Risoluzione dei problemi di backup CER con messaggio di errore non riuscito

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al mancato backup di Cisco Emergency Responder (CER) e alla visualizzazione di un messaggio di errore con il relativo stato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Emergency Responder
- Informazioni di base sui certificati di protezione

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

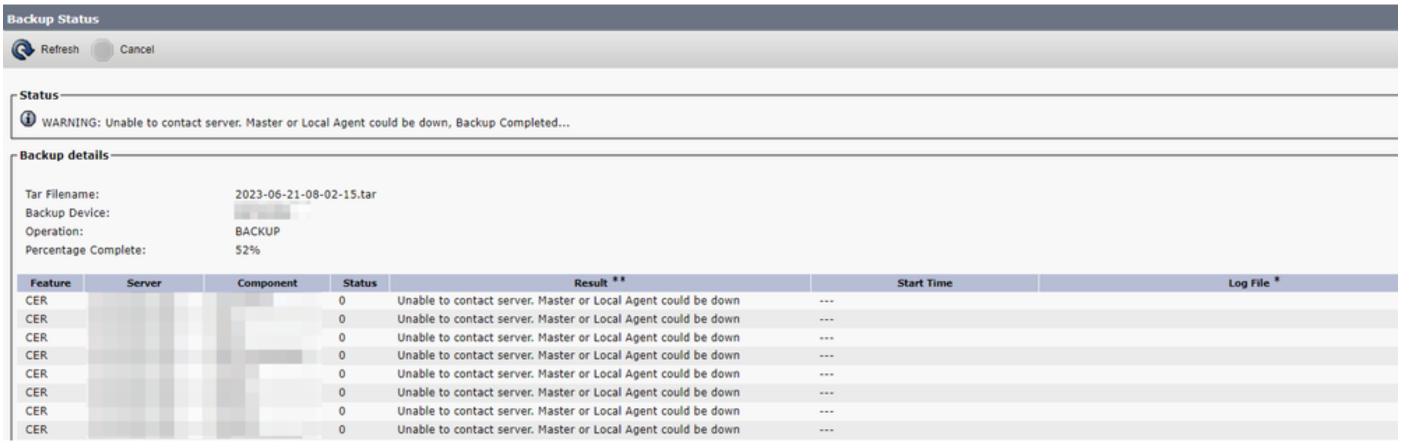
- Cisco Emergency Responder 11.5.4.6000-5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La tecnologia CER distribuita in modalità cluster potrebbe non riuscire a eseguire il backup con il messaggio di errore "Unable to contact server" (Impossibile contattare il server). Il master o l'agente locale potrebbero essere inattivi".

Ad esempio:



Backup Status

Status

WARNING: Unable to contact server. Master or Local Agent could be down, Backup Completed...

Backup details

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	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	
CER	[redacted]	[redacted]	0	Unable to contact server. Master or Local Agent could be down	---	

Messaggio di errore di backup CER

Le versioni interessate sono 11.x e successive.

