



# Installing and Maintaining Gateway Geographical Redundancy

The following topics provide procedures for setting up, installing, and maintaining the gateway geographical redundancy solution. Geographical redundancy is configured and monitored using Oracle Active Data Guard (ADG) for geographical redundancy. This chapter also explains how to install Prime Network Operations Reports and the Prime Network Integration Layer (PN-IL) with gateway geographical redundancy.



## Note

Gateway high availability is supported only when the gateway software, Oracle database, and Infobright database (applicable for Operations Reports) are installed on the same server.

This chapter covers the following topics:

- [Steps for Installing the Geographical Redundancy Solution, page 4-1](#)
- [Installation Requirements for Geographical Redundancy, page 4-4](#)
- [Preparing to Install Geographical Redundancy, page 4-6](#)
- [Installing the Prime Network Gateway Geographical Redundancy Software, page 4-6](#)
- [Verifying the Geographical Redundancy Setup, page 4-14](#)
- [Maintaining Geographical Redundancy, page 4-16](#)
- [Uninstalling the Geographical Redundancy Software, page 4-18](#)
- [Installing and Configuring PN-IL for Local + Geographical Redundancy, page 4-18](#)
- [Installing and Configuring PN-IL for Geographical Redundancy Only, page 4-27](#)

Before proceeding with this chapter, make sure you have read [Geographical Redundancy Functional Overview, page 2-5](#).

## Steps for Installing the Geographical Redundancy Solution

[Table 4-1](#) lists the steps you must follow to prepare for an installation, perform an installation and verify an installation of the Prime Network gateway geographical redundancy solution. The standby P2 node is only relevant if you are installing geographical + local redundancy. An **x** means you must perform the step *on that server*.

## ■ Steps for Installing the Geographical Redundancy Solution



**Note** The steps in the following table area based on these assumptions:

- For geographical redundancy *only*: Node P1 is the active node and has the primary database. (Installation prompts for geographical redundancy *only* are provided in [Table 4-4 on page 4-8](#).)
- For geographical + local redundancy: Node P1 has the primary database. The local site will also have a standby node (P2); it should be configured as described in [is the local redundancy standby node](#). (The installation prompts for geographical + local redundancy are provided in [Table 4-5 on page 4-10](#).)

**Table 4-1** Steps for Setting Up and Installing Geographical Redundancy

			Local		Remote
			Primary Node P1 <sup>1</sup>	Standby Node P2 <sup>2</sup>	DR NodeS1
<b>Step 1</b>	Collect the server details so that you have all information handy prior to installation.	<ul style="list-style-type: none"> <li>• Prime Network Virtual IP address</li> <li>• Oracle IP address</li> <li>• Node1, Node 2, DR Node Hostname and IP address.</li> </ul>	x	x	x
<b>Step 2</b>	Verify that the servers meet the prerequisites.	<a href="#">Installation Requirements for Geographical Redundancy, page 4-4</a>	x	x	x
<b>Step 3</b>	Configure the server hardware.  <b>Note</b> If your setup contains primary and a remote site, make sure the remote site is the replica of the primary site.	<ul style="list-style-type: none"> <li>• Geographical and local redundancy: If you have dual-node cluster configured at the primary site, see <a href="#">Configuring Hardware and External Storage for Red Hat Cluster Site, page 3-7</a>.</li> <li>• Geographical redundancy only: See the gateway hardware requirements in the <a href="#">Cisco Prime Network 4.3.1 Installation Guide</a>.</li> </ul>	x	x	x
<b>Step 4</b>	Install the RHEL and all recommended patches on the servers.	<a href="#">Installing RHEL and Verifying the Version, page 3-8</a>	x	x	x
<b>Step 5</b>	Install the RPMs required on Red Hat for Prime Network.  If you are installing Operations Reports, be sure to check this section.	<a href="#">Installing RPMs Required on Red Hat for Prime Network, page 3-8</a>	x	x	x
<b>Step 6</b>	Configure disk groups, volumes, and partitions.  If you are installing Operations Reports, be sure to check the required volume sizes.	<a href="#">Configuring Disk Group and Volumes, page 3-11</a>	x	x	x
<b>Step 7</b>	Mount the installation files (in the same directory on both nodes).	—	x	x	x

**Table 4-1** Steps for Setting Up and Installing Geographical Redundancy (continued)

			Local		Remote
			Primary Node P1 <sup>1</sup>	Standby Node P2 <sup>2</sup>	DR NodeS1
<b>Step 8</b>	Verify that all nodes are ready for installation by checking disk access, Linux versions, and NTP synchronization.	<a href="#">Verify That All Servers Are Ready for Installation, page 3-12</a>	x	x	x
<b>Step 9</b>	Configure the disk partitions.	<a href="#">Configuring Disk Group and Volumes, page 3-11</a>	x	x	x
<b>Step 10</b>	Mount the external shared storage, Oracle, and Prime Network mount points on the relevant directories.	<a href="#">Creating the Mount Points for Installation, page 3-12</a>	x	x	—
<b>Step 11</b>	Back up the /etc/host and root cron jobs files (the installation software will modify them).	—	x	x	x
<b>Step 12</b>	(Local + geographical) For cluster node makes sure the specified services are configured to start automatically each time the machine is rebooted.	<a href="#">Configure the Services for Automatic Start After Reboot, page 3-13</a>	x	x	—
<b>Step 13</b>	(Local + geographical) Stop the RHCS services.	<a href="#">Stopping the RHCS Services, page 3-14</a>	x	x	x
<b>Step 14</b>	Install the server and Oracle database using <b>install_prime_HA.pl</b> .	<a href="#">Installing the Prime Network Gateway Geographical Redundancy Software, page 4-6</a>	x	—	—
<b>Step 15</b>	Configure the embedded database (using the <b>add_emdb_storage.pl -ha</b> script).	<a href="#">Installing the Prime Network Gateway Geographical Redundancy Software, page 4-6</a>	x	—	—
<b>Step 16</b>	Configure the remote site (S1) (execute <b>setup_prime_DR.pl</b> )		x	—	x
<b>Step 17</b>	If desired, install any new device packages so that you have the latest device support.		<a href="#">Cisco Prime Network 4.3 Release Notes</a>	x	—
<b>Step 18</b>	Verify the installation.	<a href="#">Verifying the Geographical Redundancy Setup, page 4-14</a>	x	x	x
<b>Step 19</b>	(Optional) Install PN-IL	<a href="#">Installing and Configuring PN-IL for Local + Geographical Redundancy, page 4-18</a>	x	—	x
<b>Step 20</b>	(Optional) Setup RHCS Web GUI if it is not configured during installation.	<a href="#">Configuring the RHCS Web Interface (Optional), page 3-23</a>	x	—	—
<b>Step 21</b>	(Only for NAT) Update the database host.	<a href="#">Updating the Database Host in the Registry (Only for NAT), page 3-22</a>	x	x	x
<b>Step 22</b>	(Local + geographical HA only) (Optional) Setup RHCS Web GUI if it is not configured during installation.	<a href="#">Configuring the RHCS Web Interface (Optional), page 3-23</a>	x	—	—

## ■ Installation Requirements for Geographical Redundancy

1. P1 node has primary database (geographical redundancy *only*, or geographical + local redundancy).
2. P2 node is only relevant if local redundancy is also installed.

# Installation Requirements for Geographical Redundancy

These topics list the prerequisites for installing gateway geographical redundancy:

- [Hardware and Software Requirements for Geographical Redundancy, page 4-4](#)
- [Ports Usage for Geographical Redundancy, page 4-5](#)

## Hardware and Software Requirements for Geographical Redundancy

**Table 4-2** shows the core system requirements for geographical redundancy. All the hardware and software requirements are also applicable for virtual machines. Geographical redundancy requires a Prime Network embedded database and does not support IPv6 gateways or databases. If your high availability deployment differs from these requirements, please contact your Cisco account representative for assistance with the planning and installation of high availability.



**Note** Geographical redundancy for PN-IL is only supported if the local redundancy solution is also installed.

If you are installing both local and geographical redundancy, for the local redundancy site, refer to the requirements in [Hardware and Software Requirements for Local Redundancy, page 3-4](#).

**Table 4-2 System Requirements for Geographical Redundancy<sup>1</sup>**

Area	Requirements
Operating System	Red Hat 5.8, Red Hat 6.5 64-bit Server Edition (English language).
Oracle	12c. Oracle 12c is included in the Prime Network embedded database installation.
Hardware	RHEL 5.8 and RHEL 6.5 certified platform. For recommended hardware for small, medium and large networks, see the <a href="#">Cisco Prime Network 4.3 Installation Guide</a> .

