Rebuild CUCM Publisher from Subscriber

Contents

Introduction

Background

Gather Cluster Data

Stop Replication on All Subscribers

Install the CUCM Publisher

Update Processnode Values on the Publisher

Reboot the Publisher Node

Verify Cluster Authentication

Perform a New Backup

- Add a Backup Device
- Start a Manual Backup

Publisher Restore from the Subscriber DB

- Restore Status

Run a Sanity Check on the Publisher DB

Reboot the Cluster

Verify Replication Setup Requirements

Replication Setup

Post Restore

- Activate Services
- Install Data that was not Restored

Troubleshoot

- Cluster does not Authenticate
- Restoration does not Process CCMDB Component
- Replication Failure
- Phones do not Register or are Unable to Access Services

Introduction

This document describes how to restore the Cisco Unified Communications Manager (CUCM) publisher node from the subscriber database without prior backup or root access.

Background

In early versions of CUCM, the publisher node was regarded as the only authoritative source for the Structured Query Language (SQL) DB.

Consequently, if a publisher node was lost due to a hardware failure or a file system corruption, the only way to recover it was to reinstall and restore the DB from a Disaster Recovery System (DRS) backup.

Some customers did not keep proper backups, or had backups that were out-of-date, so the only option was

to rebuild and reconfigure the publisher server node.

In CUCM Version 8.6(1), a new feature was introduced in order to restore a publisher DB from a subscriber database.

This document describes how to take advantage of this feature in order to successfully restore a publisher DB from the subscriber.

Cisco strongly recommends that you keep a full Disaster Recovery Framework (DRF) backup of the entire cluster.

Since this process only recovers the CUCM DB configuration, other data, such as certificates, Music on Hold (MoH), and TFTP files, are not recovered. In order to avoid these issues, keep a full cluster DRF backup.

Note: Cisco recommends that you review and be familiar with the entire process described in this document before you begin.

Gather Cluster Data

Before you reinstall the publisher, it is critical that you gather the pertinent details about the previous publisher. These details must match the original publisher installation:

- IP address
- Host name
- Domain name
- Security passphrase
- Exact CUCM version
- Installed Cisco Options Package (COP) files

In order to retrieve the first three items in the list, enter the **show network cluster** command at the current subscriber node CLI:

<#root>

admin:

show network cluster

172.18.172.213 cucm911ccnasub1 Subscriber authenticated

172.18.172.212 cucm911ccnapub

  Publisher not authenticated - INITIATOR
 since Tue Dec 3 12:43:24 2013
172.18.172.214 cucm911ccnasub2 Subscriber authenticated using TCP since
 Sun Dec 1 17:14:58 2013

In this case, the IP address is **172.18.172.212**, the host name is **cucm911ccnapub**, and there is no domain name configured for the publisher.

The security passphrase (the fourth item in the list) is retrieved from the site documentation.

If you are unsure about the security passphrase, make a best-effort guess, and you can attempt to verify and correct it as needed based on the CUCM version.

If the security passphrase is incorrect, then a cluster outage is required in order to correct the situation.

In order to retrieve the exact CUCM version and the installed COP files (the last two items in the list), gather the system output from the **show version active** command:

```
<#root>

admin:

show version active


Active Master Version:

9.1.2.10000-28


Active Version Installed Software Options:

No Installed Software Options Found.
```

In this case, Version **9.1.2.10000-28** is installed with no add-on COP files.

Note: It is possible that some COP files were previously installed on the publisher, but were not installed on the subscriber, and vice versa. Use this output as a guideline only.

Stop Replication on All Subscribers

When the publisher is installed, it is critical that replication does not set up and delete the current subscriber DBs. In order to prevent this, enter the **utils dbreplication stop** command on all subscribers:

```
<#root>

admin:

utils dbreplication stop


********************************************************************************
This command can delete the marker file(s) so that automatic replication setup
is stopped
It can also stop any replication setup currently executing
********************************************************************************

Deleted the marker file, auto replication setup is stopped

Service Manager is running
Commanded Out of Service
A Cisco DB Replicator[NOTRUNNING]
Service Manager is running
A Cisco DB Replicator[STARTED]
```

```
Completed replication process cleanup

Please run the command 'utils dbreplication runtimestate' and make sure all nodes
are RPC reachable before a replication reset is executed
```

Install the CUCM Publisher

Gather a bootable image of the appropriate version, and perform an install with an upgrade to the appropriate version.

Note: Most CUCM Engineering Special (ES) Releases are already bootable.

Install the publisher and specify the correct values for the IP address, host name, domain name, and security passphrase mentioned previously.

Update Processnode Values on the Publisher

Note: The publisher must be aware of at least one subscriber server in order to restore the DB from that subscriber. Cisco recommends that you add all subscribers.

In order to retrieve the node list, enter the **run sql select name,description,nodeid from processnode** command at the CLI of a current subscriber.

The name values can be host names, IP addresses, or Fully Qualified Domain Names (FQDNs).

If you run CUCM Version 10.5(2) or later, the **utils disaster_recovery prepare restore pub_from_sub** command must be run on the publisher CLI before you can proceed to add nodes to **System > Server**:

```
admin:utils disaster_recovery prepare restore pub_from_sub
admin:
```

Warning: Many people using CUCM Version 10.5(2) or later skip the command **utils disaster_recovery prepare restore pub_from_sub**; however, this is a critical command. Be sure not to skip any steps in this document.

After you receive the node list, navigate to **System > Server** and add all of the name values other than **EnterpriseWideData** to the Publisher Server Unified CM Administration page.

The name values must correspond to the **Host Name/IP Address** field on the **System > Server** menu.

