APPENDIX 3

Setting Up Geographical Disaster Recovery

Revised: April 29 2018

Introduction

There may be times where Prime Central or the Cisco Prime applications integrated with Prime Central go down. To help minimize the amount of downtime for these applications, you can implement geographical disaster recovery in your network. Let's begin with an overview of the geographical disaster recovery process and a definition of three of its key components.

After completing the procedures detailed later in this section, Prime Central and integrated Cisco Prime applications reside on both a primary and standby server. When one or more of these applications go down on the primary server, you receive a system-generated email notifying you of the problem. To deal with the problem, you would first initiate switchover to the standby server. *Switchover* is the manual switch from one server to a redundant or standby server. By initiating a switchover, you can continue to manage and monitor your network while you figure out what's wrong with the primary server. You can also initiate switchover if you need to perform routine maintenance on the primary server, such as upgrading hardware or installing patches. If you resolve the problem, you switch back to the primary server and that's that. However, if all of your attempts to bring the primary server back into a working state fail and it has become completely unreachable, you would then initiate failover. *Failover* is essentially the same operation as switchover, the difference being that failover indicates a major problem with the primary server that will require some time to resolve. By initiating failover, the standby server effectively becomes the new primary server and takes over all network management and monitoring tasks. Before you initiate failover for a server, make sure that you've done everything possible to bring that server back into operation because switching to the standby server could bring about other problems. Finally, when the server previously acting as the primary server is up and running again, you would then initiate *failback*, which is the process that reinstates that server as the primary server.

In this section, the following topics are covered:

- How to prepare your network for geographical disaster recovery
- How to configure monitoring frequency and email notifications
- How to initiate switchover, failover, and failback
- How to integrate Cisco Prime applications with the standby server
- Best practices for geographical disaster recovery implementation, as well as troubleshooting information

Preparing Your Network for Geographical Disaster Recovery

To prepare your network for geographical disaster recovery, you will need to configure the following:

- Prime Central
- Prime Central Fault Management
- Application and database replication monitors, which keep tabs on the:
  - Prime Central portal
  - Integration layer
  - The current status of the database
  - Database replication between the primary and standby nodes

Typically, the Prime Central portal, integration layer, and database are located on the same server. You can also choose to place these components on multiple servers. If you want the integration layer to reside on its own server, you will need to complete the following procedures twice—once on the portal server and once on the integration layer server.

Note

- If your environment contains multiple integration layer servers, you will need to complete these procedures for each of those servers.
- Prime Central and Prime Central Fault Management patch need to be applied on both Primary and standby machines separately. Once the patch is applied on primary, *switchover* and then apply the patch on the new Primary machine.

Configuring Prime Central for Geographical Disaster Recovery

You can configure Prime Central for Geographical disaster recovery in a Primary and standby server setup.

Step 1 Install Prime Central 2.0 onto the server that will act as the primary server.

During installation, in the Embedded DB Information window, make sure that:

- You select the Enable backups on the database check box.
- You specify the desired archive log location. By default, the archive log location is set to /export/home/oracle/arch.

It is critical that you enable backups on the Oracle database. Geographical disaster recovery setup will fail unless you do so.

See "Installing Prime Central" in the *Cisco Prime Central 2.0 Quick Start Guide* for detailed installation instructions.

Step 2 Set up Prime Central for geographical disaster recovery on the server that will act as the standby server.

a. Copy and unzip disaster_recovery_v2.0.zip into a folder on the standby server.

In this example, we will use the /root/disaster_recovery folder. When setting up geographical disaster recovery in your environment, overwrite this folder with the correct one.

b. Ensure that the Prime Central database and installer binaries reside in the /root/disaster_recovery/scripts/main/installer folder. Specifically, ensure that these files are present:

- linuxamd64_12102_database_1of2.zip
- linuxamd64_12102_database_2of2.zip
- primecentral_v2.0.bin

c. Ensure that the primary server is reachable via SSH by the following means:

- IP address
- Hostname (without domain name, if applicable)
- Hostname with domain name (FQDN)

d. Navigate to the disaster recovery distribution package folder:

```
# cd /root/disaster_recovery
```

e. Enter the following commands to run the setup script:

```
# cd scripts/main
# chmod +x pc_standby_setup.sh
# ./pc_standby_setup.sh
```

f. When prompted by the setup script, enter the necessary information for the primary (active) and standby server (such as IP address, hostname and root password).

