Cisco Prime Cable Provisioning 6.3 Quick Start Guide

First Published: 2021-06-10

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

CONTENTS

PREFACE

Preface vii

Audience vii

Product Documentation vii

Obtaining Documentation and Submitting a Service Request viii

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 8

Linux PG Hardware Recommendations 8

Linux RDU Hardware Recommendations 8

Linux PWS Hardware Recommendations 9

Database Requirements 9

File-System Block Size 9

Large File Support 9

Prime Network Registrar Requirements 10

CHAPTER 3

Preparing for Installation 11

Installation Checklist 11

Installation Worksheet 16

CHAPTER 4

Installing and Uninstalling Prime Cable Provisioning 19

Installing Prime Cable Provisioning 19
Installing Components in Interactive Mode 20
Common Steps for all Components 20
Installing the RDU in Interactive Mode 21
Installing PWS in Interactive Mode 24
Installing REST PWS in Interactive Mode 27
Installing DPE in Interactive Mode 27
Installing Prime Network Registrar Extension Points in Interactive Mode 29
Installing KDC in Interactive Mode 34
Installing Components in Non-interactive Mode 36
Generating the Response File 36
Installing a Component Using the Response File 37
Adding Components 38
Uninstalling Prime Cable Provisioning 38
Post-Uninstallation Task 39

CHAPTER 5 **Setting Up RDU Redundancy** 41
Prerequisites 42
RDU HA Installation Modes 44
Common Initial Steps for Configuring RDU HA Nodes 44
RDU HA Setup in Primary-Secondary Mode 45
Preparing RDU Nodes for HA Setup in Primary-Secondary Mode 46
Setting Up RDU Two Node Failover Pair 50
RDU HA Setup in Primary-Only and Secondary-Only Modes 53
Configuring RDU Node in Primary-Only Mode 53
Configuring RDU Node in Secondary-Only Mode 55
Configuring HA Cluster from an RDU HA Ready Installation 57
Recovering an Impacted RDU Node Using Recovery Mode 59
RDU HA Uninstall Scripts 60
RDU Geo Redundancy 61

CHAPTER 6 **Upgrading Prime Cable Provisioning** 63
Upgrade Cisco PCP 5.x/6.x to Prime Cable Provisioning 6.3 63
About Backward Compatibility 64

Licensing After Migration 66
Database Migration 66
Backing Up the RDU Database 67
Recovering the Backed Up RDU Database 68
Verify Database Integrity of Cisco PCP 5.x 68
Backing up the Property Files 68
Upgrading RDU from Cisco PCP 5.x/6.x to PCP 6.3 69
Upgrading PCP along with HA 70
Migrating the RDU Database 73
DPE Cache Backup and Restore Tool 77
Upgrading DPE from Cisco PCP 5.x/6.x to PCP 6.3 78
DPE Rollback 79
Upgrading Cisco Prime Network Registrar Extensions 79
Upgrading Prime Network Registrar-EP from Cisco PCP 5.x/6.x to PCP 6.3 80
Enabling eRouter Capabilities 81
Upgrading KDC from Cisco PCP 5.x/6.x to Prime Cable Provisioning 6.3 82
eRouter Migration tool 83

CHAPTER 7 **Next Steps** 85
Licensing Prime Cable Provisioning 85
Obtaining a Permanent License 86
Obtaining an Evaluation License 88
Installing Your License File 88
Installing Your KDC License 89
Cisco Prime Network Registrar Configurations 89
Enabling a Cisco Prime Network Registrar Spoofing DNS Server 89
Cisco Prime Network Registrar Extension Point Configuration 90
Sample Script for DOCSIS Modems and Computers 90
Sample Script for DOCSIS Modems and PacketCable eMTA/eDVA 91
Setting Up a Device Provisioning Engine 91
Accessing the DPE CLI 92
Accessing DPE CLI from a Local Host 92
Accessing DPE CLI from a Remote Host 92
Logging In 92

Configuring a DPE for Data 93
Configuring a DPE for Voice Technology 95
Setting Up Voice Technology 95
Controls Available 97

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, on page vii
- Product Documentation, on page vii
- Obtaining Documentation and Submitting a Service Request, on page viii

Audience

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

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on 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 Documentation Overview for the list of Cisco Prime Network Registrar guides.

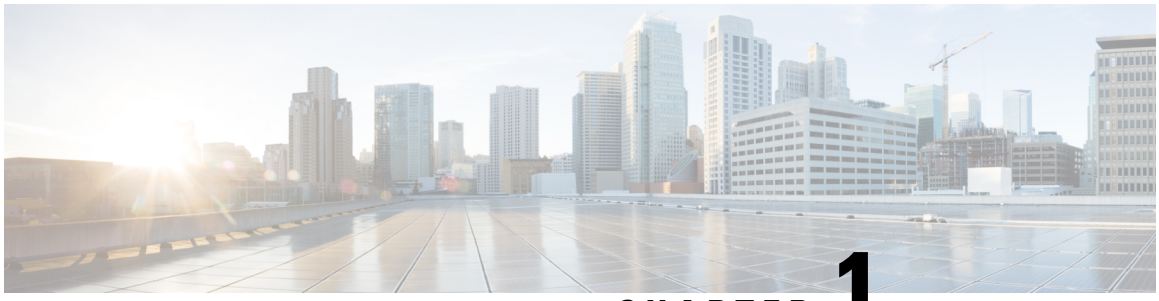
See the Prime Cable Provisioning Upgrade Matrix for the upgrade compatibility of the current release with the previous releases.

