CHAPTER **11**

Upgrading and Rolling Back Prime Network

This section covers tasks on how to upgrade from Prime Network 4.0 and 4.1 to Prime Network 4.2 or roll back from Prime Network 4.2 to Prime Network 4.1. If you want to upgrade from an earlier version of Prime Network, you must first upgrade to Prime Network 4.0 or Prime Network 4.1, and then you can upgrade to Prime Network 4.2.

To upgrade 4.0 from earlier versions of Prime Network use Disk 4 contents. For the upgrade procedure, see Cisco Prime Network 4.0 Installation Guide.

This section contains the following topics:

- Prime Network Upgrade Overview, page 11-1
- Preparing to Upgrade Prime Network (Pre-Upgrade Checklist), page 11-5
- Upgrading to Prime Network 4.2 from 4.0 and 4.1 (Intermediate Steps), page 11-7
- Upgrading to Prime Network 4.2, RHEL 6.5, and Oracle 12, page 11-9
  - Upgrading from RHEL 6.4 with PN 4.1 to RHEL 6.5 with PN 4.2 and Oracle 12, page 11-9
  - Upgrading from RHEL 5.5 - 5.8 to RHEL 6.5 with PN 4.2 and Oracle 12, page 11-10
- Rolling Back to Earlier Prime Network Version, page 11-11
- Upgrading the Prime Network Integration Layer (PN-IL), page 11-13
- Prime Network Post-upgrade Tasks, page 11-16
- Upgrading the Embedded Database to Oracle 12.1.0, page 11-19

Prime Network Upgrade Overview

The upgrade procedure described in this guide can be used to upgrade from Prime Network 4.0 and Prime Network 4.1 to Prime Network 4.2. If you have a previous version of Prime Network, you must first upgrade to Prime Network 4.0 or Prime Network 4.1, and then you can upgrade to Prime Network 4.2.

The upgrade procedure backs up the existing user directory and then adds any new Prime Network 4.2 libraries, files, and code to the existing installation. Any changes to the database are made automatically as part of the upgrade. The majority of your customizations and user-defined information remain intact

and available after upgrading. A list of what is migrated is provided in Table 11-1 on page 11-2.

If Operations Reports is installed, it will be upgraded automatically during the upgrade process.

The amount of time required to upgrade Prime Network depends on your deployment size and system performance. During upgrade, the system will be down. Contact your Cisco account representative for an estimated upgrade duration.

Table 11-1 shows the components affected by the Prime Network upgrade and whether those components are upgraded automatically. If they are not updated automatically, the manual procedure you must perform is provided.

Table 11-1 **Components Affected by the Prime Network Upgrade**

Component	Description	Upgraded Automatically?	Comments
VNE AVMs	avm*.xml files with managed element definitions	Yes	—
Third-party VNE support	Support for non-Cisco VNEs	No	Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 4.2, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.
Database schema changes	Add, change, or remove database schema tables to meet the Cisco Prime Network 4.2 schema definition	Yes	—
Database data preservation	Migrates the old data representation to the Cisco Prime Network 4.2 representation, where applicable	Yes	All tickets and events are available after upgrading. All other data (such as maps, users, and so on) are preserved and migrated.
Database (general)	—	No	You must retain the same database type after migration. In other words, you cannot upgrade from: • A database located on the gateway server to a database located on a remote server (and vice versa) • A customer-provided database to an embedded database.
Users and scopes	—	Yes	All users and scopes are maintained.
Northbound API trap forwarding and SNMP	Out-of-box support for the SNMP trap forwarding mechanism	Yes	The Cisco-EPM-NOTIFICATION-MIB structure includes a running index in the object identifier (OID) suffix, instead of a constant number as in previous releases. The cenAlarmType content was changed in Prime Network 3.8. For details, see the *Cisco Prime Network Integration Developer Guide*.
Northbound API: IMO and BQL	Changes made to information model objects (IMOs)	Yes	**Note** IMOs might change between versions to support new features. For more information, see Cisco Developer Network at: https://developer.cisco.com/site/prime-network/.

Table 11-1   Components Affected by the Prime Network Upgrade (continued)

Component	Description	Upgraded Automatically?	Comments
Customizations: Business objects	—	Yes	Review IMO changes to verify that the OID associated with the business object did not change.
Customizations: Soft properties	Soft properties remain backward compatible and are available in Prime Network 4.2 after upgrading.	Yes	—
Customizations: Command Builder	User-defined commands	Yes	—
Built-in Command Builder scripts	Prime Network built-in activation scripts	Yes	The upgrade procedure updates the built-in changes and removes scripts that are no longer part of the product. See Prime Network Post-upgrade Tasks, page 11-16 to understand which commands require installation after the upgrade.
Customizations: Drools rules	—	Yes	The Post.drl rule is available after upgrading.
Customizations: crontab files	Prime Network crontabs are configured as part of the installation	Yes, if in proper location	If you have user-defined cron jobs, place them in *NETWORKHOME*/local/cron/crontab.user.list. The upgrade will automatically add the user-defined cron jobs. User-defined cron jobs that are not placed in this directory will be removed. See Prime Network Post-upgrade Tasks, page 11-16.
Customizations: External launch points	External launch configuration	Yes	Review IMO changes to verify that the OID associated with the launch command did not change.
Customizations: Message of the Day	Message of the Day configuration	Yes	
Registry	—	Yes	New Prime Network 4.2 registry files are available automatically after the upgrade. Customizable registry files, including avm+.xml and site*, are available and upgraded automatically. Review any customized registry configurations in site.xml and avm*.xml to understand whether they are relevant to Prime Network 4.2. Contact your Cisco account representative, if necessary.
*pnuser*_admin user	User with database administrator permissions who can run maintenance tasks—such as gathering statistics—on the other Prime Network database schemas.	Yes	—

