Generieren Sie ein neues Expressway-Zertifikat mit den Informationen aus dem aktuellen Zertifikat.

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Schritt 1: Suchen Sie die aktuellen Zertifikatsinformationen. Schritt 2: Erstellen Sie einen neuen CSR mit den oben angegebenen Informationen. Schritt 3: Überprüfen und Herunterladen des neuen CSR Schritt 4: Überprüfen Sie die im neuen Zertifikat enthaltenen Informationen. Schritt 5: Laden Sie ggf. die neuen Zertifizierungsstellenzertifikate in den vertrauenswürdigen Server-Store hoch. Schritt 6: Laden Sie das neue Zertifikat auf den Expressway Server hoch. Überprüfen Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie Sie eine neue CSR-Anfrage (Certificate Signing Request) mit den Informationen im vorhandenen Expressway-Zertifikat generieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zertifikatattribute
- Expressways oder Video Communication Server (VCS)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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.

Konfigurieren

Schritt 1: Suchen Sie die aktuellen Zertifikatsinformationen.

Um die im aktuellen Zertifikat enthaltenen Informationen abzurufen, wählen Sie in der grafischen Benutzeroberfläche (GUI) von Expressway **Maintenance > Security > Server Certificate** (**Wartung > Sicherheit > Serverzertifikat**) aus.

Suchen Sie den Abschnitt Serverzertifikatdaten, und wählen Sie Show (decoded) aus.

Suchen Sie die Informationen in den Common Name (CN) und Subject Alternative Name (SAN) wie im Bild gezeigt:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA
        Validity
            Not Before: Dec 2 04:39:57 2019 GMT
            Not After : Nov 28 00:32:43 2020 GMT
        Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, CN=expe.domain.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
               Modulus:
                  -----,
        _____
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
         TLS Web Client Authentication, TLS Web Server Authentication
    X509v3 Subject Alternative Name:
        DNS:expe.domain.com, DNS:domain.com
    X509v3 Subject Key Identifier:
        92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B
    X509v3 Authority Kev Identifier:
         keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32
```

Nachdem Sie die CN und die SANs kennen, können sie dem neuen CSR hinzugefügt werden.

Optional können Sie die zusätzlichen Informationen für das Zertifikat kopieren, das Land (C), Bundesland (ST), Lokalität (L), Organisation (O), Organisationseinheit (OU) ist. Diese Informationen befinden sich neben der CN.

Schritt 2: Erstellen Sie einen neuen CSR mit den oben angegebenen Informationen.

Navigieren Sie zum Erstellen des CSR zu Maintenance > Security > Server Certificate.

Suchen Sie den Abschnitt CSR (Certificate Signing Request), und wählen Sie Generate CSR (CSR erstellen, wie im Bild gezeigt:

Г	Certificate signing request (CSR)		
	Certificate request	There is no certificate signing request in progress	
(Generate CSR		

Geben Sie die aus dem aktuellen Zertifikat gesammelten Werte ein.

Die CN kann nur geändert werden, wenn es sich um einen Cluster handelt. Im Fall eines Clusters können Sie den CN als Expressway Fully Qualified Domain Name (FQDN) oder Cluster FQDN auswählen. In diesem Dokument wird ein einzelner Server verwendet. Daher entspricht der CN dem, was Sie aus dem aktuellen Zertifikat erhalten haben, wie im Bild gezeigt:

Generate CSR			
Common name			
Common name		FQDN of Expressway	Y
Common name as it w	ill appear	expe.domain.com	

Für die SANs müssen Sie die Werte manuell eingeben, falls sie nicht automatisch kopiert werden. Um dies zu erreichen, können Sie die Werte für die **zusätzlichen alternativen Namen** eingeben, wenn Sie mehrere SANs haben, die durch Kommata getrennt werden müssen, z. B.: example1.domain.com, example2.domain.com, example3.domain.com. Nach dem Hinzufügen werden die SANs im Abschnitt **Alternative** aufgelistet, wie im Bild gezeigt:

Alternative name	
Additional alternative names (comma separated) domain.com	(i)
Unified CM registrations domains	Format DNS V
Alternative name as it will appear DNS:domain.c	m

Die **Zusatzinformationen** müssen manuell eingegeben werden, wie im Bild gezeigt, wenn sie nicht automatisch kopiert oder geändert werden müssen:

Additional information	
Key length (in bits)	4096 🗸 👔
Digest algorithm	SHA-256 🗸 👔
Country	* MX (1)
State or province	* CDMX (1)
Locality (town name)	* CDMX (1)
Organization (company name)	* TAC (1)
Organizational unit	* TAC
Email address	

