Installing the Cisco Prime Optical High Availability Solution in a Local Redundancy Configuration on a Linux Server

This section contains the following topics:

For more information about local redundancy configuration on Linux, including hardware configuration and network diagrams; see Local Redundancy Configuration, page 1-1.

Local Redundancy Configuration Checklists

This section provides checklists to help with Prime Optical HA on Linux installation tasks. We recommend that you print the checklists from the PDF, which shows the section number where you will find each task, and either check off tasks as you complete them or enter information as needed.

This section contains the following information:

Preinstallation Checklist

Before you install the Prime Optical HA solution in a local redundancy configuration, complete the field in Table 4-1. The information will assist you in completing the installation.

Table 4-1 is the preinstallation checklist for a local redundancy configuration.

Table 4-1 Preinstallation Checklist for a Local Redundancy Configuration

Information	**Primary Cluster**	
Primary site name:		
Local cluster name:		
Local cluster number:		
Prime Optical Virtual IP address:		
	Primary Server	**Secondary Server**
Hostname:		
IP address:		
Public interface device 1:		
Public interface device 2:		
Private interface device 1:		
Private interface device 2:		

Note Private interface devices are dedicated to the heartbeat connection.

Local Redundancy Configuration Installation Checklist

To help you keep track of the steps in the installation process, print the checklist from the PDF, which shows the section number where you will find each task, and check the appropriate cells in Table 4-2 as you complete each step in the HA installation configuration process. In the cells where N/A is displayed, the step is not applicable for the primary and secondary server.

Table 4-2 is the local redundancy configuration checklist.

Table 4-2 Local Redundancy Configuration Checklist

	Description	**See...**	**Primary Server**	**Secondary Server**
New Installation				
1	Mount shared storage on primary server and configure virtual IP address	Setting the Environment for Installation, page 4-3	x	
2	Run server and database installation wizard.	Installing Prime Optical, page 4-7	x	
3	Install HA RPM files.	Installing the HA Package, page 4-12	x	

Table 4-2 Local Redundancy Configuration Checklist (continued)

	Description	See...	Primary Server	Secondary Server
4	Password less authentication is configured in both Primary server and Secondary servers.	Password Less Authentication Configuration, page 4-13	x	
5	Configure HA on Linux	• Editing the Agent Configuration File, page 4-15 • Editing the Logging Configuration File, page 4-16 • Editing the RHCS Configuration File, page 4-16	x	x **Note** Copy only the RHCS configuration file.
6	Start the cluster	• Starting the Cluster, page 4-19 • Starting RHCS Services, page 4-19 • Starting ctm_services on the Primary Server, page 4-20 • Verifying Cluster Status on the Standby Node, page 4-20	x	
7	Install Multicast Heartbeat Services	• Installing the Multicast Heartbeat Services Package, page 4-20 • Editing the multicastConfig.ini File, page 4-22 • Editing the logMulticast.ini File, page 4-22 • Starting the Multicast HeartBeat Services, page 4-23 • Configuring the MultiCast Heartbeat Services on the Secondary Server, page 4-23	x	x

Setting the Environment for Installation

In this procedure you will mount the shared disks between the primary and secondary servers and configure the shared virtual IP address that will be used during installation and runtime.

Step 1 On the primary server, mount the external disk that is shared between the primary and secondary servers to the appropriate mountpoints. See Table 2-4 and Table 2-5 for disk space and partition requirements.

For example:

```
mount /dev/sde /db01
mount /dev/sdf /db02
mount /dev/sdg /db03
mount /dev/sdh /db04
mount /dev/sdi /db05
mount /dev/sdj /ctm_backup
mount /dev/sdk /cisco
```

```
mount /dev/sdt /oracle
```

Note

- You can enter the **fdisk** command to view and confirm which disks are available and connected to the disk array: `fdisk -l`.
- Verify that /cisco, /oracle, /db01, /db02, /db03, /db04, /db05, and /ctm_backup are mounted correctly. Enter the **df -h** command to verify that the file systems are mounted on the primary server.

Step 2 Enter the following command to enable the virtual IP address that will be used during the HA solution runtime. This is the shared IP address mounted to an interface on the primary server.

```
ifconfig interface virtual-IP-address netmask netmask
```

For example:

```
ifconfig eth0:1 10.58.65.22 netmask 255.255.255.0
```

You can verify if the IP address was configured correctly by issuing the `ifconfig` command. The IP address for the interface should be displayed in the inet addr field.

Verifying Packages and yum setup

Verify that the following packages are installed on the primary and secondary servers:

The RHCS packages—Available on the Red Hat Enterprise Linux (RHEL) CD under the /cluster directory. See Installation Requirements for supported RHEL version.

The list of packages includes:

For RHEL-6.x:

- cman
- rgmanager
- openais
- modcluster
- ricci
- luci
- cluster-cim
- cluster-snmp
- system-config-cluster (only for RHEL 5.8)
- rgmanager-3.0.12.1-22.el6.x86_64

Step 1 Verify that the required packages are installed. Enter one of the following commands:

```
rpm -q pkg
```

or

```
yum info pkg
```

The output displays the package details. If a required package is not installed, an error will appear.