Table 11-1   Components Affected by the Prime Network Upgrade (continued)

Component	Description	Upgraded Automatically?	Comments
Security: SSH and SSL keys	Prime Network SSL keystore and truststore keys, SSH keys, and registry encryption keys	Yes	Prime Network SSL keystore and truststore keys are maintained. These keys are used by all SSL sockets, including BQL and PTP clients. Prime Network SSH keys and registry encryption keys are also maintained.
Prime Network persistency files	Inventory, events, and link persistency data	Yes	All persistency files are available after the upgrade.
Standby units	—	Yes	Standby units complete their upgrade when they are restarted by the gateway (when an active unit goes down and the standby unit is brought online).
GUI client	—	No	If you had an installed client, you need to reinstall it after upgrade. If you access the clients via Web Start, no action is required.
Network Service Activation (NSA)	—	No	Cisco Prime Network Activation functionality is no longer available in Prime Network 4.2. Transaction Manager replaces the Prime Network Workflow and Activation features that were available in previous releases. For details on setting up Transaction Manager, see Setting Up Transaction Manager, page 13-4. For information on how to use Transaction Manager, see the Cisco Prime Network 4.2 Customization Guide.
Change and Configuration Management	Software image and device configuration files	Yes	All the software and device configuration changes are retained as part of the upgrade.
High availability configuration	Upgrades for RHCS/Oracle Active Data Guard gateway high availability	No	If you have gateway high availability, move the Prime Network and Oracle services to maintenance mode before you run the upgrade, then move them back to normal mode after it.
Operations Reports	User-defined reports	Yes	All user defined reports created prior to the upgrade will be available post-upgrade.

Preparing to Upgrade Prime Network (Pre-Upgrade Checklist)

Table 11-2 shows the pre-upgrade tasks that must be performed before upgrading to Prime Network 4.2.

Table 11-2   Gateway Pre-Upgrade Tasks

	Task	**Referred Topic/Action Required**
Step 1	If you are managing third-party devices, make note of them. You will need to give this information to your Cisco representative to enable the support after the upgrade.	Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 4.2, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.
Step 2	Familiarize yourself with the upgrade process and identify areas that may require manual changes.	Components affected by upgrade are listed in Table 11-1.
Step 3	Back up your database and files stored on the gateway. **Note** You will need this data in case you perform a rollback. You can use the script **nccmjobstore.csh** from the installation DVD to obtain the scheduled job information in CSV or HTML format.	External database: • Back up your gateway data by logging into the gateway and running this command from *NETWORKHOME*/Main/scripts: **backup.pl** *backup-folder* • Back up the Oracle database using your Oracle documentation. Embedded database: a. Log into the gateway as *pnuser*. b. Change to the embedded database directory: **# cd $PRIME_NETWORK_HOME/Main/scripts/embedded_db** c. Execute the backup script: **# emdbctl --backup** For information on emdbctl utility used in the below procedure, refer to the Cisco Prime Network 4.2 Administrator Guide.
Step 4	Back up the scheduled CCM job, other applications, and user data.	
Step 5	Apply the database configurations and recommendations.	Preparing the Oracle External Database, page 4-1
Step 6	Verify that the server machines comply with the system hardware and software requirements.	Installation Requirements, page 2-1 Gateway: CPU and Memory Requirements for Different Network Sizes, page 2-3
Step 7	Verify that the backup directory has at least 6000 MB of free space for *pnuser*.	__
Step 8	Verify that the database has at least 8 GB of RAM available (the minimum requirement).	For the database storage sizing guidelines, contact your Cisco account representative.
Step 9	Verify that all required ports are free.	Required Ports for Prime Network, page 2-17.

Table 11-2   Gateway Pre-Upgrade Tasks (continued)

	Task	Referred Topic/Action Required
Step 10	Make sure all database sessions (such as TOAD, SQL, and so on) are closed.	Other TOAD/SQL sessions apart from Prime Network established session should be closed.
Step 11	Place any customized crontab files in *NETWORKHOME*/local/cron/crontab.user.list. User-defined cron jobs that are not placed in this directory will be removed.	—

Step 12	(External database only) Restart Prime Network and the Oracle database.	1. As *pnuser*, stop Prime Network:
		
		`networkctl stop`
		
		2. As *oracle user*, stop and restart Oracle:
		
		`sqlplus`
		`shutdown immediate`
		`startup`
		
		3. As *pnuser*, restart Prime Network:
		
		`networkctl start`

Step 13	Verify that the gateway and units are powered up and connected by opening an SSH session between gateway and all units.	—
Step 14	Verify that Oracle and the Oracle listener are running.	Starting the Oracle Listener (External Database), page 3-6

Step 15	(Only for NAT units) Stop the Prime Network application and remove the current crontab.	Enter the following commands on each of the NAT units:
		
		`networkctl stop;`
		
		`crontab -r;`
		
		Note To restart the crontab later, see Restarting Crontab Jobs for NAT Units, page 11-17.

Step 16	(Local and geographic gateway high availability) Verify that the gateways and units with Red Hat installed have rsync 3.0.6 or newer. For ESXi 5.5 and RHEL6.5, see RHEL6.5 installation guide	Verify the rsync version installed on the gateway/units using the command: [root@primebgl01-lnx ~]# rpm -qa rsync rsync-3.0.6-9.el6_4.1.x86_64 [root@primebgl01-lnx ~]#
Step 17	If using an external database, verify your database settings. **Note** Prime Network 4.2 requires the Oracle JVM and partitioning options.	See Chapter 4, "Preparing the Oracle External Database"

Supported Prime Network Upgrade and Rolling back versions

Refer the following table for supported Prime Network Upgrade and rolling back versions.

