Fehlerbehebung: Fehler bei CER-Sicherung mit Fehlermeldung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie bei einem Fehler bei der Sicherung des Cisco Emergency Responder (CER) eine Fehlermeldung unter dessen Status angezeigt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, Kenntnisse zu folgenden Themen zu erwerben:

- Cisco Emergency Responder
- Grundlegendes zu Sicherheitszertifikaten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

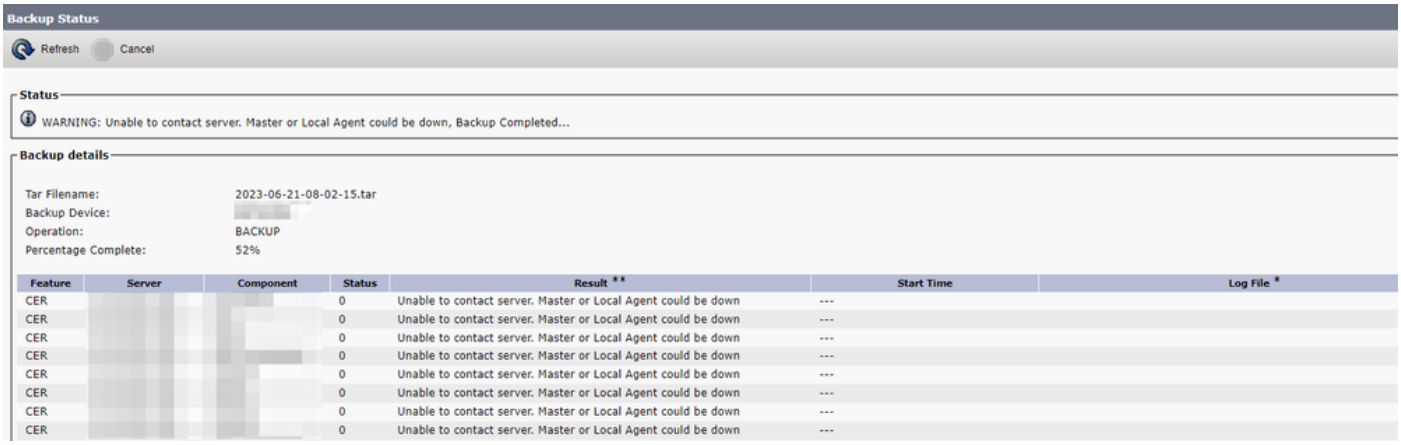
- Cisco Emergency Responder 11.5.4.60000-5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Im Clustermodus bereitgestellter CER kann nicht gesichert werden. Fehlermeldung: "Verbindung zum Server nicht möglich. Der Master- oder lokale Agent kann heruntergefahren sein."

Beispiele:



CER-Sicherungsfehlermeldung

Betroffene Versionen sind 11.x und höher.

