

Interfaz web para recuperar Video Communications Server (VCS): certificado revocado

Contenido

[Introducción](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Aplicación SCP \(por ejemplo: WinSCP\)](#)

Introducción

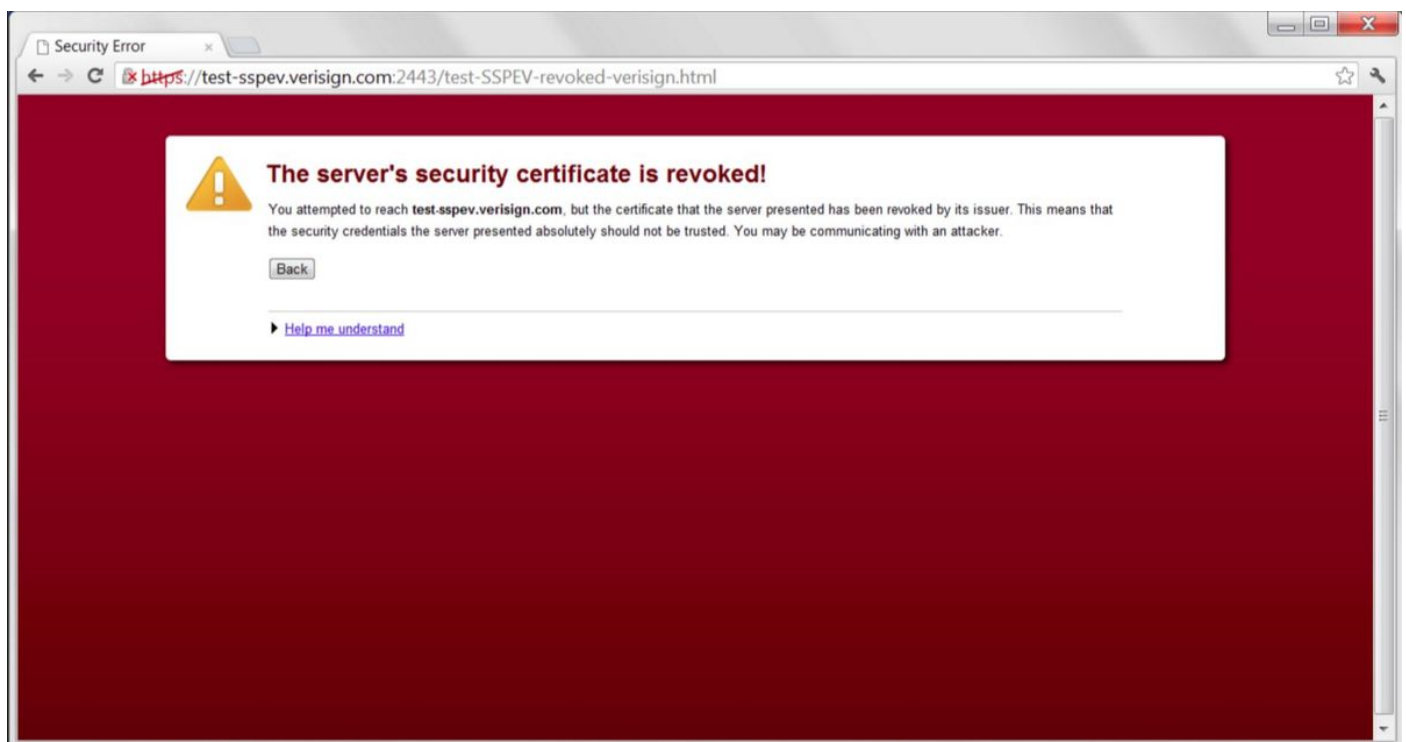
Este documento describe el escenario en el que se ha revocado el certificado en los servidores de Video Communications Server (VCS) y, como resultado, no se puede acceder a la interfaz gráfica de usuario (GUI).

