NAC (CCA): Cómo reparar los errores del certificado en el CAM/CAS después de la actualización a 4.1.6

Contenido

Introducción

Este documento describe cómo reparar los errores del certificado en el servidor de acceso limpio del Access Manager (CAM) /Clean (CAS) con la versión 4.1.6.

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del proceso de actualización para el dispositivo del Cisco Network Admission Control (NAC).

Componentes Utilizados

La información en este documento se basa en la versión 4.1.6 del dispositivo NAC de Cisco con CAM/CAS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Procedimiento

Estos errores del certificado se encuentran en */perfigo/logs/perfigo-redirect.log0.log.0* o */perfigo/logs/perfigo-log0.log.0*.

Aquí está un ejemplo de un error del certificado:

```
SEVERE: RMISocketFactory:Creating RMI socket failed to host
        10.1.20.10:sun.security.validator.ValidatorException:
        Certificate chaining error
Aug 1, 2008 1:41:22 PM com.perfigo.wlan.web.admin.ConnectorClient connect
SEVERE: Communication Exception : java.rmi.ConnectIOException: Exception
        creating connection to: 10.1.20.10; nested exception is:
 javax.net.ssl.SSLHandshakeException:
        sun.security.validator.ValidatorException: Certificate chaining error
```

Estos errores son un resultado de las mejoras de la seguridad hechas en 4.1.6. En 4.1.6, CAS y el CAM actúan como cliente y servidor el uno al otro y deben confiarse en. Cada uno requiere los Certificados de la raíz y del intermedio del otro. Por ejemplo, si CAS tiene un certificado de Verisign y el CAM tiene un certificado (temporal) del perfigo, la necesidad de CAS y CAM el encadenamiento de Verisign (raíz y los intermedios) y la raíz del perfigo.

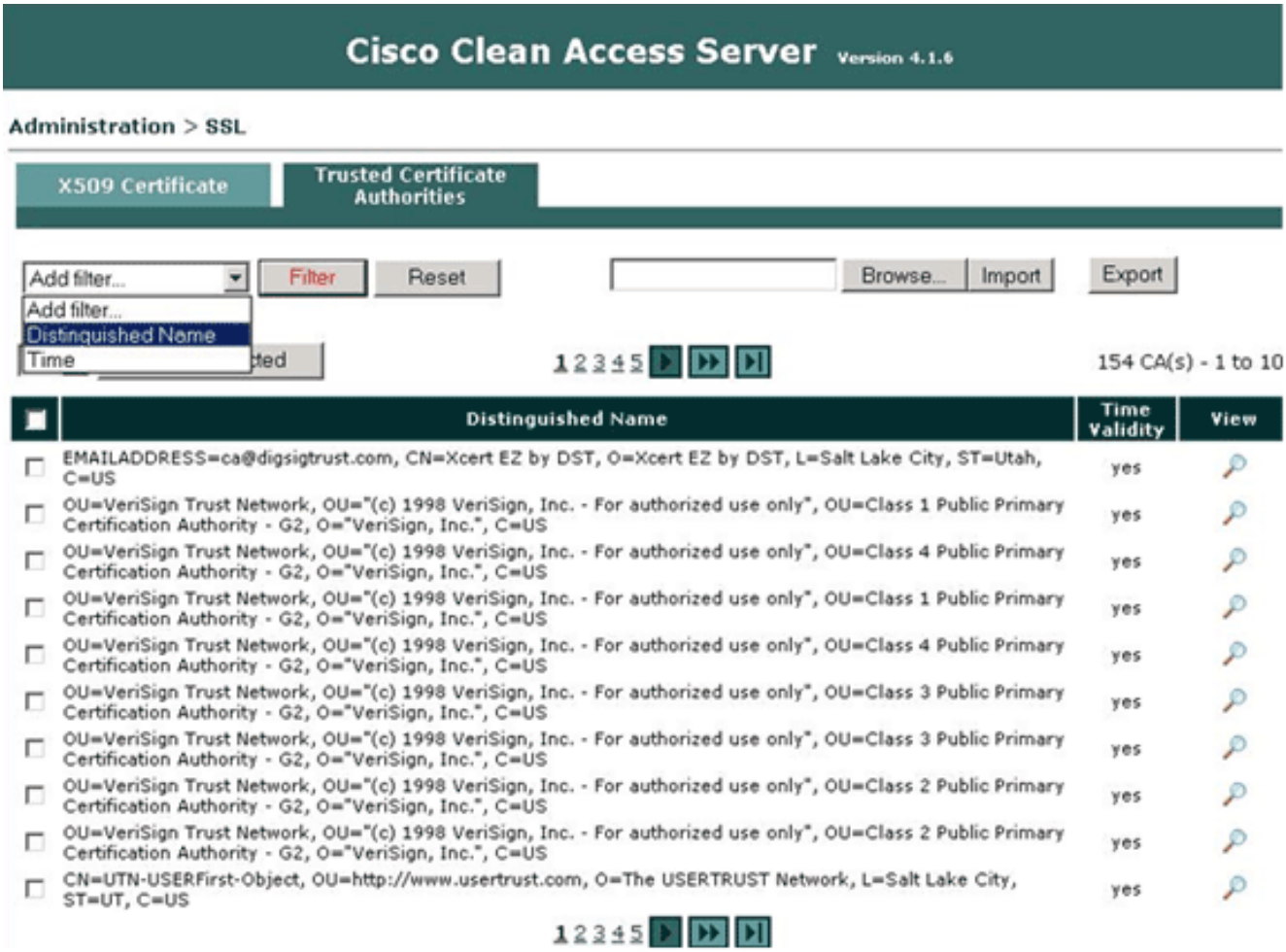
Complete estos pasos para reparar los errores del certificado:

