Genere un certificado de Expressway nuevo con la información del certificado actual.

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Paso 1. Localice la información actual del certificado. Paso 2. Cree una nueva CSR con la información obtenida anteriormente. Paso 3. Verifique y descargue la nueva CSR. Paso 4. Verifique la información contenida en el nuevo certificado. Paso 5. Cargue los nuevos certificados de CA en el almacén de confianza de servidores si procede. Paso 6. Cargue el nuevo certificado en el servidor de Expressway. Verificación Troubleshoot

Introducción

Este documento describe cómo generar una nueva solicitud de firma de certificado (CSR) con la información del certificado de Expressway existente.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Atributos de certificado
- Expressway o Video Communication Server (VCS)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1. Localice la información actual del certificado.

Para obtener la información contenida en el certificado actual, navegue hasta **Mantenimiento > Seguridad > Certificado de servidor** en la interfaz gráfica de usuario (GUI) de Expressway.

Localice la sección Datos del certificado del servidor y seleccione Mostrar (descodificado).

Busque la información en el **Nombre común (CN)** y **Nombre alternativo del sujeto (SAN)** como se muestra en la imagen:

```
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 Key Identifier:
        keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32
```

Ahora que conoce el CN y la SAN, cópielos para que se puedan agregar al nuevo CSR.

Opcionalmente, puede copiar la información adicional para el certificado que es País (C), Estado (ST), Localidad (L), Organización (O), Unidad organizativa (OU). Esta información está junto a la CN.

Paso 2. Cree una nueva CSR con la información obtenida anteriormente.

Para crear la CSR, navegue hasta Mantenimiento > Seguridad > Certificado de servidor.

Busque la sección **Solicitud de firma de certificado (CSR)** y seleccione **Generar CSR** como se muestra en la imagen:

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

Introduzca los valores recopilados del certificado actual.

El CN no puede modificarse a menos que sea un clúster. En el caso de un clúster, puede seleccionar el CN para que sea el nombre de dominio completo (FQDN) de Expressway o el FQDN del clúster. En este documento se utiliza un único servidor y, por lo tanto, el CN corresponde a lo que obtuvo del certificado actual, como se muestra en la imagen:

¢	Generate CSR		
Γ	Common name		
	Common name	FQDN of Expressway	
	Common name as it will appear	expe.domain.com	
L			

Para las SANs, debe ingresar los valores manualmente en caso de que no se rellenen automáticamente, para hacerlo puede ingresar los valores en los **nombres alternativos adicionales**, si tiene varias SANs deben estar separadas por comas, por ejemplo: ejemplo1.dominio.com, ejemplo2.dominio.com, ejemplo3.dominio.com. Una vez agregadas, las SAN se enumeran en la sección **Nombre alternativo, ya que** aparecerá, como se muestra en la imagen:

[Alternative name		
	Additional alternative names (comma separated)	domain.com	
	Unified CM registrations domains		Format DNS v
	Alternative name as it will appear	DNS:domain.com	

La **información adicional** es obligatoria, si no se rellena automáticamente o hay que cambiarla, debe introducirse manualmente como se muestra en la imagen:

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

```
Generate CSR
```

Una vez finalizado, seleccione Generar CSR.

Paso 3. Verifique y descargue la nueva CSR.

Ahora que se genera la CSR, puede seleccionar **Mostrar (decodificado)** en la sección **Solicitud de firma de certificado (CSR)** para verificar que todas las SAN estén presentes, como se muestra en la imagen:

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

Discard CSR

En la nueva ventana, busque el **CN** y el **nombre alternativo del sujeto** como se muestra en la imagen:

```
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:
```

La CN siempre se agrega como una SAN automáticamente:

```
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
```

Ahora que se ha verificado el CSR, puede cerrar la nueva ventana y seleccionar **Descargar** (descodificado) en la sección Solicitud de firma de certificado (CSR) como se muestra en la imagen:

۲	Certificate signing request (CSR)		
	Certificate request	Show (decoded) Show (PEM file) Do	wnload
	Generated on	Apr 20 2020	
-			

Discard CSR

Después de descargarlo, puede enviar la nueva CSR a su Autoridad de Certificación (CA) para que la firme.