<#root>

```
admin:
```

run sql select name,description,nodeid from processnode

```
name                 description     nodeid
```

```
================= ============== ======
EnterpriseWideData                1
```

172.18.172.212

```
     CUCM901CCNAPub  2
```

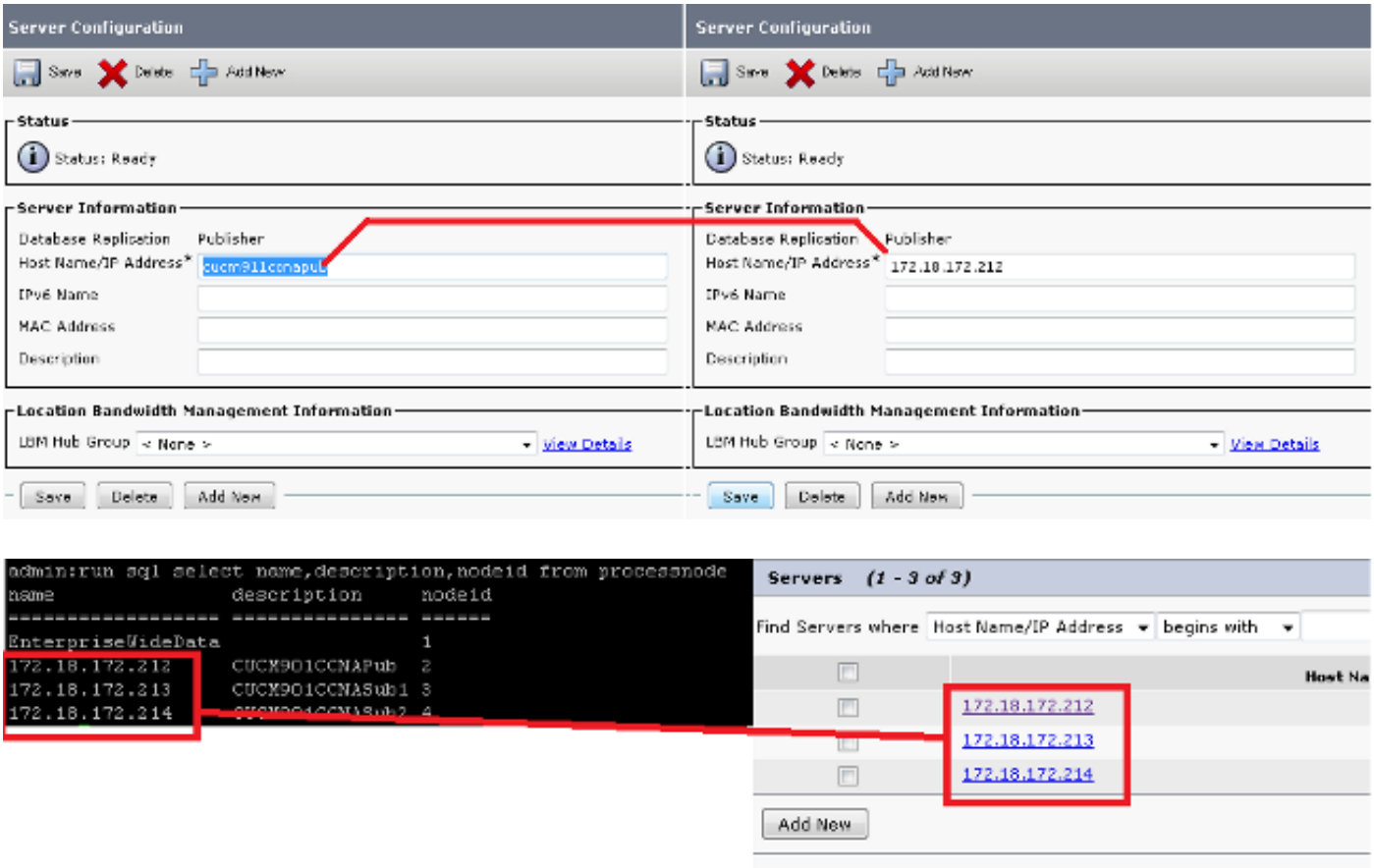
172.18.172.213

```
     CUCM901CCNASub1 3
```

172.18.172.214

```
     CUCM901CCNASub2 4
```

Note: The default installation adds the publisher host name to the processnode table. You can change it to an IP address if the name column lists an IP address for the publisher. In this case, do not remove the publisher entry, but open and modify the current **Host Name/IP Address** field.



Reboot the Publisher Node

In order to restart the publisher after the processnode changes are complete, enter the **utils system restart** command:

<#root>

```
admin:
```

utils system restart

```
Do you really want to restart ?
Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.

Shutting down Service Manager. Please wait...
 \Service Manager shutting down services... Please Wait

Broadcast message from root (Tue Dec  3 14:29:09 2013):

The system is going down for reboot NOW!
Waiting .

Operation succeeded
```

Verify Cluster Authentication

After the publisher restarts, if you made the changes correctly and the security passphrase is correct, the cluster must be in the authenticated state. In order to verify this, enter the **show network cluster** command:

<#root>

admin:

show network cluster

```
172.18.172.212 cucm911ccnapub  Publisher authenticated
172.18.172.213 cucm911ccnasub1
```

Subscriber authenticated using TCP since
Tue Dec 3 14:24:20 2013

172.18.172.214 cucm911ccnasub2

Subscriber authenticated using TCP since
Tue Dec 3 14:25:09 2013

Note: If the subscribers do not appear as **authenticated**, refer to the Troubleshoot section of this document in order to resolve this issue before you proceed.

