

Probleemoplossing voor CER-back-up mislukt met foutbericht

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleemoplossing](#)

[Logbestanden verzamelen](#)

[Analyse van logboeken](#)

[Corrigerende maatregel](#)

[Scenario 1](#)

[Scenario 2](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met de Cisco Emergency Responder (CER) door geen back-up te maken van en een foutbericht weer te geven onder de status ervan.

Voorwaarden

Vereisten

Cisco raadt aan kennis te hebben over deze onderwerpen:

- Cisco Noodrespons
- Basiskennis van beveiligingscertificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

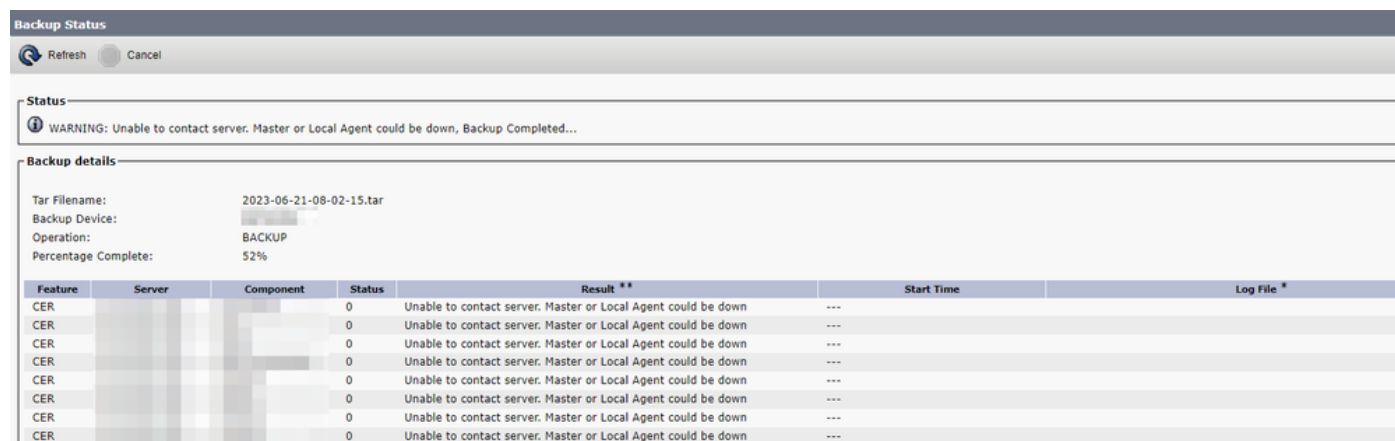
- Cisco Emergency Responder 11.5.4.60000-5

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

CER die in clustermodus wordt geïmplementeerd, kan geen back-up maken met de foutmelding "Kan geen contact opnemen met server. Hoofd of lokale agent kan zijn down".

Voorbeeld:



The screenshot shows a 'Backup Status' window with a 'Refresh' button and a 'Cancel' button. Below the buttons, there is a 'Status' section with a warning icon and the text: 'WARNING: Unable to contact server. Master or Local Agent could be down, Backup Completed...'. Below this is a 'Backup details' section with the following information:

Tar Filename: 2023-06-21-08-02-15.tar
Backup Device: [redacted]
Operation: BACKUP
Percentage Complete: 52%

Feature	Server	Component	Status	Result **	Start Time	Log File *
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	
CER			0	Unable to contact server. Master or Local Agent could be down	---	

Foutbericht voor CER Backup

Betrokken versies zijn 11.x en hoger.