See the Prime Cable Provisioning Compatibility Matrix for the PNR, PG and API compatibility of the current release with the previous releases.

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, on page 1
- High-level Installation Flow and Startup, on 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.

To compare the checksum of the downloaded image with that available in the download software page use the below command:

```
md5sum BAC_63_LinuxK9.gtar.gz
d03fa51fa9b539c43b87cc693e6448ab  BAC_63_LinuxK9.gtar.gz
```

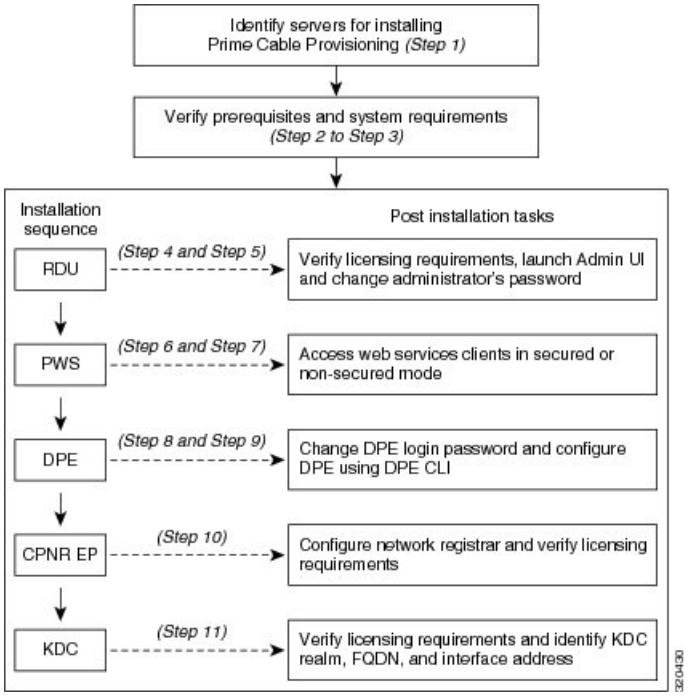
By comparing the checksum values, you can verify if the correct image has been downloaded

High-level Installation Flow and Startup

This section provides the general flow to complete the Prime Cable Provisioning 6.3 installation. For details about the complete installation, see Installing Prime Cable Provisioning, on page 19.

The following figure provides a high level flow for installing Prime Cable Provisioning 6.3:

Figure 1: High-level Installation Flow and Startup



To set up Prime Cable Provisioning 6.3 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.

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 9.

Step 3 Review the Installation Checklist, on page 11.

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 86.

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/rdu/logs*.
- Checking the status of the bprAgent using the command **`systemctl status bpragent`**

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 the login credentials

1. Enter the username and password.
2. Click **Login**
3. To change the 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 for PWS using SOAP. For REST PWS, default ports for secured mode is 9790 and nonsecured mode is 9101.

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 9.x or later. For more information on installing Prime Network Registrar, see the Cisco Prime Network Registrar Installation Guide.

Note In Linux, if RDU and Prime Network Registrar are installed on the same server, then the lease query will not work.

- When you install the Prime Network Registrar Local Cluster (LCCM), ensure that you:
  - **a.** Install Prime Cable Provisioning extensions on all Prime Network Registrar local cluster servers. See Installing Prime Cable Provisioning, on page 19.
  - **b.** Configure Prime Network Registrar, including its extensions. Specifically, you need to configure scopes, policies, client classes, and selection tags. See Configuring Extensions, on page 32. Also see the Cisco Prime Network Registrar User Guide.
  - **c.** 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.
  - **d.** 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:
  - **a.** 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.
  - **b.** Obtain a valid central-cluster license file for the Prime Network Registrar Regional Server.
  - **c.** 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 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 User Guide.

After you complete Prime Network Registrar installation, install Prime Network Registrar Extention Points. For more information see, Installing Prime Network Registrar Extension Points in Interactive Mode, on page 29.

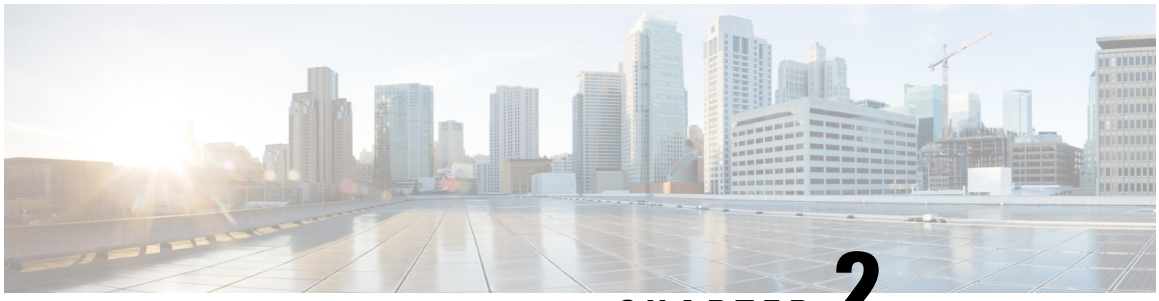
Step 11 Install and configure the KDC. When you install the KDC, ensure that you:

- 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 85.
- 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



CHAPTER 2

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, on page 7
- System Requirements, on page 7
- Prime Network Registrar Requirements, on page 10

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 85.