Step 2 Use the **yum** command to install the Linux package. The **yum** command checks all the dependencies from other packages. If you have an active connection to the Red Hat website, all dependent packages are automatically installed on the server. For more information, see the Red Hat website.

If you do not have an active connection to the Red Hat website, do the following:

a. Mount the RHEL DVD or ISO file. See Installation Requirements for supported RHEL version. For example:

For RHEL-6.x:

```
mount -o loop -t iso9660 /mnt/redhat/rhel-server-6.7-x86_64.iso /iso
```

where /mnt/redhat/rhel-server-6.7-x86_64.iso is the Red Hat ISO file.

b. Enter the following commands to get the media ID:

```
view /iso/.discinfo
cat /iso/.discinfo
```

Here is an example of the output:

```
1269263646.691048
Red Hat Enterprise Linux Server release 6.7 (Santiago)
x86_64
1,2,3,4,5,6
Server/base
Server/RPMS
Server/pixmaps
```

The media ID in the preceding example is 1269263646.691048.

c. Copy the proper local.repo file template from *DVD-mount-point*/Disk1 to /etc/yum.repos.d directory.

For RHEL 5.x installation, use the following command:

```
cp DVD-mount-point/Disk1/local.repo.5x /etc/yum.repos.d/local.repo
```

For RHEL 6.x installation, use the following command:

```
cp DVD-mount-point/Disk1/local.repo.6x /etc/yum.repos.d/local.repo
```

Open and follow the instructions in the local.repo file.

Step 3 Enter the following command to verify that the local repository has been set up correctly:

```
yum repolist
```

Output similar to the following is displayed:

```
Loaded plugins: rhnplugin, security
Local | 1.3 kB 00:00
Local/primary | 868 kB 00:00
Local 3116/3116
localHA | 1.3 kB 00:00
localHA/primary | 6.1 kB 00:00
localHA 32/32
repo id repo name status
Local Local Media Repo enabled: 3,116
localHA Local HA Media Repo enabled: 32
rhel-x86_64-server-5 Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) enabled: 14,137
```

```
repolist: 17,285
```

Step 4 Enter the following command for all the missing packages:

```
yum install <name_of_rpm_file>
```

For RHEL-6.x:

For example, for rgmanager, enter the following command:

```
yum localinstall rgmanager-3.0.12.1-21.el6.x86_64
```

Step 5 The cman and rgmanager configurations are enabled after you boot the server. To verify that cman and rgmanager are enabled, enter the following commands:

For RHEL-6.x:

```
chkconfig --list cman
chkconfig --list rgmanager
```

The following output appears when cman or rgmanager is enabled (levels 2, 3, 4, and 5 show the on state):

```
cman 0:off 1:off 2:on 3:on 4:on 5:on 6:off
rgmanager 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Step 6 Enter the following commands to enable the package:

For RHEL-6.x:

```
chkconfig --level 2345 cman on
chkconfig --list cman
chkconfig --level 2345 rgmanager on
chkconfig --list rgmanager
```

Step 7 Enter the following command to check the openais service status:

For RHEL-6.x:

```
service openais status
```

If the service is running, enter the following command to stop the openais service.

```
service openais stop
```

Step 8 Enter the following command to confirm that the openais service is not automatically started at boot time:

For RHEL-6.x:

```
chkconfig openais --list
```

The result must look like this:

```
openais 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Step 9 If any of the levels are set to on, enter the command to disable the service. For example, if levels 2,3,4, and 5 are set to on, enter the following command:

For RHEL-6.x:

```
chkconfig --level 2345 openais off
```

Installing Oracle 12c (for Oracle Not Embedded Database Setup)

To install Oracle 12c, follow these steps:

Step 1 Install Oracle 12c. Complete Oracle Prerequisites, page A-1 and Installing the Oracle 12c Software with the Response File (*.rsp) Provided by Cisco, page A-3.

Step 2 Complete Downloading and Installing the Required Oracle 12c Patch for 64-Bit Linux Platforms, page A-5.

Step 3 Edit the listener.ora file by replacing the newdbname parameter with the Oracle SID (the default is *CTM*) and the Prime Optical hostname parameter with the hostname or IP address of the workstation where the Prime Optical database will run.

Note There are multiple instances of *newdbname*. You must replace all instances with the Oracle SID.

Installing Prime Optical

To install Prime Optical:

Note This installation is performed only on the primary server because the primary and secondary servers share the disk array where the Prime Optical server and database are installed.

Step 1 Log in as the root user.

Step 2 Enter the following command to verify that the display is set correctly:

```
echo $DISPLAY
```

In the command output, you should see:

```
hostname-or-IP-address:0.0
```

Step 3 If you are using an xterm window or a remote host, enter the following command to enable the xterm connection from the clients:

```
xhost +
```

Step 4 Create a new directory *cpo107* under */ctm_backup*.