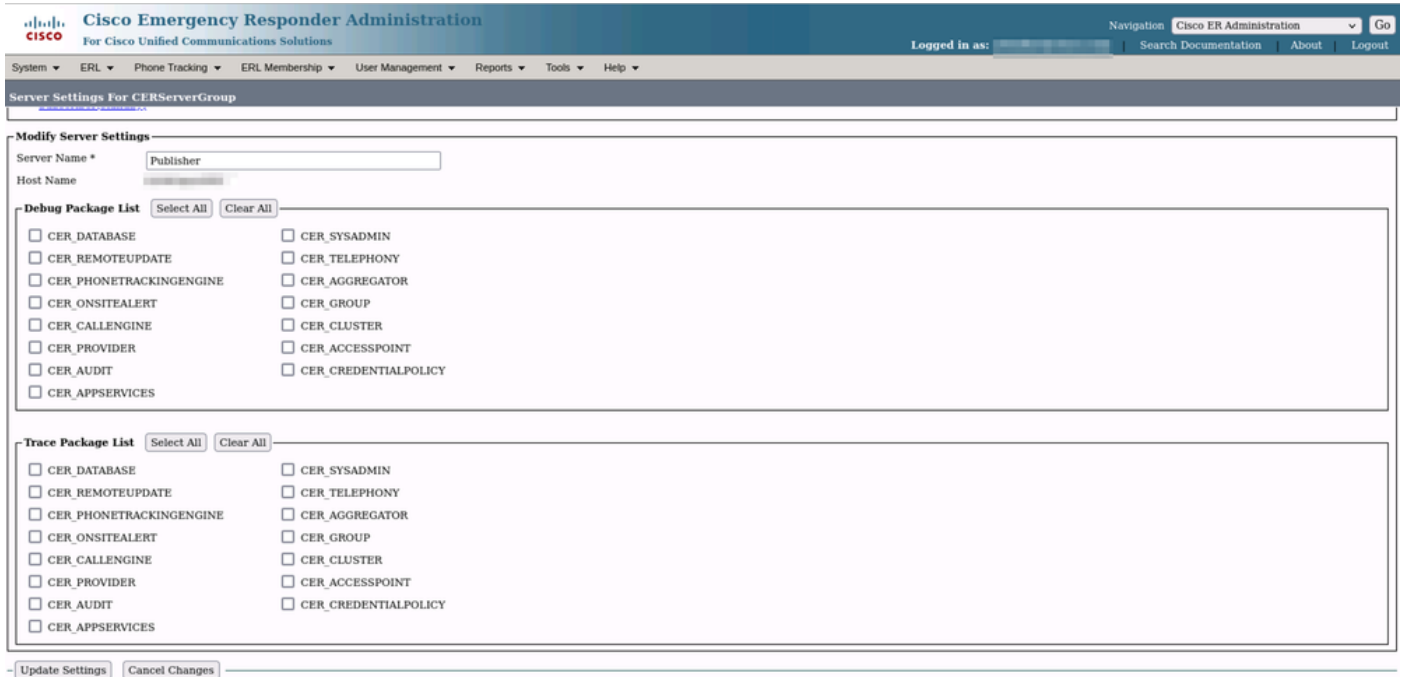
Probleemoplossing

Logbestanden verzamelen

Wanneer dit gebeurt, verzamel logbestanden om zo veel mogelijk informatie te verzamelen om te proberen de bron van het probleem te bepalen en het juiste actieplan te bepalen om het probleem op te lossen.

Alvorens de logbestanden te verzamelen, activeert u gedetailleerde overtrekken en debuggen door deze stappen te voltooien:

1. Log in op de webpagina van CER-beheer.
2. Ga naar Systeem > Serverinstellingen. CER Publisher wordt standaard geselecteerd en kan worden gewijzigd als er ook CER Subscriber-logbestanden nodig zijn.
3. Klik op Alles selecteren voor de secties "Debug Package List" en "Trace Package List".
4. Klik op Instellingen bijwerken.



CER: debugs en tracersingen inschakelen

Herhaal het probleem nu alstublieft.

Nadat het probleem is gerepliceerd, verzamelt u de DRS-logbestanden die van toepassing zijn op de replicatiepoging van de Cisco ER Serviceability Web-pagina waarin deze stappen worden voltooid:

1. Selecteer vanuit Navigatie Cisco ER Service.
2. Navigeren naar systeemlogbestanden > Platformlogbestanden > DRS.



DRS-logbestanden verzamelen met CER

Analyse van logboeken

Bij het analyseren van de logbestanden beginnen we te zien waar de server probeert de verbinding met zijn peer tot stand te brengen en we zien de foutmelding in de logbestanden die ons wijzen op de reden van de fout.