1. Sostenga cualquier Certificados instalado que no sea Certificados temporales.En el CAM, abra la interfaz Web, y vaya a la **administración > CCA administrador > el certificado SSL > X509**.

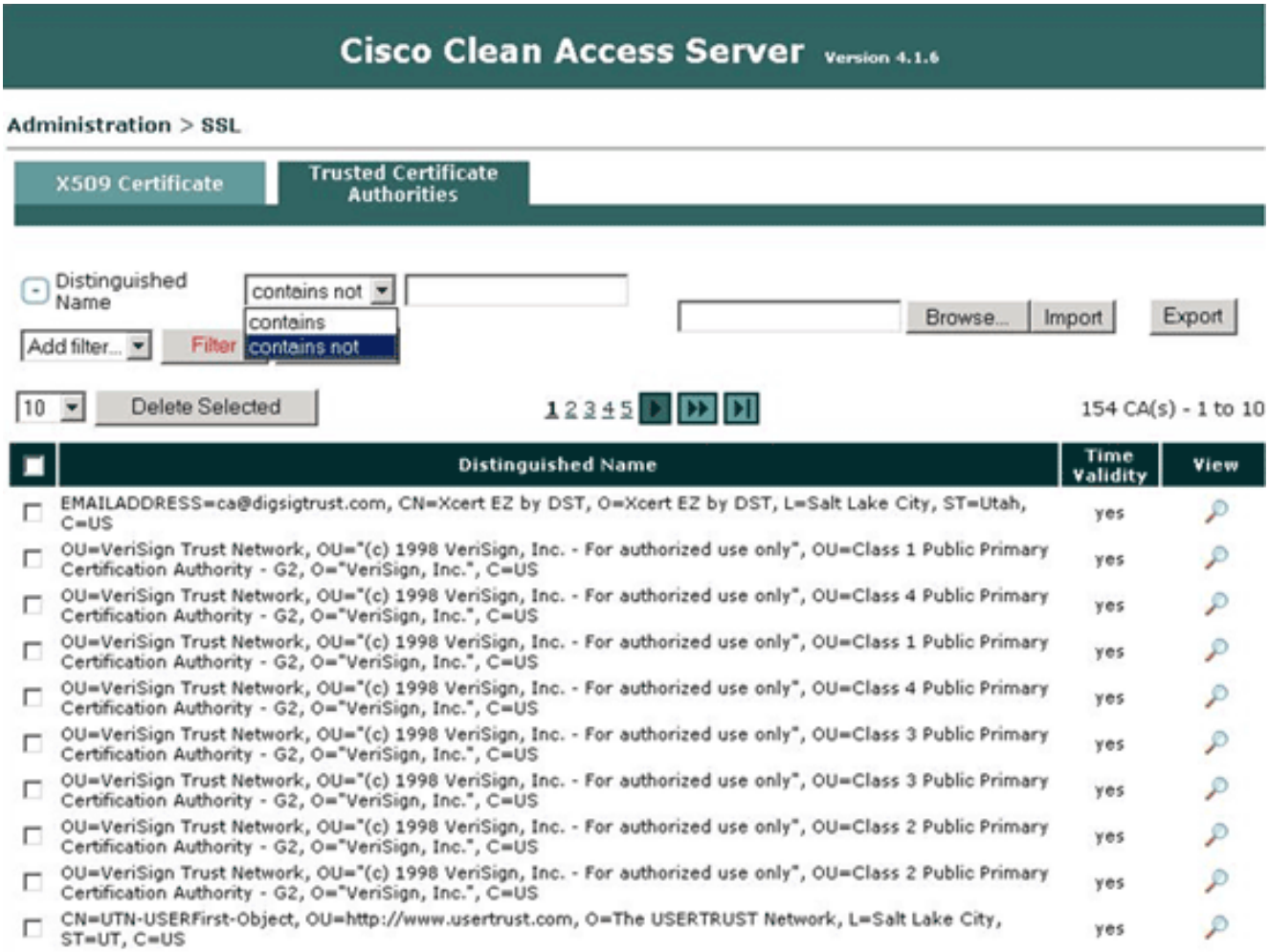
   En CAS, vaya directamente a la interfaz Web vía https:// <CAS IP>/admin, y después vaya a la **administración > al certificado SSL > X509**.