Download the digital copy of *PRIME_OPTICAL_10.7.0.0_202.tar.gz* from the Cisco partner site and copy the *PRIME_OPTICAL_10.7.0.0_202.tar.gz* under /ctm_backup/cpo107.

```
mkdir -p /ctm_backup/cpo107

cp -pvr <location where PRIME_OPTICAL_10.7.0.0_202.tar.gz is downloaded >
/ctm_backup/cpo107

cd /ctm_backup/cpo107
```

Step 5 Untar the cpo tar file using the following command:

```
tar -zxvf  PRIME_OPTICAL_10.7.0.0_202.tar.gz
```

Note *PRIME_OPTICAL_10.7.0.0_202.tar.gz* contains *PRIME_OPTICAL_10.7.0.0_202.tar*, *PRIME_OPTICAL_10.7.0.0_202.tar.signature* and *CPO_pubkey.der.*

Step 6 Verify the authenticity of the cpo tar file with the certificates:

```
openssl dgst -sha512 -keyform DER -verify CPO_pubkey.der -signature
PRIME_OPTICAL_10.7.0.0_202.tar.signature  PRIME_OPTICAL_10.7.0.0_202.tar
```

Note You must see the output as *verified*.

Step 7 Untar the cpo tar file that was received after extracting the *PRIME_OPTICAL_10.7.0.0_202.tar.gz* using the following command:

```
tar -xvf PRIME_OPTICAL_10.7.0.0_202.tar
```

Step 8 (Optional) Remove all the tar files and certificates using the following command:

```
rm -rf CPO_pubkey.der  PRIME_OPTICAL_10.7.0.0_202.tar*
```

Step 9 Enter the following command to change to the CPO-10.7 directory:

```
cd /ctm_backup/cpo107/Disk1
```

Step 10 Enter the following command to start the installation:

```
cd /ctm_backup/cpo107/Disk1
./setup.sh
```

The following happens:

1. The setup program searches for Sun Microsystems JDK Version 1.7.0_151 on your workstation.
2. For Linux, if the installed release is not Red Hat 5.x, Red Hat 6.x or Red Hat 7.x, the following message appears:

   ```
   WARNING: Installed Linux version (`cat /etc/redhat-release`) is different from the
   required one.
   Do you want to Continue? [y] :
   ```

   If you enter **y**, the following message appears:

   ```
   Continuing Cisco Prime Optical server installation.
   ```

   If you enter **n**, the installation quits.

The **Cisco Prime Optical Server Installation** wizard appears. Wait for up to 90 seconds while the following message appears:

```
Continuing Cisco Prime Optical Server Installation.
```

Step 11 At the **Introduction** screen, click **Next**.

Step 12 At the **License Agreement** screen, read the license agreement and click the **I accept the terms of the license agreement** radio button. Click **Next**.

Step 13 At the **Configure the Server and Database** screen, do the following:

a. From the list of Prime Optical installation types, select the **Prime Optical server and database** radio button to install the Prime Optical server along with the database.

The **Database** field is disabled when the server and database are installed on the same workstation. Prime Optical automatically uses the server hostname or IP address.

b. Type the Virtual IP or related hostname for the Prime Optical Server and then click **Next**.

Step 14 At the **Configure the Database** screen, select **Embedded** to install Prime Optical with an embedded database.

When you select **Embedded** as the Oracle database installation type, the rest of the fields in the screen become disabled, and you can move to the next screen.

The following message appears:

```
This installation will remove any previous Oracle database installed on the server.
If you do not want to continue, click Cancel.
```

Click **Continue** to delete the previous Oracle version and continue the installation. (If you click **Cancel**, the installation quits.)

Step 15 At the **OS Users** screen, choose the root user from the drop-down list. (The password for optusr is Ctm123!. You can change the password later using the **passwd -u optusr** command.)

Step 16 At the **Select Network Configuration** screen, specify the size of your network and then click **Next**.

At the **Oracle Pre-Installation Checks** screen, the setup program checks the RAM, swap, and temp directory sizes. The screen indicates whether you have enough space to install Prime Optical and Oracle, and whether any required packages are missing.

Step 17 Review the preinstallation checks and then click **Next**.

- If errors are discovered during the check sizes phase of the preinstallation checks, the following message appears, and the installation quits:

```
An error occurred during the pre-installation check.
/temp_CTM/report_oracle_pre_install_checks.log.
The installation has been canceled.
```

Check the log file, correct any errors noted in the file, and restart the installation.

- During the check packages phase of the preinstallation checks, the following message appears:

```
A warning occurred during the preinstallation check. See
/temp_CTM/report_oracle_pre_install_checks.log. To continue the installation, click
Continue. To cancel the installation and fix the problem, click Cancel.
```

You can choose to continue installation, or quit and fix the problem before proceeding.

Step 18 At the **Optional Features** screen, you can choose Install Prime Optical in a High Availability Setup to configure HA local redundancy setup:

If you choose this option, provide details in the **Second High Availability Server** field. If you chose optusr as the Prime Optical user, the following message appears:

```
The Prime Optical OS user must be the root user for High Availability setup. Click
Continue to proceed, or click Cancel to change the selection.
```

If you choose to continue, the Prime Optical user is automatically changed to root.