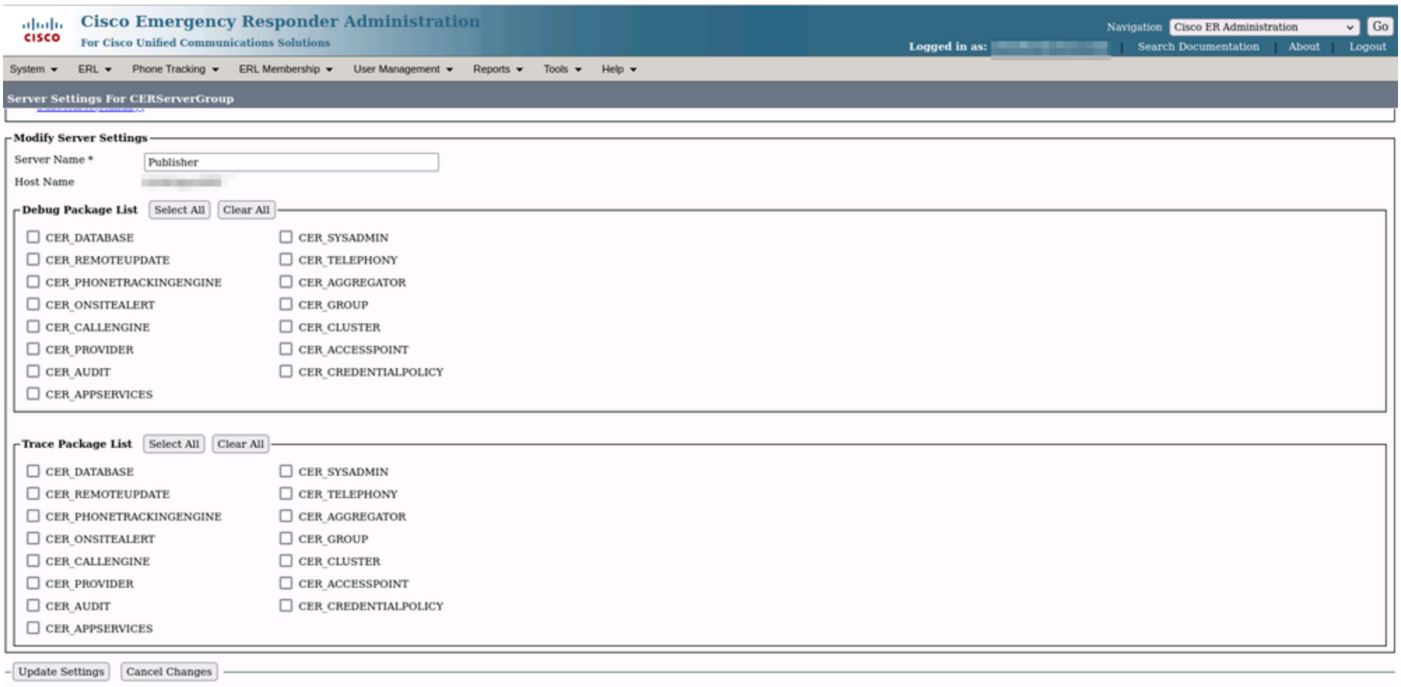
Risoluzione dei problemi

Raccolta log

Quando ciò si verifica, raccogliere i log per tentare di raccogliere quante più informazioni possibili per cercare di determinare l'origine del problema e determinare il piano di azione corretto per risolvere il problema.

Prima di raccogliere i log, attivare la traccia dettagliata e il debug completando i seguenti passaggi:

1. Accedere alla pagina Web Amministrazione CER.
2. Selezionare Sistema > Impostazioni server. Il server di pubblicazione CER è selezionato per impostazione predefinita e può essere modificato se sono necessari anche i registri del sottoscrittore CER.
3. Fare clic su Select All nelle sezioni "Debug Package List" e "Trace Package List".
4. Fare clic su Aggiorna impostazioni.


Cisco Emergency Responder Administration
For Cisco Unified Communications Solutions
Navigation Cisco ER Administration Go
Logged in as: [redacted] | Search Documentation | About | Logout
System ▾ ERL ▾ Phone Tracking ▾ ERL Membership ▾ User Management ▾ Reports ▾ Tools ▾ Help ▾

Server Settings For CERServerGroup

Modify Server Settings

Server Name * Publisher

Host Name [redacted]

Debug Package List Select All Clear All

□ CER_DATABASE
□ CER_REMOTEUPDATE
□ CER_PHONETRACKINGENGINE
□ CER_ONSITEALERT
□ CER_CALLENGINE
□ CER_PROVIDER
□ CER_AUDIT
□ CER_APPSERVICES
□ CER_SYSADMIN
□ CER_TELEPHONY
□ CER_AGGREGATOR
□ CER_GROUP
□ CER_CLUSTER
□ CER_ACCESSPOINT
□ CER_CREDENTIALPOLICY

Trace Package List Select All Clear All

□ CER_DATABASE
□ CER_REMOTEUPDATE
□ CER_PHONETRACKINGENGINE
□ CER_ONSITEALERT
□ CER_CALLENGINE
□ CER_PROVIDER
□ CER_AUDIT
□ CER_APPSERVICES
□ CER_SYSADMIN
□ CER_TELEPHONY
□ CER_AGGREGATOR
□ CER_GROUP
□ CER_CLUSTER
□ CER_ACCESSPOINT
□ CER_CREDENTIALPOLICY