Perform a New Backup

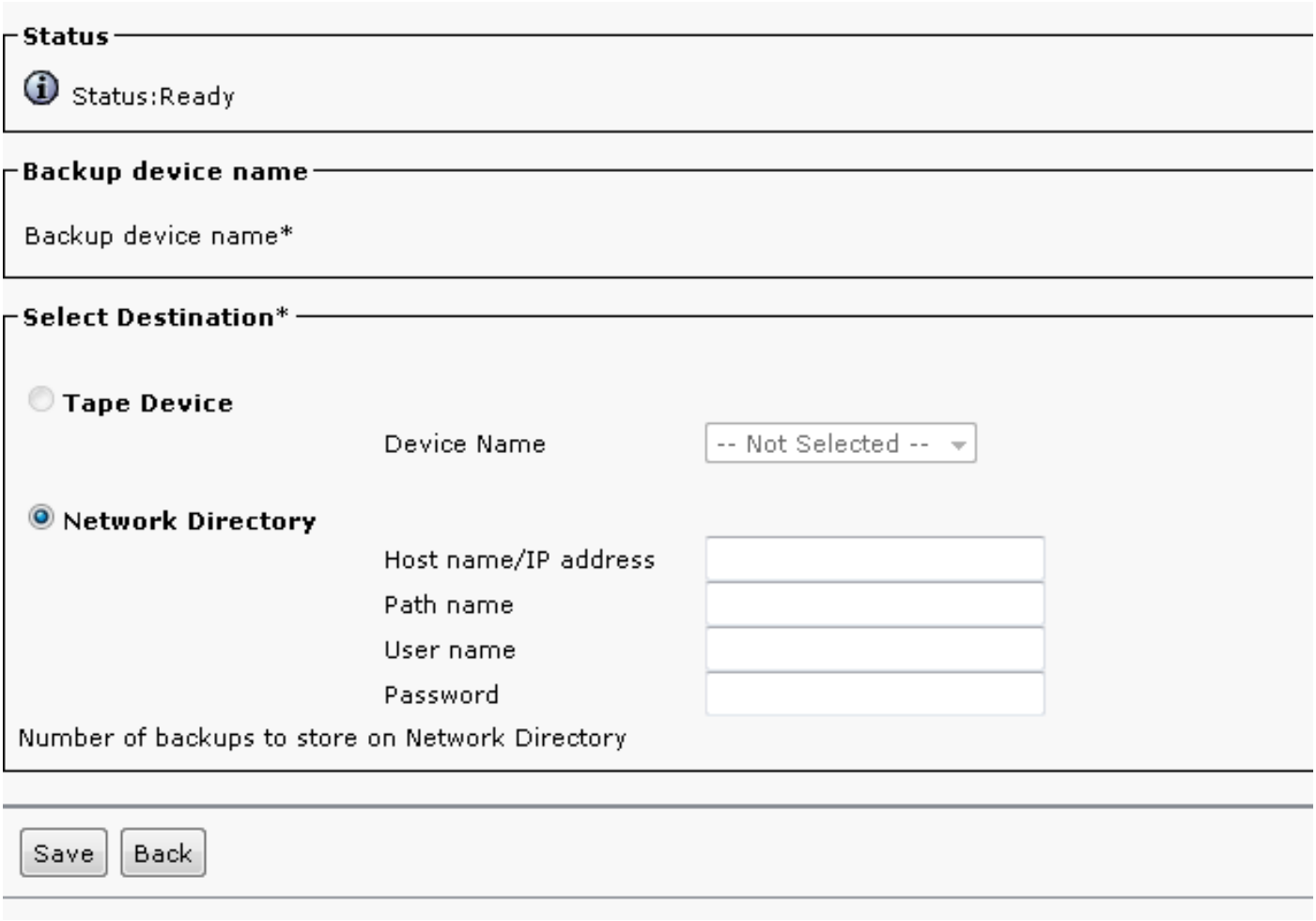
If no previous backup is available, perform a cluster backup on the DRS page.

Note: Although you can use the subscriber DB for the restore, a backup is still required in order to restore the non-DB components.

If no backup is available, then perform a new one; if a backup already exists, then you can skip this section.