- Configure FTP (ONS15216 EDFA3)
- Install Sudo Software (available for root users only)

Step 19 If you selected the **Install Sudo Software** option, at the **Prime Optical Group Information & Sudo Installation** screen, do the following:

a. Enter the name of the UNIX group to which you want to assign administrator privileges.

b. To install sudo, check the **Install Prime Optical Sudo** check box. If you do not want to install sudo, uncheck the check box.

Note If you already installed and configured sudo with rules in a file different from /etc/sudoers (for example, if you created a custom sudo configuration in the /user/local/etc/sudoers file), then you must copy the rules from /etc/sudoers to /user/local/etc/sudoers at the end of the installation.

c. Click **Next**.

Step 20 If you selected the **Configure FTP (ONS15216 EDFA3)** option, at the **FTP Information** screen, do the following to configure an FTP account for software download operations:

Note NE types that require FTP configuration are:

- Cisco ONS15216 EDFA3
- Cisco ONS15305 with release lower than 3.0 (CEC-based 15305 NEs)

a. Enter the following information:

- Username
- Password
- Confirm Password
- FTP directory

b. Check or uncheck the **Create new FTP account** check box.

If checked, the installation script automatically creates the FTP user on the Prime Optical server workstation. If unchecked, it is assumed that an FTP user already exists on the Prime Optical server workstation.

c. Click **Next**.

Step 21 At the **Destination Folder** screen, install the Prime Optical server in the default directory. The default directory is /cisco/PrimeOpticalServer. Click **Next**.

Note If the destination directory that you specified is a new directory, you will receive the message, "The specified directory does not exist. Do you want to create it?" Click **Yes**.

Caution Do not specify a mount point as the target installation directory for the Prime Optical server installation, or the installation data will be lost when the workstation restarts. You must create a dedicated Prime Optical subdirectory. For example, if /cisco is the mount point for the disk partition /dev/dsk/c0t0d0s5, you cannot specify /cisco as the Prime Optical installation directory. Instead, specify a dedicated subdirectory such as/cisco/PrimeOpticalServer.

Caution Do not delete any instances of /opt/CiscoTransportManagerServer from your Prime Optical file structure. Prime Optical checks for the /opt/CiscoTransportManagerServer directory or a symbolic link to it. If Prime Optical cannot find the /opt/CiscoTransportManagerServer directory or a symbolic link, Prime Optical creates a symbolic link automatically.

The **Pre-Installation Summary** screen shows the items that will be installed.

Step 22 Click **Install**.

Depending on your system performance, it might take 35 to 50 minutes for Linux operating systems.

If SSH is not configured, a warning message appears.

Step 23 Click **Continue**; in the terminal window that appears, enter the root password and follow the prompts to configure the SSH connection.

The installation continues.

Step 24 In the **Web Server Installation Summary** window, click **Next**.

The **Install Complete** window summarizes the results of the installation.

Step 25 Click **Done**.

Caution Do not close the terminal or reboot the host before the following message is displayed:

```
Prime Optical installation is complete.
```

Step 26 Enter the following command to shut down the interface:

```
ifconfig interface down
```

For example:

```
ifconfig eth0:1 down
```

Step 27 On the secondary server, log in as the root user.

Step 28 Enter the following command to configure the virtual IP address used in Setting the Environment for Installation:

```
ifconfig interface virtual-IP-address netmask netmask
```

For example:

```
ifconfig eth0:1 10.58.65.22 netmask 255.255.255.0
```

You can verify if the IP address was configured correctly by issuing the `ifconfig` command. The IP address for the interface should be displayed in the inet addr field.

Step 29 Verify that the **yum** repolist is available on the server, and then enter the following script from the /temp_CTM directory:

```
installHAServer.sh
```

A terminal window appears. Before continuing, perform a check on /root/.ssh/known_hosts.

Step 30 Enter the root password and follow the prompts to configure the SSH connection on the secondary server.

Step 31 Enter the following command to shut down the interface:

```
ifconfig interface down
```

For example:

```
ifconfig eth0:1 down
```

Installing the HA Package

To install the Prime Optical HA package, follow these steps:

Step 1 Create a new directory *cpo107* under */ctm_backup*.

Download the digital copy of *PRIME_OPTICAL_10.7.0.0_202.tar.gz* from the Cisco partner site and copy the *PRIME_OPTICAL_10.7.0.0_202.tar.gz* under /ctm_backup/cpo107.

```
mkdir -p /ctm_backup/cpo107

cp -pvr <location where PRIME_OPTICAL_10.7.0.0_202.tar.gz is downloaded >
/ctm_backup/cpo107

cd /ctm_backup/cpo107
```

Step 2 Untar the cpo tar file using the following command:

```
tar -zxvf  PRIME_OPTICAL_10.7.0.0_202.tar.gz
```

Note *PRIME_OPTICAL_10.7.0.0_202.tar.gz* contains *PRIME_OPTICAL_10.7.0.0_202.tar*, *PRIME_OPTICAL_10.7.0.0_202.tar.signature* and *CPO_pubkey.der.*

Step 3 Verify the authenticity of the cpo tar file with the certificates:

```
openssl dgst -sha512 -keyform DER -verify CPO_pubkey.der -signature
PRIME_OPTICAL_10.7.0.0_202.tar.signature  PRIME_OPTICAL_10.7.0.0_202.tar
```

Note You must see the output as *verified*.