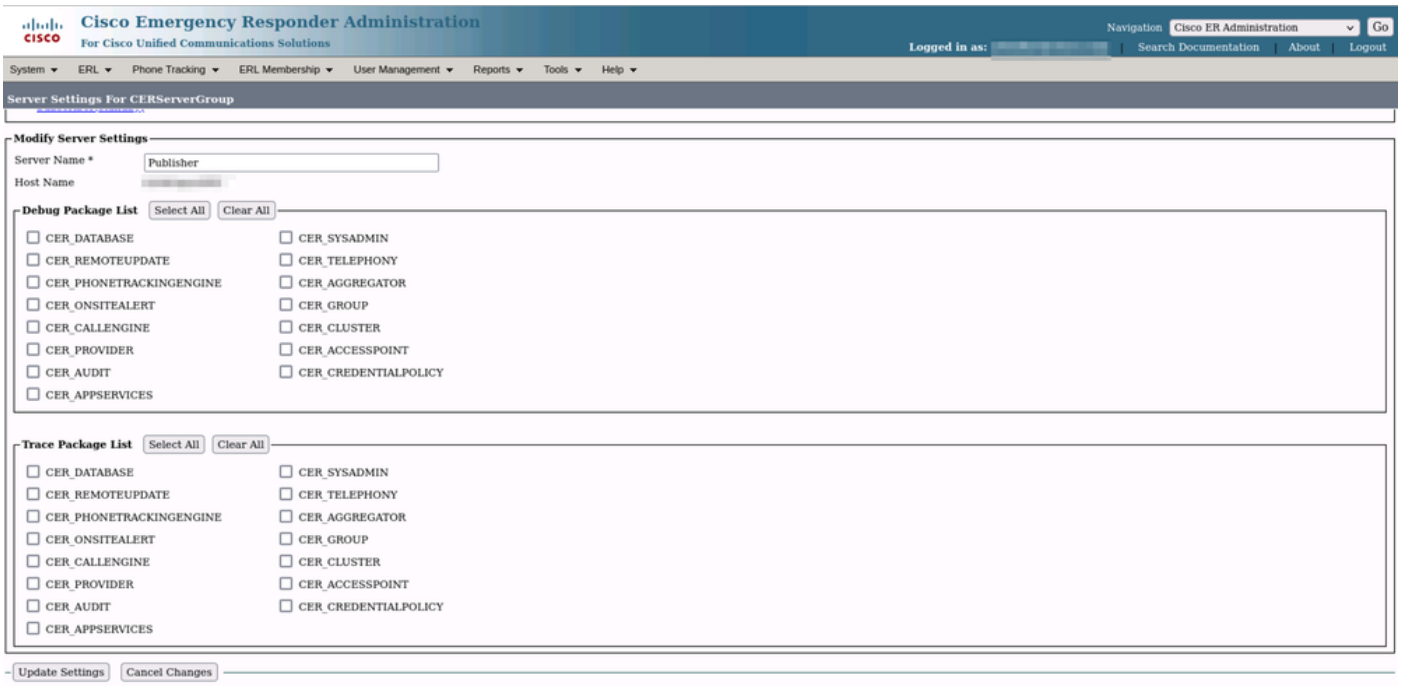
Fehlerbehebung

Protokollsammlung

Sammeln Sie in diesem Fall Protokolle, um möglichst viele Informationen zu sammeln und so die Ursache des Problems und den richtigen Aktionsplan zur Lösung des Problems zu ermitteln.

Aktivieren Sie vor dem Sammeln der Protokolle die detaillierte Ablaufverfolgung, und führen Sie das Debuggen aus, indem Sie die folgenden Schritte ausführen:

1. Melden Sie sich bei der CER Administration-Webseite an.
2. Navigieren Sie zu System > Server Settings. CER Publisher ist standardmäßig ausgewählt und kann geändert werden, wenn auch CER Subscriber-Protokolle benötigt werden.
3. Klicken Sie für die Abschnitte "Debug Package List" und "Trace Package List" auf Select All.
4. Klicken Sie auf Einstellungen aktualisieren.

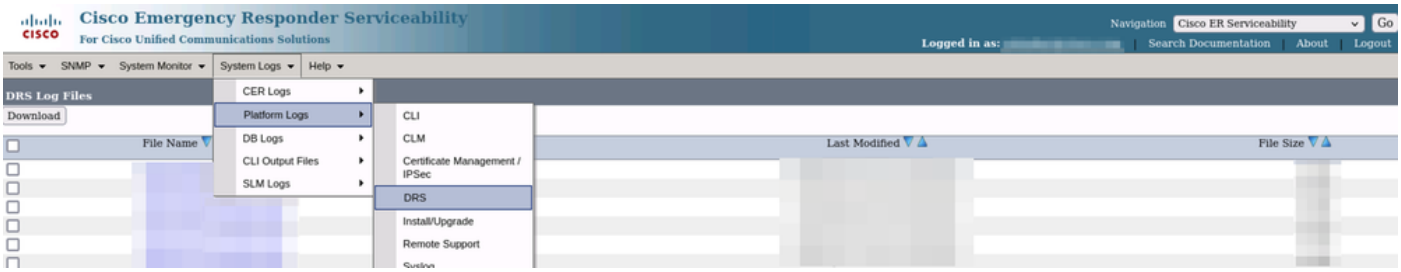


CER Aktivieren von Debuggen und Ablaufverfolgungen

Replizieren Sie das Problem an diesem Punkt.