Note In the *hostname* prompt, enter the FQDN. The host name of the primary server should exactly be same as the one that was used when Prime Central was being installed in it.

g. After Prime Central has been set up on the standby server, complete the following tasks:

- As the user *primeusr*, generate a Secure Shell (SSH) key for the primeusr user on both the primary and standby servers by entering the following commands:

```
# chmod 755 ~
# /usr/bin/ssh-keygen -t rsa -N "" -b 2047 -f ~/.ssh/id_rsa
# chmod 600 ~/.ssh/id_rsa
```

- (On the primary server only) Share the primary server's public key with the standby server so that the dynamic creation of a SSH between the servers does not prompt for a password.

  As the user *primeusr*, enter the following commands:

```
# rsync -av ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
# /usr/bin/ssh primeusr@standby-server-hostname "cat ~/.ssh/id_rsa.pub" >>
~/.ssh/authorized_keys
# rsync -av ~/.ssh/authorized_keys primeusr@standby-server-hostname:~/.ssh/
```

- (On the Standby server only) Enter the following command:

```
# rsync -av ~/.ssh/authorized_keys primeusr@primary-server-hostname:~/.ssh/
```

  where standby-server-hostname is the hostname of the standby server.

- Verify that the SSH is working and does not prompt for authentication or a password (using the FQDN hostname, non-FQDN hostname, and IP address) on both the primary and standby server.
- If you are prompted to continue connecting, enter **yes**. (The prompt should appear only the first time you use SSH to connect to the node.)

h. Integrate the relevant Cisco Prime applications, such as Prime Network and Prime Optical, with the standby server. Refer to the Integrating Applications with the Standby Server, page 3-11 for instructions.

Note Prime Central services such as, **portalctl** and **itgctl** should be running on standby server during Domain Manager integration.

Configuring Prime Central Fault Management for Geographical Disaster Recovery

You can choose to not set up Fault Management for geographical disaster recovery at this time. However, keep in mind that you may not be able to do so later.

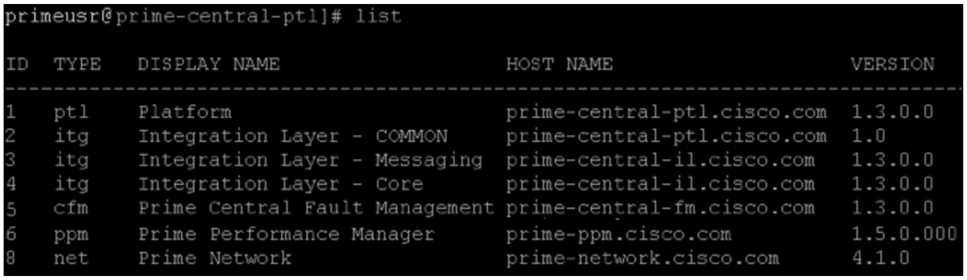
Step 1 If Fault Management and Prime Central are being installed on the same machine, open /opt/primecentral/local/disaster_recovery/rsync/fm/includeSync.txt file on the primary server and comment all the lines in it. After the installation is complete, uncomment these lines.

Note The Prime Central and Fault Management installation in the Discover Recovery (DR) site may fail if step 1 is not followed because, some files in the folder "install-directory/faultmgmt" might get synced between Primary and Standby servers. For Best Practices and troubleshooting the Prime Central Installation, see Geographical Disaster Recovery Implementation: Best Practices and Troubleshooting Information.

Step 2 Install Fault Management on the Fault Management primary server.

See "Installing Prime Central Fault Management" in the *Cisco Prime Central 2.0 Quick Start Guide* for detailed instructions.

Step 3 SSH to the primary Prime Central server as the user *primeusr* and run the **list** command to determine Fault Management's instance ID value (in this example, 5).



```
primeusr@prime-central-ptl]# list

ID  TYPE   DISPLAY NAME                    HOST NAME                     VERSION
--------------------------------------------------------------------------------
1   ptl    Platform                        prime-central-ptl.cisco.com  1.3.0.0
2   itg    Integration Layer - COMMON      prime-central-ptl.cisco.com  1.0
3   itg    Integration Layer - Messaging   prime-central-il.cisco.com   1.3.0.0
4   itg    Integration Layer - Core        prime-central-il.cisco.com   1.3.0.0
5   cfm    Prime Central Fault Management prime-central-fm.cisco.com   1.3.0.0
6   ppm    Prime Performance Manager       prime-ppm.cisco.com          1.5.0.000
8   net    Prime Network                   prime-network.cisco.com      4.1.0
```

362780

You will need this for Step 4f.

Step 4 On the standby Prime Central server, verify that the portal and integration layer are up and running.

Step 5 Set up geographical disaster recovery for Fault Management on the standby server.

a. Copy and unzip the distribution package zip file into the /root/disaster_recovery folder.

b. Copy FM2.0.0Build.tar.gz to the /root/disaster_recovery/scripts/main/installer folder.

c. Untar FM2.0.0Build.tar.gz:

```
# tar -zxf FM12.0.0 Build.tar.gz
# cd Disk1/InstData/VM
# chmod 755 primefm_v2.0.bin
```

d. Ensure that the Fault Management binary (primefm_v2.0.bin) resides in the /root/disaster_recovery/scripts/main/installer/Disk1/InstData/VM folder.

e. Enter the following commands to run the setup script:

```
# cd /root/disaster_recovery/scripts/main
# chmod +x fm_standby_setup.sh
```

f. Verify that the Fault Management component on both the primary and standby server, as well as the primary and standby Prime Central server, can be reached using their hostname.

g. Enter the following command:

- For regular standby installation:

```
# ./fm_standby_setup.sh
```

- For failback scenario:

```
# ./fm_standby_setup.sh  -g  failback_install
```

h. When prompted by the setup script, enter the necessary information for the primary and standby server (such as IP address and root password).

Note In the *hostname* prompt, enter the FQDN. The host name of the primary server should exactly be same as the one that was used when Prime Central was being installed in it.
When prompted for Prime Central database details, ensure to specify the standby database IP address.

2. After Fault Management has been set up on the standby server, complete the following tasks:

- As the user *primeusr*, generate a Secure Shell (SSH) key for the primeusr user on both the primary and standby servers by entering the following commands:

```
# chmod 755 ~
# /usr/bin/ssh-keygen -t rsa -N "" -b 2047 -f ~/.ssh/id_rsa
# chmod 600 ~/.ssh/id_rsa
```

- (On the primary server only) Share the primary server's public key with the standby server so that the dynamic creation of a SSH between the servers does not prompt for a password.

  As the user *primeusr*, enter the following commands:

```
# rsync -av ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
# /usr/bin/ssh primeusr@standby-server-hostname "cat ~/.ssh/id_rsa.pub" >>
~/.ssh/authorized_keys
# rsync -av ~/.ssh/authorized_keys primeusr@standby-server-hostname:~/.ssh/
```

- (On the Standby server only) Enter the following command:

```
# rsync -av ~/.ssh/authorized_keys primeusr@primary-server-hostname:~/.ssh/
```

  where *standby-server-hostname* is the hostname of the standby server.

- Verify that the SSH is working and does not prompt for authentication or a password (using both the hostname and IP address).

- If you are prompted to continue connecting, enter `yes`. (The prompt should appear only the first time you use SSH to connect to the server).

- Make sure all the lines in /opt/primecentral/local/disaster_recovery/rsync/fm/includeSync.txt file, on the primary server, are uncommented (which were commented during Step 1).

i. Configure Fault Management to send 3GPP alarm notifications to Northbound Interface for both primary and standby server:

```
fmctl configimpact <centraladmin pwd>
```

For example:

```
fmctl configimpact Prime123
```

j. Restart the Prime Central Fault Management:

```
fmctl restart
```

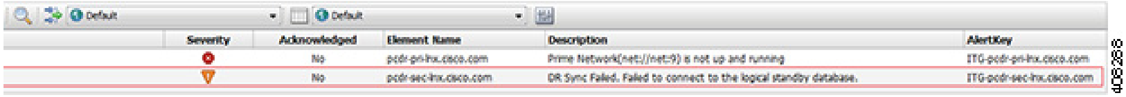
Note If centraladmin user’s password is changed, run **Step j** with the new password.

Fault Management for Disaster Recovery Synchronization Failure

This feature helps the user to get an alarm/notification if sync fails between the primary and the standby node.

If database synchronization fails, an alarm is sent to the user notifying the database sync failure along with the possible reason for failure. See Figure 3-1.

Figure 3-1 Database Synchronization Failure Alarm



	Severity	Acknowledged	Element Name	Description	AlertKey
	●	No	pcdr-pri-lnx.cisco.com	Prime Network(net://net:9) is not up and running	ITG-pcdr-pri-lnx.cisco.com
	▼	No	pcdr-sec-lnx.cisco.com	DR Sync Failed. Failed to connect to the logical standby database.	ITG-pcdr-sec-lnx.cisco.com

If file synchronization fails, an alarm is sent to the user notifying the same.

Below is the list of alarms supported for Disaster Recovery Sync Failure:

Table 3-1 List of Sync Fail Alarms

Event ID	Description	Service
PC-DR-FILE-SYNC-FAILURE	DR Sync Failed. File Sync failure.	Disaster Recovery
PC-STANDBY-CONNECT-FAILURE	DR Sync Failed. Failed to connect to the logical standby database.	Disaster Recovery
PC-DB-NOT-A-LOGICAL-STANDBY	DR Sync Failed. Database is not a logical standby.	Disaster Recovery
PC-SQL-APPLY-IS-NOT-RUNNING	DR Sync Failed. SQL Apply is not running.	Disaster Recovery

Table 3-1 List of Sync Fail Alarms (continued)

Event ID	Description	Service
PC-SQL-REALTIME-NOT-ON-FOR-STANDBY	DR Sync Failed. SQL Real time is not on for the logical standby.	Disaster Recovery
PC-LAG-IN-STANDBY-DB	DR Sync Failed. There is a lag in the logical standby database.	Disaster Recovery

Note File Sync and DB Sync alarms are ADMC (Automatic Delivery Manual Clear).

Configuring Monitoring Frequency and Email Notifications

Even though the values you configure while completing this procedure are automatically synchronized between the primary and standby servers, we recommend that you verify this has taken place. Note that the first time you initiate file synchronization, it can take 5 to 10 minutes for the process to start.

Step 1 Configure the monitoring frequency value.

By default, this value is set to 5 minutes for application, file synchronization, and data replication monitoring. If you want to keep this as is, proceed to Step 2. If you want to set another value, do the following:

a. Log into the primary server as the root user.

b. Enter the following commands:

```
# cd primeusr-home-directory/local/scripts/
# appmonctl stop
# dbmonctl stop
```

c. Open *primeusr-home-directory*/local/cron/app_mon/conf/frequency_conf and set the desired monitoring frequency value (in minutes) for the following parameters:

- FREQUENCY (application)
- RSYNC_FREQUENCY (file synchronization)
- DBMON_FREQUENCY (data replication)

d. Enter the following commands:

```
# cd primeusr-home-directory/local/scripts/
# appmonctl start
# dbmonctl start
```

Step 2 Open *primeusr-home-directory*/local/disaster_recovery/scripts/cron/app_mon/conf/email_config and specify the users that will be notified via email whenever an event occurs, as well as the email address from which these messages will be sent.

A sample email_config file looks like this:

`EMAIL_IDS=email_id1@example.com email_id2@example.com` (recipients of application monitoring messages)

`DB_ EMAIL_IDS=email_id1@example.com email_id2@example.com` (recipients of database monitoring messages)

`SENDER_EMAIL=source@example.com` (sender of application monitoring messages)

`DB_SENDER_EMAIL=source@example.com` (sender of database monitoring messages)

Note the following:

- The Application Monitor uses the sendmail email client. Verify that sendmail has been properly configured to send notification emails.
- Ensure that each recipient's email address is separated by a space.
- You can specify an email alias, provided that it is a valid email address.
- Only one sender email address can be configured at any given time.
- After setup, check your email client's junk folder for any failover-related messages. If necessary, set similar messages as being safe to read.
- If the primary server, standby server, or VM belongs to a lab where DNS configuration is not available, open /etc/hosts and add the following entry:

  server-or-VM-IP-address domain-name
- If new customized rules file or impact policy is added, the operator should add the entry in *primeusr-home-directory*/local/disaster_recovery/rsync/fm/include.txt.

Checking the Status of Disaster Recovery Node

To check the status of the disaster recovery node, follow the below steps.

Step 1 As the root user, log into the Primary server.

Step 2 Enter the following commands:

```
# cd primeusr-home-directory/local/disaster_recovery/scripts/main
# ./primedr status (for Prime Central)
[root@server main]# ./primedr status

Please wait, fetching status...
HostIP                    NodeStatus            OperationStatus
------------              ------------          ------------
10.76.81.67               Standby                   Inactive
10.76.81.66               Primary                   Active

# ./fmdr status (for Fault Management)
[root@server main]# ./fmdr status

Please wait, fetching status...
HostIP                    NodeStatus             OperationStatus
-------------          -------------          -------------
10.76.81.67               Standby                   Inactive
10.76.81.66               Primary                   Active
```

Note By default, the primeusr home directory is /opt/primecentral. You can specify another directory, if necessary.

Initiating Switchover

To initiate the Switchover process for Prime Central and Fault Management servers, follow the below steps.

Step 1 As the root user, log into the standby server.

Step 2 Enter the following commands:

```
# cd primeusr-home-directory/local/disaster_recovery/scripts/main
# ./primedr switch (for Prime Central)
# ./fmdr switch (for Fault Management)
```

Note By default, the primeusr home directory is /opt/primecentral. You can specify another directory, if necessary.

Note To make crosslaunch work on upgrade setup, de-register and register the Prime Network after Prime Central and Prime Network switchover.

Initiating Failover

To initiate the Failover process for Prime Central and Fault Management servers, follow the below steps.

Step 1 As the root user, log into the standby server.

Step 2 Enter the following commands:

```
# cd primeusr-home-directory/local/disaster_recovery/scripts/main
# ./primedr fail (for Prime Central)
# ./fmdr fail (for Fault Management)
```

Note By default, the primeusr home directory is /opt/primecentral. You can specify another directory, if necessary. Also, External Oracle Database configuration is supported only in standalone configuration and this External Oracle Database configuration is not supported with Prime Central DR configuration.

Note After failover, if "DR sync failed. Database is not a logical standy" alarm appears in the alarm browser, ignore it and clear the alarm manually.

Initiating Failback

When a server that was previously brought into failover is operational again, and all of the geographical disaster recovery installation data present before the server failed (which includes the entire database and all of the files in the primeusr home directory) has been fully restored, it is ready for failback. Complete the following procedure on that server to reinstate it as the primary server.

Step 1 If the server's data is totally erased, you first need to complete the procedure described in Configuring Prime Central for Geographical Disaster Recovery, page 3-2 and Configuring Prime Central Fault Management for Geographical Disaster Recovery, page 3-4. For Prime Central, after you enter **./pc_standby_setup.sh** command, the installer detects that you are reinstalling Prime Central on the server you are reinstating as the primary server. When prompted, enter Y to proceed with the installation.

Step 2 As the root user, log into the server you want to reinstate as the primary server.

Step 3 Enter the following commands:

```
# cd primeusr-home-directory/local/disaster_recovery/scripts/main
# ./primedr failback (for Prime Central)
# ./fmdr failback (for Fault Management)
```

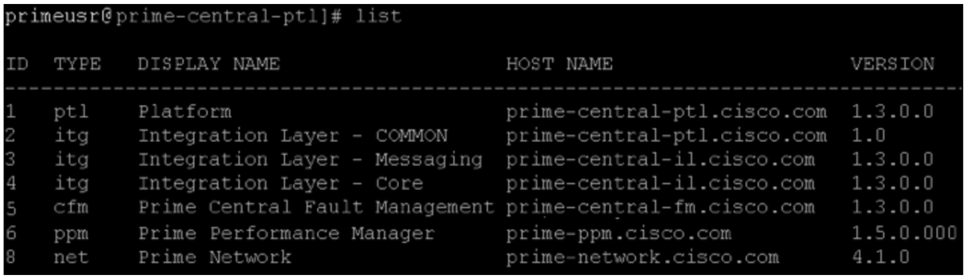
Note After failback, if Domain Manager is down in suite-monitoring or if cross-launch fails, de-register and register the respective Domain Manager.

Integrating Applications with the Standby Server

Complete the following procedure to integrate applications such as Prime Network and Prime Optical with the standby server.

Step 1 Determine the instance ID of the application on the primary server you want to integrate. To do so, run the **list** command as the user *primeusr*.

Say you want to integrate Prime Network. In the following example, Prime Network's instance ID value is 8.



```
primeusr@prime-central-ptl]# list

ID  TYPE   DISPLAY NAME                   HOST NAME                   VERSION
------------------------------------------------------------------------------------------
1   ptl    Platform                       prime-central-ptl.cisco.com 1.3.0.0
2   itg    Integration Layer - COMMON     prime-central-ptl.cisco.com 1.0
3   itg    Integration Layer - Messaging  prime-central-il.cisco.com  1.3.0.0
4   itg    Integration Layer - Core       prime-central-il.cisco.com  1.3.0.0
5   cfm    Prime Central Fault Management prime-central-fm.cisco.com  1.3.0.0
6   ppm    Prime Performance Manager      prime-ppm.cisco.com         1.5.0.000
8   net    Prime Network                  prime-network.cisco.com     4.1.0
```

362780

Step 2 Enter one of the following commands, depending on whether you want to specify the necessary values when prompted by the script (in Interactive mode) or all at once (in Non-interactive mode):

- Interactive mode:

  `# ` **`% ./DMIntegrator.sh –r DMIntegrator.prop`**

- Non-interactive mode:

  `# ` **`% ./DMIntegrator.sh -d DMIntegrator.prop`** *server db-service-name db-user db-password port dm_id*

  where:

  – *server* is the IP address of the standby Prime Central database server

  – *db-service-name* is the standby Prime Central database service name (for an embedded Oracle database, the default is primedb)

  – *db-user* is the username of the standby Prime Central database user

  – *db-password* is the password of the standby Prime Central database user

  – *port* is the port number of the standby Prime Central database port

  – *dm_id* is the instance ID value you obtained in Step 1.

Upgrading to Prime Central 2.0 and Prime Central Fault Management 2.0 in a Geographical Disaster Recovery

Step 1 Stop application monitoring, data replication monitoring and file synchronization on Primary Server.

a. Log into the primary server as the root user.

b. Enter the following commands:

```
# cd primeusr-home-directory/local/scripts/
# appmonctl stop
# dbmonctl stop
```

c. Log into the primary server as the user primeusr.

d. Enter the following command:

```
# filesyncctl stop
```

Note As part of Prime Central release 2.0, direct upgrade from 1.4.1 to 2.0.0, 1.5 to 2.0.0 and 1.5.3 to 2.0.0 are supported.

Step 2 If you are performing direct upgrade of Prime Central or Prime Central Fault Management from 1.5.3,or 1.4.1, or 1.5 to 2.0.0, follow the below direct upgrade steps mentioned in the Table 3-2

Table 3-2 Direct Upgrade Steps

Direct Upgrade Process	From Prime Central 1.5.3 to 2.0	From Prime Central 1.5 to 2.0	From Prime Central 1.4.1 to 2.0	Refer to
Upgrading from 1.5.3 to 2.0				
Step 1: Uninstall Prime Central Fault Management 1.5.3 from standby server	Yes	X	X	*Cisco Prime Central 1.5.3 Quick Start Guide* for uninstalling process.
Step 2: Uninstall Prime Central 1.5.3 from standby server	Yes	X	X	*Cisco Prime Central 1.5.3 Quick Start Guide* for uninstalling process.
Step 3: Upgrade Prime Central 1.5.3 to Prime Central 2.0 on primary server	Yes	X	X	*Cisco Prime Central 2.0 Quick Start Guide* for upgrading process.
Step 4: Upgrade Prime Central Fault Management 1.5.3 to Prime Central Fault Management 2.0 on primary server	Yes	X	X	*Cisco Prime Central 2.0 Quick Start Guide* for upgrading process.
Upgrading from 1.5 to 2.0				

Direct Upgrade Process	From Prime Central 1.5.3 to 2.0	From Prime Central 1.5 to 2.0	From Prime Central 1.4.1 to 2.0	Refer to
Step 1: Uninstall Prime Central Fault Management 1.5 from standby server	X	Yes	X	*Cisco Prime Central 1.5 Quick Start Guide* for uninstalling process.
Step 2: Uninstall Prime Central 1.5 from standby server	X	Yes	X	*Cisco Prime Central 1.5 Quick Start Guide* for uninstalling process.
Step 3: Upgrade Prime Central 1.5 to Prime Central 2.0 on primary server.	X	Yes	X	*Cisco Prime Central 2.0 Quick Start Guide* for upgrading process.
Step 4: Upgrade Prime Central Fault Management 1.5 to Prime Central Fault Management 2.0 on primary server. Refer to	X	Yes	X	*Cisco Prime Central 2.0 Quick Start Guide* for upgrading process.
Upgrading from 1.4.1 to 2.0				
Step 1: Uninstall Prime Central Fault Management 1.4.1 from standby server	X	X	Yes	*Cisco Prime Central 1.4.1 Quick Start Guide* for uninstalling process.
Step 2: Uninstall Prime Central 1.4.1 from standby server	X	X	Yes	*Cisco Prime Central 1.4.1 Quick Start Guide* for uninstalling process.
Step 3: Upgrade Prime Central 1.4.1 to Prime Central 2.0 on primary server.	X	X	Yes	*Cisco Prime Central 1.4.1 Quick Start Guide* for upgrading process.
Step 4: Upgrade Prime Central Fault Management 1.4.1 to Prime Central Fault Management 2.0 on primary server. Refer to	X	X	Yes	*Cisco Prime Central 1.4.1 Quick Start Guide* for upgrading process.

Step 3 Perform Disaster Recovery setup of Prime Central 2.0 on standby server. Refer to Configuring Prime Central for Geographical Disaster Recovery, page 3-2 for setup instructions.

Step 4 Perform Disaster Recovery setup of Prime Central Fault Management 2.0 on standby server. Refer to section Configuring Prime Central Fault Management for Geographical Disaster Recovery, page 3-4 for setup instructions.

Upgrading RHEL Operating System

The Operating System (OS) upgrade procedure supports Prime Central 1.5.1 customers to perform upgrade of Operating System from RHEL 5.8 to 6.5 and inline upgrade from RHEL 6.5 to 6.7. For more information, refer the Cisco Prime Central RHEL Operating System Upgrade guide.

Geographical Disaster Recovery Implementation: Best Practices and Troubleshooting Information

Log file locations:

- During geographical disaster recovery setup, refer to the log files located in the logs folder (which resides in the same folder as the setup scripts).
- While geographical disaster recovery is taking place, refer to the logs here: *primeusr-home-directory*/local/disaster_recovery/logs

Problem Prerequisites check failed.

Solution Make sure the server meets all required specifications in terms of:

- Hard disk space
- RAM and swap space
- RHEL versions

Problem Environment setup failed.

Solution Do the following:

- Make sure you run the script as the root user.
- Verify whether the Expect Unix tool is installed. If not, check the log files in the logs folder for any errors that occurred.

Problem Oracle database standby setup failed.

Solution Make sure that database backups and archive logs are enabled on the primary server.

1. Log into the primary server as the user *primeusr*.
2. Enter the following command:

```
# emdbctl -enable_backup
```

If any errors occur, please refer to the *Cisco Prime Central 2.0 Quick Start Guide* for more troubleshooting information.

If backups are already enabled but the Oracle database standby setup failed:

1. Log into the database server as the user oracle.
2. Enter the following command:

```
# cd ~/standby/logs
```

3. Check the log file named PCoracleADG.ksh_*.log for any errors, where * refers to the latest available log file.
4. Once the errors have been identified and resolved, clean up the server and run the geographical disaster recovery setup process again.

Problem Application Monitor always reports that the File Sync operation failed.

Solution Make sure that trust has been established between the primary and standby servers for the user primeusr. If you need to establish trust, perform the tasks described in Step 2g of Configuring Prime Central for Geographical Disaster Recovery, page 3-2.

Problem Prime Central and Fault Management failback reports that the File Sync operation failed.

Solution Make sure that trust has been established between the primary and standby servers for the user primeusr. If you need to establish trust, perform the tasks described in Step 2g of Configuring Prime Central for Geographical Disaster Recovery, page 3-2.

Problem Prime Central installation on the standby server failed.

Solution Verify that:

- The standby server meets all prerequisites.
- You entered the right passwords when prompted by the installer.
- The server is configured for DNS configured or the /etc/hosts file has the right information.

Refer to the *Cisco Prime Central 2.0 Quick Start Guide* for installation troubleshooting information.

Problem Application integration on the standby server failed.

Solution Make sure that the application's ID value specified during the integration process is valid. To check, perform the steps described in application's integration guide.

Problem Rsync failed.

Solution Make sure that both the primary and standby nodes can communicate via SSH without authentication (the process is described in Step 2g of Configuring Prime Central for Geographical Disaster Recovery, page 3-2). To view more details on the Rsync failure, navigate to *primeusr-home-directory*/local/disaster_recovery/logs and open app_mon.log.

Problem Information for the integration layer is not found in the standby database.

Solution Run the following commands:

```
# cd /root/disaster_recovery/scripts/main/
# ./install_esb_dr.sh
```

Problem Oracle database restore fails on Standby (Inactive) server after performing database restore on Primary (Active) server.

Solution Run the following commands as root user on the Standby (Inactive) server:

```
# cd primeusr-home-directory/local/disaster_recovery/scripts/main/
# ./recreatestandbyADG.sh
```

Problem Prime Central and Fault Management installation in the Discover Recovery (DR) site failed with the following error log found in "install-directory/IBM_Tivoli_Netcool_OMNIbus_Web_GUI_Install-00.log"

```
2016-04-22 08:23:52.343-04:00 :  SEVERE : The specified installation directory for the
Tivoli Integrated Portal is not empty:
/opt/primecentral/faultmgmt/tipv2
Either remove all items from the directory or choose another installation directory.
from com.ibm.tivoli.tip.install.common.ia.CheckIfPreviousInstallLeftBehindFiles.
validateInstallDirs)
```

Solution Perform the following steps:

1. On the Primary server, comment out all the lines in the file:

```
install-directory/ local/disaster_recovery/rsync/fm/includeSync.txt on the Primary
server
```

2. On the Standby server, check if there is any left behind fault management process even after the un-installation, by using the below command:

   ```
   ps -ef | grep faultmgmt
   ```

   Kill the process if any, by using the below command:

   ```
       kill -9  <process-id>
   ```

3. Delete the faultmgmt folder.

   ```
   rm -rf  install-directory/faultmgmt
   ```

Problem After initiating either switchover, failover, or failback, PC alarms from the current inactive server are present in the current active server.

Solution Ignore and manually clear the PC alarms.

Note This solution is applicable only for alarms raised by PrimeCentral (ex:Csv file download failure alarms or DM down alarms) and not for the alarms coming from Domain Manager.

Problem How to avoid netcool imapct hang?

Solution Increase the heap size of netcool impact to better its performance in production environment. To increase the heap size follow the below steps:

1. Enable debug logs in netcool impact
   a. Set the PolicyLogger for problem determination:
   - Launch Impact GUI interface (http://FMHOST:9080/nci/main)
   - Select the PolicyLogger under Service Status

   Configure the following options and Save:
   - Highest Log Level = 3
   - Check under Log What:

     All SQL statements

     Pre-execution Action Module Parameters

     Post-execution Action Module Parameters

     All Action Module Parameters
   - Check policy Profiling enabled

     and
   - Check under Service Log:

     Write to file

     Append Policy Name to log file

   b. Edit the $NCHOME/eWAS/properties/log4j.properties file:

   log4j.appender.NETCOOL.threshold=DEBUG

   log4j.category.com.micromuse=DEBUG,NETCOOL,NETCOOL-ERRORS

   log4j.appender.NETCOOL.maxBackupIndex=10

   log4j.appender.NETCOOL.maxFileSize=20MB

2. To increase the heap size, follow the steps specified below:
   a. Run the server:
   ```
   wsadmin.sh -conntype SOAP -lang jython -username wasadmin -password netcool
   ```
   b. (optional) If the server is not running, use the following:
   ```
   wsadmin.sh -conntype none -lang jython
   ```
   c. Enter the following commands at the comnad prompt (wsadmin>):
   - wsadmin>jvm=AdminConfig.list("JavaVirtualMachine").split("\r\n") [0]
   - wsadmin>AdminConfig.modify(jvm, '[[maximumHeapSize 3000]]')
   - wsadmin>attr=[]
   - wsadmin>attr.append([['name','Xmx'], ['value','3000']])
   - wsadmin>AdminConfig.modify(jvm, [['systemProperties',[]]])
   - wsadmin>AdminConfig.modify(jvm, [['systemProperties',attr]])
   - wsadmin>AdminConfig.save()
   - wsadmin>exit
3. Restart the impact either with fmctl stop/start impact or use the below commands after above steps:
   - cd $NCHOME/eWAS/profiles/ImpactProfile/bin
   - Stop eWas server
   - ./stopServer.sh server1 -username wasadmin -password netcool
   - Start eWas server
   - ./startServer.sh server1 -username wasadmin -password netcool
   -

Problem At the time of rebuilding the standby database on a HA environment, what script should be run to recover the Primary database (primedb)?

Solution 1: If you are rebuilding the standby database on HA2 when HA1 is active, use the following script:

sh PCoracleADG.ksh [PRIMARY] [STANDBY] [DB_TO_BE_DROPPED] [SYSTEM_PASSWD] [ORACLE_BASE]

[ORACLE_USER] [ARCHIVED_LOG_LOCATION] [ORACLE_DATA_FILES_LOCATION] [REDO_LOG_LOCATION]

PRIMARY = primedb

STANDBY = primstdb

DB_TO_BE_DROPPED = primstdb

SYSTEM_PASSWD = "grep Embedded_SYSTEM_PASS= install/conf/.db.conf"

Note: Use the command to decrypt password if encrypted:

java -cp install/utils/encryptionUtil.jar EncodeDecode decrypt 90f8006cd6bc0dde.

ORACLE_BASE = /orahome/oracle

ORACLE_USER = oracle

ARCHIVED_LOG_LOCATION = output of ‘show parameter log_archive_dest_1;&rsquo

ORACLE_DATA_FILES_LOCATION = output of ‘select name from v$datafile;&rsquo

REDO_LOG_LOCATION = output of ‘select member from v$logfile;’

Solution 2: If you are rebuilding the standby database on HA1 when HA2 is active, use the following script:

sh PCoracleADG.ksh [PRIMARY] [STANDBY] [DB_TO_BE_DROPPED] [SYSTEM_PASSWD] [ORACLE_BASE]

[ORACLE_USER] [ARCHIVED_LOG_LOCATION] [ORACLE_DATA_FILES_LOCATION] [REDO_LOG_LOCATION]

PRIMARY = primstdb

STANDBY = primedb

DB_TO_BE_DROPPED = primedb

SYSTEM_PASSWD = "grep Embedded_SYSTEM_PASS= install/conf/.db.conf"

Note: Use the command to decrypt password if encrypted:

java -cp install/utils/encryptionUtil.jar EncodeDecode decrypt 90f8006cd6bc0dde.

ORACLE_BASE = /orahome/oracle

ORACLE_USER = oracle

ARCHIVED_LOG_LOCATION = output of ‘show parameter log_archive_dest_1;&rsquo

ORACLE_DATA_FILES_LOCATION = output of ‘select name from v$datafile;&rsquo

REDO_LOG_LOCATION = output of ‘select member from v$logfile;’