System Requirements

On Linux

In case of Linux,Prime Cable Provisioning must be installed on Red Hat Enterprise Linux 7.x/8.x or on CentOS 7.x/8.x versions, 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 7.x or CentOS 7.x version platforms. For more information on RDU Redundancy, see Setting Up RDU Redundancy, on page 41.

Hardware Requirements

The resource recommendations for Linux is shown below. 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.

Linux PG Hardware Recommendations , on page 8

Linux RDU Hardware Recommendations, on page 8

Linux PWS Hardware Recommendations, on page 9

Note

- The resource recommendations mentioned in the above topics for 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.
- Prime Cable Provisioning recommends usage of virtual machines (VMs) which are Thick provisioned.

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 (1)				
1M	DPE	4	8 GB	8 GB	40 GB
2M	DPE				

(1) *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 (1)
250K					
500K					
1M	RDU	4	16GB	16GB	80GB (2)
2M					
Greater than 2 Million	RDU	8	32 GB	32GB	200GB (2)

%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 6.3, 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 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 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**.

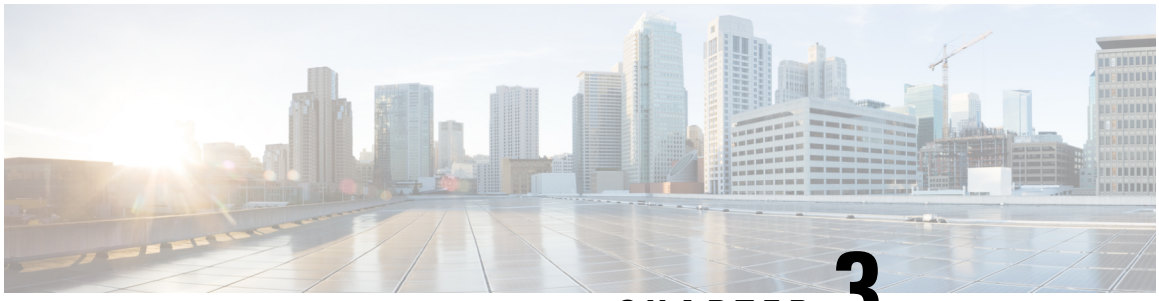
Prime Network Registrar Requirements

Note To install Prime Network Registrar Extension Points, you must install Prime Network Registrar 9.x or later.

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 9.x or later.
- You must install a Prime Network Registrar DHCP server on a system running Linux 7.x/8.x (RedHat or CentOS).
- In a failover deployment of Prime Network Registrar, you must configure two DHCP servers. For information on configuring failover on Prime Network Registrar servers, see the Cisco Prime Network Registrar 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.



CHAPTER 3

Preparing for Installation

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

This chapter contains:

- Installation Checklist, on page 11
- Installation Worksheet, on page 16

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 1: Installation Checklist

Task	Checkoff
1. Verify if your system meets the minimum system hardware and software requirements described in Installation Requirements, on page 7.	
2. Ensure that you have access to the servers on which you intend to install Prime Cable Provisioning components.	
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.	

Task	Checkoff
4. Determine the home directory (*BPR_HOME*) in which you want to install the Prime Cable Provisioning component or components. The default directory is */opt/CSCObac*. Ensure that the target installation directory has enough disk space. **Note** We recommend that you have at least 1 GB of disk space available in *BPR_HOME* otherwise launching the Admin UI might result in some errors.	
5. For the RDU, determine where you want to install the data directory (*BPR_DATA*) and the database logs (*BPR_DBLOG*). The default directory is */var/CSCObac*. Ensure that the target installation directory has enough disk space. **Note** 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. **Note** We recommend that you locate the data directory on a different physical disk than the home directory; for example, */var/disk0/CSCObac*. 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.	
6. Verify that you have minimum 500 MB of free space available in the /tmp directory for successful installation.	

Task	Checkoff
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.	☐
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.	☐

8. Configure the ephemeral UDP port range in the system to higher numbered ports. In general, some services in RDU such as SNMP service uses ephemeral UDP ports. The default ephemeral UDP port range in the system is from 32768 through 65535. RDU uses the UDP port 49187 to delete DB transaction logs. There is a possibility of SNMP service to use the same UDP port 49187 at the same time, which might lead to system crash. To avoid this, configure the range of ephemeral UDP port higher than 49187.
On Linux,
• To view the current ephemeral UDP port range setting, use:
`sysctl net.ipv4.ip_local_port_range`
Sample output:
`net.ipv4.ip_local_port_range = 32768 61000`
• To change the ephemeral UDP port range, use:
`sysctl -w net.ipv4.ip_local_port_range="50001 61000"`
	☐

10. Determine the location of the certificate files and enter it correctly when prompted. The default location is */tmp*. If you enter an incorrect location, it falls back to the nonsecure mode.	☐