Table 11-3   Supported Prime Network Upgrade and Rolling back versions

Upgrade from	Upgrade to	Rollback to
PN 3.x > 4.0	4.2	4.0
PN 4.0	4.2	4.0
PN 4.1	4.2	4.1

Upgrading to Prime Network 4.2 from 4.0 and 4.1 (Intermediate Steps)

Note   The steps provided below are intermediate steps that are to be followed while Upgrading to Prime Network 4.2, RHEL 6.5, and Oracle 12, page 11-9 from PN 4.1 with RHEL 6.4 or other lower versions of Prime Network with RHEL 5.5-5.8.

Use the procedure described in this section to upgrade from Prime Network 4.0 and Prime Network 4.1 to Prime Network 4.2.

Caution   Do *not* apply any service patches during any phase of the upgrade to Prime Network 4.2. Apply them after the upgrade is completed.

Before You Begin

Before you begin the upgrade, perform the pre-upgrade tasks in Preparing to Upgrade Prime Network (Pre-Upgrade Checklist), page 11-5.

To upgrade the Prime Network gateway:

Step 1   Create a temporary upgrade directory on the gateway.

Note   Make sure that upgrade directory is not a subdirectory of NETWORKHOME (which is /export/home/*pnuser* by default).

Step 2   Insert **Disk 5: Installation and Upgrade** into the DVD drive.

Step 3   Copy these files from the DVD to the temporary upgrade directory you created:

- ivne-drivers.tar file
- Prime_Network_upgrade directory and its contents

Step 4   Give the Prime_Network_upgrade directory and its contents *pn user* **:** *pn group* owner permissions:

`chown - R `*pnuser: pn group directory name*

Note   To verify the group name, run the following command as *pnuser*: `id --group --name`

Step 5   As *pnuser*, move to the following location in your temporary upgrade directory:

`cd Prime_Network_upgrade`

Step 6 If you have not upgraded from fresh install of Prime Network 4.0 or Prime Network 4.1 to Prime Network 4.2, execute the following command as a Prime Network user to make the Compliance Manager status as UP:

cmctl start

Step 7 Start the upgrade:

`perl upgrade.pl`

Step 8 Enter the required information as shown in the following table.

Prompt for...	Enter...	Notes
Password for OS root user	Operating system root password	Linux root password In a high availability environment, you will be required to enter the OS root user for each machine in the setup.
Verifying whether you have completed database backup	yes	This prompt is to check whether you have recently completed database backup. Default is **yes**. If you enter **no**, the upgrade process will stop and will ask you to back up the database. For information on backing up your database, see Step 3 in the pre-upgrade checklist.
Destination location for backing up the existing installation tar file	*directory*	Specify a directory with at least 6000 MB of free space. Verify that the backup directory is available for *pnuser*. The backup directory needs write permission. Enter the following command to add write permission to the backup directory: `chmod 777 <directory>`
Disabling Configuration Audit	yes	Configuration Audit is deprecated and replaced by Compliance Audit. If you still want to use Configuration Audit, enter **no** and it will remain available from Change and Configuration Management.
Path to the ivne-drivers.tar file	*full pathname*	Provide the full pathname to the temporary upgrade location from Step 1.
Prime Network root password	*root password*	The root password used to log into the Prime Network GUI applications.

Step 9 After the upgrade is complete, Prime Network restarts. Log in as *pnuser* for the environment changes to take effect.

Step 10 If any of the preceding steps fail, the following error message is shown:

```
Failed to execute hook-type for hook-name. See log for further details.
- Hook hook-name terminated with failure
- Please choose one of the following:
1. Abort the upgrade process
2. Re-run the hook
```

In the error message, *hook-type* and *hook-name* are the type and name of the procedure that failed.

a. Check the upgrade log (*NETWORKHOME*/Main/upgrade-*timestamp*.log) to identify the reason for the failure.

b. If you can identify the problem and fix it manually, do so; then, choose option **2** to rerun the hook. The upgrade procedure continues from the procedure that failed.

c. If you cannot fix the problem, choose option **1** to cancel the upgrade. After canceling the upgrade, Prime Network cannot be started. Contact your Cisco account representative to fix the problem; then, rerun the upgrade. The upgrade procedure continues from the procedure that failed.

> **Note**   If you decide not to rerun the upgrade, you must roll back to your base Prime Network environment, including rolling back the database. See Rolling Back to Earlier Prime Network Version, page 11-11.

Step 11   If you upgraded a gateway configured with local high availability, take the ana and oracle_db services out of maintenance mode:

```
clusvcadm -U ana
clusvcadm -U oracle_db
```

Step 12   Clear the web browser cache.

Step 13   Perform the necessary tasks listed in Prime Network Post-upgrade Tasks, page 11-16.

> **Note**   To remove previous device package reference errors in avm file: 11.out, execute the following command as a Prime Network user: **networkctl restart –avm 11.**

Upgrading to Prime Network 4.2, RHEL 6.5, and Oracle 12

Upgrading from RHEL 6.4 with PN 4.1 to RHEL 6.5 with PN 4.2 and Oracle 12

To upgrade from RHEL 6.4 with PN 4.1 to RHEL 6.5 with PN 4.2 and Oracle 12, follow the procedure provided below:

Step 1   Upgrade to PN 4.2 using **Prime_Network_upgrade** directory from Disk 5 to the temporary upgrade directory you created. See Upgrading to Prime Network 4.2 from 4.0 and 4.1 (Intermediate Steps), page 11-7.

Step 2   Upgrade embedded Oracle 12 using the **embedded_upgrade_12.1.zip** file from Disk 5. See Upgrading the Embedded Database to Oracle 12.1.0, page 11-19.

Step 3   Upgrade the RHEL 6.4 to 6.5 using In-line upgrade with latest Open ssl package. Contact your System Admin for RHEL in-line upgrade.

Step 4   After upgrading the RHEL, login with PN user and verify the web server status and the compliance engine status.