Componentes Utilizados

VCS con certificado de servidor caducado

Problema

En esta situación, no tendría acceso a la GUI de VCS y un intento de acceder a VCS a través de la GUI le dará un error que indica que el certificado del servidor VCS ha sido revocado



Solución

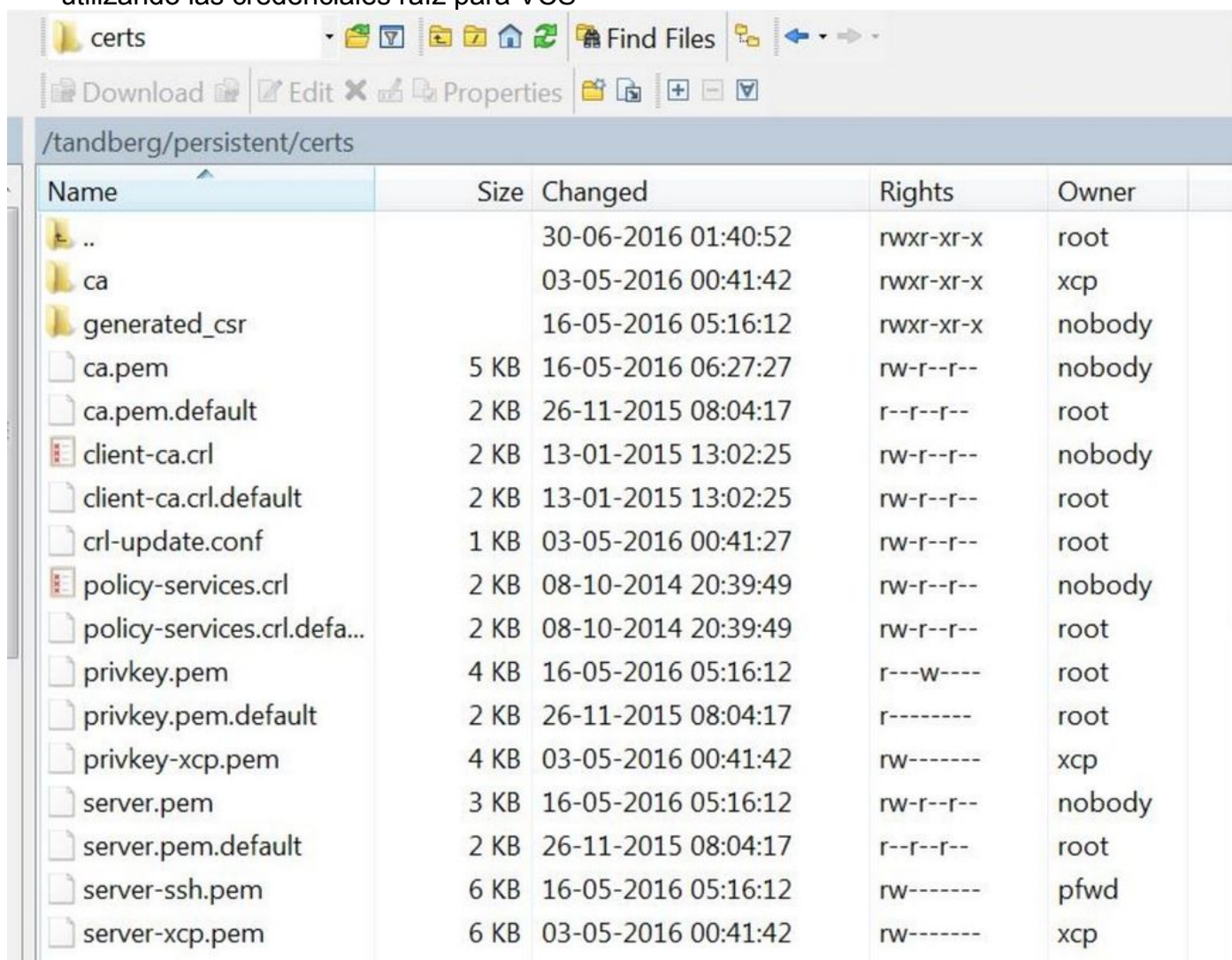
Para mitigar el problema, debería volver a los certificados predeterminados en el VCS. Esto habilitará el acceso a la GUI y, a continuación, los certificados tendrán que volver a generarse.

