Installazione e rinnovo dei certificati su un'appliance ASA gestita dalla CLI

Sommario

Introduzione

Questo documento descrive come richiedere, installare, considerare attendibili e rinnovare alcuni tipi di certificati su software Cisco ASA gestito con CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Verificare che l'ora, la data e il fuso orario di Adaptive Security Appliance (ASA) siano corretti. Con l'autenticazione dei certificati, si consiglia di usare un server Network Time Protocol (NTP) per sincronizzare l'ora sull'appliance ASA. Consultare Informazioni correlate per riferimento.
- Per richiedere un certificato che utilizza la richiesta di firma del certificato (CSR), è necessario accedere a un'Autorità di certificazione (CA) interna o di terze parti attendibile. Esempi di fornitori di CA di terze parti includono, tra gli altri, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASAv 9.18.1
- Per la creazione di PKCS12, viene utilizzato OpenSSL.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I tipi di certificati a cui si riferisce il documento sono certificati autofirmati, certificati firmati da un'Autorità di certificazione di terze parti o da un'Autorità di certificazione interna, disponibili nel software Cisco Adaptive Security Appliance e gestiti tramite l'interfaccia della riga di comando (CLI).

Installazione certificato

Registrazione certificato autofirmato

1. (Facoltativo) Creare una coppia di chiavi denominata con dimensioni di chiave specifiche.

> Nota: per impostazione predefinita, viene utilizzata la chiave RSA con il nome Default-RSA-Key e una dimensione di 2048; tuttavia, si consiglia di utilizzare un nome univoco per ciascun certificato in modo che non utilizzi la stessa coppia di chiavi privata/pubblica.

<#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...
```

La coppia di chiavi generata può essere visualizzata con il 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

- Creare un trust point con un nome specifico. Configurare il tipo di registrazione **self**.

<#root>

ASAv(config)#

crypto ca trustpoint

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

enrollment self

- Configurare il nome di dominio completo (FQDN) e il nome soggetto.

⚠ **Attenzione**: il parametro FQDN deve corrispondere all'FQDN o all'indirizzo IP dell'interfaccia ASA per cui viene utilizzato il certificato. Questo parametro imposta il nome alternativo del soggetto (SAN) per il certificato.

<#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
```

- (Facoltativo) Configurare il nome della coppia di chiavi creata nel passaggio 1. Non obbligatorio se viene utilizzata la coppia di chiavi predefinita.

<#root>

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

keypair

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

- Registrare il trust point e generare il certificato.

<#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
```

- Una volta completato, il nuovo certificato autofirmato può essere visualizzato con il comando **show crypto ca certificates** <**truspoint name**>.

```
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
```

Iscrizione tramite richiesta di firma del certificato (CSR)

- (Facoltativo) Creare una coppia di chiavi denominata con dimensioni di chiave specifiche.

Nota: per impostazione predefinita, viene utilizzata la chiave RSA con il nome Default-RSA-Key e una dimensione di 2048; tuttavia, si consiglia di utilizzare un nome univoco per ciascun certificato in modo che non utilizzi la stessa coppia di chiavi privata/pubblica.

```
    <#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...
```

La coppia di chiavi generata può essere visualizzata con il 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
```

- Creare un trust point con un nome specifico. Configurare il **terminale del** tipo di registrazione.

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

- Configurare il nome di dominio completo e il nome soggetto. I parametri FQDN e CN soggetto devono corrispondere all'FQDN o all'indirizzo IP del servizio per cui viene utilizzato il certificato.

```
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=
```

- (Facoltativo) Configurare il nome della coppia di chiavi creata nel passaggio 1.

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

- (Facoltativo) Configurare il metodo di controllo delle revoche di certificati con l'elenco di revoche di certificati (CRL) o con il protocollo di stato dei certificati in linea (OCSP). Per impostazione predefinita, il controllo di revoca dei certificati è disattivato.

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

- (Facoltativo) Autenticare il trust point e installare il certificato CA che firmerà il certificato di identità come attendibile. Se non viene installato in questo passaggio, il certificato CA può essere installato in un secondo momento insieme al certificato di identità.

```
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
BhMCUExDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
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
OjRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8odlBvnUedxGAJFHqxEQKmBE+h4w
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
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
```

- Registrare il certificato e generare un CSR che possa essere copiato e inviato a una CA per la firma. Il CSR include la chiave pubblica della coppia di chiavi utilizzata da trustpoint. Il certificato firmato può essere utilizzato solo dai dispositivi che dispongono di tale coppia di chiavi.

Nota: durante la firma del CSR e la creazione del certificato di identità firmato, CA può modificare i parametri FQDN e Nome soggetto definiti nel trust point.

```
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/noPxZXZ8YiQMiG2EP2Bg0KOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuNO8T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R5OIXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

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

- Importare il certificato di identità. Una volta firmato il CSR, viene fornito un certificato di identità.

```
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+BWTBlxgMOBosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

- Verificare la catena di certificati. Al termine, il nuovo certificato di identità e il certificato CA possono essere visualizzati con il comando **show crypto ca certificates** <**trustpoint name**>.

```
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
```

Iscrizione PKCS12

Registrarsi con il file PKCS12 che contiene la coppia di chiavi, il certificato di identità e, facoltativamente, la catena di certificati CA, ricevuti dalla CA.

- Creare un trust point con un nome specifico.

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

Nota: alla coppia di chiavi importata viene assegnato il nome del trust point.

- (Facoltativo) Configurare il metodo di controllo delle revoche di certificati con l'elenco di revoche di certificati (CRL) o con il protocollo di stato dei certificati in linea (OCSP). Per impostazione predefinita, il controllo di revoca dei certificati è disattivato.

