Genera e aggiungi i certificati necessari per l'installazione di Secure Endpoint Private Cloud 3.x e versioni successive

Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Premesse Creazione certificato Genera certificati sul server di Windows Genera una richiesta di firma del certificato (CSR) Invio del CSR alla CA e generazione del certificato Esportazione della chiave privata e conversione in formato PEM Genera certificato su server Linux (controllo SSL rigoroso DISABILITATO) Genera RootCA autofirmata Genera un certificato per ogni servizio Genera chiave privata Genera CSR Genera certificato Genera certificato su server Linux (controllo SSL rigoroso ABILITATO) Genera RootCA autofirmata Genera un certificato per ogni servizio Creare un file di configurazione delle estensioni e salvarlo (extensions.cnf) Genera chiave privata Genera CSR Genera certificato Aggiunta dei certificati al cloud privato della console protetta Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto il processo di generazione dei certificati da caricare con ogni nuova installazione di Secure Console Private Cloud o di rinnovo dei Servizi certificati installati.

Prerequisiti

Requisiti

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

hardware:

- Windows Server 2008
- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2 (In Avanti)
- OpenSSL 1.1.1

Componenti usati

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Windows Server 2008 (in avanti)
- Installazione Secure Console Private Cloud
- Infrastruttura a chiave pubblica
- OpenSSL
- CLI Linux

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

Con l'introduzione di Secure Console Private Cloud 3.X, i nomi host e le coppie certificato/chiave sono necessari per tutti i seguenti servizi:

- Portale di amministrazione
- Autenticazione (novità in Private Cloud 3.X)
- Console protetta
- Server di disposizione
- Server di disposizione Protocollo esteso
- Servizio di aggiornamento della disposizione
- Firepower Management Center

In questo documento viene illustrato come generare e caricare rapidamente i certificati richiesti. È possibile modificare ogni parametro, incluso l'algoritmo di hashing, le dimensioni della chiave e altri, in base ai criteri dell'organizzazione e il meccanismo di generazione dei certificati potrebbe non corrispondere a quanto descritto in questa sezione.

Avviso: la procedura indicata di seguito può variare in base alla configurazione del server CA. È previsto che il provisioning del server CA prescelto sia già stato eseguito e che la configurazione dello stesso sia stata completata. La nota tecnica seguente descrive solo un esempio di generazione dei certificati e Cisco TAC non è coinvolto nella risoluzione dei problemi relativi alla generazione dei certificati e/o ai problemi dei server CA di alcun tipo.

Creazione certificato

Genera certificati sul server di Windows

Verificare che i ruoli seguenti siano installati e configurati nel server Windows.

- Servizi certificati Active Directory
- Autorità di certificazione
- Registrazione Web Autorità di certificazione
- Risponditore online
- Servizio Web di registrazione certificati
- Servizio Web di informazioni sulle registrazioni di certificati
- Servizi di dominio Active Directory
- Server DNS
- Server Web (IIS)
- Active Directory Certificate Services
- Active Directory Domain Services
 DNS Server
 File Services
- Web Server (IIS)

Genera una richiesta di firma del certificato (CSR)

Passaggio 1. Passare alla console MMC e aggiungere lo snap-in Certificati per l'account computer, come illustrato nell'immagine.

p-en	Vendor 🔺		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor		Certificates (Local Compute	r)
ctive Directory Site	Microsoft Cor			Remove
ctive Directory Use	Microsoft Cor			
ctiveX Control	Microsoft Cor			Move Up
DSI Edit	Microsoft Cor			
uthorization Manager	Microsoft Cor			Move Down
Certificate Templates	Microsoft Cor	Add >		
lertificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Vevice Manager	Microsoft Cor			
lisk Management	Microsoft and			a descent
NS	Mcrosoft Cor			Advanced
alian.				
Diam.				

Passaggio 2. Espandere Certificati (Computer locale) > Personale > Certificati.

Passaggio 3. Fare clic con il pulsante destro del mouse sullo spazio vuoto e selezionare All Tasks > Advanced Operations > Create Custom Request.



Passaggio 4. Selezionare Successivo nella finestra Iscrizione.



Passaggio 5. Selezionare il criterio di registrazione dei certificati e scegliere Avanti.

Select Certificate Enrollment Policy	
Certificate enrolment policy enables enrolm enrolment policy may already be configured	ent for certificates based on predefined certificate templates. Certificate d for you.
Configured by your administrator	
Active Directory Enrolment Policy	0
Configured by you	Add Nev
Custom Request	
Proceed without enrolment policy	

Passaggio 6. Scegliere il modello come server Web e selezionare Avanti.

Certificate Enrollment	
Certificate Enrollment	
Custom request	
Chose an option from	he list below and configure the certificate options as required.
Template:	Web Server
Request format:	© PKCS #10
Note: Key archival is r specified in the certific	iot available for certificates based on a custom certificate request, even when this option is cate template.
Learn more about cust	2m request
	Next Cancel

Passaggio 7. Se il modello "Server Web" è stato configurato correttamente ed è disponibile per la registrazione, verrà visualizzato lo stato Disponibile. Selezionare **Dettagli** per espandere Proprietà.

ertificate Information		
lick Next to use the options a	ready selected for this template, or click Details to customize th	e certificate request,
Active Directory Enr	oliment Policy	
Web Server	(j) STATUS: Available	Details (8
The following options des Key usage:	cribe the uses and validity period that apply to this type of cert Digital signature Key encidement	ificate:
Application policies:	Server Authentication	
Validity period (days	: 730	
		Properties

Passaggio 8. Aggiungere almeno gli attributi CN e DNS. Gli altri attributi possono essere aggiunti in base ai requisiti di sicurezza.

ertificate Properties		×
A Subject General Extension	s Private Key	
The subject of a certificate is the u enter information about the types in a certificate.	iser or computer to which th of subject name and alterna	e certificate is issued. You can ative name values that can be used
Subject of certificate		
The user or computer that is received	ing the certificate	
Subject name:		
Type:		CN=amp-vpc.cisco.com
Common name	Add >	
Value:		
	< Remove	
Alternative name:		DNS
Type:		amp-vpc.cisco.com
Units I		
value:	Add >	
L	100 2	
	< Remove	
Learn more about subject name		
	OK	Cancel Apply

Passaggio 9. Facoltativamente, assegnare un Nome descrittivo nella scheda Generale.

Passaggio 10. Fare clic sulla scheda **Private Key** e verificare che sia attivata l'opzione **Make private key exportable** nella sezione **Key Options**.

Certificate Properties	×
🔥 Subject General Extensions Private Key	
Cryptographic Service Provider	۲
Key options	(8)
Set the key length and export options for the private key.	
Key size: 2048	I
Make private key exportable	I
Allow private key to be archived	I
Strong private key protection	I
	I
Key type	۲
Key permissions	8
	I
	I
Learn more about private key	
OK Cancel	Apply

Passaggio 11. Infine, selezionare **OK**. Verrà visualizzata la finestra di dialogo Registrazione certificato in cui è possibile selezionare **Avanti**.

Passaggio 12. Individuare il percorso in cui salvare il file con estensione req inviato al server CA per la firma.

Invio del CSR alla CA e generazione del certificato

Passaggio 1. Passare alla pagina Web di Servizi certificati MS AD come indicato di seguito e selezionare **Richiedi certificato**.

Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

Welcome

Use this Web site to request a certificate for your Web brov request, perform other security tasks.

You can also use this Web site to download a certificate au

For more information about Active Directory Certificate Ser

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Passaggio 2. Fare clic sul collegamento Richiesta avanzata di certificati.

Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

Request a Certificate

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

Passaggio 3. Selezionare Invia una richiesta di certificato utilizzando un file CMC o PKCS #10 con codifica Base 64 oppure inviare una richiesta di rinnovo utilizzando un file PKCS #7 con codifica Base 64.

Passaggio 4. Aprire il contenuto del file .req (CSR) salvato in precedenza tramite il Blocco note. Copiare il contenuto e incollarlo qui. Verificare che il modello di certificato sia selezionato come server Web

Microsoft Active Directory Certificate Services - bgl amp AD-CA	
	RIQ1 - Notepad
Submit a Certificate Request or Renewal Request	File Edit Format View Help
To submit a saved request to the CA, paste a base-64-encoded CMC or P	BEGIN NEW CERTIFICATE REQUEST WIIDDOCCARACADALITE (MCCALUEAMMAININGTS) (b03xb3xb1xmlt oc 5 (axm/bb/5) b20wpgt invalues possible Dogtangunal Itemanigge Kanttange + zgut + a 1960w03KHV V1edNu221PsEhbguct, 1 20/2xb2, e/nyggamc1wdfw2txrx880655s,y08pz3k+rabg
Saved Request	[EuPer 2687 3Fn3w0vV308PH13w23LW155KX83Ak06Cwc3ae3K58k/Ac7ua5azX25 bbsc aai au vviloc ve f0zvo76F58k1s SechvEnkcevR3Acr vrk3bk0P/btuut ks4ek2
Certificate Template: (100 Classes)	In proceeding 12 and 16 of 60 seles 12, how the unseted in the Title, 14 Seles Skywe, galaxy 22 ben 20 data 16 of data /1 Sky 71 c2 bed (51 still 2) of 61, key et al. 10 data (51 bed) of 50 bed (71 bed) A 17 Valgetta Andigoget Herbicki II statiggets (2) catagotis (2) catagotis (2) exercises in the 2 bed (71 bed) A 17 Valgetta Andigoget Herbicki II statiggets (2) catagotis (2) catagotis (2) exercises in the 2 bed (71 bed) A 17 Valgetta Andigoget Herbicki II statiggets (2) catagotis (2) catagotis (2) exercises in the 2 bed (71 bed) A 17 Valgetta Andigoget Herbicki II statiggets (2) catagotis (2) catagotis (2) exercises (2) exercis
Aven Devel	vaukckM/SwcfSoHS1asSyeH3+wgH17rfbbug28sSH15wokwkdsH0C+Tgg+
Additional Attributes:	END NEW CERTIFICATE REQUEST
Attributes:	
Submit >	

