Instalar e renovar certificados no ASA gerenciado pela CLI

Contents

Introduction

Este documento descreve como solicitar, instalar, confiar e renovar determinados tipos de certificados no software Cisco ASA gerenciado com CLI.

Prerequisites

Requirements

- Verifique se o Adaptive Security Appliance (ASA) tem a hora, a data e o fuso horário corretos. Com a autenticação de certificado, é recomendável usar um Network Time Protocol (NTP) para sincronizar a hora no ASA. Consulte Informações Relacionadas para referência.
- Para solicitar um certificado que use a CSR (Certificate Signing Request, Solicitação de assinatura de certificado), ele requer acesso a uma CA (Certificate Authority, Autoridade de certificação) de terceiros ou interna confiável. Exemplos de fornecedores de CA de terceiros incluem, entre outros, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASAv 9.18.1
- Para a criação de PKCS12, o OpenSSL é usado.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os tipos de certificados que este documento aborda são certificados autoassinados, certificados assinados por uma autoridade de certificação de terceiros ou CA interna, no software Cisco Adaptive Security Appliance gerenciado com a interface de linha de comando (CLI).

Instalação do certificado

Inscrição de certificado autoassinado

1. (Opcional) Crie um par de chaves nomeado com tamanho de chave específico.

> **Nota:** Por padrão, é usada a chave RSA com o nome Default-RSA-Key e o tamanho 2048; no entanto, é recomendável usar um nome exclusivo para cada certificado para que ele não use o mesmo par de chaves privadas/públicas.

<#root>

ASAv(config)#

crypto key generate rsa label

SELF-SIGNED-KEYPAIR

modulus

2048
INFO: The name for the keys will be: SELF-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...

O par de chaves gerado pode ser visto com o comando **show crypto key mypubkey rsa**.

<#root>

ASAv#

show crypto key mypubkey rsa

(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022

Key name:

SELF-SIGNED-KEYPAIR
Usage: General Purpose Key

Key Size

(bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4

```
af020301 0001
```

2. Crie um ponto de confiança com um nome específico. Configure o tipo de inscrição **self**.
<#root>

```
ASAv(config)#
```

```
crypto ca trustpoint
```

```
 SELF-SIGNED
ASAv(config-ca-trustpoint)#
```

```
enrollment self
```

3. Configure o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) e o Nome do assunto.

> **Cuidado**: o parâmetro FQDN deve corresponder ao FQDN ou ao endereço IP da interface ASA para a qual o certificado é usado. Esse parâmetro define o SAN (Nome Alternativo da Entidade) do certificado.

<#root>

```
ASAv(config-ca-trustpoint)#
```

```
fqdn
```

```
 asavpn.example.com
ASAv(config-ca-trustpoint)#
```

```
subject-name
```

```
CN=
```

```
asavpn.example.com,O=Example Inc,C=US,St=California,L=San Jose
```

4. (Opcional) Configure o nome do par de chaves criado na Etapa 1. Não é necessário se o par de chaves padrão for usado.
<#root>

```
ASAv(config-ca-trustpoint)#
```

```
keypair
```

```
 SELF-SIGNED-KEYPAIR
ASAv(config-ca-trustpoint)# exit
```

5. Registre o ponto confiável e gere o certificado.
<#root>

```
ASAv(config)#
```

```
crypto ca enroll
```

```
 SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
```

```
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

yes

% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]:

no

Generate Self-Signed Certificate? [yes/no]:

yes

ASAv(config)#

exit
```

6. Depois de concluído, o novo certificado autoassinado pode ser visto com o comando **show crypto ca certificates**

.

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:
start date: 15:00:58 CEDT Jul 15 2022
end date: 15:00:58 CEDT Jul 12 2032
Storage: config
Associated Trustpoints: SELF-SIGNED
```

Inscrição por solicitação de assinatura de certificado (CSR)

1. (Opcional) Crie um par de chaves nomeado com tamanho de chave específico.

> **Nota:** Por padrão, é usada a chave RSA com o nome Default-RSA-Key e o tamanho 2048; no entanto, é recomendável usar um nome exclusivo para cada certificado para que ele não use o mesmo par de chaves privadas/públicas.

<#root>

```
ASAv(config)#
```

crypto key generate rsa label

```
 CA-SIGNED-KEYPAIR
```

modulus

```
 2048
INFO: The name for the keys will be: CA-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

O par de chaves gerado pode ser visto com o comando **show crypto key mypubkey rsa**.

