



## **Cisco Prime Cable Provisioning 5.3 Quick Start Guide**

**First Published:** June 10, 2016

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-26275-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface vii

Audience vii

Product Documentation vii

Obtaining Documentation and Submitting a Service Request viii

Audience 9

Product Documentation 11

Obtaining Documentation and Submitting a Service Request 13

---

### CHAPTER 1

#### Installation Overview 1

Downloading the Prime Cable Provisioning Software Image 1

High-level Installation Flow and Startup 1

---

### CHAPTER 2

#### Installation Requirements 7

Licensing 7

System Requirements 7

Hardware Requirements 9

Solaris PG Hardware Recommendations 9

Solaris RDU Hardware Recommendations 10

Solaris PWS Hardware Recommendations 10

Linux PG Hardware Recommendations 11

Linux RDU Hardware Recommendations 11

Linux PWS Hardware Recommendations 12

Database Requirements 12

File-System Block Size 12

On Solaris 12

On Linux 13

Large File Support 13

On Solaris 13

On Linux 14

Prime Network Registrar Requirements 14

---

## CHAPTER 3

### Preparing for Installation 17

Users and Groups (for Solaris only) 17

Installation Checklist 18

Installation Worksheet 22

---

## CHAPTER 4

### Installing and Uninstalling Prime Cable Provisioning 27

Installing Prime Cable Provisioning 27

Installing Components in Interactive Mode 28

Common Steps for all Components 29

Installing the RDU in Interactive Mode 30

Installing PWS in Interactive Mode 33

Installing DPE in Interactive Mode 36

Installing Prime Network Registrar Extension Points in Interactive Mode 38

Configuring Extensions 41

Validating Extensions 42

Configuring Prime Network Registrar Extension Points Properties File 43

Installing KDC in Interactive Mode 43

Installing Components in Non-interactive Mode 45

Generating the Response File 45

Installing a Component Using the Response File 46

Adding Components 47

Uninstalling Prime Cable Provisioning 47

Post-Uninstallation Task 49

---

## CHAPTER 5

### Setting Up RDU Redundancy 51

Prerequisites 51

RDU HA Setup in Primary-Secondary Mode 53

Preparing RDU Nodes for HA Setup in Primary-Secondary Mode 54

Setting Up RDU Two Node Failover Pair 57

RDU HA Uninstall Scripts 58

RDU Geo Redundancy 59

**CHAPTER 6****Upgrading Prime Cable Provisioning 61**

Upgrade Cisco BAC 4.2.x/PCP 5.x to Prime Cable Provisioning 5.3 61

About Backward Compatibility 62

Licensing After Migration 63

Database Migration 63

Backing Up the RDU Database 64

Recovering the Backed Up RDU Database 65

Verify Database Integrity of Cisco BAC 4.2.x/ PCP 5.x 65

Backing up the Property Files 66

Upgrading RDU from Cisco BAC 4.2.x to PCP 5.3 66

Upgrading RDU from Cisco PCP 5.x to PCP 5.3 67

Upgrading PCP along with HA 68

Upgrading PCP along with HA - Procedure 1 69

Upgrading PCP along with HA - Procedure 2 70

Upgrading PCP along with HA - Procedure 3 70

Upgrading Quagga 71

Migrating the RDU Database 71

Migrating to Prime Cable Provisioning 5.3 Using In-line Migration Script 72

About Migration Performance 75

Migration of Duplicate Class of Service and Node Name 75

RDU Extension Migration 75

Enabling Password Encryption 75

Migrating to Prime Cable Provisioning 5.3 Using Migration Tool 75

Migrating Using a RAM Disk (for Solaris only) 77

Creating RAM Disk Volumes for Migration 77

Using the RAM Disk Volumes for Migration 78

Verifying Database Integrity of Prime Cable Provisioning 5.3 79

DPE Cache Backup and Restore Tool 80

Upgrading DPE from Cisco BAC 4.2.x/ PCP 5.x to PCP 5.3 80

DPE Rollback 81

Upgrading Cisco Prime Network Registrar Extensions 82

Upgrading Prime Network Registrar-EP from Cisco BAC 4.2.x/ PCP 5.x to PCP 5.3 82

Enabling eRouter Capabilities 84

Upgrading KDC from Cisco PCP 5.x to Prime Cable Provisioning 5.3 85

eRouter Migration tool 85

---

**CHAPTER 7****Next Steps 89**

Licensing Prime Cable Provisioning 89

Obtaining a Permanent License 91

Obtaining an Evaluation License 92

Installing Your License File 92

Installing Your KDC License 93

Cisco Prime Network Registrar Configurations 93

Enabling a Cisco Prime Network Registrar Spoofing DNS Server 93

Cisco Prime Network Registrar Extension Point Configuration 94

Sample Script for DOCSIS Modems and Computers 94

Sample Script for DOCSIS Modems and PacketCable eMTA/eDVA 95

Setting Up a Device Provisioning Engine 95

Accessing the DPE CLI 96

Accessing DPE CLI from a Local Host 96

Accessing DPE CLI from a Remote Host 96

Logging In 96

Configuring a DPE for Data 97

Configuring a DPE for Voice Technology 99

Setting Up Voice Technology 99

Controls Available 101



## Preface

---

The *Cisco Prime Cable Provisioning Quick Start Guide* describes general requirements and installation procedures for Cisco Prime Cable Provisioning.

This preface contains the following sections:

- [Audience, page vii](#)
- [Product Documentation, page vii](#)
- [Obtaining Documentation and Submitting a Service Request, page viii](#)

## Audience

System integrators, network administrators, and network technicians use this guide to install Prime Cable Provisioning on the Solaris and Linux operating systems.

## Product Documentation



### Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on [Cisco.com](http://Cisco.com) for any updates.

See the [Cisco Prime Cable Provisioning Documentation Overview](#) for the list of Prime Cable Provisioning guides.

### Related Documentation

See the [Cisco Prime Network Registrar 8.x Documentation Overview](#) for the list of Cisco Prime Network Registrar guides.

See the [Prime Cable Provisioning Compatibility Matrix](#) for the compatibility of the current release with the previous releases.

See the [Prime Cable Provisioning and Prime Network Registrar Compatibility Matrix](#) for the compatibility of the current release with Prime Network Registrar.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.





# Audience

---

System integrators, network administrators, and network technicians use this guide to install Prime Cable Provisioning on the Solaris and Linux operating systems.





# Product Documentation

---



## Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on [Cisco.com](https://www.cisco.com) for any updates.

See the [Cisco Prime Cable Provisioning Documentation Overview](#) for the list of Prime Cable Provisioning guides.

## Related Documentation

See the [Cisco Prime Network Registrar 8.x Documentation Overview](#) for the list of Cisco Prime Network Registrar guides.

See the [Prime Cable Provisioning Compatibility Matrix](#) for the compatibility of the current release with the previous releases.

See the [Prime Cable Provisioning and Prime Network Registrar Compatibility Matrix](#) for the compatibility of the current release with Prime Network Registrar.





## Obtaining Documentation and Submitting a Service Request

---

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.





# CHAPTER 1

## Installation Overview

---

This chapter describes how you can access the software image and also describes the high-level installation steps.

This chapter contains the following sections:

- [Downloading the Prime Cable Provisioning Software Image](#), page 1
- [High-level Installation Flow and Startup](#), page 1

## Downloading the Prime Cable Provisioning Software Image

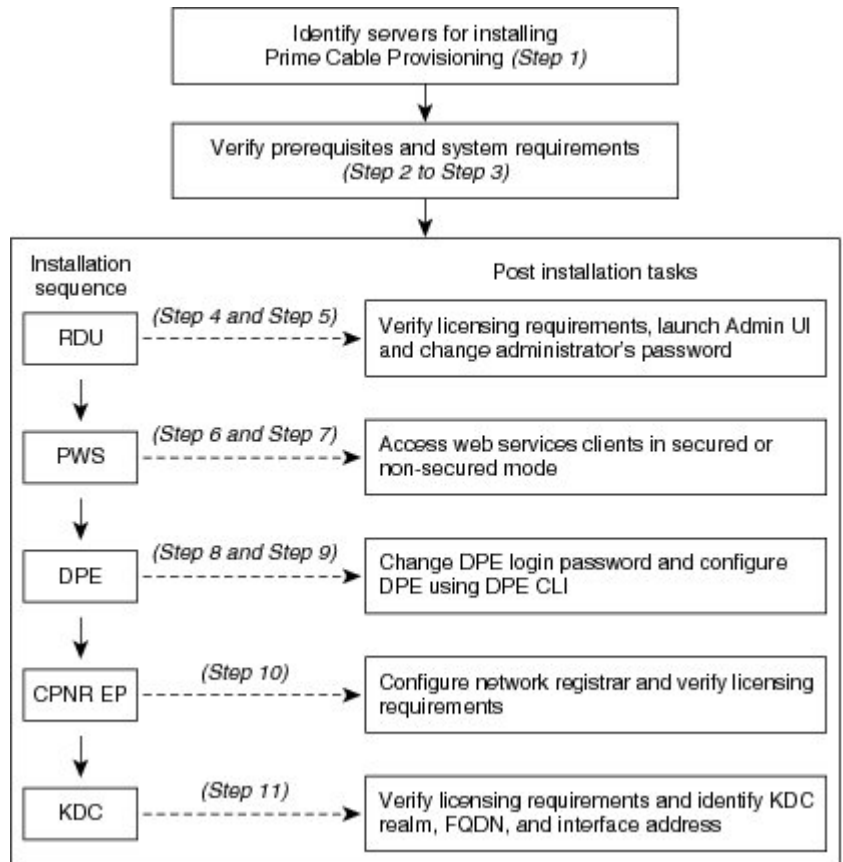
You can download the Prime Cable Provisioning software image either through the product DVD or from the [Download Software](#) page for Prime Cable Provisioning.

## High-level Installation Flow and Startup

This section provides the general flow to complete the Prime Cable Provisioning 5.3 installation. For details about the complete installation, see [Installing Prime Cable Provisioning](#), on page 27.

The following figure provides a high level flow for installing Prime Cable Provisioning 5.3:

**Figure 1: High-level Installation Flow and Startup**



To set up Prime Cable Provisioning 5.3 in your network infrastructure:

## Procedure

- Step 1** Determine the servers on which you are installing the Prime Cable Provisioning components. The components can be installed on the same host server or on different host servers, though the recommendation is to have separate servers for each component.  
**Note** In Linux, if RDU and Prime Network Registrar are installed on the same host server, then the lease query will not work whereas in Solaris it works.
- Step 2** Verify the file-system block size of the directory in which you intend to install the Prime Cable Provisioning database and the database transaction log files. See [File-System Block Size](#), on page 12.
- Step 3** Review the [Installation Checklist](#), on page 18.
- Step 4** Install the RDU. Ensure that you know the location for the Home directory, Data directory, and Database logs directory.
- Step 5** After installing the RDU, ensure that you:
  - a) Obtain a valid Prime Cable Provisioning license to provision devices. For details on obtaining and installing your license file, see [Obtaining a Permanent License](#), on page 91.



You still require separate licenses for the following Prime Cable Provisioning components:

- The DPE
- The KDC, if you configure your network to support secure PacketCable voice technology

b) Verify whether the RDU is running by:

- Checking RDU logs from the location *BPR\_DATA/rdulogs*.
- Checking the status of the bprAgent using the command `/etc/init.d/bprAgent status`

c) Launch the Admin UI.

*//server\_name:port\_number/*

where,

- *server\_name*—Identifies the server on which the RDU is running.
- *port\_number*—Identifies the server port on which the server side of the RDU is running. By default, this port number is:
  - 8100 for HTTP
  - 8443 for HTTPS

The main login screen appears.

d) Login to PCP using default credentials (admin/changeme)

- 1 Enter the default username (**admin**) and password (**changeme**).
- 2 Click **Login**
- 3 To change the default password:
  - Enter a new password; ensure that this password has at least 8 alphanumeric characters, without any special characters.
  - Click **Login**.

**Step 6** Install the PWS. Ensure that you know:

- The RDU server information; hostname, port, username, and password.

**Note** You can also configure the RDU server(s) after the PWS installation using the `ws-cli.sh` tool. The `ws-cli.sh` tool is used to change key PWS configuration properties like adding or deleting the RDU accounts and changing the log severity level. For information about the `ws-cli.sh` tool, see the [Cisco Prime Cable Provisioning User Guide](#).

- The secured port and nonsecured port for web services or API clients.

**Step 7** After installing the PWS, ensure that you can access the web services or API clients in secured mode using HTTPS or nonsecured mode using HTTP. You can use the default port 9443 for secured mode, and 9100 for nonsecured mode.

**Note** If you have configured multiple RDU servers on the same PWS, ensure that the PWS can communicate with all the RDU servers.

**Step 8** Install DPE.

**Step 9** After installing the DPE, ensure that you:

a) Change the DPE login password and the privileged password from the command-line interface (CLI).

- To change the login password, access the CLI in the privileged mode, and enter:

```
bac_dpe# password password
```

where, *password* identifies the new DPE password.

- To change the DPE privileged password, enter:

```
bac_dpe# enable password password
```

where, *password* identifies the local configured password currently in effect or, optionally, provides a new password. If this parameter is omitted, you are prompted for the password. **Note:** The **enable password** is disabled by default.

For more information, see the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#).

b) Configure the DPE from the CLI as required. For configuration instructions, see the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#).

**Step 10** Install and configure Prime Network Registrar, if it is not already installed on your system. We recommend that you use Prime Network Registrar 8.x. For more information on installing Prime Network Registrar, see the [Cisco Prime Network Registrar 8.x Installation Guide](#).

**Note** In Linux, if RDU and Prime Network Registrar are installed on the same server, then the lease query will not work. There is a workaround for Solaris installation for this issue.

- When you install the Prime Network Registrar Local Cluster (LCCM), ensure that you:
  - 1 Install Prime Cable Provisioning extensions on all Prime Network Registrar local cluster servers. See [Installing Prime Cable Provisioning](#), on page 27.
  - 2 Configure Prime Network Registrar, including its extensions. Specifically, you need to configure scopes, policies, client classes, and selection tags. See [Configuring Extensions](#), on page 41. Also see the [Cisco Prime Network Registrar 8.x User Guide](#).
  - 3 Configure the Prime Network Registrar syslog for alerts and debugging information. For information on configuring syslog file for alerts, see the [Cisco Prime Cable Provisioning User Guide](#).
  - 4 Validate the installation by connecting to the Prime Network Registrar web UI and viewing it.
- When you install Prime Network Registrar Regional Cluster (RCCM), ensure that you:
  - 1 Identify the master server for Prime Network Registrar Regional Installation, which administers all the configured Prime Network Registrar local clusters. This server can be Solaris, Windows, or Linux.
  - 2 Obtain a valid central-cluster license file for the Prime Network Registrar Regional Server.
  - 3 After you install the Prime Cable Provisioning extensions on all Prime Network Registrar local servers, replicate the local data into regional and pull the replica address space. For more information, see the [Cisco Prime Network Registrar 8.x User Guide](#).

Alternatively, you can also create subnets, client classes, policies, and so on at RCCM and push them to the required LCCM DHCP server. For more information, see the [Cisco Prime Network Registrar 8.x User Guide](#).

After you complete Prime Network Registrar installation, install Prime Network Registrar Extension Points. For more information see, [Installing Prime Network Registrar Extension Points in Interactive Mode](#), on page 38.

**Step 11** Install and configure the KDC. When you install the KDC, ensure that you:

- Obtain a valid Prime Cable Provisioning license. The KDC license is proprietary and is licensed during Prime Cable Provisioning installation. For information on installing the KDC license, see [Licensing Prime Cable Provisioning](#), on page 89.
- Have the following information at hand:
  - KDC realm—Identified by a unique name, the KDC realm consists of a KDC and the clients and servers registered to that KDC.  
**Note** The realm must match the certificate chain at the KDC.
  - KDC FQDN—Identifies the fully qualified domain name on which the KDC server is located.
  - KDC interface address—Identifies the interface (generally the IP address of the KDC server) on which the KDC listens for requests.

**Step 12** Optionally, configure the syslog file for alerts. You can set up the syslog file on any Prime Cable Provisioning component server. For information on configuring syslog file for alerts, see the [Cisco Prime Cable Provisioning User Guide](#)

---





## Installation Requirements

Before installing Prime Cable Provisioning, review the licensing and the installation requirements described in this chapter.

This chapter contains the following sections:

- [Licensing, page 7](#)
- [System Requirements, page 7](#)
- [Prime Network Registrar Requirements, page 14](#)

## Licensing

Prime Cable Provisioning enables licensing using a licensing file. Each license translates to a DOCSIS IP device. The license file that you receive will contain the number of DOCSIS IP devices that are licensed. For more licensing information, see [Licensing Prime Cable Provisioning, on page 89](#).



### Note

To access this release, you must procure a new license of Prime Cable Provisioning 5.3.

## System Requirements

### On Solaris

In case of Solaris, you must install Prime Cable Provisioning on a Sun SPARC platform that runs a Solaris 10 operating system and 64 bit hardware system with at least 4 GB memory. We recommend that you use a Sun SPARC multiprocessor platform. Also, you must configure coreadm to avoid overriding of core files. For more information, see Solaris documentation.

**Note**

Before installing Prime Cable Provisioning, download and install the recommended Solaris patches from the Oracle support site.

Prime Cable Provisioning ships with the required JRE version 1.6.0\_32, which resides in the `<BPR_HOME>/jre` directory.

You must also download and install the Java Platform Standard Edition (Java SE) cluster patches recommended by Oracle to install Prime Cable Provisioning on a system that runs Solaris 10. See the following table:

**Table 1: Java Standard Edition Cluster Patches for Solaris 10**

| Patch     | Description   |
|-----------|---|
| 120900-04 | Libzonecfg patch  |
| 121133-02 | Zones library and zones utility patch   |
| 119254-44 | Install and patch utilities patch, for more information, see <a href="#">Installing and Uninstalling Prime Cable Provisioning, on page 27</a> |
| 118918-24 | Solaris crypto framework patch  |
| 119042-10 | Svccfg and svcprop patch  |
| 119578-30 | FMA patch   |
| 144488-09 | Kernel patch  |

Before you install Prime Cable Provisioning on Solaris, ensure that you install the `—SUNWxcu4—` package, on the same server. This is an optional package available as part of the Solaris OS installation.

**On Linux**

In case of Linux, Prime Cable Provisioning must be installed on Red Hat Enterprise Linux 6.5, or on CentOS 6.5, using x86-64 (64-bit version of x86), with at least 4 GB memory.

**Note**

**The SELinux should be disabled.**

To disable SELinux feature, modify the `config` file using the following command:

```
# vi /etc/selinux/config
```

'`config`' - is the File that controls the state of SELinux on the system. SELinux value is to be set to '`disabled`' in this file.

Prior to installation of Prime Cable Provisioning on Linux, ensure that the `-sysstat-` package is installed, this is an optional package, for the proper execution of the diagnostic scripts.

RDU Redundancy (an optional feature) can be configured on RHEL 6.5 and CentOS 6.5 platform. For more information on RDU Redundancy, see [Setting Up RDU Redundancy, on page 51](#).

The below 32 bit library files need to be present in the 64 bit server which we are trying to install CNR\_EP.

- libframework.so

- libgssapi\_krb5.so.2
- libk5crypto.so.3
- libkrb5.so.3
- libkrb5support.so.0
- libsasl2.so.2
- libz.so.1

These files can be either in: */usr/lib* or */lib* location.

Once these files are copied to the location, the LD\_LIBRARY\_PATH needs to be updated accordingly with the file location. The DHCP server needs to be restarted.

## Hardware Requirements

The resource recommendations for Solaris and Linux are shown below in the respective topics. Resource recommendations corresponds to the number of devices in the provisioning group or RDU. PWS resource recommendation is independent of the number of devices in the RDU.

[Solaris PG Hardware Recommendations, on page 9](#)

[Solaris RDU Hardware Recommendations, on page 10](#)

[Solaris PWS Hardware Recommendations, on page 10](#)

[Linux PG Hardware Recommendations, on page 11](#)

[Linux RDU Hardware Recommendations, on page 11](#)

[Linux PWS Hardware Recommendations, on page 12](#)



### Note

- The resource recommendations mentioned in the above topics for Solaris and Linux, are the resources required for the components itself. These recommendations does not include the OS overhead or the overhead of any other applications installed on the server.
- **Server/VM configuration:** This is to be configured by considering the resource requirement of the component being installed on the respective Server/VM.

