、以作為憑證授權單位（ CA ）來簽署其他憑證。

   。 `-common-name` 選項會建立 SVM 的憑證授權單位（ CA ）名稱、並在產生憑證的完整名稱時使用。

   預設的憑證大小為2048位元。

   範例

   ```
   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
   ```

   顯示憑證產生的名稱時、請務必儲存以供此程序的後續步驟使用。

   如"指令參考資料ONTAP"需詳細 `security certificate create`資訊，請參閱。

2. 產生憑證簽署要求：

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

   。 `-common-name` 簽署要求的參數必須是 S3 伺服器名稱（ FQDN ）。

   如有需要、您可以提供SVM的位置和其他詳細資訊。

   這 `-dns-name`用戶端通常需要該參數來指定提供 DNS 名稱清單的主題備用名稱擴充。

   這 `-ipaddr`客戶端通常需要該參數來指定提供 IP 位址清單的主題備用名稱擴充。

   系統會提示您保留一份憑證要求和私密金鑰、以供日後參考。

   如"指令參考資料ONTAP"需詳細 `security certificate generate-csr`資訊，請參閱。

3. 使用SVM_CA簽署CSR以產生S3伺服器的憑證：

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

   輸入您在先前步驟中使用的命令選項：

   。 `-ca` — 您在步驟 1 中輸入的 CA 的一般名稱。

- `-ca-serial` — 步驟 1 中的 CA 序號。例如、如果CA憑證名稱為svm1_ca_159D1587CE21E9D4_svm1_ca、序號為159D1587CE21E9D4。

  根據預設、簽署的憑證將於365天內到期。您可以選取其他值、並指定其他簽署詳細資料。

  出現提示時、複製並輸入您在步驟2中儲存的憑證要求字串。

隨即顯示已簽署的憑證、請儲存以供日後使用。

4. 在啟用S3的SVM上安裝簽署的憑證：

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

   出現提示時、請輸入憑證和私密金鑰。

   如果需要憑證鏈結、您可以選擇輸入中繼憑證。

   顯示私密金鑰和CA簽署的數位憑證時、請將其儲存以供日後參考。

5. 取得公開金鑰憑證：

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

   儲存公開金鑰憑證以供稍後的用戶端組態使用。

   範例

```
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
```

相關資訊

- "安全性憑證安裝"
- "安全證書展示"
- "安全性憑證簽署"

建立 ONTAP S3 服務資料原則

您可以為S3資料和管理服務建立服務原則。需要S3服務資料原則、才能在LIF上啟用S3資料流量。

關於這項工作

如果您使用資料生命體和叢集間生命體、則需要S3服務資料原則。如果您使用叢集生命體來處理本機分層使用案例、則不需要使用此功能。

當為LIF指定服務原則時、該原則會用來建構LIF的預設角色、容錯移轉原則和資料傳輸協定清單。

雖然可針對SVM和LIF設定多種傳輸協定、但在處理物件資料時、S3是唯一的傳輸協定、是最佳實務做法。

步驟

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 建立服務資料原則：

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

   ◦ `data-core` 和 `data-s3-server` 雖然可視需要納入其他服務、但啟用 ONTAP S3 只需要服務。

   如"指令參考資料ONTAP"需詳細 `network interface service-policy create`資訊，請參閱。

為 ONTAP S3 建立資料生命

如果您建立新的SVM、您為S3存取所建立的專屬lifs應該是資料lifs。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

  如"指令參考資料ONTAP"需詳細 `network subnet create`資訊，請參閱。

- LIF服務原則必須已經存在。
- 最佳實務做法是、用於資料存取（資料 S3 伺服器）的生命體和用於管理作業（管理 https ）的生命體應該分開。不應在相同的 LIF 上啟用這兩項服務。
- DNS 記錄應該只有與之相關聯的資料 S3 伺服器的生命體 IP 位址。如果在 DNS 記錄中指定其他生命的 IP 位址，則其他伺服器可能會為 ONTAP S3 要求提供服務，導致非預期的回應或資料遺失。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

  深入瞭解 `network interface capacity show`及 `network interface capacity details show` "指令參考資料ONTAP"。