Task	Checkoff
11. 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.	
12. 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.	
13. 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 Cisco Prime Cable Provisioning User Guide.	
14. Determine the key password used for storing the private keys for the Admin UI, PWS, and the RDU.	
15. Determine the ports used to access the Admin UI using HTTP or HTTP over SSL (HTTPS). The default ports are: • 8100—Listening port on Admin UI web server for HTTP communication • 8443—Listening port on Admin UI web server for HTTPS communication	
16. Determine the ports used to access the PWS using HTTP or HTTP over SSL (HTTPS). The default ports are: • 9100—Listening port on PWS web server using SOAP for HTTP communication • 9443—Listening port on PWS web server using SOAP for HTTPS communication • 9101—Listening port on RESTful PWS web server for HTTP communication • 9790—Listening port on RESTful PWS web server for HTTPS communication	
17. For the DPE, ensure that 2 GB of disk space is available in the data directory.	
18. For the PWS, ensure that 500 MB of disk space is available in the data directory.	

Task	Checkoff
19. The PWS can communicate with the Prime Cable Provisioning 5.x 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.	☐
20. The web server for PWS, REST PWS, and Admin UI must be configured and functioning normally.	☐
21. Ensure that the recommended version of Prime Network Registrar is installed and running on the servers on which you are installing Prime Cable Provisioning extensions, that is, the Prime Network Registrar Extension Points.	☐
22. For the Prime Network Registrar extensions, determine the name of the provisioning group for the Prime Network Registrar server.	☐
23. For the Prime Network Registrar extensions, determine the location to install the data directory *(BPR_DATA)*. The default directory is */var/CSCObac*.	☐
24. Verify that you have the necessary Prime Network Registrar configuration files. For an example of these configuration files, see the Cisco Prime Network Registrar Configurations, on page 89.	☐
25. Verify that you have the KDC servers available, if you want to configure your network to support secure PacketCable voice technology.	☐

26. Enable your server to support IPv6.
To enable IPv6, login as root, and run:
`# ifconfig intf inet6 plumb up`
`# /usr/lib/inet/in.ndpd`
`# touch /etc/hostname6.intf`
where, intf—identifies the interface on which you want to enable IPv6.
	☐

In case of Linux, perform the following extra steps	
27. Modify the *config* file to disable SELinux using the following command: `# vi /etc/selinux/config` where, config—File that controls the state of SELinux on the system. In this file, set the value of SELINUX to *disabled*.	☐

Task	Checkoff
28. Disable iptables using the following command: `# systemctl stop firewalld.service` **Note** The Admin UI page will not open if iptables is in enabled state on the system.	
29. Reboot the Prime Cable Provisioning host using the following command: `# reboot`	
30. Wait till the server boots up and re-login to continue with the installation.	

Installation Worksheet

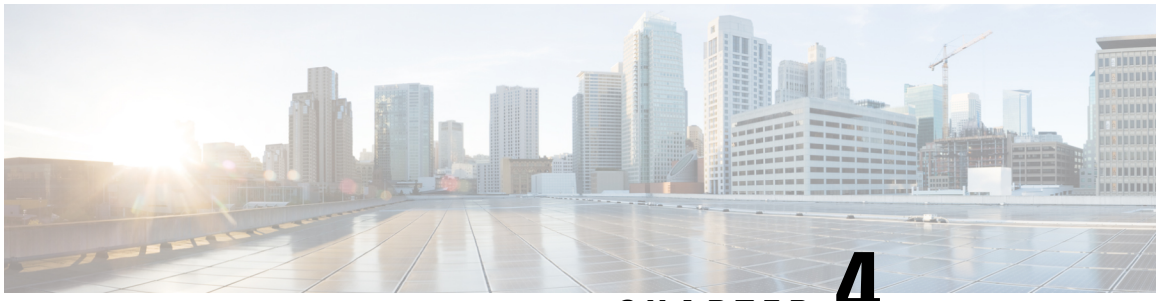
During the installation of Prime Cable Provisioning, you are prompted for configuration information. The following table is a worksheet that you can use to record the information specific to your installation.

Table 2: Prime Cable Provisioning Installation Parameters

Prompt	Description	Default Value	Your Value
Home directory	Root directory to install Prime Cable Provisioning component	*/opt/CSCObac*	
Data directory	Root directory to install the data directory for Prime Cable Provisioning component	*/var/CSCObac*	
Database logs directory	Root directory to install the database transaction logs for Prime Cable Provisioning component	*/var/CSCObac/rdu/dblog*	
Logs directory	Root directory to install the general transaction logs for Prime Cable Provisioning components	• For RDU: */var/CSCObac/rdu/logs* • For DPE: */var/CSCObac/dpe/logs* • For PWS: */var/CSCObac/pws/logs* • For REST: */var/CSCObac/restpws/logs*	
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: • RDU • PWS • REST PWS • DPE • Prime Network Registrar Extension Points • KDC	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 using SOAP or API clients using HTTP	9100	
	Port number through which you access the web services using SOAP or API clients using HTTP over SSL (HTTPS)	9443	
	Port number through which you access the RESTful web services or API clients using HTTP	9101	
	Port number through which you access the RESTful web services or API clients using HTTP over SSL (HTTPS)	9790	
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): /opt/CSCObac/lib/security/rootCA.crt /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	



CHAPTER 4

Installing and Uninstalling Prime Cable Provisioning

This chapter describes how to work with the installation program.