Nachdem das Problem repliziert wurde, sammeln Sie die DRS-Protokolle für den Replikationsversuch von der Cisco ER Serviceability-Webseite. Gehen Sie wie folgt vor:

1. Wählen Sie in der Navigationsleiste Cisco ER Serviceability aus.
2. Navigieren Sie zu Systemprotokolle > Plattformprotokolle > DRS.



CER sammelt DRS-Protokolle

Protokollanalyse

Bei der Analyse der Protokolle wird angezeigt, wo der Server versucht, die Verbindung mit dem Peer herzustellen, und die Fehlermeldung in den Protokollen weist auf den Grund des Fehlers hin.

Vom CER Publisher aus protokolliert DRF MA:

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: Anzahl der Einträge in IPSec trustStore: 1
2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient:drfQueryTruststore - Query truststore for every 20 hours

21.06.2023 07:58:58,168 FEHLER [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Fehler beim Erstellen des Eingabe-/Ausgabestreams zum Client. Schwerwiegende Warnung erhalten: Fehlerhaftes Zertifikat

21.06.2023 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run: Empfangene Client-Socket-Anforderung von /IP:Port
21.06.2023 08:04:46,274 DEBUG [NetServerWorker] - Validieren, wenn die Client-Anforderung von einem Knoten im Cluster stammt
21.06.2023 08:04:46,278 DEBUG [NetServerWorker] - Validated Client. IP = 10.10.20.25 Hostname = device.test.org. Anforderung stammt von einem Knoten im Cluster.
21.06.2023 08:04:46,278 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Socket Object InputStream to be created
2023-06-21 08:04:46,313 FEHLER [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Fehler beim Erstellen des Eingabe-/Ausgabestreams zum Client. Schwerwiegende Warnung erhalten: Fehlerhaftes Zertifikat

Von CER Publisher DRF Lokale Protokolle:

2023-06-21 07:58:47,453 DEBUG [main] - drfNetServerClient:Reconnect, Konnte keine Verbindung zum Host herstellen: [X], Meldung: Verbindung verweigert (Verbindung verweigert), Ursache: null

Bis jetzt sehen wir, dass die Verbindung aufgrund eines schlechten Zertifikats abgelehnt wird.

Das Zertifikat, mit dem die vertrauenswürdige Verbindung zwischen den Knoten für Backups/Wiederherstellungen hergestellt wird, ist IPSec. An diesem Punkt können wir bereits feststellen, dass das Problem damit zusammenhängt, dass das IPSec-Zertifikat abgelaufen ist oder ein falsches Zertifikat auf einem der Server vorhanden ist.

