

在SDWAN vEdge上安装根证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[解决方案](#)

[在vShell中使用Linux CAT命令创建root-ca](#)

[在vShell中使用VI文本编辑器创建root-ca](#)

[安装证书](#)

简介

本文档介绍如何使用不同工具在SD-WAN vEdge中安装根证书。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Catalyst软件定义的广域网(SD-WAN)
- 证书
- 基本Linux

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

- 思科Catalyst SD-WAN验证器20.6.3
- 思科vEdge 20.6.3

问题

数字证书是一种电子文件，通过使用加密和公钥基础设施(PKI)来验证设备、服务器或用户的真实性。数字证书身份验证可帮助组织确保只有受信任设备和用户才能连接到其网络。

vEdge硬件路由器的身份由Avnet签名的设备证书提供，该证书是在制造过程中生成并烧录到可信平台模块(TPM)芯片中。Symantec/DigiCert和Cisco根证书在软件中预加载，以信任控制组件的证书

。其他根证书必须手动加载、由SD-WAN Manager自动分配，或在自动调配过程中安装。

SD-WAN中最常见的问题之一是由于无效证书导致的控制连接失败。发生这种情况的原因可能是证书从未安装或证书损坏。

要验证控制连接错误图例，请使用执行命令show control connections-history。

```
<#root>
```

```
vEdge #
```

```
show control connections-history
```

Legend for Errors

ACSRREJ	- Challenge rejected by peer.	NOVMCFG	- No cfg in vmanage for device.
BDSGVERFL	- Board ID Signature Verify Failure.	NOZTPEN	- No/Bad chassis-number entry in ZTP.
BIDNTPR	- Board ID not Initialized.	OPERDOWN	- Interface went oper down.
BIDNTVRFD	- Peer Board ID Cert not verified.	ORPTMO	- Server's peer timed out.
BIDSIG	- Board ID signing failure.	RMGSPR	- Remove Global saved peer.
CERTEXPRD	- Certificate Expired	RXTRDWN	- Received Teardown.
CRTREJSER	- Challenge response rejected by peer.	RDSIGFBD	- Read Signature from Board ID failed.

CRTVERFL - Fail to verify Peer Certificate.

SERNTPRES - Serial Number not present.


CTORGNMIS	- Certificate Org name mismatch.	SSLNFAIL	- Failure to create new SSL context.
DONFAIL	- DTLS connection failure.	STNMODETD	- Teardown extra vBond in STUN server
DEVALC	- Device memory Alloc failures.	SYSIPCHNG	- System-IP changed
DHSTMO	- DTLS HandShake Timeout.	SYSRCH	- System property changed
DISCVBD	- Disconnect vBond after register reply.	TMRALC	- Timer Object Memory Failure.
DISTLOC	- TLOC Disabled.	TUNALC	- Tunnel Object Memory Failure.
DUPCLHELO	- Recd a Dup Client Hello, Reset GI Peer.	TXCHTOBD	- Failed to send challenge to BoardID.
DUPSER	- Duplicate Serial Number.	UNMSGBDRG	- Unknown Message type or Bad Register
DUPSYSIPDEL	- Duplicate System IP.	UNAUTHHEL	- Recd Hello from Unauthenticated peer
HAFAIL	- SSL Handshake failure.	VBDEST	- vDaemon process terminated.
IP_TOS	- Socket Options failure.	VECRTREV	- vEdge Certification revoked.
LISFD	- Listener Socket FD Error.	VSCRTREV	- vSmart Certificate revoked.
MGRTBLOCKD	- Migration blocked. Wait for local TMO.	VB_TMO	- Peer vBond Timed out.
MEMALCFL	- Memory Allocation Failure.	VM_TMO	- Peer vManage Timed out.
NOACTVB	- No Active vBond found to connect.	VP_TMO	- Peer vEdge Timed out.
NOERR	- No Error.	VS_TMO	- Peer vSmart Timed out.
NOSLPRCRT	- Unable to get peer's certificate.	XTVMTRDN	- Teardown extra vManage.
NTPRVMIINT	- Not preferred interface to vManage.	XTVSTRDN	- Teardown extra vSmart.
STENTRY	- Delete same tloc stale entry.		