<#root>

```
ASAv#
```

show crypto key mypubkey rsa

```
(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022
```

Key name:

```
 CA-SIGNED-KEYPAIR
Usage: General Purpose Key
```

Key Size

```
 (bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001
```

2. Crie um ponto de confiança com um nome específico. Configure o **terminal** do tipo de registro.

```
ASAv(config)# crypto ca trustpoint CA-SIGNED
ASAv(config-ca-trustpoint)# enrollment terminal
```

3. Configure o nome de domínio totalmente qualificado e o nome do assunto. Os parâmetros FQDN e CN do assunto devem corresponder ao FQDN ou ao endereço IP do serviço para o qual o certificado é usado.

```
ASAv(config-ca-trustpoint)# fqdn asavpn.example.com
ASAv(config-ca-trustpoint)# subject-name CN=asavpn.example.com,O=Example Inc,C=US,St=California,L=
```

4. (Opcional) Configure o nome do par de chaves criado na etapa 1.

```
ASAv(config-ca-trustpoint)# keypair CA-SIGNED-KEYPAIR
```

5. (Opcional) Configure o método de verificação de revogação de certificados - com a Lista de Revogação de Certificados (CRL) ou com o Protocolo de Status de Certificados Online (OCSP). Por padrão, a verificação de revogação de certificado está desabilitada.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

6. (Opcional) Autentique o ponto confiável e instale o certificado CA que assinará o certificado de identidade como confiável. Se não estiver instalado nesta etapa, o certificado CA poderá ser instalado posteriormente junto com o certificado de identidade.

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0zMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTAlBMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29LynOg9/CTiOGYa+WFTcZXSLHZA6WTUzLYM19IbSFHWa6
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QG0+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
0jRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8odlBvnUedxGAJFHqxEQKmBE+h4w
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0gqhUlSlkFBtLRt6Z2uCot00NoMHI0hh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----

quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

7. Inscreva o certificado e gere um CSR que possa ser copiado e enviado a uma CA para assinatura. O CSR inclui a chave pública do par de chaves usado pelo ponto confiável. O certificado assinado só pode ser usado por dispositivos que tenham esse par de chaves.

Observação: a CA pode alterar os parâmetros FQDN e Nome da Entidade definidos no ponto

---

de confiança ao assinar o CSR e criar o certificado de identidade assinado.

```
ASAv(config)# crypto ca enroll CA-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor

% The fully-qualified domain name in the certificate will be: asavpn.example.com

% Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2Bg0KOT3Fzx0mVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH130JlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuN08T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

8. Importe o certificado de identidade. Depois que o CSR for assinado, um certificado de identidade será fornecido.

```
ASAv(config)# crypto ca import CA-SIGNED certificate
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.



Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIIKbLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
```

```
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmVO9l6iSF/ULGlzXMSOUX6N
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgM0BosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

9. Verifique a cadeia de certificados. Depois de concluído, o novo certificado de identidade e o certificado CA podem ser vistos com o comando **show crypto ca certificates**
.

```
ASAv# show crypto ca certificates CA-SIGNED
CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: CA-SIGNED

Certificate
Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

Inscrição PKCS12

Inscreva-se no arquivo PKCS12 que contém o par de chaves, o certificado de identidade e, opcionalmente, a cadeia de certificados CA recebidos de sua CA.

1. Crie um ponto de confiança com um nome específico.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12
ASAv(config-ca-trustpoint)# exit
```

Nota: O par de chaves importado é nomeado após o nome do ponto confiável.

---

2. (Opcional) Configure o método de verificação de revogação de certificados - com a Lista de Revogação de Certificados (CRL) ou com o Protocolo de Status de Certificados Online (OCSP). Por padrão, a verificação de revogação de certificado está desabilitada.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. Importe o certificado de um arquivo PKCS12.

Nota: O arquivo PKCS12 precisa ser codificado na base64. Se os caracteres imprimíveis forem vistos quando o arquivo for aberto no editor de texto, ele será codificado na base64. Para converter um arquivo binário para a forma codificada na base64, openssl pode ser usado.

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/hqoKcwECD05
dnxCNJx6
quit

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.
```

4. Verifique os certificados instalados.