**Table 4-2 System Requirements for Geographical Redundancy<sup>1</sup> (continued)**

<b>Area</b>	<b>Requirements</b>
Network	<ul style="list-style-type: none"> <li>Gateway and database should use logical IP addresses which are different between two sites (the sites can be on different subnets).</li> </ul> <p><b>Note</b> If you are using the <b>network-conf</b> script, when you are prompted for the IP address of units, use the floating IP address of the gateway.</p> <ul style="list-style-type: none"> <li>A SSH connection between all nodes is required.</li> <li>Port 1521 must be open between all nodes to allow ADG data to transfer between the primary and standby database.</li> <li>IP reachability to the primary site.</li> <li>SSL connectivity to primary site. For SSL, generate SSL keys and copy to all nodes in primary site.</li> <li>If you use LDAP authentication in a geographical redundancy configuration, the gateway servers must be configured to communicate with two different LDAP servers, one at the local site and one at the remote site. For this reason the switchover and failover utilities will prompt you for the relevant LDAP parameters. The LDAP parameters are set once using Prime Network Administration.</li> </ul> <p>If for some reason the necessary IP addresses are not updated after a switchover or failover, you can set them manually (which includes setting the necessary LDAP parameters). See <a href="#">Changing the Gateway IP Address on a Gateway and All Units (changeSite.pl), page 6-14</a>.</p> <p>For more information on using LDAP for user authentication, see <a href="#">Using an External LDAP Server for Password Authentication in the Cisco Prime Network 4.3 Administrator Guide</a>.</p>
Storage	<p>Based on requirements determined by the <i>Cisco Prime Network Capacity Planning Guide</i>. To obtain a copy of <i>Capacity Planning Guide</i>, contact your Cisco representative. Geographical redundant storage should have the same capacity and mount points as the local site.</p>
File system	ext3
Disk space	5 GB under /tmp is required for installation
rsync	The rsync utility must be installed on all servers that are part of the geographical redundant solution.
scp	The scp program must be installed on all servers that are part of the geographical redundant solution.

- Virtual machine and bare metal requirements for hard disk, memory, and processor are same. Refer to the [Cisco Prime Network 4.3 Installation Guide](#) for memory and processor requirements.

## Ports Usage for Geographical Redundancy

In addition to the ports listed in the [Cisco Prime Network 4.3 Installation Guide](#), the following ports must be free.

You can check the status of the listed ports by executing the following command:

```
# netstat -tulnap | grep port-number
```

To free any ports, contact your system administrator.

**Table 4-3 Additional Ports Required for Local Redundancy**

Port No.	Used for:
9096	Prime Network cluster web interface

## Preparing to Install Geographical Redundancy

There are a number of pre installation steps you need to perform before you install the geographical redundancy solution. These steps are similar to those for local redundancy, except that you are performing them on the primary server (P1) and the remote DR server (S2). These steps include the following:

- Configuring the server hardware, disk groups, volumes, and partitions
- Installing RHEL and the recommended patches and RPMs
- Mounting the installation files, and creating the mount points for the external shared storage, Oracle, and Prime Network
- Backing up your deployment

Extra steps are included if you are using both geographical *and* local redundancy. The preparation procedures are in [Table 4-1 on page 4-2](#), starting with [Step 3](#). Some procedures will refer you to the instructions for local redundancy; this is because the steps are identical but are performed on the primary node (P1) and the remote DR node (S1) instead of the primary and secondary cluster nodes (P1 and P2).

## Installing the Prime Network Gateway Geographical Redundancy Software

The geographical redundancy solution uses a remote site that contains a single server that provides failover in case of a failure at the primary site. It is installed using `install_prime_HA.pl` script that is available in RH\_ha.zip file in the installation DVD as described in [Installation DVDs, page 1-1](#).

You can use this procedure to:

- Install the geographical redundancy software only on a remote server (S1 in [Figure 2-4 on page 2-6](#))
- Install the geographical redundancy software on a deployment that is also using local redundancy (P1, P2, S1 in [Figure 2-4 on page 2-6](#))

You can run the installation in interactive or in non-interactive mode. Interactive mode installation prompts you to enter the gateway HA data values one at a time. The Prime Network installer then updates the `auto_install_RH.ini` file template, which populates the `install_Prime_HA.pl` script.



**Note** It is recommended you run the installation in interactive mode first to populate the `auto_install_RH.ini` template with the user input. This gives you the ability to verify the input and run the installation again in non-interactive mode, if needed.

Alternatively, you can enter all the installation values in the `auto_install_RH.ini` template, located in the RH\_ha directory, then run the installation in non-interactive mode. The installation mode is determined by the presence or absence of the `-autoconf` flag.



- Note** The geographic redundancy configuration takes time. Depending on the speed of the local and remote site connection and size of the database, the configuration can take several hours.

To set up and configure the geographical redundancy site:

- Step 1** Change to root user, then **unzip the RH\_ha.zip** file located on the installation DVD in the **/tmp** path. This is a mandatory process to unzip the **RH\_ha** file in the **/tmp/RH\_ha** directory.



- Note** If you are running the Korn shell (/bin/ksh) and the prompt is the hash tag (#), the installation will fail. Run the installation script using bash.

- Step 2** From the **/tmp/RH\_ha** directory, run the **install\_Prime\_HA.pl** in interactive or non-interactive mode.

- Step 3** Depending on whether you want to configure geographical + local redundancy or geographical redundancy only, do one of the following for the prompts shown in [Table 4-4](#) or [Table 4-5](#):

- For geographical redundancy only, enter:  
local HA= no, DR= yes.
- For local + geographical redundancy, enter:  
local HA= yes, DR= yes.

- Step 4** Execute the **install\_Prime\_HA.pl** script in interactive or non-interactive method.

- **For Interactive Installation:**

For interactive installation, execute the following commands:

```
cd /tmp/RH_ha
perl install_Prime_HA.pl
```

See [Table 4-4](#) or [Table 4-5](#) for descriptions of parameters you will be asked to enter at various stages of the interactive installation.

- **For Non-Interactive Installation (Automatic):**

- a. Edit the **auto\_install\_RH.ini** file template found under the **RH\_ha** directory with all of the installation details.

- b. Run the following command:

```
cd /tmp/RH_ha
perl install_Prime_HA.pl -autoconf auto_install_RH.ini full path
```



- Note** To prevent a security violation, it is highly recommended to remove the password in **auto\_install\_RH.ini** file after the successful installation.

After the **install\_Prime\_HA.pl** script is completed, Prime Network gateway and embedded database are installed on the remote site.

The following tables describe the installation prompts, depending on your deployment:

- [Table 4-4, Installation Prompts for Geographical Redundancy Only](#) (this deployment is not supported for PN-IL)
- [Table 4-5, Installation Prompts for Local and Geographical Redundancy](#)

**Table 4-4** Installation Prompts for Geographical Redundancy Only

Prompt for.	Enter...	Notes
Configure local HA	no	Enter <b>no</b> ; this procedure is for geographical redundancy <i>alone</i> . To install geographical redundancy with local redundancy, see <a href="#">Table 4-5</a> . To install local redundancy, see <a href="#">Installing and Maintaining Gateway Local Redundancy, page 3-1</a>
Configure DR	yes	—
Configuring NTP on the 2 gateways	yes   no	<b>yes</b> or <b>no</b> depending on whether NTP should be configured on two gateways. If not configured, first configure NTP and then continue with the installation. For more details on procedures, see configuring NTP in the <a href="#">Cisco Prime Network 4.3 Installation Guide</a> .
OS user of the database	oracledb	Oracle installation owner (default is oracle).
Oracle file system mount point	Example:/opt/ora/oracle	Location of the mount point given for the <i>oracle-home</i> or <i>oracle-user</i> .
Configure another oracle file system mount	no	<b>yes</b> or <b>no</b> value indicating whether you want to use the default Oracle mount point or not.
Home directory of the OS user of the database	Example:/opt/ora/oracledb	OS user home directory ( default is /opt/ora/oracledb).
Oracle database redolog location	Example:/opt/ora/oracledb/redo	Location of the database redologs. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Oracle database data files location	Example:/opt/ora/oracledb/oradata/anadb	Location of the database data files. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Oracle database backup location	Example:/opt/ora/oracledb/backup	Location of the database backup files. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Oracle database archive location	Example:/opt/ora/oracledb/arch	Location of the database archive files. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Prime Network OS user	<i>pnuser</i>	User-defined Prime Network OS user ( <i>pnuser</i> ). Username must start with a letter and contain only the following characters: [A-Z a-z 0-9].
Prime Network file system mount point	Example: /export/home/ana	Location of the mount point for Prime Network.

