CAPF-Zertifikat signiert von CA für CUCM

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Einschränkung Hintergrundinformationen Zweck von CA Signed CAPF Mechanismus für diese PKI Wie unterscheidet sich CAPF CSR von anderen CSRs? Konfigurieren Überprüfen LSC bei selbstsignierter CAPF LSC bei cA-signiertem CAPF Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie ein CAPF-Zertifikat (Certificate Authority Proxy Function) erhalten, das von der Zertifizierungsstelle (Certificate Authority, CA) für Cisco Unified Communications Manager (CUCM) signiert wurde. Es gibt immer Anforderungen, die CAPF mit einer externen CA zu signieren. Dieses Dokument zeigt, warum es genauso wichtig ist wie das Konfigurationsverfahren, zu verstehen, wie es funktioniert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Public Key Infrastructure (PKI)
- CUCM-Sicherheitskonfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Unified Communications Manager Version 8.6 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Einschränkung

Eine andere CA hat möglicherweise andere Anforderungen als die CSR. Es gibt Berichte, dass verschiedene Versionen von OpenSSL CA haben einige spezifische Fragen für die CSR aber Microsoft Windows CA funktioniert gut mit dem CSR von Cisco CAPF, die Diskussion wird in diesem Artikel nicht behandelt werden.

Zugehörige Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- Microsoft Windows Server 2008 CA.
- Cisco Jabber für Windows (verschiedene Versionen können einen anderen Namen für Ordner zum Speichern der LSC haben).

Hintergrundinformationen

Zweck von CA Signed CAPF

Einige Kunden möchten die globale Zertifikatsrichtlinie einhalten, die für das Unternehmen gilt. Daher müssen sie die CAPF mit derselben Zertifizierungsstelle wie andere Server unterzeichnen.

Mechanismus für diese PKI

Standardmäßig wird das LSC (Locally Significant Certificate) von der CAPF signiert, daher ist die CAPF in diesem Szenario die CA für Telefone. Wenn Sie jedoch versuchen, den CAPF von der externen CA zu signieren, fungiert der CAPF in diesem Szenario als untergeordnete CA oder zwischengeschaltete CA.

Der Unterschied zwischen selbstsigniertem CAPF und CA-signiertem CAPF ist: CAPF ist die Root-CA für LSC, wenn selbstsigniertes CAPF ausgeführt wird. CAPF ist die untergeordnete CA-CA für LSC, wenn CA-signiertes CAPF ausgeführt wird.

Wie unterscheidet sich CAPF CSR von anderen CSRs?

Bezüglich des <u>RFC5280</u> definiert die Schlüsselverwendungserweiterung den Zweck (z. B. Verschlüsselung, Signatur, Zertifikatssignierung) des im Zertifikat enthaltenen Schlüssels. CAPF ist ein Zertifikatsproxy und eine Zertifizierungsstelle, die Zertifikate an die Telefone signieren kann. Das andere Zertifikat wie CallManager, Tomcat, IPSec fungiert jedoch als Leaf (Benutzeridentität). Wenn Sie sich die CSR-Anfrage ansehen, sehen Sie, dass der CAPF CSR über eine **Zertifikatsignaturfunktion** verfügt, aber nicht die anderen.

CAPF CSR:

```
Attributes:
Requested Extensions:
X509v3 Extended Key Usage:
TLS Web Server Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Certificate Sign
```

Tomcat CSR:

```
Attributes:

Requested Extensions:

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System

X509v3 Key Usage:

Digital Signature, Key Encipherment, Data Encipherment, Key Agreement

CallManager CSR:
```

```
Attributes:

Requested Extensions:

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System

X509v3 Key Usage:

Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

IPSec CSR:

Attribute: Angeforderte Durchwahlen: X509v3 Extended Key Usage: TLS-Webserver-Authentifizierung, TLS-Webclient-Authentifizierung, IPSec-Endsystem X509v3 Schlüsselverwendung: Digitale Signatur, Schlüsselwahrnehmung, Datenverschlüsselung, Schlüsselvereinbarung

Konfigurieren

In einem Szenario wird die externe Root-CA zum Signieren des CAPF-Zertifikats verwendet: zur Verschlüsselung des Signals/der Medien für Jabber Client und IP-Telefon.

Schritt 1: Machen Sie Ihr CUCM-Cluster zu einem Sicherheitscluster.