```
ASAv# show crypto ca certificates TP-PKCS12
```

```
Certificate
Status: Available
Certificate Serial Number: 2b368f75e1770fd0
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
CN=asavpnpkcs12chain.example.com
O=Example Inc
L=San Jose
ST=California
C=US
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: TP-PKCS12

CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: TP-PKCS12
```

No exemplo anterior, o PKCS12 continha a identidade e o certificado CA - as duas entradas - Certificate e CA Certificate. Caso contrário, somente o Certificado estará presente.

5. (Opcional) Autentique o ponto de confiança.

   Se o PKCS12 não contiver o certificado CA e o certificado CA tiver sido obtido separadamente no formato PEM, ele poderá ser instalado manualmente.

```
ASAv(config)# crypto ca authenticate TP-PKCS12
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0gqhUlSlkFBtLRt6Z2uCot00NoMHI0hh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes

WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Renovação de certificado

Renovar certificado autoassinado

1. Verifique a data de expiração do certificado atual.
<#root>

```
# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:
```

start date: 15:00:58 CEDT Jul 15 2022

end date: 15:00:58 CEDT Jul 12 2032

```
Storage: config
Associated Trustpoints: SELF-SIGNED
```

2. Regenerar o certificado.

```
ASAv# conf t
ASAv(config)# crypto ca enroll SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

WARNING: Trustpoint TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
the current certificate will be replaced.
Do you want to continue with re-enrollment? [yes/no]: yes
% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]: no
Generate Self-Signed Certificate? [yes/no]: yes
ASAv(config)# exit
```

3. Verifique o novo certificado.
<#root>

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16085
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:09:09 CEDT Jul 20 2022

end date: 15:09:09 CEDT Jul 17 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

Renovar Certificado Registrado com CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado)

Nota: Se qualquer um dos novos elementos do certificado (subject/fqdn, keypair) precisar ser alterado

---

para o novo certificado, crie um novo certificado. Consulte a seção Inscrição usando CSR (Certificate Signing Request, Solicitação de assinatura de certificado). O próximo procedimento apenas atualiza a data de expiração do certificado.

1. Verifique a data de expiração do certificado atual.
<#root>

```
ASAv# show crypto ca certificates CA-SIGNED


Certificate

Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023

Storage: config
Associated Trustpoints: CA-SIGNED

Certificate
Subject Name:
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 790aa617 c30c6894 0bdc0327 0d60b032
Associated Trustpoint: CA-SIGNED
```

2. Registre o certificado. Gerar um CSR que possa ser copiado e enviado a um CA para assinatura. O CSR inclui a chave pública do par de chaves usado pelo ponto confiável - o certificado assinado só pode ser usado por dispositivos que tenham esse par de chaves.

> **Observação:** a CA pode alterar os parâmetros FQDN e Nome da Entidade definidos no ponto de confiança ao assinar o CSR e criar o certificado de identidade assinado.

> **Nota:** Para o mesmo ponto confiável, sem nenhuma alteração na configuração de assunto/fqdn e par de chaves, as inscrições subsequentes geram o mesmo CSR que a inicial.

```
ASAv# conf t
ASAv(config)# crypto ca enroll CA-SIGNED
```

```
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor
% The fully-qualified domain name in the certificate will be: asavpn.example.com
% Include the device serial number in the subject name? [yes/no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2Bg0KOT3Fzx0mVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH130JlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuN08T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

3. Importe o certificado de identidade. Depois que o CSR for assinado, um certificado de identidade será fornecido.

```
ASAv(config)# crypto ca import CA-SIGNED certificate

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIMA+aIxCtNtMwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMzA3MjAxNDA5MDBaMIGL
MRswGQYDVQQDDBJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUg
SW5jMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAfBgkqhkiG9w0BCQIMEmFzYXZwbi5leGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8olf9yvdiCE/9K/HLgFHua0eLI072l2AksnEm8CnOJGW698ddtL
LPCLXeYOJAXa1Egqa5flTIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoI09cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+IN0dTjg5nsr+LhDGC0v
```

```
56D8WV2fGIkDIhthD9gYNCjk9xc8dJlbnpKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRIOSf6R9d9CZYrTlCRMiJRaFR6r94y+83wPYpSJ7jWh5Iq9OtlUDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAfQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqWlY3fXC27TwweREwMbq8NsJrr80hsChYby8kwE
LnTkrN7dJBl7u5OVQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9rulDVRImd0KYEOx+HYav2INT2udc0G1yDwml/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfN8uR2z5xpzxnEDUBoHOipGlgb1I6G1ARXWO+LwfBl
n1QD5b/RdQOUbLCpfKNPdE/9wNnoXGDlJ7qfZxrO4T7ld2Idug==
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
```

4. Verifique a data de expiração do novo certificado.
<#root>