**Table 4-4 Installation Prompts for Geographical Redundancy Only (continued)**

Prompt for.	Enter...	Notes
Home directory of the Prime Network user	Example: /export/home/ana/pn41	Directory should be located under <i>Prime Network file system mount point</i> but not the mount point itself.
Prime Network user password	<i>password</i>	User-defined password for the <i>pnuser</i> .
Location of the Prime Network installation file	Example: /dvd/Server	Mount point of Prime Network installation. Should be the same for all relevant nodes. Example: For <b>install.pl</b> the path will be /dvd/Server.
Directory for the Oracle zip files	Example: /opt/ora/oracle_zip	Directory containing the embedded Oracle zip files. Can be a temporary location where the files were copied from the installation DVDs; or directly specify the location on DVD.
Node one password	node1 password	Root user password for the node running the installation. For local redundancy dual-node clusters, this node must be one of the cluster nodes.
DR node name	DR hostname	For geographic redundancy, hostname for the remote site (the value returned by the system call <code>hostname</code> ).
DR node password	DR node password	For geographic redundancy, root user password for the remote site.
DB profile	The number corresponding to the DB profile required.	Select from 1-7 (estimated DB profile).
Password for 5 built-in users	<i>password</i>	<p>Password for Prime Network root, bosenable, bosconfig, bosusermngr, and web monitoring users (users for various system components). Passwords must contain:</p> <ul style="list-style-type: none"> <li>• Contain at least eight alphanumeric characters.</li> <li>• Contain upper and lower case letters.</li> <li>• Contain one number and one special character.</li> <li>• Cannot contain: @ / ! \$ ~ * ( ) - + = [ {</li> </ul>
SMTP server	Example: outbound.cisco.com	Local e-mail server.
User email	<i>email address</i>	E-mail address to which embedded database will send error messages.
Run database backups?	Y/N	Whether to enable embedded database automated backups.
Public network interface	Example: eth0	Name of network interface to which logical IPs will be added. Must be identical on all servers (for example: eth0, bge0).

Table 4-5 shows the installation prompts when setting up local and geographical redundancy.

**Table 4-5 Installation Prompts for Local and Geographical Redundancy**

Prompt for...	Enter...	Notes
Configure local HA?	yes	Enter <b>yes</b> ; this procedure is for geographical redundancy + local redundancy. To install geographical only, see <a href="#">Table 4-4</a> . To install local redundancy, see <a href="#">Installing and Maintaining Gateway Local Redundancy, page 3-1</a>
Configure DR?	yes	—
Is NTP configured on the 3 gateways (local and remote)?	yes	<b>yes</b> or <b>no</b> depending on whether NTP should be configured on three gateways. If not configured, first configure NTP and then continue with the installation. For more details on procedures, see configuring NTP in the <a href="#">Cisco Prime Network 4.3 Installation Guide</a> .
OS user of the database	oracledb	Oracle installation owner (default is oracle).
Configuring multipath	no	Answer <b>yes</b> if the node is connected to storage with more than one connection (recommended).
Oracle file system mount point	Example:/opt/ora/oracle	Location of the mount point given for the <i>oracle-home</i> or <i>oracle-user</i> .
Configure another oracle file system mount	no	<b>yes</b> or <b>no</b> value indicating whether you want to use the default Oracle mount point or not.
Home directory of the OS user of the database	Example:/opt/ora/oracledb	OS user home directory ( default is /opt/ora/oracledb).
Oracle database redolog location	Example:/opt/ora/oracledb/redo	Location of the database redologs. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Oracle database data files location	Example:/opt/ora/oracledb/oradata/anadb	Location of the database data files. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Oracle database backup location	Example:/opt/ora/oracledb/backup	Location of the database backup files. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Oracle database archive location	Example:/opt/ora/oracledb/arch	Location of the database archive files. Should be located under one of the Oracle mounts but not directly on the mount, and should be compliant with the storage requirements.
Prime Network OS user	<i>pnuser</i>	User-defined Prime Network OS user ( <i>pnuser</i> ). Username must start with a letter and contain only the following characters: [A-Z a-z 0-9].

**Table 4-5 Installation Prompts for Local and Geographical Redundancy**

Prompt for.	Enter...	Notes
Prime Network file system mount point	Example: /export/home/ana	Mount point of Prime Network installation.
Home directory of the Prime Network user	Example: /export/home/ana/pn41	Directory should be located under <i>Prime Network file system mount point</i> but <i>not</i> the mount point itself.
Prime Network user password	<i>password</i>	User-defined password for the <i>pnuser</i> .
Location of the Prime Network installation file	Example: /dvd/Server	The mount point of the Prime Network installation. The mount point should be the same for all relevant nodes. Example: For <b>install.pl</b> the path will be /dvd/Server.
Directory for the Oracle zip files	Example: /opt/ora/oracle_zip	Directory containing the embedded Oracle zip files. Can be a temporary location where the files were copied from the installation DVDs; or directly specify the location on DVD.
Node one password	node1 password	Root user password for the node running the installation. For local redundancy dual-node clusters, this node must be one of the cluster nodes.
DR node hostname	DR hostname	For geographic redundancy, hostname for the remote site . This is the value returned by the system call hostname.
DR node password	DR node password	For geographic redundancy, root user password for the remote site.
DB profile	The number corresponding to the DB profile required.	Select from 1-7 (estimated DB profile).
Password for 5 built-in users	<i>password</i>	Password for Prime Network root, bosenable, bosconfig, bosusermgr, and web monitoring users (users for various system components). Passwords must contain: <ul style="list-style-type: none"> <li>• Contain at least eight alphanumeric characters.</li> <li>• Contain upper and lower case letters.</li> <li>• Contain one number and one special character.</li> <li>• Cannot contain: @ / ! \$ ~ * ( ) - + = [ {</li> </ul>
SMTP server	Example: outbound.cisco.com	Local e-mail server.
User email	email address	E-mail address to which embedded database will send error messages.
Oracle service IP address	IP address	Logical IP of Oracle service group.
Prime Network service IP address	IP address	Logical IP of Prime Network service group.

**Table 4-5** Installation Prompts for Local and Geographical Redundancy

Prompt for...	Enter...	Notes
Multicast address for the cluster nodes	IP address	An available multicast address accessible and configured for both cluster nodes.
Prime Network cluster name	<i>username</i>	User-defined cluster name. Cannot be more than 15 non-NUL (ASCII 0) characters. For local redundancy, cluster name must be unique within the LAN.
Node one fence agent	The number corresponding to the fencing agent required	Type of fencing device configured for the node running the installation. (See <a href="#">Fencing Options, page 2-3</a> .)
Node two fence agent	The number corresponding to the fencing agent required	Type of fencing device configured for the second cluster running the installation. (See <a href="#">Fencing Options, page 2-3</a> .)
Prime Network cluster web interface password	port number and password	Port and the password for cluster web interface. <i>LUCI_PORT</i> must be available and should not be in Prime Network debug range: $60000 \leq x < 61000$ or in Prime Network AVM port range: $2000 \leq x < 3000$ or $8000 \leq x < 9000$ Password must contain at least 6 characters.
Prime Network cluster web interface port		
Node one IP	node1 IP address	IP address of the node running the installation. Local redundancy dual-node clusters: Must be one of the cluster nodes.
DR node IP	DR node IP address	IP address of DR node at remote site (geographical redundancy).
Run database backups?	Y/N	Whether to enable embedded database automated backups.
Public network interface	Example: eth0	Name of network interface to which logical IPs will be added. Must be identical on all servers (for example: eth0, bge0).
Node one fence hostname	hostname	Hostname of fencing device configured for node running the installation (for some fencing devices, this can be an IP address).
Node one fence login	login name	Login name for fencing device configured for node running the installation.
Node one fence passwd	password	Password for fencing device configured for node running the installation.
Node two fence hostname	hostname	Hostname of fencing device configured for second cluster node (for some fencing devices, this can be an IP address).

**Table 4-5 Installation Prompts for Local and Geographical Redundancy**

Prompt for.	Enter...	Notes
Node two fence login	login name	Login name for fencing device configured for second cluster node.
Node two fence passwd	password	Password for fencing device configured for node second cluster node.

**Step 5** Configure the Embedded Database by running the **add\_emdb\_storage.pl** utility and you must include **-ha** flag while running this utility.

- a. Log in as prime network user

```
su - pnuser
```

- b. Change directories to *NETWORKHOME/Main/scripts/embedded\_db* and enter the following command:

```
./add_emdb_storage.pl -ha
```

- c. Enter the number corresponding to the estimated database profile that meets your requirement.
- d. Insert the event and workflow archiving size in days.

**Step 6** Configure the remote site using the **setup\_Prime\_DR.pl** command in interactive or non-interactive mode. For more information on **setup\_Prime\_DR.pl** script, see [Installation DVDs, page 1-1](#).



**Note** The **setup\_Prime\_DR.pl** script must run on the node running the primary database.

- **For Interactive Installation:**

For interactive mode, enter the following commands:

```
cd /tmp/RH_ha
perl setup_Prime_DR.pl
```

- **For Non- Interactive Installation (Automatic):**

- a. Edit the *auto\_install\_RH.ini* file template found under the *RH\_ha* directory with all of the installation details.

- b. Run the following command:

```
cd /tmp/RH_ha
perl setup_Prime_DR.pl -autoconf auto_install_RH.ini full path
```

Example: perl **setup\_Prime\_DR.pl** -autoconf /tmp/RH\_dr/ *auto\_install\_RH.ini*



**Note** If the **setup\_Prime\_DR.pl** script is executed from the same node as the **install\_Prime\_HA.pl** script, and if all the parameters are same, you can use the same *auto\_install\_RH.ini* file. The prompts and outputs while executing this script are a subset of the install script prompts.