Elija la **clave/el certificado de la exportación CSR/Private del** elegir una lista desplegable de la acción.Haga clic la **exportación** situada al lado del certificado actualmente instalado, y salve este archivo.Haga clic la **exportación** situada al lado de la clave privada actualmente instalada, y salve este archivo.

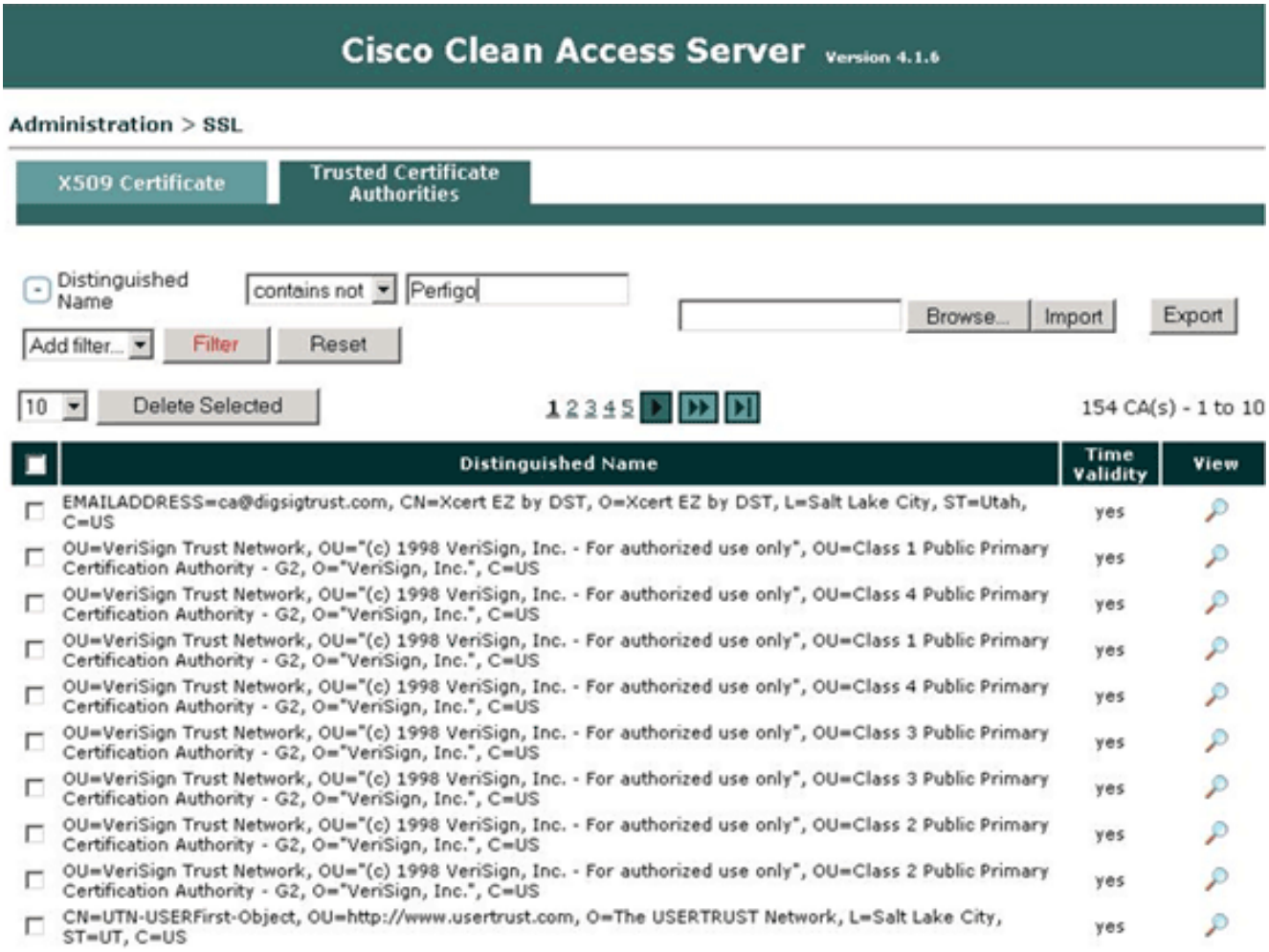
2. Después del respaldo, si CAS y el CAM no utilizan ya los Certificados temporales, genérelos.En el CAM, abra la interfaz Web, y vaya a la **administración > CCA administrador > el certificado SSL > X509**.En CAS, vaya directamente a la interfaz Web vía https:// <CAS IP>/admin, y después vaya a la **administración > al certificado SSL > X509**.Elija **generan el certificado temporal de la** lista desplegable.Complete los campos enumerados, y el tecleo **genera**.**Note**: Esto requiere no más una reinicialización tomar el efecto.
3. Quite todas las autoridades del certificado confiable de CAS y del CAM. Este paso hace más fácil manejar y mejorar la Seguridad.En el CAM, van a la **administración > CCA el administrador > el SSL > las autoridades del certificado confiable**.En CAS, vaya a la **administración > al SSL > a las autoridades del certificado confiable**.Cree un filtro para excluir el certificado del
perfigo.