This chapter contains the following sections:

- Installing Prime Cable Provisioning, on page 19
- Uninstalling Prime Cable Provisioning, on page 38
- Post-Uninstallation Task, on page 39

Installing Prime Cable Provisioning

To install Prime Cable Provisioning 6.3:

Note To configure Prime Cable Provisioning in SSL mode post installation, refer to the section **Configuring SSL Post Installation** in Cisco Prime Cable Provisioning 6.3 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 6.3 installation file, and:

a. Change to the directory in which you will decompress and extract the installation file.

b. Extract the file with the *.gtar.gz* extension. Enter:

For Linux:

```
# <install_path>/gtar -zxvf BAC_63_LinuxK9.gtar.gz
```

The utility creates the *BAC_63_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 20
- Installing Components in Non-interactive Mode, on page 36

Installing Components in Interactive Mode

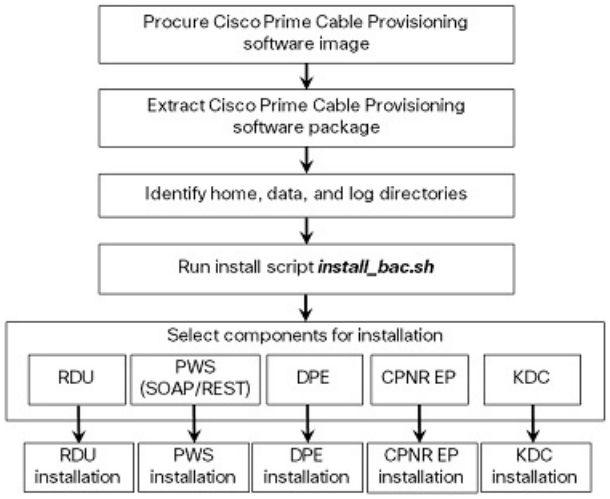
This section explains how to install Prime Cable Provisioning 6.3 components interactively from the command line.

Note Before you begin any of these procedures, you must complete the initial procedure described in Installation Checklist, on page 11.

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 Linux:

```
# <install-path>/BAC_63_LinuxK9/install_bac.sh
```

where, <*install-path*>—Specifies the complete path to the directory in which the *BAC_63_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.

Step 3 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.

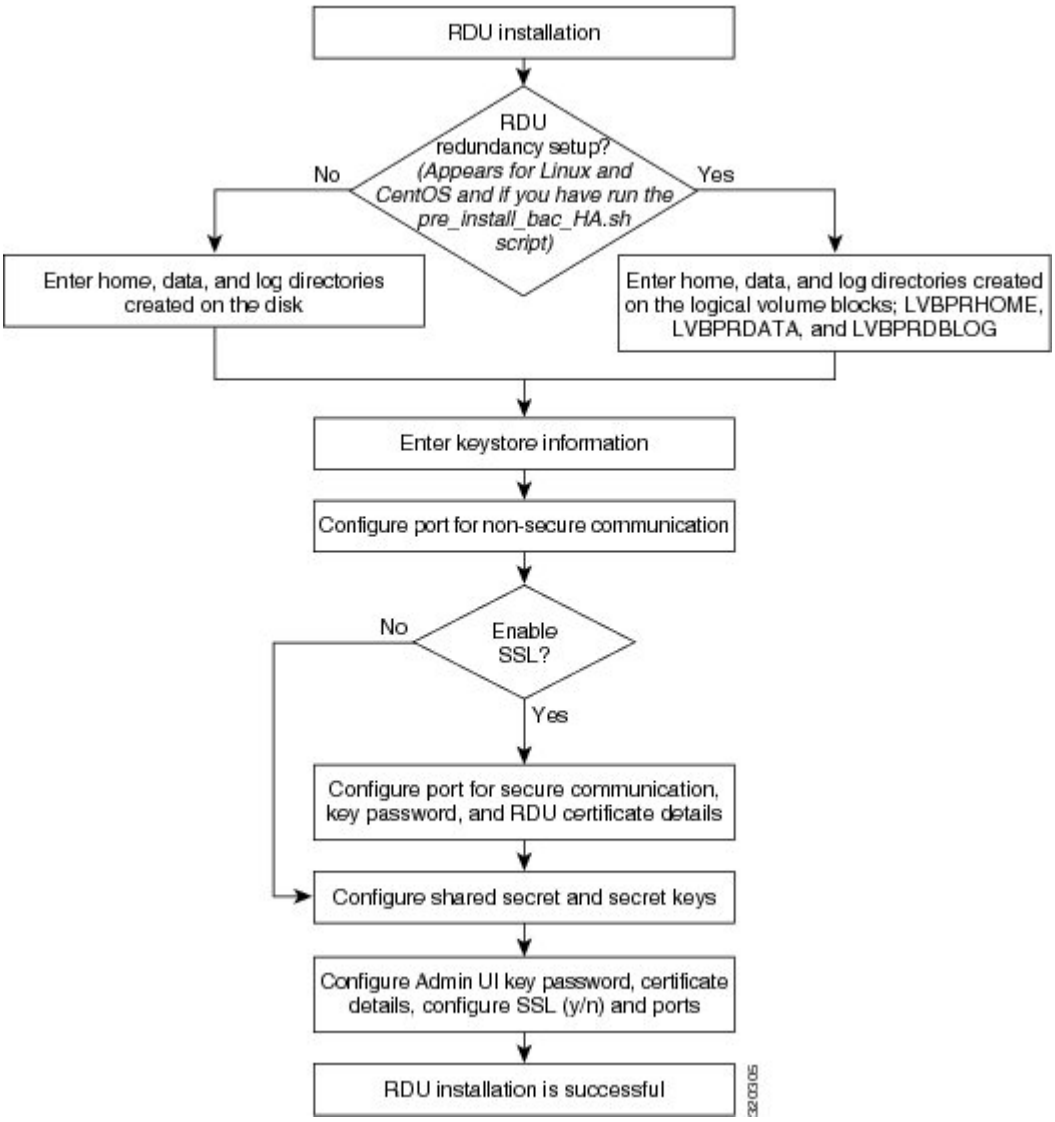
Installing the RDU in Interactive Mode

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 20.

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 3: Lease Query Address for Binding

Protocol	IP Address	Port
IPv4	Wildcard[1]	67
IPv6	Wildcard	547

[1] 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**.

Note The default is secure mode.

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 To accept the default value y, press Enter; or enter n to disable SNMP agent.

Step 20 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

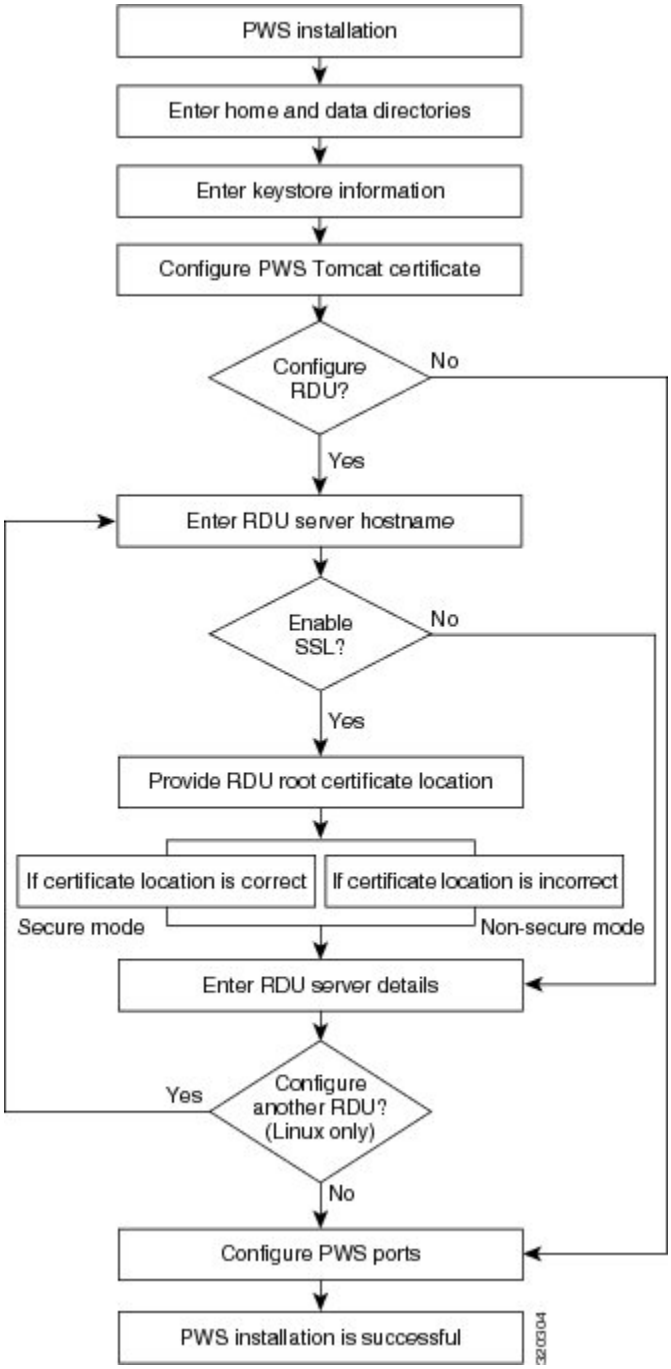
Install the PWS (Provisioning Web Services) on a server that meets the requirements described in System Requirements, on page 7.

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 20.

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 PWS information.

The installation program prompts you to select whether to support the PWS instance with a load balancer. The default value is set as **n**.

Step 8 Enter **y** to enable the load balancer support, and enter the REST PWS cluster name.

Note Load Balancer is supported only for the REST PWS component.

The installation program prompts you to enter the RDU information.

Step 9 To add RDU information, enter **y**.

Step 10 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 11 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 12 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 13 Enter RDU information; port, username, and password, and press **Enter** to continue.

The installation program prompts you to confirm the RDU information.

Step 14 Enter **y** and press **Enter** to continue.

The installation program prompts you to add the second RDU.

Step 15 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. For information on how to run the ws-cli.sh tool, see the Cisco Prime Cable Provisioning User Guide.

Step 16 To accept the default PWS HTTP port for the API clients, 9100 (SOAP) / 9101 (REST), press **Enter**; or enter another port number.

Step 17 To accept the default PWS HTTPS port for the API clients, 9443 (SOAP) / 9790 (REST), press **Enter**; or enter another port number.

