

# 在SDWAN vEdge上安裝根證書

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[解決方案](#)

[在vShell中使用Linux CAT命令建立root-ca](#)

[在vShell中使用VI文本編輯器建立root-ca](#)

[安裝憑證](#)

---

## 簡介

本文說明如何使用不同工具在SD-WAN vEdge中安裝根證書。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義廣域網路(SD-WAN)
- 憑證
- 基本Linux

## 採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

- Cisco Catalyst SD-WAN驗證器20.6.3
- Cisco vEdge 20.6.3

## 問題

數位證書是一種電子檔案，通過使用密碼學和公鑰基礎設施(PKI)來認證裝置、伺服器或使用者的真實性。數位證書身份驗證可幫助組織確保只有受信任的裝置和使用者才能連線到其網路。

vEdge硬體路由器的身份由Avnet簽名的裝置證書提供，該證書在製造過程中生成，並燒錄到可信平台模組(TPM)晶片中。Symantec/DigiCert和Cisco根證書已預載入到軟體中，以便信任控制元件的

證書。其他根證書必須手動載入、由SD-WAN Manager自動分發或在自動配置過程中安裝。

SD-WAN中最常見的問題之一是由於無效證書導致的控制連線故障。發生這種情況的原因可能是證書從未安裝，或者證書已損壞。

若要驗證控制連線錯誤圖例，請使用EXEC命令show control connections-history。

<#root>

vEdge #

show control connections-history

Legend for Errors


- ACSRREJ - Challenge rejected by peer.
- BDSGVERFL - Board ID Signature Verify Failure.
- BIDNTPR - Board ID not Initialized.
- BIDNTVRFD - Peer Board ID Cert not verified.
- BIDSIG - Board ID signing failure.
- CERTEXPRD - Certificate Expired
- CRTREJSER - Challenge response rejected by peer.
- NOVMCFG - No cfg in vmanage for device.
- NOZTPEN - No/Bad chassis-number entry in ZTP.
- OPERDOWN - Interface went oper down.
- ORPTMO - Server's peer timed out.
- RMGSPR - Remove Global saved peer.
- RXTRDWN - Received Teardown.
- RDSIGFBD - Read Signature from Board ID failed.
- CRTVERFL - Fail to verify Peer Certificate.
- SERNTPRES - Serial Number not present.
- CTORGNMIS - Certificate Org name mismatch.
- DCONFAIL - DTLS connection failure.
- DEVALC - Device memory Alloc failures.
- DHSTMO - DTLS HandShake Timeout.
- DISCVBD - Disconnect vBond after register reply.
- DISTLOC - TLOC Disabled.
- DUPCLHELO - Recd a Dup Client Hello, Reset GI Peer.
- DUPSER - Duplicate Serial Number.
- DUPSYSIPDEL - Duplicate System IP.
- HAFAIL - SSL Handshake failure.
- IP\_TOS - Socket Options failure.
- LISFD - Listener Socket FD Error.
- MGRTBLOCKD - Migration blocked. Wait for local TMO.
- MEMALCFL - Memory Allocation Failure.
- NOACTVB - No Active vBond found to connect.
- NOERR - No Error.
- NOSLPRCRT - Unable to get peer's certificate.
- NTPRVMIINT - Not preferred interface to vManage.
- STENTRY - Delete same tloc stale entry.
- SSLNFAIL - Failure to create new SSL context.
- STNMODETD - Teardown extra vBond in STUN server
- SYSIPCHNG - System-IP changed
- SYSPRCH - System property changed
- TMRALC - Timer Object Memory Failure.
- TUNALC - Tunnel Object Memory Failure.
- TXCHTOBD - Failed to send challenge to BoardID.
- UNMSGBDRG - Unknown Message type or Bad Register
- UNAUTHHEL - Recd Hello from Unauthenticated peer
- VBDEST - vDaemon process terminated.
- VECRTREV - vEdge Certification revoked.
- VSCRTREV - vSmart Certificate revoked.
- VB\_TMO - Peer vBond Timed out.
- VM\_TMO - Peer vManage Timed out.
- VP\_TMO - Peer vEdge Timed out.
- VS\_TMO - Peer vSmart Timed out.
- XTVMTRDN - Teardown extra vManage.
- XTVSTRDN - Teardown extra vSmart.

PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PRIVATE PORT	PEER PUBLIC IP	PUBLIC PORT
vbond	dtls	-	0	0	10.10.10.1	12346	10.10.10.1	12346
vbond	dtls	-	0	0	10.10.10.2	12346	10.10.10.2	12346

錯誤標籤CRTVERFL的一些常見原因是：

- 證書的到期時間。
- 根ca不同。

- 控制器中是否發生根ca的更新。
- 使用由思科提供的不同憑證授權單位(CA)，且裝置需要手動安裝根CA。
- 在重疊中更改證書頒發機構。

 註：有關控制連線錯誤的詳細資訊，請訪問[排除SD-WAN控制連線故障](#)。

在重疊中的所有元件中，根ca檔案需要完全相同。有兩種方法可以驗證所用的root-ca檔案是否正確

1.檢查檔案的大小，這在root-ca有更新的情況下很有用。

<#root>

```
vBond:/usr/share/viptela$ ls -l
total 5
-rw-r--r-- 1 root root 294 Jul 23 2022 ISR900_pubkey.der
-rw-r--r-- 1 root root 7651 Jul 23 2022 TPMRootChain.pem
-rw-r--r-- 1 root root 16476 Jul 23 2022 ViptelaChain.pem
-rwxr-xr-x 1 root root 32959 Jul 23 2022 ios_core.pem

-rw-r--r-- 1 root root 24445 Dec 28 13:59 root-ca.crt
```

<#root>

```
vEdge:/usr/share/viptela$ ls -l
total 6
drwxr-xr-x 2 root root 4096 Aug 28 2022 backup_certs
-rw-r--r-- 1 root root 1220 Dec 28 13:46 clientkey.crt
-rw----- 1 root root 1704 Dec 28 13:46 clientkey.pem
-rw----- 1 root root 1704 Dec 28 13:46 proxy.key
-rw-r--r-- 1 root root 0 Aug 28 2022 reverse_proxy_mapping

-rw-r--r-- 1 root root 23228 Aug 28 2022 root-ca.crt
```

2.使用md5sum root-ca.crt vshell命令驗證檔案與原始檔完全相同的第二種、也是最可靠的方法。提供md5後，比較控制器元件和邊緣裝置的結果。

<#root>

```
vBond:/usr/share/viptela$
md5sum root-ca.crt
```

```
a4f945b9a1f50f1fa68d539dcf2e54f2 root-ca.crt
```


```
<#root>
```

```
vEdge:/usr/share/viptela$
```

```
md5sum root-ca.crt
```

```
b36358d01b36254a54db2f8db2266ced root-ca.crt
```

---

 註：由於md5sum root-ca.crt vshell命令用於驗證檔案的完整性，實際上對檔案的任何更改都會導致MD5雜湊值不同。


---

## 解決方案

裝置的根證書鏈可以安裝多個工具。使用Linux命令有兩種安裝方法。

### 在vShell中使用Linux CAT命令建立root-ca

---

 註：此過程適用於內容中沒有空白行的根ca檔案，適用於使用Linux vi編輯器過程的空白行的情況。

---

步驟 1. 從驗證器獲取並複製root-ca.crt檔案。

所有控制器上的根ca都相同，可從路徑/usr/share/viptela/中的任意一個控制器複製。

```
<#root>
```

```
vBond#
```

```
vshell
```

```
vBondvBond:~$
```

```
cat /usr/share/viptela/root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpbm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/  
NIewiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
```

```
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

步驟 2. 在 vedge 中建立根 ca.crt 檔案。

從 vshell 導航到 /home/admin 或 /home/<username> 並建立 root-ca.crt 檔案。