Add a Backup Device

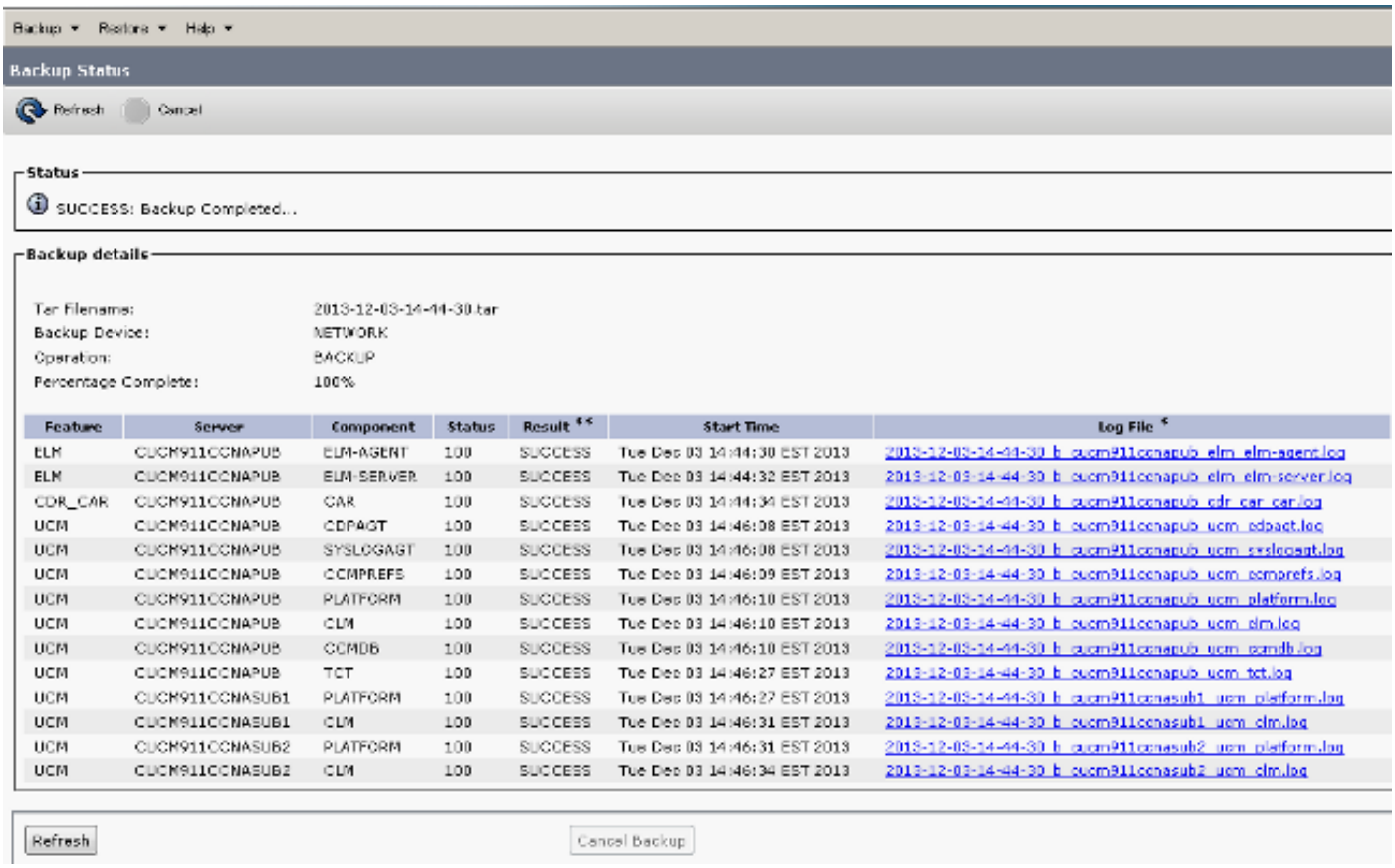
Use the Navigation Menu in order to navigate to the Disaster Recovery System, and add a backup device.



Start a Manual Backup

After the backup device is added, start a manual backup.

Note: It is critical that the publisher node has the CCMDB component registered.