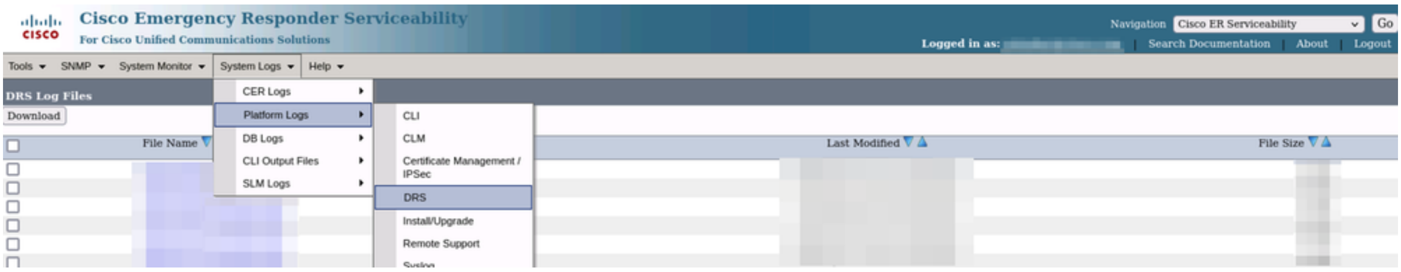
Update Settings Cancel Changes

Debug e tracce di CER

A questo punto, replicare il problema.

Una volta replicato il problema, procedere alla raccolta dei log DRS applicabili al tentativo di replica dalla pagina Web Cisco ER Serviceability effettuando le seguenti operazioni:

1. Da Navigazione selezionare Cisco ER Serviceability.
2. Passare a Log di sistema > Log piattaforme > DRS.


Cisco Emergency Responder Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco ER Serviceability Go
Logged in as: [redacted] | Search Documentation | About | Logout
Tools ▾ SNMP ▾ System Monitor ▾ System Logs ▾ Help ▾
DRS Log Files
Download
File Name
Last Modified
File Size
CER Logs
Platform Logs
DB Logs
CLI Output Files
SLM Logs
CLI
CLM
Certificate Management / IPSec
DRS
Install/Upgrade
Remote Support
Syslog

CER - Raccolta dei log DRS

Analisi log

Quando si analizzano i registri, si inizia a vedere dove il server sta tentando di stabilire la connessione con il peer e nei registri viene visualizzato il messaggio di errore che indica la causa dell'errore.

Dai registri MA DRF di CER Publisher:

```
2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: Numero di voci in IPSec trustStore: 1
2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient:drfQueryTruststore - Query truststore per ogni 20 ore
```

```
2023-06-21 07:58:58,168 ERRORE [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: impossibile creare il flusso di input/output per il client Avviso irreversibile ricevuto: certificato non valido
```

```
2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run: Ricevuta richiesta socket client da /IP:Port
2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - Convalida se la richiesta del client proviene da un nodo nel cluster
2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - Client convalidato. IP = 10.10.20.25 Nome host = device.test.org. La richiesta proviene da un nodo all'interno del cluster
2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: flusso di input dell'oggetto socket da creare
2023-06-21 08:04:46,313 ERRORE [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: impossibile creare il flusso di input/output per il client Avviso irreversibile ricevuto: certificato non valido
```

Dai log locali DRF del server di pubblicazione CER:

```
2023-06-21 07:58:47,453 DEBUG [main] - drfNetServerClient:Reconnect, Unable to connect to host: [X], messaggio: Connessione rifiutata (Connessione rifiutata), causa: null
```

Fino a questo momento la connessione viene rifiutata a causa di un certificato non valido.

Il certificato utilizzato per stabilire la connessione trusted tra i nodi per i backup e i ripristini è IPSec. A questo punto è già possibile determinare se il problema è correlato alla scadenza del certificato IPSec o alla presenza di un certificato non corretto in uno dei server.

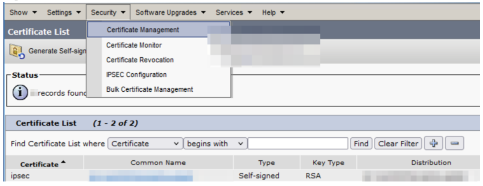
Azione correttiva

1. Verificare il numero di serie (SN) dei certificati di attendibilità IPSec in tutti i nodi del sottoscrittore CER. Tale numero deve corrispondere al numero di serie (SN) del file IPSec.prem del server di pubblicazione CER (scenario 1).
2. Confermare la validità del certificato IPSec.pem nel nodo CER Publisher. La data deve essere valida oppure è necessario rigenerare il certificato IPSec (scenario 2).

