Upgrading Prime Cable Provisioning

Prime Cable Provisioning 6.1.3 can be upgraded from PCP 4.2.x/ 5.x/6.x. Prime Cable Provisioning 6.1.3 supports only 64-bit servers. If you are running any earlier 4.2.x version of Prime Cable Provisioning (referred to as Cisco BAC) on 32-bit servers, you should first upgrade to 64-bit servers and then upgrade to Prime Cable Provisioning 6.1.3.

All components of Prime Cable Provisioning 4.2.x/ 5.x/6.x can be upgraded to Prime Cable Provisioning 6.1.3. You need to migrate the database, irrespective of whether you upgrade to Prime Cable Provisioning 6.1.3 from Cisco BAC 4.2.x or from Prime Cable Provisioning 5.x.

See Cisco Prime Cable Provisioning Upgrade Matrix for more details about which components can be auto-upgraded to Prime Cable Provisioning 6.1.3and which need fresh installation.

Prime Cable Provisioning supports inline migration, using which you can migrate one server at a time without disrupting the entire Prime Cable Provisioning deployment.

This chapter contains the following sections:

Upgrade Cisco BAC 4.2.x/PCP 5.x/6.x to Prime Cable Provisioning 6.1.3

You can upgrade all components of Cisco BAC 4.2.x/ PCP 5.x/6.x by running the Prime Cable Provisioning 6.1.3 installer. The installer automatically upgrades the installed components to Prime Cable Provisioning 6.1.3. However, for RDU, you will first need to complete the upgrade, and then migrate the database.

The main points to be considered for this upgrade are :

- Back up the 4.2.x/5.x/6.x RDU database and verify the same.

- Install the Prime Cable Provisioning 6.1.3 RDU. After the fresh installation, you need to migrate the database either using the migration tool or the migration script.

- Auto-upgrade is not supported for KDC on Linux. Though you can manually upgrade KDC, we recommend fresh installation to avoid any installation issues.

- You can upgrade RDU, DPE, CPNR-EP and PWS from Cisco BAC 4.2.x or above to Prime Cable Provisioning 6.1.3 .

- In case of Prime Network Registrar and its extension points you will need to first upgrade from the earlier version of Prime Network Registrar to Prime Network Registrar 8.x and then upgrade the Prime Network Registrar Extension Points to Prime Cable Provisioning 6.1.3. For the Prime Network Registrar upgrade to 8.x see the *Cisco Prime Network Registrar 10.x Installation Guide* and for the extension points upgrade, see Upgrading Cisco Prime Network Registrar Extensions, on page 18.

The following table represents the components that can be upgraded from the previous versions to Prime Cable Provisioning 6.1.3.

Components	5.x	4.2.x
RDU	Y (After upgrade, migrate the database)	Y
RDU HA	Y	NA
PWS	Y	NA
DPE	Y	Y
CPNR Extension point	Y	Y
KDC	Y	N

See Cisco Prime Cable Provisioning Compatibility Matrix for more details about which components can be auto-upgraded to Prime Cable Provisioning 6.1.3 and which need fresh installation.

Note It is recommended to backup the database before upgrading any of the Prime Cable Provisioning components.

About Backward Compatibility

Prime Cable Provisioning 6.1.3 RDU can interoperate with 4.x, 5.x, 6.x versions of Provisioning Group components (DPE and PNR EP).

Note In Prime Cable Provisioning 6.1, to avoid the java secure mode communication issue during interoperability (DPE in 5.x and RDU 6.1) follow the below steps:

1. After upgrading the RDU to PCP 6.1, edit the following properties in $BPR_HOME/jre/lib/security/java.security file .

- Remove RC4 from the property, jdk.tls.disabledAlgorithms

```
jdk.tls.disabledAlgorithms=SSLv3, MD5withRSA,DH keySize < 768, \
 EC keySize < 224
```

- Remove RC4_128 from the property, jdk.tls.legacyAlgorithms

```
jdk.tls.legacyAlgorithms= \
 K_NULL, C_NULL, M_NULL, \
 DHE_DSS_EXPORT, DHE_RSA_EXPORT, DH_anon_EXPORT, DH_DSS_EXPORT, \
 DH_RSA_EXPORT, RSA_EXPORT, \
 DH_anon, ECDH_anon, \
 RC4_40, DES_CBC, DES40_CBC, \
 3DES_EDE_CBC
```

2. Restart the RDU and start testing for InterOperability in secure mode.

After upgrading the DPE to 6.1, add the above removed content back to the java.security file.

Migration preserves the device record revision numbers used in DPE synchronization. As a result, DPE repopulation is not triggered after the RDU database upgrade, ensuring the least disruption until you upgrade the specific DPE.

Note
- In Prime Cable Provisioning 6.1.3, the RDU user configuration overrides RADIUS user configuration for authorization. This is done to support backward compatibility of existing RADIUS users. After migrating from an earlier version to Prime Cable Provisioning 6.1.3, all existing RADIUS users are migrated as local users in RDU. So it is advised that you delete all the existing duplicate RADIUS users once the RADIUS users are configured with the appropriate Cisco AV Pairs.

  - Existing read-only and read-write users would be mapped to new ReadOnly and ReadWrite users.

  - Default out of the box (OOTB) admin user will be mapped to Admin role.

  - Radius users will be migrated as local RDU users.

- Prime Cable Provisioning provides multivendor support through Option 43 and its suboptions. When using this option, ensure that you modify templates used in earlier releases to be compatible with the template grammar that Prime Cable Provisioning 6.1.3 uses.