Paso 4. Verifique la información contenida en el nuevo certificado.

Una vez que el nuevo certificado se devuelve de la CA, puede verificar si todas las SAN están presentes en el certificado. Para ello, puede abrir el certificado y buscar los atributos de SAN. En este documento se utiliza un equipo de Windows para ver los atributos, este no es el único método siempre y cuando pueda abrir o descodificar el certificado para revisar los atributos.

Abra el certificado y navegue hasta la pestaña **Detalles** y busque **Asunto**, debe contener la CN y la Información Adicional como se muestra en la imagen:

			Cert	ificate	x
General	Details	Certification	Path]	
Show: <	All>			~	
Field				Value	^
📴 Valid	to			Friday, November 27, 2020 5:	
🧱 Subje	ect			expe.domain.com, TAC, TAC,	
🕎 Public	c key			RSA (4096 Bits)	
Enha	nced Ke	ey Usage		Client Authentication (1.3.6.1	≡
Subje	ect Alter	mative Name		DNS Name=expe.domain.com,	
Subje	ect Key	Identifier		92 d0 d7 24 4a bc e3 c0 02 e5	
Authority	ority Ke	y Identifier		KeyID=6c 71 80 4c 9a 21 79 d	
CRL 0	Distribu	tion Points		[1]CRL Distribution Point: Distr	~
CN = exp OU = TAC O = TAC L = CDMX S = CDM0 C = MX	e.doma C (in.com			
			Ed	it Properties Copy to File	

También busque la sección **Nombre alternativo del asunto**, debe contener las SAN que ingresó en la CSR como se muestra en la imagen:

📃 Cer	tificate	x
General Details Certification Path]	
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 =evne domain com		
DNS Name=domain.com		
E	dit Properties Copy to File	
	OK	

Si todas las SAN que ha introducido en la CSR no están presentes en el nuevo certificado, póngase en contacto con su CA para ver si se permiten SAN adicionales para su certificado.

Paso 5. Cargue los nuevos certificados de CA en el almacén de confianza de servidores si procede.

Si la CA es la misma que firmó el certificado antiguo de Expressway, puede descartar este paso. Si se trata de una CA diferente, debe cargar los nuevos certificados de CA en la lista de CA de confianza en cada uno de los servidores de Expressway. Si tiene zonas de seguridad de la capa de transporte (TLS) entre Expressway, por ejemplo entre Expressway-C y Expressway-E, debe cargar las nuevas CA en ambos servidores para que puedan confiar entre sí.

Para hacerlo, puede cargar sus certificados de CA uno por uno. Vaya a **Mantenimiento >** Seguridad > Certificados CA de confianza en Expressway.

- 1. Seleccione Examinar.
- 2. En la nueva página, seleccione el certificado de CA.
- 3. Seleccione Agregar certificado de CA.

Este procedimiento debe realizarse para cada certificado de CA en la cadena de certificados (raíz e intermedio) y debe hacerse en todos los servidores de Expressway incluso si están agrupados.

Paso 6. Cargue el nuevo certificado en el servidor de Expressway.

Si toda la información en el nuevo certificado es correcta, para cargar el nuevo certificado navegue a: Mantenimiento > Seguridad > Certificado de servidor.

Localice la sección Cargar certificado nuevo como se muestra en la imagen:

- 1. Seleccione Browse en la sección Select the server certificate file .
- 2. Seleccione el nuevo certificado.
- 3. Seleccione Cargar datos del certificado de servidor.

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

Si Expressway acepta el nuevo certificado, Expressway solicita un reinicio para aplicar los cambios y el mensaje muestra la nueva fecha de vencimiento del certificado, como se muestra en la imagen:

;	Server certificate			
	Files 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		

Para reiniciar Expressway seleccione reinicio.

Verificación

Una vez que el servidor haya recuperado el nuevo certificado debe haber sido instalado, puede navegar a: **Mantenimiento > Seguridad > Certificado de servidor** para confirmar.

Localice los **datos del certificado del servidor** y busque la sección **El certificado cargado actualmente caduca en**, muestra la nueva fecha de vencimiento del certificado como se muestra en la imagen:

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				

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.