Installare un certificato di terze parti firmato dall'autorità di certificazione in ISE

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Passaggio 1. Generare una richiesta di firma del certificato (CSR).
Passaggio 2. Importa una nuova catena di certificati.
<u>Verifica</u>
Risoluzione dei problemi
<u>Il richiedente non considera attendibile il certificato del server locale ISE durante</u> un'autenticazione dot1x
La catena di certificati ISE è corretta, ma l'endpoint rifiuta il certificato ISEServer durante l'autenticazione
Informazioni correlate

Introduzione

In questo documento viene descritto come installare un certificato firmato da un'Autorità di certificazione (CA) di terze parti in Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle infrastrutture a chiave pubblica di base.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Identity Services Engine (ISE) versione 3.0. La stessa configurazione si applica alle release 2.X

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

Questo processo è lo stesso indipendentemente dal ruolo del certificato finale (autenticazione EAP, portale, amministrazione e pxGrid).

Configurazione

Passaggio 1. Generare una richiesta di firma del certificato (CSR).

Per generare CSR, selezionare Amministrazione > Certificati > Richieste di firma certificato, quindi fare clic su Genera richieste di firma certificato (CSR).

Certificate Management ~ System Certificates	Certificate Signing Requests			
Trusted Certificates	Generate Certificate Signing Requests (CSR)			
OCSP Client Profile	A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Clic			
Certificate Signing Requests	request has been signed, click "bind" to bind the request to the signed certificate issued by that au			
Certificate Periodic Check Se	Q View 🛧 Export 🝵 Delete Bind Certificate			
Certificate Authority	Friendly Name Certificate Subjec			

- 1. Nella sezione Utilizzo selezionare il ruolo da utilizzare dal menu a discesa. Se il certificato viene utilizzato per più ruoli, è possibile selezionare Multiuso. Una volta generato il certificato, i ruoli possono essere modificati, se necessario.
- 2. Selezionare il nodo per il quale è possibile generare il certificato.
- 3. Compilare le informazioni necessarie (unità organizzativa, organizzazione, città, stato e paese).

Nota: nel campo CN (Common Name), ISE compila automaticamente il nome di dominio completo (FQDN) del nodo.

Caratteri jolly:

- Se l'obiettivo è generare un certificato con caratteri jolly, selezionare la casella Consenti certificati con caratteri jolly.
- Se il certificato viene utilizzato per le autenticazioni EAP, il simbolo * non deve essere presente nel campo CN soggetto in quanto i supplicant Windows rifiutano il certificato server.

- Anche quando la funzione Convalida identità server è disabilitata sul supplicant, l'handshake SSL può non riuscire quando * è nel campo CN.
- È invece possibile utilizzare un nome di dominio completo (FQDN) generico nel campo CN e quindi *.domain.com nel campo Nome DNS alternativo soggetto (SAN).
- Nota: alcune autorità di certificazione (CA) possono aggiungere automaticamente il carattere jolly (*) nel CN del certificato anche se non è presente nel CSR. In questo scenario, è necessario inviare una richiesta speciale per impedire questa azione.

Esempio di CSR del certificato del server singolo:

Usage

Certificate(s) will be used for Multi-Use			You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual
			certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates	\odot		
Node(s)			
Generate CSR's for these Nodes:			
Node	CSR Friendly Name		
🔽 abtomar30	abtomar30#Multi-Use		
Subject			
Common Name (CN) \$FQDN\$		()	
Organizational Unit (OU) Cisco TAC		<u>(</u>)	
Organization (O) Cisco		<u>(</u>)	
City (L) Bangalore			
State (ST) Karnataka			
Country (C) IN			
Subject Alternative Name (SAN)			
IP Address	~ 10.106.120.87		- + 0
* Key type			
RSA	× (j)		

Esempio di CSR con caratteri jolly:

Jsage			
Certificate(s) will be used for	Multi-Use	~	You can use a single certificate for multiple services, but doing so is not a recommended
			practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals.
Allow Wildcard Certificates 🗸	(\mathbf{i})		EAP, and pxGrid).
Subject			
Common Name (CN) Mycluster.mydomain,com		()	
Organizational Unit (OU) Cisco TAC		<u>(</u>)	
Organization (O) Cisco		Ġ	
		_	
City (L) Bangalore			
State (ST) Karnataka			
Country (C) IN			
Subject Alternative Name (SAN)			
IP Address	∽ 10.106.120.87		- +
DNS Name	~ *.mydomain.com		- + 0
* Key type			
RSA	~ (i)		

Nota: è possibile aggiungere al campo SAN ogni indirizzo IP del nodo o dei nodi di distribuzione per evitare di ricevere un avviso di certificato quando si accede al server tramite l'indirizzo IP.