- You must upgrade the existing API client libraries (.jar files) to Prime Cable Provisioning 6.1.3. For this, you need to copy the bpr.jar, bacbase.jar, and bac-commons.jar to the API client libraries location. For more information on API client libraries, see Cisco Prime Cable Provisioning User Guide.

Licensing After Migration

To configure Prime Cable Provisioning licensing, you must obtain the license files via a license claim process and install them using the Admin UI. For details, see the Cisco Prime Cable Provisioning User Guide and Licensing Prime Cable Provisioning.

Database Migration

The Prime Cable Provisioning database migration procedure requires that you migrate the components in the sequence recommended in below-mentioned sections. Performing the migration in any other sequence may result in error during provisioning.

1. Backing Up the RDU Database

2. Recovering the Backed Up RDU Database

3. Verify Database Integrity of Cisco BAC 4.2.x/PCP 5.x/6.x

4. Backing up the Property Files

5. Upgrading RDU from Cisco PCP 5.x/6.x to PCP 6.1.3

6. Migrating the RDU Database

7. Verifying Database Integrity of Prime Cable Provisioning 6.1.3

The following figure describes the workflow for database migration.

Figure 1: Database Migration
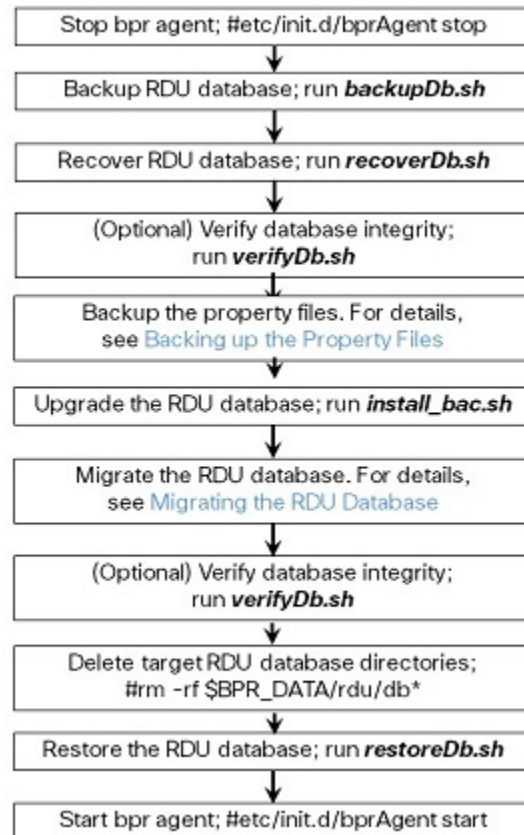
Backing Up the RDU Database

Note   We recommend you to take two backup of RDU Database. This is to ensure that when something goes wrong, or when there is a need to roll back the upgrade process, you can revert the database to previous version.

Before upgrading Prime Cable Provisioning components, ensure that you back up the RDU database files. Throttling limits the I/O bandwidth used by the database with backup utility. Throttle option specifies the rate at which the backup tool reads the files it copies. While using this option, if the reading rate is high, the tool goes to sleep mode till the rate comes down.

Note   We recommend that you use the throttle option always since it is not an I/O intensive operation. The throttle option is supported in Prime Cable Provisioning 6.1.3.

To back up the RDU database, run the **backupDb.sh** script in the *$BPR_HOME/rdu/bin directory*.

For example:

```
# $BPR_HOME/rdu/bin/backupDb.sh -throttle 500 /var/backup
```

where, */var/backup*—identifies the database backup directory.

In this example, all the backed up database files are stored in a directory called */var/backup/rdu-backup-20130829-031028*. The last subdirectory (*rdu-backup-20130829-031028*) is automatically created with a current time stamp.

Note   The time-stamped subdirectory format is *rdu-backup-yyyyMMdd-HHmmss*. In this example, the subdirectory would be *rdu-backup-20130829-031028*, meaning that the directory contains a backup that was started at 3:10:28 a.m. on August 29, 2013.

For additional information on using the **backupDb.sh** tool, see the Cisco Prime Cable Provisioning User Guide.

Recovering the Backed Up RDU Database

After taking the backup, you need to recover the database by using the command:

$BPR_HOME/rdu/bin/recoverDb.sh */var/backup/rdu-backup-20130829-031028*

Verify Database Integrity of Cisco BAC 4.2.x/ PCP 5.x

We recommend that you perform a dry run of the migration process on a staging (nonproduction) system, instead of on a live system during RDU downtime. These steps may not be practical during live migration, because in the case of a large database, verification can take an extended length of time.

To verify the database, run the **verifyDb.sh** tool on a backup snapshot.

Note   To verify the database before migration, use the **verifyDb.sh** tool from the Cisco PCP 5.x installation corresponding to the version of the database. You cannot verify a non-migrated database with the Prime Cable Provisioning 6.1.3 version of **verifyDb.sh**.

For example, enter:

$BPR_HOME/rdu/internal/db/bin/verifyDb.sh -dbdir /var/backup/rdu-backup-20130829-031028

This pathname is specific to the Cisco BAC installation version before migration.

For details on the **verifyDb.sh** tool, see the Cisco Prime Cable Provisioning User Guide.

Backing up the Property Files

If you have customized any of the property files during your current installation (BAC 4.2.x, PCP 5.x/6.x), you will need to first back them up and then copy them manually to the Prime Cable Provisioning 6.1.3 database.

To back up the property files:

Procedure

Step 1   Stop the *bprAgent* using the following command:

RHEL/CentOS 6.x

/etc/init.d/bprAgent stop

RHEL/CentOS 7.x

systemctl stop bpragent

Step 2 Back up the following files.