Puede realizar la tarea anterior de cualquiera de las dos maneras siguientes:

1. Uso de un software de protocolo de copia segura (SCP) (por ejemplo: WinSCP)
2. Uso de la interfaz de línea de comandos (CLI) raíz

Aplicación SCP (por ejemplo: WinSCP)

- Uso de la aplicación SFTP (protocolo seguro de transferencia de archivos) (por ejemplo: WinSCP), desplácese al directorio /tandberg/persistent/certs después de iniciar sesión utilizando las credenciales raíz para VCS



Name	Size	Changed	Rights	Owner
..		30-06-2016 01:40:52	rw-r--r--	root
ca		03-05-2016 00:41:42	rw-r--r--	xcp
generated_csr		16-05-2016 05:16:12	rw-r--r--	nobody
ca.pem	5 KB	16-05-2016 06:27:27	rw-r--r--	nobody
ca.pem.default	2 KB	26-11-2015 08:04:17	r--r--r--	root
client-ca.crl	2 KB	13-01-2015 13:02:25	rw-r--r--	nobody
client-ca.crl.default	2 KB	13-01-2015 13:02:25	rw-r--r--	root
crl-update.conf	1 KB	03-05-2016 00:41:27	rw-r--r--	root
policy-services.crl	2 KB	08-10-2014 20:39:49	rw-r--r--	nobody
policy-services.crl.defa...	2 KB	08-10-2014 20:39:49	rw-r--r--	root
privkey.pem	4 KB	16-05-2016 05:16:12	r---w----	root
privkey.pem.default	2 KB	26-11-2015 08:04:17	r-----	root
privkey-xcp.pem	4 KB	03-05-2016 00:41:42	rw-----	xcp
server.pem	3 KB	16-05-2016 05:16:12	rw-r--r--	nobody
server.pem.default	2 KB	26-11-2015 08:04:17	r--r--r--	root
server-ssh.pem	6 KB	16-05-2016 05:16:12	rw-----	pfwd
server-xcp.pem	6 KB	03-05-2016 00:41:42	rw-----	xcp

- Remove (KEEP BACKUP) server.pem, privkey.pem, ca.pem, client-ca.crl, policy-services.crl
- Reiniciar el servicio HTTP desde la raíz (/etc/init.d/S80httpd restart)

CLI DE RAÍZ

Utilice cualquier cliente SSH y ssh para VCS usando credetials raíz.

Para las versiones anteriores a VCS 12.5(todas las versiones 8.x), reemplace los certificados existentes por los certificados predeterminados utilizando los siguientes comandos:

```
~ # cp /tandberg/persistent/certs/server.pem.default /tandberg/persistent/certs/server.pem
~ # cp /tandberg/persistent/certs/privkey.pem.default /tandberg/persistent/certs/privkey.pem
~ # cp /tandberg/persistent/certs/ca.pem.default /tandberg/persistent/certs/ca.pem
~ # cp /tandberg/persistent/certs/client-ca.crl.default /tandberg/persistent/certs/client-ca.crl
~ # cp /tandberg/persistent/certs/policy-services.crl.default /tandberg/persistent/certs/policy-
services.crl

~ # /etc/init.d/S80httpd restart
```

Para la versión 12.5, los certificados predeterminados ya no existen en:

```
~ # cd /tandberg/persistent/certs

~ # ls
```

Aquí no verá los certificados .default.

Debe eliminar el server.pem y reiniciar el VCS, que volverá al VCS con los certificados predeterminados.

```
~ # rm server.pem

~ # reboot
```