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

错误标签CRTVERFL的一些常见原因是：

- 证书的到期时间。
- 根ca不同。

- 在控制器中是否发生根ca的更新。
- 使用思科不同的证书颁发机构(CA)，设备需要手动安装根CA。
- 覆盖中的证书颁发机构更改。

 注意：有关控制连接错误的详细信息，请访问[排除SD-WAN控制连接故障](#)。

在重叠中的所有组件中，root-ca文件需要完全相同。有两种方法可以验证所用的root-ca文件不正确

1.检查文件大小，这在root-ca有更新的情况下很有用。

<#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.验证文件与源文件完全相同的第二种、也是最可靠的方法是使用md5sum root-ca.crt vshell命令。提供md5后，比较控制器组件和边缘设备组件的结果。

<#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
```

 注：由于md5sum root-ca.crt vshell命令用于验证文件的完整性，因为实际上对文件的任何更改都会导致MD5哈希值不同。

解决方案

设备的根证书链可以安装多个工具。使用Linux命令有两种安装方法。

在vShell中使用Linux CAT命令创建root-ca

 注：此过程适用于内容中没有空白行的根ca文件，适用于空白行使用Linux vi编辑器过程的情况。

步骤1:从验证器获取并复制root-ca.crt文件。

所有控制器上的root-ca都相同，并且可从路径/usr/share/viptela/中的任意控制器复制。

```
<#root>
```

```
vBond#
```

```
vshell
```

```
vBondvBond:~$
```

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U2lnbiBDbGFzcyAzIFB1Ym9yYyBQcm1tYXJ5IEN1cnRpb24gQXV0aG9y  
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-----
```

第二步：在网格中创建root-ca.crt文件。

从vshell导航到/home/admin或/home/<username>，然后创建root-ca.crt文件。

```
<#root>
```

```
vEdge#
```

```
vshell
```

```
vEdge:~$
```

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZzZG9nby5naWYwHQYDVR00BBYEFH/TZaFc3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

```
>
```

```
vEdge:~$
```

第三步：验证它是否完整。

```
<#root>
```


```
vEdge:~$
```

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZzZG9nby5naWYwHQYDVR00BBYEFH/TZaFc3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

```
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPksEdao7WNq
-----END CERTIFICATE-----
vEdge: ~$
```

 注：必须验证文件是否完整，如果不完整，请使用rm root-ca.crt vshell命令删除文件，然后从步骤2重新创建该文件。

退出vshell并继续执行部分。

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

在vShell中使用VI文本编辑器创建root-ca

步骤1:从验证器获取并复制root-ca.crt文件。

所有控制器上的root-ca都相同，并且可从路径/usr/share/viptela/中的任意控制器复制。

```
<#root>
vBond#
    vshell

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

-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrNiZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAKGA1UEBhMCVVMxZzAVBgNVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IIC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1Ym9yYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWi u5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPksEdao7WNq
-----END CERTIFICATE-----
```

第二步：在网格中创建root-ca.crt文件。

从vshell导航到/home/admin或/home/<username>，然后创建root-ca.crt文件。

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

vEdge:~$
pwd

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

点击enter后，将显示编辑器提示符。

第三步：进入插入模式

- 键入：i，粘贴第1步中的证书内容。向下滚动并验证证书已完成。

第四步：转义插入模式并保存证书。

- 按ESC键。
- 键入:wq!，然后按enter以保存更改并退出编辑器。

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

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFTZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1Ym9yYyBQcm1tYXJ5IEN1cnRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rW8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

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

第五步：验证它是否完整。

```
<#root>
```

```
vEdge: ~$
```


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

-----BEGIN CERTIFICATE-----

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAkGA1UEBhMCVVMxFTZAVBgNVBAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL  
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: ~$
```

 注：必须验证文件是否完整，如果不完整，请使用rm root-ca.crt vshell命令删除文件，然后从步骤2重新创建该文件。

退出vshell并继续执行部分。

```
<#root>
```

```
vEdge: ~$
```

```
exit
```

安装证书

步骤1:使用命令request root-cert-chain install <path> 安装root-ca证书。

```
<#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
```

第二步：使用show control local properties命令验证它是否已安装。

```
<#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
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。