```
admin:utils ctl set-cluster mixed-mode
```

Schritt 2: Generieren Sie, wie im Bild gezeigt, den CAPF-CSR.

Attps://10.67.81.2	115/cmplatform/certificateGenerateNewCsr.do
Generate Certificate	Signing Request
Generate 🖳 Clo	se
Status	
Warning: Genera	ting a new CSR for a specific certificate type will overwrite
- Gpc	
Generate Certificate	Signing Request
Certificate Purpose*	CAPF 🔻
Distribution*	CCM105PUB.sophia.li
Common Name*	CCM105PUB.sophia.li
Key Length*	2048
Hash Algorithm*	SHA256 ¥
Generate Close	

Schritt 3: Signiert mit der CA (unter Verwendung einer untergeordneten Vorlage in Windows 2008 CA).

Hinweis: Sie müssen die Vorlage der Subordinate Certification Authority verwenden, um dieses Zertifikat zu unterzeichnen.

€ € 10.67.81.12	0/certsrv/certrqxt.asp	
Cisco Service Aw	ard 🚾 OS X Yosemite 虚拟机 📙 CALO 📘 Project Square	ed
Microsoft Active	Directory Certificate Services sophia-WIN-3S18JC3LN	12A
Submit a Cert	ficate Request or Renewal Request	
To submit a say	ved request to the CA, paste a base-64-encode	ed
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	d43Q6Zx+jfHozMpIIxPBY2ZMh3tqY5jBSawd8SBq C+kM7fAJFtVGtvt+yeG5+P1HPGCr7r87171uXA+g o/rAeJgnLbNRSXRPOM0aGhMJ2Hd7R6sQ64iB8gng DiwxAgQaeJw7n8vd4ehZSN1Z46gm+wx0Tk94yDed J7Xot0WbkseyQVWsHBY17w== END CERTIFICATE REQUEST	•
Certificate Temp	ate:	
	Subordinate Certification Authority 🝷	
Additional Attribu	ites:	
Attributes:		
	Submit >	_

Interventional and the second seco
🔅 Cisco Service Award 🚾 OS X Yosemite 虛拟机 📙 CALO 📘 Project Squared 餐
Microsoft Active Directory Certificate Services sophia-WIN-3S18JC3LM2A-C
Certificate Issued
The certificate you requested was issued to you.
DER encoded or <a>O Base 64 encoded
Download certificate Download certificate chain

Schritt 4: Laden Sie die Root-CA als CAPF-trust und das Serverzertifikat als CAPF hoch. Laden Sie für diesen Test auch diese Root-CA als CallManager-Vertrauenswürdigkeit hoch, um über eine TLS-Verbindung zwischen dem Jabber- und dem CallManager-Dienst zu verfügen, da der signierte LSC auch vom CallManager-Dienst als vertrauenswürdig eingestuft werden muss. Wie am Anfang dieses Artikels erwähnt, muss die CA für alle Server angepasst werden, sodass diese CA bereits zur Signal-/Medienverschlüsselung in CallManager hochgeladen werden sollte. Für die Bereitstellung des IP-Telefons 802.1x müssen Sie den CUCM nicht als gemischten Modus festlegen oder die CA hochladen, die die CAPF als CallManager-Vertrauenswürdigkeit in den CUCM-Server signiert.

Schritt 5: Starten Sie den CAPF-Dienst neu.

Schritt 6: Starten Sie die CallManager/TFTP-Dienste in allen Notizen neu.

Schritt 7: Jabber Softphone LSC signiert.

-Certification Authority P	Proxy Function (CAPF) Information	
Certificate Operation*	Install/Upgrade	-
Authentication Mode*	By Authentication String	-
Authentication String	12345	
Generate String		
Key Size (Bits)*	1024	-
Operation Completes By	2015 12 27 12 (YYYY:MM:DD:HH)	
Certificate Operation Status Note: Security Profile Cont	s: Upgrade Success ains Addition CAPF Settings.	

🕑 Cisco Jabber		cure Phone Verification	×	
Li Sophia Available	o- 🛕	You must complete the verification proc	ess.	