```
<#root>
```

```
vEdge#
```

```
vshell
```

```
vEdge:~$
```

```
cat <<" >> root-ca.crt
```

```
> -----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIewiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

```
>
```

```
vEdge:~$
```

步驟 3. 驗證它是否完整。

```
<#root>
```

```
vEdge:~$
```


```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
```

```
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPksEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

---

 註：必須驗證檔案是否完整，如果不完整，請使用rm root-ca.crt vshell命令刪除檔案，然後從步驟2中再次建立該檔案。

---

退出vshell並繼續執行部分。

```
<#root>
vEdge:~$
exit
```

## 在vShell中使用VI文本編輯器建立root-ca

步驟 1. 從驗證器獲取並複製root-ca.crt檔案。

所有控制器上的根ca都相同，可從路徑/usr/share/viptela/中的任意一個控制器複製。

```
<#root>
vBond#
    vshell

vBond:~$
cat /usr/share/viptela/root-ca.crt

-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrNiZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAKGA1UEBhMCVVMxZzAvBzB0eDQwODQwODQwODQwODQwODQwODQwODQwODQw
aG9yaXR5ICh0ZG90aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50
U21nbiBDbGFzcyAzIFB1Ym90aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50
SdhDY2pSS9Kp6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPksEdao7WNq
-----END CERTIFICATE-----
```

步驟 2. 在 vedge 中建立根 ca.crt 檔案。

從 vshell 導航到 /home/admin 或 /home/<username>，然後建立根 ca.crt 檔案。

```
<#root>
vEdge#
vshell
vEdge:~$
  cd /usr/share/viptela/

vEdge:~$
pwd

/home/admin
vEdge:~$ vi root-ca.crt
```

按一下 Enter 後，將顯示編輯器提示。

步驟 3. 進入插入模式

- 鍵入 :i，然後貼上步驟 1 中的證書內容。向下滾動並驗證證書是否完成。

步驟 4. 轉義插入模式並儲存證書。

- 按 ESC 鍵。
- 鍵入 :wq!，然後輸入，以儲存更改並退出編輯器。

```
<#root>
vEdge:/usr/share/viptela$
cat root-ca.crt

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMx FzAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gwzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rwr8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ228udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

-----END CERTIFICATE-----

步驟 5. 驗證它是否完整。

```
<#root>
```

```
vEdge: ~$
```

```
cat root-ca.crt
```


```
-----BEGIN CERTIFICATE-----
```

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/  
NIEwiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH  
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy  
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv  
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

```
-----END CERTIFICATE-----
```

```
vEdge: ~$
```

---

 註：必須驗證檔案是否完整，如果不完整，請使用rm root-ca.crt vshell命令刪除檔案，然後從步驟2中再次建立該檔案。

---

退出vshell並繼續執行部分。

```
<#root>
```

```
vEdge: ~$
```

```
exit
```

## 安裝憑證

步驟 1. 使用request root-cert-chain install <path>命令安裝root-ca證書。

```
<#root>
```

```
vEdge#
```

```
request root-cert-chain install /home/admin/root-ca.crt
```



```
Uploading root-ca-cert-chain via VPN 0  
Copying ... /home/admin/PKI.pem via VPN 0  
Updating the root certificate chain..  
Successfully installed the root certificate chain
```

步驟 2.使用show control local properties命令驗證它是否已安裝。

```
<#root>
```

```
vEdge#
```

```
show control local-properties
```

```
personality vedge  
organization-name organization-name  
root-ca-chain-status Installed  
  
certificate-status Installed  
certificate-validity Valid  
certificate-not-valid-before Apr 11 17:57:17 2023 GMT  
certificate-not-valid-after Apr 10 17:57:17 2024 GMT
```

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。