VERLOOP VAN HET CER-certificaat EN UITSCHAKELING

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Een nieuw certificaat genereren](#)
[Verlopen certificaten verwijderen](#)

Inleiding

In dit document wordt een probleem beschreven met de Cisco Noodrespons (CER) waarbij u de **noodtoestand** ontvangt**: EINDTIJD_ALARM** alarmbericht van het CLI-certificaat bij **EX** en biedt een oplossing voor het probleem.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van CER versies 2.x tot en met 9.x.

Bovendien vereist deze configuratie dat uw systeem:

- Bevat geen DNS-configuratie (Domain Name Server)
- Heeft een CER-server geïnstalleerd en certificaten die binnenkort verlopen

  Opmerking: Het IP-adres van het systeem doet er niet toe of u de opdrachten **Generate New** of Regenerate invoert nadat u de hostnaam of IP-adres hebt gewijzigd.

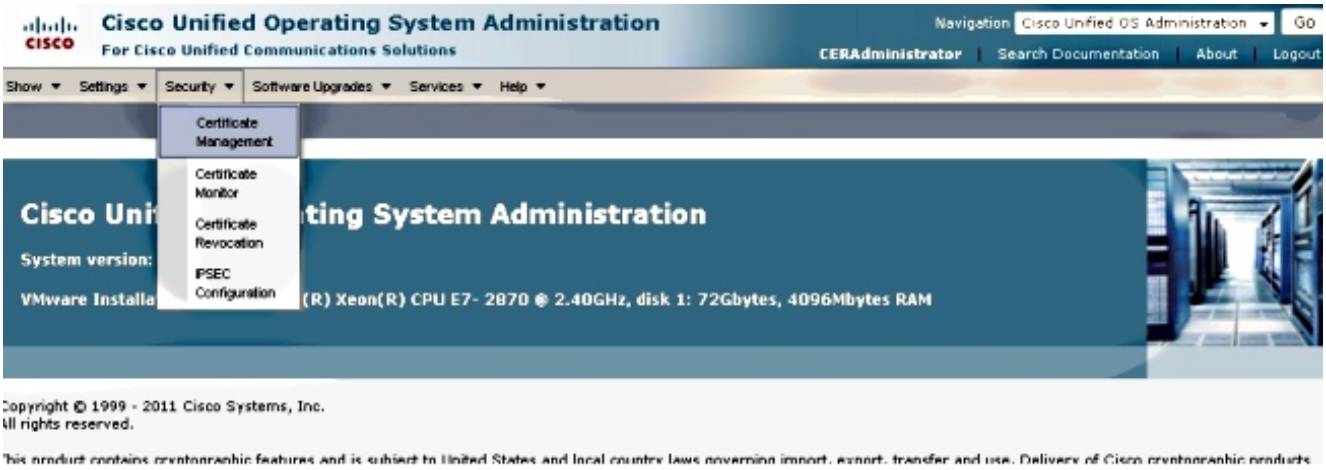
Gebruikte componenten

De informatie in dit document is gebaseerd op CER versie 9.x.

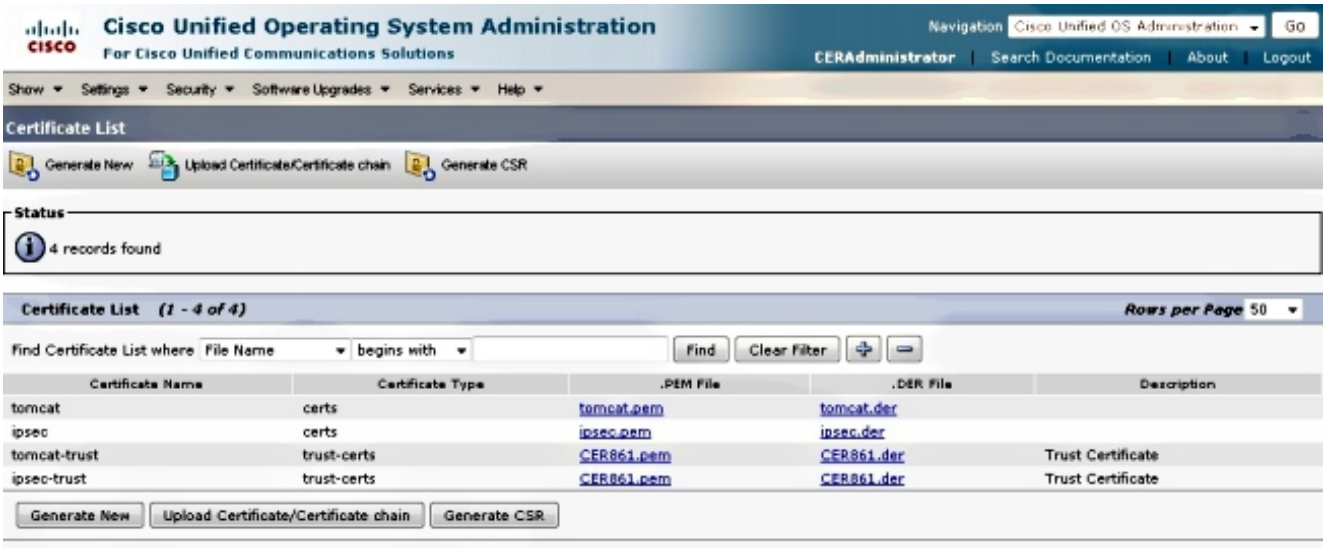
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Een nieuw certificaat genereren