## Solaris PG Hardware Recommendations

| Devices | Server | # Cores | Memory | %Swap | Disk  |
|---------|--------|---------|--------|-------|-------|
| 100K    | DPE    | 2       | 2 GB   | 2 GB  | 20 GB |
|         | KDC    |         |        |       |       |
| 250K    | DPE    | 2       | 2 GB   | 2 GB  | 20 GB |
|         | KDC    |         |        |       |       |

|      |                    |   |      |      |       |
|------|--------------------|---|------|------|-------|
| 500K | DPE                | 2 | 4 GB | 4 GB | 20 GB |
|      | KDC <sup>(1)</sup> |   |      |      |       |
| 1M   | DPE                | 4 | 8 GB | 8 GB | 40 GB |
| 2M   | DPE                |   |      |      |       |

<sup>(1)</sup> No more than 500K SECURE mode MTA devices recommended per provisioning group ( 500K MTA equals 500K eCM and 500K eMTA)

# Cores assumes 8 threads/core (UltraSPARC T2 Core)

%Swap space should be equal or more than memory (RAM)

Solaris DPE that requires 20 GB disk space uses BPR\_DATA=10 GB and BPR\_HOME=10 GB

Solaris DPE that requires 40 GB disk space uses BPR\_DATA=30 GB and BPR\_HOME=10 GB

## Solaris RDU Hardware Recommendations

| Devices                | Server | # Cores | Memory | %Swap | Disk                 |
|------------------------|--------|---------|--------|-------|----------------------|
| 100K                   | RDU    | 2       | 8GB    | 8GB   | 40GB <sup>(1)</sup>  |
| 250K                   |        |         |        |       |                      |
| 500K                   |        |         |        |       |                      |
| 1M                     | RDU    | 4       | 16GB   | 16GB  | 80GB <sup>(2)</sup>  |
| 2M                     |        |         |        |       |                      |
| Greater than 2 Million | RDU    | 8       | 32 GB  | 32GB  | 200GB <sup>(2)</sup> |

<sup>(1)</sup> 3 drive configuration - 1 drive for OS, 1 drive for DB logs and 1 drive for DB

<sup>(2)</sup> External RAID array recommended

# Cores assumes 8 threads/core (UltraSPARC T2 Core)

%Swap space should be equal to memory(RAM)

Solaris RDU that requires 40 GB disk space uses BPR\_DATA=15 GB, BPR\_DBLOG=15 GB and BPR\_HOME=10 GB

Solaris RDU that requires 80 GB disk space uses BPR\_DATA=30 GB, BPR\_DBLOG=30 GB and BPR\_HOME=20 GB

Solaris RDU that requires 200 GB disk space uses BPR\_DATA=150 GB, BPR\_DBLOG=30 GB and BPR\_HOME=20 GB

## Solaris PWS Hardware Recommendations

| Server | # Cores | Memory | %Swap | Disk |
|--------|---------|--------|-------|------|
|--------|---------|--------|-------|------|



|     |   |      |      |       |
|-----|---|------|------|-------|
| PWS | 4 | 4 GB | 4 GB | 20 GB |
|-----|---|------|------|-------|

# Cores assumes 8 threads/core (UltraSPARC T2 Core)

%Swap space should be equal to memory(RAM)

Solaris PWS that requires 20 GB disk space uses BPR\_DATA=10 GB and BPR\_HOME=10 GB

## Linux PG Hardware Recommendations

| Devices | Server             | # Cores | Memory | %Swap | Disk  |
|---------|--------------------|---------|--------|-------|-------|
| 100K    | DPE                | 2       | 2 GB   | 2 GB  | 20 GB |
|         | KDC                |         |        |       |       |
| 250K    | DPE                | 2       | 2 GB   | 2 GB  | 20 GB |
|         | KDC                |         |        |       |       |
| 500K    | DPE                | 2       | 4 GB   | 4 GB  | 20 GB |
|         | KDC <sup>(1)</sup> |         |        |       |       |
| 1M      | DPE                | 4       | 8 GB   | 8 GB  | 40 GB |
| 2M      | DPE                |         |        |       |       |

<sup>(1)</sup> No more than 500K SECURE mode MTA devices recommended per provisioning group ( 500K MTA equals 500K eCM and 500K eMTA)

%Swap space should be equal or more than memory (RAM)

Linux DPE that requires 20 GB disk space uses BPR\_DATA=10 GB and BPR\_HOME=10 GB

Linux DPE that requires 40 GB disk space uses BPR\_DATA=30 GB and BPR\_HOME=10 GB

## Linux RDU Hardware Recommendations

| Devices                | Server | # Cores | Memory | %Swap | Disk                 |
|------------------------|--------|---------|--------|-------|----------------------|
| 100K                   | RDU    | 2       | 8GB    | 8GB   | 40GB <sup>(1)</sup>  |
| 250K                   |        |         |        |       |                      |
| 500K                   |        |         |        |       |                      |
| 1M                     | RDU    | 4       | 16GB   | 16GB  | 80GB <sup>(2)</sup>  |
| 2M                     |        |         |        |       |                      |
| Greater than 2 Million | RDU    | 8       | 32 GB  | 32GB  | 200GB <sup>(2)</sup> |

%Swap space should be equal or more than memory (RAM)

**Linux RDU that requires 40 GB disk space uses BPR\_DATA=15 GB, BPR\_DBLOG=15 GB and BPR\_HOME=10 GB**

**Linux RDU that requires 80 GB disk space uses BPR\_DATA=30 GB, BPR\_DBLOG=30 GB and BPR\_HOME=20 GB**

**Linux RDU that requires 200 GB disk space uses BPR\_DATA=150 GB, BPR\_DBLOG=30 GB and BPR\_HOME=20 GB**

## Linux PWS Hardware Recommendations

| Server | # Cores | Memory | %Swap | Disk  |
|--------|---------|--------|-------|-------|
| PWS    | 4       | 4 GB   | 4 GB  | 20 GB |

**PWS that requires 20 GB disk space uses BPR\_DATA=10 GB and BPR\_HOME=10 GB**

## Database Requirements

Before you install Prime Cable Provisioning 5.3, ensure that the requirement for the file system block size and the support for large files in the file system are met.

### File-System Block Size

#### On Solaris

For optimum performance and reliability of the Prime Cable Provisioning database, configure the file system or systems that contain the database files and database log files with an 8 KB or greater block size. If your system configuration does not support an 8-KB block size, then configure the block size in multiples of 8 KB; for example, 16 KB or 32 KB.



#### Note

The block size cannot be changed after the Unix File System (UFS) is mounted with a value. The value has to be set during Solaris disk partition.

ZFS is a new file system in Solaris 10 OS which provides excellent data integrity and performance compared to other file systems. The default block size for ZFS is 128 KB. In Prime Cable Provisioning, the RDU and DPE support file system with block size of 8 KB to 64 KB. So it is recommended to configure a block size of 8KB for optimal performance.

The installation program prompts you to specify a directory in which to install database files, and database transaction log files. These directories are identified in Prime Cable Provisioning with the system variables BPR\_DATA, and BPR\_DBLOG, respectively. You can specify the same directory for these, which will contain both database files and database transaction log files.

To verify that a directory resides on a file system with a minimum of 8-KB block size:

## Procedure

- Step 1** Run the UNIX **mount** command without any parameters to determine on which file-system device the directory resides. The default directory is */var/CSCObac*.

For example:

```
# mount
```

```
/var on /dev/dsk/c0t0d0s4
read/write/setuid/intr/largefiles/logging/xattr/onerror=panic/
dev=2200004 on Thu Jun 15 16:58:21 2006
```

In this example, the file-system device is */dev/dsk/c0t0d0s4*.

- Step 2** To determine the file-system block size, use the **df** command.  
For example:

```
# df -g /dev/dsk/c0t0d0s4
```

```
/var (/dev/dsk/c0t0d0s4): 8192 block size 1024 frag size
961240 total blocks 851210 free blocks 755086 available 243712 total files
239730 free files 35651588 filesys id
ufs fstype 0x00000004 flag 255 filename length
```

In this example, the block size is 8192 bytes, which is 8 KB. The block size of the selected directory, therefore, is correct.

## On Linux

File system of all components of Prime Cable Provisioning supports a block size of 4 KB.

You can specify the block size when you create the file system using the command **mkfs**. For more details on the command **mkfs**, see **man mkfs** manual page.

To verify that a directory resides on a file system with a minimum of 4 KB block size run the following command:

```
# tune2fs -l /dev/sda2 | grep "Block size"
```

```
Block size: 4096
```

In this example, the block size is 4096 bytes, which is 4 KB.

## Large File Support

Ensure that the file system in which you place database files is configured to support files larger than 2 GB.

## On Solaris

To verify large file support:

## Procedure

- Step 1** Run the UNIX **mount** command without parameters.
- Step 2** Check whether the intended file system contains the keyword **largefiles**.  
For example:

```
# mount
```

```
/var on /dev/dsk/c0t0d0s4
read/write/setuid/intr/largefiles/onerror=panic/dev=2200004 on
Thu Jun 15 08:07:53
```

In this example, the output contains the keyword *largefiles*. This file system, therefore, can support files larger than 2 GB.

**Note** If large file support is not configured, add the *largefiles* option in the file system features using the command:

```
# vi /etc/mnttab
```

## On Linux

To verify large file support:

## Procedure

- Step 1** Run the following command:
- ```
# tune2fs -l /dev/sda2 | grep large_file
```
- Step 2** Check whether the intended file system contains the keyword **large\_file**.

```
Filesystem features: has_journal ext_attr resize_inode dir_index filetype
needs_recovery extent flex_bg sparse_super large_file huge_file uninit_bg
dir_nlink
extra_isize
```

In this example, the output contains the keyword *large\_files*. This file system, therefore, can support files larger than 2 GB.

**Note** If large file support is not configured, modify the file system features using the command **tune2fs** to enable large file support. For more details on the command, see the Linux man page for **tune2fs**.

# Prime Network Registrar Requirements



## Note

To install Prime Network Registrar Extension Points, you must install Prime Network Registrar 8.x.

The following are the prerequisites for installing Prime Network Registrar:

- Prime Network Registrar must be compatible with Prime Cable Provisioning. For details, see [Prime Cable Provisioning and Prime Network Registrar Compatibility Matrix](#).
- You must install the compatible version of Prime Network Registrar 8.x.
- You must install a Prime Network Registrar DHCP server on a computer running Solaris 10, or Linux 6.5, or CentOS 6.5.
- In a failover deployment of Prime Cable Provisioning, you must configure two DHCP servers. For information on configuring failover on Prime Network Registrar servers, see the [Cisco Prime Network Registrar 8.x User Guide](#).
- After you install Prime Cable Provisioning, you must create its scopes and policies in Prime Network Registrar.

**Note**

---

Prime Network Registrar Extension Points must be installed in the Prime Network Registrar setup and it must be able to communicate with the other Prime Cable Provisioning components.

---





## Preparing for Installation

---

This chapter covers the tasks that you must perform before installing Prime Cable Provisioning.

This chapter contains:

- [Users and Groups \(for Solaris only\), page 17](#)
- [Installation Checklist, page 18](#)
- [Installation Worksheet, page 22](#)

### Users and Groups (for Solaris only)

The Prime Cable Provisioning root user can create users and groups, and assign appropriate privileges to the users.

A non-root user should be assigned with the following privileges to run Prime Cable Provisioning:

- file\_chown
- file\_link\_any
- file\_owner
- net\_privaddr
- proc\_exec
- proc\_fork
- proc\_info
- proc\_owner
- proc\_session
- proc\_setid
- net\_access

**Note**

The Prime Cable Provisioning non-root user can run any process associated with socket connection, only if the `net_access` privilege is assigned to the non-root user. The `net_access` privilege is available only in Solaris 10 (update 9 and 10) platform.

**Note**

During installation, it may be necessary to install several Solaris patches on your computer. Should patch installation become necessary, see the Sun Microsystems support site to download these patches. For a list of recommended patches, see [System Requirements](#).

A root user should perform the following pre-installation steps:

**Procedure**

**Step 1** Create groups and users. Assign users to the groups.

**Note** You must have system administrator privileges to create groups and users and assign users to groups.

If you are installing each of the Prime Cable Provisioning components in different servers, then you must create groups and users in all the different servers.

To create a group, run the following command.

```
groupadd -g 1110 baceng
```

where, `-g`—is the argument for representing group ID. This creates a group named `1110 baceng`.

To create a user, run the following command:

```
useradd -u 102 -g 1110 -d /home/user -m -s /bin/sh -c "Test User" user
```

where, `-u`—is the argument for representing user ID, `-g` is the group ID, `-d` is the directory location.

**Step 2** Assign privileges to users using the command:

```
usermod -K defaultpriv=file_chown,file_link_any,file_owner,net_privaddr,proc_exec,proc_fork,proc_info,proc_owner,proc_session,proc_setid user
```

**Step 3** Set password for the user using the command:

```
passwd <user_name>
```

New Password:

Re-enter new Password:

```
passwd: password successfully changed for user
```

where, `<user_name>`—Specifies the name of the root or non-root user.

## Installation Checklist

This section explains the procedures you must follow to install Prime Cable Provisioning.

Before you install Prime Cable Provisioning, ensure that you are ready by reviewing the checklist that the following table describes.



**Table 2: Installation Checklist**

| Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Checkoff                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 1. Verify if your system meets the minimum system hardware and software requirements described in <a href="#">Installation Requirements</a> , on page 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <input type="checkbox"/> |
| 2. Ensure that you have access to the servers on which you intend to install Prime Cable Provisioning components.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <input type="checkbox"/> |
| 3. Save your license file on the system from which you intend to launch the Prime Cable Provisioning Admin UI via a web browser. You need a valid license file to configure Prime Cable Provisioning licensing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <input type="checkbox"/> |
| 4. Determine the home directory ( <i>BPR_HOME</i> ) in which you want to install the Prime Cable Provisioning component or components. The default directory is <i>/opt/CSCObac</i> . Ensure that the target installation directory has enough disk space.<br><b>Note</b> We recommend that you have at least 1 GB of disk space available in <i>BPR_HOME</i> otherwise launching the Admin UI might result in some errors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <input type="checkbox"/> |
| 5. For the RDU, determine where you want to install the data directory ( <i>BPR_DATA</i> ) and the database logs ( <i>BPR_DBLOG</i> ). The default directory is <i>/var/CSCObac</i> . Ensure that the target installation directory has enough disk space.<br><b>Note</b> The RDU and the DPE database directory must be empty or manually cleaned up before proceeding with the Prime Cable Provisioning installation. A warning message is displayed. If you click OK, the database directory is deleted.<br><b>Note</b> We recommend that you locate the data directory on a different physical disk than the home directory; for example, <i>/var/disk0/CSCObac</i> . The disk should have at least 8 GB and up to 30 GB of free space. The installation program, by default, installs the data directory, the database transaction logs directory, and the logs directory in the same location. We recommend that you locate the database transaction logs directory on the fastest disk on the system. Also, ensure that 8 GB of disk space is available. The minimum required free space may be greater than 8 GB, depending on the number of devices and the required log level. | <input type="checkbox"/> |
| 6. Verify that you have minimum 500 MB of free space available in the <i>/tmp</i> directory for successful installation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <input type="checkbox"/> |
| 7. The RDU uses an interface (listening port number) to communicate with other Prime Cable Provisioning components. Ensure that this port is not used by any other processes. The default port is 49187 for non-secured communication, and 49188 for secured communication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <input type="checkbox"/> |

| Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Checkoff                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <p>8. Determine the certificate details to generate the certificates for RDU, Admin UI, and PWS, used for SSL or HTTPS communication.</p> <p><b>Note</b> You can also generate the certificates after installing Prime Cable Provisioning, and create a Certificate Signing Request (CSR) for an un-signed certificate. For information on how to generate certificates, import certificates in key store, and create a CSR, see the <a href="#">Cisco Prime Cable Provisioning User Guide</a>.</p> | <input type="checkbox"/> |
| 9. Determine the location of the certificate files and enter it correctly when prompted. The default location is <i>/tmp</i> . If you enter an incorrect location, it falls back to the nonsecure mode.                                                                                                                                                                                                                                                                                             | <input type="checkbox"/> |
| 10. Determine the shared secret for the RDU. The Prime Cable Provisioning components (DPE and Prime Network Registrar Extension Points) use shared secret as a token to authenticate with the RDU. Ensure that you configure the same shared secret while installing the Prime Cable Provisioning components.                                                                                                                                                                                       | <input type="checkbox"/> |
| 11. Determine the secret key that is used to encrypt the shared secret for the RDU. The Prime Cable Provisioning components (DPE and Prime Network Registrar Extension Points) use the secret key for double encryption, apart from the shared secret. Ensure that you configure the same secret key while installing the Prime Cable Provisioning components.                                                                                                                                      | <input type="checkbox"/> |
| 12. Determine the key store password to be used for the key store. The key store stores the certificate keys. For more information about key store, see the <a href="#">Cisco Prime Cable Provisioning User Guide</a> .                                                                                                                                                                                                                                                                             | <input type="checkbox"/> |
| 13. Determine the key password used for storing the private keys for the Admin UI, PWS, and the RDU.                                                                                                                                                                                                                                                                                                                                                                                                | <input type="checkbox"/> |
| <p>14. Determine the ports used to access the Admin UI using HTTP or HTTP over SSL (HTTPS). The default ports are:</p> <ul style="list-style-type: none"> <li>• 8100—Listening port on Admin UI web server for HTTP communication</li> <li>• 8443—Listening port on Admin UI web server for HTTPS communication</li> </ul>                                                                                                                                                                          | <input type="checkbox"/> |
| <p>15. Determine the ports used to access the PWS using HTTP or HTTP over SSL (HTTPS). The default ports are:</p> <ul style="list-style-type: none"> <li>• 9100—Listening port on PWS web server for HTTP communication</li> <li>• 9443—Listening port on PWS web server for HTTPS communication</li> </ul>                                                                                                                                                                                         | <input type="checkbox"/> |

| Task                                                                                                                                                                                                                                                                                 | Checkoff                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 16. For the DPE, ensure that 2 GB of disk space is available in the data directory.                                                                                                                                                                                                  | <input type="checkbox"/> |
| 17. For the PWS, ensure that 500 MB of disk space is available in the data directory.                                                                                                                                                                                                | <input type="checkbox"/> |
| 18. The PWS can communicate only with the Prime Cable Provisioning 5.3 RDU. It is not compatible with the RDUs of earlier versions. If you configure multiple RDU servers with PWS, ensure that the information of all the RDU servers is available.                                 | <input type="checkbox"/> |
| 19. The web server for PWS and Admin UI must be configured and functioning normally.                                                                                                                                                                                                 | <input type="checkbox"/> |
| 20. Ensure that Prime Network Registrar 8.x is installed and running on the servers on which you are installing Prime Cable Provisioning extensions, that is, the Prime Network Registrar Extension Points.                                                                          | <input type="checkbox"/> |
| 21. For the Prime Network Registrar extensions, determine the name of the provisioning group for the Prime Network Registrar server.                                                                                                                                                 | <input type="checkbox"/> |
| 22. For the Prime Network Registrar extensions, determine the location to install the data directory ( <i>BPR_DATA</i> ). The default directory is <i>/var/CSCObac</i> .                                                                                                             | <input type="checkbox"/> |
| 23. Verify that you have the necessary Prime Network Registrar configuration files. For an example of these configuration files, see the <a href="#">Cisco Prime Network Registrar Configurations, on page 93</a> .                                                                  | <input type="checkbox"/> |
| 24. Verify that you have the KDC servers available, if you want to configure your network to support secure PacketCable voice technology.                                                                                                                                            | <input type="checkbox"/> |
| 25. Enable your server to support IPv6.<br>To enable IPv6, login as root, and run:<br><br><pre># ifconfig intf inet6 plumb up</pre> <pre># /usr/lib/inet/in.ndpd</pre> <pre># touch /etc/hostname6.intf</pre> where, intf—identifies the interface on which you want to enable IPv6. | <input type="checkbox"/> |
| <b>In case of Linux, perform the following extra steps</b>                                                                                                                                                                                                                           |                          |

| Task                                                                                                                                                                                                                                                         | Checkoff                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 26. Modify the <i>config</i> file to disable SELinux using the following command:<br><pre># vi /etc/selinux/config</pre> where, config—File that controls the state of SELinux on the system.<br>In this file, set the value of SELINUX to <i>disabled</i> . | <input type="checkbox"/> |
| 27. Disable iptables using the following command:<br><pre># chkconfig iptables off</pre> <b>Note</b> The Admin UI page will not open if iptables is in enabled state on the system.                                                                          | <input type="checkbox"/> |
| 28. Reboot the Prime Cable Provisioning host using the following command:<br><pre># reboot</pre>                                                                                                                                                             | <input type="checkbox"/> |
| 29. Wait till the server boots up and re-login to continue with the installation.                                                                                                                                                                            | <input type="checkbox"/> |

## Installation Worksheet

During the installation of Prime Cable Provisioning, you are prompted for configuration information. The following table is a worksheet that you can use to record the information specific to your installation.