Step 5   Login as PN user and restart AVM11 using **$ANA_HOME# anactl restart -avm 11.**

> **Note**   If you have Unit server attached with Gateway, first upgrade the Gateway as mentioned in the above steps, and Upgrade the RHEL version 6.5 in the Unit server with the latest Open ssl package by using the In-line upgrade.

Upgrading from RHEL 5.5 - 5.8 to RHEL 6.5 with PN 4.2 and Oracle 12

Upgrading from RHEL 5.5-5.8 to 6.5 consists of upgrading to PN 4.2 on a local RHEL 5.5-5.8 system, backing up the database, and saving it to a different location. After which, you need to re-image the system with RHEL 6.5, reinstall the PN 4.2, and restore the previous database from the location where you saved it.

✎ **Note**   If you have RHEL 5.8 and do not wish to re-image to RHEL 6.5, you can continue to upgrade PN 4.2 with RHEL 5.8

To upgrade RHEL from 5.5, 5.6, 5.7, and 5.8 with lower version of prime network to RHEL 6.5 with PN 4.2 and Oracle 12, follow the steps provided below:

Step 1   Note down the PN Username and Password, and Oracle username and Database profile that you had selected while installing PN lower version.

Step 2   Upgrade to PN4.2 from PN lower version using **Prime_Network_upgrade** directory from Disk 5. See Upgrading to Prime Network 4.2 from 4.0 and 4.1 (Intermediate Steps), page 11-7.

Step 3   Upgrade embedded Oracle 12 using the **embedded_upgrade_12.1.zip** file from Disk 5. See Upgrading the Embedded Database to Oracle 12.1.0, page 11-19.

Step 4   Login as Prime user and Backup the Embedded oracle database **$ANAHOME/Main/scripts/embedded_db# emdbctl --backup.** Please refer PN 4.2 Admin guide for knowing how to back up the Gateway data and the Embedded Database.

✎ **Note**   If you have operations reports in Gateway, Uninstall it before performing PN Database backup.

Step 5   Copy the latest backup folder in **$ANA_HOME/backup#** to your local server (for example, other than the server you are currently using).

Step 6   Re-image the Gateway server to RHEL 6.5. If you have a Unit server attached in the Gateway, re-image the Unit server to RHEL6.5.

Step 7   Install the PN4.2 Gateway, Oracle 12 and the Unit server. If you have unit Gateway setup in PN lower version, use the PN Username and Password, and Oracle username and Database profile that you had chosen while installing PN Gateway lower version.

✎ **Note**   If you have installed the embedded Oracle in remote server for PN lower version, install embedded database 12 on the same server for PN 4.2.

Step 8   Once installation is complete, login as a Prime user, back up the Prime network Gateway data and embedded database **$ANAHOME/Main/scripts/embedded_db # emdbctl --backup**. Please refer PN 4.2 Admin guide to know more on how to back up the Gateway data and the embedded database.

Step 9   Navigate to **$ANA_HOME/backup** location, and remove the back up file folder in the location.

Step 10   Paste the backup file folder which you already have in your local machine to the location **$ANA_HOME/backup**.

Step 11   Provide the group owner permissions to the backup file directory and its contents as follows:

chown - R pnuser: pngroup directory_name . Example: chown -R pn40:ana 201503101439

Step 12   Login as Prime user and restore the embedded database with Prime network gateway data by using the command **$ANAHOME/Main/scripts/embedded_db # emdbctl --restore**. Please refer PN 4.2 Admin guide to know more on how to restore the gateway data and the embedded database.

Step 13   Once the restoring process is completed, check the status of PN.

Step 14   Ensure that the status of both compliance engine and web server is up.

Step 15   Start the Unit server as a Prime user using the command **$ANA_HOME# anactl start**, if it is attached with the Gateway.

Step 16   Restart the PN as Prime user using the command **$ANA_HOME# anactl restart**.

Rolling Back to Earlier Prime Network Version

Rollback to Prime Network 4.1 or 4.0 is available if you encounter problems during the upgrade, or if you want to roll back to the previous version after the upgrade completes. For information on rolling back from 4.2 to 4.1 or 4.0, see Cisco Prime Network 4.0 Installation Guide or Cisco Prime Network 4.1 Installation Guide.

Before You Begin

- Verify that the gateway and units are powered up and connected; that is, you can open an SSH session between the gateway and all units.

- Disconnect standby and NAT units from the gateway using the Administration GUI.

- Verify that the Prime Network application is *not* running with **networkctl status**.

To Roll back Prime Network gateway to Prime Network 4.1

Note   After upgrading from RHEL 6.4 or RHEL 5.5 - 5.8 to Prime Network 4.2 with RHEL 6.5 and Oracle 12, you cannot rollback to the previous versions of Prime Network.

Step 1   If your deployment has units that are connected to the gateway, roll back the units (before rolling back the gateway). The rollback will remove redundant units from the registry and the golden source.

Step 2   Configure all units using the following command:

network-conf -rollback

Step 3   Enter **no** at the prompt to start the unit.

Step 4   Restore the backed-up database and start the database services and the listener. Because the database table structure changes after the upgrade, the database is backed up as part of the upgrade process. The old table structure must be recovered.

Note   If you have a gateway high availability deployment, the services ana and oracle_db services should be moved to maintenance state.

- To restore an external database, contact your database administrator.

- To restore an embedded database:
  - Log into the gateway as *pnuser*.
  - Change to the directory *NETWORKHOME*/Main/scripts/embedded_db:

    # cd $PRIME_NETWORK_HOME/Main/scripts/embedded_db

  - Execute the restoration script for restoring the embedded database:

    # emdbctl --restore_db

  For more information on prompts that appear while restoring an embedded database, see the

  Cisco Prime Network 4.2 Administrator Guide.