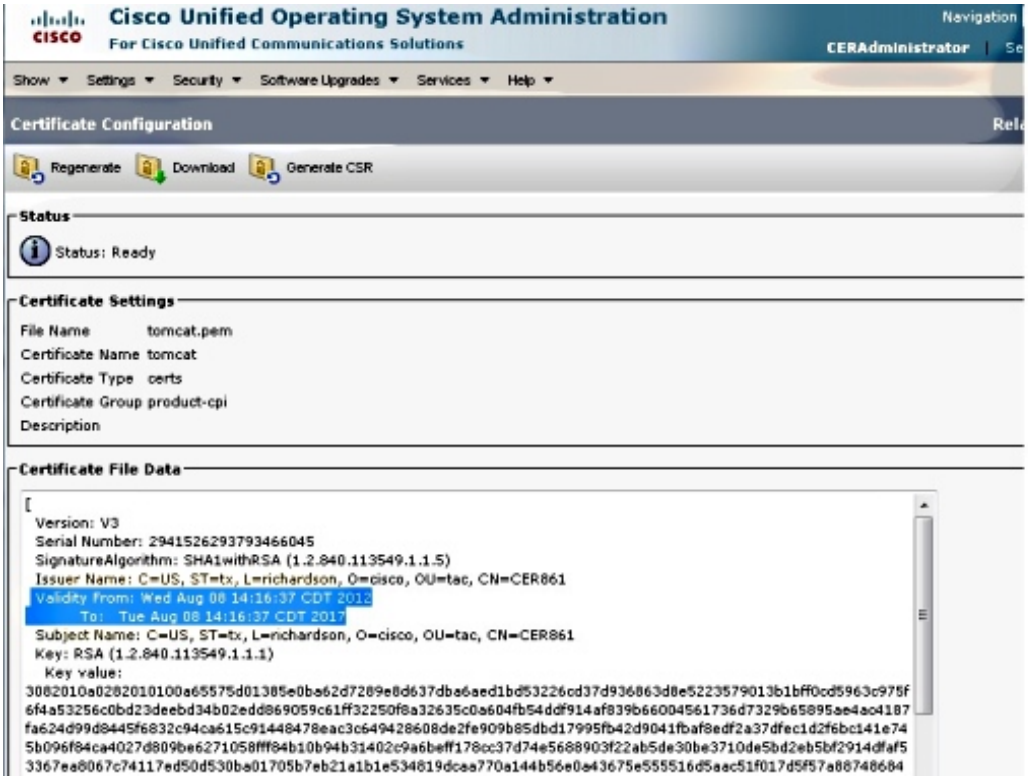
1. Ga naar de GUI in het besturingssysteem en selecteer de pagina **Beveiliging > certificaatbeheer**.



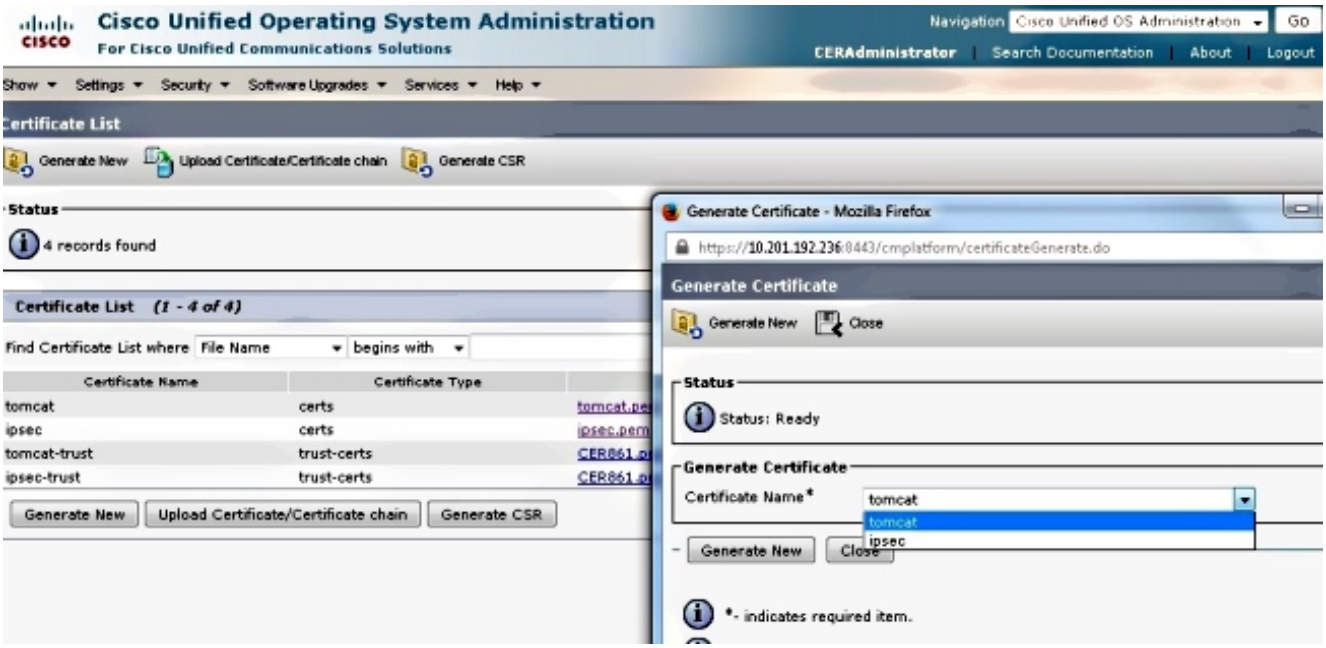
2. Klik op de knop **Zoeken** om de lijst met certificaten weer te geven.