Step 4 Untar the cpo tar file that was received after extracting the *PRIME_OPTICAL_10.7.0.0_202.tar.gz* using the following command:

```
tar -xvf PRIME_OPTICAL_10.7.0.0_202.tar
```

Step 5 (Optional) Remove all the tar files and certificates using the following command:

```
rm -rf CPO_pubkey.der  PRIME_OPTICAL_10.7.0.0_202.tar*
```

Step 6 Enter the following command to change to the HA RPMS directory.

For RHEL-6.x:

```
cd /ctm_backup/cpo107/HA/RPMS/x86_64
yum install --nogpgcheck GEOManager-1.5-2.x86_64.rpm
```

For RHEL-7.x:

```
cd /ctm_backup/HA7/cpo107/RPMS/x86_64
yum install --nogpgcheck GEOManager-1.0-5.x86_64.rpm
```

The following output appears:

```
Preparing...########################################### [100%]
1: HA########################################### [100%]
Installation DONE!
```

Step 7 Enter the following command to install the GEO Manager:

For RHEL-6.x:

```
cd /ctm_backup/cpo107/HA/RPMS/x86_64

yum install --nogpgcheck GEOManager-1.5-2.x86_64.rpm
```

For RHEL-7.x:

```
cd /ctm_backup/cpo107/HA7/RPMS/x86_64

yum install --nogpgcheck GEOManager-1.0-5.x86_64.rpm
```

Step 8 Enter the following command:

```
yum install --nogpgcheck HA-1.5-3.x86_64.rpm
```

The following output appears:

```
Preparing...########################################### [100%]
1: HA########################################### [100%]
Installation DONE!
```

If the installation was successful, you should see the directory structure when installation is complete. Navigate to /opt/CiscoTransportManagerServer/HA directory. See HA Directory Structure, page 3-47 for more information on the directory structure.

Password Less Authentication Configuration

Follow these steps to configure password less configuration in both the primary and secondary servers:

Step 1 Enter the following commands from the primary node to configure SSH:

```
ssh "secondary-replication-if" ls
ssh "secondary-heartbeat-if" ls
```

Where:

- secondary-replication-if—Indicates the hostname associated with the interface used for the replication link on the secondary node. (For example, ha2-107.cisco.com)
- secondary-heartbeat-if—Indicates the hostname associated with the interface used for the heartbeat link on the secondary node. (For example, ha2-107.cisco.com)

Note Both commands must display the contents of the secondary node's /root directory.

SSH with root access is configured between the primary and the secondary nodes. Configure SSH for the replication and heartbeat links (see Figure 1-4).

Step 2 Enter the following commands from the secondary node:

```
ssh "primary-replication-if" ls
ssh "primary-heartbeat-if" ls
```

Where:

- primary-replication-if—Indicates the hostname associated with the interface used for the replication link on the primary node. (For example, ha1-107.cisco.com).
- primary-heartbeat-if—Indicates the hostname associated with the interface used for the heartbeat link on the primary node. (For example, ha1-107.cisco.com)

Note Both commands must display the contents of the primary node's /root directory.

Step 3 If SSH verification fails, open a shell from the Prime Optical server workstation and do the following on the Primary and secondary cluster servers:

On the primary cluster:

a. As the root user, enter the following command to start the SSH service:

```
service sshd start
```

b. If the /.ssh/id_rsa and /.ssh/id_rsa.pub files do not exist, enter the following command to generate public and private keys:

```
ssh-keygen -t rsa
```

Press **Return** to accept the default values for the following prompts:

```
Enter file in which to save the key (//.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

c. Enter the following command to publish the public key to the secondary cluster server:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@Secondary-Cluster-Server
```

where secondary-cluster-server is the name of the secondary cluster server.

d. Edit the /etc/ssh/sshd_config file on the primary cluster server and change the PermitRootLogin value to **yes**.

e. Enter the following command on the primary cluster server to save and apply the changes:

```
service sshd restart
```

f. Enter the following command to open an SSH connection from the primary cluster server to the secondary cluster server and register the SSH key:

```
ssh Secondary Cluster server
```

g. Repeat Step 1 and Step 2 to verify the SSH configuration.

On the secondary cluster:

a. As the root user, enter the following command to start the SSH service:

```
service sshd start
```

b. If the /.ssh/id_rsa and /.ssh/id_rsa.pub files do not exist, enter the following command to generate public and private keys:

```
ssh-keygen -t rsa
```

Press **Return** to accept the default values for the following prompts:

```
Enter file in which to save the key (//.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

c. Enter the following command to publish the public key to the primary cluster server:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@Primary-Cluster-Server
```

d. Edit the /etc/ssh/sshd_config file on the secondary cluster server and change the PermitRootLogin value to **yes**.

e. Enter the following command on the secondary cluster server to make the changes take effect:

```
service sshd restart
```

f. Enter the following command to open an SSH connection from the secondary cluster server to the primary cluster server and register the SSH key:

```
ssh Primary Cluster server
```

g. Repeat Step 1 and Step 2 to verify the SSH configuration.