Scenario 1

Il numero di serie del certificato IPSec non corrisponde tra il numero di serie pubblicato da CER e i sottoscrittori CER. Procedere come segue:

1. Eliminare il certificato di attendibilità IPSec nel sottoscrittore o nei sottoscrittori CER i cui numeri di serie non corrispondono a quello nel server di pubblicazione CER.
2. Scaricare "IPSec.pem" dal server di pubblicazione CER dal percorso: Cisco Unified OS Administration > Security > Certificate Management > Find



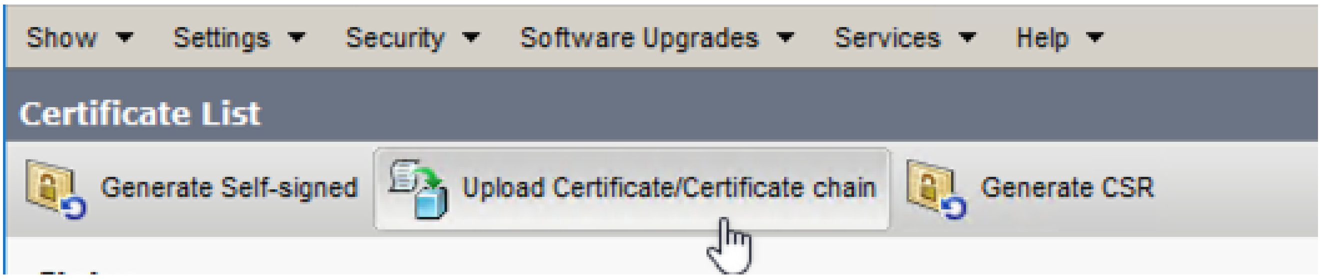
Certificate List (1 - 2 of 2)

Find Certificate List where Certificate begins with

Certificate	Common Name	Type	Key Type	Distribution
ipsec		Self-signed	RSA	

Certificato CER ipsec.pem

3. Caricare il file "IPSec.pem" nei Sottoscrittori CER necessari come certificato di attendibilità nel percorso: Cisco Unified OS Administration > Security > Certificate Management > Upload the certificate as IPSec-trust.