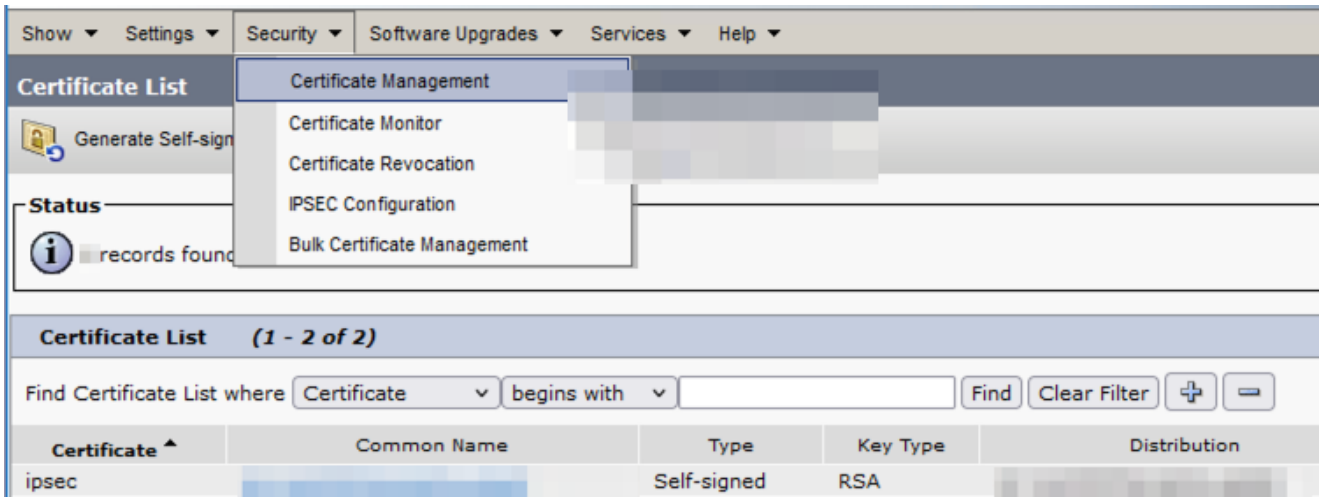
Korrekturmaßnahme

1. Überprüfen Sie die Seriennummer (SN) der IPSec-Vertrauenszertifikate in allen CER Subscriber-Knoten. Diese muss mit der SN der IPSec.prem vom CER Publisher übereinstimmen (Szenario 1).
2. Bestätigen Sie die Gültigkeit des Zertifikats "IPSec.pem" im Knoten "CER Publisher". Das Datum muss gültig sein, oder das IPSec-Zertifikat muss neu generiert werden (Szenario 2).

Szenario 1

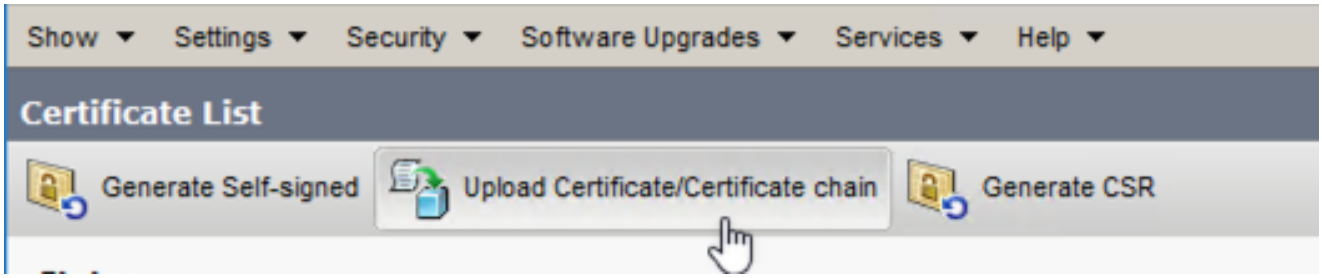
Die IPSec-Zertifikat-SN stimmt nicht mit den veröffentlichten CER- und CER-Abonnenten überein. Gehen Sie wie folgt vor:

1. Löschen Sie das IPSec-trust-Zertifikat in den CER-Abonnenten, wenn die Seriennummern nicht mit denen des CER-Verlegers übereinstimmen.
2. Laden Sie die Datei "IPSec.pem" vom CER Publisher herunter: Cisco Unified OS Administration > Security > Certificate Management > Find



CER ipsec.pem-Zertifikat

3. Laden Sie die Datei "IPSec.pem" in die CER-Abonnenten hoch, die als Vertrauenszertifikat im Pfad benötigt werden: Cisco Unified OS Administration > Security > Certificate Management > Laden Sie das Zertifikat als IPSec-trust hoch.