Una volta creato il CSR, ISE visualizza una finestra pop-up con l'opzione di esportazione. Una

volta esportato	, il file deve	essere inviato	alla CA per	la firma.
-----------------	----------------	----------------	-------------	-----------



Passaggio 2. Importa una nuova catena di certificati.

L'autorità di certificazione restituisce il certificato del server firmato insieme alla catena di certificati completa (radice/intermedio). Una volta ricevuti, eseguire la procedura seguente per importare i certificati nel server ISE:

- 1. Per importare i certificati radice e/o intermedi forniti dalla CA, selezionare Amministrazione > Certificati > Certificati protetti.
- 2. Fare clic su Importa, quindi scegliere il certificato radice e/o intermedio e selezionare le caselle di controllo appropriate per l'invio.
- 3. Per importare il certificato del server, selezionare Amministrazione > Certificati > Richieste di firma del certificato.
- 4. Selezionare il CSR creato in precedenza e fare clic su Binding Certificate.
- 5. Selezionare il percorso del nuovo certificato e ISE assocerà il certificato alla chiave privata creata e memorizzata nel database.

Nota: se per questo certificato è stato selezionato il ruolo di amministratore, i servizi server ISE specifici verranno riavviati.

Attenzione: se il certificato importato si riferisce al nodo di amministrazione principale della distribuzione e se è stato selezionato il ruolo Admin, i servizi su tutti i nodi verranno riavviati

▲ uno dopo l'altro. Questa operazione è prevista e per eseguirla si consiglia un tempo di inattività.

Verifica

Se il ruolo di amministratore è stato selezionato durante l'importazione del certificato, è possibile verificare che il nuovo certificato sia presente caricando la pagina di amministrazione nel browser. Il browser deve considerare attendibile il nuovo certificato di amministratore se la catena è stata creata correttamente e se è considerata attendibile dal browser.

Attps://abtomar30.abtomar.local/admin/login.jsp) → 🗎 Ċ 🥖 Identity Services Engine 🛛 🖌
Certificate Certification Path Certificatio	
abtomar 30. abtomar . local	CISCO
	Identity Services Engine
	Intuitive network security
	Username
View Certificate	
Certificate status:	Password
This certificate is UK.	
	Login
ОК	
	English 日本語
	Problems logging in?
2020 Olive Surface Inc. Olive Surface and Olive Surface Inc.	

View third-party licenses and notices

Per ulteriori verifiche, selezionare il simbolo del lucchetto nel browser e, sotto il percorso del certificato, verificare che l'intera catena sia presente e considerata attendibile dal computer. Questo non è un indicatore diretto che la catena completa sia stata passata correttamente dal server, ma un indicatore del browser in grado di considerare attendibile il certificato del server in base al relativo archivio attendibile locale.

Risoluzione dei problemi

Il richiedente non considera attendibile il certificato del server locale ISE durante

un'autenticazione dot1x

Verificare che ISE stia passando l'intera catena di certificati durante il processo di handshake SSL.

Quando si utilizzano metodi EAP che richiedono un certificato server (PEAP) e si seleziona Convalida identità server, il richiedente convalida la catena di certificati utilizzando i certificati presenti nel proprio archivio attendibilità locale come parte del processo di autenticazione. Nell'ambito del processo di handshake SSL, ISE presenta il proprio certificato nonché qualsiasi certificato radice e/o intermedio presente nella propria catena. Il richiedente non sarà in grado di convalidare l'identità del server se la catena è incompleta. Per verificare che la catena di certificati venga restituita al client, è possibile eseguire la procedura seguente:

- 1. Per acquisire un'immagine da ISE (TCP/IPump) durante l'autenticazione, selezionare Operazioni > Strumenti diagnostici > Strumenti generali > TCP Dump.
- 2. Scaricare/aprire l'acquisizione e applicare il filtro ssl.handshake.certificates in Wireshark e trovare un access-challenge.
- Dopo aver selezionato questa opzione, selezionare Espandi protocollo Radius > Coppie valore attributo > Ultimo segmento messaggio EAP > Protocollo di autenticazione estensibile > SSL (Secure Sockets Layer) > Certificato > Certificati.