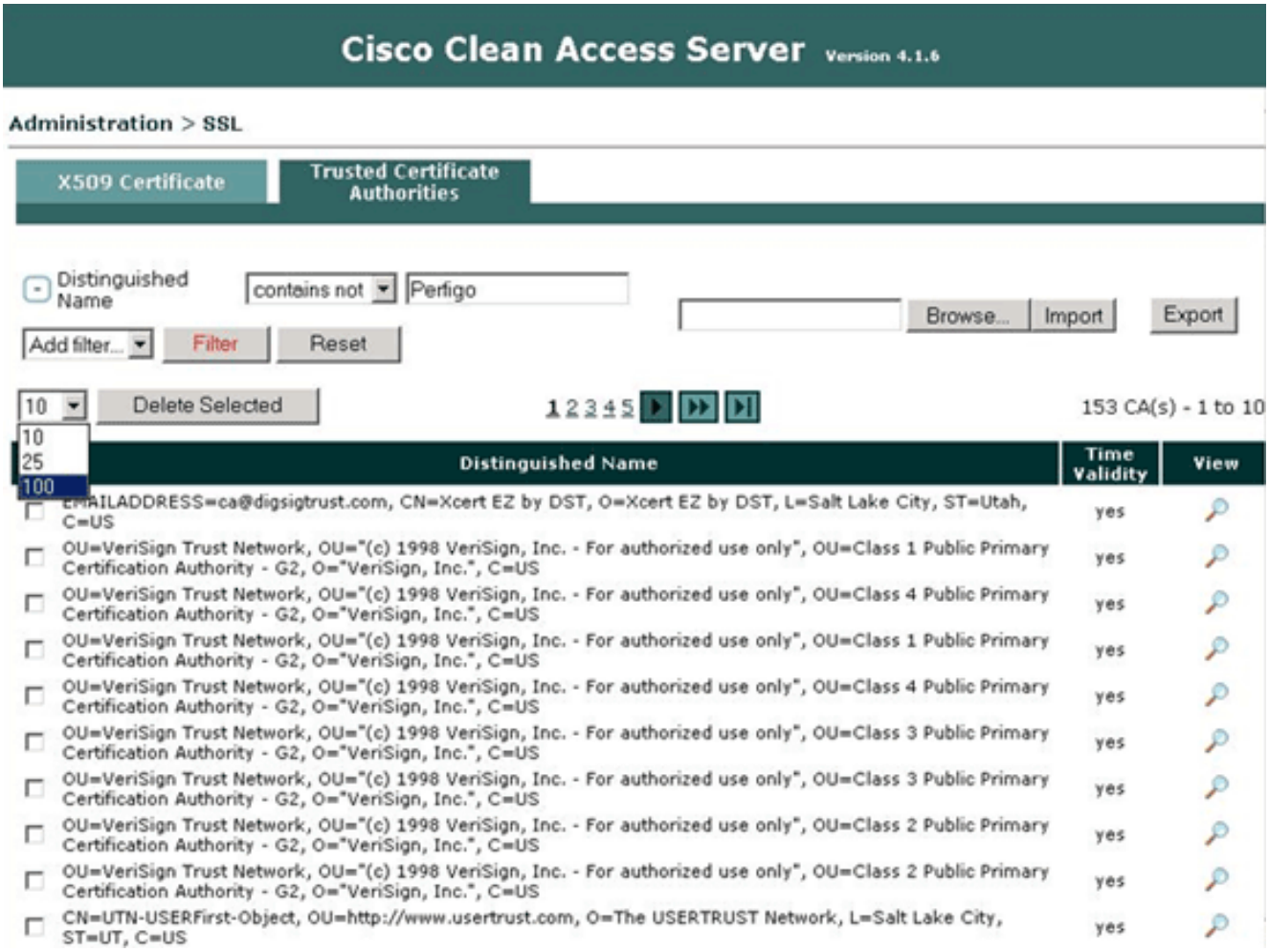
Elija el **nombre distintivo de la** lista desplegable del filtro del agregar.