```
ASAv# show crypto ca certificates CA-SIGNED
Certificate
Status: Available
Certificate Serial Number: 300f9a2310ad36d3
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 16:09:00 CEDT Jul 20 2022
end date: 16:09:00 CEDT Jul 20 2023

Storage: config
Associated Trustpoints: CA-SIGNED
```

Renovação de PKCS12

Não é possível renovar um certificado no ponto confiável registrado usando o arquivo PKCS12. Para instalar um novo certificado, é necessário criar um novo ponto de confiança.

1. Crie um ponto de confiança com um nome específico.

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12-2022
ASAv(config-ca-trustpoint)# exit
```

2. (Opcional) Configure o método de verificação de revogação de certificados - com a Lista de Revogação de Certificados (CRL) ou com o Protocolo de Status de Certificados Online (OCSP). Por padrão, a verificação de revogação de certificado está desabilitada.

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. Importe o novo certificado de um arquivo PKCS12.

Nota: O arquivo PKCS12 precisa ser codificado na base64. Se os caracteres imprimíveis forem vistos quando o arquivo for aberto no editor de texto, ele será codificado na base64. Para converter um arquivo binário para a forma codificada na base64, o openssl pode ser usado.

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12-2022 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiK0c
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/hqoKcwECD05
dnxCNJx6
quit

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.
```

Nota: Se o novo arquivo PKCS12 contiver um certificado de identidade com o mesmo par de chaves usado com o certificado antigo, o novo ponto confiável se referirá ao nome antigo do par de chaves.
Exemplo:

<#root>

```
ASAv(config)# crypto ca import
```

TP-PKCS12-2022

```
 pkcs12 cisco123

Enter the base 64 encoded pkcs12. End with the word "quit" on a line by itself:

MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
...
dnxCNJx6
quit
```

```
WARNING: Identical public key already exists as TP-PKCS12


ASAv(config)# show run crypto ca trustpoint
TP-PKCS12-2022
crypto ca trustpoint TP-PKCS12-2022


keypair TP-PKCS12
 no validation-usage crl configure
```

4. Verifique os certificados instalados.
<#root>

```
ASAv# show crypto ca certificates TP-PKCS12-2022


Certificate

 Status: Available
 Certificate Serial Number: 2b368f75e1770fd0
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: RSA-SHA256
 Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Subject Name: unstructuredName=asavpn.example.com CN=asavpnpkcs12chain.example.com O=Example Inc
 Validity Date:
 start date: 15:33:00 CEDT Jul 15 2022
 end date: 15:33:00 CEDT Jul 15 2023
 Storage: config
 Associated Trustpoints: TP-PKCS12-2022


CA Certificate

 Status: Available
 Certificate Serial Number: 0ccfd063f876f7e9
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: RSA-SHA256
 Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Subject Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Validity Date:
 start date: 15:10:00 CEST Feb 6 2015
 end date: 15:10:00 CEST Feb 6 2030
 Storage: config
 Associated Trustpoints: TP-PKCS12-2022
```

No exemplo anterior, o PKCS12 continha o certificado de identidade e o certificado CA, portanto, duas entradas são vistas após a importação, Certificate e CA Certificate. Caso contrário, somente a entrada do Certificado estará presente.

5. (Opcional) Autentique o ponto de confiança.

Se o PKCS12 não contiver o certificado CA e o certificado CA tiver sido obtido separadamente no formato PEM, ele poderá ser instalado manualmente.

```
ASAv(config)# crypto ca authenticate TP-PKCS12-2022
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0gqhUlSlkFBtLRt6Z2uCot00NoMHI0hh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes

WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

6. Reconfigure o ASA para usar o novo ponto confiável em vez do antigo.

Exemplo:

```
ASAv# show running-config ssl trust-point
ssl trust-point TP-PKCS12
ASAv# conf t
ASAv(config)#ssl trust-point TP-PKCS12-2022
ASAv(config)#exit
```

Observação: um ponto confiável pode ser usado em diferentes elementos de configuração. Verifique sua configuração onde o ponto de confiança antigo é usado.

Informações Relacionadas

Como definir as configurações de hora em um ASA.

Verifique o Guia de configuração da CLI de operações gerais do Cisco ASA Series 9.18 para obter as etapas necessárias para configurar a hora e a data corretamente no ASA.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa918/configuration/general/asa-918-general-config/basic-hostname-pw.html#ID-2130-000001bf

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.