```
Generate CSR
```

Wählen Sie anschließend CSR erstellen.

Schritt 3: Überprüfen und Herunterladen des neuen CSR

Nachdem der CSR generiert wurde, können Sie im CSR-Abschnitt der

Zertifikatssignierungsanfrage die Option Show (decoded) auswählen, um zu überprüfen, ob alle SANs vorhanden sind, wie im Bild gezeigt:

Г	Certificate signing request (CSR)]	
	Certificate request Generated on	Show (decoded) Show (PEM file) Download Apr 20 2020	

Discard CSR

Suchen Sie im neuen Fenster nach dem **CN** und dem **Betreff Alternative Name**, wie im Bild gezeigt:

```
Certificate Request:

Data:

Version: 0 (0x0)

Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:
```

Die CN wird immer automatisch als SAN hinzugefügt:

```
X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Subject Alternative Name:

DNS:expe.domain.com, DNS:domain.com

Signature Algorithm: sha256WithRSAEncryption
```

Nachdem die CSR-Anfrage überprüft wurde, können Sie das neue Fenster schließen und im CSR-Bereich (Certificate Signing Request) Download (decodiert) auswählen, wie im Bild gezeigt:

Н	Certificate signing request (CSR)		
	Certificate request Generated on	Show (decoded) Show (PEM file) Apr 20 2020	Download
L			

Discard CSR

Nach dem Download können Sie die neue CSR an Ihre Zertifizierungsstelle (Certificate Authority, CA) senden, um sie zu signieren.

Schritt 4: Überprüfen Sie die im neuen Zertifikat enthaltenen Informationen.

Wenn das neue Zertifikat von der CA zurückgegeben wurde, können Sie überprüfen, ob alle SANs im Zertifikat vorhanden sind. Dazu können Sie das Zertifikat öffnen und nach den SAN-Attributen suchen. In diesem Dokument wird ein Windows-PC verwendet, um die Attribute anzuzeigen. Dies ist nicht die einzige Methode, solange Sie das Zertifikat zum Überprüfen der Attribute öffnen oder decodieren können.

Öffnen Sie das Zertifikat, navigieren Sie zur Registerkarte **Details**, und suchen Sie nach **Betreff**. Es sollte den CN und die zusätzlichen Informationen enthalten, wie im Bild gezeigt:

		C	ertificate	x
General	Details	Certification Pa	ath	
Show:	<all></all>		~	
Field	lid to biect		Value Friday, November 27, 2020 5: expe.domain.com, TAC, TAC,	
En Su	blic key hanced Ki bject Alte	ey Usage rnative Name	RSA (4096 Bits) Client Authentication (1.3.6.1 DNS Name=expe.domain.com,.	=
a Sul Au a CR	bject Key thority Ke L Distribu	Identifier y Identifier tion Points	92 d0 d7 24 4a bc e3 c0 02 e5. KeyID=6c 71 80 4c 9a 21 79 d. [1]CRL Distribution Point: Distr.	
CN = e OU = T O = TA L = CD S = CD C = MX	xpe.doma AC IC MX MX	ain.com	Edit Properties Copy to File	ž
				ОК

Suchen Sie auch nach dem Abschnitt **Subject Alternative Name** (**Subject Alternative Name**), der die SANs enthalten muss, die Sie im CSR eingegeben haben, wie im Bild gezeigt:

📃 Ce	rtificate	x
General Details Certification Pat	h	
Show: <all></all>	*	
Field	Value	
🕎 Valid to	Friday, November 27, 2020 5:	
Subject	expe.domain.com, TAC, TAC,	
Public key	RSA (4096 Bits)	
Enhanced Key Usage	Client Authentication (1.3.6.1	=
Subject Alternative Name	DNS Name=expe.domain.com,	
Subject Key Identifier	92 d0 d7 24 4a bc e3 c0 02 e5	
Authority Key Identifier	KeyID=6c 71 80 4c 9a 21 79 d	
CRL Distribution Points	[1]CRL Distribution Point: Distr	~
		_
DNS Name=expe.domain.com		
DNS Name=domain.com		
1		_
	dit Properties	
	copy to meth	- 1
	OK	

Wenn nicht alle SANs vorhanden sind, die Sie im CSR eingegeben haben, wenden Sie sich an das CA, um zu sehen, ob zusätzliche SANs für Ihr Zertifikat zulässig sind.