Editing the Agent Configuration File

The agent configuration file allows you to configure the agents that RHCS uses. To edit the agent configuration file:

Step 1 Connect to the primary server. Enter the following command:

```
cd /opt/Cisco*Server/HA/cfg
```

Step 2 Edit the clusterConfig.ini file. Enter the following command:

```
vim clusterConfig.ini
```

Step 3 For local redundancy configuration, do the following:

Note Only two fields need to be edited.

a. Specify the cluster type. Replace `type=TODO_ClusterType` with **`type=LOCAL`**.

b. Specify the network interface that Prime Optical uses to retrieve data from a monitored network element. Replace `interface=TODO_interface` with **`interface=`*`interface`***.

For example:

`interface=eth0`.

Note This interface is a critical resource; we strongly recommend that you protect it by bonding interfaces on different NICs; for example, eth0, eth1, and bond0.

Step 4 Save the file.

Note For more information on the clusterConfig.ini file, see Table 3-5 on page 3-26.

Editing the Logging Configuration File

When the cluster agent detects a failure in a resource, any critical error is mailed to a receiver that is configured in the logHAconf.ini file.

To edit the file:

Step 1 Connect to the primary server. Enter the following command:

```
cd /opt/Cisco*Server/HA/cfg
```

Step 2 Edit the logHAconf.ini file. Enter the following command:

```
vim logHAconf.ini
```

Step 3 Specify the mail receiver. Under the [handler_mail] header, replace `<hostname>` and `<mail_address@<domain>` in the following line:

```
args=('localhost', 'root@cpo<hostname>, ['<mail_address@<domain>'], 'CTM High
Availability notification'
```

for example,

```
args=('localhost', 'root@cpo-local-cluster.cisco.com', ['jsmith@cisco.com'], 'CTM High
Availability notification'
```

Step 4 Save the file.

Note For more information on the clusterConfig.ini file, see Table 3-7 on page 3-30.

Editing the RHCS Configuration File

In /opt/Cisco*ver/HA/template there are three different cluster configuration template for local configuration:

- Cluster.conf.local

  This is the base configuration without any fencing device. It is not recommended for the production environment.

- Cluster.conf.local.fenceipmi

  This template contains a customizable configuration for fence device base in IPMI (Intelligent Platform Management Interface).

- Cluster.conf.local.fencevmware

  This template contained a customizable configuration for fence based on VMWARE.

  For details about fence device and configuration see the RHCS documentation.

Choose the template that match you environment and edit it substituting all the "TODO" tags.

To edit the RHCS file:

Step 1 Connect to the primary server. Enter the following command:

```
cd /opt/Cisco*Server/HA/template
```

Step 2 Edit the cluster.conf.local file. Enter the following command:

```
vim cluster.conf.local
```

Step 3 Replace all tags listed in Table 4-3.

Table 4-3 RHCS Configuration Parameters

Tags	Description	Example
TODO_alias	Alias name of the cluster. It can be any string.	building1_cluster
TODO_name	Name of the cluster.	building1_cluster
TODO_Node1	Local cluster name on the primary server.	clusterA-abc.cisco.com
TODO_Node2	Local cluster name on the secondary server.	clusterB-abc.cisco.com
TODO_Failover_name	Failover domain name of the cluster.	building1_domain
TODO_VirtualIP	Enter the virtual IP address that was configured in Setting the Environment for Installation, page 4-3.	10.58.65.22
TODO_NetMask	Enter the netmask used.	/24
TODO_Dev_cisco[1]	Enter the disk that you associated with /cisco. See example in Setting the Environment for Installation, page 4-3.	/dev/sdk
TODO_Dev_oracle[1]	Enter the disk that you associated with /oracle. See the example in Setting the Environment for Installation, page 4-3.	/dev/sdt
TODO_Dev_db01[1]	Enter the disk that you associated with /db01. See the example in Setting the Environment for Installation, page 4-3.	/dev/sde
TODO_Dev_db02[1]	Enter the disk that you associated with /db02. See the example in Setting the Environment for Installation, page 4-3.	/dev/sdf
TODO_Dev_db03[1]	Enter the disk that you associated with /db03. See the example in Setting the Environment for Installation, page 4-3.	/dev/sdg
TODO_Dev_db04[1]	Enter the disk that you associated with /db04. See the example in Setting the Environment for Installation, page 4-3.	/dev/sdh

Table 4-3 RHCS Configuration Parameters (continued)

Tags	Description	Example
TODO_Dev_db05[1]	Enter the disk that you associated with /db05. See the example in Setting the Environment for Installation, page 4-3.	/dev/sdi
TODO_Dev_ctm_backup[1]	Enter the disk that you associated with /ctm_backup. See the example in Setting the Environment for Installation, page 4-3.	/dev/sdj

1.Be sure that the disk space meets the requirements listed in Table 2-4 and Table 2-5.

The following is an example of a cluster.conf.local file:

```
<?xml version="1.0"?>
<cluster alias="local" config_version="3" name="local">
    <fence_daemon clean_start="1" post_fail_delay="20" post_join_delay="6"/>
    <clusternodes>
        <clusternode name="vesuvio.cisco.com" nodeid="1" votes="1">
            <fence/>
        </clusternode>
        <clusternode name="bernina.cisco.com" nodeid="2" votes="1">
            <fence/>
        </clusternode>
    </clusternodes>
    <cman expected_votes="1" two_node="1"/>
    <fencedevices/>
    <rm log_level="7">
        <failoverdomains>
            <failoverdomain name="local_domain" nofailback="0" ordered="0"
restricted="1"/>
        </failoverdomains>
        <resources/>
        <service autostart="0" name="ctm_service" recovery="relocate">
            <ip address="10.58.65.22/24" monitor_link="1"/>
            <fs device="/dev/sdk" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/cisco" name="cisco" options="" self_fence="0"/>
            <fs device="/dev/sdt" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/oracle" name="oracle" options="" self_fence="0"/>
            <fs device="/dev/sde" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/db01" name="ora_db01" options="" self_fence="0"/>
            <fs device="/dev/sdf" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/db02" name="ora_db02" options="" self_fence="0"/>
            <fs device="/dev/sdg" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/db03" name="ora_db03" options="" self_fence="0"/>
            <fs device="/dev/sdh" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/db04" name="ora_db04" options="" self_fence="0"/>
            <fs device="/dev/sdi" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/db05" name="ora_db05" options="" self_fence="0"/>
            <fs device="/dev/sdj" force_fsck="1" force_unmount="1" fstype="ext3"
mountpoint="/ctm_backup" name="ctm_backup" options="" self_fence="0"/>
            <script file="/opt/CiscoTransportManagerServer/HA/bin/NtwIFAgent.py"
name="NTW_IF"/>
            <script file="/opt/CiscoTransportManagerServer/HA/bin/OracleAgent.py"
name="CTM_SID">
                <script file="/opt/CiscoTransportManagerServer/HA/bin/CtmAgent.py"
name="CTM_SRV">
                    <script file="/opt/CiscoTransportManagerServer/HA/bin/ApacheAgent.py"
name="CTM_APACHE"/>
                </script>
            </script>
```

```
        </service>
    </rm>
</cluster>
```

Step 4 Locate the line that begins with **<service autostart**. In the recovery parameter, enter **relocate**.

For example,

```
<service autostart="0" name="ctm_service" recovery="relocate">
```

Step 5 Save the file as cluster.conf file.

Step 6 Copy the modified cluster.conf file to the /etc/cluster directory on both the primary and secondary servers.

Starting the Cluster

The following sections describe the process of starting the cluster:

- Starting RHCS Services, page 4-19
- Starting ctm_services on the Primary Server, page 4-20
- Verifying Cluster Status on the Standby Node, page 4-20

Starting RHCS Services

To start RHCS services, follow these steps:

Step 1 Shut down the interface associated to virtual IP on the primary server that is managed by the cluster:

```
ifconfig vip-interface down
```

Step 2 Enter the following command to disable dbora services (which are on during installation):

```
chkconfig --del dbora
```

Step 3 Enter the following command on the primary server:

```
service cman start
```

Step 4 Enter the following command on the standby server:

```
service cman start
```

Step 5 Enter the following command on the primary server:

```
service rgmanager start
```

Step 6 Enter the following command on the standby server:

```
service rgmanager start
```

ctm_heartbeat automatically starts when you start rgmanager. On the primary server, ctm_heartbeat pings the standby server at startup to find out if the RHCS services (cman and rgmanager) are running. This check is performed three times, with a 10-second wait between attempts. If the three attempts fail, RHCS moves ctm_heartbeat to the failed state.

Starting ctm_services on the Primary Server

After you have successfully started RHCS services, you can start Prime Optical from the primary server. All resources used by Prime Optical are defined in the ctm_service in /etc/cluster/cluster.conf file.

To start ctm_services on the primary server:

Step 1 Check the state of the cluster by executing the following command:

```
clustat
```

If ctm_service is not disabled, invoke it by executing the following command:

```
clusvcadm -d ctm_service
```

Step 2 Start the ctm_service. Enter the following command:

```
clusvcadm -e ctm_service
```

The **clusvcadm -e ctm_service** command starts all Prime Optical resources. You can check the startup sequence detailed in the /var/log/message directory and the output of /opt/Cisco*Server/HA/log/cisco_agents_cluster.log (or the filename that you specified in the logHAgent.ini file when you configured logging).

Step 3 Check the state of the cluster by executing the following command:

```
clustat
```

The **clustat** command output should show that the ctm_service has started.

Verifying Cluster Status on the Standby Node

Enter the following command to verify the status of the standby server:

```
clustat
```

The output must show that ctm_service has started on the primary server.

Installing the Multicast Heartbeat Services Package

Multicast Heartbeat services checks the healthy status between the cluster nodes and sends e-mail notifications when there are connection problems between nodes.