  After restoring the database, enter **no** at the prompt to start Prime Network.

Step 5   As *pnuser*, move to the temporary upgrade directory (created in Step 1 of the procedure in Upgrading to Prime Network 4.2 from 4.0 and 4.1 (Intermediate Steps), page 11-7).

Step 6   Enter the following command to change to the upgrade directory:

cd Prime_Network_upgrade

Step 7   Enter the following command on the gateway (only):

perl rollback.pl

Step 8   Perform the rollback by entering the required information as shown in the following table.

Prompt for...	Enter:	Notes
Confirm that you have restored the database	yes	Confirm that you performed Step 2. **Note** If you have *not* restored the database, enter **no** and exit the script. Restore the database and begin again.
Confirm whether you have reinstalled units	yes	Confirm that you performed Step 5. **Note** If you have *not* rolled back the units, enter **no** and exit the script. Rollback the units and begin again.
Confirm whether you want to roll back to the older version	yes	—
Full path to the backup file	*full pathname*	Location of the backup file (it is not deleted during the rollback). An example is: /export/home/PrimeNetworkBackUp _xxxxxxxxxx.tar.gz

Step 9   When the rollback is complete, log in as the *pnuser* to apply the environment changes.

Step 10   Start the unit:

- **networkctl start** (without running **network-conf** again)

Step 11   Reconnect standby and NAT units to the gateway using the Administration GUI.

Note   Rollback logs can be found in the Prime_Network_upgrade folder under *NETWORKHOME*.

Upgrading the Prime Network Integration Layer (PN-IL)

If the PN-IL is installed on your system, you can upgrade using the instructions in these topics:

Note If the PN-IL is not installed on your system, you can install it using the instructions in

Upgrading PN-IL in Standalone Mode

Before You Begin

Perform these tasks as *pnuser*:

- Disable the health monitor to disable the PN-IL services permanently otherwise the services will start automatically after a delay of 3 minutes.

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

- Back up the $PRIMEHOME directory.
- Stop the PN-IL using the following command:

    `itgctl stop`

To upgrade a standalone PN-IL:

Step 1   As the root user, launch a terminal on the Prime Network gateway server where you want to install PN-IL.

Step 2   Insert **Disk 5: Installation and Upgrade** in the DVD drive.

Step 3   Mount the inserted DVD using **mount** and move to the mount location.

Step 4   Log in as *pnuser*:

`su` - *pnuser*

Step 5   Create a temporary PN-IL upgrade directory.

`mkdir -p $PRIME_NETWORK_HOME/pnilupgrade`

Step 6   Copy the PN-IL upgrade tar file from the mount location to the `pnilupgrade` directory.

```
cp /mnt/**/Upgrade/PNIntegrationLayerUpgrade_1.0.0.0-1.3.0.tar.gz
$PRIME_NETWORK_HOME/pnilupgrade
```

Step 7   Navigate to the directory in which the tar file was copied and extract the PN-IL upgrade tar.

```
cd $PRIME_NETWORK_HOME/pnilupgrade
tar -zxf PNIntegrationLayerUpgrade_1.0.0.0-1.3.0.tar.gz
```

Step 8   Navigate to the extracted files directory.

`cd PNIntegrationLayerUpgrade_1.0.0.0-1.3.0`

Step 9   Run the upgrade script

`./upgradeIntegrationLayer.sh`

Step 10   Enter **yes** at the prompt to continue the upgrade process. The upgrade process is completed and the log files can be located at $PRIMEHOME/upgrade/1.0.0.0-1.3.0.0/upgrade.log.

Step 11   Perform the following post-upgrade tasks:

    a.   As *pnuser*, reload the user profile:

       source $PRIME_NETWORK_HOME/.cshrc

    b.   Configure the PN-IL in standalone mode:

       itgctl config 1

    c.   Start the PN-IL:

       $PRIMEHOME**/bin/itgctl start**

    d.   Enable the health monitor:

       $PRIMEHOME/local/scripts/il-watch-dog.sh enable

Upgrading PN-IL in Suite Mode

If you have been working with Prime Network 4.2, you will have PN-IL 1.3 installed on your system. The procedure for upgrading to PN-IL 1.3 in suite mode is the same as upgrading in standalone mode. See Upgrading PN-IL in Standalone Mode, page 11-13.

If you have been working with a release prior to Prime Network 4.0, follow the instructions below to upgrade to PN-IL 1.3.

Step 1   Upgrade PN-IL in standalone mode as described in Upgrading the Prime Network Integration Layer (PN-IL).

Step 2   Perform these tasks on the Prime Central Server to create a backup of the PN-IL configuration data.

    a.   Log in to the Prime Central server as root.

       ssh root@*Prime-Central-host-IP-address*
       su - *prime-central-user*

    b.   Create Prime Central upgrade directory

       mkdir -p $PRIMEHOME/upgrade

    c.   Copy the PN-IL upgrade tar file (example: PNIntegrationLayerUpgrade_1.0.0.0-1.3.0.tar.gz) from the upgrade directory on the Prime Network server to the upgrade directory on the Prime Central server.

    d.   Extract the files.

       tar -zxf PNIntegrationLayerUpgrade_1.0.0.0-1.3.0.tar.gz

    e.   Run the PN-IL upgrade utility script to create a backup tar file in $PRIMEHOME/backup.

       ./ilUpgradeUtility.sh backup

Step 3   Perform these tasks on the Prime Network server to restore the PN-IL configuration.

    a.   As *pnuser*, copy the backup tar from the Prime Central upgrade directory to Prime Network server.

    b. Extract the files:

        `tar -zxf il_backup_1.3.0.0.tar.gz`

    c. Run the PN-IL utility script to restore the PN-IL configuration:

        `./ilUpgradeUtility.sh restore` *untar-files-directory*

Step 4   Perform these tasks on Prime Central as described in Cisco Prime Central Quick Start Guide, 1.4

     • Upgrade Prime Central

     • Integrate Prime Network and PN-IL with Prime Central

Step 5   Start the upgraded PN-IL:

    $PRIMEHOME/bin/itgctl start

Prime Network Post-upgrade Tasks

After the upgrade to Prime Network 4.2 is complete, perform the post-upgrade tasks that apply to your deployment.