Elija **contiene no de la** lista desplegable que aparece al lado del nombre distintivo.



Teclee el perfigo en el campo de texto, y después haga clic el **filtro**.



Elija 100 de la lista desplegable situada al lado del botón seleccionado cancelación.Haga clic la casilla de verificación debajo de la lista desplegable seleccionada cancelación para seleccionar todas las autoridades de certificación (CA) en la lista.Haga clic la **cancelación seleccionada** para borrar todos los CA en la lista.Continúe haciendo clic el cuadro, y haga clic la **cancelación seleccionada** hasta que se borren todos los CA.

4. Después de que usted quite todos los CA, los Certificados de la raíz y del intermedio deben ser importados.En el CAM, van a la **administración > CCA el administrador > el SSL > las autoridades del certificado confiable**.En CAS, vaya a la **administración > al SSL > a las autoridades del certificado confiable**.El tecleo **hojea**, y elige el certificado raíz primero.**Note**: El tema y el emisor se deben fijar al mismo valor.Haga clic la **importación**, y CA debe aparecer en la lista abajo.Realice el mismo procedimiento para cualquier Certificados intermedio.
5. Instale los Certificados de CAS y CAM que usted sostuvo en el primer paso.En el CAM, abra la interfaz Web, y vaya a la **administración > CCA administrador > el certificado SSL > X509**.En CAS, vaya directamente a la interfaz Web vía https:// <CAS IP>/admin, y después vaya a la **administración > al certificado SSL > X509**.Elija **Import Certificate (Importar certificado) de la** lista desplegable.El tecleo **hojea**, y elige el certificado guardado del paso 1.**Carga del** tecleo.Haga clic **hojean** otra vez, y eligen la clave privada que fue guardada del paso 1.Elija la **clave privada de la** lista desplegable del tipo de archivo, y después haga clic la **carga**.El tecleo **verifica y instala los Certificados cargados**.**Note**: Este mensaje de error no debe ser reparado por estos procedimientos:

```
SEVERE: SSLFilter:access deniedCN=cas1.domain.com,
        OU=Information Technologies, O=Company, ST=State,
        C=US:Netscape cert type does not permit use for SSL client
```

Si los registros contienen este mensaje, usted debe entrar en contacto el proveedor del certificado. El certificado se debe reeditar con el campo definido del tipo CERT de Netscape al servidor SSL y al cliente SSL.

Información Relacionada

- Página de soporte del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems