Resolución de problemas de falla de respaldo CER con mensaje de error

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Resolución de problemas

- Recopilación de registros
- Análisis de registro
- Acción Correctiva
  - Escenario 1
  - Escenario 2

Información Relacionada

Introducción

Este documento describe cómo resolver problemas de cómo Cisco Emergency Responder (CER) no realiza una copia de seguridad y muestra un mensaje de error en su estado.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre estos temas:

- Cisco Emergency Responder
- Comprensión básica de los certificados de seguridad

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

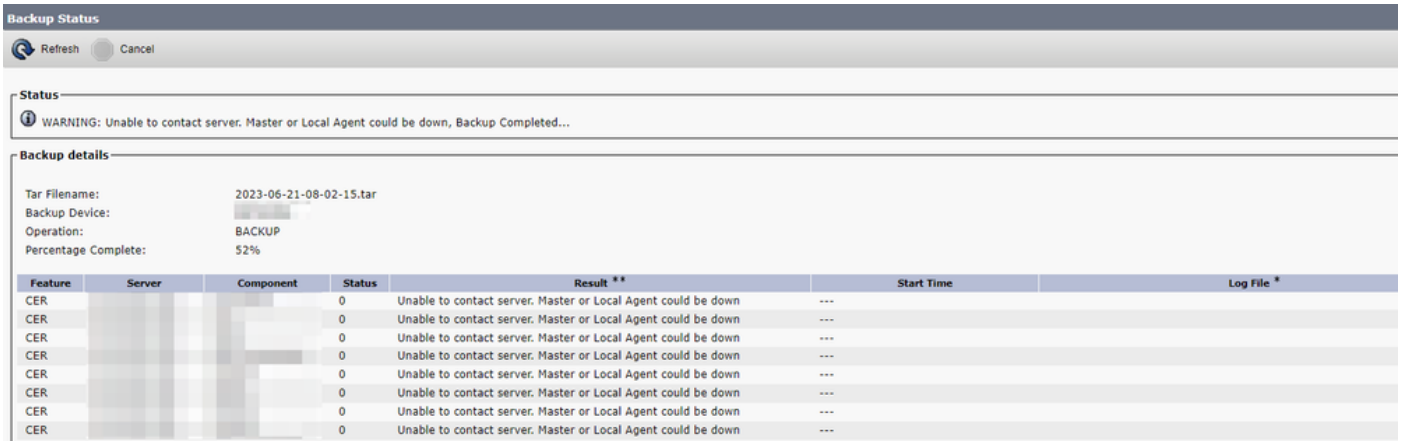
- Cisco Emergency Responder 11.5.4.60000-5

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El CER implementado en modo de clúster puede fallar al realizar la copia de seguridad con el mensaje de error "No se puede contactar con el servidor. Es posible que el agente maestro o local no funcione".

Por ejemplo:



Mensaje de error de respaldo CER

Las versiones afectadas son 11.x y superiores.

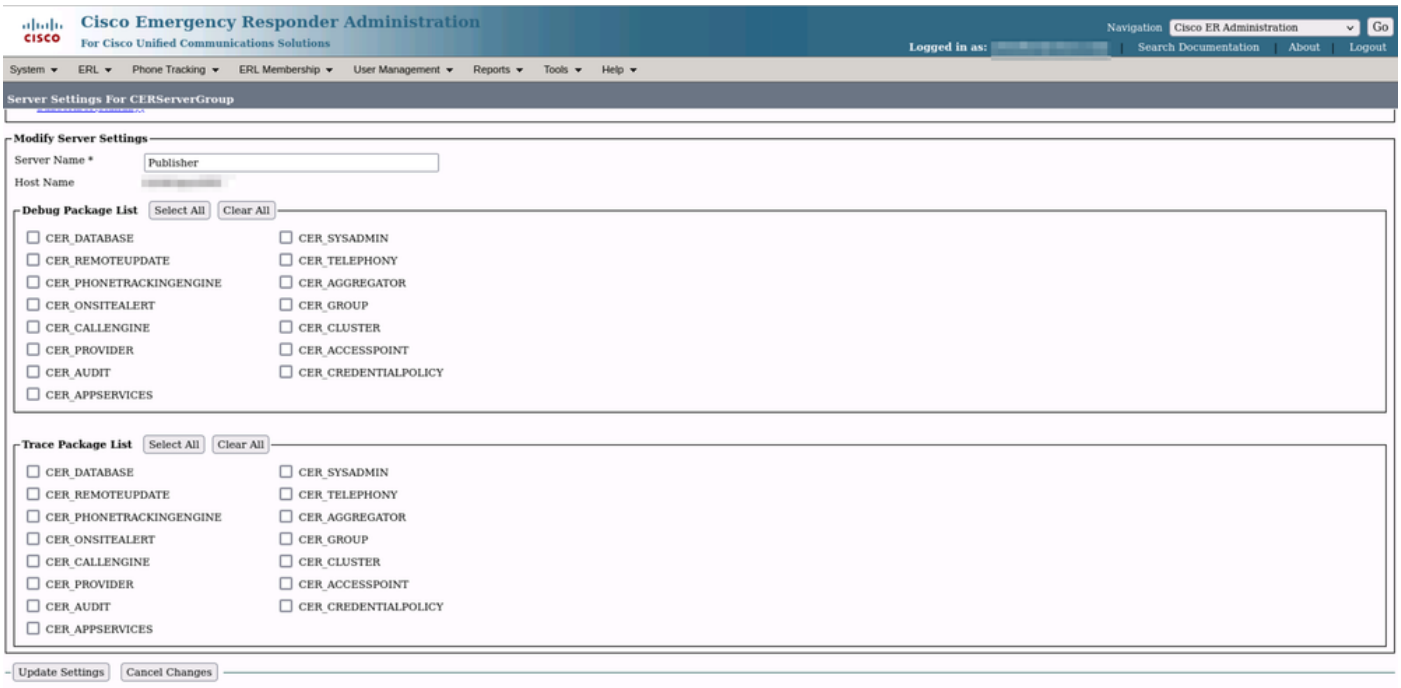
Resolución de problemas

Recopilación de registros

Cuando esto ocurra, recopile registros para intentar recopilar la mayor cantidad de información posible para intentar determinar el origen del problema y determinar el plan de acción correcto para resolverlo.

Antes de recopilar los registros, active el seguimiento detallado y la depuración siguiendo estos pasos:

1. Inicie sesión en la página web de administración de CER.
2. Vaya a System > Server Settings. El publicador CER está seleccionado de forma predeterminada y se puede cambiar si también se necesitan registros del suscriptor CER.
3. Haga clic en Select All para las secciones "Debug Package List" y "Trace Package List".
4. Haga clic en Update Settings.

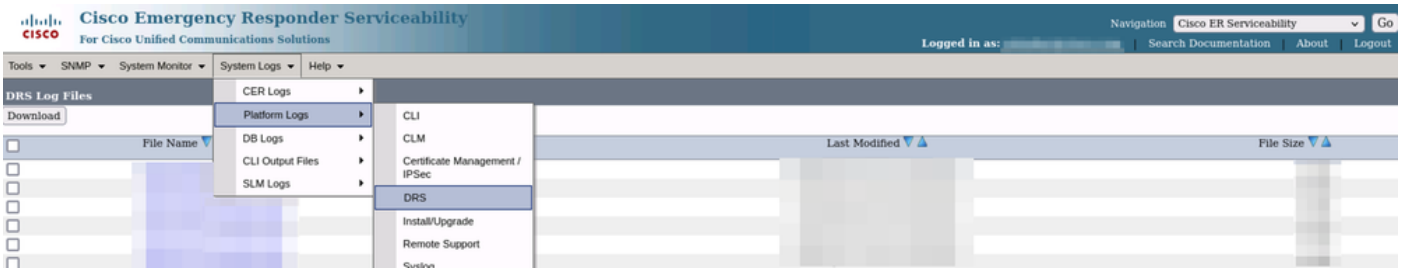


CER Habilitación de Depuraciones y Seguimientos

Llegados a este punto, replique el problema.

Una vez que se haya replicado el problema, continúe para recopilar los registros DRS aplicables al intento de replicación desde la página web Serviciabilidad de Cisco ER y complete estos pasos:

1. En Navigation, seleccione Cisco ER Serviceability.
2. Vaya a Registros del sistema > Registros de plataforma > DRS.



CER que recopila registros DRS

Análisis de registro

Cuando analizamos los registros, empezamos a ver dónde está tratando el servidor de establecer la conexión con su par y vemos el mensaje de error en los registros que nos señala la razón de la falla.

Desde los registros de MA de DRF del Editor CER:

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: Número de entradas en IP trustStore : 1
2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient:drfQueryTruststore - Consulta truststore cada 20 horas

2023-06-21 07:58:58,168 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: No se puede crear la secuencia de entrada/salida al cliente Alerta fatal recibida: Certificado incorrecto

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run: Solicitud de socket de cliente recibida desde /IP:Port
2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - Validación si la solicitud del cliente es de un nodo dentro del clúster
2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - Cliente validado. IP = 10.10.20.25 Nombre de host = device.test.org. La solicitud proviene de un nodo del clúster
2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Socket Object InputStream que se creará
2023-06-21 08:04:46,313 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: No se puede crear la secuencia de entrada/salida al cliente Alerta fatal recibida: Certificado incorrecto

Desde los registros locales de DRF del editor CER:

2023-06-21 07:58:47,453 DEBUG [principal] - drfNetServerClient: Reconnect, No se puede conectar al host: [X], mensaje: Conexión rechazada (Conexión rechazada), causa: null

Vemos hasta este punto que la conexión se rechaza debido a un certificado incorrecto.

El certificado que se utiliza para establecer la conexión de confianza entre los nodos para copias de seguridad o restauraciones es el IPSec. En ese momento, ya podemos determinar que el problema está relacionado con el certificado IPSec que ha caducado o con un certificado incorrecto que está presente en uno de los servidores.

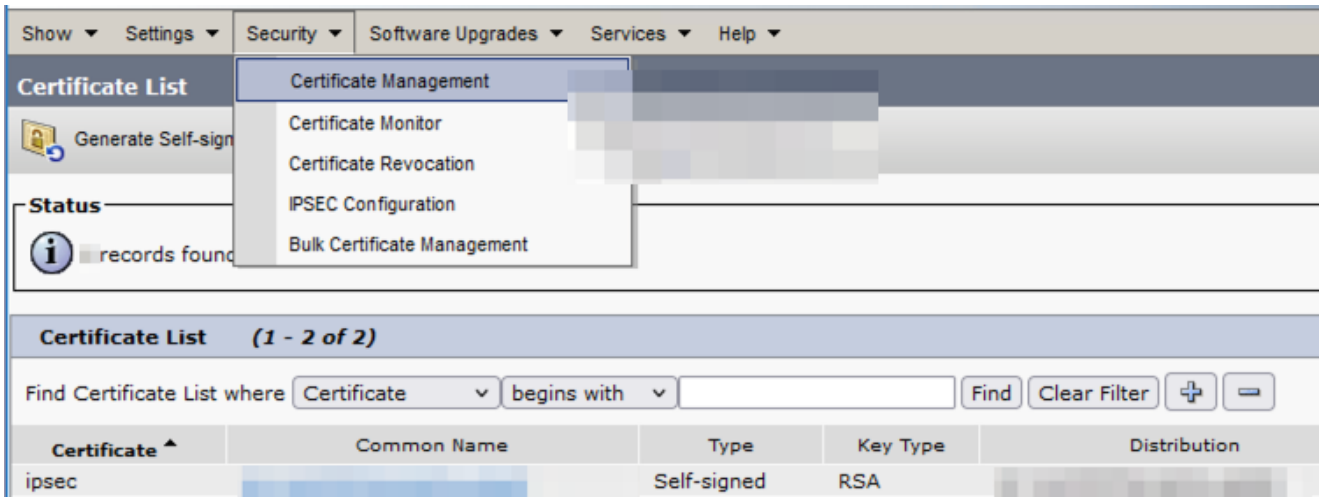
Acción Correctiva

1. Verifique el número de serie (SN) de los certificados de confianza IPSec en todos los nodos del suscriptor CER, éste debe coincidir con el SN del IPSec.prem del editor CER (Escenario 1).
2. Confirme la validez del certificado IPSec.pem en el nodo de editor CER. La fecha debe ser válida o el certificado IPSec debe regenerarse (situación 2).

Escenario 1

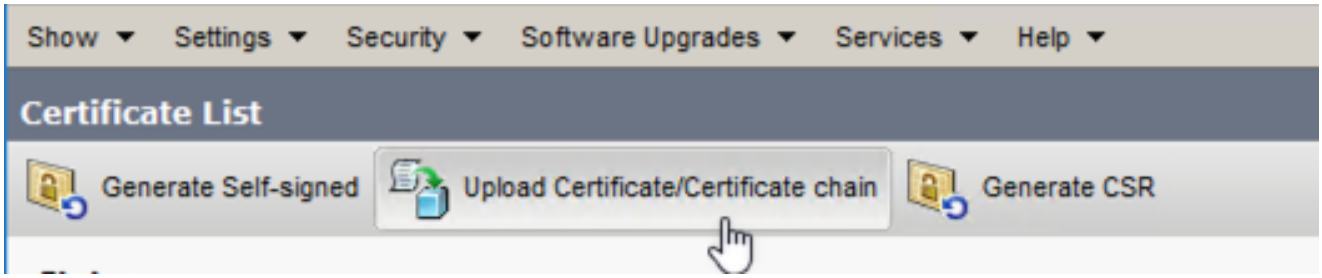
El SN del certificado IPSec no coincide entre el CER publicado y los suscriptores CER. Siga estos pasos:

1. Elimine el certificado de confianza IPSec en el suscriptor o suscriptores de CER donde los números de serie no coincidan con el del editor de CER.
2. Descargue "IPSec.pem" del publicador CER desde la ruta: Administración de Cisco Unified OS > Seguridad > Administración de certificados > Buscar



Certificado CER ipsec.pem

3. Cargue el archivo "IPSec.pem" en el CER Subscribers necesario como certificado de confianza en la ruta: Cisco Unified OS Administration > Security > Certificate Management > Upload the certificate as IPSec-trust.



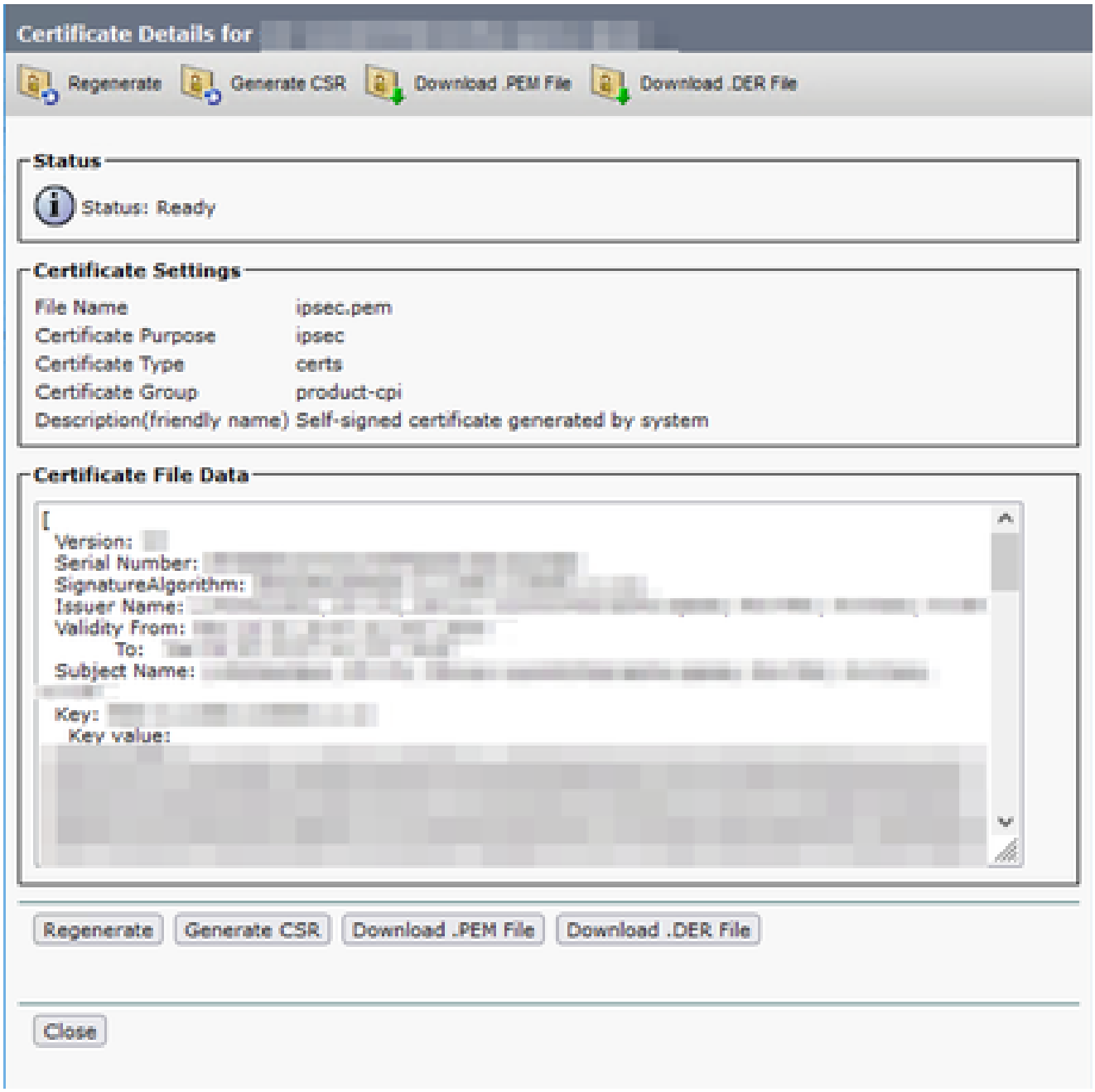
Carga de certificado CER ipsec.trust

4. Reinicie los servicios DRF Local y DRF Master en todos los nodos CER.

Escenario 2

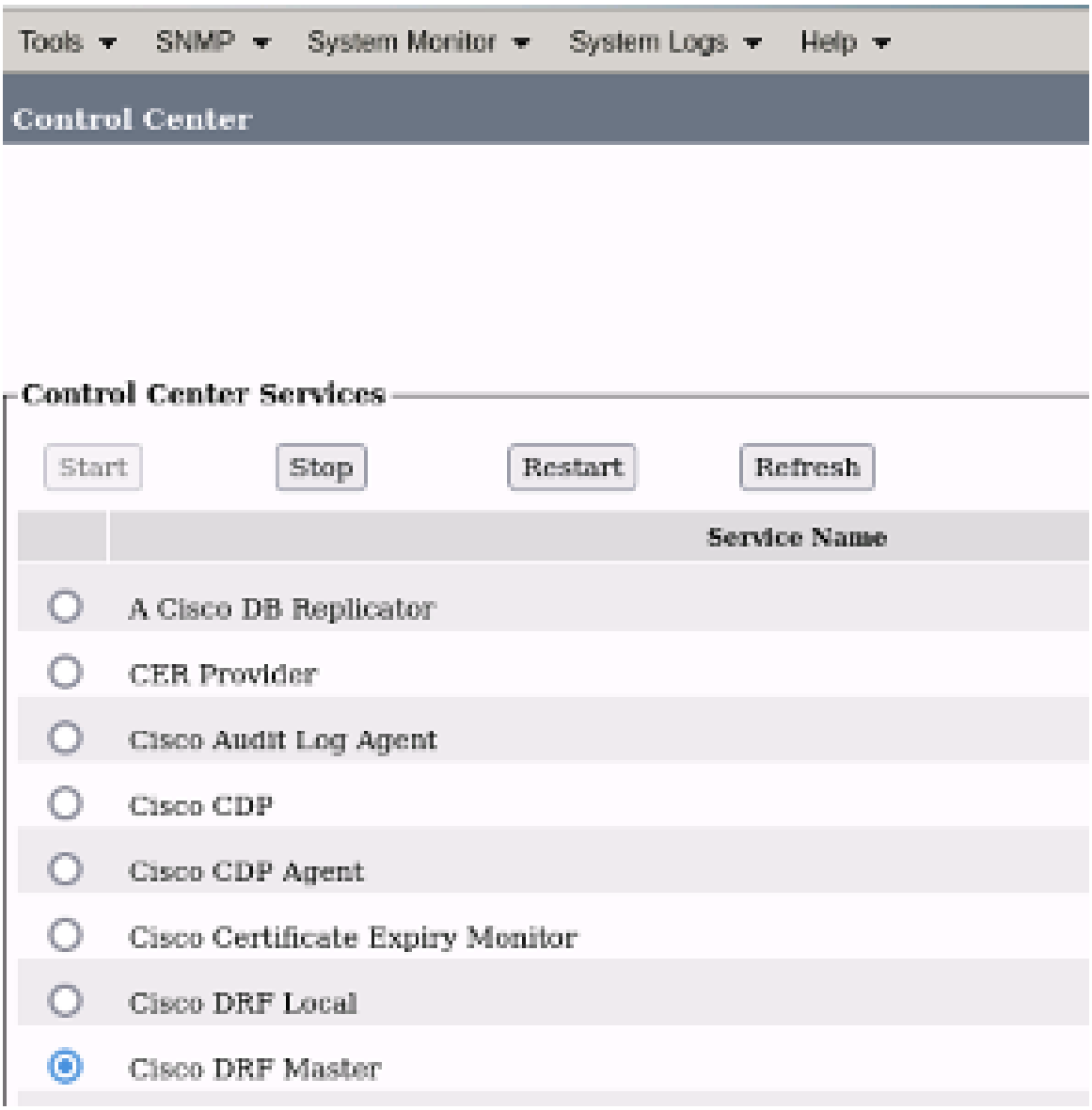
IPSec ha caducado y debe volver a generarse. Siga estos pasos:

1. Vaya a Administración de Cisco Unified OS > Seguridad > Administración de certificados, para cada servidor del clúster. Empezando por el editor, luego cada suscriptor.
2. A partir del publicador CER, haga clic en Find para mostrar todos los certificados del servidor.
3. Haga clic en el certificado "IPSec.pem".
4. Esto hace que aparezca la información del certificado y luego haga clic en Regenerar.



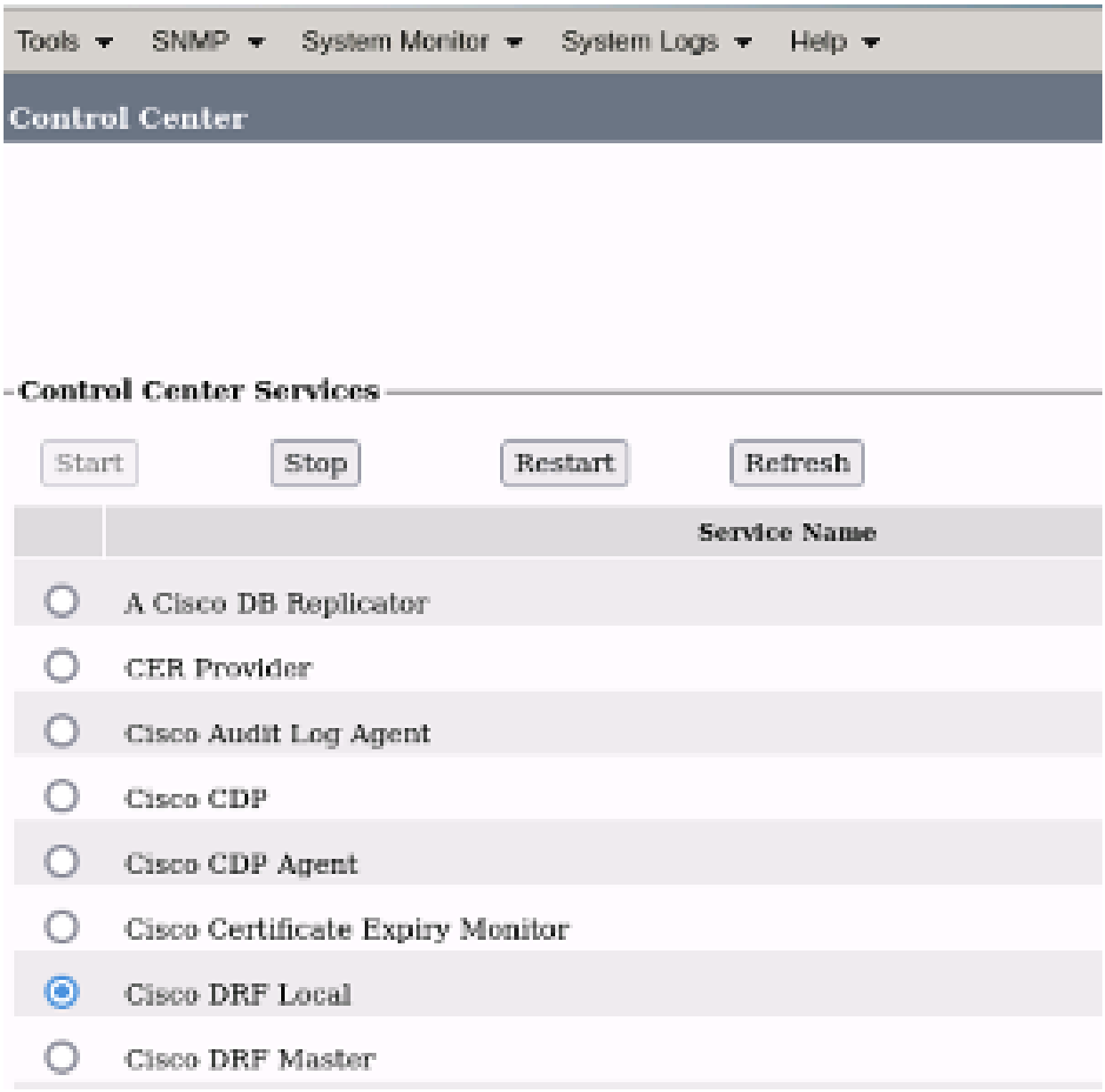
CER ipsec.pem Regenerate

5. Una vez que se regenere el certificado en el Editor CER y se vea el mensaje Success, repita los pasos 1-4 en los nodos del Suscriptor CER.
6. Una vez que el certificado se haya regenerado en todos los nodos, reinicie estos servicios:
    - Cisco DRF Master solo en el publicador CER:
        - Vaya a Serviciabilidad de CER > Herramientas > Servicios del Centro de Control > Maestro de Cisco DRF



CER Cisco DRF Master Restart

- Una vez que el servicio Cisco DRF Master esté activo, reinicie Cisco DRF Local en el editor CER primero.



CER Cisco DRF Local Restart

- Una vez que el servicio Cisco DRF Local esté activo en el nodo del editor CER, reinicie este servicio en todos los nodos del suscriptor CER.

7. Después de reiniciar los servicios en todos los nodos, realice una copia de seguridad manual del sistema:
   - Vaya a Sistema de recuperación ante desastres > Copia de seguridad > Copia de seguridad manual.
   - Seleccione el nombre del dispositivo de copia de seguridad.
   - Seleccione las funciones de la copia de seguridad.
   - Haga clic para iniciar la copia de seguridad.

Información Relacionada

Cómo recopilar registros para CER

Regenere el certificado de CUCM

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).