

SDWAN vEdgeでのルート証明書のインストール

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

[vShellでのLinux CATコマンドによるroot-caの作成](#)

[vShellでVIテキストエディタを使用してroot-caを作成する](#)

[証明書のインストール](#)

はじめに

このドキュメントでは、さまざまなツールを使用してSD-WAN vEdgeにルート証明書をインストールする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Catalystソフトウェア定義型ワイドエリアネットワーク(SD-WAN)
- 証明書
- 基本的なLinux

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

- Cisco Catalyst SD-WANバリデータ20.6.3
- Cisco vEdge 20.6.3

問題

デジタル証明書は、暗号化および公開キーインフラストラクチャ(PKI)を使用して、デバイス、サーバ、またはユーザの信頼性を証明する電子ファイルです。デジタル証明書認証は、信頼できるデバイスとユーザだけがネットワークに接続できるようにするのに役立ちます。

vEdgeハードウェアルータのIDは、Avnetによって署名されたデバイス証明書によって提供され、製造プロセス中に生成され、トラステッドプラットフォームモジュール(TPM)チップに焼き付けられます。Symantec/DigiCertおよびシスコのルート証明書は、コントロールコンポーネントの証明書を信頼するためにソフトウェアにプリロードされています。追加のルート証明書は、手動でロードするか、SD-WAN Managerによって自動的に配布されるか、自動プロビジョニングプロセス中にインストールする必要があります。

SD-WANで最も一般的な問題の1つは、無効な証明書による制御接続の失敗です。これは、証明書がインストールされなかったか、証明書が破損したことが原因で発生します。

制御接続エラーの凡例を検証するには、EXECコマンドshow control connections-historyを使用します。

```
<#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.
BIDNTPRFD	- 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.
DCONFAL	- 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.
NTPRVMI	- Not preferred interface to vManage.	XTVSTRDN	- Teardown extra vSmart.
STENTRY	- Delete same tloc stale entry.		

PEER TYPE	PEER PROTOCOL	PEER SYSTEM	PEER 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

エラーラベルCRTVERFLの一般的な原因には、次のものがあります。

- 証明書の有効期限。
- ルートcaは異なります。
 - コントローラでルートcaの更新が行われるかどうか。
 - シスコによって異なる認証局(CA)が使用されており、デバイスではルートCAを手動でインストールする必要があります。
- オーバーレイでの認証局の変更。

 注：コントロール接続エラーの詳細については、「[SD-WANコントロール接続のトラブルシューティング](#)」を参照してください。

ルートcaファイルは、オーバーレイ内のすべてのコンポーネントで完全に同じである必要があります。使用されているルートcaファイルが正しくないことを確認するには、2つの方法があります

1.ファイルのサイズを確認します。これは、ルートcaに更新があった場合に役立ちます。

<#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.md5sum root-ca.crt vshellコマンドを使用して、ファイルがソースファイルとまったく同じであることを検証する2番目の最も信頼性の高い方法。md5を指定したら、コントローラとエッジデバイスの両方のコンポーネントの結果を比較します。

```
<#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:md5sum root-ca.crt vshellコマンドはファイルの整合性を確認するために使用されるため、ファイルを実質的に変更するとMD5ハッシュが異なるものになります。

解決方法

デバイスのルート証明書チェーンは、複数のツールを使用してインストールできます。Linuxコマンドを使用してインストールする方法は2つあります。

vShellでのLinux CATコマンドによるroot-caの作成

 注：この手順は、コンテンツ内に空白行がないroot-caファイルに適用されます。空白行がある場合は、Linux viエディタ手順を使用します。

ステップ 1：バリデータからroot-ca.crtファイルを取得してコピーします。

ルートcaはすべてのコントローラで同じであり、パス/usr/share/viptela/内の任意のコントローラからコピーできます。

```
<#root>
```

```
vBond#
```

```
vshell
```

```
vBondvBond:~$
```

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yJELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/  
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH  
BgUrDgMCGGQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy  
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv  
hnacRHR21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

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

ステップ 2 : vedgeにroot-ca.crtファイルを作成します。

vshellから/home/adminまたは/home/<username>に移動し、root-ca.crtファイルを作成します。

```
<#root>
```

```
vEdge#
```

```
vshell
```

```
vEdge:~$
```

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yJELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/  
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH  
BgUrDgMCGGQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy  
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv  
hnacRHR21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

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

```
>
```

```
vEdge:~$
```

ステップ 3 : 完了したことを確認します。

```
<#root>
```

```
vEdge:~$
```


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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwHcNMzYwNzE2MjM1OTU5WjCBYjEL  
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
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：ファイルが完全であることを検証することが重要です。完全でない場合は、`rm root-ca.crt` vshellコマンドを使用してファイルを削除し、ステップ2で再度作成します。

vshellを終了し、セクションに進みます。

```
<#root>
```

```
vEdge:~$
```

```
exit
```

vShellでVIテキストエディタを使用してroot-caを作成する

ステップ 1 : バリデータからroot-ca.crtファイルを取得してコピーします。

ルートcaはすべてのコントローラで同じであり、パス/usr/share/viptela/内の任意のコントローラからコピーできます。

```
<#root>
```

```
vBond#
```

```
vsshell
```

```
vBond:~$
```

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yJELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBjbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U21nbiBDbGFzcyAzIFB1Ym90YyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCh71P59zuDMKz10/  
NIeWi5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH  
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy  
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv  
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

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

ステップ 2 : vedgeにroot-ca.crtファイルを作成します。

vsshellから/home/adminまたは/home/<username>に移動し、root-ca.crtファイルを作成します。

```
<#root>
```

```
vEdge#
```

```
vsshell
```

```
vEdge:~$
```

```
cd /usr/share/viptela/
```

```
vEdge:~$
```

```
pwd
```

```
/home/admin
```

```
vEdge:~$ vi root-ca.crt
```

Enterキーをクリックすると、エディタのプロンプトが表示されます。

ステップ 3 : 挿入モードに入ります

- iと入力し、手順1の証明書の内容を貼り付けます。下にスクロールして、証明書が完了していることを確認します。

ステップ 4 : 挿入モードをエスケープし、証明書を保存します。

- Escキーを押します。
- :wq!と入力してからEnterキーを押して、変更を保存し、エディタを終了します。

```
<#root>
```

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

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAKGA1UEBhMCMVVMxZzZlcm1TaWduLCBJbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/  
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH  
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy  
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv  
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

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

ステップ 5 : 完了したことを確認します。

```
<#root>
```

```
vEdge:~$
```


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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB  
yjELMAKGA1UEBhMCMVVMxZzZlcm1TaWduLCBJbmMuMR8wHQYDVQQL  
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL  
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y  
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG  
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+  
rCpSx4/VBEnkjWNHiDxpg8v+r70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/  
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E  
BAMCAQYwbQYIKwYBBQUHAQEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH  
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy  
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZafC3ey78DAJ80M5+gKv  
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
```

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

```
vEdge:~$
```

 注 : ファイルが完全であることを検証することが重要です。完全でない場合は、rm root-ca.crt vshellコマンドを使用してファイルを削除し、ステップ2で再度作成します。

vshellを終了し、セクションに進みます。

```
<#root>
```

```
vEdge:~$
```

```
exit
```

証明書のインストール

ステップ 1 : request root-cert-chain install <path>コマンドを使用して、ルートca証明書をインストールします。

```
<#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
```

ステップ 2 : show control local propertiesコマンドを使用して、インストールされていることを確認します。

```
<#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
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。