Schritt 5: Laden Sie ggf. die neuen Zertifizierungsstellenzertifikate in den vertrauenswürdigen Server-Store hoch.

Wenn die CA die gleiche ist, die Ihr altes Expressway-Zertifikat signiert hat, können Sie diesen Schritt verwerfen. Wenn es sich um eine andere CA handelt, müssen Sie die neuen Zertifizierungsstellenzertifikate in die Liste der vertrauenswürdigen Zertifizierungsstellen auf jedem der Expressway-Server hochladen. Wenn Sie Transport Layer Security (TLS)-Zonen zwischen den Expressways haben, z.B. zwischen einem Expressway-C und einem Expressway-E, müssen Sie die neuen CAs auf beide Server hochladen, damit sie sich gegenseitig vertrauen können.

Dazu können Sie Ihre Zertifizierungsstellenzertifikate einzeln hochladen. Navigieren Sie zu Maintenance > Security > Trusted CA Certificates (Wartung > Sicherheit > Vertrauenswürdige Zertifizierungsstellenzertifikate) auf dem Expressway's.

1. Wählen Sie Durchsuchen aus.

- 2. Wählen Sie auf der neuen Seite das Zertifizierungsstellenzertifikat aus.
- 3. Wählen Sie Zertifizierungsstellenzertifikat anhängen aus.

Dieses Verfahren muss für jedes CA-Zertifikat in der Zertifikatskette (Root und Intermediate) durchgeführt werden und muss auf allen Expressway-Servern auch dann durchgeführt werden, wenn sie geclustert sind.

Schritt 6: Laden Sie das neue Zertifikat auf den Expressway Server hoch.

Wenn alle Informationen im neuen Zertifikat korrekt sind, gehen Sie zum Hochladen des neuen Zertifikats zu: Wartung > Sicherheit > Serverzertifikat.

Suchen Sie den Abschnitt Neues Zertifikat hochladen, wie im Bild gezeigt:

- 1. Wählen Sie Durchsuchen im Abschnitt Serverzertifikatdatei auswählen aus.
- 2. Wählen Sie das neue Zertifikat aus.
- 3. Wählen Sie Serverzertifikatdaten hochladen aus.

Г	Upload new certificate	
	Select the server private key file Select the server certificate file	System will use the private key file generated at the same time as the CSR. Browse ExpECertNew.cer
1	Upload server certificate data	

Wenn das neue Zertifikat vom Expressway akzeptiert wird, fordert der Expressway einen Neustart an, um die Änderungen anzuwenden, und die Meldung zeigt das neue Ablaufdatum für das Zertifikat an, wie im Bild gezeigt:

Server certificate			
Eiles uploaded: Server certificate updated, however a restart s required for this to take effect.			
Certificate info: This certificate expires on Nov 28 2020.			
Server certificate data			
Server certificate	Show (decoded) Show (PEM file)		
Currently loaded certificate expires on	Nov 28 2020		
Certificate Issuer	anmiron-SRV-AD-CA		

Reset to default server certificate

Um den Expressway neu zu starten, wählen Sie restat.

Überprüfen

Wenn der Server wieder installiert ist, muss das neue Zertifikat installiert worden sein, können Sie folgendermaßen navigieren: Wartung > Sicherheit > Serverzertifikat zur Bestätigung

Suchen Sie die **Serverzertifikatdaten**, und suchen Sie nach dem **derzeit geladenen Zertifikat**, das **im** Abschnitt **abläuft**, und zeigen Sie das neue Ablaufdatum für das Zertifikat an, wie im Bild gezeigt:

Server certificate	
Server certificate data]
Server certificate	Show (decoded) Show (PEM file)
Currently loaded certificate expires on	Nov 28 2020
Certificate Issuer	anmiron-SRV-AD-CA

Reset to default server certificate

Fehlerbehebung

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