Passaggio 5. Infine, selezionare Invia.

Passaggio 6. A questo punto, è necessario essere in grado di **scaricare** il certificato, come mostrato nell'immagine.

Certificate Issued
The certificate you requested was issued to you.
DER encoded or Dase 64 encoded Download certificate Download certificate chain

Esportazione della chiave privata e conversione in formato PEM

Passaggio 1. Installare il certificato nell'archivio certificati aprendo il file con estensione cer e selezionando **Installa certificato**.

Passaggio 2. Passare allo snap-in di MMC selezionato in precedenza.

Passaggio 3. Passare all'archivio in cui è stato installato il certificato.

Passaggio 4. Fare clic con il pulsante destro del mouse sul certificato corretto, selezionare **Tutte le attività > Esporta**.

🔄 console	Open	bgl-amp-AD-CA		
🔄 dispex		bgl-amp-AD-CA		
🔄 disp-pr	All Tasks 🕨 🕨	Open		
Gispupi Gifmc-pri Ciprivate	Cut Copy Delete	Request Certificate with New Key Renew Certificate with New Key		
	Properties	Manage Private Keys Advanced Operations		
	Help	Export		

Passaggio 5. Nell'Esportazione guidata certificati confermare l'esportazione della chiave privata, come illustrato nell'immagine.

Certificate Export Wizard 🛛 🗙
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
O No, do not export the private key
Learn more about exporting private keys
< Back Next > Cancel

Passaggio 6. Immettere una password e selezionare **Avanti** per salvare la chiave privata sul disco.

Passaggio 7. In questo modo la chiave privata viene salvata in formato PFX, tuttavia è necessario convertirla in formato PEM per utilizzarla con Secure Endpoint Private Cloud.

Passaggio 8. Installare le librerie OpenSSL.

Passaggio 9. Aprire una finestra del prompt dei comandi e passare alla directory in cui è stato installato OpenSSL.

Passaggio 10. Eseguire il comando seguente per estrarre la chiave privata e salvarla in un nuovo file: (Se il file PFX non si trova nello stesso percorso in cui è memorizzata la libreria OpenSSL, è necessario specificare il percorso esatto insieme al nome del file)

openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes Passaggio 11. Eseguire il comando seguente per estrarre anche il certificato pubblico e salvarlo in un nuovo file:

openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes

Genera certificato su server Linux (controllo SSL rigoroso DISABILITATO)

Nota: Strict TLS Check verifica che il certificato soddisfi i requisiti TLS di Apple. Per ulteriori informazioni, consultare la <u>Guida dell'amministratore</u>.

Verificare che nel server Linux che si sta tentando di generare i certificati richiesti siano installate le librerie OpenSSL 1.1.1. Verificare se questa e la procedura riportata di seguito possono variare rispetto alla distribuzione Linux in esecuzione. Questa parte è stata documentata, come avviene su un server CentOS 8.4.

Genera RootCA autofirmata

Passaggio 1. Generare la chiave privata per il certificato CA radice.

openssl genrsa -out Passaggio 2. Generare il certificato CA.

openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"

Genera un certificato per ogni servizio

Creare il certificato per l'autenticazione, la console, l'eliminazione, l'eliminazione estesa, il server di aggiornamento, il servizio Firepower Management Center (FMC) in base alla voce relativa al nome DNS. È necessario ripetere il processo di generazione del certificato seguente per ogni servizio (autenticazione, console e così via).