- files under *<BAC_HOME>/rdu/conf/*

  - *rdu.properties*

  - *adminui.properties*

  - Other xml files and dtd files
    - /opt/CSCObac/rdu/conf/CABLEHOME_OptionDesc.dtd
    - /opt/CSCObac/rdu/conf/PKTCBL_OptionDesc.dtd

    - /opt/CSCObac/rdu/conf/DOCSIS_OptionDesc.dtd

    - /opt/CSCObac/rdu/conf/log4j.xml

    - /opt/CSCObac/rdu/conf/PKTCBL_OptionDesc.xml

    - /opt/CSCObac/rdu/conf/CABLEHOME_OptionDesc.xml

    - /opt/CSCObac/rdu/conf/DOCSIS_OptionDesc.xml

    - /opt/CSCObac/rdu/conf/AuditLog.properties

- the MIB files under *$BAC_HOME/rdu/mibs/*

- the *.xml files under *$BAC_HOME/snmp/conf/*

In addition to the above files when you upgrade from Cisco BAC 4.2.x, PCP 5.x/6.x to PCP 6.1.3, back up the:

- api.properties file under *$BAC_HOME api/conf* for RDU.
- tomcat server.xml file for RDU and PWS.
- respective keystore files for RDU, DPE, CPNR-EP and PWS.

Upgrading RDU from Cisco BAC 4.2.x to PCP 6.1.3

Use this procedure to upgrade the RDU of Cisco BAC 4.2.x to PCP 6.1.3:

Procedure

Step 1 **Note** You cannot upgrade RDU from 4.2.x to 6.1.3 directly. You need to first uninstall 4.2.x RDU and then install PCP 6.1.3.

Uninstall PCP 4.2.x as described in section Uninstalling Prime Cable Provisioning.

Step 2 Continue performing from step 1 mentioned in the section , to proceed with the RDU upgrade process.

Upgrading RDU from Cisco PCP 5.x/6.x to PCP 6.1.3

Use this procedure to upgrade the RDU of Cisco PCP 5.x/6.x to PCP 6.1.3:

Procedure

Step 1 Unpack the Prime Cable Provisioning 6.1.3 install package with .gtar extension using the following command:

On Linux:

```
gtar -zxpf BAC_613_LinuxK9.gtar.gz
```

Step 2 To start the upgrade process for RDU, select the RDU component after running the install script of Prime Cable Provisioning 6.1.3 using the following command:

On Linux:

```
# <install-path>/BAC_613_LinuxK9/install_bac.sh
```

The installation program prompts you to confirm if you want to proceed with the upgrade.

Step 3 To confirm that you want to upgrade, enter **y** and press **Enter**.

The installation program prompts you to enter the backup directory location.

Step 4 To accept the default backup directory location for properties file, */tmp*, press **Enter**; or enter another backup directory location.

The installation program prompts you to remove the Cisco PCP 5.x package.

Step 5 Enter **y** and press **Enter** to continue.

The installation program will take the required backup, and remove Cisco PCP 5.x RDU. The installation program also prompts you to proceed with the installation of Prime Cable Provisioning 6.1.3 RDU. To continue with the installation see, Installing the RDU in Interactive Mode.

Note If you want to change the data directory during upgrade, ensure that you manually migrate the data from the previous data directory to the new data directory.

Step 6 To verify if the output information indicates Prime Cable Provisioning 6.1.3, enter:

On Linux:

```
# # rpm -qa CSCObac
```

Upgrading PCP along with HA

Before Upgrading PCP along with HA, please go through the below point and the upgrade scenarios carefully.

- Geo HA is available only from 5.2.x. Fresh Installation and PCP 6.1 Geo and Local HA setup works only on RHEL / CENTOS 7.4 (kernel - 3.10.0-693.11.6).

Note If you are upgrading to 6.1 and higher version, then you must upgrade the OS to RHEL/CENT 7.4 with kernel (3.10.0-693.11.6).

If you are upgrading from any one of the scenario mentioned below, please follow the steps mentioned in Upgrading PCP along with HA - Procedure 1, on page 9 or Upgrading PCP along with HA - Procedure 2, on page 10.

Note Below scenarios need OS upgrade to RHEL 7.4 / CentOS 7.4.

- Upgrading from PCP 5.x/5.2.x/5.3.x/6.0 RDU to 6.1.3 RDU Local / Geo HA Cluster.
- Upgrading from PCP 5.x/5.2.x/5.3.x/6.0 RDU Local HA Cluster to 6.1.3 RDU Local HA Cluster with OS Upgrade
- Upgrading from PCP 5.x/5.2.x/5.3.x/6.0 RDU Local HA Cluster to 6.1.3 RDU GEO HA Cluster.

If you are upgrading from any one of the scenario mentioned below, please follow the steps mentioned in Upgrading PCP along with HA - Procedure 3, on page 11.

Note Below scenarios does not require OS upgrade.

- Upgrading from PCP 6.1/6.1.x RDU GEO HA Cluster to 6.1.3 RDU GEO HA Cluster.
- Upgrading from PCP 6.1/6.1.x RDU Local HA Cluster to 6.1.3 RDU Local HA Cluster.
- Upgrading from PCP 6.1/6.1.x RDU Local HA Cluster to 6.1.3 RDU GEO HA Cluster.

Upgrading PCP along with HA - Procedure 1

Procedure

Step 1 Turn the primary RDU to standby mode, so that the VIP will be reachable through the secondary RDU node.

Step 2 Upgrade the OS to RHEL/CENTOS 7.4 on primary node with kernel - 3.10.0-693.11.6.

Step 3 Run the pre-installation script on the primary node and select option 2. For details, see: Configuring RDU Node in Primary-Only Mode.