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

- Importare il certificato da un file PKCS12.

Nota: il file PKCS12 deve essere codificato in base64. Se vengono visualizzati caratteri stampabili quando il file viene aperto nell'editor di testo, viene codificato in base64. Per convertire un file binario nel formato codificato in base64, è possibile utilizzare openssl.

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

Comando:

crypto ca import trustpoint pkcs12 passphrase [nointeractive]

```
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.
```

- Verificare i certificati installati.

```
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
```

Nell'esempio precedente, il PKCS12 conteneva l'identità e il certificato CA, ovvero le due voci Certificato e Certificato CA. In caso contrario, è presente solo il certificato.

- (Facoltativo) Autenticare il trust point.

Se il PKCS12 non contiene il certificato CA e il certificato CA è stato ottenuto separatamente in formato PEM, è possibile installarlo 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
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
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
```

Rinnovo certificato

Rinnova certificato autofirmato

- Controllare la data di scadenza del certificato corrente.

  <#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
```

- Rigenerare il certificato.

```
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
```

- Verificare il nuovo certificato.

<#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
```

Rinnova certificato registrato con richiesta di firma del certificato (CSR)

Nota: se è necessario modificare uno dei nuovi elementi del certificato (soggetto/fqdn, coppia di chiavi) per il nuovo certificato, creare un nuovo certificato. Fare riferimento alla sezione Iscrizione mediante la richiesta di firma di certificato (CSR). La procedura successiva aggiorna semplicemente la data di scadenza del certificato.

- Controllare la data di scadenza del certificato corrente.

  <#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
```

- Registrare il certificato. Generare un CSR che possa essere copiato e inviato a una CA per la firma. Il CSR include la chiave pubblica della coppia di chiavi utilizzata dal trust point. Il certificato firmato può essere utilizzato solo dai dispositivi che dispongono di tale coppia di chiavi.

Nota: durante la firma del CSR e la creazione del certificato di identità firmato, CA può modificare i parametri FQDN e Nome soggetto definiti nel trust point.

Nota: per lo stesso Trustpoint, senza alcuna modifica dell'oggetto/FQDN e della configurazione della coppia di chiavi, le iscrizioni successive danno lo stesso CSR di quello iniziale.

```
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/noPxZXZ8YiQMiG2EP2Bg0KOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
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
```

- Importare il certificato di identità. Una volta firmato il CSR, viene fornito un certificato di identità.

```
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/HLgFHuaOeLIO72l2AksnEm8CnOJGW698ddtL
LPCLXeYOJAXa1Egqa5flTIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoIO9cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+INOdTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYNCjk9xc8dJlbnpKJ0LUYYmbfnM8sn0kaKsgUmpBGQcAA
aHfKtRIOSf6R9d9CZYrTlCRMiJRaFR6r94y+83wPYpSJ7jWh5Iq9OtlUDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAfQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqWlY3fXC27TwweREwMbq8NsJrr8OhsChYby8kwE
LnTkrN7dJBl7u5OVQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
p7cB6veTcF9rulDVRImd0KYEOx+HYav2INT2udc0G1yDwml/mqdf0/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfN8uR2z5xpzxnEDUBoHOipGlgb1I6G1ARXWO+LwfBl
n1QD5b/RdQOUbLCpfKNPdE/9wNnoXGDlJ7qfZxrO4T7ld2Idug==
-----END CERTIFICATE-----
```

```
quit

INFO: Certificate successfully imported
```

- Verificare la data di scadenza del nuovo certificato.

<#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
```

Rinnovo PKCS12

Impossibile rinnovare un certificato in un trust point registrato utilizzando il file PKCS12. Per installare un nuovo certificato, è necessario creare un nuovo trust point.

- Creare un trust point con un nome specifico.

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

• (Facoltativo) Configurare il metodo di controllo delle revoche di certificati con l'elenco di revoche di certificati (CRL) o con il protocollo di stato dei certificati in linea (OCSP). Per impostazione predefinita, il controllo di revoca dei certificati è disattivato.

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

• Importa il nuovo certificato da un file PKCS12.

Nota: il file PKCS12 deve essere codificato in base64. Se vengono visualizzati caratteri stampabili quando il file viene aperto nell'editor di testo, viene codificato in base64. Per convertire un file binario in formato codificato in base64, è possibile utilizzare openssl.

```
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 il nuovo file PKCS12 contiene un certificato di identità con la stessa coppia di chiavi utilizzata con il vecchio certificato, il nuovo trust point fa riferimento al vecchio nome della coppia di chiavi.
Esempio:

```
<#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
```

- Verificare i certificati installati.

<#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
```

Nell'esempio precedente, il PKCS12 conteneva il certificato di identità e il certificato CA, pertanto dopo l'importazione vengono visualizzate due voci, Certificato e Certificato CA. In caso contrario, è presente solo la voce Certificato.

- (Facoltativo) Autenticare il trust point.

Se il PKCS12 non contiene il certificato CA e il certificato CA è stato ottenuto separatamente in formato PEM, è possibile installarlo 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
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
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
```

- Riconfigurare l'ASA in modo che usi il nuovo trust point anziché quello vecchio.

Esempio:

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

---

Nota: un trust point può essere utilizzato in diversi elementi di configurazione. Controllare la configurazione in cui è utilizzato il vecchio trust point.

Informazioni correlate

Come configurare le impostazioni di tempo su un'appliance ASA.

Verificare in questo riferimento i passaggi necessari per impostare correttamente l'ora e la data sull'appliance ASA. CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide, 9.18

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).