Certificate (PEM .crt)		<pre> Q_t Key (PEM .key) </pre>
0	Certificate file has been uploaded.	Key file has been uploaded.
0	Certificate is in a readable format.	Key contains a supported key type.
0	Certificate start and end dates are valid.	Key contains public key material.
0	Certificate contains a subject.	Key contains private key material.
0	Certificate contains a common name.	Key contains a public key matching the uploaded certificate.
0	Certificate contains a public key matching the upl	ed key. + Choose Key
0	Certificate matches hostname.	
0	Certificate is signed by a trusted root authority.	
	+ Choose	rtificate

Genera chiave privata

openssl genrsa -out

Sostituire <YourServiceName.key> con il nuovo nome del file KEY da creare come Auth-Cert.key

Genera CSR

openssl req -new \ -subj '/CN= -key Sostituire il <YourServiceName.key> con il file KEY del certificato corrente o nuovo, ad esempio Auth-Cert.key

Sostituire <YourServiceName.csr> con il nome del file CSR da creare, ad esempio Auth-Cert.crt

Genera certificato

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
Sostituire <YourServiceName.csr> con il CSR del certificato effettivo o nuovo, ad esempio Auth-
Cert.csr
```

Sostituire <YourRootCAName.pem> con il nome file PEM effettivo (o nuovo) come RootCAName.pem

Sostituire <YourServiceName.key> con il file KEY del certificato corrente o nuovo, ad esempio Auth-Cert.key

Sostituire <YourServiceName.crt> con il nome del file da creare, ad esempio Auth-Cert.crt

Genera certificato su server Linux (controllo SSL rigoroso ABILITATO)

Nota: Strict TLS Check verifica che il certificato soddisfi i requisiti TLS di Apple. Per ulteriori informazioni, consultare la <u>Guida dell'amministratore</u>.

Genera RootCA autofirmata

Passaggio 1. Generare la chiave privata per il certificato CA radice.

openssl genrsa -out Passaggio 2. Generare il certificato CA.

openssl req \ -subj '/CN= -outform pem -out -key -days "1000"

Genera un certificato per ogni servizio

Creare il certificato per l'autenticazione, la console, l'eliminazione, l'eliminazione estesa, il server di aggiornamento, il servizio Firepower Management Center (FMC) in base alla voce relativa al nome DNS. È necessario ripetere il processo di generazione del certificato seguente per ogni servizio (autenticazione, console e così via).

MP fo	r Endpoints Console Certificate		Disable Strict TLS Check	Undo	Replace Certificate
	• Certificate (PEM .crt)	L	Q. Key (PEM	key)	
0	Certificate file has been uploaded.	0	Key file has been uploaded.		
0	Certificate is in a readable format.		Key contains a supported key type.		
0	Certificate start and end dates are valid.		Key contains public key material.		
0	Certificate contains a subject.	٥	Key contains private key materia	d.	
0	Certificate contains a common name.	٥	Key contains a public key match	ing the u	ploaded certificate.
0	Certificate contains a public key matching the uploaded key.				+ Choose Key
0	Certificate matches hostname.				
٥	Certificate is signed by a trusted root authority.				
0	Certificate issued after 07/01/2019 must have a validity period of 825 days or less.				
0	Certificate issued after 09/01/2020 must have a validity period of 398 days or less.				
0	Certificate does not use sha-1 signature algorithm.				
0	Certificate using RSA keys must use a key size of 2048 or more.				
0	Certificate must specify server certificate in Extended Key Usage extension.				
	+ Choose Certificate				

Creare un file di configurazione delle estensioni e salvarlo (extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

Genera chiave privata

openss1 genrsa -out Sostituire <YourServiceName.key> con un nuovo nome file KEY da creare come Auth-Cert.key

Genera CSR

```
openssl req -new \
-key
-subj '/CN=
-out
```

Sostituire il <YourServiceName.key> con la chiave del certificato corrente o nuova, ad esempio

Auth-Cert.key

Sostituire <YourServiceName.csr> con il CSR del certificato corrente o nuovo, ad esempio Auth-Cert.csr

Genera certificato

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Sostituire <YourServiceName.csr> con il CSR del certificato corrente o nuovo, ad esempio Auth-Cert.csr

Sostituire <YourRootCAName.pem> con il nome file PEM corrente (o nuovo) come RootCAName.pem

Sostituire <YourServiceName.key> con il file KEY del certificato corrente o nuovo, ad esempio Auth-Cert.key

Sostituire <YourServiceName.crt> con il nome del file da creare, ad esempio Auth-Cert.crt

Aggiunta dei certificati al cloud privato della console protetta

Passaggio 1. Una volta generati i certificati utilizzando uno dei metodi descritti in precedenza, caricare il certificato corrispondente per ogni servizio. Se sono stati generati correttamente, tutti i segni di spunta sono attivati come mostrato nell'immagine qui.



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

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).