**Step 7** Verify the setup as described in [Verifying the Geographical Redundancy Setup, page 4-14](#).

After the **setup\_Prime\_DR.pl** script is completed:

**Verifying the Geographical Redundancy Setup**

- The Prime Network and embedded database files are replicated to the remote site.
- All utility scripts are located under /var/adm/cisco/prime-network/scripts/ha/util/.

# Verifying the Geographical Redundancy Setup

**Table 4-6** shows the geographical redundancy verification tests.



**Note** The geographical redundancy verification tests are for the embedded database and must be performed by Cisco personnel only.

**Table 4-6 Geographical Redundancy Verification Tests**

Description	Procedure	Expected Results
<b>Database Replication</b>		
<b>Name:</b> tnsping Test: Primary to remote site	From the primary DB server enter the following as the OS Oracle UNIX user:  <b>tnsping anadb</b> <b>tnsping anadb_sb</b>	Verify that the TNS connection on port 1521 is available between the two database servers.
<b>Purpose:</b> Verify tnsping from the primary to the remote site.		
<b>Name:</b> tnsping Test: remote site to Primary	From the standby database server enter the following as the as Oracle UNIX user:  <b>tnsping anadb</b> <b>tnsping anadb_sb</b>	Verify that the TNS connection on port 1521 is available between the two database servers.
<b>Purpose:</b> Verify tnsping from the remote site to the primary site.		
<b>Name:</b> Get the <i>pnuser_admin</i> Password	As the Prime Network UNIX user, enter:  <b>cd NETWORKHOME/Main</b> <b>./runRegTool.sh localhost get persistency/nodes/admin/PASS</b>	Derive the password for <i>pnuser_admin</i> database user from the registry for creating db_links.
<b>Purpose:</b> Get the <i>pnuser_admin</i> login password from the registry for later tests.		
<b>Name:</b> Replication Test	1. On the primary database server, connect to sqlplus as <i>pnuser_admin</i> , then enter the following:  <b>CREATE TABLE NETWORK_TEST REP (NUM NUMBER);</b> <b>INSERT INTO NETWORK_TEST REP VALUES(1);</b> <b>COMMIT;</b> <b>ALTER SYSTEM SWITCH LOGFILE;</b>	The table and data are replicated
<b>Purpose:</b> Verify the object and data replication.	2. On the standby database server, connect to sqlplus as <i>pnuser_admin</i> and query this table:  <b>SELECT * FROM NETWORK_TEST REP;</b>	

**Table 4-6 Geographical Redundancy Verification Tests (continued)**

Description	Procedure	Expected Results
<b>Name and Purpose:</b> Create Database Links on the Primary Database <b>Note</b> Perform this step once, after installing RHEL. Do not repeat this step when verifying the setup after a switchover or failover.	Connect to sqlplus as the <i>pnuser_admin</i> , then enter the following: <pre>CREATE DATABASE LINK TO_anadb_sb CONNECT TO pnuser_ADMIN IDENTIFIED BY pnuser_admin_password USING 'anadb_sb'; CREATE DATABASE LINK TO_anadb CONNECT TO pnuser_ADMIN IDENTIFIED BY pnuser_admin password USING 'anadb';</pre>	The database link is created.
<b>Name:</b> Query Replication SCN Gap. <b>Purpose:</b> Verify that an SCN gap is not growing between the two databases.	<ol style="list-style-type: none"> <li>1. Connect to sqlplus as <i>pnuser_admin</i>.</li> <li>2. Run the following query several times to verify gap is not growing:  <pre>with v1 as (select current_scn anadb_sb_SCN from v\$database@TO_anadb_sb), v2 as (select current_scn anadb_SCN from v\$database@TO_anadb) select v1.anadb_sb_SCN anadb_sb_SCN,v2.anadb_SCN anadb_SCN,v1.anadb_sb_SCN-v2.anadb_SCN "SCN GAP" from v1,v2;</pre> </li> </ol>	Run the query several times to verify the gap is not growing. The SCN gap should be less than 100,000.
<b>Name:</b> Replication is running <b>Purpose:</b> Verify the file replication process is running correctly by checking the monitoring log files under the Prime Network home directory.	Check the following log files under <i>NETWORKHOME</i> . <ul style="list-style-type: none"> <li>• <i>NETWORKHOME/.replication</i>—A time stamp file is created on the primary Prime Network node.</li> <li>• <i>NETWORKHOME/.replication_remote</i>—A time stamp file is created on the primary Prime Network node and replicated to the remote Prime Network node and back again. This will hold the time stamp of the last Prime Network file replication.</li> <li>• <i>NETWORKHOME/.replication_log</i>—Log file created by the Prime Network replication monitoring. It will be empty if all is considered OK (the difference between the time stamp files is within range).</li> <li>• <i>NETWORKHOME/oracle_monitor.log</i>—Remote database monitoring log.</li> </ul>	The replication is running correctly.
<b>File Replication</b>		
<b>Name:</b> File replication <b>Purpose:</b> Verify the file replication process.	<ol style="list-style-type: none"> <li>1. Create a file under <i>NETWORKHOME</i> by entering:  <code>touch filename</code></li> <li>2. Verify that the file is created on the geographical remote node.</li> <li>3. Remove the file and verify that the file is removed on the remote node.</li> </ol>	The file is created and removed. <b>Note</b> File replication from primary to geographical remote node takes some time.

**Table 4-6** Geographical Redundancy Verification Tests (continued)

Description	Procedure	Expected Results
<b>Name:</b> Replication is running <b>Purpose:</b> Verify the file replication process is running correctly by checking the monitoring log files under the Prime Network home directory.	Check the following log files under NETWORKHOME. <ul style="list-style-type: none"> <li>• <i>NETWORKHOME/.replication</i>—A time stamp file is created on the primary Prime Network node.</li> <li>• <i>NETWORKHOME/.replication_remote</i>—A time stamp file is created on the primary Prime Network node and replicated to the remote Prime Network node and back again. This will hold the time stamp of the last Prime Network file replication.</li> <li>• <i>NETWORKHOME/.replication_log</i>—Log file created by the Prime Network replication monitoring. It will be empty if all is considered OK (the difference between the time stamp files is within range).</li> <li>• <i>NETWORKHOME/oracle_monitor.log</i>—Remote database monitoring log.</li> </ul>	The replication is running correctly.

**Key Files for Geographical Redundancy**

<b>Name:</b> Checking the key files under Prime Network and Oracle home directories. <b>Purpose:</b> Verify that the both the remote site and primary sites are properly marked with key files under the Prime Network and oracle home directories.	Check the following files under NETWORKHOME (Prime Network Home directory) and Oracle home directories. <ul style="list-style-type: none"> <li>• .local_ana</li> <li>• .remote_ana</li> <li>• .local_db</li> <li>• .remote_db</li> </ul>	Key files should be under Prime Network and Oracle home directory.
--	--	--

## Maintaining Geographical Redundancy

These topics provide information pertaining to ongoing management of an ADG geographical redundancy configuration. The utilities used for these operations are stored in /var/adm/cisco/prime-network/scripts/ha/util.

This section includes:

- [Checking Log Messages, page 4-16](#)
- [Monitoring Overall Status, page 4-17](#)

## Checking Log Messages

Prime Network generates the following system events for geographical redundancy monitoring:

- **Informational event** to indicate that both ADG and GWSync monitoring is active. This is done on an hourly basis based on cron jobs.
- **Critical events** when the following occur:
  - An GWSync has not occurred in the last 10 minutes.
  - The standby database is down.

- The standby database is up but has been out of sync for 60 minutes.

The log files for data replication are described in the following table. To troubleshoot problems with the replication process, see [Verifying the Geographical Redundancy Setup, page 4-14](#).

Log File	Description
<i>NETWORKHOME/.replication</i>	Contains the local and remote timestamps used by GWSync.
<i>NETWORKHOME/.replication_remote</i>	
<i>NETWORKHOME/.replication_log</i>	This log is only populated if the GWSync local and remote timestamps are more than 10 minutes apart (and a System event is generated), as in the following example:  Replication failed since: date
<i>NETWORKHOME/oracle_monitoring.log</i>	Information on the Redo-apply log from the standby server.  + Testing the replication state on the remote database  - Redo transport lag: NAME VALUE TIME_COMPLETED ----- transport lag +00 00:00:00 04/14/2013 10:30:34  - Redo apply lag: NAME VALUE TIME_COMPLETED ----- apply lag +00 00:00:00 04/14/2013 10:30:35  - Active apply rate: ITEM UNITS SO FAR ----- Active Apply Rate KB/sec 286  - Data base role: PHYSICAL STANDBY

## Monitoring Overall Status

The **primeha** command is a central utility for checking the status of the high availability nodes, performing switchovers and failovers, and stopping and resuming data replication.