Catena di certificati nell'acquisizione.

Eile <u>E</u> dit	View Go Capture Analyze St	tatistics Telephony Iools Internals Hel	p					
0 0 1	■ A B B X Ø Q ♦	••• •*± == 0000	i 🕷 🗹 💐	\$ \$				
Filter:	ssLhandshake.certificates	 Expression 	Clear	Apply	Save			
ю.	Time	Source	Destinatio	on .	Protocol	Length Info		
334	13:59:41.137274	14.36.157.20	14.36.	157.21	TLSv1.2	992 Server	Hello, Certific	ate, Server Hello Done
857	13:59:53.158063	14.36.157.21	14.36.	154.5	RADIUS	1178 Access	-Challenge(11) (id-198, 1-1136)
860	13:59:53.193912	14.36.157.21	14.36.	154.5	RADIUS	1174 Access	-Challenge(11) (1d=199, 1=1132)
862	13:59:53.213/15	14.36.157.21	14.36.	154.5	RADIUS	1174 Access	-Challenge(11) (id=200, 1=1132)
864	13:59:53.231653	14.36.157.21	14.36.	154.5	RADIUS	301 Access	-Challenge(11) (10=201, 1=259)
1265	14:00:01.253698	14.36.157.20	14.36.3	157.21	TLSV1.2	992 Server	Hello, Certific	ate, Server Hello Done
	I LEIN THE AND MARKANNEL	(ii) Second (ii)						
D AM	P: 1=235 t=EAP-Message()	79) Segment[1]						
10 AV	P: 1=255 t=EAP-Message()	79) Segment[2]						
0.41	P. 1=255 C=EAP-Message() 1=255 E_EAP-Message()	70) Lost Segment[4]						
	AD fragment	sy case segmenc(4)						
	xtensible Authenticatio	n Protocol						
	Code: Request (1)							
	Id: 41							
	Length: 1012							
	Type: Protected EAP (E)	AP-PEAP) (25)						
9	EAP-TLS Flags; 0xc0							
	EAP-TLS Length: 3141							
0	[4 EAP-TLS Fragments (3141 bytes): #857(1002), #860	(1002),	#862(100	2), #864(135)]			
9	Secure Sockets Layer							
	IN TLSV1 Record Layer: H	landshake Protocol: Server He	110					
	□ TLSv1 Record Layer: ►	landshake Protocol: Certifica	te					
	Content Type: Hands	hake (22)						
	Version: TLS 1.0 (0	x0301)						
	Length: 3048							
	Handshake Protocol:	Certificate						
	Handshake Type: Co	ertificate (11)						
	Length: 3044							
	Certificates Lengt	th: 3041						
	Certificates (304)	1 bytes)						
	Certificate Leng	th: 1656						
	Certificate (id-	at-commonName=TORISE20A.rtpaz	aa.net,id	l-at-orga	anizationalUnitNa	ane=RTPAAA,io	d-at-organization	Name=CISCO,id-at-localityNam
	Certificate Leng	th: 1379						
	Certificate (id-	at-commonName=rtpaaa-ca,dc=rt	tpaaa,dc=	net)				
	III TLSv1 Record Layer: H	landshake Protocol: Server He	110 Done					
					-			

Se la catena è incompleta, selezionare Amministrazione ISE > Certificati > Certificati attendibili e verificare che i certificati radice e/o intermedi siano presenti. Se la catena di certificati viene

passata correttamente, è necessario verificarne la validità utilizzando il metodo descritto di seguito.

Aprire ogni certificato (server, intermedio e radice) e verificare la catena di attendibilità confrontando lo SKI (Subject Key Identifier) di ogni certificato con l'AKI (Authority Key Identifier) del certificato successivo nella catena.