Van de weblogs van CER Publisher DRF MA:

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: Aantal items in IPSec trustStore: 1

2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore - Query

truststore voor elke 20 uur

2023-06-21 07:58:58,168 FOUT [NetServerWorker] - drfNetServerWorker.drfNetServerWorker:
Kan geen invoer/uitvoerstream naar client maken Fatal Alert ontvangen: Slecht certificaat

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run: Ontvangen client Socket
aanvraag van /IP:poort

2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - Verifiëren als clientverzoek afkomstig is
van een knooppunt in de cluster

2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - gevalideerde client. IP = 10.10.20.25
Hostname = device.test.org. Aanvraag wordt gedaan via een knooppunt binnen de cluster

2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker:
Socket Object InputStream worden gemaakt

2023-06-21 08:04:46,313 FOUT [NetServerWorker] - drfNetServerWorker.drfNetServerWorker:
Kan geen invoer/uitvoerstream naar client maken Fatal Alert ontvangen: Slecht certificaat

Uit de lokale logs van CER Publisher DRF:

2023-06-21 07:58:47,453 DEBUG [hoofd] - drfNetServerClient:Reconconnect, kan geen
verbinding maken met host: [X], bericht: Verbinding geweigerd (verbinding geweigerd), oorzaak:
ongeldig

Tot nu toe zien we dat de verbinding wordt geweigerd vanwege een slecht certificaat.

Het certificaat dat wordt gebruikt om de vertrouwde verbinding tussen de knooppunten voor back-
ups/herstel tot stand te brengen, is de IPSec. Op dat punt kunnen we al bepalen dat het probleem
gerelateerd is aan het verlopen IPSec-certificaat of aan de aanwezigheid van een onjuist
certificaat in een van de servers.

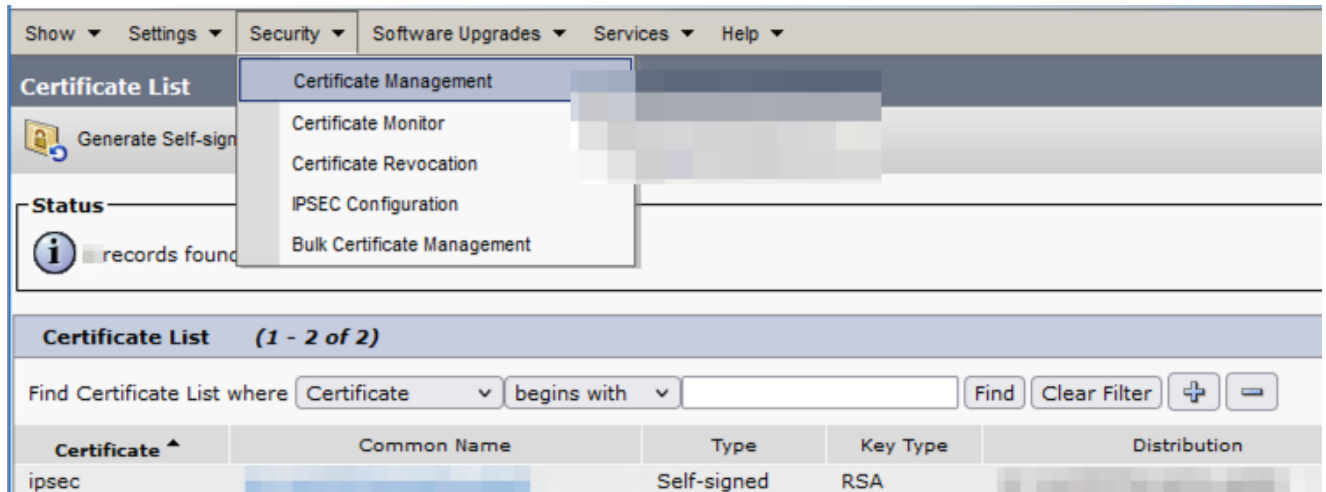
Corrigerende maatregel

1. Controleer het serienummer (SN) van de IPSec-trust certificaten in alle CER Subscriber knooppunten, dit moet overeenkomen met het SN van de IPSec.prem van de CER Publisher (scenario 1).
2. Bevestig de geldigheid van het IPSec.pem-certificaat in het knooppunt CER Publisher. De datum moet geldig zijn of het IPSec-certificaat moet opnieuw worden gegenereerd (scenario 2).

