

Installer le certificat racine sur les périphériques SDWAN

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

[Créer root-ca avec la commande CAT de Linux dans vShell](#)

[Créer root-ca avec VI Text Editor dans vShell](#)

[Installer le certificat](#)

Introduction

Ce document décrit comment installer un certificat racine dans les vEdge SD-WAN avec différents outils.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco Catalyst
- Certificats
- Linux de base

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

- Cisco Catalyst SD-WAN Validator 20.6.3
- Cisco vEdge 20.6.3

Problème

Un certificat numérique est un fichier électronique qui certifie l'authenticité d'un périphérique, d'un

serveur ou d'un utilisateur par le biais de la cryptographie et de l'infrastructure à clé publique (PKI). L'authentification par certificat numérique aide les entreprises à garantir que seuls les périphériques et les utilisateurs de confiance peuvent se connecter à leurs réseaux.

L'identité des routeurs matériels vEdge est fournie par un certificat de périphérique signé par Avnet, généré pendant le processus de fabrication et gravé dans la puce du module de plateforme sécurisée (TPM). Les certificats racine Symantec/DigiCert et Cisco sont préchargés dans le logiciel pour la confiance des certificats des composants de contrôle. Les certificats racine supplémentaires doivent être chargés manuellement, distribués automatiquement par le gestionnaire SD-WAN ou installés au cours du processus de provisionnement automatisé.

L'un des problèmes les plus courants dans SD-WAN est l'échec des connexions de contrôle en raison d'un certificat non valide. Cela se produit soit parce que le certificat n'a jamais été installé, soit en raison d'une corruption.

Afin de valider la légende d'erreur de connexion de contrôle, utilisez la commande EXEC 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.
BIDNTRFD	- 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.
MGRBTBLCKD	- 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.
NTPRVMINT	- 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

Voici quelques causes courantes de l'étiquette d'erreur CRTVERFL :

- Heure d'expiration du certificat.
- Root-ca est différent.
 - Si une mise à jour de root-ca se produit dans les contrôleurs.
 - Une autorité de certification (CA) différente de celle de Cisco est utilisée et les périphériques nécessitent l'installation manuelle de l'autorité de certification racine.
- Modification de l'autorité de certification dans la superposition.

 Remarque : pour plus d'informations sur les erreurs de connexion de contrôle, consultez [Dépannage des connexions de contrôle SD-WAN.](#)

Le fichier root-ca doit être exactement le même pour tous les composants de la superposition. Il y a deux façons de valider le fichier root-ca utilisé n'est pas le bon

1. Vérifiez la taille du fichier, ce qui est utile dans les situations dans lesquelles le root-ca a eu une mise à jour.

<#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. Deuxième méthode, la plus fiable, pour valider que le fichier est exactement le même que le fichier source, à l'aide de la commande vshell md5sum root-ca.crt. Une fois que le md5 est fourni, comparez le résultat des deux composants Contrôleur et Périphérique Edge.

```
<#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
```

 Remarque : comme la commande md5sum root-ca.crt vshell est utilisée pour vérifier l'intégrité des fichiers, puisque pratiquement toute modification apportée à un fichier entraîne une différence du hachage MD5.

Solution

La chaîne de certificats racine d'un périphérique peut être installée avec plusieurs outils. Il y a deux façons de l'installer avec l'utilisation de commandes Linux.

Créer root-ca avec la commande CAT de Linux dans vShell

 Remarque : cette procédure s'applique aux fichiers root-ca qui n'ont pas de lignes vides dans le contenu, pour les situations avec des lignes vides utilisées par la procédure d'éditeur Linux vi.

Étape 1. Obtenez et copiez le fichier root-ca.crt à partir du validateur.

La commande root-ca est la même sur tous les contrôleurs et peut être copiée à partir de n'importe lequel d'entre eux dans le chemin /usr/share/viptela/.

```
<#root>
vBond#
  vshell

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

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
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-----
```

Étape 2. Créez le fichier root-ca.crt sur le bord.

À partir de vshell, naviguez jusqu'à /home/admin ou /home/<username> et créez le fichier root-ca.crt.

```
<#root>
vEdge#
  vshell

vEdge:~$
cat <<" " >> root-ca.crt

> -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
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-----
>
vEdge: ~$
```


Étape 3. Validez-le comme terminé.

```
<#root>
```

```
vEdge: ~$
```

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

```
-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Z1cm1TaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbjBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QeQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIeWiU5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR00BBYEFH/TZaFC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge: ~$
```

 Remarque : il est important de valider que le fichier est terminé. Si ce n'est pas le cas, supprimez le fichier à l'aide de la commande `rm root-ca.crt vshell` et recréez-le à partir de l'étape 2.

Quittez vshell et passez à la section.

```
<#root>
```

```
vEdge: ~$
```

```
exit
```

Créer root-ca avec VI Text Editor dans vShell

Étape 1. Obtenez et copiez le fichier root-ca.crt à partir du validateur.

La commande root-ca est la même sur tous les contrôleurs et peut être copiée à partir de n'importe lequel d'entre eux dans le chemin /usr/share/viptela/.

```
<#root>
vBond#
  vshell

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

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAKGA1UEBhMCVVMxZzAVBgNVBAoTD1Z1cm1TaWduLCBjbmuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCBYjEL
U21nbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEN1cnRpZm1jYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bT1r8Vd6Gw9KI18q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0P07gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/F1a40ndTRQ8Bnc+MUCH71P59zuDMKz10/
NIewiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQWEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ21mMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVRO0BBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRhr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Étape 2. Créez le fichier root-ca.crt dans la périphérie.

À partir de vshell, accédez à /home/admin ou /home/<username> et créez le fichier root-ca.crt.

```
<#root>
vEdge#
  vshell

vEdge:~$
  cd /usr/share/viptela/

vEdge:~$
  pwd

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

Une fois que vous avez cliqué sur Entrée, l'invite de l'éditeur apparaît.

Étape 3. Passez en mode insertion

- Tapez : i et collez le contenu du certificat de l'étape 1. Faites défiler vers le bas et le certificat de validation est terminé.

Étape 4. Échapper le mode insertion et enregistrer le certificat.

- Appuyez sur la touche ESC.
- Tapez :wq! suivi de Entrée afin d'enregistrer les modifications et de quitter l'éditeur.

```
<#root>
```

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

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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL
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-----
```

Étape 5. Validez-le comme terminé.

```
<#root>
```

```
vEdge:~$
```


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

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

```
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCBJbmMuMR8wHQYDVQQL
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:~\$

 Remarque : il est important de valider que le fichier est terminé. Si ce n'est pas le cas, supprimez le fichier à l'aide de la commande `rm root-ca.crt vshell` et recréez-le à partir de l'étape 2.

Quittez vshell et passez à la section.

<#root>

vEdge:~\$

`exit`

Installer le certificat

Étape 1. Installez le certificat root-ca avec la commande `request root-cert-chain install <path>`.

<#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
```

Étape 2. Vérifiez qu'il est installé avec la commande `show control local properties`.

<#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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.