Use the following command to view the status of the cluster:

```
perl primeha -status
```

The below output is an example for a network that has both local and geographical redundancy.

- The first portion of the output as shown below, shows the status of the geographical redundancy configuration. The server hostname1.cisco.com is the remote gateway and database server. The server hostname2.cisco.com is the other node in the local redundancy cluster and is not running any service.

```
- Installing Perl-5.16.0-x86_64-linux-thread-multi
  Log can be found at
  /var/adm/cisco/prime-network/scripts/ha/util/perlForHA/installPerlForHA-1365070277.log
```

HOST	ANA SERVICE	ORACLE SERVICE
hostname.cisco.com	Active Prime Network	Active oracle local
hostname1.cisco.com	Standby Prime Network	Standby oracle

## ■ Uninstalling the Geographical Redundancy Software

```
hostname2.cisco.com    Prime Network not running on this node    oracle not running on
this node
```

- The second portion of the output as shown below (that begins with Cluster Status) shows the status of the local redundancy configuration. (This is displayed because this setup also contains a local redundancy configuration.)

```
Cluster Status for ana_cluster @ Mon Aug  1 12:34:40 2013
Member Status: Quorate
```

Member Name	ID	Status
hostname.cisco.com	1	Online, Local, rgmanager
hostname2.cisco.com	2	Online, rgmanager
Service Name	Owner (Last)	State
service:ana	hostname.cisco.com	started
service:oracle_db	hostname.cisco.com	started

## Uninstalling the Geographical Redundancy Software

To uninstall geographical redundancy, use this procedure. If Operations Reports was also installed, this procedure will remove it.

If your deployment also has local redundancy, uninstall the software on the primary cluster server (P1) first using the procedure in [Uninstalling Local Redundancy, page 3-28](#).

- 
- Step 1** If any RHCS services are running, log into the primary cluster server and freeze the relevant services (service can be **ana**, **oracle**, and, if Operations Reports is installed, **ifb**).

```
clusvcadm -z service
```

- Step 2** Log in as the root user and change to the following directory:

```
cd /var/adm/cisco/prime-network/reg/pnuser
```

- Step 3** Enter the following command:

```
perl uninstall.pl
```

---

## Installing and Configuring PN-IL for Local + Geographical Redundancy

This section explains how to install the Prime Network Integration Layer (PN-IL) 1.2 for a local + geographical redundancy deployment. It also explains how to integrate the deployment with Cisco Prime Central. For information on the Prime Central releases with which you can integrate PN-IL 1.2, see the [Cisco Prime Network 4.3 Release Notes](#).

These topics provide the information you will need to install and configure PN-IL geographical, and local redundancy:

- [Installation DVD, page 4-19](#)

- Steps for Installing PN-IL with Local + Geographical Redundancy, page 4-19
- Installing PN-IL on a Prime Network Server (Local + Geographical Redundancy), page 4-20
- Configuring PN-IL on a Prime Network Gateway (Local + Geographical Redundancy), page 4-22
- Disabling the PN-IL Health Monitor, page 4-26

If you want to migrate an *existing* standalone installations of PN-IL (local + geographical) to suite mode, you can use the procedure in [Configuring and Migrating PN-IL with Prime Central \(Suite Mode with Local + Geographical Redundancy\)](#), page 4-23.

## Installation DVD

The PN-IL high availability files are provided on the Prime Network installation DVD named **Disk 1: New Install DVD**. **Disk 2** contains the tar file **sil-esb-1.2.0.tar.gz**, which contains the PN-IL installation files and scripts, including:

- `installAndConfigureESB.sh`—PN-IL installation script
- `itgctl`—PN-IL configuration script
- `il-watch-dog.sh`—PN-IL health monitor control script
- `DMSwitchToSuite.sh`—Script to migrate to suite

## Steps for Installing PN-IL with Local + Geographical Redundancy

[Table 4-7](#) provides the basic steps you must follow to set up local + geographical redundancy for PN-IL. If you want to migrate an *existing* standalone installations of PN-IL (local + geographical) to suite mode, you can use the procedure in [Configuring and Migrating PN-IL with Prime Central \(Suite Mode with Local + Geographical Redundancy\)](#), page 4-23.

Note that you only have to install PN-IL on the primary cluster server (P1), not on the remote (DR) server (S2). However, you will have to do some configuration tasks on the remote server.

**Table 4-7** Steps for Setting Up PN-IL Local + Geographical Redundancy

Task	Topic/Action Required	Local Cluster		Remote(DR) Server	
		Server (P1) (has Primary database)	Server (P2)	Remote Server (S1)	
<b>Step 1</b>	Collect server details, so that you have all information handy prior to installation.	<ul style="list-style-type: none"> <li>Virtual IP address of P1</li> <li>IP Address of remote DR server S1</li> <li>Prime Network application root username and password for primary cluster and remote DR servers (P1 and S1)</li> <li>URL for authenticating Prime Network calls for P1 and S1 (normally <a href="https://localhost:6081/ana/services/userman">https://localhost:6081/ana/services/userman</a>)</li> <li>((Suite mode) For the Prime Central server where Oracle is installed: Hostname, database service name, database username and password, and database port.</li> </ul>	x	—	—
<b>Step 2</b>	Verify the server meets the prerequisites.	<a href="#">Installation Requirements for Geographical Redundancy, page 4-4</a>	x	—	—
<b>Step 3</b>	Freeze RHCS and install PN-IL.	<a href="#">Installing PN-IL on a Prime Network Server (Local + Geographical Redundancy), page 4-20</a>	x	—	—
<b>Step 4</b>	Configure PN-IL (in standalone or suite mode) on both nodes, and unfreeze RHCS.	<a href="#">Configuring PN-IL on a Prime Network Gateway (Local + Geographical Redundancy), page 4-22</a>	x	—	x
<b>Step 5</b>	Disable the PN-IL Health Monitor.	<a href="#">Disabling the PN-IL Health Monitor, page 4-26</a>	x	—	x

## Installing PN-IL on a Prime Network Server (Local + Geographical Redundancy)

Use this procedure to install PN-IL with local + geographical redundancy on the primary cluster server (P1). The primary cluster node will copy the necessary files to the remote DR node (S1). For the remote DR node, you only have to perform some minor configurations.

### Before You Begin:

Make sure Prime Network is installed and is up and running on the both the primary cluster node (P1) and the remote DR node (S2). In the following procedure, \$ANAHOME is the *pnuser* environment variable for the Prime Network installation directory (/export/home/pnuser by default).

- 
- Step 1** On the primary cluster node (P1), log in as root and freeze the ana service.



**Note** The cluster server should be the active node where the ana service is running.

```
ssh root@active-cluster-node
clusvcadm -Z ana
```

- Step 2** On the remote DR node (S1), log in as root and save your rsync settings so they are not overwritten during the PN-IL installation process.

```
ssh root@remote-DR-node-name
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt rsync_exclude_pnil.txt.org
mv rsync_exclude_pnil_cfg.txt rsync_exclude_pnil_cfg.txt.org
```

- Step 3** On the primary cluster node (P1), log in as *pnuser*.

```
su - pnuser
```

For example:

```
su - pn41
```

- Step 4** On the primary cluster node, create an installation directory for PN-IL.

```
mkdir -p $ANAHOME/new-pnil-dir
```

For example, if the Prime Network installation directory was /export/home/pn41, you would run this command to create an installation directory called pnil:

```
mkdir -p $ANAHOME/pnil
```

- Step 5** On the primary cluster node (P1), copy the installation files from the installation DVD, extract them, and start the installation script. These examples use the PN-IL installation directory /pnil.

- Copy the PN-IL installation tar file from Disk 2 to the directory you created in [Step 4](#). In the following example, the installation directory is named **pnil**.

```
cp /tmp/sil-esb-1.2.0.tar.gz $ANAHOME/pnil
```

- Change to the directory you created in [Step 4](#) and extract the files from the PN-IL installation tar:

```
cd $ANAHOME/pnil
tar -zxf sil-esb-1.2.0.tar.gz
```

- Change to directory where the installation tar files were extracted and run the installation script:

```
cd sil-esb-1.2.0/install/packages
./installAndConfigureEsb.sh
```

- Step 6** On the primary cluster node (P1), reload the user profile.

```
source $ANAHOME/.cshrc
```

- Step 7** Log into the remote DR server (S1) as root and move the original rsync exclude file (that you moved in [Step 2](#)) back to its proper place.

```
ssh root@remote-DR-server
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt.org rsync_exclude_pnil.txt
mv rsync_exclude_pnil_cfg.txt.org rsync_exclude_pnil_cfg.txt
```

- Step 8** Configure PN-IL as described in [Configuring PN-IL on a Prime Network Gateway \(Local + Geographical Redundancy\)](#), page 4-22.

**Note**

Do not unfreeze the ana service until PN-IL has been configured.