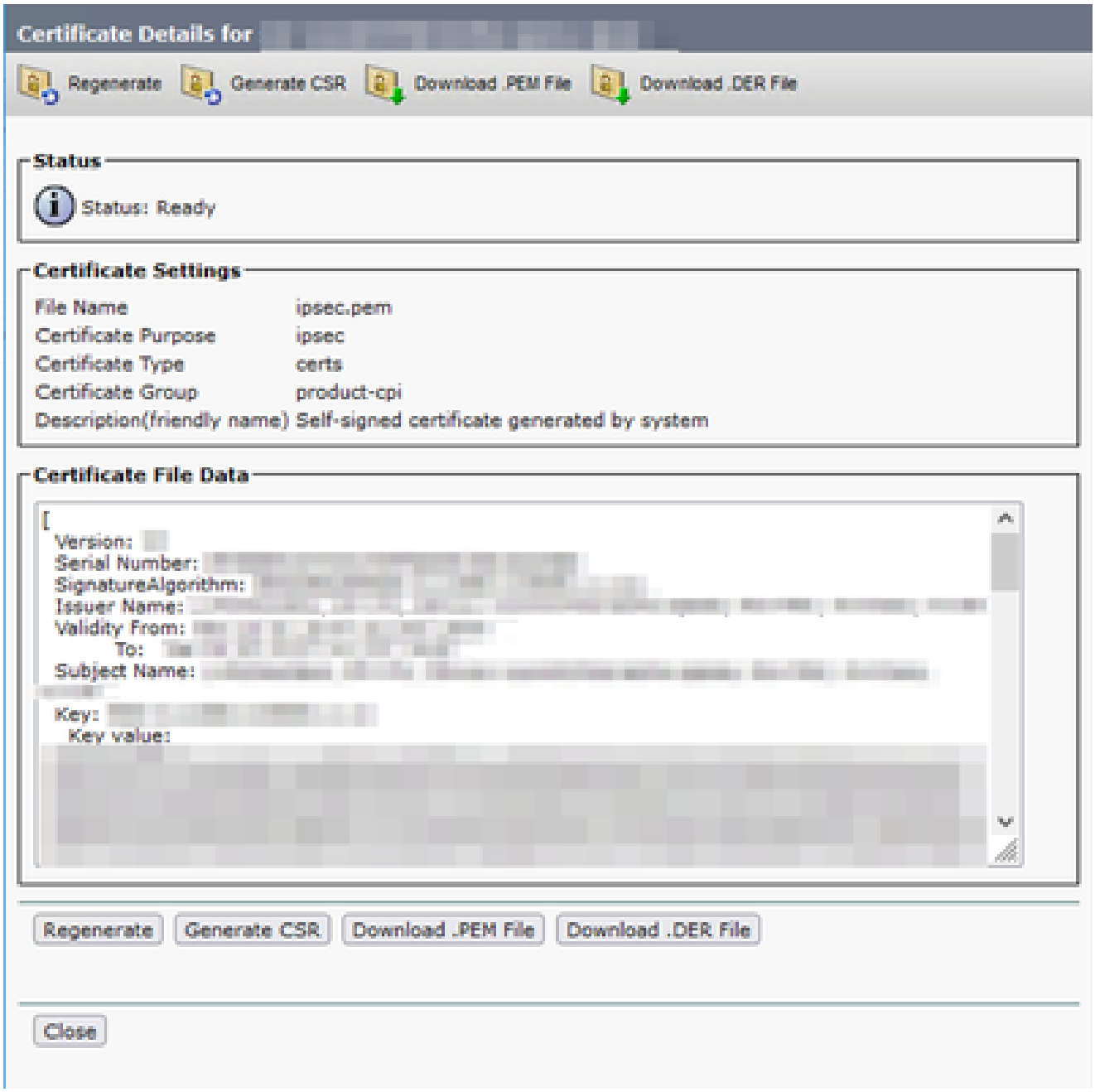
CER IPSec.trust-Zertifikat-Upload

4. Starten Sie die DRF Local- und DRF Master-Dienste in allen CER-Knoten neu.

Szenario 2

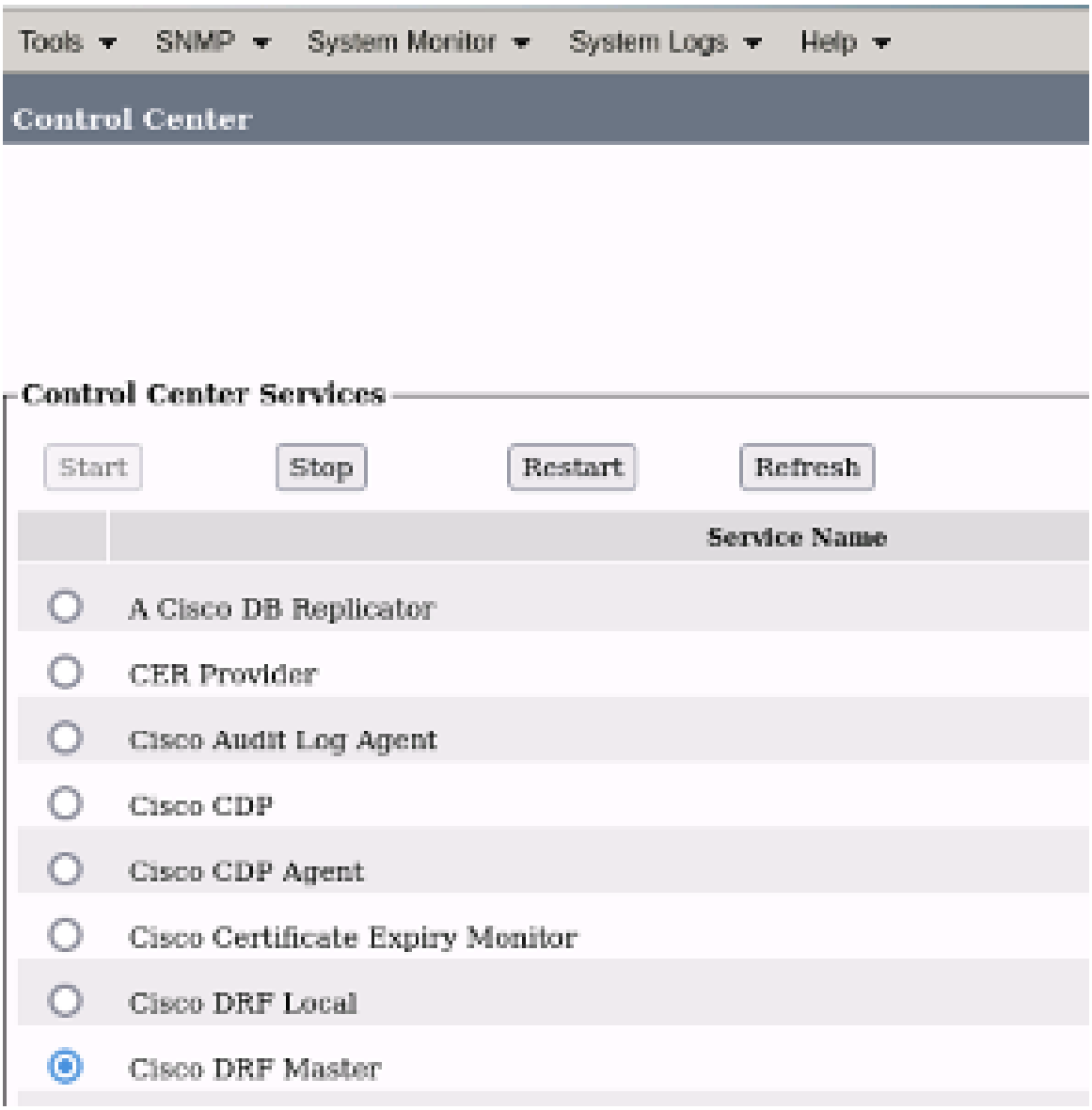
IPSec ist abgelaufen und muss neu generiert werden. Gehen Sie wie folgt vor:

1. Navigieren Sie für jeden Server im Cluster zu Cisco Unified OS Administration > Security > Certificate Management. Beginnend mit dem Herausgeber, dann jedem Abonnenten.
2. Beginnend mit dem CER Publisher klicken Sie auf Suchen, um alle Zertifikate auf dem Server anzuzeigen.
3. Klicken Sie auf das Zertifikat "IPSec.pem".
4. Dadurch werden die Zertifikatinformationen angezeigt, und klicken Sie dann auf Regenerieren.