Esempio di catena di certificati.

Certificate 26	Certificate 26	Certificate 28
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show	Show <al></al>	Show <al></al>
Field Value Public key RSA (2048 84s) Subject Key Mentfler da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6 Einhanced Key Usage Server Authentication (1.3:6.1:5.5.7.3.1)	Field Value	Field Volue Public key RSA (4996 Bits) RKey Usage Digital Signature, Certificate Signing, Off-Iu, Subject Key Ident 52 2e e5 2c 38 29 06 da 81 19 11 70 74 00,
Subject Alternative P Address=14.36.157.21 Authority Key Identi KeyID=fe 34 as ad 22 9b 6e d7 ad 86 11 CRL Distribution Pol [L]CRL Distribution Pol [L]Authority Info Access: Access Method	Authority Key (Sectif Key(D=32 2e e5 22 36 29 00 03 81 19 11 CRL Distribution Pol [1] CRL Distribution Pol [1] Authority Informatio [2] Authority Informatio.	CA Version V0.0 Basic Constraints Subject Type=CA, Path Length Constraint= Thumbprint elgori shal Thumbprint cb 24 48 as 30 11 72 as da 9e 31 d1 f3 f6 +
V3	V3	V3
Edit Properties Copy to File	Edit Properties Copy to File	Edit Properties Copy to File
ОК	OK	OK

La catena di certificati ISE è corretta, ma l'endpoint rifiuta il certificato del server ISE durante l'autenticazione

Se ISE presenta la catena di certificati completa durante l'handshake SSL e il supplicant rifiuta ancora la catena di certificati, il passaggio successivo consiste nel verificare che i certificati radice e/o intermedi si trovino nell'archivio di attendibilità locale del client.

Per verificare questa condizione da un dispositivo Windows, passare a mmc.exe File > Aggiungi-Rimuovi snap-in. Dalla colonna Snap-in disponibili selezionare Certificati e fare clic su Aggiungi. Selezionare Account utente o account computer a seconda del tipo di autenticazione in uso (Utente o Computer) e quindi fare clic su OK.

Nella visualizzazione della console selezionare Autorità di certificazione radice attendibili e Autorità di certificazione intermedie per verificare la presenza di certificati radice e intermedi nell'archivio attendibile locale. Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help					
♦ ⇒ 2 □ □ 0 ≥ 2 □					
📫 Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name St
A 🕼 Certificates - Current User	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenti	USERTrust
Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenti	Baltimore Cybe
Trusted Root Certification Authorities	Certum CA	Certum CA	6/11/2027	Server Authenti	Certum
Certificates	Cisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>
Intermediate Certification Authorities	Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>
Certificate Revocation List	Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, S	CertPlus Class 2
Certificates	Class 3 Public Primary Ce	Class 3 Public Primary Certi	8/1/2028	Secure Email, C	VeriSign Class 3
Active Directory User Object	COMODO RSA Certificati	COMODO RSA Certificatio	1/18/2038	Server Authenti	COMODO
Trusted Publishers	Copyright (c) 1997 Micro	Copyright (c) 1997 Microso	12/30/1999	Time Stamping	Microsoft Time
Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root C	11/9/2031	Server Authenti	DigiCert
Third-Party Root Certification Authorities	DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenti	DigiCert
Trusted People	DigiCert High Assurance	DigiCert High Assurance E	11/9/2031	Server Authenti	DigiCert
Other People	DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, S.,	DST Root CA X3
Certificate Enrollment Requests	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>
Image: Smart Card Trusted Roots	Entrust Root Certification	Entrust Root Certification	11/27/2026	Server Authenti	Entrust

Per verificare in modo semplice se si tratta di un problema di controllo dell'identità del server, deselezionare Convalida certificato server nella configurazione del profilo del supplicant e testarlo di nuovo.

Connection Security	When connecting:
Security type: WPA2-Enterprise Encryption type: AES	Connect to these servers:
	Trusted Root Certification Authorities:
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings	Certum CA Cisco Root CA 2048
Remember my credentials for this connection each time I'm logged on	Class 2 Primary CA Class 3 Public Primary Certification Authority

Informazioni correlate

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.0
- Supporto tecnico Cisco e download

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).