**Note**

You do not have to install the geographical redundancy files on the remote server (S1); the necessary files will be copied to the remote DR server by the primary cluster node.

## Configuring PN-IL on a Prime Network Gateway (Local + Geographical Redundancy)

Configuration tasks must be performed on both the primary cluster node (P1) and the remote DR node (S1).

- For standalone mode (that is, Prime Network is not integrated with Prime Central), follow the instructions in [Configuring PN-IL with Prime Network \(Standalone Mode with Local + Geographical Redundancy\), page 4-22](#).
- For suite mode (Prime Network is integrated with Prime Central), follow the instructions in [Configuring and Migrating PN-IL with Prime Central \(Suite Mode with Local + Geographical Redundancy\), page 4-23](#).

### Configuring PN-IL with Prime Network (Standalone Mode with Local + Geographical Redundancy)

In standalone mode, Prime Network is not integrated with Prime Central and can independently expose MTOSI and 3GPP web services to other OSS/applications. In the following procedure:

- \$PRIMEHOME is the *pnuser* environment variable for the PN-IL installation directory you created in [Installing PN-IL on a Prime Network Server \(Local + Geographical Redundancy\), page 4-20](#).
- \$ANAHOME is the *pnuser* environment variable for the Prime Network installation directory (/export/home/pnuser by default).

**Step 1** From the primary cluster node (P1), log in as *pnuser*.

**Step 2** On the primary cluster node (P1), configure PN-IL in standalone mode.

```
itgctl config 1 --anaPtpServer ana-cluster-ip --anaPtpUser pn-root-user --anaPtpPw
pn-root-user-password --authURL network-authentication-URL
```

**itgctl** uses these arguments.

Argument	Description
<i>ana-cluster-ip</i>	<ul style="list-style-type: none"> <li>• When run on the primary cluster node (P1), this is the IP address of the primary cluster server.</li> <li>• When run on the remote DR node, this is the IP address of the remote DR server.</li> </ul>
<i>pn-root-user</i>	Name of Prime Network root user (usually <b>root</b> )

Argument	Description
<i>pn-root-user-password</i>	Password for Prime Network root user
<i>network-authentication-URL</i>	URL used to authenticate Prime Network calls (usually <a href="https://localhost:6081/ana/services/userman">https://localhost:6081/ana/services/userman</a> )

For example:

```
itgctl config 1 --anaPtpServer 192.0.2.22 --anaPtpUser root --anaPtpPw myrootpassword
--authURL https://192.0.2.22:6081/ana/services/userman
```

**Step 3** On the primary cluster node (P1), start PN-IL.

```
$PRIMEHOME/bin/itgctl start
```

**Step 4** Open a new session on the remote DR server (S1) and log in as *pnuser*.

**Step 5** On the remote DR server (S1), configure PN-IL in standalone mode but use the *remote DR server's IP address* (**--anaPtpServer** *remote-DR-ip*).

```
itgctl config 1 --anaPtpServer remote-DR-server-ip --anaPtpUser pn-root-user --anaPtpPw
pn-root-user-password --authURL network-authentication-URL
```

**Step 6** On the primary cluster node (P1), start PN-IL.

```
$PRIMEHOME/bin/itgctl start
```



**Note**

To avoid the automatic start of PN-IL on the DR server, disable the PN-IL Health monitor, and stop the PN-IL service on that server, using the following command:

```
$PRIMEHOME/local/scripts/il-watch-dog.sh disableandstop.
```

**Step 7** On the primary cluster node, log in as the operating system root user and unfreeze the ana service.

```
clusvcadm -U ana
```

**Step 8** To enable NBI, contact Cisco representative.

---

Next, perform the necessary configuration steps that are described in [Configuring PN-IL on a Prime Network Gateway \(Local + Geographical Redundancy\)](#), page 4-22.

## Configuring and Migrating PN-IL with Prime Central (Suite Mode with Local + Geographical Redundancy)

When Prime Network and PN-IL are running in *suite mode*, that means they are integrated with Prime Central. This procedure explains how to integrate PN-IL with a deployment of Prime Central that uses geographical redundancy. You can use this procedure for:

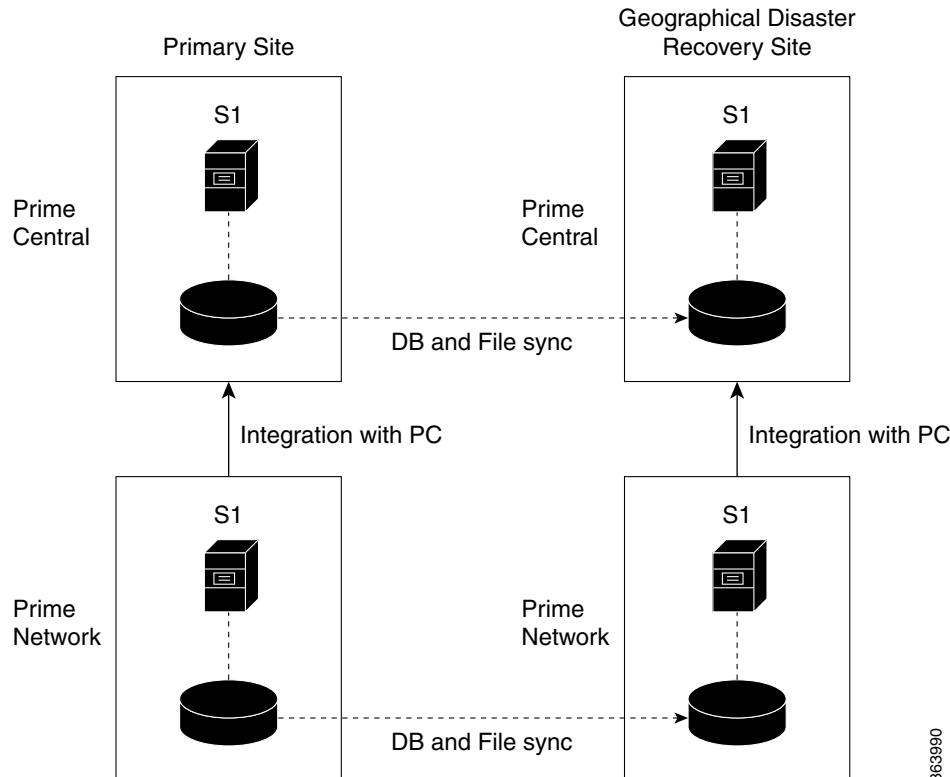
- New installations of PN-IL with geographical redundancy.
- Existing standalone installations of PN-IL with geographical redundancy, that you want to move from standalone to suite mode.

[Figure 4-1](#) illustrates the deployment of both local and geographical redundancy in Suite Mode.



PN-IL geographical redundancy is only supported when the deployment also has local redundancy. Therefore, Prime Central must also be using both local and geographical redundancy.

**Figure 4-1 Local Redundancy with Geographical Redundancy Suite Mode**



In the following procedure, \$PRIMEHOME is the *pnuser* environment variable for the PN-IL installation directory you created in [Installing PN-IL on a Prime Network Server \(Local + Geographical Redundancy\), page 4-20](#).

### Before You Begin

Before you begin, verify the following:

- PN-IL is already installed. If it is not, install it as described in [Installing and Configuring PN-IL for Local + Geographical Redundancy, page 4-18](#).
- Prime Network is running suite mode.
- Prime Central is using both local geographical redundancy.

To integrate PN-IL with Prime Central:

- 
- Step 1** From the Prime Network primary cluster node (P1), log in as *pnuser*.
  - Step 2** On the Prime Network primary cluster node (P1), configure PN-IL in suite mode, edit the necessary integration files, and run the integration script:
    - a. Move to the PN-IL integration directory.

```
cd $PRIMEHOME/integration
```

- b. Edit the **ILIntegrator.prop** file and change the value of the ‘HOSTNAME’ property to ana-cluster-ana, which is the fixed name for the Prime Network cluster server.

```
HOSTNAME=ana-cluster-ana
```

- c. Execute the following integration script to integrate PN-IL with Prime Central. Prime Central will assign an ID number to PN-IL. Note the ID number because you will need it later to integrate the remote DR server (S1) with Prime Central.



**Note** When you run DMIntegrator.sh, you must exactly follow the format below or the script will fail.

```
./DMIntegrator.sh -a ILIntegrator.prop prime-central-db-hostname
prime-central-db-service-name prime-central-db-user prime-central-db-user-password
prime-central-port-number
```

**DMIntegrator** uses these variables. You must enter them in this exact order.

DMIntegrator.sh Variable	Description
<i>prime-central-server-hostname</i>	Specifies the IP address of the Prime Central database server
<i>prime-central-db-service-name</i>	Specifies the name of Prime Central database service
<i>prime-central db-user</i>	Specifies the name of Prime Central database user (usually <b>primedba</b> )
<i>prime-central-db-user-password</i>	Specifies the password for Prime Central database user
<i>prime-central-db-port</i>	Specifies the port for Prime Central database (usually <b>1521</b> )

Example:

```
./DMIntegrator.sh -a ILIntegrator.prop 10.10.10.10 primedb primedba mypassword 1521
```

- Step 3** On the Prime Network primary cluster node (P1), reload the user profile:

```
source $PRIMEHOME/.cshrc
```

- Step 4** On the Prime Network primary cluster node (P1), retrieve the ID that Prime Central assigned to Prime Network using **itgctl list**. You will need it in a future step.

```
$PRIMEHOME/bin/itgctl list
```

- Step 5** Open a new session to the Prime Network remote DR server (S1) as a root user and rename file as shown below.

```
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt rsync_exclude_pnil.txt.org
mv rsync_exclude_pnil_cfg.txt rsync_exclude_pnil_cfg.txt.org
```

- Step 6** On the Prime Network remote DR server (S1), configure PN-IL in suite mode as *pnuser*. Edit the necessary integration files, and run the integration script.

a. su - *pnuser*

b. Move to the PN-IL integration directory.

```
cd $PRIMEHOME/integration
```

- c. Edit the **ILIntegrator.prop** file and change the value of the ‘HOSTNAME’ property to the Prime Network remote DR server (S1) hostname. For example:

```
HOSTNAME=remote-pn-DR-server
```

- d. Execute the following integration script to integrate PN-IL into the deployment:

```
./DMIntegrator.sh -a ILIntegrator.prop prime-DR-db-server-hostname db-service-name
db-user db-user-password db-port pn-id
```

**DMIntegrator** uses these variables. You must enter them in this exact order.

DMIntegrator.sh Variable	Description
<i>prime-DR-db-server-hostname</i>	IP address of the Prime Central DR database server
<i>db-service-name</i>	Name of Prime Central database service
<i>db-user</i>	Name of Prime Central database user (usually <b>primedba</b> )
<i>db-user-password</i>	Password for Prime Central database user
<i>db-port</i>	Port for Prime Central database (usually <b>1521</b> )
<i>prime-pn-id</i>	Prime Network ID number assigned by Prime Central

Example:

```
./DMIntegrator.sh -a ILIntegrator.prop 10.10.1.11 primedb primedba mypassword 1521 10
```

- Step 7** On the remote DR node (S1), reload the user profile:

```
source $ANAHOME/.cshrc
```

- Step 8** Log out from Prime Network application user and as root user change the following file name

```
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt.org rsync_exclude_pnil.txt
mv rsync_exclude_pnil_cfg.txt.org rsync_exclude_pnil_cfg.txt
```

- Step 9** As the operating system root user, on the primary cluster node (P1), unfreeze the ana service.

```
clusvcadm -U ana
```

---

Next, disable the PN-IL health monitor as described in [Disabling the PN-IL Health Monitor, page 4-26](#).

## Disabling the PN-IL Health Monitor

When PN-IL is installed in a geographical redundancy deployment, the RHCS cluster service monitors PN-IL’s status. Therefore, you should disable the PN-IL health monitor.

To disable the PN-IL health monitor, execute the following command as *pnuser*:

```
$ANAHOME/local/scripts/il-watch-dog.sh disable
```

# Installing and Configuring PN-IL for Geographical Redundancy Only

This section explains how to install the Prime Network Integration Layer (PN-IL) 1.2 for a geographical redundancy only deployment. It also explains how to integrate the deployment with Cisco Prime Central. For information on the Prime Central releases with which you can integrate PN-IL 1.2, see the [Cisco Prime Network 4.3 Release Notes](#).

**Note**

PN-IL geographical redundancy only has a primary server (P1) at the local site and remote server (S1) at a remote geographical site for a full disaster recovery.

These topics provide the information you will need to install and configure PN-IL geographical only deployments:

- [Installation DVD, page 4-19](#)
- [Steps for Installing PN-IL with Geographical Redundancy Only, page 4-27](#)
- [Installing PN-IL on a Prime Network Server \(Geographical Redundancy Only\), page 4-28](#)
- [Configuring PN-IL on a Prime Network Gateway \(Geographical Redundancy Only\), page 4-30](#)
- [Disabling the PN-IL Health Monitor, page 4-26](#)

If you want to migrate an *existing* standalone installations of PN-IL (with geographical redundancy) to suite mode, you can use the procedure in [Configuring and Migrating PN-IL with Prime Central \(Suite Mode with Local + Geographical Redundancy\), page 4-23](#).

## Steps for Installing PN-IL with Geographical Redundancy Only

[Table 4-7](#) provides the basic steps you must follow to set up geographical redundancy only for PN-IL. If you want to migrate an *existing* standalone installations of PN-IL (with geographical redundancy only) to suite mode, you can use the procedure in [Configuring and Migrating PN-IL with Prime Central \(Suite Mode with Local + Geographical Redundancy\), page 4-23](#).

Note that you only have to install PN-IL on the primary server (P1), not on the remote (DR) server (S2). However, you will have to do some configuration tasks on the remote server.

**Table 4-8** Steps for Setting Up PN-IL Geographical Redundancy

	Task	Topic/Action Required	Local Cluster		Remote(DR) Server
			Server (P1) (has Primary database)	Server (P2)	Remote Server (S1)
<b>Step 1</b>	Collect server details, so that you have all information handy prior to installation.	<ul style="list-style-type: none"> <li>IP address of P1</li> <li>IP Address of remote DR server S1</li> <li>Prime Network application root username and password for primary and remote DR servers (P1 and S1)</li> <li>URL for authenticating Prime Network calls for P1 and S1 (normally <a href="https://localhost:6081/ana/services/userman">https://localhost:6081/ana/services/userman</a>)</li> <li>((Suite mode) For the Prime Central server where Oracle is installed: Hostname, database service name, database username and password, and database port.</li> </ul>	X	—	X
<b>Step 2</b>	Verify the server meets the prerequisites.	<a href="#">Installation Requirements for Geographical Redundancy, page 4-4</a>	X	—	—
<b>Step 3</b>	Configure PN-IL (in standalone or suite mode) on both nodes.	<a href="#">Configuring PN-IL on a Prime Network Gateway (Local + Geographical Redundancy), page 4-22</a>	X	—	X
<b>Step 4</b>	Disable the PN-IL Health Monitor.	<a href="#">Disabling the PN-IL Health Monitor, page 4-26</a>	X	—	X

## Installing PN-IL on a Prime Network Server (Geographical Redundancy Only)

Use this procedure to install PN-IL with geographical redundancy on the primary server (P1). The primary node will copy the necessary files to the remote DR node (S1). For the remote DR node, you only have to perform some minor configurations.

### Before You Begin:

Make sure Prime Network is installed and is up and running on the both the primary node (P1) and the remote DR node (S1). In the following procedure, \$ANAHOME is the *pnuser* environment variable for the Prime Network installation directory (/export/home/pnuser by default).

- 
- Step 1** On the remote DR node (S1), log in as root and save your rsync settings so they are not overwritten during the PN-IL installation process.

```
ssh root@remote-DR-node-name
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt rsync_exclude_pnil.txt.org
mv rsync_exclude_pnil_cfg.txt rsync_exclude_pnil_cfg.txt.org
```

- Step 2** On the primary node (P1), log in as *pnuser*.

```
su - pnuser
```

For example:

```
su - pn41
```

- Step 3** On the primary node, create an installation directory for PN-IL.

```
mkdir -p $ANAHOME/new-pnil-dir
```

For example, if the Prime Network installation directory was /export/home/pn41, you would run this command to create an installation directory called pnil:

```
mkdir -p $ANAHOME/pnil
```

- Step 4** On the primary cluster node (P1), copy the installation files from the installation DVD, extract them, and start the installation script. These examples use the PN-IL installation directory /pnil.

- a. Copy the PN-IL installation tar file from Disk 2 to the directory you created in [Step 4](#). In the following example, the installation directory is named **pnil**.

```
cp /tmp/sil-esb-1.2.0.tar.gz $ANAHOME/pnil
```

- b. Change to the directory you created in [Step 4](#) and extract the files from the PN-IL installation tar:

```
cd $ANAHOME/pnil  
tar -zxf sil-esb-1.2.0.tar.gz
```

- c. Change to directory where the installation tar files were extracted and run the installation script:

```
cd sil-esb-1.2.0/install/packages  
.installAndConfigureEsb.sh
```

- Step 5** On the primary node (P1), reload the user profile.

```
source $ANAHOME/.cshrc
```

- Step 6** Log into the remote DR server (S1) as root and move the original rsync exclude file (that you moved in [Step 1](#)) back to its proper place.

```
ssh root@remote-DR-server  
cd /var/adm/cisco/prime-network/scripts/ha/rsync  
mv rsync_exclude_pnil.txt.org rsync_exclude_pnil.txt  
mv rsync_exclude_pnil_cfg.txt.org rsync_exclude_pnil_cfg.txt
```

- Step 7** Configure PN-IL as described in [Configuring PN-IL on a Prime Network Gateway \(Local + Geographical Redundancy\)](#), page 4-22.



