

Solución de problemas de IOS XR 30 de septiembre de 2021 - Vencimiento del certificado CA X3 raíz DST

Contenido

[Introducción](#)

[Ejemplo de certificado](#)

[30 de septiembre de 2021](#)

[El 30 de septiembre de 2021 y después](#)

[Mensajes de vencimiento del certificado](#)

[Solución Alternativa](#)

[Pre-caducidad](#)

[Post-caducidad](#)

[Solución](#)

Introducción

Este documento describe el significado del 30 de septiembre de 2021, el vencimiento del certificado integrado 'DST Root CA X3' y cualquier acción necesaria que sea necesaria para resolver. En la mayoría de los casos, no se necesita ninguna acción inmediata.

Una comunicación externa del editor de CA raíz está disponible aquí:

<https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/>

Ejemplo de certificado

```
RP/0/RP0/CPU0:NCS-5516-A#show crypto ca trustpool
Fri Oct 1 00:00:35.206 UTC
```

```
Trustpool: Built-In
```

```
=====
```

```
CA certificate
```

```
Serial Number : 5F:F8:7B:28:2B:54:DC:8D:42:A3:15:B5:68:C9:AD:FF
```

```
Subject:
```

```
CN=Cisco Root CA 2048,O=Cisco Systems
```

```
Issued By :
```

```
CN=Cisco Root CA 2048,O=Cisco Systems
```

```
Validity Start : 20:17:12 UTC Fri May 14 2004
```

```
Validity End : 20:25:42 UTC Mon May 14 2029
```

```
SHA1 Fingerprint:
```

```
DE990CED99E0431F60EDC3937E7CD5BF0ED9E5FA
```

```
Trustpool: Built-In
```

```
=====
```

```
CA certificate
```

```
Serial Number : 2E:D2:0E:73:47:D3:33:83:4B:4F:DD:0D:D7:B6:96:7E
```

```
Subject:
```

CN=Cisco Root CA M1,O=Cisco
Issued By :
CN=Cisco Root CA M1,O=Cisco
Validity Start : 21:50:24 UTC Tue Nov 18 2008
Validity End : 21:59:46 UTC Fri Nov 18 2033
SHA1 Fingerprint:
45AD6BB499011BB4E84E84316A81C27D89EE5CE7

Trustpool: Built-In

=====

CA certificate

Serial Number : 44:AF:B0:80:D6:A3:27:BA:89:30:39:86:2E:F8:40:6B

Subject:

CN=DST Root CA X3,O=Digital Signature Trust Co.

Issued By :

CN=DST Root CA X3,O=Digital Signature Trust Co.

Validity Start : 21:12:19 UTC Sat Sep 30 2000

Validity End : 14:01:15 UTC Thu Sep 30 2021

SHA1 Fingerprint:

DAC9024F54D8F6DF94935FB1732638CA6AD77C13

Trustpool: Built-In

=====

CA certificate

Serial Number : 3C:91:31:CB:1F:F6:D0:1B:0E:9A:B8:D0:44:BF:12:BE

Subject:

OU=Class 3 Public Primary Certification Authority,O=VeriSign\, Inc.,C=US

Issued By :

OU=Class 3 Public Primary Certification Authority,O=VeriSign\, Inc.,C=US

Validity Start : 00:00:00 UTC Mon Jan 29 1996

Validity End : 23:59:59 UTC Wed Aug 02 2028

SHA1 Fingerprint:

A1DB6393916F17E4185509400415C70240B0AE6B

Trustpool: Built-In

=====

CA certificate

Serial Number : 05:09

Subject:

CN=QuoVadis Root CA 2,O=QuoVadis Limited,C=BM

Issued By :

CN=QuoVadis Root CA 2,O=QuoVadis Limited,C=BM

Validity Start : 18:27:00 UTC Fri Nov 24 2006

Validity End : 18:23:33 UTC Mon Nov 24 2031

SHA1 Fingerprint:

CA3AFBCF1240364B44B216208880483919937CF7

30 de septiembre de 2021

Antes del 30 de septiembre de 2021, los usuarios pueden obtener un mensaje de registro que indica que un certificado está a punto de caducar, como

%SECURITY-PKI-6-ERR_1_PARAM : CA certificate to be expired in 480 days

Este mensaje de registro puede continuar apareciendo hasta que el certificado caduque con una cuenta atrás en el número de días.

Los 480 días son incorrectos, los días se multiplican erróneamente por 24 horas, esto es manejado por el ID de bug de Cisco [CSCvz62603](#).

Por ejemplo, $480/24 = 20$ días.

El 30 de septiembre de 2021 y después

Este certificado no se utiliza y no afecta al tráfico de producción ni a los servicios de criptografía cuando se probó el vencimiento en el laboratorio.

Mensajes de vencimiento del certificado

Se pueden ver algunos mensajes de vencimiento diferentes en función de su versión de código:

```
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: syslog_dev[113]: cepki[261] PID-7101: % CA certificate is not yet valid or has expired.
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: syslog_dev[113]: cepki[261] PID-7101: % Make sure the clock is synchronized with CA's clock.
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: cepki[261]: %SECURITY-PKI-1-CACERT_NOT_VALID : Failed to add CA certificate with subject name /O=Digital Signature Trust Co./CN=DST Root CA X3 to trustpool because certificate has expired or is not yet valid
RP/0/RP0/CPU0:Oct 1 00:06:14.054 UTC: cepki[261]: %SECURITY-CEPKI-6-KEY_INFO : One or more host keypairs exist. Not auto-generating keypairs.
```

Estos mensajes pueden aparecer cada vez que se reinicia el proceso cepki o se recarga el router / se inicia el procesador de ruta (RP).

Solución Alternativa

- Para inhabilitar estos mensajes de syslogs, puede configurarlos para que sean eliminados, como en este ejemplo.
- No es necesario instalar el certificado de reemplazo, ya que no hay impacto en el certificado que vence.

Pre-caducidad

```
%SECURITY-PKI-6-ERR_1_PARAM : CA certificate to be expired in 480 days
```

```
logging suppress rule PRE_CERT_EXPIRY
alarm SECURITY PKI ERR_1_PARAM
!
logging suppress apply rule PRE_CERT_EXPIRY
all-of-router
!
```

Post-caducidad

```
RP/0/RP0/CPU0:Oct 1 00:06:13.572 UTC: cepki[261]: %SECURITY-PKI-1-CACERT_NOT_VALID : Failed to add CA certificate with subject name /O=Digital Signature Trust Co./CN=DST Root CA X3 to trustpool because certificate has expired or is not yet valid
```

```
logging suppress rule POST_CERT_EXPIRY
alarm SECURITY PKI CACERT_NOT_VALID
!
logging suppress apply rule POST_CERT_EXPIRY
```

all-of-router
!

Solución

- Debido a que el router tiene otro certificado válido en el Trustpool, el único impacto son los mensajes syslog. El certificado que vence no tiene impacto en el servicio y los servicios criptográficos todavía se pueden utilizar.
- Se ha abierto el Id. de error de Cisco [CSCvs7334](#) que elimina completamente este certificado de las versiones 7.3.2, 7.3.16, 7.4.1, 7.4.2 y 7.5.1 de XR.
- Este certificado ya no es utilizado por XR, ni es un certificado de reemplazo.