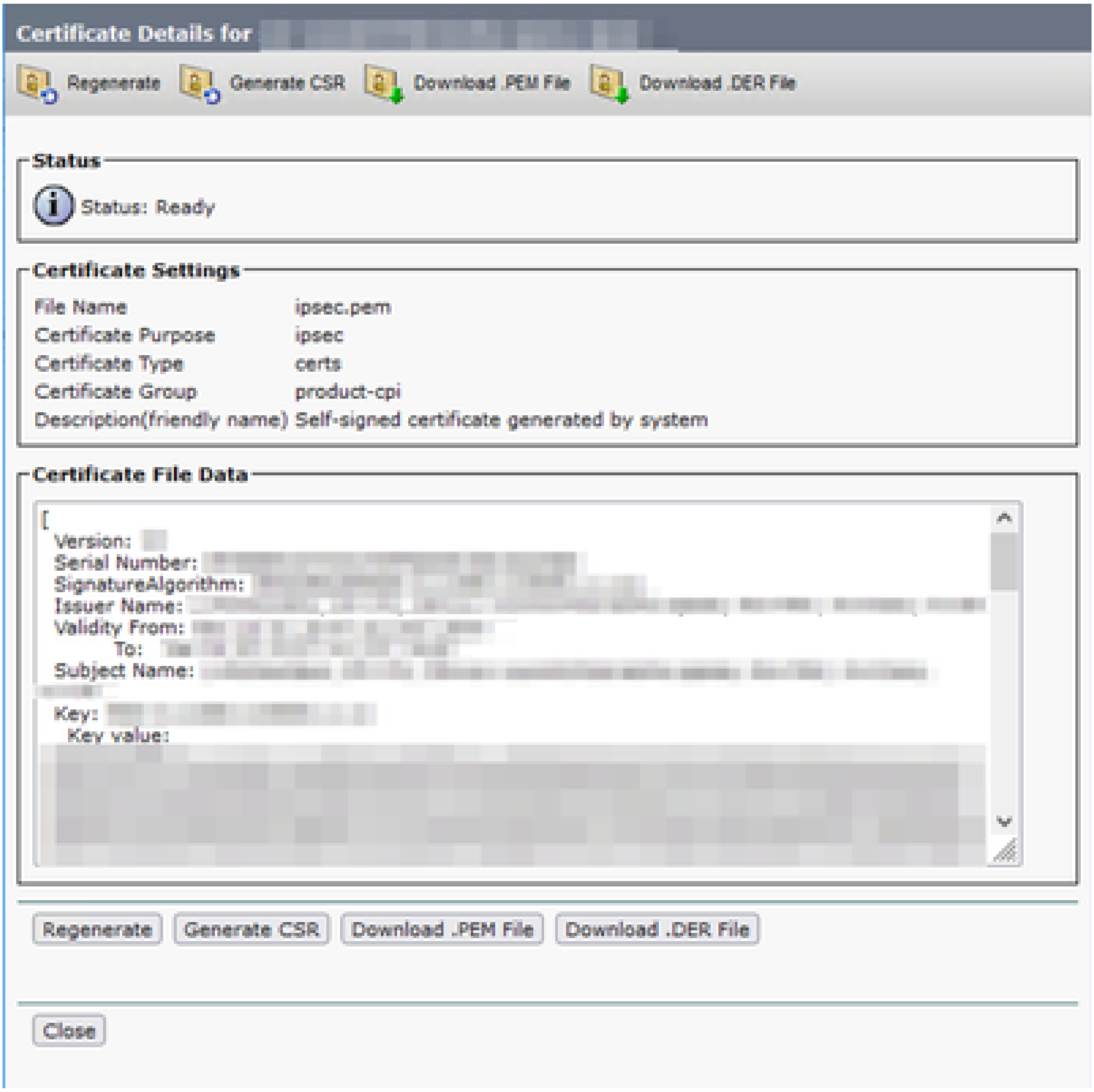
Caricamento certificato CER ipsec.trust

4. Riavviare i servizi DRF Local e DRF Master in tutti i nodi CER.

Scenario 2

IPSec è scaduto e deve essere rigenerato. Procedere come segue:

1. Passare a Cisco Unified OS Administration > Security > Certificate Management (Amministrazione del sistema operativo unificato Cisco > Sicurezza > Gestione certificati) per ogni server del cluster. A partire dall'autore, quindi da ogni sottoscrittore.
2. A partire dal server di pubblicazione CER, fare clic su Trova per visualizzare tutti i certificati nel server.
3. Fare clic sul certificato IPSec.pem.
4. Verranno visualizzate le informazioni sul certificato, quindi fare clic su Rigenera.



Certificate Details for [redacted]

Status

Status: Ready

Certificate Settings

File Name	ipsec.pem
Certificate Purpose	ipsec
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Self-signed certificate generated by system