**Note** Do not unfreeze the ana service until PN-IL has been configured.



You do not have to install the geographical redundancy files on the remote server (S1); the necessary files will be copied to the remote DR server by the primary node.

## Configuring PN-IL on a Prime Network Gateway (Geographical Redundancy Only)

Configuration tasks must be performed on both the primary node (P1) and the remote DR node (S1).

- For standalone mode (that is, Prime Network is not integrated with Prime Central), follow the instructions in [Configuring PN-IL with Prime Network \(Standalone Mode with Local + Geographical Redundancy\), page 4-22](#).
- For suite mode (Prime Network is integrated with Prime Central), follow the instructions in [Configuring and Migrating PN-IL with Prime Central \(Suite Mode with Local + Geographical Redundancy\), page 4-23](#).

### Configuring PN-IL with Prime Network (Standalone Mode with Geographical Redundancy Only)

In standalone mode, Prime Network is not integrated with Prime Central and can independently expose MTOSI and 3GPP web services to other OSS/applications. In the following procedure:

- \$PRIMEHOME is the *pnuser* environment variable for the PN-IL installation directory you created in [Installing PN-IL on a Prime Network Server \(Local + Geographical Redundancy\), page 4-20](#).
- \$ANAHOME is the *pnuser* environment variable for the Prime Network installation directory (/export/home/pnuser by default).

---

**Step 1** From the primary node (P1), log in as *pnuser*.

**Step 2** On the primary node (P1), configure PN-IL in standalone mode.

```
itgctl config 1 --anaPtpServer ana-primary-ip --anaPtpUser pn-root-user --anaPtpPw
pn-root-user-password --authURL network-authentication-URL
```

**itgctl** uses these arguments.

Argument	Description
<i>ana-primary-ip</i>	<ul style="list-style-type: none"> <li>• When run on the primary cluster node (P1), this is the IP address of the primary server.</li> <li>• When run on the remote DR node, this is the IP address of the remote DR server.</li> </ul>
<i>pn-root-user</i>	Name of Prime Network root user (usually <b>root</b> )
<i>pn-root-user-password</i>	Password for Prime Network root user
<i>network-authentication-URL</i>	URL used to authenticate Prime Network calls (usually <a href="https://localhost:6081/ana/services/userman">https://localhost:6081/ana/services/userman</a> )

For example:

```
itgctl config 1 --anaPtpServer 192.0.2.22 --anaPtpUser root --anaPtpPw myrootpassword
--authURL https://192.0.2.22:6081/ana/services/userman
```

**Step 3** On the primary node (P1), start PN-IL.

```
$PRIMEHOME/bin/itgctl start
```

**Step 4** Open a new session on the remote DR server (S1) and log in as *pnuser*.

- Step 5** On the remote DR server (S1), configure PN-IL in standalone mode but use the *remote DR server's IP address* (`--anaPtpServer remote-DR-ip`).

```
itgctl config 1 --anaPtpServer remote-DR-server-ip --anaPtpUser pn-root-user --anaPtpPw
pn-root-user-password --authURL network-authentication-URL
```

- Step 6** On the primary cluster node (P1), start PN-IL.

```
$PRIMEHOME/bin/itgctl start
```

- Step 7** Enable NBI:

```
cd $PRIMEHOME/install/scripts
./accessconfig.sh nbi enable
```

---

Next, perform the necessary configuration steps that are described in [Configuring PN-IL on a Prime Network Gateway \(Local + Geographical Redundancy\), page 4-22](#).

## Configuring and Migrating PN-IL with Prime Central (Suite Mode with Geographical Redundancy Only)

When Prime Network and PN-IL are running in *suite mode*, that means they are integrated with Prime Central. This procedure explains how to integrate PN-IL with a deployment of Prime Central that uses geographical redundancy only. You can use this procedure for:

- New installations of PN-IL with geographical redundancy.
- Existing standalone installations of PN-IL with geographical redundancy, that you want to move from standalone to suite mode.

In the following procedure, `$PRIMEHOME` is the *pnuser* environment variable for the PN-IL installation directory you created in [Installing PN-IL on a Prime Network Server \(Local + Geographical Redundancy\), page 4-20](#).

### Before You Begin

Before you begin, verify the following:

- PN-IL is already installed. If it is not, install it as described in [Installing and Configuring PN-IL for Local + Geographical Redundancy, page 4-18](#).
- Prime Network is running suite mode. For information on integrating Prime Network with Prime Central, see *Cisco Prime Central Quick Start Guide, 1.3*.
- Prime Central is using both local geographical redundancy.

To integrate PN-IL with Prime Central:

- 
- Step 1** From the Prime Network primary node (P1), log in as *pnuser* and stop prime network integration layer.

```
su - pnuser
$PRIMEHOME/itgctl stop
```

- Step 2** On the Prime Network primary node (P1), configure PN-IL in suite mode, edit the necessary integration files, and run the integration script:

- a. Move to the PN-IL integration directory.

```
cd $PRIMEHOME/integration
```

## ■ Installing and Configuring PN-IL for Geographical Redundancy Only

- b. Execute the following integration script to integrate PN-IL with Prime Central. Prime Central will assign an ID number to PN-IL. Note the ID number because you will need it later to integrate the remote DR server (S1) with Prime Central.



**Note** When you run DMIntegrator.sh, you must exactly follow the format below or the script will fail.

```
./DMIntegrator.sh -a ILIntegrator.prop prime-central-db-hostname
prime-central-db-service-name prime-central-db-user prime-central-db-user-password
prime-central-port-number
```

**DMIntegrator** uses these variables. You must enter them in this exact order.

DMIntegrator.sh Variable	Description
<i>prime-central-server-hostname</i>	Specifies the IP address of the Prime Central database server
<i>prime-central-db-service-name</i>	Specifies the name of Prime Central database service
<i>prime-central db-user</i>	Specifies the name of Prime Central database user (usually <b>primedba</b> )
<i>prime-central-db-user-password</i>	Specifies the password for Prime Central database user
<i>prime-central-db-port</i>	Specifies the port for Prime Central database (usually <b>1521</b> )

Example:

```
./DMIntegrator.sh -a ILIntegrator.prop 10.10.10.10 primedb primedba mypassword 1521
```

- Step 3** On the Prime Network primary cluster node (P1), reload the user profile:

```
source $PRIMEHOME/.cshrc
```

- Step 4** On the Prime Network primary node (P1), retrieve the ID that Prime Central assigned to Prime Network using **itgctl list**. You will need it in a future step.

```
$PRIMEHOME/bin/itgctl list
```

- Step 5** Open a new session to the Prime Network remote DR server (S1) as a root user and rename file as shown below.

```
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt rsync_exclude_pnil.txt.org
mv rsync_exclude_pnil_cfg.txt rsync_exclude_pnil_cfg.txt.org
```

- Step 6** On the Prime Network remote DR server (S1), configure PN-IL in suite mode as *pnuser*. Edit the necessary integration files, and run the integration script.

- a. su - *pnuser*

- b. Move to the PN-IL integration directory.

```
cd $PRIMEHOME/integration
```

- c. Edit the **ILIntegrator.prop** file and change the value of the ‘HOSTNAME’ property to the Prime Network remote DR server (S1) hostname. For example:

```
HOSTNAME=remote-pn-DR-server
```

- d. Execute the following integration script to integrate PN-IL into the deployment:

```
./DMIntegrator.sh -a ILIntegrator.prop prime-DR-db-server-hostname db-service-name
db-user db-user-password db-port pn-id
```

**DMIntegrator** uses these variables. You must enter them in this exact order.

DMIntegrator.sh Variable	Description
<i>prime-DR-db-server-hostname</i>	IP address of the Prime Central DR database server
<i>db-service-name</i>	Name of Prime Central database service
<i>db-user</i>	Name of Prime Central database user (usually <b>primedba</b> )
<i>db-user-password</i>	Password for Prime Central database user
<i>db-port</i>	Port for Prime Central database (usually <b>1521</b> )
<i>prime-PNIL-DMID</i>	Prime Network Integration Layer Domain ID number assigned by Prime Central

Example:

```
./DMIntegrator.sh -a ILIntegrator.prop 10.10.1.11 primedb primedba mypassword 1521 10
```

- Step 7** On the remote DR node (S1), reload the user profile:

```
source $ANAHOME/.cshrc
```

- Step 8** Log out from Prime Network application user and as root user change the following file name

```
cd /var/adm/cisco/prime-network/scripts/ha/rsync
mv rsync_exclude_pnil.txt.org rsync_exclude_pnil.txt
mv rsync_exclude_pnil_cfg.txt.org rsync_exclude_pnil_cfg.txt
```

---

Next, disable the PN-IL health monitor as described in [Disabling the PN-IL Health Monitor, page 4-26](#).

**■ Installing and Configuring PN-IL for Geographical Redundancy Only**