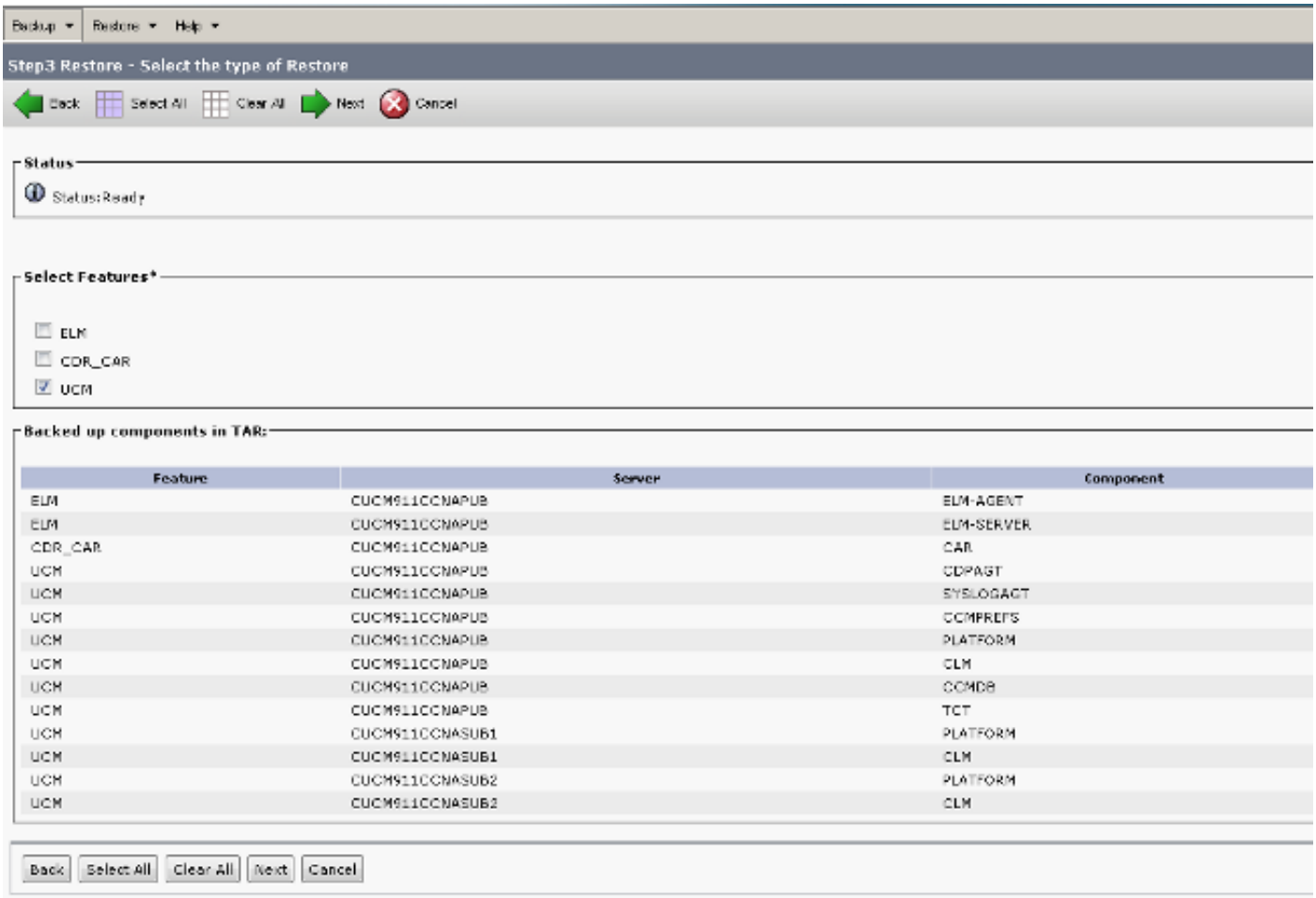


Publisher Restore from the Subscriber DB

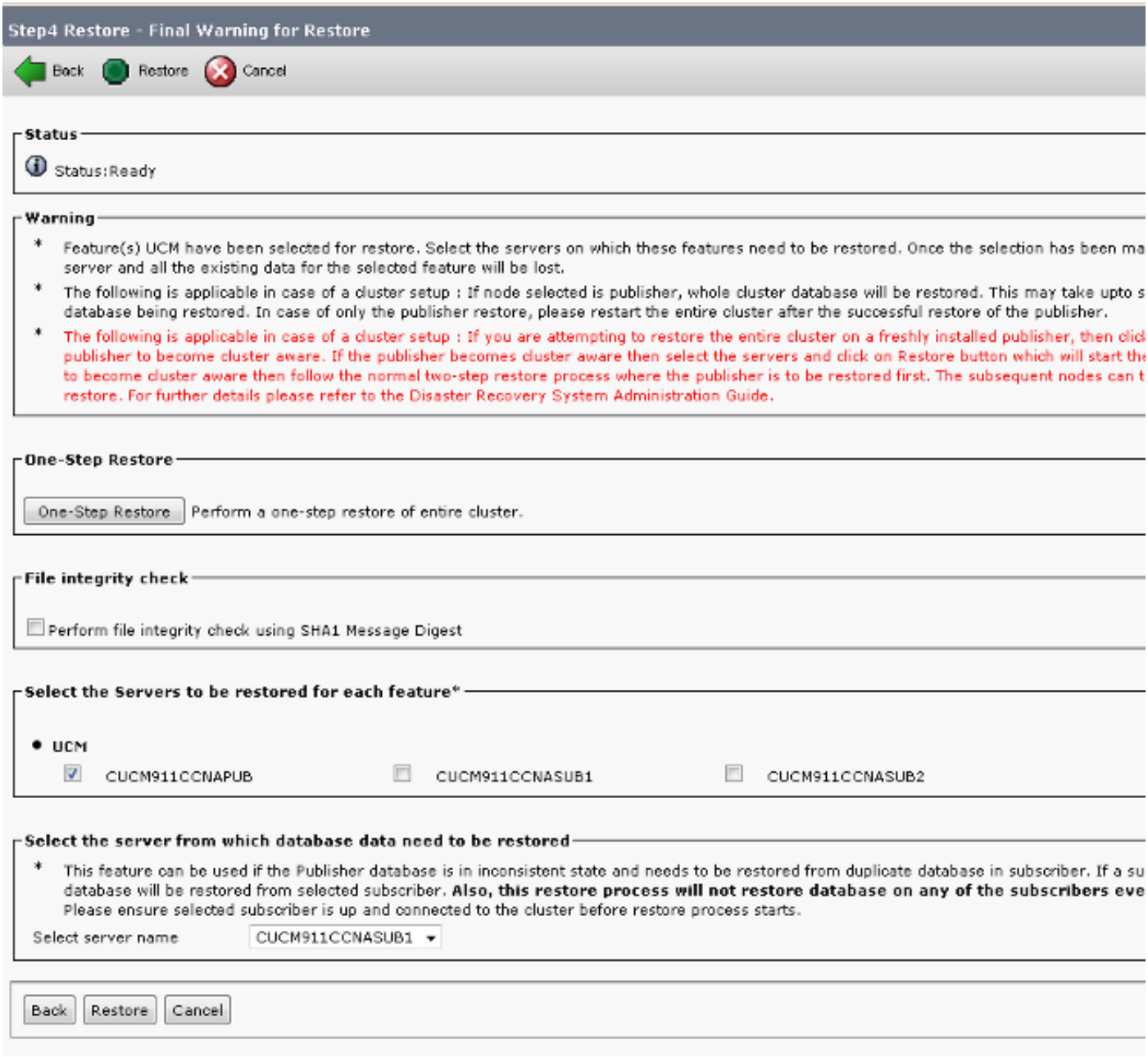
On the Disaster Recovery System page, navigate to **Restore > Restore Wizard**.

If a current backup was available, and you skipped the previous section, check all of the feature check boxes in the Select Features section: Enterprise License Manager (**ELM**) if available, **CDR_CAR**, and Unified Communications Manager (**UCM**).

If you use a backup that was performed in the previous section, check only the **UCM** check box:

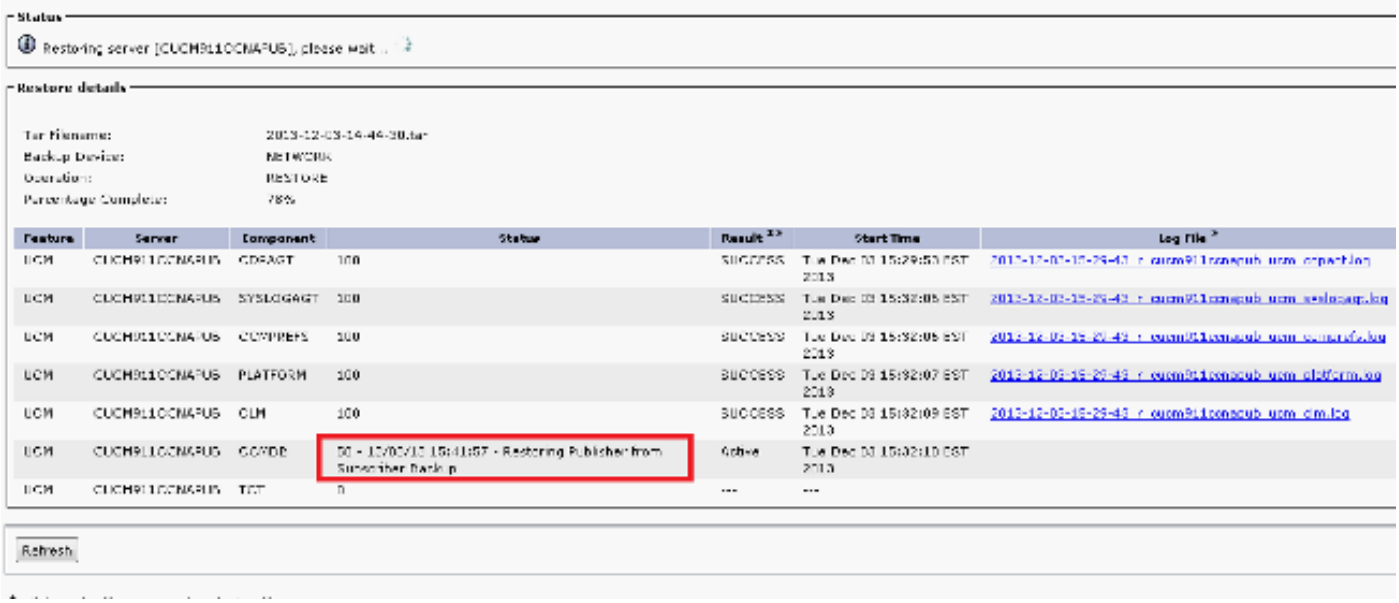


Click **Next**. Check the publisher node check box (**CUCM911CCNAPUB**), and choose the subscriber DB from which the restoration takes place. Then, click **Restore**.



Restore Status

When the restoration reaches the **CCMDB** component, the Status text must appear as **Restoring Publisher from Subscriber Backup**:



Run a Sanity Check on the Publisher DB

Before you reboot and set up replication, it is a good practice to verify that the restoration is successful and that the publisher DB contains the required information.

Ensure that these queries return the same values on the publisher and subscriber nodes before you proceed:

- **run sql select count(*) from device**
- **run sql select count(*) from enduser**

Reboot the Cluster

After the restoration is complete, enter the **utils system restart** command on every node. Start with the publisher followed by each subscriber.

<#root>

admin:

utils system restart

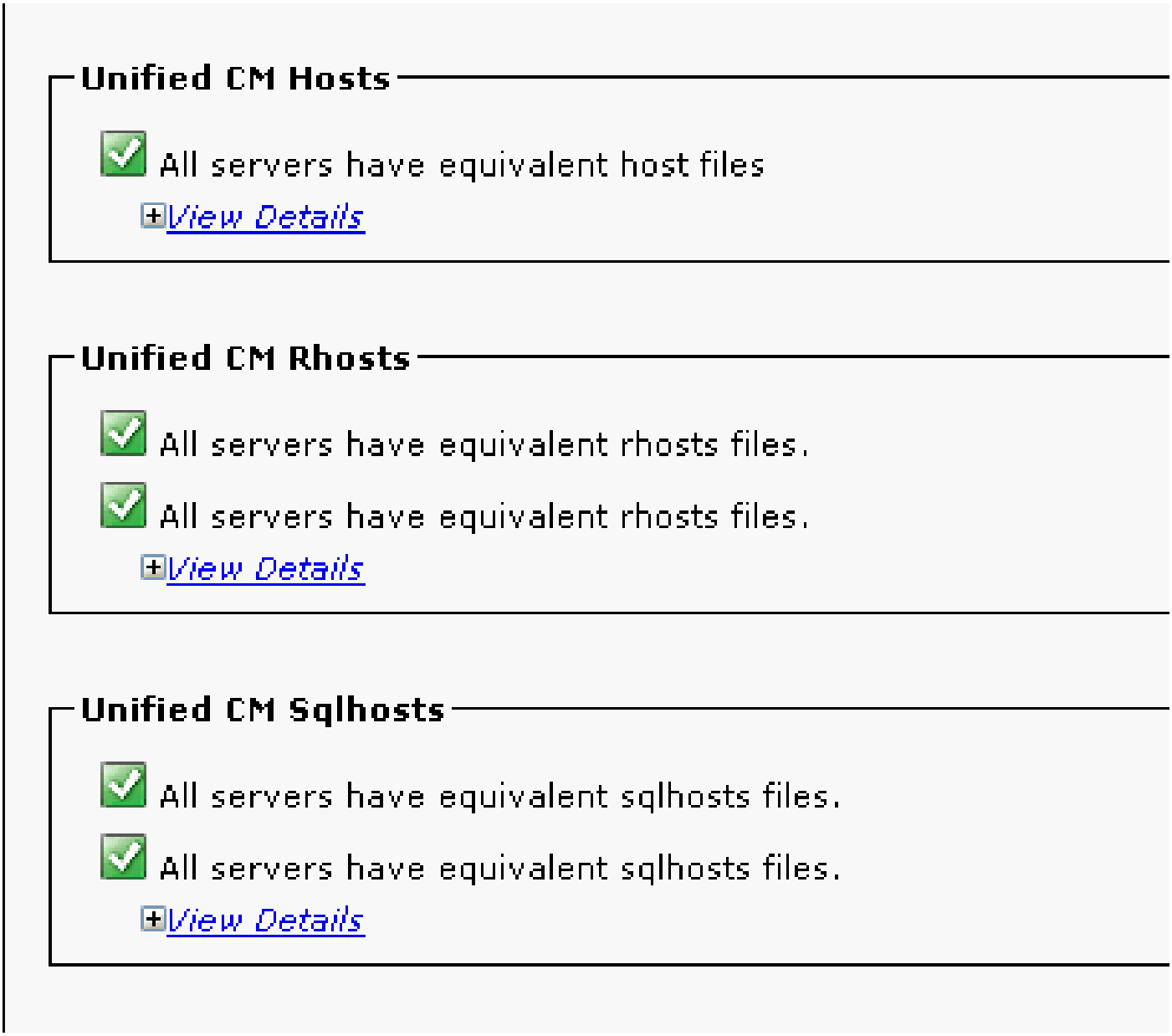
```
Do you really want to restart ?
Enter (yes/no)? yes

 Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.

Shutting down Service Manager. Please wait...
 \ Service Manager shutting down services... Please Wait

Broadcast message from root (Tue Dec  3 14:29:09 2013):

The system is going down for reboot NOW!
Waiting .

Operation succeeded
```