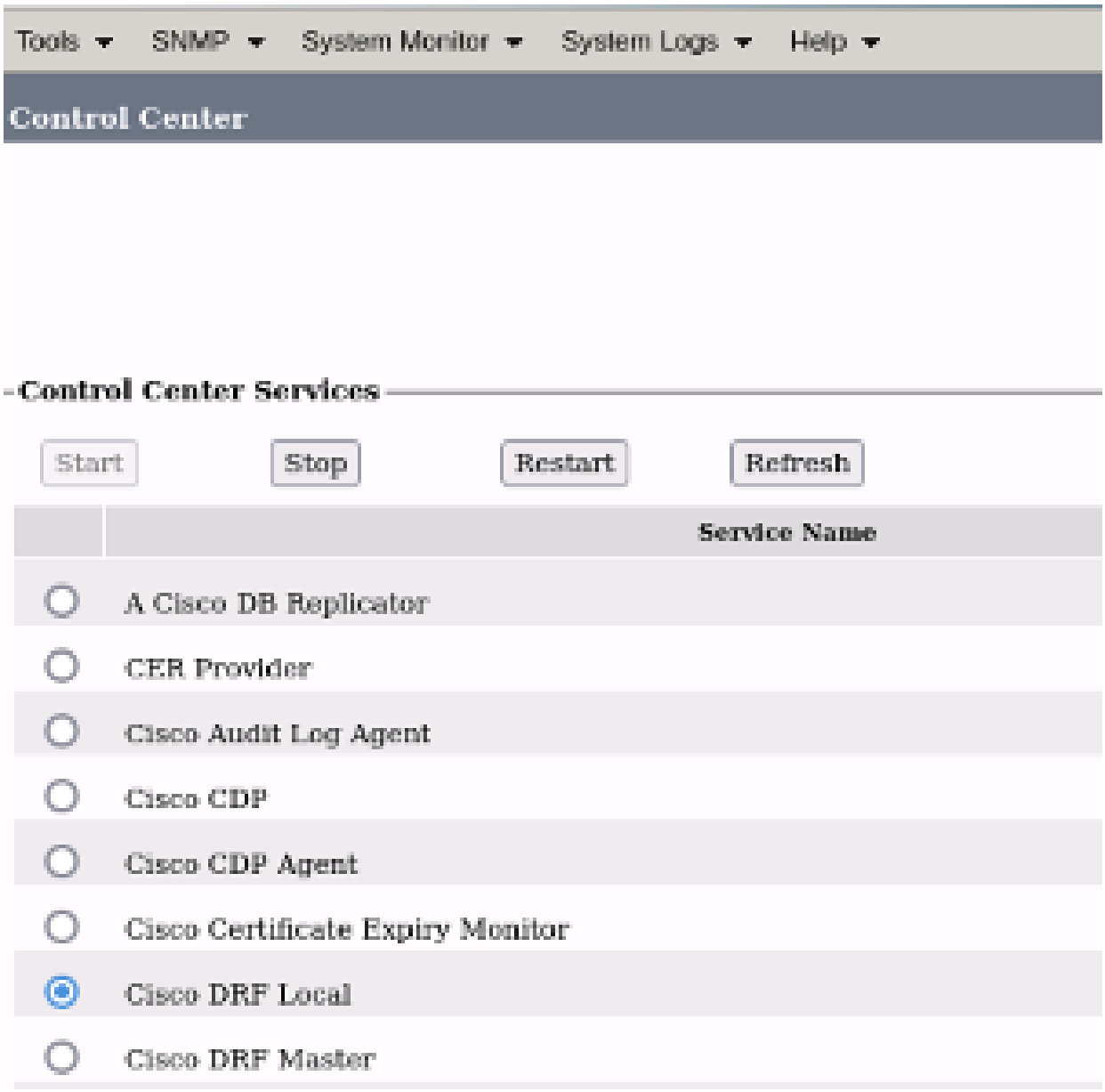
CER ipsec.pem Regenerieren

5. Wenn das Zertifikat im CER Publisher neu generiert wurde und die Erfolgsmeldung angezeigt wird, wiederholen Sie die Schritte 1-4 in den CER Subscriber-Knoten.
6. Sobald das Zertifikat auf allen Knoten neu generiert wurde, starten Sie die folgenden Dienste neu:
    - Cisco DRF Master nur im CER Publisher:
        - Navigieren Sie zu CER Serviceability > Tools > Control Center Services > Cisco DRF Master



CER Cisco DRF Master-Neustart

- Sobald der Cisco DRF Master-Service aktiviert ist, starten Sie Cisco DRF Local im CER Publisher neu.



CER Cisco DRF Lokaler Neustart

- Sobald der lokale Cisco DRF-Dienst im CER Publisher-Knoten aktiv ist, starten Sie diesen Dienst in allen CER Subscriber-Knoten neu.

7. Nachdem die Dienste auf allen Knoten neu gestartet wurden, führen Sie eine manuelle Sicherung des Systems durch:
   - Navigieren Sie zu Disaster Recovery System > Backup > Manual Backup.
   - Wählen Sie den Namen des Sicherungsgeräts aus.
   - Wählen Sie die Funktionen für die Sicherung aus.
   - Klicken Sie auf Sicherung starten.

Zugehörige Informationen

Sammeln von Protokollen für CER

CUCM-Zertifikat neu generieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.