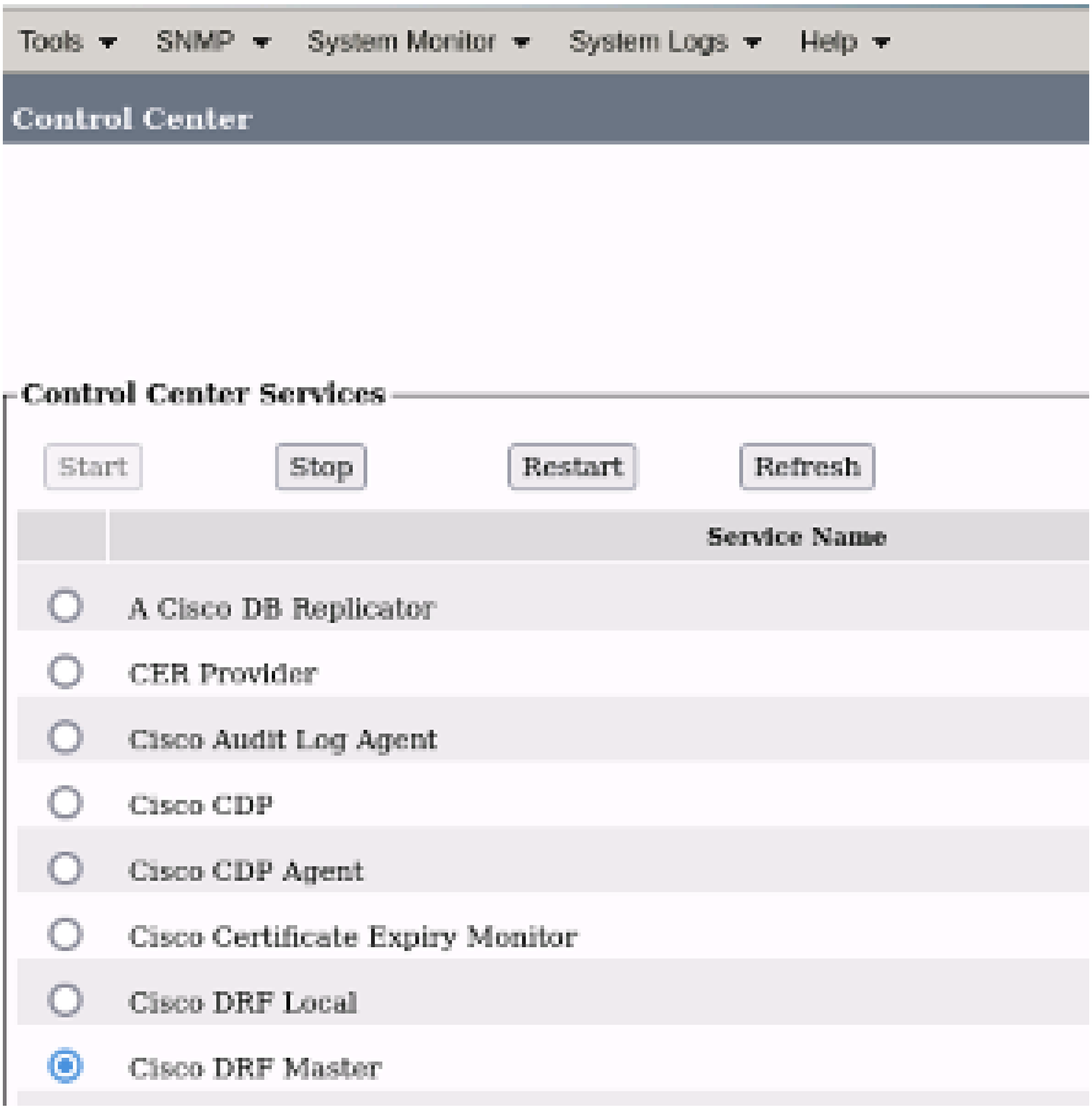
Certificate File Data

```
[
  Version: [redacted]
  Serial Number: [redacted]
  SignatureAlgorithm: [redacted]
  Issuer Name: [redacted]
  Validity From: [redacted]
           To: [redacted]
  Subject Name: [redacted]

  Key: [redacted]
    Key value:
[redacted]
```