Verify Replication Setup Requirements

Navigate to the Cisco Unified Reporting page and generate a Unified CM Database Status Report.

It is likely that replication cannot have set up yet, but it is important to ensure that the Unified CM Hosts, Unified CM Rhosts, and Unified CM Sqlhosts files match the publisher.

If they do not, those nodes that do not match need to be rebooted again. If these files do not match, do not proceed to the next step or reset replication.



Replication Setup

Dependent upon the version, replication cannot set up automatically. In order to check this, wait for all of the services to start, and enter the **utils dbreplication runtimestate** command.

A state value of **0** indicates that setup is in progress, while a value of **2** indicates that replication is set up successfully for that node.

This output indicates that the replication setup is in progress (state appears as **0** for two of the nodes):

```
admin:utils dbreplication runtimestate

                                PING            CDR Server      REPL.   DBver&  REPL.   REPLICATION SETUP
SERVER-NAME     IP ADDRESS      (msec)  RPC?    (ID) & STATUS   QUEUE   TABLES  LOOP?   (RTMT) & details
-----------     ------------    ------  ----    --------------  -----   -------  -----   ----------------
cucm911ccnapub  172.18.172.212  0.043   Yes     (2)  Connected   0      match   Yes     (2) PUB Setup
Completed
cucm911ccnasub1 172.18.172.213  0.626   Yes     (3)  Connected   1920   match   Yes     (0) Setup Completed
cucm911ccnasub2 172.18.172.214  0.676   Yes     (4)  Connected   0      match   Yes     (0) Setup Completed
```

This output indicates that replication is set up successfully:

```
admin:utils dbreplication runtimestate

Cluster Detailed View from cucm911ccnapub (3 Servers):

                                PING            CDR Server      REPL.   DBver&  REPL.   REPLICATION SETUP
SERVER-NAME     IP ADDRESS      (msec)  RPC?    (ID) & STATUS   QUEUE   TABLES  LOOP?   (RTMT) & details
-----------     ------------    ------  ----    --------------  -----   -------  -----   ----------------
cucm911ccnapub  172.18.172.212  0.043   Yes     (2)  Connected   0      match   Yes     (2) PUB Setup
Completed
cucm911ccnasub1 172.18.172.213  8.858   Yes     (3)  Connected   0      match   Yes     (2) Setup Completed
cucm911ccnasub2 172.18.172.214  0.729   Yes     (4)  Connected   0      match   Yes     (2) Setup Completed
```

If any nodes appear with a state value of **4**, or if replication does not successfully set up after several hours, enter the **utils dbreplication reset all** command from the publisher node.

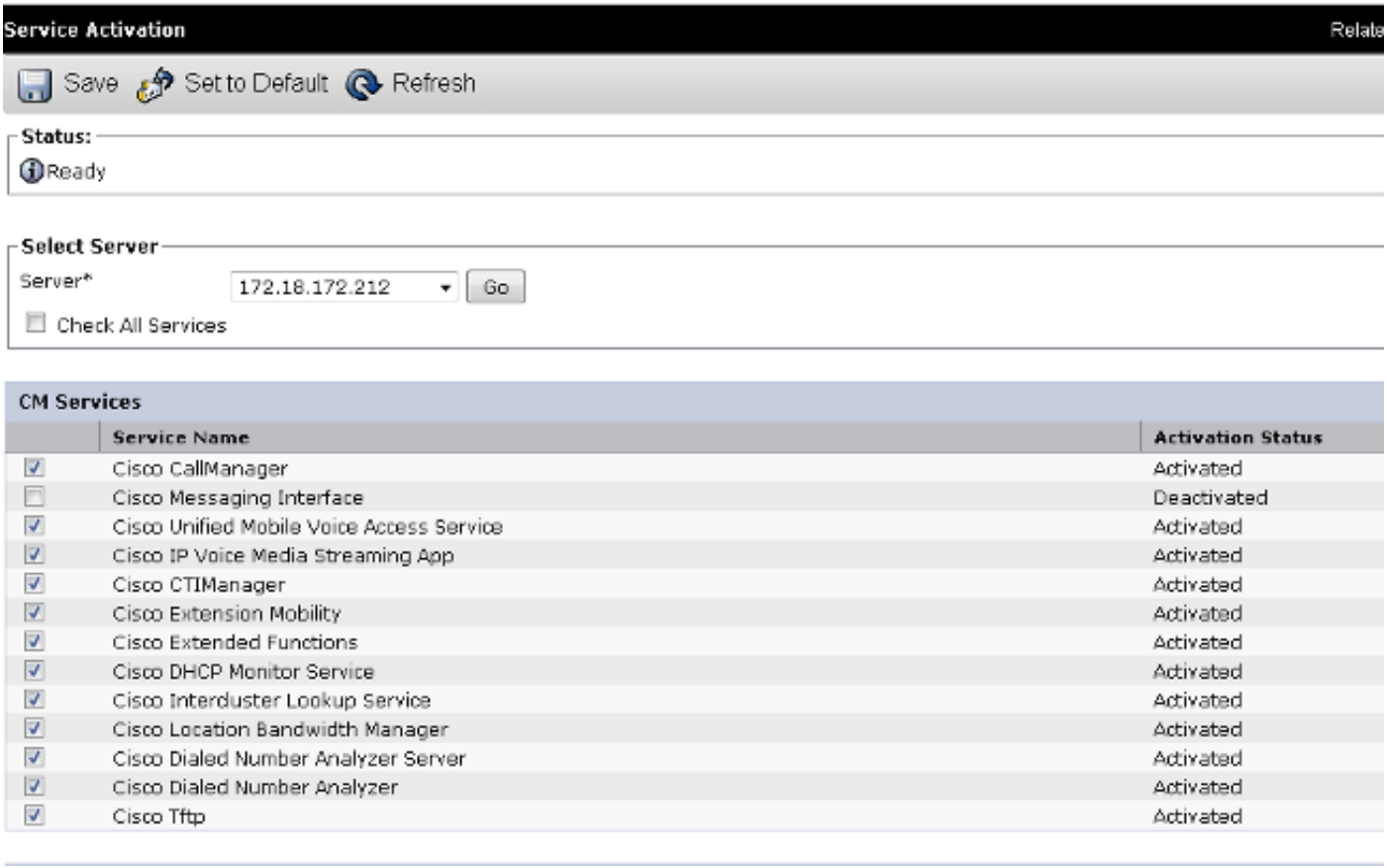
If replication continues to fail, refer to the Troubleshooting CUCM Database Replication in Linux Appliance Model Cisco article for more information about how to troubleshoot the issue.