**Table 3: Prime Cable Provisioning Installation Parameters**

| Prompt                  | Description                                                                                    | Default Value                                                                                                                                                                               | Your Value |
|-------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Home directory          | Root directory to install Prime Cable Provisioning component                                   | <i>/opt/CSCObac</i>                                                                                                                                                                         |            |
| Data directory          | Root directory to install the data directory for Prime Cable Provisioning component            | <i>/var/CSCObac</i>                                                                                                                                                                         |            |
| Database logs directory | Root directory to install the database transaction logs for Prime Cable Provisioning component | <i>/var/CSCObac/rdu/dblog</i>                                                                                                                                                               |            |
| Logs directory          | Root directory to install the general transaction logs for Prime Cable Provisioning components | <ul style="list-style-type: none"> <li>• For RDU: <i>/var/CSCObac/rdu/logs</i></li> <li>• For DPE: <i>/var/CSCObac/dpe/logs</i></li> <li>• For PWS: <i>/var/CSCObac/pws/logs</i></li> </ul> |            |
| RDU host                | Hostname of the server on which the RDU is installed                                           | None                                                                                                                                                                                        |            |

| Prompt                                                           | Description                                                                                                                                                                                                                                                                         | Default Value | Your Value |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------|
| RDU port number for nonsecured communication                     | Port number through which the RDU communicates with other Prime Cable Provisioning components in nonsecured mode                                                                                                                                                                    | 49187         |            |
| RDU port number for secured communication                        | Port number through which the RDU communicates with other Prime Cable Provisioning components in secured mode using SSL                                                                                                                                                             | 49188         |            |
| Prime Network Registrar Extension Points provisioning group name | Name of the provisioning group for Prime Network Registrar Extension Points                                                                                                                                                                                                         | None          |            |
| KDC realm name                                                   | Name of the Kerberos realm required by the KDC component                                                                                                                                                                                                                            | None          |            |
| KDC service key                                                  | Service key that the KDC server uses for communication with the provisioning FQDNs of DPEs                                                                                                                                                                                          | None          |            |
| Response file                                                    | Name and location of the response file that you generate to install these components during a noninteractive installation: <ul style="list-style-type: none"> <li>• RDU</li> <li>• PWS</li> <li>• DPE</li> <li>• Prime Network Registrar Extension Points</li> <li>• KDC</li> </ul> | None          |            |
| Port number of Admin UI                                          | Port number through which you access the Prime Cable Provisioning Admin UI using HTTP                                                                                                                                                                                               | 8100          |            |
|                                                                  | Port number through which you access the Prime Cable Provisioning Admin UI using HTTP over SSL (HTTPS)                                                                                                                                                                              | 8443          |            |

| Prompt                                      | Description                                                                                                                                                    | Default Value                                                                                                                            | Your Value |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Port number of web services and API clients | Port number through which you access the web services or API clients using HTTP                                                                                | 9100                                                                                                                                     |            |
|                                             | Port number through which you access the web services or API clients using HTTP over SSL (HTTPS)                                                               | 9443                                                                                                                                     |            |
| Admin UI user password                      | Password using which you access the Prime Cable Provisioning Admin UI                                                                                          | changeme                                                                                                                                 |            |
| Web UI password                             | Password using which you access the Prime Network Registrar Admin UI                                                                                           | changeme                                                                                                                                 |            |
| Shared Secret password                      | Password using which you can encrypt the communication between Prime Cable Provisioning components and RDU                                                     | None                                                                                                                                     |            |
| Shared Secret key                           | Key using which you can encrypt the shared secret password                                                                                                     | None                                                                                                                                     |            |
| Key Store password                          | Password using which you can encrypt the key store                                                                                                             | None                                                                                                                                     |            |
| Key password                                | Password using which you can encrypt the certificate keys added in the key store                                                                               | None                                                                                                                                     |            |
| Certificate files location                  | The location of the certificate files.                                                                                                                         | Default location (certificate is stored in these files):<br>/opt/CSCObac/lib/security/rootCA.crt<br>/opt/CSCObac/lib/security/rootCA.pem |            |
| Certificate details                         | The inputs to generate the RDU certificate, Admin UI certificate, and the PWS certificate. The certificate is used for authentication during SSL communication | Unknown                                                                                                                                  |            |
| DPE password                                | Password using which you access the DPE in the login mode                                                                                                      | changeme                                                                                                                                 |            |
|                                             | Password using which you access the DPE in the privileged mode                                                                                                 | None                                                                                                                                     |            |
| User and Group                              | Name of a root or non-root user                                                                                                                                | root/user1                                                                                                                               |            |
|                                             | Name of a root or non-root group                                                                                                                               | root/group1                                                                                                                              |            |









## CHAPTER

# 4

# Installing and Uninstalling Prime Cable Provisioning

This chapter describes how to work with the installation program. The installation steps for Solaris and Linux are identical with a very few exceptions.



### Note

The procedure of running Prime Cable Provisioning as a non-root user is similar to that of a root user. The non-root user should have appropriate permissions to run the product. For list of permissions, see [Installation Checklist](#), on page 18. Non-root is supported only on Solaris.

This chapter contains the following sections:

- [Installing Prime Cable Provisioning](#), page 27
- [Uninstalling Prime Cable Provisioning](#), page 47
- [Post-Uninstallation Task](#), page 49

## Installing Prime Cable Provisioning

To install Prime Cable Provisioning 5.3:



### Note

To configure Prime Cable Provisioning in SSL mode post installation, refer to the section **Configuring SSL Post Installation** in [Cisco Prime Cable Provisioning 5.3 User Guide](#)

### Procedure

- Step 1** Log into the intended Prime Cable Provisioning host as *root*.
- Step 2** At the system prompt, change directory to your CD-ROM drive or other installation media. Ensure that the **gzip** and **gtar** utilities are available on your system to decompress and unpack the Prime Cable Provisioning 5.3 installation file, and:

- 1 Change to the directory in which you will decompress and extract the installation file.
- 2 Extract the file with the *.gtar.gz* extension. Enter:

For Solaris:

```
# <install_path>/gtar -zxvf BAC_53_SolarisK9.gtar.gz
```

For Linux:

```
# <install_path>/gtar -zxvf BAC_53_LinuxK9.gtar.gz
```

The utility creates the *BAC\_53\_SolarisK9* or *BAC\_53\_LinuxK9* directory into which the installation program is extracted.

**Note** If the program displays a checksum error while unpacking, specify the path to the GNU tar on your machine.

**Step 3** After the installation program is extracted, you can choose to install the components either in interactive or in non-interactive mode.

- [Installing Components in Interactive Mode, on page 28](#)
  - [Installing Components in Non-interactive Mode, on page 45](#)
- 

## Installing Components in Interactive Mode

This section explains how to install Prime Cable Provisioning 5.3 components interactively from the command line.



**Note**

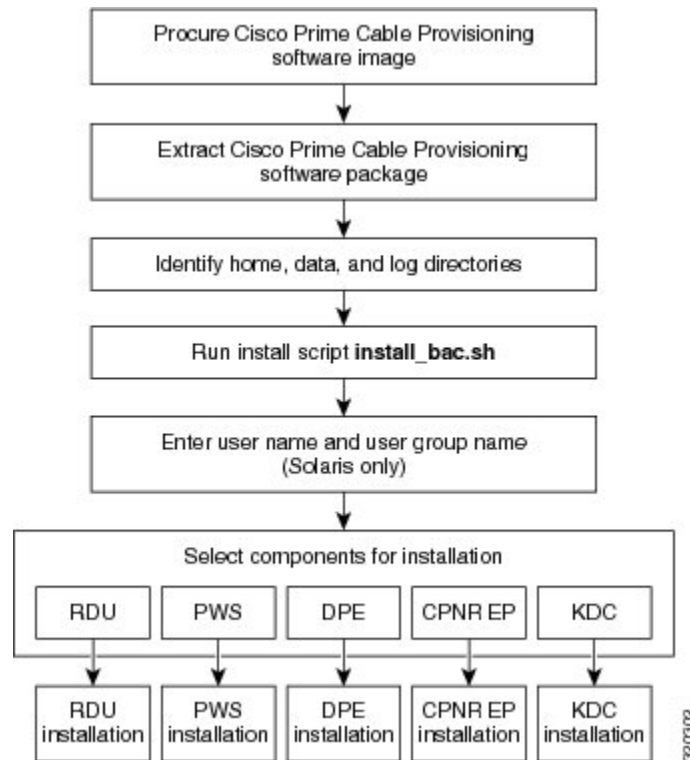
Before you begin any of these procedures, you must complete the initial procedure described in [Installation Checklist, on page 18](#).

---

## Common Steps for all Components

Perform the following steps to start the installation program. The following figure describes the workflow of installation steps that are common for all Prime Cable Provisioning components.

**Figure 2: Common Installation Steps**



To install Prime Cable Provisioning:

### Procedure

#### Step 1 Enter the following command:

On Solaris:

```
# <install-path>/BAC_53_SolarisK9/install_bac.sh
```

On Linux:

```
# <install-path>/BAC_53_LinuxK9/install_bac.sh
```

where, *<install-path>*—Specifies the complete path to the directory in which the *BAC\_53\_SolarisK9* or *BAC\_53\_LinuxK9* directory has been created.

The installation program checks for the Prime Cable Provisioning components installed on the host server. When the check ends, a message appears informing the possible installation modes; interactive and non-interactive, and the location where the response file is to be stored for non-interactive mode.

The installation program prompts you to select whether to proceed with the non-interactive mode or the interactive mode. The default value is set as **n** to proceed with interactive mode.

**Step 2** Press **Enter** to proceed with interactive mode.

The installation program prompts you to add username and user group name. This step is applicable only in case of Solaris as non-root user support is available only on Solaris and not on Linux.

**Step 3** Specify the username and group name to run Prime Cable Provisioning.

**Note** If you want to run Prime Cable Provisioning as a root user, enter the user and user group as root.

**Step 4** Press **Enter** to continue.

In case IPv6 is not enabled in the system, a warning message is displayed. You can either [Enable your machine to support IPv6](#), and continue with the installation, or just continue with the installation without enabling IPv6.

---

After you complete performing the steps explained in [Common Steps for all Components](#), on page 29, perform the following individual component level steps:

- [Installing the RDU in Interactive Mode](#), on page 30
- [Installing PWS in Interactive Mode](#), on page 33
- [Installing DPE in Interactive Mode](#), on page 36
- [Installing Prime Network Registrar Extension Points in Interactive Mode](#), on page 38
- [Installing KDC in Interactive Mode](#), on page 43

## Installing the RDU in Interactive Mode

Install the RDU on a server that meets the requirements described in [System Requirements](#), on page 7. You should install the RDU on a high-end system that is the most reliable server in your network.



**Note**

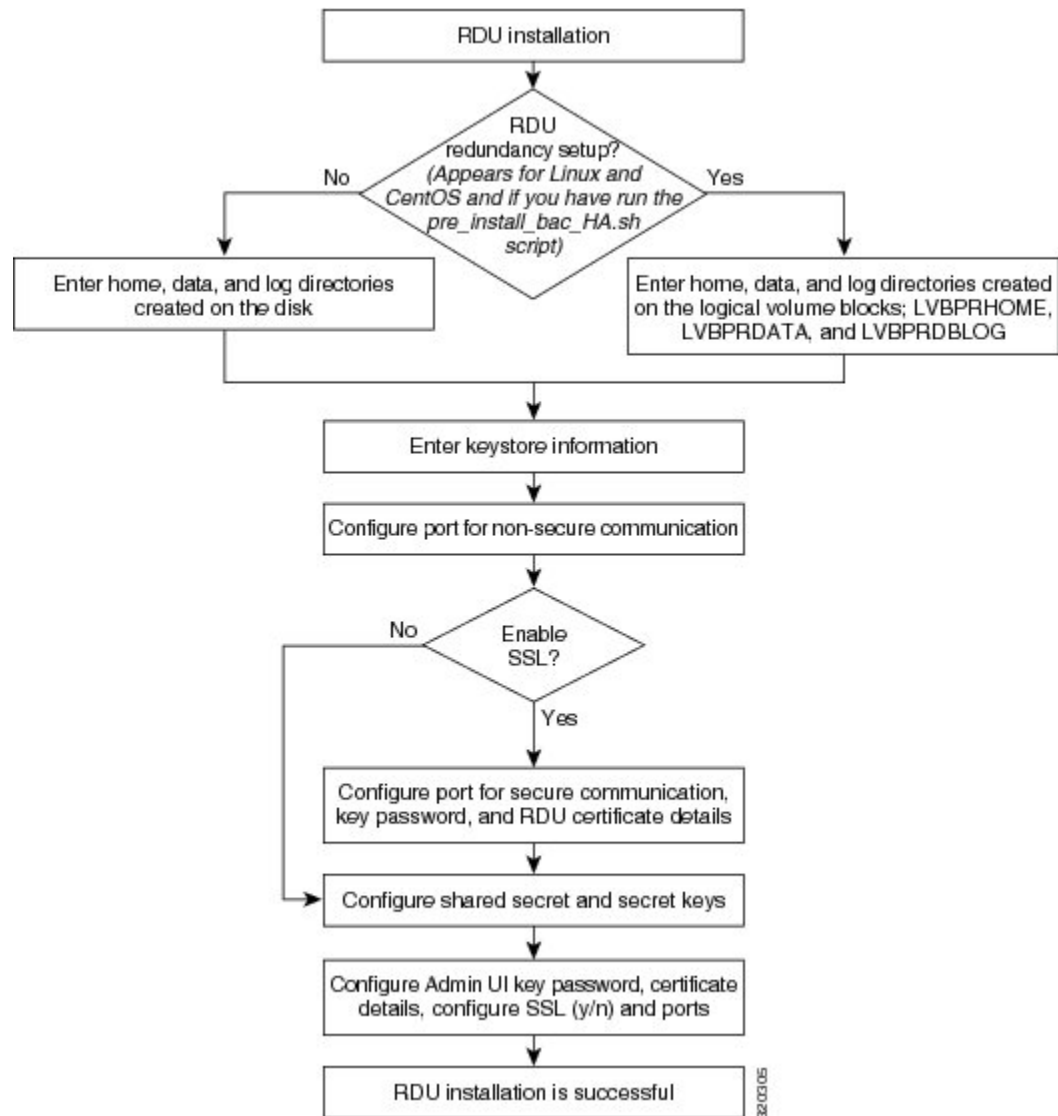
---

We recommend that you configure the RDU server to use a static IP address.

---

The following figure provides a high level RDU installation workflow.

**Figure 3: RDU Installation**



To install the RDU:

### Procedure

- 
- Step 1** Perform steps 1 to 4 from [Common Steps for all Components](#) , on page 29.
- Step 2** From the installer, select RDU as the component.  
Prime Cable Provisioning performs lease query requests by binding to the IP addresses and ports that are described in the following table.

**Table 4: Lease Query Address for Binding**

| Protocol | IP Address            | Port |
|----------|-----------------------|------|
| IPv4     | Wildcard <sup>1</sup> | 67   |
| IPv6     | Wildcard              | 547  |

<sup>1</sup> The wildcard is a special local IP address. It usually means “any” and can only be used for bind operations.

If the installation program detects that either of these ports is being used by another process, it recommends that you use the dynamic ports that the operating system selects.

If you have run the pre-installation script **pre\_install\_bac\_HA.sh** with the operating system as Linux 6.5, the installation program prompts you to select whether to proceed with the RDU redundancy setup or not.

- Step 3** Enter **y** to proceed with the RDU redundancy setup and **n** to proceed with RDU non-redundancy setup. The default is **y**.
- Step 4** To accept the default home, data, and database log directories, press **Enter** for each directory prompt; or enter different directory locations.
- Note** For RDU redundancy feature, the default home, data, and database log directories exist on the logical volume blocks. For example, the default home, data, and database log directories may exist on the logical volume blocks; **LVBPRHOME** mounted on */bprHome*, **LVBPRDATA** mounted on */bprData*, and **LVBPRLOG** mounted on */bprLog*. You can also enter different directory locations.
- Step 5** Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.
- Step 6** To accept the default listening port number, 49187, press **Enter**; or enter another port number. The listening port is the port number that the RDU uses to communicate with other Prime Cable Provisioning components.
- Caution** If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. For details on configuring the DPE, see the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#).
- Step 7** To enable RDU secure mode communication, enter **y**. For nonsecure communication, enter **n**. If you have enabled the RDU secure communication, the installation program prompts you to enter the default port for secure communication, key password, and RDU certificate details. For nonsecure communication, the installation program skips these prompts.
- Step 8** To accept the default port number for secure communication, 49188, press **Enter**; or enter another port number. Ensure that you enter the port number that is created for secure communication in RDU.
- Step 9** Enter the key password and confirm the key password. The key password is used to encrypt the RDU certificate key in the key store.
- Step 10** Enter the RDU certificate details used for SSL communication.
- Step 11** Enter the shared secret password that you want to use for authentication among Prime Cable Provisioning servers, and confirm the password. The shared secret password is used to encrypt the information shared between Prime Cable Provisioning servers.
- Note** You must use the same shared secret password for the RDU, all DPEs, and Prime Network Registrar Extension Points in your network.

- Step 12** Enter the secret key password that you want to use for shared secret authentication, and confirm the secret key password. The secret key password is used to encrypt the shared secret password.
- Step 13** Enter the key password for Admin UI certificate, and confirm the password. The key password is used to encrypt the Admin UI certificate key in the key store.
- Step 14** Enter the Admin UI certificate details used for SSL communication.
- Step 15** Store the certificate details and enter **y**.  
The installation program prompts you to select whether to enable the secure mode communication between RDU and API clients. The default value is set as **n** to proceed with nonsecure mode communication
- Step 16** Enter **y** to enable the secure communication mode.  
The installation program adds the certificate to the key store. This certificate is used for authentication during SSL communication.
- Step 17** To accept the default port, 8100, press **Enter**; or enter another port number.
- Step 18** To accept the default HTTPS port, 8443, press **Enter**; or enter another port number.
- Step 19** The RDU component of Prime Cable Provisioning is installed on the host.  
After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

## Installing PWS in Interactive Mode

Install the PWS (Provisioning Web Services) on a server that meets the requirements described in [System Requirements](#), on page 7.

**Note**

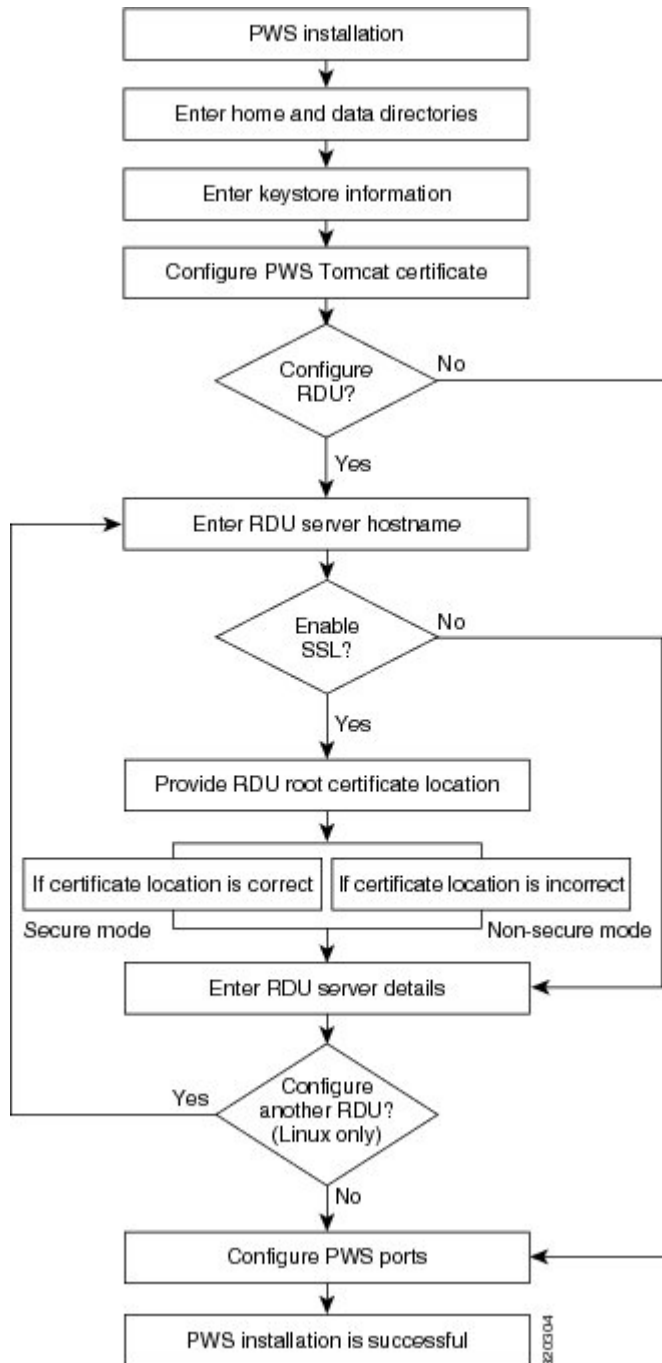
If you are installing both RDU and PWS on the same server, the installation configurations chosen for PWS take precedence over the Admin UI configurations. For example, if you have chosen secured mode of communication for Admin UI and non-secured mode for PWS, non-secured mode is chosen for both Admin UI and PWS.

**Note**

We recommend that you configure the PWS server to use a static IP address.

The following figure provides a high level PWS installation workflow.

**Figure 4: PWS Installation**



To install the PWS:



## Procedure

- Step 1** Perform steps 1 to 4 from [Common Steps for all Components](#) , on page 29.  
From the installer, select PWS as the component.
- Step 2** To accept the default home directory, `/opt/CSCObac`, press **Enter**; or enter another directory.
- Step 3** To accept the default data directory, `/var/CSCObac`, press **Enter**; or enter another directory.
- Step 4** Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.
- Step 5** Enter the key password, and confirm the key password. The key password is used to encrypt the PWS certificate key in the key store.
- Step 6** Enter the PWS certificate details used for SSL communication.
- Step 7** Store the certificate details; enter **y** to continue.  
The installation program prompts you to enter the RDU information.
- Step 8** To add RDU information, enter **y**.
- Step 9** Enter RDU hostname.  
The installation program prompts you to select whether to enable the secure mode communication between RDU and PWS web server. The default value is set as **n** to proceed with nonsecure mode communication.
- Step 10** To enable secure communication, enter **y**. For nonsecure communication, enter **n**.  
If you have enabled secure communication, the installation program prompts you to enter the RDU certificate location. For nonsecure communication, the installation program skips this prompt.
- Step 11** To accept the default RDU certificate location, `[/tmp/rootCA.crt]`, press **Enter**; or enter another location.  
Ensure that you enter the location where the RDU certificate is placed else the communication mode falls back to nonsecured mode. If PWS is installed on a separate web server, ensure that you copy the RDU certificate from the location `$BPR_HOME/lib/security/` on the PWS web server.
- Note** For every RDU added, certificates must be placed in separate locations.  
The installation program adds the certificate to the trust store. This certificate is used for authentication during SSL communication.  
The installation program prompts you to enter the RDU information.
- Step 12** Enter RDU information; port, username, and password, and press **Enter** to continue.  
The installation program prompts you to confirm the RDU information.
- Step 13** Enter **y** and press **Enter** to continue.  
The installation program prompts you to add the second RDU.
- Step 14** On Linux, repeat step 9 to 13 to add multiple RDUs, else enter **n**. The PWS component can communicate with multiple RDUs.
- Note** You can also configure RDUs after the PWS installation using the `ws-cli.sh` tool. The `ws-cli.sh` tool is used to change key PWS configuration properties like adding or deleting the RDU accounts and changing the log severity level. On Solaris, configuring multiple RDUs is not possible during the PWS installation. You must use the `ws-cli.sh` tool to configure the RDUs . RDU added using the `ws-cli.sh` tool is always in the nonsecured mode. For information on how to run the `ws-cli.sh` tool, see the [Cisco Prime Cable Provisioning User Guide](#).

- Step 15** To accept the default PWS HTTP port for the API clients, 9100, press **Enter**; or enter another port number.
- Step 16** To accept the default PWS HTTPS port for the API clients, 9443, press **Enter**; or enter another port number.
- Step 17** Confirm the PWS installation information; enter **y** and press **Enter**.
- Step 18** Press **Enter** to continue. The PWS component of Prime Cable Provisioning is installed on the host. After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

## Installing DPE in Interactive Mode

Install the DPE on a server that meets the requirements described in [System Requirements](#), on page 7.



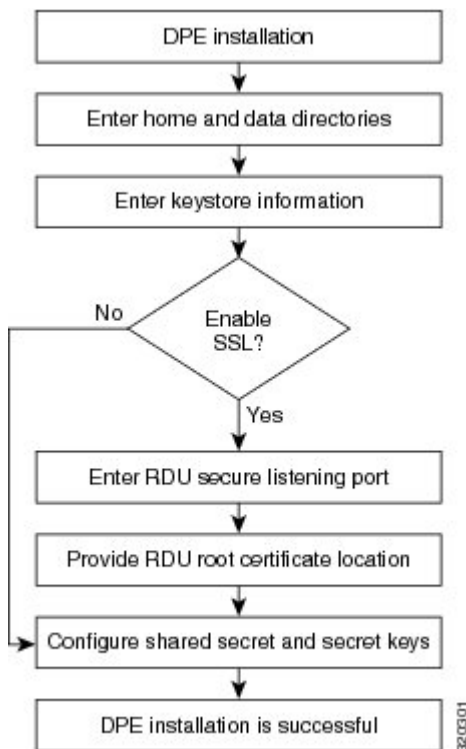
### Note

We recommend that you configure the DPE server to use a static IP address.

During DPE installation, if the program detects a TFTP server or a ToD server running on the same server as the DPE, the installation displays an error message and quits. To stop the TFTP or ToD server, carry out the steps that the error message lists.

The following figure provides a high level DPE installation workflow.

**Figure 5: DPE Installation**



To install the DPE:

### Procedure

- 
- Step 1** Perform steps 1 to 4 from [Common Steps for all Components](#) , on page 29.  
From the installer, select DPE as the component.
- Step 2** To accept the default home directory, `/opt/CSCObac`, press **Enter**; or enter another directory.
- Step 3** To accept the default data directory, `/var/CSCObac`, press **Enter**; or enter another directory.  
**Note** A message is displayed in case there is not enough space in the directory.
- Step 4** Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.  
The installation program prompts you to select whether to enable the secure mode communication between RDU and DPE. The default value is set as **n** to proceed with nonsecure mode communication.
- Step 5** To enable secure communication, enter **y**. For nonsecure communication, enter **n**.  
If you have enabled secure communication, the installation program prompts you to enter the default port for secure communication and RDU certificate location. For nonsecure communication, the installation program skips these prompts.
- Step 6** To accept the default port number for secured communication, 49188, press **Enter**; or enter another port number. Ensure that you enter the port number that is created for secure communication in RDU.
- Step 7** Confirm the listening port number for secured communication; enter **y** to continue.
- Step 8** To accept the default RDU certificate location, `[/tmp/rootCA.crt]`, press **Enter**; or enter another location. Ensure that you enter the location where the RDU certificate is placed else the communication mode falls back to nonsecured mode. If DPE is installed on a separate server, ensure that you copy the RDU certificate from the location `$BPR_HOME/lib/security/` to the DPE server.  
The installation program prompts you to enter the authentication password for Prime Cable Provisioning servers.
- Step 9** Enter the shared secret password that you want to use for authentication among Prime Cable Provisioning servers, and confirm the password. The shared secret password is used to encrypt the information shared between Prime Cable Provisioning servers.  
**Note** You must use the same shared secret password for the RDU, all DPEs, and Prime Network Registrar extension points in your network.
- Step 10** Enter the secret key password that you want to use for shared secret authentication, and confirm the secret key password. The shared secret key password is used to encrypt the shared secret password.
- Step 11** Press **Enter** to continue. The DPE component of Prime Cable Provisioning is installed on the host.  
After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

**Note** After you install the DPE, you must configure the DPE with the RDU. For details, see [Setting Up a Device Provisioning Engine](#), on page 95.

---

## Installing Prime Network Registrar Extension Points in Interactive Mode

Install Prime Cable Provisioning extensions on all Prime Network Registrar servers in your network infrastructure. If you are deploying Prime Cable Provisioning in a failover environment, you must also install the extensions on the failover servers. After you install extensions, you must configure them. This section explains how to install, configure, and validate these extensions.

**Note**

---

We recommend that you configure the Prime Network Registrar server to use a static IP address.

---

Before you install Prime Network Registrar Extension Points, complete the initial installation described in [Installation Checklist, on page 18](#). Ensure that Prime Network Registrar is installed and running. To install Prime Network Registrar, see the [Cisco Prime Network Registrar 8.x Installation Guide](#).

**Note**

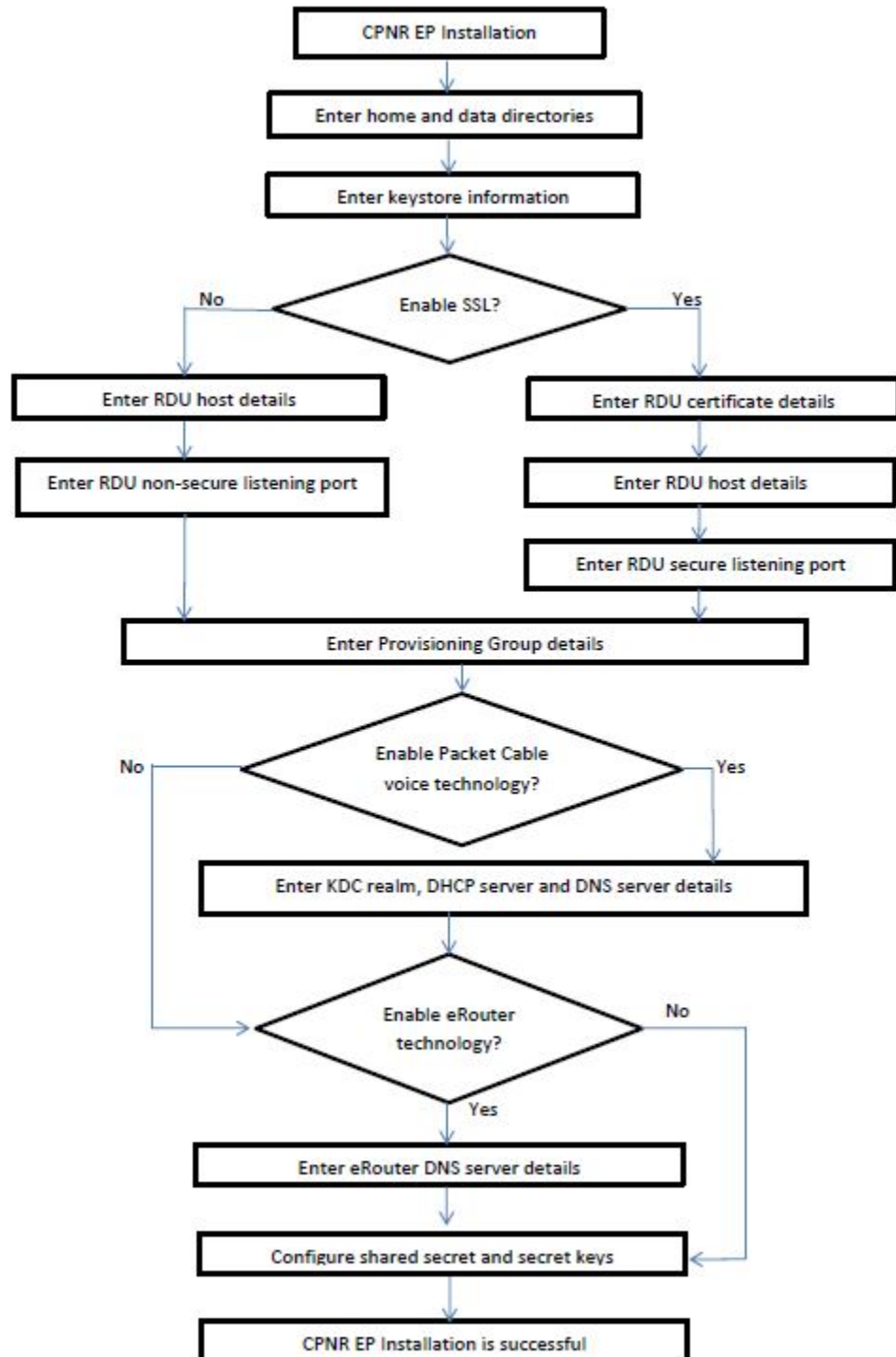
---

For SSL to work on a fresh installation of Prime Cable Provisioning, you must install Prime Network Registrar 8.x or higher and then install the extension points.

---

The following figure provides a high level Prime Network Registrar extension point installation workflow.

**Figure 6: Prime Network Registrar Extension Point Installation**



To install Prime Network Registrar extension points:

### Procedure

- 
- Step 1** Perform steps 1 to 4 from [Common Steps for all Components](#), on page 29.  
From the installer, select CPNR EP as the component.
- Step 2** The installation program prompts you to select whether to proceed with the 64-bit mode or 32-bit mode. The default value is set as y to proceed with 64-bit mode, press **Enter**; or enter n to proceed with 32-bit mode.
- Step 3** To accept the default home directory, */opt/CSCObac*, press **Enter**; or enter another directory.
- Step 4** To accept the default data directory, */var/CSCObac*, press **Enter**; or enter another directory.
- Step 5** Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.  
The installation program prompts you to select whether to enable the secure mode communication between RDU and Prime Network Registrar extension point. The default is set as n to proceed with nonsecure mode communication.
- Step 6** To enable secure communication, enter **y**. For nonsecure communication, enter **n**.  
If you have enabled secure communication, the installation program prompts you to enter the RDU certificate location and default port for secure communication. For nonsecure communication, the installation program skips these prompts.
- Step 7** To accept the default RDU certificate location, *[/tmp/rootCA.pem]*, press **Enter**; or enter another location. Ensure that you enter the location where the RDU certificate is placed else the communication mode falls back to nonsecured mode. If Prime Network Registrar is installed on a separate server, ensure that you copy the RDU certificate from the location *\$BPR\_HOME/lib/security/* on the Prime Network Registrar server. The installation program prompts you to enter the RDU's IP address or hostname.
- Step 8** To accept the default RDU's IP address or hostname, press **Enter**; or enter another RDU's IP address or hostname.
- Step 9** To accept the default listening port number for secure communication, 49188, press **Enter**; or enter another port number. You must enter the port number that is created for secure communication in RDU.
- Step 10** Enter the appropriate provisioning group name, and press **Enter** to continue.  
The installation program prompts you to select whether the support for packet cable voice technology is required. The default value is set as n to proceed without support of packet cable voice technology.
- Step 11** To accept the default value n, press **Enter**; or enter y to enable support of packet cable voice technology. If you enter y to enable packet cable support, the installation program prompts you to enter the packet cable configuration information:
- 1 Enter details on the KDC realm name, the IP addresses for the primary and secondary DHCP servers, and the primary and secondary DNS servers.
  - 2 Confirm the information; enter **y** and press **Enter**.
  - 3 Press **Enter** to continue.
- Step 12** To accept the default value n, press **Enter**; or enter y to enable support of eRouter technology. If you enter y to enable eRouter support, the installation program prompts you to enter the eRouter configuration information:
- 1 Enter details of the DNS server. Enter a single IP Address or a list of comma separated IP Addresses.

For example: 192.168.4.3 (or) 192.168.5.1,192.168.4.3

- 2 Confirm the information; enter "Y" and press Enter.
- 3 Press Enter to continue.

**Step 13** Enter the shared secret password that you want to use for authentication among Prime Cable Provisioning servers, and confirm the password. The shared secret password is used to encrypt the information shared between Prime Cable Provisioning servers.

**Note** You must use the same shared secret password for the RDU, all DPEs, and Prime Network Registrar extension points in your network.

**Step 14** Enter the secret key password that you want to use for shared secret authentication, and confirm the secret key password. The shared secret key password is used to encrypt the shared secret password.

**Step 15** Confirm the details entered for RDU IP address or hostname, listening port number for secured communication, provisioning group, and packet cable voice technology support selection. The Prime Network Registrar extension points component of Prime Cable Provisioning is installed on the host.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

## Configuring Extensions

After you install the Prime Network Registrar extension points, you must configure the extensions. The procedure described in this section assumes that:

- The Prime Cable Provisioning component is installed in `/opt/CSCObac`.
- Prime Network Registrar is installed in `/opt/nwreg2`.
- The Prime Network Registrar username and password are known.



### Note

Before you can use the Prime Network Registrar server, you must configure client classes, scope-selection tags, policies, and scopes. In an IPv6 environment, you must configure links and prefixes as well. For details, see the [Cisco Prime Cable Provisioning User Guide](#).

To configure extensions:

### Procedure

**Step 1** Log into the Prime Network Registrar server, with *root* access.

**Step 2** At the command line, enter:

```
# NR_HOME/local/usrbin/nrcmd -N username -P password -b <
BAC_HOME/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd
```

**Step 3** To reload the Prime Network Registrar server, enter:

```
# /etc/init.d/nwreglocal stop
# /etc/init.d/nwreglocal start
```

Alternatively, to reload the DHCP server alone, enter:

```
# NR_HOME/local/usrbin/nrcmd -N username -P password "dhcp reload"
```

## Validating Extensions

To validate the extensions installed on the Prime Network Registrar server, from the Prime Network Registrar Command Line Tool (**nrcmd**), run:



### Note

Depending on whether you installed a local or regional cluster, the **nrcmd** tool is located in:

- Local—`/opt/nwreg2/local/usrbin`
- Regional—`/opt/nwreg2/regional/usrbin`

```
nrcmd> extension list
100 Ok
dexdropas:
  entry = dexdropas
  file = libdexextension.so
  init-args =
  init-entry =
  lang = Dex
  name = dexdropas
preClientLookup:
  entry = bprClientLookup
  file = libbprextensions.so
  init-args = BPR_HOME=/opt/CSCObac,BPR_DATA=/var/CSCObac
  init-entry = bprInit
  lang = Dex
  name = preClientLookup
prePacketEncode:
  entry = bprExecuteExtension
  file = libbprextensions.so
  init-args =
  init-entry = initExtPoint
  lang = Dex
  name = prePacketEncode
nrcmd>
```



### Note

The `$BPR_HOME` and `$BPR_DATA` values may be different in your installation.

Also, in the **nrcmd** program, run:



```
nrcmd> dhcp listextensions
100 Ok
post-packet-decode: dexdropras
pre-packet-encode: prePacketEncode
pre-client-lookup: preClientLookup
post-client-lookup:
post-send-packet:
pre-dns-add-forward:
check-lease-acceptable:
post-class-lookup:
lease-state-change:
generate-lease:
environment-destructor:
pre-packet-decode:
post-packet-encode:

nrcmd>
```

### Configuring Prime Network Registrar Extension Points Properties File

After you install the Prime Network Registrar extension points, depending on the Prime Network Registrar provided libraries for SSL and Crypto, you must modify the *cnr\_ep.properties* file located in *<BAC\_HOME>/cnr\_ep/conf/* directory to include the appropriate SSL and Crypto libraries version.

For example:

If the SSL and Crypto libraries shipped with Prime Network Registrar are 1.0.1d, ensure that you remove the patch character d while loading the SSL and Crypto libraries.

To load the SSL and Crypto libraries, enter the SSL and Crypto libraries in the *cnr\_ep.properties* file as:

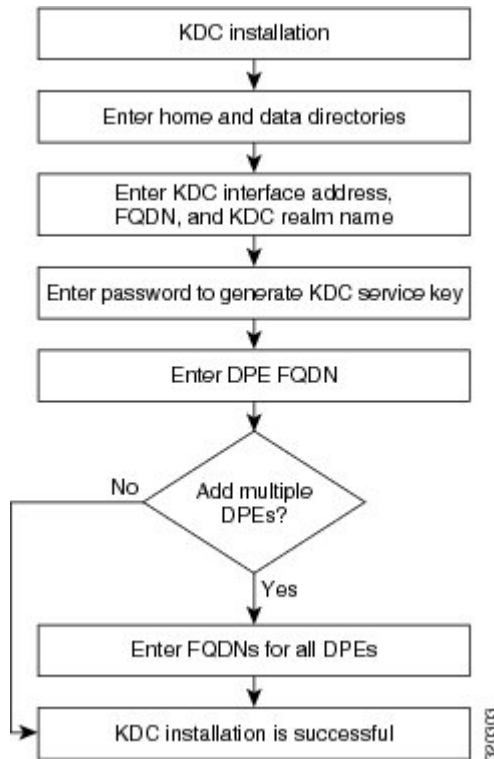
```
/lib/cpcp/cryptolib=/opt/nwreg2/local/lib/libcrypto.so.1.0.1
/lib/cpcp/ssllib=/opt/nwreg2/local/lib/libssl.so.1.0.1
```

### Installing KDC in Interactive Mode

You must install the KDC (Key Distribution Center) only when configuring a system to support voice technology operations.

Install the KDC on a server that meets the requirements described in [System Requirements](#), on page 7. For performance reasons, you should install the KDC on a separate server. The following figure provides a high level KDC installation workflow.

**Figure 7: KDC Installation**



To install the KDC:

### Procedure

- Step 1** Perform steps 1 to 4 from [Common Steps for all Components](#), on page 29. From the installer, select KDC as the component.
- Step 2** To accept the default home directory, `/opt/CSCObac`, press **Enter**; or enter another directory.
- Step 3** To accept the default data directory, `/var/CSCObac`, press **Enter**; or enter another directory.
- Step 4** Enter the KDC interface address, the fully qualified domain name (FQDN), and the Kerberos realm name. The realm name should be consistent with the realm you give to the DPEs that belong to this provisioning group.
- Step 5** To confirm your entry and continue, enter `y` and press **Enter**. The installation program prompts you to enter a password to generate the KDC service key.
- Step 6** For each DPE, enter a password from 6 to 20 characters. The KDC service key mentioned here is one that you must generate on the DPE and the KDC to enable communication between the two components. To generate this service key, the password that you enter for the KDC must match the one that you enter for the corresponding DPE; otherwise, the DPE does not function.

**Note** To generate the service key on the:

- DPE, use the `service packetcable 1 registration kdc-service-key` command from the DPE CLI. For details, see the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#).
- KDC, use the KeyGen tool. For details, see the [Cisco Prime Cable Provisioning User Guide](#).

**Step 7** To confirm and continue, enter **y** and press **Enter**.

The installation program prompts you to enter the DPE FQDN.

**Step 8** Enter the FQDN of the DPE, and press **Enter**.

**Step 9** Enter **y** and press **Enter** to confirm and continue.

**Step 10** To add another DPE, enter **y** and press **Enter**, or enter **n** and press **Enter**. The installation program uses the same voice technology shared key for all DPEs.

**Step 11** Enter **y** and press **Enter**. The KDC component of Prime Cable Provisioning is installed on the host. After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

**Caution** After installing the KDC, install the licenses and the chain of certificates; otherwise, you cannot launch the KDC.

## Installing Components in Non-interactive Mode

The non-interactive mode installation is similar to that of the interactive mode with just a few exceptions. This section explains the exceptions that you follow to install the components from the command line in non-interactive mode.

In order to install Prime Cable Provisioning 5.3 in non-interactive mode, you must first generate a response file, in which you store values for installing a component. You then use the response file as input while installing that component. For subsequent installations of the same component, you only need to use a single command, which removes all installation prompts and installs the component using the values contained in the response file.

To install Prime Cable Provisioning 5.3 in non-interactive mode, you must perform these steps:

- 1 [Generating the Response File, on page 45](#)
- 2 [Installing a Component Using the Response File, on page 46](#)

### Generating the Response File

To generate the response file:

#### Procedure

**Step 1** Generate a response file, using:

For Solaris:

```
# pkgask -r response -d <install-path>/BAC_53_SolarisK9/CSCObac.pkg CSCObac
```

For Linux:

```
#<install-path>/BAC_53_LinuxK9/install_bac.sh -response
```

**Note** In Linux environment, the response file is generated in the installation directory. In Solaris, the response file is created in the directory in which you run the `pkgask -r` command. If you want the response file to be generated in a specific location, enter: `# pkgask -r response-file-path -d CSCObac.pkg` where, *response-file-path*—Specifies the path to the directory in which you want the response file to be generated; for example, */tmp/response*. You can also give the response file any name; for example, *outputFile*. But ensure that you place the response file in the installation directory while carrying out the installation process.

Running the command does not install Prime Cable Provisioning on your system; it only generates the response file in which you store values for installation.

Note that there can only be one response file. As a result, you can use the response file only to install the component for which you generate the response file. If you want to install another component, you must generate a response file for that component and install that component using the response file generated for it.

**Example:**

You cannot use the response file that you generated to install the DPE, to install Prime Network Registrar extensions.

The installation program verifies that you have installed the required patches of the operating system. When the verification ends, the welcome information appears.

- Step 2** Carry out the steps as listed in [Installing Components in Interactive Mode](#), on page 28. A message appears indicating that a response file has been created.

**Example:**

```
Response file /response> was created.
Processing of request script was successful.
```

## Installing a Component Using the Response File

After you generate the response file, you can install the component in noninteractive mode.

To install the component in noninteractive mode:

### Procedure

- Step 1** Enter the following command to start the installation program:  
On Solaris:

```
<install-path>/BAC_53_SolarisK9/install_bac.sh
```

On Linux:

```
#<install-path>/BAC_53_LinuxK9/install_bac.sh
```

where, *install-path*—Specifies the complete path to the directory in which the *BAC\_53\_SolarisK9* or *BAC\_53\_LinuxK9* directory has been created.

The installation program checks for the Prime Cable Provisioning components installed on the host server. When the check ends, a message appears informing the possible installation modes; interactive and non-interactive, and the location where the response file is to be stored for non-interactive mode.

The installation program prompts you to select whether to proceed with the non-interactive mode. The default value is set as *n* to proceed with interactive mode.

- Step 2** Enter **y** and press **Enter** to proceed with noninteractive mode.  
After the successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

## Adding Components

This section describes how you can add one component of Prime Cable Provisioning to a system on which other components have already been installed. This situation arises largely in a deployment similar to a lab installation, where, for the purposes of testing, more than one component is installed on a single machine. The definitions file (*bpr\_definitions.sh*) is updated whenever you add new components. The procedures for adding a component are similar to those for a fresh installation.

When the installation program detects the presence of one component on your system, it does not allow you the option of adding that particular component. It prompts you to add or install other components only.



### Note

You cannot reinstall a component that you have already installed. If you must carry out a reinstallation, first uninstall that component, and then install it again.

## Uninstalling Prime Cable Provisioning

The procedure described in this section uninstalls the RDU, Prime Network Registrar extensions, the DPE, the PWS and the KDC, but it does not uninstall the Prime Network Registrar application. Before removing Prime Cable Provisioning, manually remove the Prime Cable Provisioning configuration on Prime Network Registrar.

The uninstallation program removes all files found in the installation directory (the default directory is */opt/CSCObac*). The program also shuts down and removes these processes, if they are detected: RDU, KDC, SNMP Agent, Tomcat, Prime Cable Provisioning agent, and DPE.

The uninstallation program does not remove files that were placed outside the installation directory. For example, a component installation places the database and database logs directories under */var/CSCObac*. These files must be removed manually. (Subsequent sections describe how to delete these files.) Also, the program does not remove any files found in the Prime Network Registrar directory

If you have installed Prime Cable Provisioning extensions on Prime Network Registrar, you must first uninstall it for a complete uninstallation of the Prime Cable Provisioning program; otherwise, an error message similar to the following appears:

The uninstall program found a copy of the BAC extensions in the NR extension directory (/opt/nwreg2/local/extensions/dhcp/dex/libbprextensions.so), please disable the extensions and remove the library before uninstalling BAC.

The path to the Prime Network Registrar extensions differs based on the location where you have installed Prime Network Registrar; the default location is /opt/nwreg2.

If the uninstallation program fails to uninstall Prime Cable Provisioning, an error message appears.

After uninstalling Prime Cable Provisioning, manually remove the data and database logs directories. See [Post-Uninstallation Task](#), on page 49.

To uninstall Prime Cable Provisioning from the command line:

## Procedure

- 
- Step 1** Log into the Prime Cable Provisioning server as the *root* user.
- Step 2** Manually remove the configuration of the Prime Cable Provisioning extensions on the Prime Network Registrar server. You can do this from any server that has nrcmd installed and connectivity with Prime Network Registrar.
- 1 To uninstall the Prime Cable Provisioning extensions from your Prime Network Registrar configuration, enter:
 

```
# NR_HOME/local/usrbin/nrcmd -N <username> -P <password> -b
<$BPR_HOME/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
```
  - 2 To reload your DHCP server, enter:
 

```
# /etc/init.d/nwreglocal stop
# /etc/init.d/nwreglocal start
```

Alternatively, enter:

```
# NR_HOME/local/usrbin/nrcmd -N <username> -P <password> "dhcp reload"
```
  - 3 To remove the Prime Cable Provisioning extensions from the Prime Network Registrar extensions directory, enter:
 

```
# rm -rf NR_HOME/local/extensions/dhcp/dex/libbprextensions.so
```
- Step 3** To uninstall Prime Cable Provisioning run the following command:
- On Solaris:
- ```
# pkgrm CSCObac
```
- On Linux:
- ```
# install-path/BAC_521_LinuxK9/uninstall_bac.sh
```
- Step 4** Enter *y*, and press **Enter** to start uninstalling.
- When uninstalling is complete, the following message appears:

Removal of <CSCObac> was successful.

---

# Post-Uninstallation Task

After you have uninstalled Prime Cable Provisioning, manually remove the data and database logs directories.

**Note**

Back up the important files before removing the data.

To remove these directories:

**Procedure**

**Step 1** Log in as *root*.

**Step 2** Remove the data and the database logs directories. The default directory for both is */var/CSCObac*. For example, enter:

```
# rm -rf /var/CSCObac
```

The data and the database logs directories are deleted.







## Setting Up RDU Redundancy

The RDU (Regional Distribution Unit) redundancy feature involves setting up the RDU in High Availability (HA) mode where a two node failover pair is configured for the RDU.

This chapter describes how to configure the RDU redundancy feature in Prime Cable Provisioning.

- [Prerequisites, page 51](#)
- [RDU HA Setup in Primary-Secondary Mode, page 53](#)
- [RDU HA Uninstall Scripts, page 58](#)
- [RDU Geo Redundancy, page 59](#)

## Prerequisites

The following prerequisites must be met before you proceed with RDU redundancy setup:

### Utility Requirements

- Identify the two servers on which you wish to configure the primary and secondary RDU nodes.

### Redundancy Requirements

- Redundant network configuration should be available to avoid network downtime.
- Redundant electrical supply must be available on both servers. Ensure that the electrical supply source for both servers is reachable.

### PCP Geo Redundancy Requirements

Route injection for VIP (virtual IP) needs to be done on the ingress routers to which primary and secondary servers are connected.

The VIP will be advertised as RIP2 advertisement from the active server ,so route redistribution needs to be done for RIP2 to the dynamic routing protocol running in the user environment.

**Example:** Here OSPF is the dynamic protocol

```
router ospf 1
```

```
redistribute rip metric-type 1 subnets.
```

### Logical Volume Manager (LVM) Setup

Both RDU nodes must be configured over Logical Volume Manager (LVM). The LVM allows you to create a volume group which can be further divided into logical volumes based on the requirement. The LVM also provides the flexibility to resize the volume group and logical volumes based on the dynamic memory usage.

The LVM setup involves the following considerations:

- 1 On both primary and secondary RDU nodes, a logical volume group must be created with three logical volumes on it. The logical volumes are created based on the following specifications:
  - *<logical volume for Prime Cable Provisioning install directory>* - Mounted on /bprHome directory. For example, LVBPRHOME.
  - *<logical volume for Prime Cable Provisioning data directory>* - Mounted on /bprData directory. For example, LVBPRDATA
  - *<logical volume for Prime Cable Provisioning log directory>* - Mounted on /bprLog directory. For example, LVBPRDBLOG
- 2 Ensure that the /etc/fstab entries are updated for these logical volumes.
- 3 Ensure that the /bprData, /bprHome, and /bprLog directories are empty.
- 4 The logical volumes should be of same capacity on both the nodes with a pre-created ext4 filesystem.

### Requirements for Proper Synchronization between Nodes

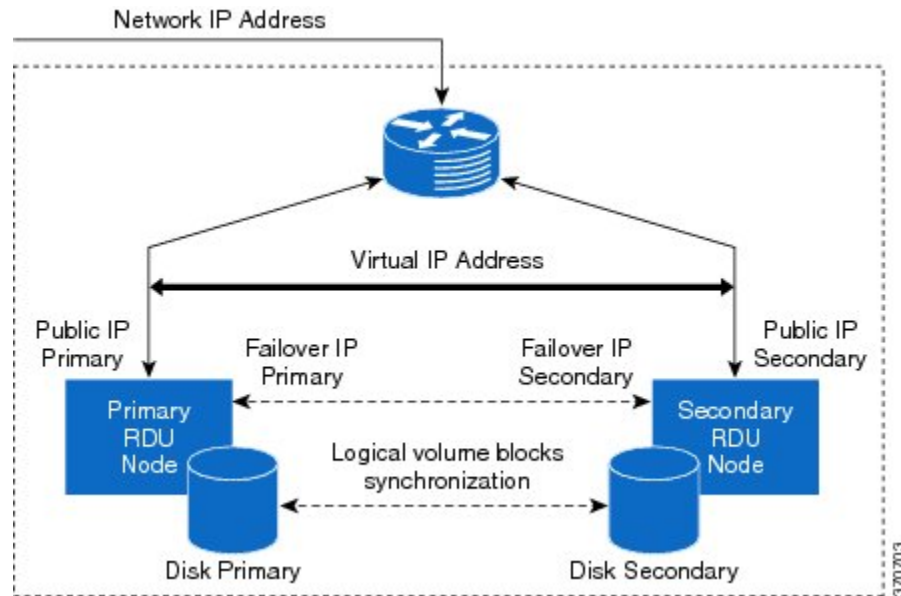
- Identify the virtual IP address that can be used to locate both servers. Ensure that this virtual IP address is not configured for any physical interfaces in the network infrastructure. Also, this virtual IP address must belong to the network cluster in which you configure the primary and secondary RDU nodes.
- The Network Time Protocol (NTP) must be synchronized between primary and secondary RDU nodes.
- Both RDU nodes must exist in the same network cluster. This ensures that the same virtual IP address can be used to reach both the RDU nodes.
- Both RDU nodes must be configured with the following two network interfaces:
  - Public access - Used for external communication. The DPE, PWS, CPNR\_EP, and API clients use this interface to communicate with the RDU. A public IP address is configured to access this network interface.
  - Failover link between RDU nodes - Used for disk synchronization. If the RDU nodes are co-located, the failover link can be a crossover link, else the failover link must be configured in the private LAN. The failover IP addresses for primary and secondary nodes must be unique in the network cluster. This is to achieve the high speed access between primary and secondary RDU nodes, and also make them isolated from the network traffic.

### Miscellaneous Requirements

- Both RDU nodes must be configured with Gigabyte network interfaces.

The following figure provides a high level RDU HA setup.

**Figure 8: RDU HA Setup**



## RDU HA Setup in Primary-Secondary Mode

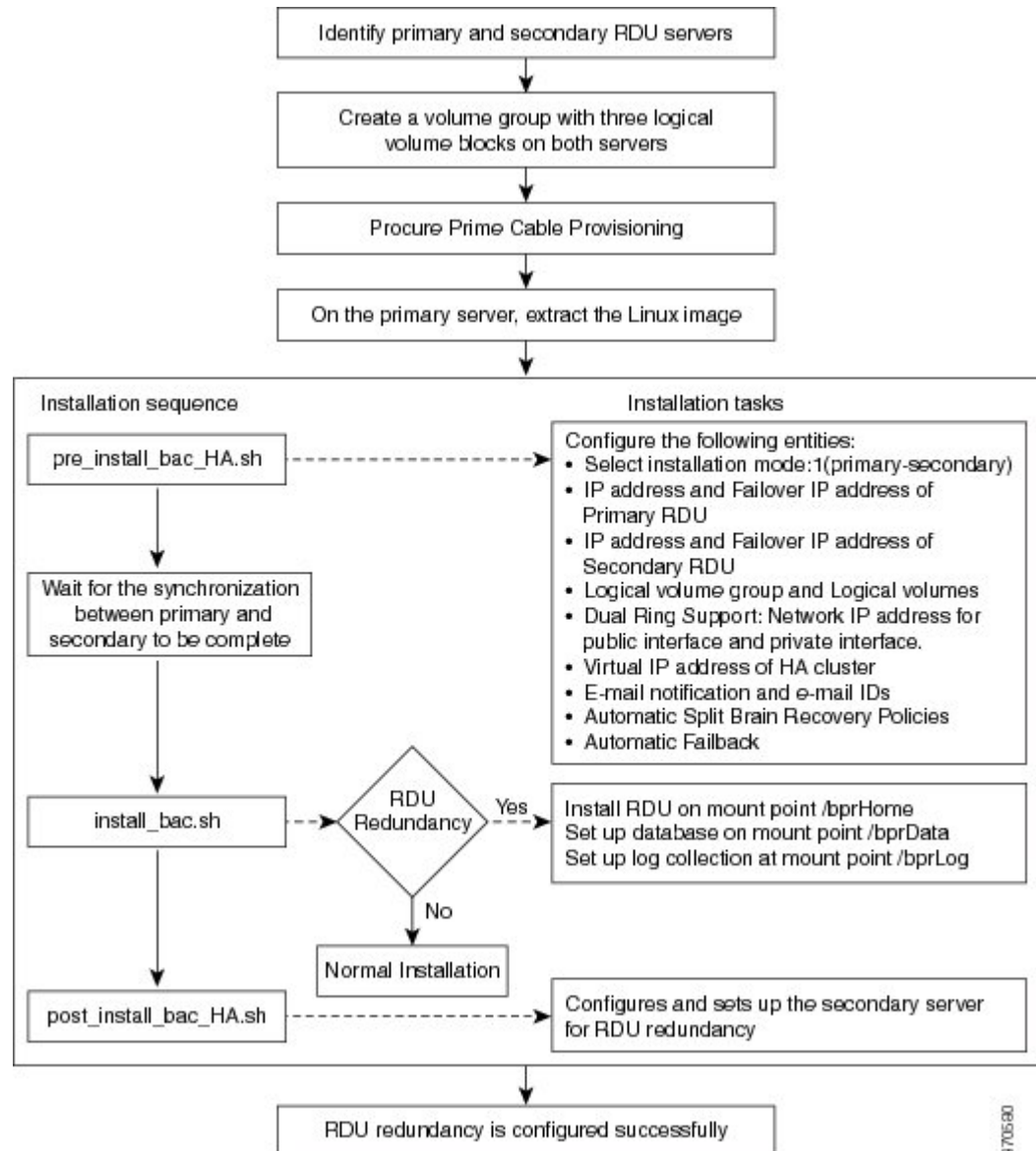
If both primary and secondary RDU nodes are available in the network infrastructure, you can use primary-secondary installation mode to configure HA cluster.

To configure the RDU HA setup using primary-secondary installation mode, you must perform the following tasks sequentially:

- 1 Configure RDU nodes for HA setup
- 2 Set up RDU two node failover pair

The following figure describes the workflow for configuring RDU HA setup using primary-secondary installation mode.

**Figure 9: RDU HA Setup - primary-secondary mode**



## Preparing RDU Nodes for HA Setup in Primary-Secondary Mode

Before installing the RDU redundancy function, you must perform the required server configurations and establish a communication channel between primary and secondary RDU servers.

To prepare primary and secondary RDU nodes for HA setup:

## Procedure

**Step 1** Configure the SSH access between primary and secondary RDU nodes and disable the password authentication:

1 On the primary RDU node, run the following command to create the SSH keys:

```
# ssh-keygen -t dsa -f ~/.ssh/id_dsa -N ""
```

The system generates the SSH keys as follows:

```
Generating public/private dsa key pair.
/root/.ssh/id_dsa already exists.
Overwrite (y/n)? y
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
14:50:6f:46:39:67:35:89:37:87:55:29:90:fd:49:0b root@<rdy-primary>
The key's randomart image is:
+--[ DSA 1024]-----+
| .oo .o+oo+=|
| +o.+E=+.|
| . ++ .=oo|
| . o + |
| S |
| |
| |
| |
| |
+-----+

```

2 Copy the SSH keys to the secondary RDU node:

```
# cp ~/.ssh/id_dsa.pub ~/.ssh/authorized_keys
```

```
# scp -r ~/.ssh <rdy-secondary>:
```

The system prompts you to enter the password for secondary RDU node. Once you enter the password, the system copies the SSH keys to the secondary RDU node:

```
root@<rdy-secondary>'s password:
known_hosts
100% 1199 1.2KB/s 00:00
id_dsa.pub
100% 606 0.6KB/s 00:00
authorized_keys
100% 606 0.6KB/s 00:00
id_dsa
100% 668 0.7KB/s 00:00

```

3 On the primary and secondary RDU servers, verify if the SSH access is available without password authentication:

```
# ssh <target RDU server> -- uname -n
```

where, <target RDU server> is the server name of primary or secondary RDU. For example, <rdu-primary> or <rdu-secondary>. If you verify the SSH access from primary RDU, you must enter the secondary RDU as the <target RDU server>.

The following output confirms that SSH access is enabled between primary and secondary RDU nodes:

```
Linux <target RDU server> 2.6.32-279.el6.x86_64 #1 SNP Wed Jun 13
18:24:36 EDT 2012
x86_64 x86_64 x86_64 GNU/Linux
```

**Step 2** Verify if the network access is available and the ethernet links are functioning normal:

# **ifconfig**

The following output confirms that the network access is available:

```
eth0 Link encap:Ethernet HWaddr 00:0C:29:ED:AE:75
      inet addr:10.104.182.92 Bcast:10.104.182.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:feed:ae75/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:761 errors:0 dropped:0 overruns:0 frame:0
      TX packets:272 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:66998 (65.4 KiB) TX bytes:41753 (40.7 KiB)

eth1      Link encap:Ethernet HWaddr 00:0C:29:ED:AE:7F
      inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:feed:ae7f/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:6 errors:0 dropped:0 overruns:0 frame:0
      TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:360 (360.0 b) TX bytes:830 (830.0 b)

lo        Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

**Step 3** Verify the accessibility between primary and secondary RDU nodes:

- Ping secondary RDU node from the primary server:

```
# ping <rdu-secondary>
```

- Ping primary RDU node from the secondary server:

```
# ping <rdu-primary>
```

## Setting Up RDU Two Node Failover Pair

The RDU two node failover pair setup involves running three installation scripts sequentially on the primary RDU. The following table describes each installation script and the sequence in which you run them.

**Table 5: RDU Two Node Failover Pair Setup**

| Sequence | Installation Scripts   | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | pre_install_bac_HA.sh  | Used to configure the following entities: <ul style="list-style-type: none"> <li>• Logical volume group and logical volumes</li> <li>• Failover IP addresses of both the RDU nodes</li> <li>• Network IP address</li> <li>• Automatic failback</li> <li>• Virtual IP address</li> <li>• Secondary RDU server public IP address</li> <li>• Utilities required for RDU redundancy function setup.</li> </ul> |
| 2        | install_bac.sh         | Used to install the RDU component on the logical volumes.                                                                                                                                                                                                                                                                                                                                                  |
| 3        | post_install_bac_HA.sh | Used to automate the supported configuration tasks for RDU redundancy function setup.                                                                                                                                                                                                                                                                                                                      |

To set up the RDU two node failover pair:

### Procedure

- 
- Step 1** Log into the primary RDU as root.
- Step 2** Extract the installation package using the following commands:
- Step 3** Run the preinstallation script using the following command:
- ```
# sh pre_install_bac_HA.sh
```
- Step 4** Enter the RDU redundancy information. The RDU redundancy information includes:
- Failover IP addresses of primary and secondary RDU servers - Unique IP address in the network cluster that are used for data synchronization between primary and secondary RDU nodes.
  - Public IP address of the secondary RDU - Public IP address that is used for external communication.

- Step 5** Enter the name of the logical volume group. For example, VGBPR.
- Step 6** Enter the name of the logical volumes created for home, data, and database log directories. For example, you can enter **LVBPRHOME** for home directory, **LVBPRDATA** for data directory, and **LVBPRDBLOG** for database log directory.
- Step 7** Enter the network IP address of the subnet under which both the RDU cluster nodes exist.
- Step 8** Enter the virtual IP address. The virtual IP address is the floating IP address that is used to reach both primary and secondary RDU nodes, but allocated to only active RDU node. Ensure that this virtual IP address is not configured for any physical interfaces in the network.
- Step 9** Enter **y** to enable automatic failback, else enter **n**. If the automatic failback is enabled, the primary RDU node becomes active once it comes up after the failover event.  
The preinstallation script performs the following automated operations on both primary and secondary RDU nodes:
- Installs the utilities for RDU redundancy setup.
  - Creates the required resources for synchronizing the block devices.
- Step 10** Install RDU on the synchronized logical volumes; **LVBPRHOME**, **LVBPRDATA**, and **LVBPRDBLOG**. For details, see [Installing the RDU in Interactive Mode](#), on page 30.
- Step 11** Run the post-installation script available under directory:  
# `sh post_install_bac_HA.sh`  
The post-installation script performs the automated configuration tasks required for RDU redundancy function setup.

## RDU HA Uninstall Scripts

To uninstall the RDU HA setup in the primary and secondary RDU nodes, you must run the uninstall scripts sequentially. The following table describes the uninstall scripts and the sequence in which you run them.

**Table 6: Uninstall RDU HA Setup**

| Sequence | Uninstall Scripts   | Description  |
|----------|---------------------|--|
| 1        | uninstall_bac.sh    | Used to unistall the RDU component from the logical volume blocks; /bacHAHome, /bacHADData, and /bacHADBLog . For details, see <a href="#">Uninstalling Prime Cable Provisioning</a> , on page 47. |
| 2        | uninstall_bac_HA.sh | Used to remove the utilities installed for RDU redundancy function.  |



# RDU Geo Redundancy

RDU Geo Redundancy is an enhanced feature of RDU HA supported on RHEL 6.5 or CentOS 6.5 (both 64bit), wherein the RDU primary and secondary node can be in different geographical location or both the nodes can be in different subnet.

- In Geo redundancy mode the VIP can be in any subnet it is not necessary to have in the subnet range common to both nodes.
- In Geo redundancy mode the CIDR value of VIP should be 32.
- The VIP will be advertised as a RIP advertisement from the active server, so on the ingress router of both the nodes route injection need to be done.

For setting up RDU in Geo redundancy mode follow steps mentioned in [Setting Up RDU Redundancy](#), on [page 51](#)





## CHAPTER

# 6

## Upgrading Prime Cable Provisioning

Prime Cable Provisioning 5.3 can be upgraded from PCP 4.2.x/ 5.x. Prime Cable Provisioning 5.3 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 5.3.

All components of Prime Cable Provisioning 4.2.x/ 5.x can be upgraded to Prime Cable Provisioning 5.3. You need to migrate the database, irrespective of whether you upgrade to Prime Cable Provisioning 5.3 from Cisco BAC 4.2.x or from Prime Cable Provisioning 5.x.

See [Cisco Prime Cable Provisioning Compatibility Matrix](#) for more details about which components can be auto-upgraded to Prime Cable Provisioning 5.3 and 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 to Prime Cable Provisioning 5.3, page 61](#)
- [eRouter Migration tool, page 85](#)

## Upgrade Cisco BAC 4.2.x/PCP 5.x to Prime Cable Provisioning 5.3

You can upgrade all components of Cisco BAC 4.2.x/ PCP 5.x by running the Prime Cable Provisioning 5.3 installer. The installer automatically upgrades the installed components to Prime Cable Provisioning 5.3. 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 RDU database and verify the same.
- Install the Prime Cable Provisioning 5.3 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 both Linux and Solaris. 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 5.3 .
- 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 5.3. For the Prime Network Registrar upgrade to 8.x see the [Cisco Prime Network Registrar 8.x Installation Guide](#) and for the extension points upgrade, see [Upgrading Cisco Prime Network Registrar Extensions, on page 82](#).

The following table represents the components that can be upgraded from the previous versions to Prime Cable Provisioning 5.3.

| 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 5.3 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 5.3 RDU can interoperate with 4.x, 5.x versions of Provisioning Group components (DPE and PNR EP).

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 5.3, 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 5.3, 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 5.3 uses.
- You must upgrade the existing API client libraries (.jar files) to Prime Cable Provisioning 5.3. 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](#), on page 89.

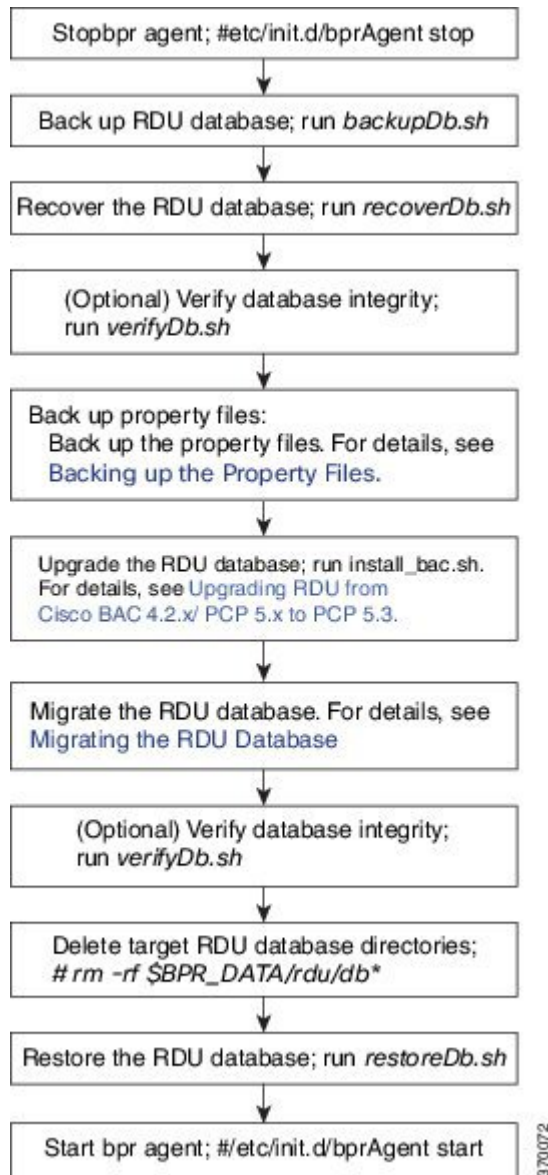
## Database Migration

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](#), on page 64
- 2 [Recovering the Backed Up RDU Database](#), on page 65
- 3 [Verify Database Integrity of Cisco BAC 4.2.x/ PCP 5.x](#), on page 65
- 4 [Backing up the Property Files](#), on page 66
- 5 [Upgrading RDU from Cisco PCP 5.x to PCP 5.3](#), on page 67
- 6 [Migrating the RDU Database](#), on page 71
- 7 [Verifying Database Integrity of Prime Cable Provisioning 5.3](#), on page 79

The following figure describes the workflow for database migration.

**Figure 10: 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 5.3.

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 5.3 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), you will need to first back them up and then copy them manually to the Prime Cable Provisioning 5.3 database.

To back up the property files:

### Procedure

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

```
# /etc/init.d/bprAgent stop
```

**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 to PCP 5.3, 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 5.3

Use this procedure to upgrade the RDU of Cisco BAC 4.2.x to PCP 5.3:



## Procedure

- 
- Step 1** **Note** You cannot upgrade RDU from 4.2.x to 5.3 directly. You need to first uninstall 4.2.x RDU and then install PCP 5.3.  
Uninstall PCP 4.2.x as described in section Uninstalling Prime Cable Provisioning.
- Step 2** Continue performing from step 1 mentioned in the section [Upgrading RDU from Cisco PCP 5.x to PCP 5.3, on page 67](#), to proceed with the RDU upgrade process.
- 

## Upgrading RDU from Cisco PCP 5.x to PCP 5.3

Use this procedure to upgrade the RDU of Cisco BAC PCP 5.x to PCP 5.3:

## Procedure

- 
- Step 1** Unpack the Prime Cable Provisioning 5.3 install package with .gtar extension using the following command:  
On Solaris:
- ```
gtar -zxpf BAC_53_SolarisK9.gtar.gz
```
- On Linux:
- ```
gtar -zxpf BAC_53_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 5.3 using the following command:  
On Solaris:
- ```
# <install-path>/BAC_53_SolarisK9/install_bac.sh
```
- On Linux:
- ```
# <install-path>/BAC_53_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 5.3 RDU. To continue with the installation see, [Installing the RDU in Interactive Mode, on page 30](#).
- 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 5.3, enter:  
On Solaris:
- ```
# pkgparam CSCObac VERSION
```

On Linux:

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

## Upgrading PCP along with HA

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

- Geo HA is available only from 5.2.x. Fresh Installation and PCP 5.3 Geo HA setup works only on RHEL / CENTOS 6.5.
- PCP 5.3 also works on existing installation of RDU Local / GEO HA that is already available on RHEL / CENTOS 6.3 OS. But, we recommend you to upgrade to the latest HA components that runs on RHEL/CENTOS 6.5.

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 69](#).



### Note

Below scenarios doesn't require an OS upgrade to RHEL 6.5 / CentOS 6.5

- Upgrading from PCP 5.2.x RDU GEO HA Cluster to 5.3 RDU GEO HA Cluster.
- Upgrading from PCP 5.2.x RDU Local HA Cluster(RHEL6.5/ CentOS 6.5) to 5.3 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 2, on page 70](#).



### Note

Below scenarios need OS upgrade to RHEL 6.5 / CentOS 6.5.

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

If you are upgrading from 5.x RDU Local HA Cluster to 5.3 RDU on Local HA Cluster, please follow the steps mentioned in [Upgrading PCP along with HA - Procedure 3, on page 70](#).



### Note

In this scenario, the 5.x Local HA runs on RHEL 6.3 / CentOS 6.3. The procedure 3 discusses only the upgrade steps of PCP RDU component and not the HA components. Also, the OS upgrade to RHEL 6.5 / CentOS 6.5 is not described as PCP 5.3 RDU can also run on 6.3 OS Local HA setup.

## Upgrading PCP along with HA - Procedure 1

### Procedure

---

- Step 1** Back up the 5.2.x RDU database and property files as described in section [Database Migration](#) and [Backing up the Property Files](#).
- Step 2** If you are upgrading from Prime Cable Provisioning **5.2.x RDU GEO HA Cluster to 5.3 RDU GEO HA Cluster**, execute the below steps:
- If you want to upgrade Quagga to the latest version, refer to [Upgrading Quagga](#),
  - Upgrade the RDU as described in Upgrade from Prime Cable Provisioning 5.2.x to 5.3.
- Step 3** If you are upgrading from Prime Cable Provisioning **5.2.x RDU Local HA Cluster to 5.3 RDU GEO HA Cluster**, execute the below steps:
- Uninstall PCP 5.x as described in section RDU HA Uninstall Scripts.
  - Install 5.3 RDU HA as described in [Setting Up RDU Redundancy](#).
- Step 4** Migrate backed up DB as described in section [Database Migration](#).
- Step 5** Stop the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1`
- Step 6** Verify if the bprAgent has stopped using the command: `/etc/init.d/bprAgent status`
- Step 7** Run the restoreDB.sh on the newly copied directory.
- Step 8** Merge the backed up property files and MIB files in the 5.3 RDU HA setup.
- **Note:** While restoring the files, make sure that you merge the changes without overwriting the newly installed files.
- Step 9** Start the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh start res_bprAgent_1`
- Step 10** Check the status of bprAgent using the command: `/etc/init.d/bprAgent status`
- Step 11** Check the RDU HA cluster status using the command:  
`/bprHome/CSCObac/agent/HA/bin/monitor_ha_cluster.sh`
-

## Upgrading PCP along with HA - Procedure 2

### Procedure

- 
- Step 1** Back up the 5.x RDU database and property files as described in section [Database Migration](#) and [Backing up the Property Files](#).
  - Step 2** Uninstall PCP 5.x as described in section [Uninstalling Prime Cable Provisioning](#).
  - Step 3** Upgrade OS from CentOS / RHEL 6.3 to CentOS / RHEL 6.5
  - Step 4** Install 5.3 RDU HA as described in [Setting Up RDU Redundancy](#), on page 51
  - Step 5** Migrate backed up DB as described in section [Database Migration](#)
  - Step 6** Stop the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1`
  - Step 7** Verify if the bprAgent has stopped using the command: `/etc/init.d/bprAgent status`
  - Step 8** Run the restoreDB.sh on the newly copied directory. Merge the backed up property files and MIB files in the 5.3 RDU HA setup.  
**Note:** While restoring the files, make sure that you merge the changes without overwriting the newly installed files.
  - Step 9** Start the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh start res_bprAgent_1`
  - Step 10** Check the status of bprAgent using the command: `/etc/init.d/bprAgent status`
  - Step 11** Check the RDU HA cluster status using the command:  
`/bprHome/CSCObac/agent/HA/bin/monitor_ha_cluster.sh`
- 

## Upgrading PCP along with HA - Procedure 3

### Procedure

- 
- Step 1** Back up the 5.x RDU database and property files as described in section [Database Migration](#) and [Backing up the Property Files](#).
  - Step 2** Upgrade the RDU as described in [Upgrade from Prime Cable Provisioning 5.x to 5.3](#).
  - Step 3** Migrate backed up DB as described in section [Database Migration](#).
  - Step 4** Stop the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1`.
  - Step 5** Verify if the bprAgent has stopped using the command: `/etc/init.d/bprAgent status`.
  - Step 6** Run the restoreDB.sh on the newly copied directory.
  - Step 7** Merge the backed up property files and MIB files in the 5.3 RDU HA setup.

- **Note:** While restoring the files, make sure that you merge the changes without overwriting the newly installed files.

- Step 8** Start the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh start res_bprAgent_1`
- Step 9** Check the status of bprAgent using the command: `/etc/init.d/bprAgent status`
- Step 10** Check the RDU HA cluster status using the command:  
`/bprHome/CSCObac/agent/HA/bin/monitor_ha_cluster.sh`
- 

## Upgrading Quagga

You can use the old Quagga version bundled with PCP 5.2.x in 5.3 as well. But, there is vulnerability with the Old Quagga version. For details, refer to [Vulnerability details](#).

So, we have upgraded Quagga to the latest version and bundled with 5.3. We strongly recommend you to upgrade Quagga to the latest version using the below steps:

### Procedure

---

- Step 1** Turn primary and secondary RDU nodes to standby mode using the following commands:
- `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh primary on`
  - `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh secondary on`
- Step 2** Upgrade Quagga to the latest version that is bundled with PCP 5.3.
- Step 3** Turn primary and secondary RDU nodes to active.
- `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh primary off`
  - `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh secondary off`
- 

## Migrating the RDU Database

After you perform the sequence of steps (steps 1 to 5) as explained in [Database Migration](#), on page 63, two options are available for migrating the RDU database to Prime Cable Provisioning 5.3:

- Migration tool - *BAC\_53\_MigrationTool.tar.gz*
- Migration script - **migrateDb.sh**

You must use either the migration tool or the migration script, based on the following migration scenarios, for migrating the RDU database:

- Cisco BAC 4.2.x/ PCP 5.x on Solaris to PCP 5.3 on Solaris, use the migration tool (*BAC\_53\_MigrationTool.tar.gz*) only.

- Cisco BAC 4.2.x/ PCP 5.x on Solaris to PCP 5.3 on Linux, use the migration tool (*BAC\_53\_MigrationTool.tar.gz*) only.
- Cisco BAC 4.2.x/ PCP 5.x on Linux to PCP 5.3 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.

**Table 7: migrateDb.sh Options**

| Argument                | Description                                                                                                                                                                                                                                                                                                                                                           | Required | Optional | Default                                        |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------|------------------------------------------------|
| -dbdir <i>dir</i>       | Specifies the location of the database backup that is to be migrated.                                                                                                                                                                                                                                                                                                 | ✓        |          | None                                           |
| -dblogdir <i>dir</i>    | Specifies the location of the database logs that are to be migrated.                                                                                                                                                                                                                                                                                                  |          | ✓        | The directory that the -dbdir option specifies |
| -cachesize <i>value</i> | Specifies, in MB, the size of the memory cache.<br>If you use this parameter, you must not exceed the 100-MB limit, unless you reduce the value of the <b>-Xmx</b> 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 <b>-Xmx</b> to:<br>$(200-100)*2 = 200$ MB |          | ✓        | 100 MB                                         |
| -help                   | Specifies usage for the tool                                                                                                                                                                                                                                                                                                                                          |          | ✓        |                                                |

### Migrating to Prime Cable Provisioning 5.3 Using In-line Migration Script

Migrating the RDU database to Prime Cable Provisioning 5.3, using the in-line migration script - **migrateDb.sh**, consists of five main steps:

- 1 Install/ Upgrade the Prime Cable Provisioning 5.3 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 Linux to Prime Cable Provisioning 5.3 Linux using examples that assume that:

- Cisco BAC 4.2.x/ PCP 5.x is installed in the default home directory */opt/CSCObac*.
- The migration from Cisco BAC 4.2.x/ PCP 5.x to 5.3 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 8: RDU Migration Workflow from Cisco BAC 4.2.x/ PCP 5.x Linux to Cisco Prime Cable Provisioning 5.3 Linux**

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | See |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1    | Stop the <i>bprAgent</i> using the following command:<br><br># <code>/etc/init.d/bprAgent stop</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |
| 2    | Run PCP 5.3 <i>migrateDb.sh</i> on the backed up database. The <i>migrateDb.sh</i> script resides in the <code>\$BPR_HOME/migration</code> directory. For a description of all arguments that this tool supports, see <a href="#">Migrating Using a RAM Disk (for Solaris only)</a> , on page 77.<br><br>For example:<br><br># <code>\$BPR_HOME/migration/migrateDb.sh -dbdir /var/backup/rdu-backup-20130829-031028</code><br><br><i>-dbdir</i> —Specifies the location of the database backup that is to be migrated; in this case, <i>/var/backup</i> . |     |
| 3    | Observe the migration progress using the <i>migration.log</i> file.<br><br>For example:<br><br># <code>tail -f /var/backup/rdu-backup-20130829-031028/migration.log</code>                                                                                                                                                                                                                                                                                                                                                                                 |     |

| Step | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | See                                                       |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 4    | <p>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.</p> <p>For example:</p> <pre># tail /var/backup/rdu-backup-20130829-031028/migration.log</pre>                                                                                                                                                                                                                | <a href="#">Cisco Prime Cable Provisioning User Guide</a> |
| 5    | <p>After migrating the database, verify it by running the command:</p> <p>For example:</p> <pre># \$BPR_HOME/rdu/internal/db/bin/verifydb.sh -dbdir /var/backup/rdu-backup-20130829-031028</pre> <p><b>Note</b> If any error occurs during the process, the log file, <b>bpr-verify-db-log.xml</b> is generated in the path <i>\$BPR_HOME/rdu/internal/db/bin</i>, which contains the details of the error. For further assistance, you can contact Cisco Support.</p> |                                                           |
| 6    | <p>Delete the target RDU database directories.</p> <p>For example:</p> <pre># rm -rf /var/CSCObac/rdu/db*</pre>                                                                                                                                                                                                                                                                                                                                                        |                                                           |
| 7    | <p>Restore the migrated database into the RDU <i>\$BPR_DATA</i> and <i>\$BPR_DBLOG</i> directories.</p> <p>For example:</p> <pre># \$BPR_HOME/rdu/bin/restoreDb.sh /var/backup/rdu-backup-20130829-031028</pre>                                                                                                                                                                                                                                                        | <a href="#">Cisco Prime Cable Provisioning User Guide</a> |
| 8    | <p>Start the <i>bprAgent</i> using the following command:</p> <pre># /etc/init.d/bprAgent start</pre> <p>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.</p>                                                                                                                                                                                                  | <a href="#">Cisco Prime Cable Provisioning User Guide</a> |
| 9    | <p>Also, you can check if the <i>\$BPR_DATA/rdu/db/DB_VERSION</i> file indicates the database version as 5.3.</p>                                                                                                                                                                                                                                                                                                                                                      | <a href="#">Cisco Prime Cable Provisioning User Guide</a> |
|      | <p><b>Note</b> 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.</p>                                                                                                                                                                                                                |                                                           |
| 10   | <p>Verify the RDU operations by logging into the Admin UI. From <b>Servers &gt; RDU</b>, you can check if the RDU version is 5.3 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)</p>                                                                                                                                                                                   | <a href="#">Cisco Prime Cable Provisioning User Guide</a> |



### 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 5.3, 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/rdubin`.

## Migrating to Prime Cable Provisioning 5.3 Using Migration Tool

The migration tool used for migrating to Prime Cable Provisioning 5.3 is `BAC_53_MigrationTool.tar.gz`.



#### Note

Before you start with the migration task, ensure you carry out the steps explained in [Database Migration, on page 63](#) section.

**Note**

The following procedure is for migrating the database from Cisco PCP 5.x Solaris to PCP 5.3 Linux. In the procedure, steps 1 to 10 must be carried out on the Solaris server which has the earlier version of Cisco PCP and steps 11 to 13 must be carried out on the Linux server where Prime Cable Provisioning 5.3 needs to be installed.

To perform a database migration:

**Procedure**

**Step 1** Stop the *brpAgent*.

**Step 2** Back up the existing RDU database, using the **backupDb.sh** tool. For details, see the [Cisco Prime Cable Provisioning User Guide](#).  
For example:

```
# $BPR_HOME/rdu/bin/backupDb.sh -nosubdir /disk1/backup
```

where,

- **-nosubdir**—Disables the automatic creation of a subdirectory. If you do not use this option, a subdirectory is created and reported to the console.
- **/disk1/backup**—Identifies the location for the database backup files.

**Note** You must stop the *bprAgent* before taking backup of the database.

**Step 3** Back up the necessary files.

For the recommended files to be backed up, see [Backing up the Property Files](#), on page 66.

**Step 4** Verify if the database has been backed up by checking the *history.log* file, which resides in the *\$BPR\_DATA* directory.

**Step 5** Recover the database that you have backed up to a consistent state, using the *recoverDb.sh* tool. For details, see the [Cisco Prime Cable Provisioning User Guide](#).  
For example:

```
# $BPR_HOME/rdu/bin/recoverDb.sh /disk1/backup
```

where, */disk1/backup* identifies the location of the database backup files.

**Step 6** After recovering the database, verify it by running the command:  
For example:

```
# $BPR_HOME/rdu/internal/db/bin/verifydb.sh -dbdir /disk1/backup
```

**Note** In case of any error while verifying the database, see [Verify Database Integrity of Cisco BAC 4.2.x/PCP 5.x](#), on page 65.

**Step 7** Copy the *BAC\_53\_MigrationTool.tar.gz* from [Cisco.com](#) location.

**Step 8** Go to the directory *BAC\_53\_MigrationTool /migration*.

**Step 9** Run *migrationTool.sh > help* and follow the help instructions.

**Step 10** After the migration is complete, copy the whole database directory and backed-up files to the Linux server where Prime Cable Provisioning 5.3 is being installed.

**Step 11** Merge the files backed up in Step 3.

- Note**
- In Prime Cable Provisioning 5.3, the `api.properties` file comes as part of the software bundle. If you have added any properties to this file earlier than merge those with the 5.3 `api.properties` file.
  - While restoring the files, make sure that you merge the changes without overwriting the newly installed files.

**Step 12** Run the `restoreDB.sh` on the newly copied directory.

- Note** Before running the `restoreDb.sh` tool, you must stop the RDU server by running the `/etc/init.d/bprAgent stop rdu` command. Also, remember to back up the database, then remove all files from the `rdu/db` and the `rdu/dblog` directories.

**Step 13** Start the `bprAgent`.

---

### Migrating Using a RAM Disk (for Solaris only)

The RAM disk is a Solaris feature that allows you to mount a portion of the RAM as a disk volume. Disk I/O operations on such volumes are considerably faster and can be useful when you have large databases on systems with sufficient memory.

The procedures described in this section are optional and describe how to create and use different RAM disks to migrate your database instead of a regular disk volume, such as a fast RAID array with battery-backed write cache:

- [Creating RAM Disk Volumes for Migration, on page 77](#)
- [Using the RAM Disk Volumes for Migration, on page 78](#)

#### Creating RAM Disk Volumes for Migration

The following procedure creates three volumes for migration and assumes that the size of the original database is 9 GB. Adjust the volume sizes as required for your database and according to what the available memory permits.

Using the following procedure, you can create three RAM disks that you could use for migration:

- `/ram-disk1`—To contain the source database
- `/ram-disk2`—To contain the migrated database directory
- `/ram-disk3`—To contain the temporary migration transaction logs

To create RAM Disk volumes for migration:

#### Procedure

---

**Step 1** Ensure that enough memory is allocated to the RAM disk in the `/etc/system` file. This figure is a percentage of the total RAM on the system. Assuming a 64-GB RAM, this setting dedicates 32 GB to the RAM disk. For example:

```
# less /etc/system
...
set ramdisk:rd_percent_physmem=50
```

**Note** If you also set the `segmap_percent` parameter, which determines the quantity of memory allocated to the OS I/O buffer cache, make sure that there is sufficient memory for both settings and some space is left for the OS operation.

**Step 2** Reboot the system.

For example:

```
# shutdown -i6 -g0 -y
```

**Step 3** Create three RAM volumes.

For example:

```
# ramdiskadm -a volume1 10g
```

```
# ramdiskadm -a volume2 12g
```

```
# ramdiskadm -a volume3 2g
```

**Step 4** Create new file systems on each volume.

For example:

```
# newfs /dev/ramdisk/volume1
```

```
# newfs /dev/ramdisk/volume2
```

```
# newfs /dev/ramdisk/volume3
```

**Step 5** Mount the volumes.

For example:

```
# rmdir /ram-disk1
```

```
# rmdir /ram-disk2
```

```
# rmdir /ram-disk3
```

```
# mkdir /ram-disk1
```

```
# mkdir /ram-disk2
```

```
# mkdir /ram-disk3
```

```
# mount /dev/ramdisk/volume1 /ram-disk1
```

```
# mount /dev/ramdisk/volume2 /ram-disk2
```

```
# mount /dev/ramdisk/volume3 /ram-disk3
```

**Step 6** Verify the mount points and their size.

For example:

```
# df -kh
```

### *Using the RAM Disk Volumes for Migration*

To use the RAM-disk volumes that you have created for migration:

#### **Procedure**

**Step 1** Copy the backup of your database to `/ram-disk1`.

For example:

```
# mkdir /ram-disk1/backup
# cp /disk1/backup/* /ram-disk1/backup/.
```

- Step 2** Perform the first phase of migration according to the procedure that [Table 8: RDU Migration Workflow from Cisco BAC 4.2.x/ PCP 5.x Linux to Cisco Prime Cable Provisioning 5.3 Linux](#), on page 73 describes. Remember to use a command similar to the one described here instead of the one mentioned in Step 1 of the table.

For example:

```
# $BPR_HOME/migration/migrateDb.sh -dbdir /ram-disk1 /ram-disk2/ram-disk3/target
&> /var/run/migration-console.log &
```

- Step 3** To ensure that the second phase of migration is executed with the database of the RAM disk:
- Install the Prime Cable Provisioning 5.3 RDU such that the database directory and the database logs directory (defined by the *BPR\_DATA* and *BPR\_DBLOG* variables, respectively) point to the volumes on the RAM disk.
  - After the second phase of migration is complete, stop the Prime Cable Provisioning process watchdog, using the */etc/init.d/bprAgent* stop command.
  - Back up the database using:  
`$ BPR_HOME/du/bin/backupDb.sh -nosubdir /ram-diskX/migrated-db/`  
 where,

- *BPR\_HOME*—Specifies the home directory, which is by default */opt/CSCObac*.
- *X*—Specifies the RAM disk to which the RDU database is migrated.

For details on using these scripts, see the [Cisco Prime Cable Provisioning User Guide](#).

- Edit the *bpr\_definitions.sh* file that is found in the home directory (by default */opt/CSCObac*) and change the *\$BPR\_DATA* and *\$BPR\_DBLOG* locations to new directories located on permanent storage drives.  
**Note** Ensure that you backup the *bpr\_definitions.sh* file before editing and that you manually migrate the data from the previous data directory to the new data directory.
- Restore the database to the new RDU locations. Run the **restoreDb.sh** scripts, using:  
`$ BPR_HOME/du/bin/restoreDb.sh /ram-diskX/migrated-db/`  
 where,

- *BPR\_HOME*—Specifies the home directory, which is by default */opt/CSCObac*.
- *X*—Specifies the RAM disk to which the RDU database is migrated.

For details on using these scripts, see the [Cisco Prime Cable Provisioning User Guide](#).

- Start the process watchdog, by running the */etc/init.d/bprAgent* start command.

### Verifying Database Integrity of Prime Cable Provisioning 5.3

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 nonmigrated database with the Prime Cable Provisioning 5.3 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 5.3. 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 synchronizing 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 to PCP 5.3

Use this procedure to upgrade the DPE of Cisco BAC 4.2.x/ PCP 5.x to PCP 5.3:

**Note**

PCP 5.3 RDU is compatible with Cisco BAC 4.x DPE.

**Procedure**

- Step 1** Unpack the Prime Cable Provisioning 5.3 install package with .gtar extension using the following command:  
On Solaris:

```
gtar -zxpf BAC_53_SolarisK9.gtar.gz
```

On Linux:

```
gtar -zxpf BAC_53_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 5.3 using the following command:

On Solaris:

```
# <install-path>/BAC_53_SolarisK9/install_bac.sh
```

On Linux:

```
# <install-path>/BAC_53_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 DPE. The installation program also prompts you to proceed with the installation of Prime Cable Provisioning 5.3 DPE. To continue with the installation see, [Installing DPE in Interactive Mode](#), on page 36.

**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 5.3, enter:  
On Solaris:

```
# pkgparam CSCObac VERSION
```

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 5.3 DPE, as described in the section [Uninstalling Prime Cable Provisioning, on page 47](#)
- Step 2** Install the DPE version that you used for rollback, as described in the section [Installing Prime Cable Provisioning, on page 27](#).
- 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:

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

The Prime Network Registrar extensions can be upgraded from Cisco BAC 4.2.x/ PCP 5.x version to Prime Cable Provisioning 5.3 version.

**Note**

Prime Cable Provisioning 5.3 supports only Prime Network Registrar 8.x or higher.

### Upgrading Prime Network Registrar-EP from Cisco BAC 4.2.x/ PCP 5.x to PCP 5.3

Use this procedure to upgrade the Prime Network Registrar extension points of Cisco BAC 4.2.x/ PCP 5.x to PCP 5.3:

**Note**

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

- Upgrade RDU to 5.3 (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 5.3 (single step).
-



## Procedure

- Step 1** Back up the file:  
`<BAC_HOME>/cnr_ep/conf/cnr_ep.properties`
- Step 2** Unpack the Prime Cable Provisioning 5.3 install package with .gtar extension using the following command:  
 On Solaris:  
`gtar -zxpf BAC_53_SolarisK9.gtar.gz`  
 On Linux:  
`gtar -zxpf BAC_53_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 5.3 version using the following command:  
 On Solaris:  
`# <install-path>/BAC_53_SolarisK9/install_bac.sh`  
 On Linux:  
`# <install-path>/BAC_53_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 package, and prompts you to proceed with Prime Cable Provisioning 5.3 installation. To continue with the installation, see [Installing Prime Network Registrar Extension Points in Interactive Mode](#), on page 38.
- 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 5.3, enter:  
 On Solaris:  
`# pkgparam CSCObac VERSION`  
 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 |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| <b>Step 1</b> | Enable eRouter1.0 IPv4 registered capability in CNR using the script <i>/opt/CSCObac/cnr_ep/bin/changeNRProperties.sh</i><br><br><b>Example:</b><br><i>./changeNRProperties.sh -ee "enabled"</i>                                                                                                                                                                                                                                                                                                                                                                                                         |         |
| <b>Step 2</b> | Enable eRouter1.0 IPv6 registered capability in CNR using the script <i>/opt/CSCObac/cnr_ep/bin/changeNRProperties.sh</i><br><br><b>Example:</b><br><i>./changeNRProperties.sh -eev6 "enabled"</i>                                                                                                                                                                                                                                                                                                                                                                                                       |         |
| <b>Step 3</b> | Run the script <i>/opt/CSCObac/cnr_ep/bin/changeNRProperties.sh</i> with option <i>-edns</i> to initialize the <i>/eRouter/dns/server</i> 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.<br><br><b>Example:</b><br><i>./changeNRProperties.sh -edns DNS-Server-IP</i><br><i>./changeNRProperties.sh -edns 192.168.4.3</i><br><i>./changeNRProperties.sh -edns 192.168.4.3,192.168.5.2,192.168.3.1</i> |         |
| <b>Step 4</b> | Restart the DHCP server using the command <i>/opt/nwreg2/local/usrbin/nrcmd dhcp reload</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |         |
| <b>Step 5</b> | Enable the <b>eRouter Feature</b> 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.                                                                                                                                                                                                                                                                                                                                                                        |         |
| <b>Step 6</b> | Enable the eRouter IPv4 and IPv6 capabilities in the Provisioning Group associated with the CNR Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |

## Upgrading KDC from Cisco PCP 5.x to Prime Cable Provisioning 5.3

Prime Cable Provisioning does not support automatic upgrade for KDC on both Linux and Solaris. We recommend fresh installation of Prime Cable Provisioning 5.3 KDC. Here is the manual procedure to upgrade the KDC of Cisco PCP 5.x to Prime Cable Provisioning 5.3:

### 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 5.3 KDC. See [Installing KDC in Interactive Mode](#), on page 43.
- 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

|                         |                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------|
| <code>-cachesize</code> | An optional parameter that specifies cache size in MB. The default cache size is 100MB. |
|-------------------------|-----------------------------------------------------------------------------------------|

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





## Next Steps

This chapter describes the tasks that you perform after installing Prime Cable Provisioning.

- [Licensing Prime Cable Provisioning, page 89](#)
- [Cisco Prime Network Registrar Configurations, page 93](#)
- [Setting Up a Device Provisioning Engine, page 95](#)

## Licensing Prime Cable Provisioning

To access this release, you must procure a new license of Prime Cable Provisioning 5.3.



### Note

You need to get the permanent or evaluation license of 5.3 to upgrade from 4.2.x/5.0/5.1/5.2 to 5.3.

Prime Cable Provisioning software must be registered via Cisco.com in order to obtain a license file (\*.lic). The license file will be sent to you by e-mail. For any licensing issues, please contact your Cisco account representative or <mailto:ask-cableprovisioning@cisco.com>.

Prime Cable Provisioning licenses are available either as a permanent or an evaluation license.

- **Permanent** -A permanent license is purchased for use in your network environment and activates the specific features for which it is intended.
- **Evaluation** -An evaluation license enables functionality for a specific length of time.

Prime Cable Provisioning evaluation licenses become invalid on a predetermined date. As such, evaluation licenses must be created when needed. To create your evaluation license, contact your Cisco representative, who will generate the necessary license file online and forward it to you via e-mail.

Prime Cable Provisioning enables you to install permanent and evaluation licenses at the same time. In addition, it also allows you to install more than one evaluation license. This enables you to increase your device limit when you are in short of licenses till you purchase a permanent license. While you can install more than one evaluation license, an expired license can be deleted and a new evaluation license (with a later expiry date), or a permanent license can be added. While deleting the expired license, ensure that the device limit of the new license at least equals the number of devices that is currently stored in the database.

Prime Cable Provisioning enables licensing using a Service License file. Each license translates to a DOCSIS IP device. The license file that you receive will contain the number of DOCSIS IP devices that are licensed.

Prior to Prime Cable Provisioning 5.x, every device type instance such as, DOCSIS, Computer, PacketCable, CableHome, etc. consumed a separate license. In addition, with dual-stack Computers, this approach created two IPDevice records, one each for IPv4 and IPv6, resulting in two licenses being consumed instead of one. In Prime Cable Provisioning, the licensing scheme counts only the DOCSIS IP devices irrespective of whether the device is a stand-alone CM or an embedded eCM, each DOCSIS IP device consumes one license. Apart from the DOCSIS IP device, all other device types consume no license. In other words, Prime Cable Provisioning consumes only one license:

- if a subscriber has a CM to which a Computer and a PacketCable devices are connected.
- if a subscriber has a CM to which a dual-stack Computer and a PacketCable devices are connected.
- if a subscriber has an e-MTA or e-STB.

To know how the license mechanism for Prime Cable Provisioning 5.x is different from BAC 4.x, see the [BAC 4.x and Prime Cable Provisioning 5.x Licensing Model](#) document.

The Prime Cable Provisioning Admin UI shows the available and used licenses. You can also see the available and used licenses count through the API client.

**Caution**

---

Do not edit your license file. Changing the data in any way invalidates the license file.

---

You still require separate licenses for the following Prime Cable Provisioning components:

- The DPE
- The KDC, if you configure your network to support voice technology

While you must install the DPE license from the Admin UI, the KDC license continues to be proprietary as in previous releases, and is licensed during Prime Cable Provisioning installation.

The DPE license is either included in a single license file along with the Service License or it is a separate license file by itself. The DPE is licensed only when you install this license file from the Admin UI.

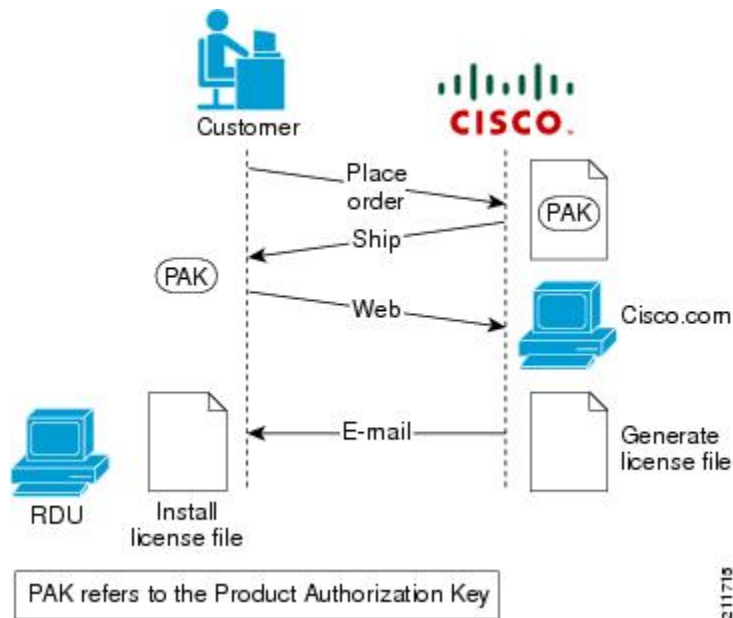
For detailed information on how to add and delete licenses, see the [Cisco Prime Cable Provisioning User Guide](#).



## Obtaining a Permanent License

The following figure describes the procedure to request a permanent license.

**Figure 11: License Claim Process**



### Note

With FlexLM licensing, you receive a Product Authorization Key (PAK) for each software CD package that you purchase. The PAK is affixed as a sticky label on the Software License Claim Certificate card that is included in your CD-ROM package.

To obtain a permanent license:

### Procedure

- Step 1** Keep your PAK handy and access <http://www.cisco.com/go/license>. You must have a valid Cisco.com account to log into this site.  
The Product License Registration website appears.
- Step 2** Complete the steps detailed at the Product License Registration page.  
**Note** During license registration, submit each PAK that you have received. For each PAK that you submit, a license file is generated and sent to you via e-mail.
- Step 3** Once you receive your license file, install it using the procedure described in [Installing Your License File, on page 92](#).

## Obtaining an Evaluation License

For an evaluation license, contact your Cisco representative, who will generate the necessary key from the Cisco licensing website and e-mail it to you. Once you receive your license file, install it using the procedure described in [Installing Your License File](#), on page 92.

## Installing Your License File

Before installing your license file, ensure that you back up your licenses in case you have to reinstall the Prime Cable Provisioning software.

To install your permanent or evaluation license:

### Procedure

**Step 1** Once you receive your license file, save each file to the local system on which you intend to launch your web browser.

**Step 2** Launch your web browser on that system.

**Step 3** Enter the administrator's location using this syntax:

`http://machine_name:port_number/`

where,

- *machine\_name*—Identifies the computer on which the RDU is running.

**Note** To access the Admin UI via HTTP over SSL, also known as HTTPS, enter `https://machine_name:port_number/`

- *port\_number*—Identifies the computer port on which the server side of the administrator application runs. The default port number is:

- 8100 for HTTP
- 8443 for HTTPS

The main login page appears.

**Step 4** Enter the default username (**admin**) and password (**changeme**).

**Note** If you are logging in for the first time, the Change Password screen appears. Enter a new password and confirm it.

**Step 5** Click **Login**.

The Main Menu page appears.

**Step 6** Click the license link at the top of the Main Menu page, or choose **Configuration > License Keys**. The Manage License Keys page appears.

**Step 7** In the License File field, enter the complete path to the location of the license file on your local system. Remember to include the name of the license file while specifying the pathname. Or, click **Browse** and navigate to the license file.

- Step 8** Click **Add**. The details regarding the number of services, the DPEs that you are licensed to use, and the type of license (Permanent or Evaluation) appear.
- 

## Installing Your KDC License

Obtain a KDC license from your Cisco representative and then install it in the correct directory.

To install the KDC license file (*backkdc.license*):

### Procedure

---

- Step 1** Obtain your license file from your Cisco representative.
- Step 2** Log into the Prime Cable Provisioning host as root or non-root.
- Step 3** Change to the `<BPR_HOME>/kdc` directory.
- Step 4** Copy the license file to this `<BPR_HOME>/kdc` directory.
- Caution**
- Be careful not to copy the license file as an ASCII file. The file contains binary data susceptible to unwanted modification during an ASCII transfer.
  - Do not copy KDC license files between operating systems because the transfer process may damage the file.
- Step 5** To restart the KDC server and make the changes take effect, run the **bprAgent restart kdc** command from the `/etc/init.d` directory.
- 

## Cisco Prime Network Registrar Configurations

After installing Prime Cable Provisioning, you must set up the Prime Network Registrar DNS server and Prime Network Registrar Extension Points.

### Enabling a Cisco Prime Network Registrar Spoofing DNS Server

A spoofing DNS server redirects all DNS requests to the same IP address. You can enable spoofing to enforce a self-provisioning flow for a new subscriber.

For example, assume that a DNS host is `dns.example.com`, and has an IP address of `10.10.10.5`. Assume also that the web server with the self-provisioning flow is `10.10.10.6`.

On the DNS server, set the following parameters in Prime Network Registrar:

```
nrcmd> zone . delete

nrcmd> zone . create primary dns.example.com postmaster.dns.example.com

nrcmd> zone . addrr * a 10.10.10.6

nrcmd> save
```

```
nrcmd> dns reload
```

When DNS reloads, the changes take effect.

On the DHCP server, set the following parameters in Prime Network Registrar:

```
nrcmd> policy unprovisioned setoption domain-name-servers 10.10.10.5
```

```
nrcmd> policy unprovisioned setoption domain-name example.com
```

```
nrcmd> save
```

```
nrcmd> dhcp reload
```

Syslog is now ready to receive alerts from Prime Cable Provisioning.

This appendix describes the sample configuration file included with this installation of Prime Cable Provisioning. This file is typical of the files you use during the Prime Cable Provisioning installation.

You can copy and use the sample configuration scripts to work with your Prime Cable Provisioning implementation. One script exists for DOCSIS modems and computers, while another script is available for DOCSIS modems and PacketCable MTAs.

## Cisco Prime Network Registrar Extension Point Configuration

This section describes the sample configuration file included with this installation of Prime Cable Provisioning. This file is typical of the files you use during the Prime Cable Provisioning installation.

You can copy and use the sample configuration scripts to work with your Prime Cable Provisioning implementation. One script exists for DOCSIS modems and computers, while another script is available for DOCSIS modems and PacketCable MTAs.

### Sample Script for DOCSIS Modems and Computers

The sample configuration nrcmd script (**bpr\_cnr\_hsd\_sample\_config.nrcmd**) is used for a high-speed data deployment of DOCSIS modems and computers in a multiple-host configuration with failover protection. It is installed in the *<BPR\_HOME>/cnr\_ep/samples* directory.

To create this script, assume that the:

- DHCP primary server IP address is: 192.168.0.32
- DNS primary server IP address is: 192.168.0.32



#### Note

---

Ensure that these IP addresses cannot be pinged from outside.

---

This sample script defines:

- Scope selection tag objects for provisioned client classes.
- Client-class objects for provisioned DOCSIS modems and computers.
- Policy objects for unprovisioned and provisioned devices. (The only difference is that DNS servers are not given to unprovisioned devices.)
- Scope and scope policy objects for unprovisioned and provisioned DOCSIS modems and computers.

- Disabled TFTP server.

To run this script, in the Prime Network Registrar **nrcmd** program, enter:

```
# NR_HOME/local/usrbin/nrcmd -N username -P password -b < bpr_cnr_hsd_sample_config.nrcmd
```

- *username*—Identifies the username.
- *password*—Identifies the password.

## Sample Script for DOCSIS Modems and PacketCable eMTA/eDVA

This sample configuration nrcmd script (**bpr\_cnr\_pktcbl\_sample\_config.nrcmd**) is used for a high-speed data deployment of DOCSIS modems and PacketCable eMTA's/eDVA's. A multiple-host configuration with failover protection is also used, and the script is installed in the `<BPR_HOME>/cnr_ep/samples` directory.

To create this script, assume that the:

- DHCP primary server IP address is: 192.168.0.32
- DNS primary server IP address is: 192.168.0.32



### Note

Ensure that these IP addresses cannot be pinged from outside.

This sample script defines objects similar to those described in [Sample Script for DOCSIS Modems and Computers](#), on page 94

To run this script, in the Prime Network Registrar **nrcmd** program, enter:

```
# NR_HOME/local/usrbin/nrcmd -N username -P password -b < bpr_cnr_pktcbl_sample_config.nrcmd
```

- *username*—Identifies the username.
- *password*—Identifies the password.

# Setting Up a Device Provisioning Engine

This section describes how you set up the DPE component of Prime Cable Provisioning.

The DPE caches provisioning information and handles all configuration requests, including downloading configuration files to devices. It is integrated with the Prime Network Registrar DHCP server to control the assignment of IP addresses. Multiple DPEs can communicate with a single DHCP server.

To configure the DPE from the CLI, you must have a valid license. If you run the commands described in this chapter on an unlicensed DPE, the following message appears:

This DPE is not licensed. Your request cannot be serviced. Please check with your system administrator for DPE licenses.

For details on DPE licensing and how to install your license, see [Licensing Prime Cable Provisioning](#), on page 89.

## Accessing the DPE CLI

The Prime Cable Provisioning CLI is an IOS-like command-line interface that you use to configure and view the status of the DPE by using Telnet or SSH. The CLI supports built-in command help and command autocompletion.

You can enable authentication of the CLI through a locally configured login and privileged passwords, or through a remote username and password for a TACACS+ service.

To access the DPE CLI, open a Telnet session to port 2323 from a local or remote host.

### Accessing DPE CLI from a Local Host

To access the CLI from a local host, use:

```
# telnet localhost 2323
```

or,

```
# telnet 0 2323
```

### Accessing DPE CLI from a Remote Host

To access the CLI from a remote host, enter:

```
# telnet remote-hostname 2323
```

**Note**

If you cannot establish a Telnet connection to the CLI, the CLI server is probably not running. You may need to start the server. To start the server, enter:

```
# /etc/init.d/bprAgent start cli
```

After you access the CLI, you must enter the DPE password to continue. The default login and privileged passwords are changeme.

See the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#) for specific information on the CLI commands that a DPE supports.

## Logging In

To log into the DPE:

### Procedure

- Step 1** At the username and password prompt, enter the appropriate username and password. For security reasons, we recommend that you change the original password.
- Step 2** **Change your login and privileged mode passwords.**
  - 1** To change the login password:
    - a** Access the DPE in the privileged mode.

- b** At the prompt, enter the **password** command.

For example:

```
bac_dpe# password
```

- c** At the password prompt, enter the new password, then re-enter it.

For example:

```
New password: <password1>
```

```
Retype new password: <password1>
```

```
Password changed successfully.
```

- 2** To change the privileged mode password:

- a** Access the DPE in the privileged mode. You must have the PRIV\_DPE\_UPDATE privilege to run this command.

- b** At the password prompt, enter the new password, then re-enter it.

For example:

```
New enable password: <password2>
```

```
Retype new enable password: <password2>
```

```
Password changed successfully.
```

---

## Configuring a DPE for Data

To configure a DPE, you must know the:

- IP address or fully qualified domain name (FQDN) of the RDU for the DPE.
- Provisioning group or groups to which the DPE belongs.



### Tip

You can use the show run command to view the running configuration. A complete list of commands is available through the use of the show commands command. For additional information, see the [Cisco Prime Cable Provisioning DPE CLI Reference](#).

To configure a DPE:

### Procedure

- Step 1** Configure the DPE interface to handle provisioning requests, by specifying the IP address of the interface in the IPv4 or the IPv6 addressing formats.

For example:

Using IPv4 format:

```
bac_dpe# interface ip 10.10.10.133 provisioning
```

```
% OK (Requires DPE restart "> dpe reload")
```

Using IPv6 format:

```
bac_dpe# interface ip 2001:0DB8:0:0:203:baff:fe12:d5ea provisioning
```

```
% OK (Requires DPE restart "> dpe reload")
```

**Note** The values provided here are sample values only. Use values appropriate for your network.

- Step 2** Configure the IPv4 ONLY address for communication with Prime Network Registrar.  
For example:

```
bac_dpe# interface ip 10.10.10.133 pg-communication
```

```
% OK (Requires DPE restart "> dpe reload")
```

- Step 3** Enter the IP address for the RDU or its domain name if you are implementing DNS. Also, identify the port on which the RDU is listening. The default listening port is 49187. Identify whether to enable secure mode of communication with the RDU. The value can either be true or false, where true indicates secure mode.  
For example:

Using IPv4 format:

```
bac_dpe# dpe rdu-server 10.10.10.1 49187 false
```

```
% OK (Requires DPE and DPE CLI restart)
```

- Step 4** Specify the provisioning group or groups of the DPE. Where appropriate, specify the secondary provisioning group to which the DPE belongs to.  
For example:

```
bac_dpe# dpe provisioning-group primary group1
```

```
% OK (Requires appliance restart "> reload")
```

```
bac_dpe# dpe provisioning-group secondary group2
```

```
% OK (Requires appliance restart "> reload")
```

- Step 5** Set the shared secret password to be the same as that on the RDU.  
**Note** You must have the PRIV\_DPE\_SECURITY privilege to run this command.

For example:

```
bac_dpe# dpe shared-secret secret
```

```
% OK (Requires DPE and DPE CLI restart)
```

- Step 6** Enable the TFTP service running on the DPE.  
For example:

Using IPv4 format:

```
bac_dpe# service tftp 1 ipv4 enabled true
```

```
% OK (Requires DPE restart "> dpe reload")
```

Using IPv6 format:

```
bac_dpe# service tftp 1 ipv6 enabled true
```

```
% OK (Requires DPE restart "> dpe reload")
```



**Step 7** Enable the Time of Day (ToD) service running on the DPE.

For example:

Using IPv4 format:

```
bac_dpe# service tod 1 ipv4 enabled true
% OK (Requires DPE restart "> dpe reload")
```

Using IPv6 format:

```
bac_dpe# service tod 1 ipv6 enabled true
% OK (Requires DPE restart "> dpe reload")
```

**Step 8** For the configuration to take effect, you must reload the DPE and restart the DPE CLI.

For example:

```
bac_dpe# dpe reload
Process [dpe] has been restarted
bac_dpe# /etc/init.d/bprAgent restart cli
Process [cli] has been restarted.
```

After you reload the DPE, you can establish a Telnet session to the DPE using its IP address. Remember to use the new login and enable password that you created in [Logging In](#), on page 96.

After the successful configuration of the DPE, the configured DPE must appear under the Servers tab in the Admin UI.

## Configuring a DPE for Voice Technology

This section describes the configuration tasks that you must perform to set up a DPE to support voice technology.

For using the tips provided in this section, see the *dpe.properties* file, located in the `<BPR_HOME>/dpe/conf` directory. You change the properties specified, as indicated in the tips, to enable the described feature. If you edit the properties, you must restart the DPE.

**Caution**

In the *dpe.properties* file, there should be only one instance of each property described in these tips.

## Setting Up Voice Technology

To set up voice technology on your DPE:

**Procedure****Step 1** To set the FQDN for each enabled DPE interface in the IPv4 or IPv6 format, enter:

```
interface ip ip_address provisioning fqdn fqdn
```

**Tip** dpe.properties: /server/provFQDNs=FQDN[IP address]:port. This could translate, for example, into c3po.pcnnet.cisco.com[10.10.10.5]:49186.

The FQDN is sent as the SNMPEntity in DHCP option 177 suboption 3.

For example:

Using the IPv4 format:

```
bac_dpe# interface ip 10.10.1.2 provisioning fqdn dpe.example.com
% OK (Requires DPE restart "> dpe reload")
```

Using the IPv6 format:

```
bac_dpe# interface ip 2001:0DB8:0:0:203:baff:fe12:d5ea provisioning fqdn dpe.example.com
% OK (Requires DPE restart "> dpe reload")
```

**Step 2** Configure the IPv4 ONLY address for communication with Prime Network Registrar.  
For example:

```
bac_dpe# interface ip 10.10.10.133 pg-communication
% OK (Requires DPE restart "> dpe reload")
```

**Step 3** To configure voice technology at DPE, enter:

**service packetcable 1 registration kdc-service-key password**

**Note** The DPE password that you enter by using this CLI command must match the corresponding password used in the KeyGen utility when generating service keys for the KDC.

**Tip** dpe.properties: /pkcbl/regsvr/KDCServiceKey=(xx: ... xx)

where (xx: ... xx) represents a 24-byte randomly selected, colon-separated, hexadecimal value; for example: 31:32:33:34:35:36:37:38:39:30:31:32:33:34:3 5:36:37:38:39:30:31:32:33:34.

For example:

```
bac_dpe# service packetcable 1 registration kdc-service-key password3
% OK (Requires DPE restart "> dpe reload")
```

**Step 4** To control the choice of encryption algorithm for use during SNMPv3, enter:

```
bac_dpe# service packetcable 1 registration policy-privacy value
```

If you enter a value of zero (which is the default value) for this policy privacy, the MTA will choose a privacy option for SNMPv3. Entering any nonzero value means the Provisioning Server will set its privacy option in SNMPv3 to a specific protocol. Although, currently, DES is the only privacy option supported by voice technology.

**Tip** dpe.properties: /pkcbl/regsvr/policyPrivacy=1 (enables DES privacy)

For example:

```
bac_dpe# service packetcable 1 registration policy-privacy 1
% OK (Requires DPE restart "> dpe reload")
```

**Step 5** Enter this command to set the SNMP service key used for SNMPv3 cloning to the RDU.

```
bac_dpe# service packetcable 1 snmp key-material password
```

The default value for this command is null. Enter this default to disable SNMPv3 cloning on this DPE.

**Caution** To enable SNMP cloning, set this property to the identical 46 hexadecimal bytes that are used at the RDU (*rdu.properties* file, which resides in the /<BPR\_HOME>/rdu/conf directory).







## INDEX

### A

- adding components [47](#)
- Admin UI [1](#)
  - login password [1](#)
  - login username [1](#)
- assign [17](#)
  - privileges to users [17](#)
- audience [vii, 9](#)
- available disk space [18](#)
  - data directory [18](#)

### B

- backkdc.license [93](#)

### C

- checklist [18](#)
  - installing [18](#)
- commands [27, 45](#)
  - Prime Cable Provisioning:pkgask (noninteractive) [45](#)
  - UNIX [27](#)
    - tar [27](#)
- Common Steps [29](#)
- components [47](#)
  - adding to install [47](#)
- configuration [42, 97, 99](#)
  - DPE [97, 99](#)
    - for data [97](#)
    - for voice technology (PacketCable) [99](#)
  - Network Registrar extensions [42](#)
    - validating [42](#)
- Configuring [43](#)
  - CPNR-EP Properties File [43](#)
- create [17](#)
  - group [17](#)
  - user [17](#)
- Crypto libraries [43](#)

### D

- data directory [18](#)
- database logs directory [18](#)
- DHCP [93](#)
  - configuring for Network Registrar [93](#)
  - reload [93](#)
- directories [18](#)
  - data [18](#)
  - database logs [18](#)
  - default location [18](#)
    - database logs [18](#)
    - home [18](#)
    - Network Registrar extensions [18](#)
  - disk space [18](#)
    - data [18](#)
    - home [18](#)
    - home [18](#)
- DNS [93](#)
  - enabling a spoofing server [93](#)
  - reload [93](#)
- DPE [95, 96, 97, 99, 101](#)
  - about [95](#)
  - configuring [97, 99, 101](#)
    - for data [97](#)
    - for voice technology [99](#)
  - dpe.properties file [99](#)
  - dpe.properties file:/pkcbl/enable [99](#)
  - dpe.properties file:/pkcbl/regsvr/configEncrypt=0 [101](#)
  - dpe.properties file:/pkcbl/regsvr/configEncrypt=1 [101](#)
  - dpe.properties file:/pkcbl/regsvr/KDCServiceKey [99](#)
  - dpe.properties file:/pkcbl/regsvr/policyPrivacy [99](#)
  - dpe.properties file:/pkcbl/snmp/keyMaterial [99](#)
  - dpe.properties file:/pkcbl/snmp/timeout=1 [101](#)
  - dpe.properties file:/pkcbl/snmp/timeout=10 [101](#)
  - dpe.properties file:/server/provFQDNs [99](#)
  - logging in [96](#)
- DPE Cache [80, 81](#)
  - backup tool [80, 81](#)

**F**

File-System Block Size [12](#)  
 Linux [12](#)  
 Solaris [12](#)

**G**

generate [45](#)  
 response file [45](#)

**H**

home directory [18](#)

**I**

installation [14, 18](#)  
 checklist [18](#)  
 directories [18](#)  
   data [18](#)  
   database logs [18](#)  
   home [18](#)  
 requirements [14](#)  
   Network Registrar [14](#)  
 Installation [7, 22](#)  
   Requirements [7](#)  
   worksheet [22](#)  
 installation checklist [18](#)  
 installing [22, 30, 33, 36, 38, 43, 45](#)  
   components [43](#)  
   components interactive [30, 33](#)  
     PWS [33](#)  
     RDU [30](#)  
   components, interactive [36, 38](#)  
     DPE [36](#)  
     Network Registrar extensions [38](#)  
   components, noninteractive [45](#)  
   initial steps [22](#)  
   pkgask install [45](#)  
     components (noninteractive) [45](#)  
   pkgask install (noninteractive) [45](#)  
 Installing [27](#)  
   initial steps [27](#)  
 interactive [43](#)  
   KDC [43](#)  
 interactive installation [27, 33, 36, 38, 43](#)  
   components [33, 36, 38, 43](#)  
     DPE [36](#)  
     Network Registrar extensions [38](#)

interactive installation (*continued*)  
   components (*continued*)

    PWS [33](#)  
   initial steps [27](#)  
   KDC [43](#)

interactive installation components [30](#)  
   RDU [30](#)

**K**

KDC [43, 89](#)  
   FQDN [43](#)  
   interactive installation [43](#)  
   interface address [43](#)  
   Kerberos realm [43](#)  
   KeyGen tool [43](#)  
   license [89](#)  
   service key [43](#)  
     on DPE [43](#)  
     on KDC [43](#)

**L**

large file support [13](#)  
   linux [13](#)  
   Solaris [13](#)  
 license file [1, 18](#)  
 licensing [89, 92, 93](#)  
   DPE [89](#)  
     about [89](#)  
     installing license [89](#)  
   KDC [89, 93](#)  
     about [89](#)  
     backdc.license [93](#)  
     installing license [93](#)  
   license file [89, 92](#)  
     about [89](#)  
     installing [92](#)  
 listening port [18](#)  
   about [18](#)  
   default number [18](#)  
 logical volume blocks [51](#)  
 logical volume group [51](#)

**M**

migrateDb.sh tool [71](#)  
   arguments [71](#)  
   using [71](#)

## N

Network Registrar [1, 14, 18, 41, 42, 47, 82, 94](#)  
   about [1](#)  
   clusters [1](#)  
     local [1](#)  
     regional [1](#)  
   default location [18](#)  
   installing extensions [1, 14, 41, 42](#)  
     configuring [41](#)  
     requirements [14](#)  
     tasks [1](#)  
     validating [42](#)  
   license key [1](#)  
   nrcmd CLI [94](#)  
   reloading server [41](#)  
   uninstalling [47](#)  
   upgrading [82](#)  
   web UI [41](#)  
     login username [41](#)  
 noninteractive installation [45, 46](#)  
   about [45](#)  
   installing using response file [46](#)  
 nrcmd CLI [94](#)

## O

obtain license [91](#)  
 operating system [7](#)  
   patches [7](#)  
     Solaris 10 [7](#)  
   requirements [7](#)  
 overview [1](#)

## P

PacketCable [99](#)  
   configuring DPE [99](#)  
 patches [7](#)  
   Solaris 10 [7](#)  
 post-uninstallation task [49](#)  
 preinstallation procedure [17](#)  
 product documentation [vii, 11](#)  
 PWS [33](#)  
   interactive installation [33](#)

## R

RAM Disk Volumes [77, 78](#)  
   create [77](#)

RAM Disk Volumes (*continued*)  
   use [78](#)

RDU [18, 30, 47, 71, 77, 79](#)  
   interactive installation [30](#)  
   listening port [18](#)  
   migrating database [71, 77, 79](#)  
     RAM disk, using [77](#)  
     using migrateDb.sh tool [71](#)  
     verifying integrity [79](#)  
   RDU agent [47](#)  
   shared secret [18](#)  
 RDU Redundancy [51, 54, 57, 58](#)  
   uninstall [58](#)  
   HA Setup [54](#)  
   install\_bac.sh [57](#)  
   installation scripts [57](#)  
   logical volume manager [51](#)  
   miscellaneous requirements [51](#)  
   post\_install\_bac\_HA.sh [57](#)  
   pre\_install\_bac\_HA.sh [57](#)  
   prerequisites [51](#)  
   primary server [54](#)  
   redundancy requirements [51](#)  
   secondary server [54](#)  
   SSH keys [54](#)  
   Two Node Failover Pair [57](#)  
   utility requirements [51](#)  
 recovering [63](#)  
   RDU database [63](#)  
 requirements [7, 9, 14](#)  
   hardware [9](#)  
   Network Registrar [14](#)  
   patches [7](#)  
 Requirements [12](#)  
   Database [12](#)

## S

scope selection tag [94](#)  
 set [17](#)  
   password [17](#)  
 shared secret [18](#)  
 Solaris 10 patches [7](#)  
 SSL libraries [43](#)  
 Supports [61](#)  
   64-bit servers [61](#)  
   inline migration [61](#)

**T**

Tomcat process [47](#)  
    detecting [47](#)  
tool [71](#)  
    migrateDb.sh [71](#)

**U**

uninstall [47](#)  
uninstall\_bac\_HA.sh [58](#)  
uninstallation [47, 49](#)  
    post-uninstallation task [49](#)  
    uninstalling [47](#)  
upgrade [66, 67, 80, 82, 85](#)  
    CPNR-EP [82](#)  
    DPE [66, 67, 80](#)

upgrade (*continued*)  
    KDC [85](#)  
Upgrade requirements [61](#)  
upgrading [63, 71, 77, 79, 82](#)  
    components [82](#)  
        Network Registrar extensions [82](#)  
    migrating RDU database [71, 77, 79](#)  
        RAM disk [77](#)  
        using migrateDb.sh [71](#)  
        verifying database integrity [79](#)  
    RDU migration [63, 71](#)  
Users and groups [17](#)

**V**

verify [63](#)  
    database integrity [63](#)