Scenario 1

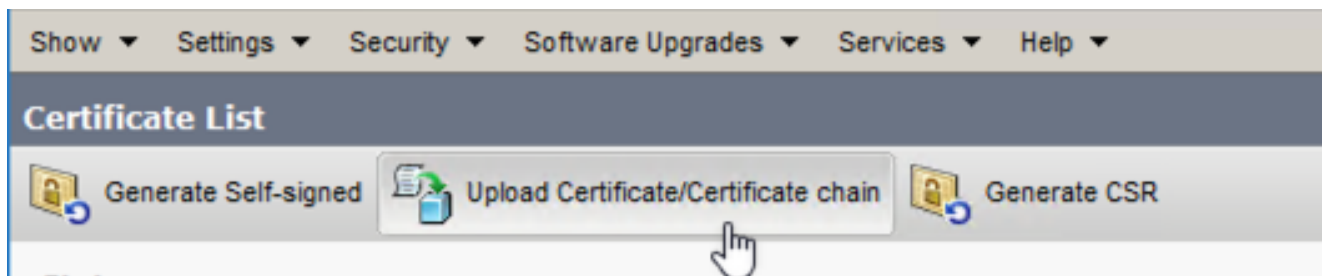
Het IPSec-certificaat SN komt niet overeen tussen de gepubliceerde CER en de CER-abonnees.
Ga verder met deze stappen:

1. Verwijdert het IPSec-trust certificaat in de CER-abonnee(s) waar de serienummers niet overeenkomen met die in de CER-uitgever.
2. Download "IPSec.pem" van de CER Publisher vanuit het pad: Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoeken



CER ipsec.pem-certificaat

3. Upload het bestand "IPSec.pem" in de CER-abonnees die nodig zijn als vertrouwenscertificaat op het pad: Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Upload het certificaat als IPSec-vertrouwen.