Enable Units to Restart Automatically After they are Rebooted

After upgrade, you need to perform the following steps on each unit in your setup otherwise the units will not restart automatically after they are rebooted.

Step 1 Log into the unit as *pnuser*.

Step 2 Copy rootdeploy.cmd from the gateway, as follows:

```
remote_copy.cmd "<Gateway_IP>:.deploy/independent/on_boot/rootdeploy.cmd"
".deploy/independent/on_boot/rootdeploy.cmd"
```

Step 3 Switch to the root user:

```
su - root
```

As the root user, execute the rootdeploy command:

```
cd $PRIME_NETWORK_HOME/.deploy/independent/on_boot ; ./rootdeploy.cmd
```

Restoring Customized Crontabs

If you saved user-defined cron jobs in *NETWORKHOME*/local/cron/crontab.user.list, they are restored. User-defined cron jobs that are not placed in this directory must be manually recreated.

Restarting Crontab Jobs for NAT Units

Cron jobs on NAT units must be manually restarted.

Step 1 Log into the unit as *pnuser*.

Step 2 Copy the upgrade_restart_crons.pl script from the gateway, as follows:

```
remote_copy.cmd [gw-ip]:$PRIME_NETWORK_HOME/Main/scripts/upgrade_restart_crons.pl
Main/scripts
```

Step 3 Run the upgrade_restart_crons.pl script. It will display output similar to the following:

```
./Main/scripts/upgrade_restart_crons.pl
+ Updating the unit's cronjobs
- Writing log to ~/Main/logs/upgrade_crons.log
- Copying the files from the gateway (gateway's_ip)
- Restarting the cronjobs
+ Please wait while the unit is being updated................................Done.
```

Step 4 Verify that the crontab list is not empty:

```
crontab -l
```

Step 5 The upgrade is now complete. Run the **status** command and check the version number to make sure that the upgrade has been successful.

Fixing the Database Entry for Vision Clients with NAT

If you are using network address translation (NAT) with the Prime Network Vision client, update the database host in the Prime Network registry to contain the hostname instead of the IP address.

If you already use a hostname instead of an IP   address, you do not have to repeat this procedure.

Step 1 Make sure Prime Network is running.

Step 2 Verify that the client workstations have the correct Domain Name System (DNS) mapping.

Step 3 From *NETWORKHOME*/Main, run the following commands:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/persistency/nodes/main/Host database-server-hostname
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/persistency/nodes/ep/Host database-server-hostname
```

Step 4 Enter the following command to restart Prime Network:

```
networkctl restart
```

Updating the Port Watchdog (AVM Protection) Scripts

After upgrading to Prime Network 4.2, copy the port watchdog scripts to /var/adm/cisco/prime-network/scripts. Enter the following commands as the root user:

```
mkdir -p /var/adm/cisco/prime-network/scripts
cp NETWORKHOME/Main/scripts/port_watchdog.pl /var/adm/cisco/prime-network/scripts
```

```
cp NETWORKHOME/Main/scripts/keep_alive_port_watchdog.pl
/var/adm/cisco/prime-network/scripts
chmod -R 700 /var/adm/cisco/prime-network/scripts
chown -R pnuser:network /var/adm/cisco/prime-network/scripts
```

Restore Links Between Devices and Cloud VNEs

If your deployment had cloud VNEs that were connected to devices with static links, the connection between the cloud VNE and the device may be lost after the upgrade. Delete and recreate the link using the Administration GUI.

Support for Third-Party VNEs

Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 4.2, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.

Command Builder Scripts

If you had customized Command Builder scripts (which you should have uninstalled), you may need to update your scripts if your deployment:

- Executes command scripts using the Prime Network northbound APIs (for example, BQL)
- Includes references to IMOs or to the Prime Network internal model

Verify whether the command names, parameters, or IMO references have changed, in which case you must update your scripts. The reinstall your customized scripts.

Gathering DB Statistics in First 24 Hours

The *pnuser*_admin user performs maintenance tasks—such as gathering statistics—on the other Prime Network database schemas. After this user is created, a cron job runs every 24 hours to gather statistics on the Fault Database tables.

However, if you expect a high scale in the first 24 hours, you might need to manually force statistics gathering twice during the first day, 1 and 5 hours after noise start. To force statistics gathering, enter the following UNIX command as *pnuser*:

```
cd $PRIME_NETWORK_HOME/Main/scripts ; ./call_update_ana_stats.pl >& /dev/null
```

If you deploy Prime Network to handle a high event rate, disabling Oracle's automatic maintenance jobs is recommended. Automatic maintenance significantly affects Oracle performance and increases event processing time. See Disabling Automatic Maintenance Jobs, page 4-8.

Integration Changes

For details on BQL and other integrations after the upgrade, refer to the Cisco Developer Network at https://developer.cisco.com/site/prime-network/.

Upgrading the Embedded Database to Oracle 12.1.0

You must upgrade the embedded Oracle database to version 12.1.0 if:

- You have been using Prime Network 4.1 or a lower version and you want to upgrade to Prime Network 4.2.
  AND

- You are planning to upgrade your operating system to Red Hat 6.

If the conditions specified are not met, there is no need to upgrade to Oracle 12.1.0, and the upgraded Prime Network 4.2 can run with Oracle 11.2.0.3 as well.

While upgrading to Oracle 12.1.0, follow the steps:

1. First upgrade to Prime Network 4.1.

2. Upgrade Oracle from earlier version to Oracle 11.2.0.3.

3. Upgrade your Operating System.

4. Upgrade from Prime Network 4.1 to Prime Network 4.2.

5. Upgrade to Oracle 12.1.0.

Before you Begin

- Copy the following Oracle installation.zip files from **Disk 3: Database Binaries** to a directory on the machine on which the embedded database is installed (either on the local gateway server or a remote server):

  - linuxamd64_12c_database_1of2.zip

  - linuxamd64_12c_database_2of2.zip

- Ensure that there is a minimum of 12 GB free disk space. This space is freed up after the upgrade has completed successfully.

- Ensure that database backup and restore are enabled. See the "Enabling Embedded Oracle Database Backups" section in the Cisco Prime Network 4.2 Administrator Guide.

Step 1   As the root user, locate the **embedded_upgrade_12.1.zip file** on **Disk 5** and copy it to a directory on the machine on which the embedded database is installed (either on the local gateway server or a remote server).

Step 2   Unzip the file:

unzip embedded_upgrade_12.1.zip

Step 3   If your setup has cluster, freeze the cluster configured services (ana and oracle_db) using the following command:

clusvcadm -Z service

Step 4   Start the database upgrade by entering the following command:

 # perl upgrade_embedded_oracle_12.pl

Example-Upgrading the Embedded Database to Oracle 12.1.0

Step 1 In the database server, perform the following steps:

a. Unzip the **embedded_upgrade_12.1.zip** to **/tmp/upg12c** by entering the following command:

```
chmod a+x /tmp/upg12c/*.pl
```

b. Copy the following two zip files to **/tmp/upg12c.**

   – linuxamd64_12c_database_1of2.zip

   – linuxamd64_12c_database_2of2.zip

c. Create the staging directory by entering the following commands:

```
mkdir /export/home/stg
cd /tmp/upg12c
```

d. Upgrade to Oracle 12.1.0 by entering the following command:

```
# perl upgrade_embedded_oracle_12.pl

Enter the name of the OS user of the database [oracle]
Enter the staging/upgrade directory. This directory should have at least 9GB free space
[/export/home/stg]
Running pre-upgrade validations
Extracting /tmp/upg12c/linuxamd64_12c_database_2of2.zip
Extracting /tmp/upg12c/linuxamd64_12c_database_1of2.zip
Diagnosing the database status
Installing the software
Running pre-upgrade tasks
Copying files to new Oracle home
Verifying no files needs media recovery and no backup is running
Before proceeding with the upgrade, this procedure will take a backup of the database. you
may choose between
  1. Offline (Cold) backup (requires database downtime) [default]
  2. Online (Hot) backup
   Enter option: (1-2) 1

The database is about to be shutdown. Please stop PrimeNetwork and any other application
using the database.
Hit the 'Enter' key when ready to continue

Stopping the database & listener
Backing up the database.
Stopping the database & listener
Backing up system files
Upgrading the database. This step may take at least 40 minutes.
Executing post upgrade tasks.
Upgrading timezone file
Identifying new invalid objects
Copying PrimeNetwork scripts to new Oracle home
Restarting Oracle cronjobs
Upgrade completed successfully. Logs can be found under /opt/ora/oracle/ana_logs/upgrade
To complete the upgrade, enter the following command as the Prime Network user:
cd ~/Main/scripts/embedded_db ; emdbctl --update_oracle_home
You have new mail in /var/spool/mail/root
```

Step 2   Enter the required information as shown in the following table.

Prompt for...	Enter...	Notes
OS username	Username for the Oracle database user.	Default is **oracle**.
Staging/upgrade directory	Path to the directory from which the upgrade will run and to which the database zip files will be extracted.	Default is /export/home/stg
Location of zip files	Path to the directory to which the Oracle zip files were copied.	—
Database backup method	Offline (Cold) backup or Online (Hot) backup	With cold backup, the database is down during the backup. With hot backup, the database continues to run until the upgrade starts. Downtime is shorter but the backup might take longer. Default is cold backup.

Step 3   Navigate to **/export/home/oracle/product/12.1.0/db_1/network/admin/listener.ora**, and update **oracle_home=/export/home/oracle/product/12.1.0/db_1**

Step 4   Login to Oracle, and restart the embedded Oracle by following command:

#lsnrctl stop

#lsnrctl start

Upgrading the Embedded Database to Oracle 12.1.0 in a HA Setup with Geographical Redundancy and Oracle ADG

You must upgrade the embedded Oracle database to version 12.1.0 if:

- You have been using Prime Network 3.9 or a lower version and you want to upgrade to Prime Network 4.2.
  AND

- You are planning to upgrade your operating system to Red Hat 6.

If the conditions specified are not met, there is no need to upgrade to Oracle 12.1.0, and the upgraded Prime Network 4.2 can run with Oracle 11.2.0.3 as well.

While upgrading to Oracle 12.1.0, follow the steps:

1. First upgrade to Prime Network 4.1.

2. Upgrade Oracle from earlier version to Oracle 11.2.0.3.

3. Upgrade your Operating System.

4. Upgrade from Prime Network 4.1 to Prime Network 4.2.

    5. Upgrade to Oracle 12.1.0.

Before you Begin

- Copy the following **Oracle installation.zip** files from **Disk 3: Database Binaries** to a directory on the machines on which the embedded database is installed (both the primary and standby gateway servers:

  – linuxamd64_12c_database_1of2.zip

  – linuxamd64_12c_database_2of2.zip

- Ensure that there is a minimum of 12 GB free disk space on each of the servers. This space is freed up after the upgrade has completed successfully.

- Verify that database replication works properly prior to starting the database upgrade by performing the geographical redundancy verification tests described in the Cisco Prime Network 4.2 Gateway High Availability Guide.

Step 1   To be performed on both primary and standby gateway servers.
As the root user, locate the **embedded_upgrade_12.1.zip** file on **Disk 5** and copy it to a directory on the machines on which the embedded database is installed.

Step 2   To be performed on both primary and standby gateway servers.
As the root user, unzip the file:

```
unzip embedded_upgrade_12.1.zip
```

Step 3   On the standby gateway server, run the Oracle software upgrade and prepare the standby server for database upgrade.

Navigate to the upgrade scripts directory and enter the following command:

```
# perl standby_db_prepare_for_upgrade_12.1.pl
```

Step 4   On the primary gateway server, start the database upgrade by entering the following command:

```
# perl upgrade_embedded_oracle_12.pl
```

Step 5   Enter the required information as shown in the following table.

Prompt for...	Enter...	Notes
OS user name	Username for the Oracle database user.	Default is **oracle**.
Staging/upgrade directory	Path to the directory to which the upgrade zip file was copied.	—
Location of zip files	Path to the directory to which the Oracle zip files were copied.	—
Database backup method	Offline (Cold) backup or Online (Hot) backup	With cold backup, the database is down during the backup and the gateway is stopped. With hot backup, the database continues to run until the upgrade starts. Downtime is shorter but the backup might take longer. Default is cold backup.

Step 6   On the primary gateway server, verify that the Oracle listener is running by entering the following command as the root user:

```
su - oracle -c "lsnrctl status"
```

Step 7   On the standby gateway server, set back the replication redo apply by running the **standby_post_upgrade.pl** to **perl ./standby_db_post_upgrade12.1.pl**.

Example-Upgrading the Embedded Database to Oracle 12.1.0 in a HA Setup with Geographical Redundancy and Oracle ADG

Step 1   Stop the Prime Network.

Step 2   Verify if the replication between databases work.

Step 3   In the STANDBY database server, perform the following steps:

   a. Navigate to the location where the embedded Oracle software is available.

   b. Unzip the **embedded_upgrade_12.1.zip** to a location **/tmp/upg12c** by entering the following command:

```
chmod a+x /tmp/upg12c/*.pl
```

   c. Copy the two zip files to **/tmp/upg12c**:

      – linuxamd64_12c_database_1of2.zip

      – **linuxamd64_12c_database_2of2.zip**

   d. Create the staging directory by entering the following commands:

```
mkdir /export/home/stg
cd /tmp/upg12c
```

   e. Upgrade to Oracle 12.1.0 by entering the following command:

```
# perl standby_db_prepare_for_upgrade_12.1.pl

Enter the name of the OS user of the database [oracle]
Enter the staging/upgrade directory. This directory should have at least 9GB free space
[/export/home/stg]
Running pre-upgrade validations
Extracting /tmp/upg12c/linuxamd64_12c_database_2of2.zip
Extracting /tmp/upg12c/linuxamd64_12c_database_1of2.zip
Installing the software
Copying files to new Oracle home
Backing up system files
Starting the standby database in mount mode.
Copying PrimeNetwork scripts to new Oracle home
Restarting Oracle cronjobs
Standby database is ready for upgrade. Please run the upgrade procedure for the primary
database. Logs can be found under /opt/ora/oracle/ana_logs/upgrade
```

Step 4   In the PRIMARY database server, perform the following steps:

   a. Navigate to the location where the embedded Oracle software is available.

   b. Unzip the **embedded_upgrade_12.1.zip** to **/tmp/upg12c** by entering the following command:

```
chmod a+x /tmp/upg12c/*.pl
```

c. Copy the two zip files to **/tmp/upg12c**:

- linuxamd64_12c_database_1of2.zip

- linuxamd64_12c_database_2of2.zip

d. Create the staging directory by entering the following commands:

```
mkdir /export/home/stg
cd /tmp/upg12c
```

e. Upgrade to Oracle 12.1.0 by entering the following command:

```
# perl upgrade_embedded_oracle_12.pl

Enter the name of the OS user of the database [oracle]
Enter the staging/upgrade directory. This directory should have at least 9GB free space
[/export/home/stg]
Running pre-upgrade validations
Extracting /tmp/upg12c/linuxamd64_12c_database_2of2.zip
Extracting /tmp/upg12c/linuxamd64_12c_database_1of2.zip
Diagnosing the database status
Installing the software
Running pre-upgrade tasks
Copying files to new Oracle home
Verifying no files needs media recovery and no backup is running
Before proceeding with the upgrade, this procedure will take a backup of the database. you
may choose between
1. Offline (Cold) backup (requires database downtime) [default]
2. Online (Hot) backup
   Enter option: (1-2) 1
The database is about to be shutdown. Please stop PrimeNetwork and any other application
using the database.
Hit the 'Enter' key when ready to continue
Stopping the database and listener
Backing up the database
Stopping the database and listener
Backing up system files
Upgrading the database. This step may take at least 40 minutes.
Executing post upgrade tasks
Upgrading timezone file
Identifying new invalid objects
Copying PrimeNetwork scripts to new Oracle home
Restarting Oracle cronjobs
Upgrade completed successfully. Logs can be found under /opt/ora/oracle/ana_logs/upgrade
To complete the upgrade, enter the following command as the Prime Network user:
cd ~/Main/scripts/embedded_db; emdbctl --update_oracle_home
You have new mail in /var/spool/mail/root.
```

Step 5 In the STANDBY database server, perform the following steps:

a. Enter the following command:

```
cd /tmp/upg12c
```

b. Upgrade the Oracle version by entering the following command:

```
# perl standby_db_post_upgrade12.1.pl

Enter the name of the OS user of the database [oracle]
Setting standby DB for redo apply
Enter the staging/upgrade directory, same one that was provided earlier [/export/home/stg]
Starting the STANDBY database in mount mode.
Standby database is ready. Please verify replication.
```