Post Restore

Since the DB restoration does not restore all of the previous components, many server-level items must be manually installed or restored.

Activate Services

The DRF restoration does not activate any services. Navigate to **Tools > Service Activation**, and activate any necessary services that the publisher must run, based on the site documentation from the Unified Serviceability page:



Install Data that was not Restored

If a full backup was not available, you must reproduce certain manual configurations. Particularly, those configurations that involve certificates and TFTP functions:

- MoH files
- Device packs
- Dial plans (for non-North American Numbering Plan (NANP) dialing)
- Locales
- Any other miscellaneous COP files
- Any files that previously were manually uploaded to the publisher (if it was a TFTP server)
- Simple Network Management Protocol (SNMP) community strings
- Bulk certificate exports for Extension Mobility Cross Cluster (EMCC), Intercluster Location Bandwidth Manager (LBM), and Intercluster Lookup Service (ILS)
- Certificate exchanges for secure trunks, gateways, and conference bridges

Note: For mixed-mode clusters, you must run the Certificate Trust List (CTL) client again.

Troubleshoot

This section describes various scenarios that can cause this procedure to fail.

Cluster does not Authenticate

If the cluster does not authenticate, the two most common causes are mismatched security passphrases and connectivity issues on TCP port 8500.

In order to verify that the cluster security passphrases match, enter the **utils create report platform** command at the CLI of both nodes, and inspect the hash value from the **platformConfig.xml** file. These must match on the publisher and subscriber nodes.

```
<#root>

  <IPSecSecurityPwCrypt>
    <ParamNameText>Security PW for this node</ParamNameText>
    <ParamDefaultValue>password</ParamDefaultValue><ParamValue>

0F989713763893AC831812812AB2825C8318
    12812AB2825C831812812AB2825C

 </ParamValue>
  </IPSecSecurityPwCrypt>
```

If these match, verify the TCP connectivity on port 8500. If they do not match, there can be difficulties when you attempt to fix the passphrase due to several defects in the CUCM code that surround the procedure:

- Cisco bug ID CSCtn79868 - pwrecovery tool resetting only sftpuser password
- Cisco bug ID CSCug92142 - pwrecovery tool does not update the internal user passwords
- Cisco bug ID CSCug97360 - selinux denials in pwrecovery utility
- Cisco bug ID CSCts10778 - Denials thrown for security Password Recovery procedure
- Cisco bug ID CSCua09290 - CLI "set password user security" did not set the correct apps password
- Cisco bug ID CSCtx45528 - pwd reset cli returns good but does not change password
- Cisco bug ID CSCup30002 - DB service is down, after changing the security password on CUCM 10.5
- Cisco bug ID CSCus13276 - CUCM 10.5.2 security password recovery causes DB to not start at reboot

If the CUCM version contains fixes for all of these issues, the easiest solution is to complete the password recovery procedure detailed in Cisco Unified Communications Operating System Administration Guide, Release 10.0(1) on all nodes.

If the CUCM version does not contain the fixes for these issues, then the Cisco Technical Assistance Center (TAC) can have the ability to perform a workaround, dependent upon the situation.

Restoration does not Process CCMDB Component

If the restoration does not list the DB component, then it is possible that the backup itself does not contain a DB component. Ensure that the publisher DB runs and can accept queries, and perform a new backup.

Replication Failure

Refer to the Troubleshooting CUCM Database Replication in Linux Appliance Model Cisco article in order to troubleshoot a replication failure.

Phones do not Register or are Unable to Access Services

Since the DB restoration does not restore any certificates, if the publisher is the primary TFTP server, the signer is different.

If the phones trust subscriber Trust Verification Service (TVS) certificates, and TCP port 2445 is open between the phones and the TVS servers, the issue must be resolved automatically.

For this reason, Cisco recommends that you maintain full cluster DRF backups.

CUCM versions prior to Version 8.6 can also have certificate issues, even with a previous successful backup, due to Cisco bug ID CSCtn50405.

Note: Refer to the Communications Manager Security By Default and ITL Operation and Troubleshooting Cisco article for additional information about how to troubleshoot Initial Trust List (ITL) files.