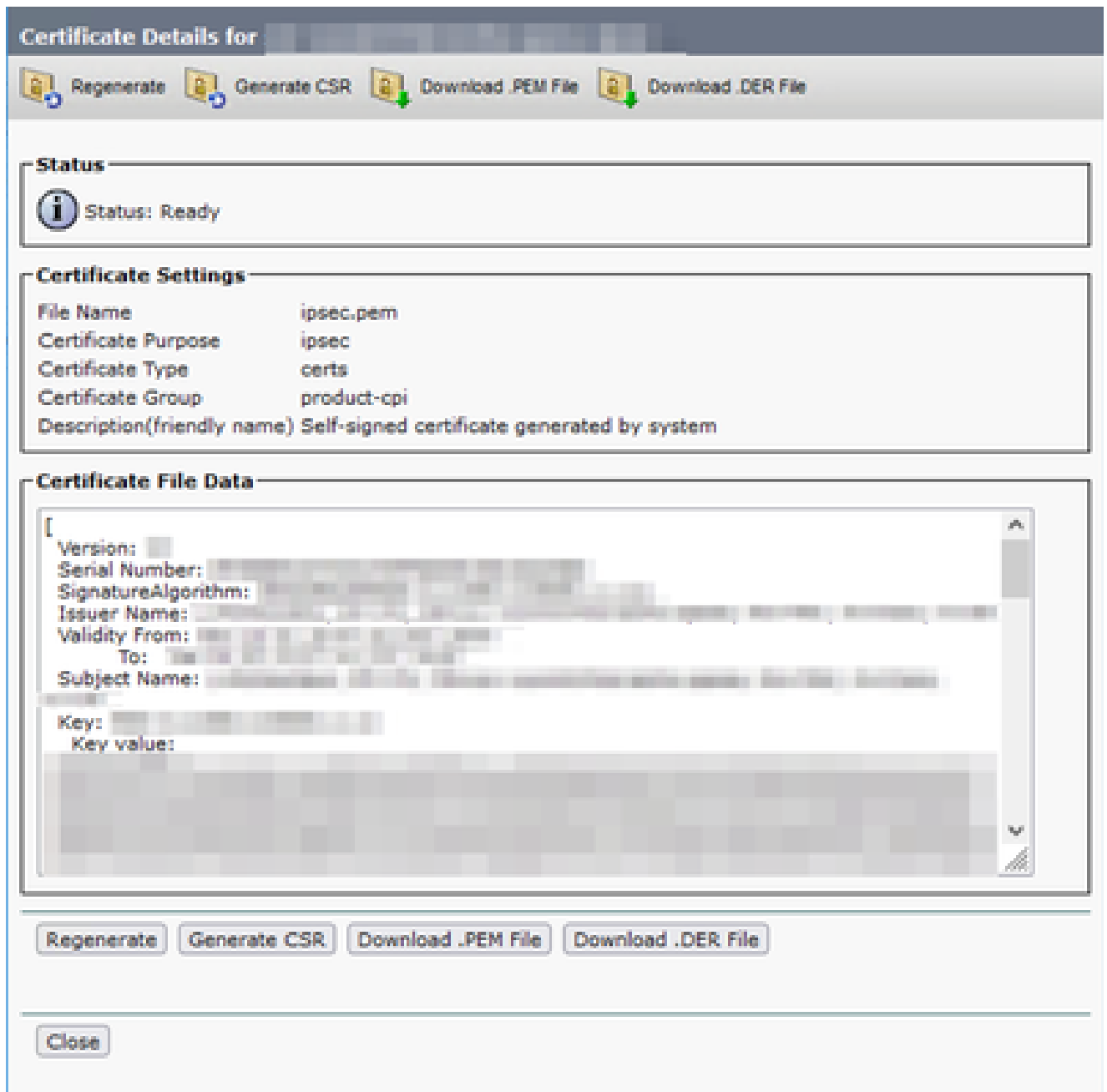
CER ipsec.trust certificaat uploaden

4. Start de DRF Local en DRF Master services in alle CER knooppunten.

Scenario 2

IPsec is verlopen en moet opnieuw worden gegenereerd. Ga verder met deze stappen:

1. Navigeer naar Cisco Unified OS-beheer > Beveiliging > certificaatbeheer voor elke server in het cluster. Beginnend met de uitgever, dan elke abonnee.
2. Klik vanaf de CER Publisher op Find om alle certificaten in de server weer te geven.
3. Klik op het certificaat "IPSec.pem".
4. Dit brengt de informatie van het Certificaat omhoog en klikt dan op Regenerate.



CER ipsec.pem regenereren

5. Zodra het certificaat in de CER Publisher wordt geregenereerd en het Success-bericht wordt gezien, herhaalt u stap 1-4 in de CER Subscriber-knooppunten.
6. Nadat het certificaat in alle knooppunten is geregenereerd, kunt u deze services opnieuw opstarten:
 - Cisco DRF-master alleen in de CER-uitgever:
 - Navigeren naar CER Service > Tools > Control Center Services > Cisco DRF Master

Tools ▾ SNMP ▾ System Monitor ▾ System Logs ▾ Help ▾

Control Center

Control Center Services

	Service Name
<input type="radio"/>	A Cisco DB Replicator
<input type="radio"/>	CER Provider
<input type="radio"/>	Cisco Audit Log Agent
<input type="radio"/>	Cisco CDP
<input type="radio"/>	Cisco CDP Agent
<input type="radio"/>	Cisco Certificate Expiry Monitor
<input type="radio"/>	Cisco DRF Local
<input checked="" type="radio"/>	Cisco DRF Master

CER Cisco DRF - herstart voor master

- Nadat de Cisco DRF Master service is geactiveerd, moet u Cisco DRF Local eerst opnieuw opstarten in de CER Publisher.

Tools ▾ SNMP ▾ System Monitor ▾ System Logs ▾ Help ▾

Control Center

-Control Center Services

Start Stop Restart Refresh

	Service Name
<input type="radio"/>	A Cisco DB Replicator
<input type="radio"/>	CER Provider
<input type="radio"/>	Cisco Audit Log Agent
<input type="radio"/>	Cisco CDP
<input type="radio"/>	Cisco CDP Agent
<input type="radio"/>	Cisco Certificate Expiry Monitor
<input checked="" type="radio"/>	Cisco DRF Local
<input type="radio"/>	Cisco DRF Master

Lokale herstart van CER Cisco DRF

- Zodra de lokale service van Cisco DRF in de CER Publisher-knooppunt actief is, moet u deze service in alle CER Subscriber-knooppunten opnieuw opstarten.
7. Nadat de services op alle knooppunten opnieuw zijn gestart, voert u een handmatige back-up van het systeem uit:
- Ga naar Noodherstelsysteem > Back-up > Handmatige back-up.
 - Selecteer de naam van het back-upapparaat.
 - Selecteer de functies voor de back-up.
 - Klik om de back-up te starten.

Gerelateerde informatie

[Hoe logbestanden te verzamelen voor CER](#)

[CUCM-certificaat regenereren](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.