Available Q. Search or call Contacts Contacts Contacts Contacts Contacts Contacts Contacts Contacts Contacts Contacts Contacts Contacts Contacts Simon Li Simon Li Friends Contact		You must complete the verification proc Your administrator has enabled call security. computer for calls, you must complete the ve process. Enter the authentication code you received fr administrator. Enter code: 12345 OK	Cancel Cancel Music Pictures Videos Computer Local Disk (C:) DVD Drive (D:) GR8 New Volume (E:) f (\\10.66.90.19) (Z	Security Search in library Share with Search Name AppDialRules.xml.adr CSFSOPHIA.cnf.xml.sgn CSFSOPHIA.thv DirLookupDialRules.xml.dlr Me 20
🝙 -			4 items	<

AppData ▶ Roaming ▶ Cisco ▶ Unified Communications ▶ Jabber ▶ CSF ▶ Security ▶

•

Open	Share with 🔻 New folder			
	Name	Date modified	Туре	Size
	AppDialRules.xml.adr	20/03/2015 12:37	ADR File	
	📾 CSFSOPHIA.cnf.xml.enc.sgn	20/03/2015 12:37	XML Configuratio	
:es	📾 CSFSOPHIA.cnf.xml.sgn	20/03/2015 12:37	XML Configuratio	
	CSFSOPHIA.key	20/03/2015 10:42	KEY File	
		20/03/2015 10:42	LSC File	
:	CSFSOPHIA.tlv	20/03/2015 12:37	TLV File	
	📄 DirLookupDialRules.xml.dlr	20/03/2015 12:37	DLR File	
	🜗 Security	20/03/2015 2:20 PM	Compressed (zipp	

Schritt 8: Aktivieren Sie das Sicherheitsprofil für Jabber-Softphone.

Protocol Specific Information-

Packet Capture Mode*	None	•
Packet Capture Duration	0	
BLF Presence Group*	Standard Presence group	•
SIP Dial Rules	< None >	•
MTP Preferred Originating Codec*	711ulaw	Ŧ
Device Security Profile*	secured-Cisco Unified Client Services Framework	•

Schritt 9: Sicheres RTP wird jetzt wie folgt durchgeführt:



Überprüfen

Vergleichen Sie das LSC, wenn Sie CAPF selbst und CAPF mit CA-Zeichen signieren:

Wie Sie in diesen Bildern für LSC sehen können, ist CAPF aus LSC-Sicht die Root-CA, wenn selbstsigniertes CAPF verwendet wird. CAPF ist jedoch die untergeordnete (intermediäre) CA, wenn CA-signiertes CAPF verwendet wird.

LSC bei selbstsignierter CAPF

Cert	ficate	×
Ge	Details Certification Path	_
[Certificate Information	_
	Windows does not have enough information to verify this certificate.	
	Termed has conscioned	-
	Issued to: CSPSOPHIA	
	Issued by: CAPF-15b63ca4	
	Valid from 20/ 03/ 2015 to 18/ 03/ 2020	
	Instal Certificate Issuer Statemen	2
Le	earn more about <u>certificates</u>	
	ОК	
	A	
Cert	ificate	×
Cert	ificate neral Details Certification Path	×
Ge	ificate neral Details Certification Path Certification path	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CAPF-15b63ca4 CAPF-15b63ca4	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSORHIA	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSOPHIA	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSORHIA	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSORHIA	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSOPHIA	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSORHIA View Certificate	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSOPHIA View Certificate	
Gert	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CSFSOFHIA CSFSOFHIA View Certificate View Certificate tertificate status: This certificate has expired or is not yet valid.	
Ge	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CAPF-15b63ca4 CERTIFICATE CERTIFICATE View Certificate this certificate status:	
Cert	ificate neral Details Certification Path Certification path CAPF-15b63ca4 CAPF-15b63ca4 CERTIFICATE CERTIFICATE View Certificate View Certificate tertificate status: This certificate has expired or is not yet valid. earn more about certification paths	