Step 18 Confirm the PWS installation information; enter **y** and press **Enter.**

Step 19 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 REST PWS in Interactive Mode

For installing the REST PWS, see Installing PWS in Interactive Mode, on page 24.

Note PWS RESTful can communicate only with PCP 6.1.3 RDU version or above. It is not compatible with RDUs of earlier releases of Prime Cable Provisioning.

Note During Upgrade procedure, after successful upgrade of REST PWS to PCP 6.3, the installation program prompts you for enabling Load Balancer support.

Installing DPE in Interactive Mode

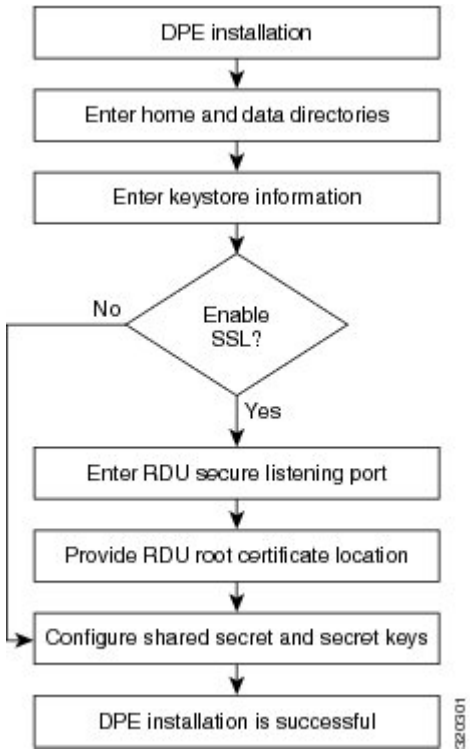
Install the DPE on a server that meets the requirements described in System Requirements, on page 7.

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 20.

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**.

Note The default is secure mode.

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 To accept the default value y, press Enter; or enter n to disable SNMP agent.

Step 12 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 91.

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.

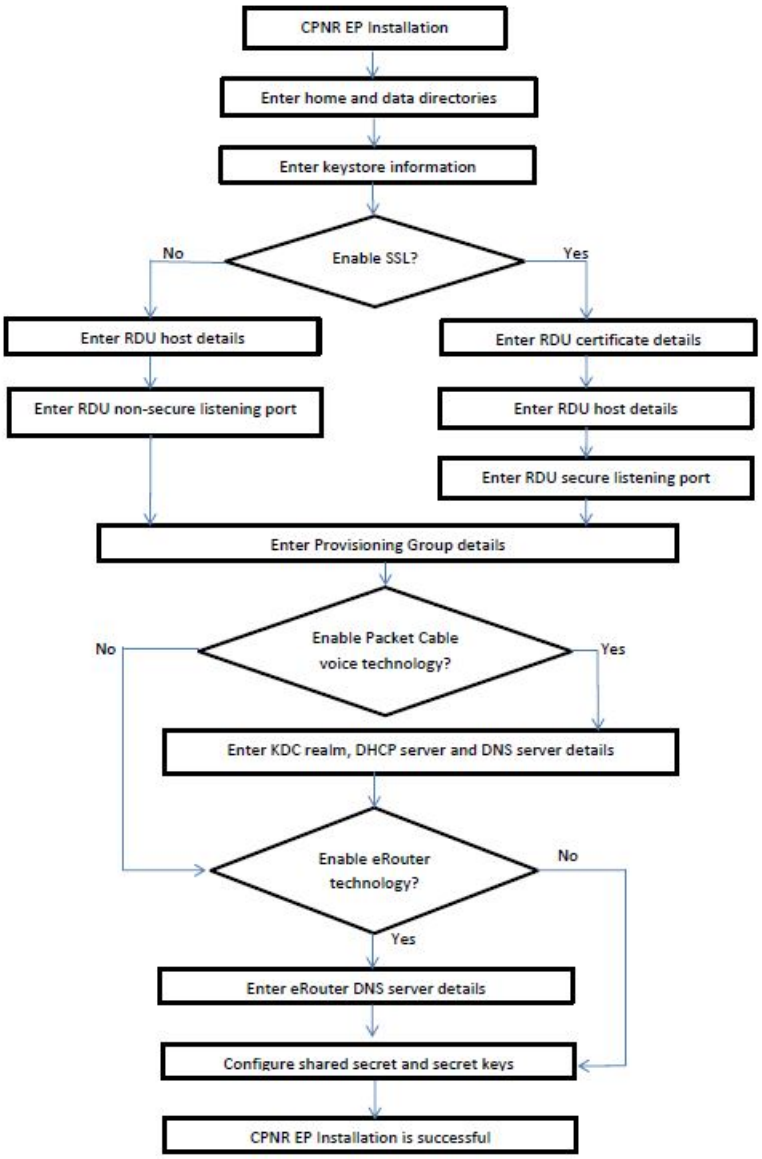
Note We recommend that you configure the Prime Network Registrar server to use a static IP address.

Before you install Prime Network Registrar Extension Points, complete the initial installation described in Installation Checklist, on page 11. Ensure that Prime Network Registrar is installed and running. To install Prime Network Registrar, see the Cisco Prime Network Registrar 11.x Installation Guide.