To install the Multicast Heartbeat Services package, follow these steps:

Step 1 Create a new directory *cpo107* under */ctm_backup.*

Download the digital copy of *PRIME_OPTICAL_10.7.0.0_202.tar.gz* from the Cisco partner site and copy the *PRIME_OPTICAL_10.7.0.0_202.tar.gz* under /ctm_backup/cpo107.

```
mkdir -p /ctm_backup/cpo107

cp -pvr <location where PRIME_OPTICAL_10.7.0.0_202.tar.gz is downloaded >
/ctm_backup/cpo107

cd /ctm_backup/cpo107
```

Step 2 Untar the cpo tar file using the following command:

```
tar -zxvf  PRIME_OPTICAL_10.7.0.0_202.tar.gz
```

Note *PRIME_OPTICAL_10.7.0.0_202.tar.gz* contains *PRIME_OPTICAL_10.7.0.0_202.tar*, *PRIME_OPTICAL_10.7.0.0_202.tar.signature* and *CPO_pubkey.der.*

Step 3 Verify the authenticity of the cpo tar file with the certificates:

```
openssl dgst -sha512 -keyform DER -verify CPO_pubkey.der -signature
PRIME_OPTICAL_10.7.0.0_202.tar.signature  PRIME_OPTICAL_10.7.0.0_202.tar
```

Note You must see the output as *verified*.

Step 4 Untar the cpo tar file that was received after extracting the *PRIME_OPTICAL_10.7.0.0_202.tar.gz* using the following command:

```
tar -xvf PRIME_OPTICAL_10.7.0.0_202.tar
```

Step 5 (Optional) Remove all the tar files and certificates using the following command:

```
rm -rf CPO_pubkey.der  PRIME_OPTICAL_10.7.0.0_202.tar*
```

Step 6 Enter the following command to change to the HA RPMS directory.

For RHEL-6.x:

```
cd /ctm_backup/cpo107/HA/RPMS/x86_64
```

Step 7 Enter the following command:

```
rpm -ivh --relocate /=/opt MulticastHBService-1.5-2.x86_64.rpm
```

The following output appears:

```
Preparing...########################################### [100%]
1: MulticastHBSrv########################################### [100%]
Installation DONE!
```

Step 8 Copy the MulticastHBService-1.5-2.x86_64.rpm file to the /root directory of the secondary server.

Step 9 Enter the following command:

```
yum install-nogpgcheck MulticastHBService-1.5-2.x86_64.rpm
```

The following output appears:

```
Preparing...########################################### [100%]
1: MulticastHBSrv########################################### [100%]
Installation DONE!
```

After the rpm file is installed, a MulticastHeartBeat directory is created, containing the following files:

Table 4-4 MulticastHeartBeat Directory Files

Files	Description
MulticastHeartBeat.ph	Python script to probe the communication status of cluster servers.
MulticastHBService	Start, stop, and status operations.
multicastConfig.ini	Configuration file that sets the network interface and polling period to monitor the connection between nodes.
logMulticast.ini	Log activity configuration file for the MulticastHBService service.
clusterModule.PY	Module that provides functions for cluster (RHCS) management; for example, starting, stopping, and retrieving status on the cluster.

Editing the multicastConfig.ini File

Step 1 Connect to the primary server and navigate to the /opt/MulticastHeartBeat directory.

Step 2 Edit the multicastConfig.ini file:

```
vim multicastConfig.ini
```

Step 3 Replace the tags listed in Table 4-5:

Table 4-5 MulticastConfig.ini File Parameters

Tags	Description
TODO_Ifname	Network interface used by the heartbeat service to monitor the connection between nodes; for example, eth1.
TODO_othernode	The name associated to the multicast interface of the other node on the cluster; for example, node2-abc.cisco.com.

Step 4 Save the multicastConfig.ini file.

Editing the logMulticast.ini File

Step 1 Connect to the primary server and navigate to the /opt/MulticastHeartBeat directory.

Step 2 Edit the logMulticast.ini file:

```
vim logMulticast.ini
```

Step 3 Specify the mail receiver. Under the [handler_mail] header, replace `<hostname>` and `<mail_address@<domain>` in the following line:

```
args=('localhost', 'root@cpo<hostname>, ['<mail_address@<domain>'], 'Multicast interface
heartbeat notification'
```

For example:

```
args=('localhost', 'root@cpo-local-cluster.cisco.com', ['jsmith@cisco.com'], 'Multicast
interface heartbeat notification'
```

Step 4 Save the logMulticast.ini file.

Starting the Multicast HeartBeat Services

Step 1 Connect to the primary server and navigate to the /etc/init.d directory.

Step 2 Enter the following command to create a symbolic link:

```
ln -s /opt/MulticastHeartBeat/MulticastHBService
```

Step 3 Enter the following command to start the MulticastHBService on the primary server:

```
service MulticastHBService start
```

Configuring the MultiCast Heartbeat Services on the Secondary Server

Step 1 Connect to the secondary server.

Step 2 Follow the steps described in the Editing the multicastConfig.ini File, page 4-22 on the secondary server.

Note Be sure to enter values that are applicable to the secondary server.

Step 3 Follow the steps described in the Editing the logMulticast.ini File, page 4-22 on the secondary server.

Note Be sure to enter values that are applicable to the secondary server.