Rigenerazione CER ipsec.pem

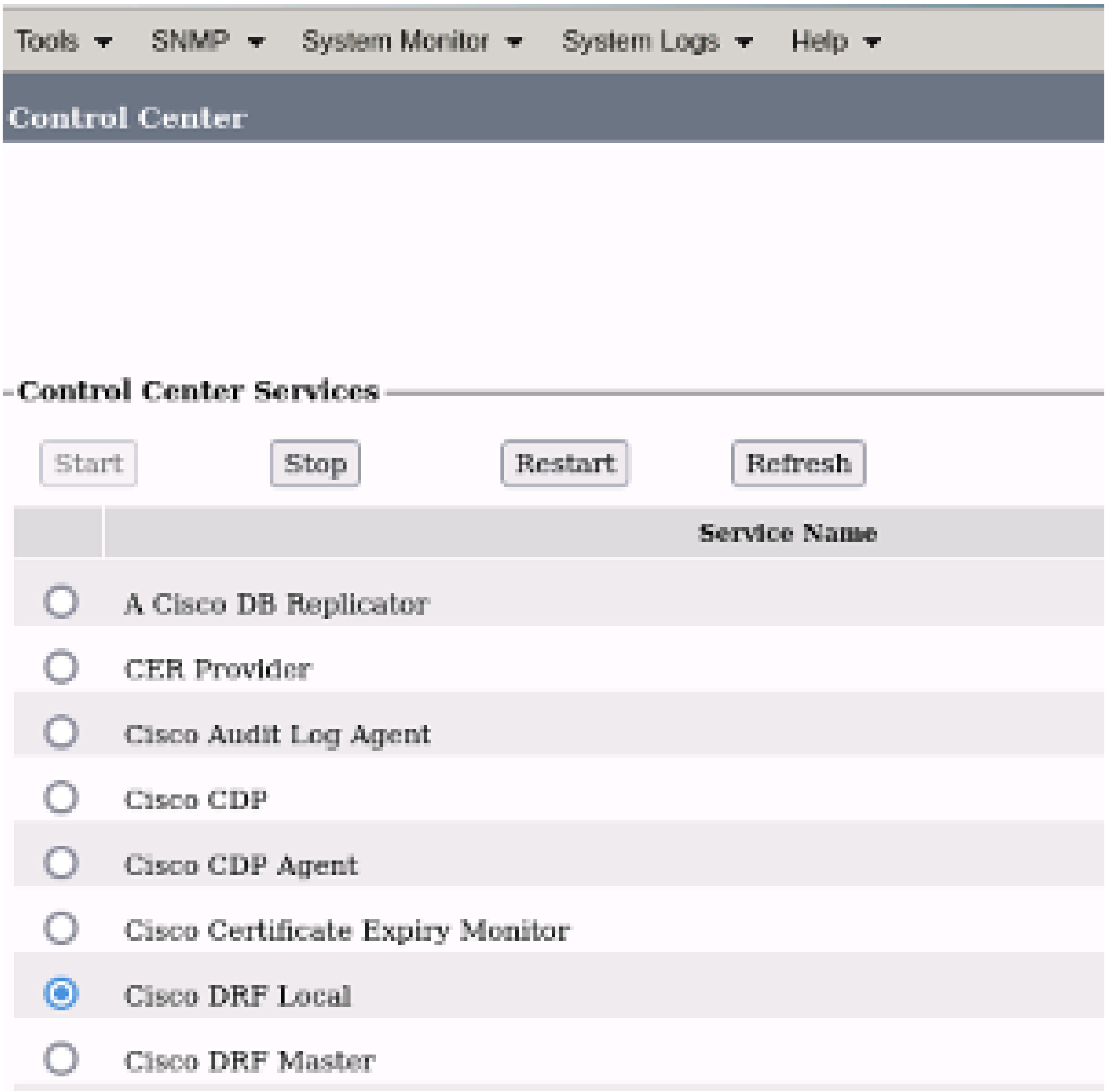
5. Una volta rigenerato il certificato nel server di pubblicazione CER e visualizzato il messaggio Operazioni riuscite, ripetere i passaggi da 1 a 4 nei nodi del server di sottoscrizione CER.
6. Una volta rigenerato il certificato in tutti i nodi, riavviare i seguenti servizi:
   - Cisco DRF Master solo in CER Publisher:
     - Passare a CRE Serviceability > Strumenti > Control Center Services > Cisco DRF Master



	Service Name
○	A Cisco DB Replicator
○	CER Provider
○	Cisco Audit Log Agent
○	Cisco CDP
○	Cisco CDP Agent
○	Cisco Certificate Expiry Monitor
○	Cisco DRF Local
●	Cisco DRF Master

Riavvio master CER DRF

- Una volta attivato il servizio Cisco DRF Master, riavviare Cisco DRF Local nel server di pubblicazione CER.



	Service Name
○	A Cisco DB Replicator
○	CER Provider
○	Cisco Audit Log Agent
○	Cisco CDP
○	Cisco CDP Agent
○	Cisco Certificate Expiry Monitor
●	Cisco DRF Local
○	Cisco DRF Master

Riavvio locale CER DRF

- Quando il servizio Cisco DRF Local è attivo nel nodo CER Publisher, riavviare il servizio in tutti i nodi del sottoscrittore CER.

7. Dopo il riavvio dei servizi su tutti i nodi, eseguire un backup manuale del sistema:
    - Passare a Disaster Recovery System > Backup > Backup manuale.
    - Selezionare il nome del dispositivo di backup.
    - Selezionare le funzionalità per il backup.
    - Fare clic per avviare il backup.

Informazioni correlate

Come raccogliere i log per CER

Rigenera certificato CUCM