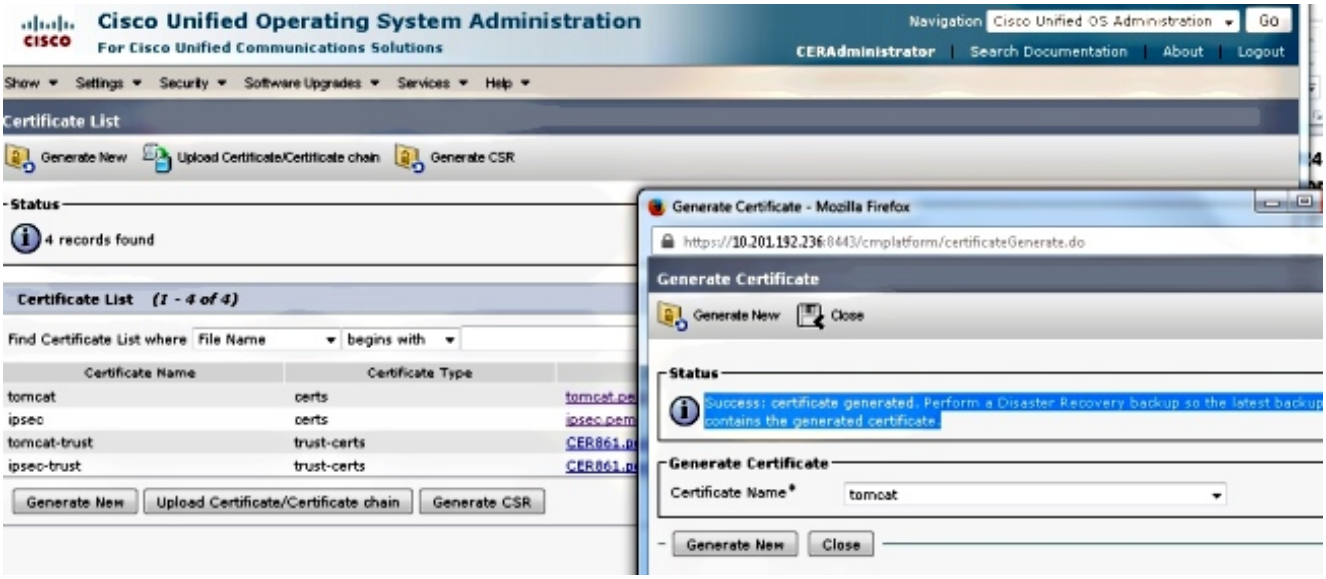
Deze schermopname toont het **tomcat.pem** certificaat en de **Geldigheidsdatum** wordt gemarkeerd. Als het certificaat binnenkort zal verlopen, voert u de volgende stappen uit.



3. Navigeer naar de vorige pagina en klik op het pictogram **Generate New**. Dit scherm verschijnt:



4. Klik om het certificaat te regenereren op **Generate New** in het pop-upvenster. Er verschijnt een succesbericht om aan te geven dat het certificaat wordt geregenereerd.



5. U moet de eg-service (Internet Protocol Security) (als u IPSec-certificaten hebt gegenereerd) opnieuw opstarten. Om Tomcat opnieuw te starten, opent u een CLI voor het knooppunt en voert u de **utils service opnieuw uit, de** opdracht **Cisco Tomcat**. Nadat de pagina weer online is, kunt u het nieuwe certificaat downloaden op de website.

Verlopen certificaten verwijderen

Belangrijke opmerkingen over het wissen van certificaten:

- Zorg ervoor dat certificaten die zijn ingesteld voor het wissen niet langer in gebruik zijn of daadwerkelijk zijn verlopen.
- Controleer altijd alle informatie in het certificaat, omdat het niet meer kan worden opgeslagen nadat het is verwijderd.

Controleer alle certificaten met de **.pem-**extensie en controleer of ze binnen een geldig tijdsbereik zijn. Als dit niet het geval is, kunnen ze worden verwijderd.

Als er meerdere servers in de cluster staan, moet u naar het IP-adres van elk van de servers gaan. Vervolgens kunt u binnen de pagina OS Admin de stappen voltooien die in de sectie Configure worden opgesomd.