Step 4 Install RDU on the synchronized logical volumes; **LVBPRHOME**, **LVBPRDATA**, and **LVBPRDBLOG**. For details, see Installing the RDU in Interactive Mode.

Step 5 Enable the firewall, so that the DPE and CNR-EP will not reach the VIP on the secondary node.

Step 6 Stop the bprAgent on secondary node using the command:

`/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1`

Step 7 Back up the RDU database and property files as described in section Backing Up the RDU Database and Backing up the Property Files.

Step 8 Move the DB Backup from secondary to primary node and migrate the DB and restore the same.

Step 9   Upgrade the OS to RHEL/CentOS 7.4 on the secondary node.

Step 10   Run the pre-installation script on the secondary node and select option 3. For details, see: Configuring RDU Node in Secondary-Only Mode.

Step 11   Run the pre-installation script on the primary node and select option 4. For details, see: Configuring HA Cluster from an RDU HA Ready Installation.

- It will stop the bprAgent and move the contents from /BPR_HOME /BPR_DATA and /BPR_LOG to /BPR_HOME_TMP /BPR_DATA_TMP and /BPR_LOG_TMP folders.

- It will revert back the contents from TMP to /BPR_HOME /BPR_DATA and /BPR_LOG.

Step 12   Run the post-installation script available under **BAC_613_LinuxK9** directory:

```
# sh post_install_bac_HA.sh
```

The post-installation script performs the automated configuration tasks required for RDU redundancy function setup.

Step 13   Disable the firewall, so that the DPE and CNR-EP can reach the VIP.

Upgrading PCP along with HA - Procedure 2

Procedure

Step 1   Turn the secondary RDU to standby mode, so that the VIP will be reachable through the primary RDU node.

Step 2   Upgrade the OS to RHEL/CENTOS 7.4 on secondary node with kernel - 3.10.0-693.11.6.

Step 3   Run the pre-installation script on the secondary node and select option 3. For details, see: Configuring RDU Node in Secondary-Only Mode.

Step 4   Enable the firewall, so that the DPE and CNR-EP will not reach the VIP on the primary node.

Step 5   Stop the bprAgent on primary node using the command:
```
/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1
```

Step 6   Back up the RDU database and property files as described in section Backing Up the RDU Database and Backing up the Property Files.

Step 7   Move the DB Backup to some common repository.

Step 8   Upgrade the OS to RHEL/CentOS 7.4 on the primary node.

Step 9   Run the pre-installation script on the primary node and select option 1. For details, see: Setting Up RDU Two Node Failover Pair.

Step 10   Stop the bprAgent on primary node using the command:
```
/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1 .
```

Step 11   Move the DB Backup from common repository to primary node and migrate the DB and restore the same.

Step 12   Start the bprAgent on primary node using the command:
```
/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh start res_bprAgent_1 .
```

Step 13   Disable the firewall, so that the DPE and CNR-EP can reach the VIP.

Upgrading PCP along with HA - Procedure 3

Procedure

Step 1	Turn the secondary RDU to standby mode, so that the VIP will be reachable through the primary RDU node. using the command: `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh secondary on`
Step 2	Enable the firewall, so that the DPE and CNR-EP will not reach the VIP on the primary node.
Step 3	Stop the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1`
Step 4	Back up the RDU database and property files as described in section Backing Up the RDU Database and Backing up the Property Files.
Step 5	Move the DB Backup to some common repository.
Step 6	Delete the bprAgent resources using the command: `pcs resource delete res_bprAgent_1`
Step 7	Start the upgrade process for RDU `/BAC_613_Linux/install_bac.sh`
Step 8	Move the DB Backup from common repository to primary node and migrate the DB and restore the same, as described in Database Migration, on page 4 section.
Step 9	Turn off the secondary RDU to standby mode using the command: `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh secondary off`
Step 10	Run the post-installation script available under **BAC_613_LinuxK9** directory on the primary node: `./post_install_bac_HA.sh`. The post-installation script performs the automated configuration tasks required for RDU redundancy function setup.
Step 11	Command is not Mandatary if bpragent service running: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh start res_bprAgent_1`
Step 12	Disable the firewall, so that the DPE and CNR-EP can reach the VIP.

Migrating the RDU Database

After you perform the sequence of steps (steps 1 to 5) as explained in Database Migration section , use the migration script (**migrateDb.sh**) for migrating the RDU database to Prime Cable Provisioning 6.1.3.

You must use the migration script, for migrating the RDU database:

- Cisco BAC 4.2.x/ PCP 5.x/6.x on Linux to PCP 6.1.3 on Linux, use the migration script (**migrateDb.sh**) only.

Options for the In-line Migration Script - migrateDb.sh

To migrate the database, you must run the **migrateDb.sh** shell script which is located under *$BPR_HOME/migration*. The following table describes the arguments of the **migrateDb.sh** script to carry out the migration operation.

Note In Prime Cable Provisioning 6.1.3 migration, migrateDB script does not migrate all the custom files from MIBs directory. It migrates only the MIB files that are mentioned in the rdu.properties. If the mibList property is not defined in rdu.properties, then it uses the MIB file names from the System Default Configuration and migrate those files to the database.

Table 1: migrateDb.sh Options

Argument	Description	Required	Optional	Default
-dbdir *dir*	Specifies the location of the database backup that is to be migrated.	✓		None
-dblogdir *dir*	Specifies the location of the database logs that are to be migrated.		✓	The directory that the -dbdir option specifies
-cachesize *value*	Specifies, in MB, the size of the memory cache. If you use this parameter, you must not exceed the 100-MB limit, unless you reduce the value of the **-Xmx** variable in the migrateDb.sh script by double the increase in the cache size. For example, if you set cache size to 200 MB, you must reduce the value of **-Xmx** to: (200-100)*2 = 200 MB		✓	100 MB
-help	Specifies usage for the tool		✓	

Migrating to Prime Cable Provisioning 6.1.3 Using In-line Migration Script

Migrating the RDU database to Prime Cable Provisioning 6.1.3, using the in-line migration script - **migrateDb.sh**, consists of five main steps:

1. Install/ Upgrade the Prime Cable Provisioning 6.1.3 RDU.

2. Stop the bprAgent.

3. Run the **migrateDb.sh** script (which is located under *$BPR_HOME/migration*) on the backed up database.

4. Restore the migrated database.

5. Start the bprAgent. After the migration is complete, a message is displayed indicating the same. You cannot launch the Admin UI until this step is completed.

The migration script (**migrateDb.sh**) is available in the Prime Cable Provisioning installation package. Migration is accomplished by reading from the original database and writing it into a new database. For this purpose, you must allocate additional disk space for accommodating the newly created database.

The status of the first two steps is recorded in a migration log file, which is stored in the migrated database directory. The migration.log file identifies the version of the database that is being migrated and provides status messages for the migration process.

Note   Migration deletes any outstanding jobs stored in the database, such as reliable batches that did not finish execution or pending Configuration Regeneration Service (CRS) jobs.

The following table describes the process of migration from Cisco BAC 4.2.x/ PCP 5.x/6.x Linux to Prime Cable Provisioning 6.1.3 Linux using examples that assume that:

- Cisco BAC 4.2.x/ PCP 5.x/6.x is installed in the default home directory */opt/CSCObac*.

- The migration from Cisco BAC 4.2.x/ PCP 5.x/6.x to 6.1.3 is an inline migration where the source and the target database are the same and a separate target database need not be created. The source database is restored once the migration is complete.

- The backup of the previous version of the RDU database is located in the */var/backup* directory.

Table 2: RDU Migration Workflow from Cisco BAC 4.2.x/ PCP 5.x/6.x Linux to Cisco Prime Cable Provisioning 6.1.3 Linux

Step	Task	See
1	Stop the *bprAgent* using the following command: RHEL/CentOS 6.x - # `/etc/init.d/bprAgent stop` RHEL/CentOS 7.x - # `systemctl stop bpragent`	
2	Run PCP 6.1.3 migrateDb.sh on the backed up database. The migrateDb.sh script resides in the $BPR_HOME/migration directory. For example: **# $BPR_HOME/migration/migrateDb.sh** *-dbdir* **/var/backup/rdu-backup-20130829-031028** *-dbdir*—Specifies the location of the database backup that is to be migrated; in this case, */var/backup*.	
3	Observe the migration progress using the *migration.log* file. For example: # `tail -f /var/backup/rdu-backup-20130829-031028/migration.log`	
4	Verify if the migration is complete using the migration.log file. If you find any warnings or notices, use the grep command-line tool to search them. For example: # `tail /var/backup/rdu-backup-20130829-031028/migration.log`	Cisco Prime Cable Provisioning User Guide

Step	Task	See

5	After migrating the database, verify it by running the command:
	
	For example:
	
	`# $BPR_HOME/rdu/internal/db/bin/verifydb.sh -dbdir`
	
	`/var/backup/rdu-backup-20130829-031028`
	
	Note If any error occurs during the process, the log file, **bpr-verify-db-log.xml** is generated in the path *$BPR_HOME/rdu/internal/db/bin*, which contains the details of the error. For further assistance, you can contact Cisco Support.	

6	Delete the target RDU database directories. For example: `# rm –rf /var/CSCObac/rdu/db*`	

7	Restore the migrated database into the RDU *$BPR_DATA* and *$BPR_DBLOG* directories.
	
	For example:
	
	`# $BPR_HOME/rdu/bin/restoreDb.sh`
	
	`/var/backup/rdu-backup-20130829-031028`
		[Cisco Prime Cable Provisioning User Guide]

8	Start the *bprAgent* using the following command: RHEL/CentOS 6.x - `# /etc/init.d/bprAgent start` RHEL/CentOS 7.x - `# systemctl start bpragent` This also starts the RDU process. Check the rdu.log file for messages on successful initialization, which also indicate that RDU will be up and running.	[Cisco Prime Cable Provisioning User Guide]
9	Also, you can check if the *$BPR_DATA/rdu/db/DB_VERSION* file indicates the database version as 6.1.3. **Note** Migration preserves the device record revision numbers used in DPE synchronization. As a result, DPE repopulation is not triggered after the RDU database upgrade, ensuring the least disruption until you upgrade the specific DPE.	[Cisco Prime Cable Provisioning User Guide]
10	Verify the RDU operations by logging into the Admin UI. From **Servers > RDU**, you can check if the RDU version is 6.1.3 and if the device count statistics is correct (same number of devices as before and all the devices are in the same state as they were earlier)	[Cisco Prime Cable Provisioning User Guide]

About Migration Performance

A large RDU database can be several gigabytes in size, and may take an extended length of time to migrate. This depends largely on your hardware. Using faster disks improves the time significantly.

Migration automatically compacts your database that may be fragmented. However, this Prime Cable Provisioning release stores additional data for every device. You can expect the size of the database to increase after migration by as much as 10 percent.

The migration process is optimized for speed and database compactness. As a result, migration requires a large amount of process heap size (memory). For example, migrating a 7-million device database requires approximately 1,024 MB of process heap size.

The **-Xmx** parameter in the **migrateDb.sh** script determines the maximum process heap size for migration. The default setting of 3,072 MB for this parameter is sufficient for migrating a 20-million device database. You may need to fine-tune this setting to suit your environment. For example, to migrate smaller databases running on low-end systems with less memory, you can reduce the value of the maximum heap size setting. For databases that exceed the maximum supported scale, you may need to increase this setting.

To change the heap size parameter, in the **migrateDb.sh** script edit the value for the **-Xmx** parameter.

Migration of Duplicate Class of Service and Node Name

Prime Cable Provisioning does not support duplicate names across technologies for Class of Service and nodes. If Prime Cable Provisioning detects duplicate names during database migration, the duplicate entries are automatically renamed in the following format:

- Class of Service—{*Technology_Name*}_{*Original_ClassOfService_Name*}

- Nodes—{*Node_Type*}_{*Node_Name*}

For example, if Prime Cable Provisioning encounters a gold Class of Service for a computer and a DOCSIS modem, either the computer Class of Service is renamed as Computer_gold or the DOCSIS modem Class of Service is renamed as DOCSISModem_gold. The appropriate warnings are issued to the console and migration log, and all properties containing the specific Class of Service value are automatically updated.

RDU Extension Migration

During database migration, custom extensions are retained for using it after the migration process. For details, see the Cisco Prime Cable Provisioning User Guide.

Enabling Password Encryption

Prime Cable Provisioning uses SHA1 digest algorithm for password encryption. However, when you migrate from Cisco BAC 4.2.x/ PCP 5.x to PCP 6.1.3, it continues to use the encryption algorithms used in Cisco BAC 4.2.x/ PCP 5.x. After successful migration, you can enable SHA1 digest algorithm for password encryption using the script **passwordEncryption.sh** available in *BPR_HOME/rdu/bin*.

Verifying Database Integrity of Prime Cable Provisioning 6.1.3

We recommend that you perform a dry run of the migration process on a staging (nonproduction) system, instead of on a live system during RDU downtime. These steps may not be practical during live migration, because in the case of a large database, verification can take an extended length of time.

After migration, run the verifyDb.sh tool on the migrated database.

For example, enter:

```
# $BPR_HOME/rdu/internal/db/bin/verifyDb.sh -dbdir /disk2/target
```

If any optimization is needed during this process, it will be mentioned in the log file bpr-verify-db-log.xml that is generated in the path $BPR_HOME/rdu/internal/db/bin.

Note   You cannot verify a non-migrated database with the Prime Cable Provisioning 6.1.3 version of verifyDb.sh.

For details on the **verifyDb.sh** tool, see the Cisco Prime Cable Provisioning User Guide.

DPE Cache Backup and Restore Tool

The DPE Cache Backup and Restore Tool supports populating the DPE cache from Cisco BAC 4.2.x or above to Prime Cable Provisioning 6.1.3. This reduces the time required for the synchronization with RDU while porting all the devices to the new DPE.

While upgrading from 4.2.x, it is recommended to synchronize DPE with the RDU and create a new cache. For example, if there are five DPEs in a provisioning group, then instead of synchrozing each DPE with RDU, you can synchronize one DPE and create a new cache. You can further copy this DPE cache to the remaining four DPEs.

Procedure

Step 1 Follow the below steps, to perform the DPE cache backup operation:

a) Stop the Cisco BAC 4.2.x/ PCP 5.x DPE server.

b) Run the following command in the source DPE.

```
# $BPR_HOME/dpe/internal/bin/createDbTar.sh <tarfile>
```

c) Take the backup of dpe.properties file located at **$BPR_HOME/dpe/conf/** directory.

Step 2 Follow the below steps, to perform the DPE cache Restore operation:

a) Stop the Cisco BAC 4.2.x/ PCP 5.x DPE server.

b) Copy the created database tar to the Cisco BAC 4.2.x/ PCP 5.x DPE and then run the script:

```
# $BPR_HOME/dpe/internal/bin/extractDbTar.sh <tarfile>
```

c) Verify if the cache data is copied properly to **$BPR_DATA/dpe/cache/** directory.

d) Start the Cisco BAC 4.2.x/ PCP 5.x DPE.

If the cache is successful, there should not be any more synchronization.

Upgrading DPE from Cisco BAC 4.2.x/ PCP 5.x/6.x to PCP 6.1.3

Use this procedure to upgrade the DPE of Cisco BAC 4.2.x/ PCP 5.x/6.x to PCP 6.1.3:

Note PCP 6.1.3 RDU is compatible with Cisco BAC 4.x DPE.

Procedure

Step 1 Unpack the Prime Cable Provisioning 6.1.3 install package with .gtar extension using the following command:

On Linux:

```
gtar -zxpf BAC_613_LinuxK9.gtar.gz
```

Step 2   To start the upgrade process for DPE, select the DPE component after running the install script of Prime Cable Provisioning 6.1.3 using the following command:

On Linux:

`# <install-path>`**/BAC_613_LinuxK9/install_bac.sh**

The installation program prompts you to confirm if you want to proceed with the upgrade.

Step 3   To confirm that you want to upgrade, enter **y** and press **Enter**.

The installation program prompts you to enter the backup directory location.

Step 4   To accept the default backup directory location, */tmp*, press **Enter**; or enter another backup directory location.

The installation program prompts you to remove the Cisco BAC 4.2.x/ PCP 5.x package.

Step 5   Enter **y** and press **Enter** to continue.

The installation program will take the required backup, and remove Cisco BAC 4.2.x/ PCP 5.x/6.x DPE. The installation program also prompts you to proceed with the installation of Prime Cable Provisioning 6.1.3 DPE. To continue with the installation see, Installing DPE in Interactive Mode.

Note   If you want to change the data directory during upgrade, ensure that you manually migrate the data from the previous data directory to the new data directory.

Step 6   To verify if the output information indicates Prime Cable Provisioning 6.1.3, enter:

On Linux:

`#` **# rpm -qa CSCObac**

DPE Rollback

If you want to perform DPE rollback due to the issues faced while upgrading Prime Cable Provisioning to higher version, you need to first uninstall the upgraded version and perform the below steps for DPE rollback:

Note   You must have taken a backup of DPE Cache before upgrading it for an effective rollback. If you have not taken the backup then the synchronisation time between RDU and DPE will increase, thereby overloading both the components.

Procedure

Step 1   Uninstall PCP 6.1.2 DPE, as described in the section Uninstalling Prime Cable Provisioning

Step 2   Install the DPE version that you used for rollback, as described in the section Installing Prime Cable Provisioning.

Step 3   Copy the created database tar to the Cisco BAC 4.2.x/ PCP 5.x DPE and then run the script:

```
# $BPR_HOME/dpe/internal/bin/extractDbTar.sh <tarfile>
```

Step 4   Verify if the cache data is copied properly to *$BPR_DATA/dpe/cache/* directory.

Step 5   Copy the dpe.properties file.

Step 6   Start the Cisco BAC 4.2.x/ PCP 5.x DPE.

If the cache is successful, there should not be any more synchronization.

Upgrading Cisco Prime Network Registrar Extensions

Before upgrading Prime Network Registrar extensions, we recommend that you archive your files in the *$BPR_HOME/cnr_ep/conf* directory. Also disable the Prime Network Registrar extensions point and then stop the DHCP server by using following commands:

For **RHEL/CentOS 6.x**:

```
# /opt/nwreg2/local/usrbin/nrcmd -s < /opt/CSCObac/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
# /etc/init.d/nwreglocal stop
```

For **RHEL/CentOS 7.x**:

```
# /opt/nwreg2/local/usrbin/nrcmd -s < /opt/CSCObac/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
# systemctl stop nwreglocal
```

The Prime Network Registrar extensions can be upgraded from Cisco BAC 4.2.x/ PCP 5.x/PCP 6.x version to Prime Cable Provisioning 6.1.3 version.

Note   Prime Cable Provisioning 6.1.3 supports only Prime Network Registrar 8.x or higher.

Upgrading Prime Network Registrar-EP from Cisco BAC 4.2.x/ PCP 5.x/6.x to PCP 6.1.3

Use this procedure to upgrade the Prime Network Registrar extension points of Cisco BAC 4.2.x/ PCP 5.x/6.x to PCP 6.1.3:

Note   Upgrade from 32-bit to 64-bit CNR-EP:

- Upgrade RDU to 6.1.3 (RDU will continue to interoperate with DPE (5.x), CPNR 8.x (32 bit)).
- Upgrade CPNR to 64-bit & upgrade CNR EP to 64-bit PCP 6.1.3 (single step).

Procedure

Step 1   Back up the file:

```
<BAC_HOME>/cnr_ep/conf/cnr_ep.properties
```

Step 2   Unpack the Prime Cable Provisioning 6.1.3 install package with .gtar extension using the following command:

On Linux:

```
gtar -zxpf BAC_613_LinuxK9.gtar.gz
```

Step 3   To start the upgrade process for Prime Network Registrar extensions, select the CPNR-EP component after running the install script of Prime Cable Provisioning 6.1.3 version using the following command:

On Linux:

```
# <install-path>/BAC_613_LinuxK9/install_bac.sh
```

The installation program prompts you to confirm if you want to proceed with the upgrade.

Step 4   To confirm that you want to upgrade, enter **y** and press **Enter**.

The installation program prompts you to enter the backup directory location.

Step 5   To accept the default backup directory location, */tmp*, press **Enter**; or enter another backup directory location.

The installation program prompts you to remove the Cisco BAC 4.2.x/ PCP 5.x package.

Step 6   Enter **y** and press **Enter** to continue.

The installation program removes the Cisco BAC 4.2.x/ PCP 5.x/PCP 6.x package, and prompts you to proceed with Prime Cable Provisioning 6.1.3 installation. To continue with the installation, see Installing Prime Network Registrar Extension Points in Interactive Mode.

Step 7   Enable the Prime Network Registrar extension points and restart the DHCP server using following commands respectively:

```
/opt/nwreg2/local/usrbin/nrcmd -s < /opt/CSCObac/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd
```

```
/opt/nwreg2/local/usrbin/nrcmd dhcp reload
```

The upgrade script automatically copies the upgraded extension point files to the required directories. When complete, it prompts you to restart the Prime Network Registrar Server Agent.

Step 8   To verify if the output information indicates Prime Cable Provisioning 6.1.3, enter:

On Linux:

```
# rpm -qa CSCObac
```

Step 9   Go to the *$BPR_HOME/lib* directory. If the upgrade was successful, the directory content appears similar to the list of installed files for the DPE upgrade with the addition of the `libbprextensions.so` file. The date shown should be the current date. To check this, run the command:

```
# ls -l $BPR_HOME/lib
```

Step 10   If a second check is required to verify if the upgrade was successful, go to the *CNR_HOME/extensions/dhcp/dex* directory and verify the libbprextensions.so file with the current date. To check this, run the command:

```
# ls -l /opt/nwreg2/local/extensions/dhcp/dex
```

Depending on the components installed, the directory content shown in this procedure may differ from the output featured above.

Enabling eRouter Capabilities

Procedure

	Command or Action	**Purpose**
Step 1	Enable eRouter1.0 IPv4 registered capability in CNR using the script /opt/CSCObac/cnr_ep/bin/changeNRProperties.sh **Example:** `./changeNRProperties.sh -ee "enabled"`	
Step 2	Enable eRouter1.0 IPv6 registered capability in CNR using the script /opt/CSCObac/cnr_ep/bin/changeNRProperties.sh **Example:** `./changeNRProperties.sh -eev6 "enabled"`	

Step 3	Run the script /opt/CSCObac/cnr_ep/bin/changeNRProperties.sh with option -edns to initialize the /eRouter/dns/server property with the DNS Server details. The DNS Server can be a single IP Address or a list of comma separated IP addresses. This will ensure that "domain-name-servers" mandatory Option is sent from PCP during the eRouter provisioning process.
	
	Example:
	`./changeNRProperties.sh -edns DNS-Server-IP`
	
	`./changeNRProperties.sh -edns 192.168.4.3`
	
	`./changeNRProperties.sh -edns 192.168.4.3,192.168.5.2,192.168.3.1`	

Step 4	Restart the DHCP server using the command /opt/nwreg2/local/usrbin/nrcmd dhcp reload.	
Step 5	Enable the **eRouter Feature** global flag by navigating through the path: Configuration > Defaults > ERouter Defaults. Please note that the eRouters will be discovered as computers, when this feature is in disabled state.	
Step 6	Enable the eRouter IPv4 and IPv6 capabilities in the Provisioning Group associated with the CNR Server.	

Upgrading KDC from Cisco PCP 5.x/6.x to Prime Cable Provisioning 6.1.3

Prime Cable Provisioning does not support automatic upgrade for KDC on Linux. We recommend fresh installation of Prime Cable Provisioning 6.1.3 KDC. Here is the manual procedure to upgrade the KDC of Cisco PCP 5.x to Prime Cable Provisioning 6.1.3:

Procedure

Step 1 Back up the following files:

- All certificates from `<BPR_HOME>/kdc/<Operating_System>/packetcable/certificates` directory.

- KDC_private_key.pkcs8 from `<BPR_HOME>/kdc/OS/` directory.

- bacckdc.license from `<BPR_HOME>/kdc` directory.

Step 2 Uninstall the 5.x KDC.

Step 3 Install the Prime Cable Provisioning 6.1.3 KDC. See Installing KDC in Interactive Mode.

Step 4 After the upgrade is complete, restore:

- All certificates to `<BPR_HOME>/kdc/<Operating_System>/packetcable/certificates` directory.

- KDC_private_key.pkcs8 to `<BPR_HOME>/kdc/OS/` directory.

- bacckdc.license to `<BPR_HOME>/kdc` directory.

eRouter Migration tool

Prior to 5.2 release, eRouter device was not supported and it was discovered as Computer. When the RDU is upgraded to PCP 5.2 or later versions, the eRouter device would continue to remain as Computer unless the eRouter capability is enabled in the following ways.

- Configuration > Defaults > eRouter Defaults > Click the Enabled radio button of the eRouter Feature.

- Enable the IPv4 - ERouter 1.0 , IPv6 - ERouter 1.0 capability in the provisioning group details page.

The **eRouter Migration tool**, located in $BPR_HOME/rdu/internal/db/bin is used to migrate the devices which are detected as *Computer* to **eRouter** in PCP 5.2 or later versions.

The help option (`eRouterMigrationTool.sh -help`) of the eRouter Migration Tool will provide the different options available for the tool.

Parameters

-cachesize	An optional parameter that specifies cache size in MB. The default cache size is 100MB.
-dbdir	An optional parameter to specify the database directory path. If not specified, RDU database will be used by default.

-dblogdir	An optional parameter for database log directory path, if **-dbdir** is used. If not specified the directory specified with - **dbdir** option is used by default.
-detecterouterdevices	An optional parameter for directory path to write MAC/DUID address. If specified, tool will find MAC address of the device which are detected as computer and write to a file in the specified directory. If MAC address is not available, it will print DUID address to a file.
-inputmacfile	An optional parameter to read MAC address. If specified, tool reads MAC address from this file for migration and convert as eRouter. Cannot be used with - **detecterouterdevices** or **-inputduidfile** option.
-inputduidfile	An optional parameter to read DUID address. If specified, tool reads the DUID address from this file for migration and converts it as eRouter. Cannot be used with - **detecterouterdevices** or - **inputmacfile** option.

SAMPLE USAGE:

Migrating the **eRouter** devices which are detected as Computer is a two-step process

1. To get the MAC address/DUID of the eRouter devices which are detected as Computer, the following command shall be used.

   ```
   ./eRouterMigrationTool.sh -dbdir <db_dir_path> -detecterouterdevices
   <dir_to_write_address>
   ```

   By running the above command, MAC address of the eRouter devices which are detected as Computer will be written to the file `<dir_to_write_address>/eRouterDevicesMAC`.

   If MAC address does not exist for the device, DUID will be written to the file `<dir_to_write_address>/eRouterDevicesDUID`.

2. To convert as eRouter , the following commands shall be used.

   ```
   ./eRouterMigrationTool.sh -dbdir <db_dir_path> -inputmacfile <dir_to_write_address>/
   eRouterDevicesMAC
   ```

   ```
   ./eRouterMigrationTool.sh -dbdir <db_dir_path> -inputduidfile <dir_to_write_address>/
   eRouterDevicesDUID
   ```

Note   After migration, Class of Service associated with eRouter devices will remain unchanged. Since the default Class of Service associated with eRouter devices detected as computer was unprovisioned-computer in previous releases, it needs to be manually changed to a eRouter type Class of Service (such as unprovisioned-erouter). This enables the PCP to send domain-name-servers DHCP option (property eRouter/dns/server configured in cnr_ep.properties) during eRouter provisioning.