- 如果您要啟用遠端FabricPool 的靜態容量（雲端）分層、則也必須設定叢集間的LIF。

步驟

1. 建立LIF：

   ```
   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 是 LIF 在返回時返回的節點 network interface revert 命令會在LIF上執行。

  如"指令參考資料ONTAP"需詳細 `network interface revert`資訊，請參閱。

  您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 -auto-revert 選項。

- -home-port 是 LIF 在時傳回的實體或邏輯連接埠 network interface revert 命令會在LIF上執行。
- 您可以使用指定 IP 位址 -address 和 -netmask 或是您可以使用從子網路進行分配 -subnet_name 選項。
- 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
- 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資料ONTAP"。
- 適用於 -firewall-policy 選項、請使用相同的預設值 data 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  > 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- -auto-revert 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 false`但您可以將其設定為 `false 視環境中的網路管理原則而定。
- 。 -service-policy 選項會指定您建立的資料和管理服務原則、以及您需要的任何其他原則。

2. 如果您要在中指派 IPv6 位址 -address 選項：

   a. 使用 network ndp prefix show 用於查看在各種接口上學習的 RA 前綴列表的命令。

      。 network ndp prefix show 命令可在進階權限層級使用。

   b. 使用格式 prefix:id 手動建構 IPv6 位址。

      prefix 是在各種介面上學習的首碼。

   用於導出 id，選擇隨機 64 位元十六進位數字。

3. 使用確認 LIF 已成功建立 network interface show 命令。
4. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	network ping

若要驗證...	使用...
IPv6位址	`network ping6`

範例

下列命令顯示如何建立指派給的 S3 資料 LIF `my-S3-policy` 服務原則：

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

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
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.
```

相關資訊

- "網路ping"
- "網路介面"
- "顯示網路NDP前置詞"

使用 ONTAP S3 建立叢集間的階層式生命體，以進行遠端 FabricPool 分層

如果FabricPool 您使用ONTAP 支援使用支援的物件S3來啟用遠端的功能（雲端）分層、

則必須設定叢集間的生命體。您可以在與資料網路共用的連接埠上設定叢集間的LIF。如此可減少叢集間網路所需的連接埠數量。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- LIF服務原則必須已經存在。

關於這項工作

本機Fabric集區分層或外部S3應用程式不需要叢集間生命體。

步驟

1. 列出叢集中的連接埠：

   ```
   network port show
   ```

   下列範例顯示中的網路連接埠 `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
   ```

   如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

2. 在系統SVM上建立叢集間LIF：

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

   以下範例建立叢集間的生命體 `cluster01_icl01` 和 `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
```

如"指令參考資料ONTAP"需詳細 `network interface create`資訊，請參閱。

3. 驗證是否已建立叢集間的LIF：

```
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. 驗證叢集間的LIF是否為備援：

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

以下範例顯示叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在上 `e0c` 連接埠將容錯移轉至 `e0d` 連接埠。

```
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
```

如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

建立 ONTAP S3 物件存放區伺服器

與由NAS和SAN伺服器提供的檔案或區塊儲存設備相比、物件儲存伺服ONTAP 器可將資料管理為S3物件ONTAP 。

開始之前

您應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將使用此名稱來存取S3。FQDN不得以儲存區名稱開頭。使用虛擬代管型存取貯體時、伺服器名稱會用作 `mydomain.com`。例如 `bucketname.mydomain.com`：。

您應該擁有自我簽署的CA憑證（在先前步驟中建立）或由外部CA廠商簽署的憑證。本機分層使用案例不需要CA憑證、因為IP流量只會流經叢集生命體。

關於這項工作

建立物件存放區伺服器時、會建立一個具有UID 0的root使用者。不會為此root使用者產生存取金鑰或秘密金鑰。ONTAP 管理員必須執行 `object-store-server users regenerate-keys` 命令來設定此使用者的存取金鑰和秘密金鑰。

NetApp最佳實務做法是、請勿使用此root使用者。任何使用root使用者存取金鑰或秘密金鑰的用戶端應用程式、都能完整存取物件存放區中的所有儲存區和物件。

如"指令參考資料ONTAP"需詳細 `vserver object-store-server`資訊，請參閱。

範例 **2.** 步驟

系統管理員

如果您要將S3伺服器新增至現有的儲存VM、請使用此程序。若要將S3伺服器新增至新的儲存VM、請參閱"為S3建立儲存SVM"。

您應準備好輸入介面角色資料的IP位址。

1. 在現有的儲存VM上啟用S3。
   a. 選取儲存 VM ：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * S2* 下的。
   b. 按一下「啟用**S2**」、然後輸入「S3伺服器名稱」。
   c. 選取憑證類型。

      無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。

   d. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 建立S3伺服器：

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

   您可以在建立S3伺服器時或稍後隨時指定其他選項。

   - 如果您正在設定本機分層、 SVM 名稱可以是資料 SVM 或系統 SVM （叢集）名稱。
   - 憑證名稱應為伺服器憑證的名稱（終端使用者或葉憑證）、而非伺服器 CA 憑證（中繼或根 CA 憑證）。
   - 預設會在連接埠443上啟用HTTPS。您可以使用變更連接埠號碼 `-secure-listener-port` 選項。

     啟用 HTTPS 時、必須有 CA 憑證才能與 SSL/TLS 正確整合。從 ONTAP 9.15.1 開始、 S3 物件儲存支援 TLS 1.3 。

   - HTTP 預設為停用。啟用時、伺服器會在連接埠 80 上接聽。您可以使用啟用 `-is-http-enabled` 或使用變更連接埠編號 `-listener-port` 選項。

     啟用 HTTP 時、要求和回應會以純文字透過網路傳送。

2. 確認 S3 已設定：

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

範例

此命令可驗證所有物件儲存伺服器的組態值：

```
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
```