Gert	ificate neral Details Certification Path Certification path CAPF-1Sb63ca4 Certificate Status: User Certificate status: This certificate has expired or is not yet valid. Certificate has expired or is not yet valid. Certificate has expired or is not yet valid.	

LSC bei CA-signiertem CAPF

Certificate 🗾
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
Ensures the identity of a remote computer Allows secure communication on the Internet
Issued to: CSFSOPHIA
Issued by: CAPF-fe816e37
Valid from 20/ 03/ 2015 to 18/ 03/ 2020
Install Certificate Issuer Statement
Learn more about certificates
Certificate 🗾
Certificate
Certificate General Details Certification Path Certification path
Certificate General Details Certification Path Certification path Sophia-WIN-3518JC3LM2A-CA
Certificate
Certificate
Certificate General Details Certification Path Certification path Sophia-WIN-35183C3LM2A-CA CAPF-fe816e37 CSFSORHIA
Certificate
Certificate General Details Certification Path Certification path Certification path CAPF-fe816e37 CAPF-fe816e37 CSFSORHIA
Certificate General Details Certification Path Certification path Certification path CAPF-fe816e37 CSFSOPHIA
Certificate General Details Certification Path Certification pat
Certificate General Details Certification Path Certification Ce
Certificate General Details Certification Path Certification path Certification path Certification SIBJC3LM2A-CA CAPF-fe816e37 CSFSOPHIA View Certificate
Certificate General Details Certification Path Certification path Certification path Certificate status:
Certificate General Details Certification Path Certification path Certification path Certificate status: This certificate is OK.
Certificate General Details Certification Path Certification path Certification path Certification path CAPF-fe816e37 CAPF-fe816e37 Certificate status: This certificate is OK.
Certificate General Details Certification Path Certification path Certification path Certificate status: This certificate is OK. Learn more about certification paths
Certificate General Details Certification Path Certification path Certification path Certificates37 CAPF-fe816e37 CAPF-fe816e37 Certificate status: Certificate status: This certificate is OK. Learn more about certification paths

Warnung:

Das Jabber Client LSC, das die gesamte Zertifikatkette in diesem Beispiel anzeigt, unterscheidet sich vom IP-Telefon. AS IP-Telefone sind auf der Basis von RFC 5280 (3.2) konzipiert. Zertifizierungspfade und Vertrauenswürdigkeit), dann fehlt die AKI (Authority Key Identifier), dann sind CAPF und das Stammzertifikat der Zertifizierungsstelle nicht in der Zertifikatskette vorhanden. Wenn die CAPF/Root CA-Zertifizierung in der Zertifikatskette fehlt, kann die ISE bei der 801.x-Authentifizierung Probleme mit der Authentifizierung von IP-Telefonen haben, ohne die CAPF- und Root-Zertifikate in die ISE hochzuladen. Es gibt eine weitere Option in CUCM 12.5, bei der LSC direkt von einer externen Offline-CA signiert wird, sodass das CAPF-Zertifikat für die 802.1x-Authentifizierung des IP-Telefons nicht in die ISE hochgeladen werden muss.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

Bekannter Fehler: CAPF-Zertifikat mit CA-Vorzeichen, Root-Zertifikat muss als CM-Trust hochgeladen werden:

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir_