Troubleshoot CER Backup Failing with Error Message

Contents

Introduction

This document describes how to troubleshoot the Cisco Emergency Responder (CER) failing to back up and displaying an error message under its status.

Prerequisites

Requirements

Cisco recommends to have knowledge on these topics:

- Cisco Emergency Responder
- Basic Understanding of Security Certificates

Components Used

The information in this document is based on these software versions:

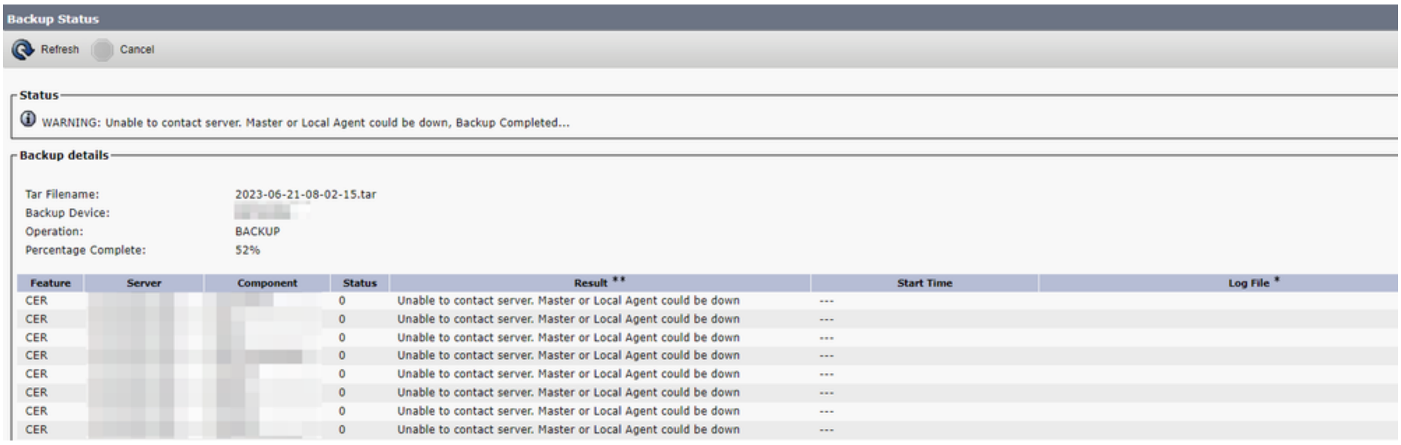
- Cisco Emergency Responder 11.5.4.60000-5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

CER deployed in cluster mode can fail to back up with the error message "Unable to contact server. Master or Local Agent could be down".

For example:



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	---	

CER Backup Error Message

Affected versions are 11.x and above.

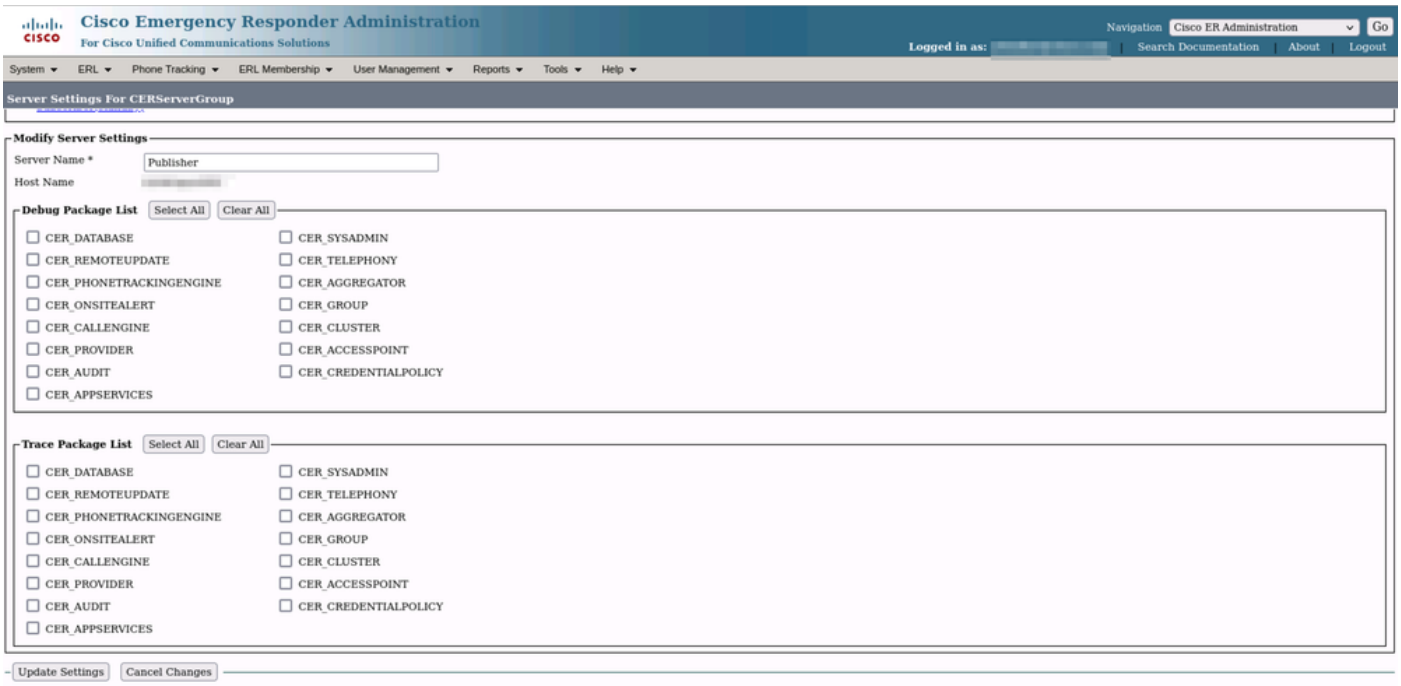
Troubleshooting

Log Collection

When this occurs, gather logs as to try to collect as much information as possible to try to determine the source of the issue and determine the correct action plan to resolve the problem.

Before collecting the logs, please activate detailed tracing and debugging completing these steps:

1. Log on to CER Administration web page.
2. Navigate to **System** > **Server Settings**. CER Publisher is selected by default and can be changed if CER Subscriber logs are also needed.
3. Click **Select All** for the sections "Debug Package List" and "Trace Package List".
4. Click **Update Settings**.



Logged in as: [redacted]

Server Settings For CERServerGroup

Modify Server Settings

Server Name * Publisher

Host Name [redacted]

Debug Package List

□ 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

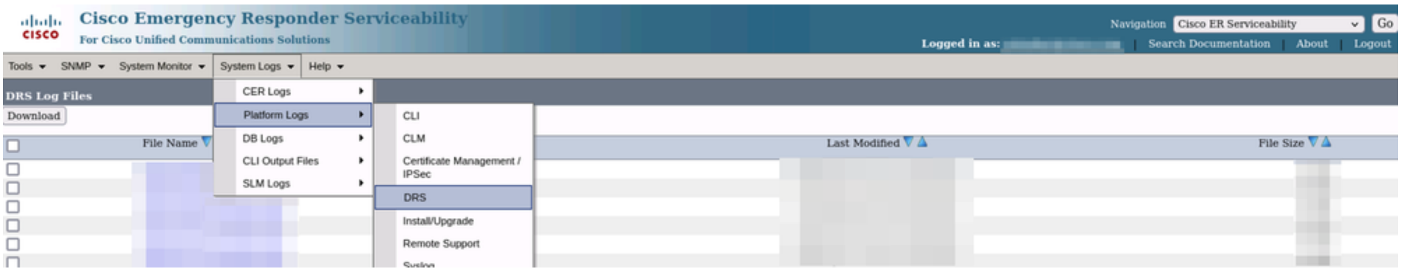
□ CER_DATABASE
□ CER_REMOTEUPDATE
□ CER_PHONETRACKINGENGINE
□ CER_ONSITEALERT
□ CER_CALLENGINE
□ CER_PROVIDER
□ CER_AUDIT
□ CER_APPSERVICES
□ CER_SYSADMIN
□ CER_TELEPHONY
□ CER_AGGREGATOR
□ CER_GROUP
□ CER_CLUSTER
□ CER_ACCESSPOINT
□ CER_CREDENTIALPOLICY

CER Enabling Debugs and Traces

At this point, please replicate the issue.

Once the issue has been replicated, proceed to gather the **DRS logs** applicable to the replication attempt from the Cisco ER Serviceability Web page completing these steps:

1. From **Navigation** select **Cisco ER Serviceability**.
2. Navigate to **System Logs** > **Platform Logs > DRS.**



CER Collecting DRS Logs

Log Analysis

When analyzing the logs, we start to see where the server is trying to establish the connection with its peer and we see the error message in the logs pointing us to the reason of the failure.

From the CER Publisher DRF MA logs:

```
2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient: drfQueryTruststore: Number of entries in IPSec trustStore : 1
2023-06-21 07:58:58,148 DEBUG [Thread-16] - drfNetServerClient:drfQueryTruststore - Query truststore for every 20 hours
2023-06-21 07:58:58,168 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Unable to create input/output stream to client Fatal Alert received: Bad Certificate
```

```
2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - drfNetServer.run: Received Client Socket request from /IP:Port
2023-06-21 08:04:46,274 DEBUG [NetServerWorker] - Validating if client request is from a Node within the Cluster
2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - Validated Client. IP = 10.10.20.25 Hostname = device.test.org. Request is from a Node within the Cluster
2023-06-21 08:04:46,278 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Socket Object InpuputStream to be created
2023-06-21 08:04:46,313 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Unable to create input/output stream to client Fatal Alert received: Bad Certificate
```

From the CER Publisher DRF Local logs:

```
2023-06-21 07:58:47,453 DEBUG [main] - drfNetServerClient:Reconnect, Unable to connect to host: [X], message: Connection refused (Connection refused), cause: null
```

We see up until this point that the connection is refused due to a bad certificate.

The certificate that is used to establish the trusted connection between the nodes for backups/restores is the IPSec. At that point we can already determine that the issue is related to the IPSec certificate being expired or an incorrect certificate being present in one of the servers.

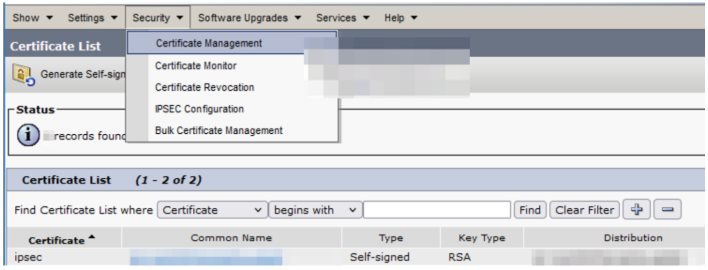
Corrective Action

1. Verify the Serial Number (SN) of the IPSec-trust certificates in all the CER Subscriber nodes, this must match the SN of the IPSec.prem from the CER Publisher (**Scenario 1**).
2. Confirm the validity of the IPSec.pem Certificate in the CER Publisher node. The date must be valid or the IPSec certificate must be regenerated (**Scenario 2**).

Scenario 1

IPSec Certificate SN does not match between CER Published and CER Subscribers. Proceed with these steps:

1. Delete the IPSec-trust Certificate in the CER Subscriber(s) where the serial numbers do not match with the one in the CER Publisher.
2. Download the "IPSec.pem" from the CER Publisher from the path: Cisco Unified OS Administration > **Security** > **Certificate Management** > **Find**



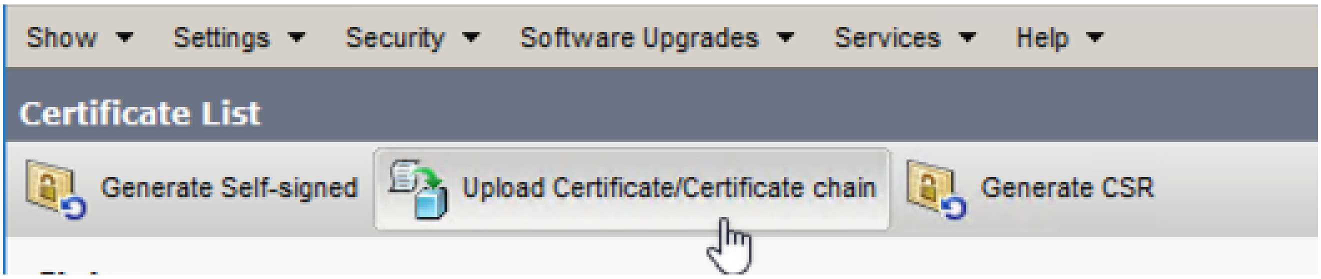
Certificate List (1 - 2 of 2)

Find Certificate List where Certificate begins with Find Clear Filter

Certificate ▲	Common Name	Type	Key Type	Distribution
ipsec	[redacted]	Self-signed	RSA	[redacted]

CER ipsec.pem Certificate

3. Upload the file "IPSec.pem" in the CER Subscribers needed as a trust Certificate on the path: Cisco Unified OS Administration > **Security** > **Certificate Management** > Upload the certificate as IPSec-trust.



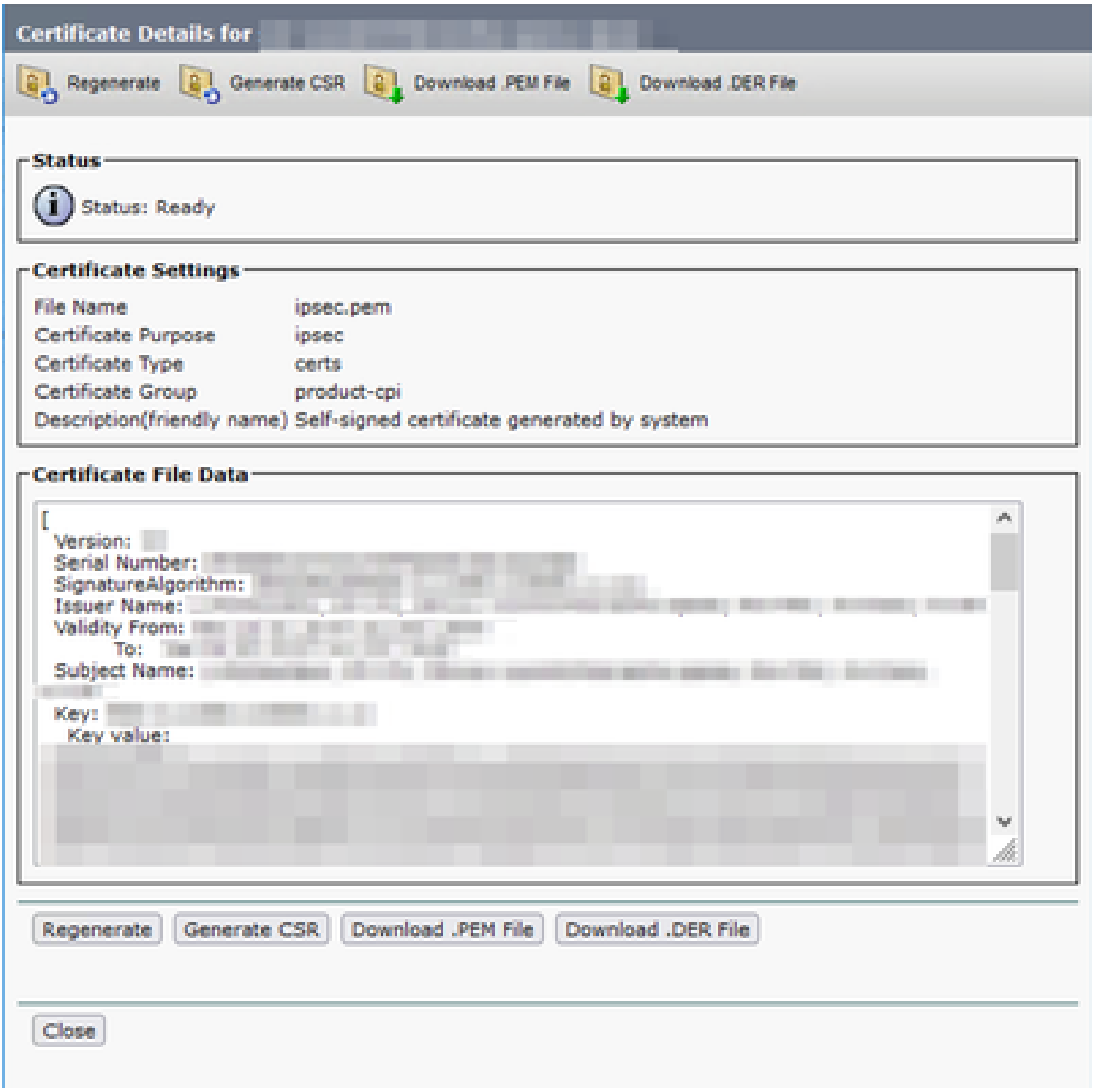
CER ipsec.trust Certificate Upload

4. Restart the **DRF Local** and **DRF Master** services in all the CER nodes.

Scenario 2

IPSec is expired and needs to be regenerated. Proceed with these steps:

1. Navigate to **Cisco Unified OS Administration** > **Security** > **Certificate Management,** for each server in the cluster. Starting with the publisher, then each subscriber.
2. Starting with the CER Publisher, click **Find** to show all Certificates in the server.
3. Click on the Certificate "IPSec.pem".
4. This brings up the Certificate information and then click on **Regenerate.**



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

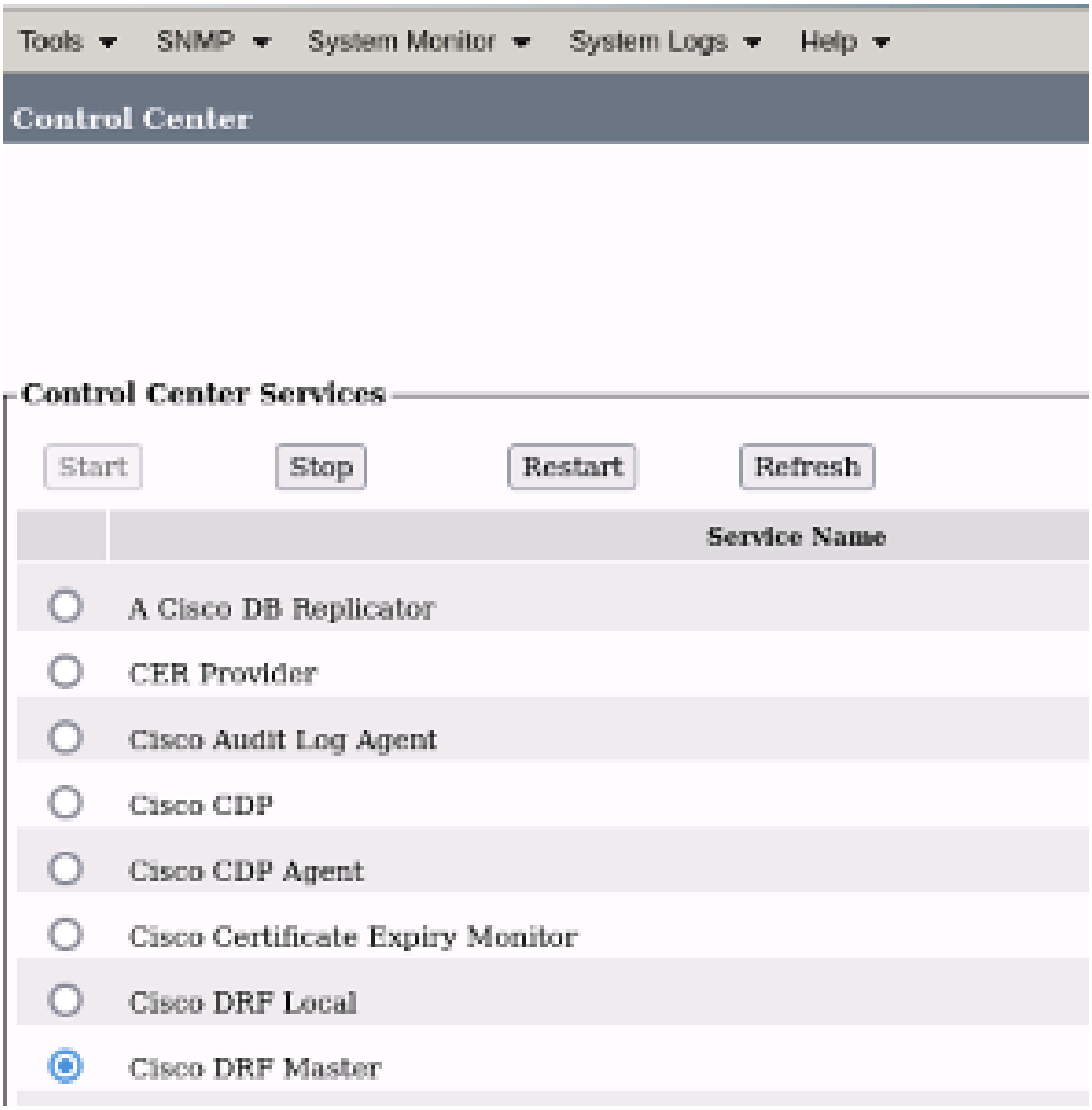
Certificate File Data

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

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

CER ipsec.pem Regenerate

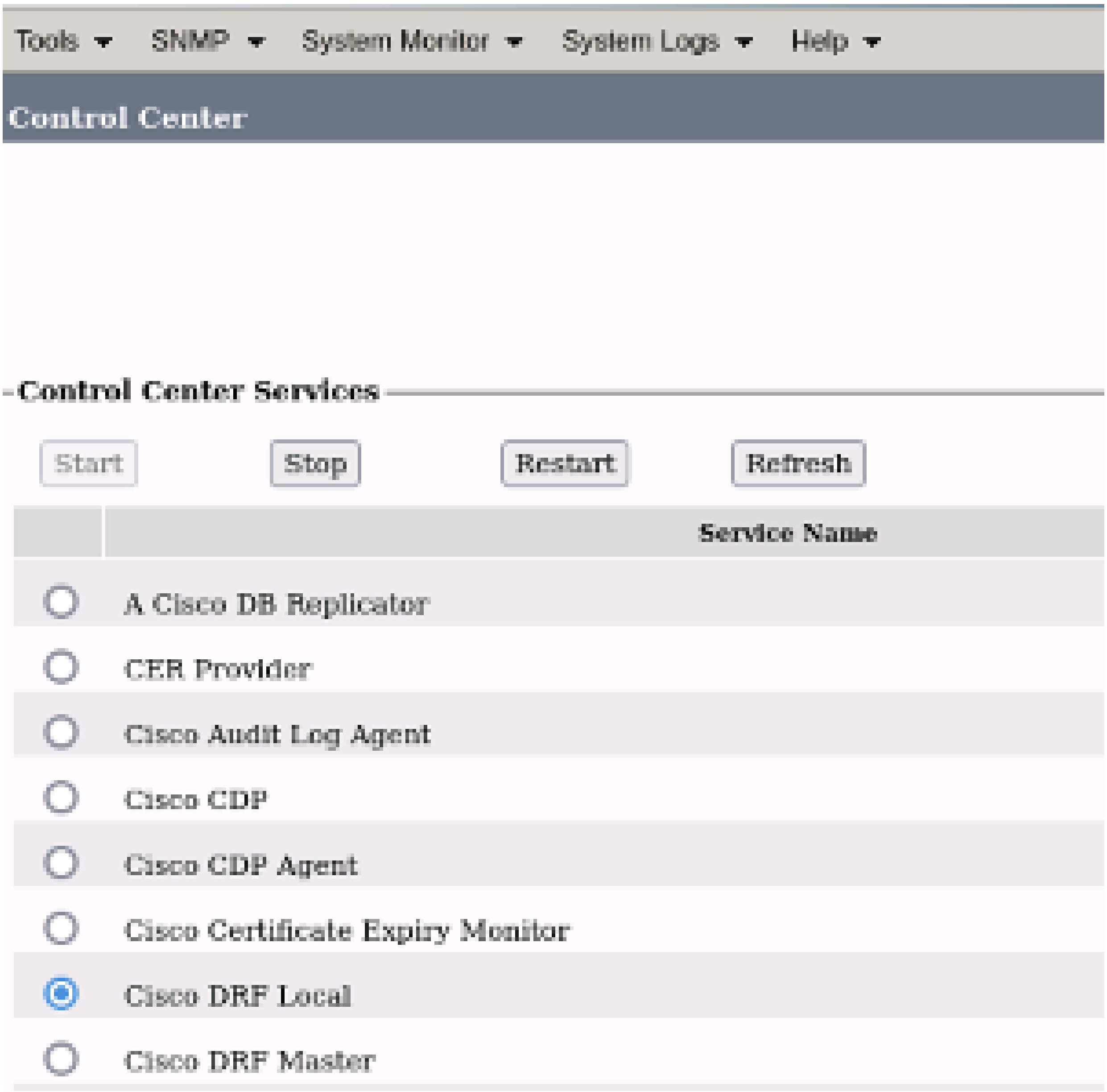
5. Once the certificate is regenerated in the CER Publisher and the **Success** message is seen, please repeat steps 1-4 in the CER Subscriber nodes.
6. Once the certificate is regenerated in all nodes, restart these services:
   - **Cisco DRF Master** in the CER Publisher only:
     - Navigate to **CER Serviceability** > **Tools** > **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

CER Cisco DRF Master Restart

- Once the Cisco **DRF Master** service is active, restart the **Cisco DRF Local** in the CER Publisher first.



	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

CER Cisco DRF Local Restart

- Once the Cisco **DRF Local** service is active in the CER Publisher node, restart this service in all the CER Subscriber nodes.

7. After the services have been restarted on all nodes, perform a manual backup of the system:
    - Navigate to **Disaster Recovery System** > **Backup** > **Manual Backup**.
    - Select the Backup Device Name.
    - Select the Features for the Backup.
    - Click to Start Backup.

Related Information

How to Collect Logs for CER

Regenerate CUCM Certificate