Note For SSL to work on a fresh installation of Prime Cable Provisioning, you must install Prime Network Registrar 10.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 20.

From the installer, select CPNR EP 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.

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 5 To enable secure communication, enter **y**. For nonsecure communication, enter **n**.

Note The default is secure mode.

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 6 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 7 To accept the default RDU's IP address or hostname, press **Enter**; or enter another RDU's IP address or hostname.

Step 8 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 9 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 10 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:

a. Enter details on the KDC realm name, the IP addresses for the primary and secondary DHCP servers, and the primary and secondary DNS servers.

b. Confirm the information; enter **y** and press **Enter**.

c. Press **Enter** to continue.

Step 11 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:

a. 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

b. Confirm the information; enter "Y" and press Enter.

c. Press Enter to continue.

Step 12 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 13 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 14 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:

```
# systemctl stop nwreglocal
# systemctl start nwreglocal
```

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
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
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
```

Note Prime Network Registrar does not ship SSL and Crypto libraries as part of CPNR **9.1.3 and above**, **10.1 and above**, instead it uses the system libraries. Modify the *cnr_ep.properties* file located in *<BAC_HOME>/cnr_ep/conf/* directory to include the appropriate SSL and Crypto system libraries.

To identify the SSL and Crypto libraries used by CPNR execute the below command:

```
ldd /opt/nwreg2/local/bin/dhcp
```

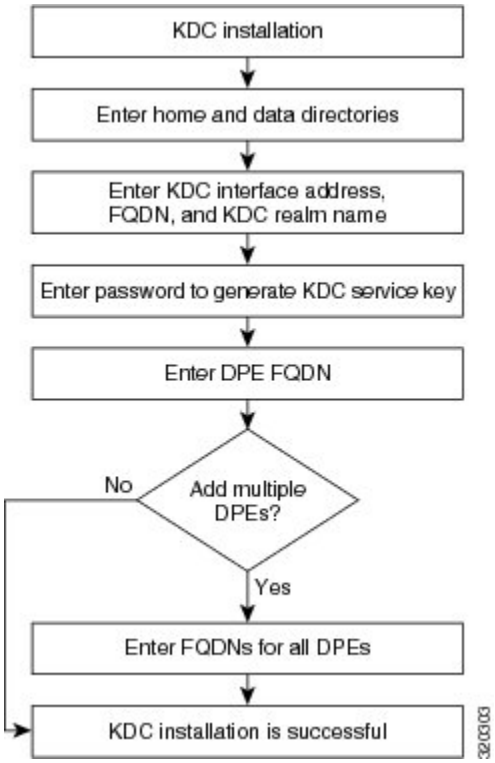
Note You must modify cnr_ep.properties file with the appropriate details, whenever you change the library files.

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 20.

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 6.3 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 6.3 in non-interactive mode, you must perform these steps:

1. Generating the Response File, on page 36
2. Installing a Component Using the Response File, on page 37

Generating the Response File

To generate the response file:

Procedure

Step 1 Generate a response file, using:

For Linux:

```
#<install-path>/BAC_63_LinuxK9/install_bac.sh -response
```

Note In Linux environment, the response file is generated in the installation directory.

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 20.

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 Linux:

```
#<install-path>/BAC_63_LinuxK9/install_bac.sh
```

where, install-path—Specifies the complete path to the directory in which the *BAC_62_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:

```
Error: Unable to uninstall until the CNR extension points are disabled

To disable, use the NRCMD file /opt/CSCObac/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
and then delete the extensions library, for example:

/opt/nwreg2/local/usrbin/nrcmd -b <
/opt/CSCObac/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
/opt/nwreg2/local/usrbin/nrcmd dhcp reload
rm /opt/nwreg2/local/extensions/dhcp/dex/libbprextensions.so
```

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 39.

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.

a. 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
```

b. To reload your DHCP server, enter:

```
# systemctl stop nwreglocal
# systemctl start nwreglocal
```

Alternatively, enter:

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

c. 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 Linux:

```
# install-path/BAC_63_LinuxK9/uninstall_bac.sh
```

Step 4 Enter **y**, and press **Enter** to start uninstalling.

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

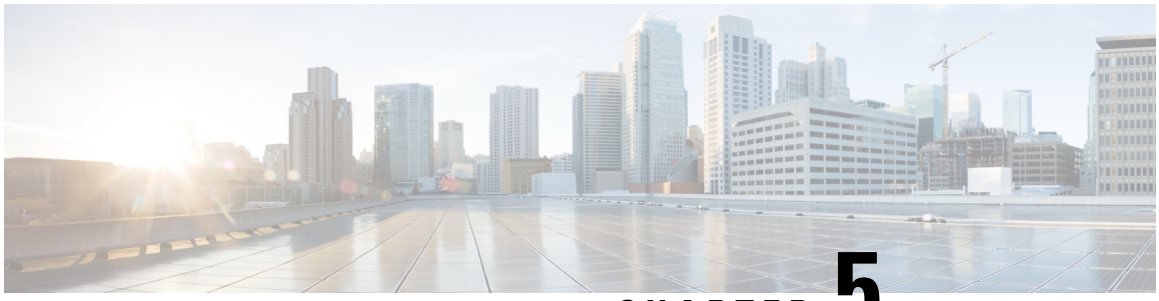
Step 1 Log in as *root*.

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.



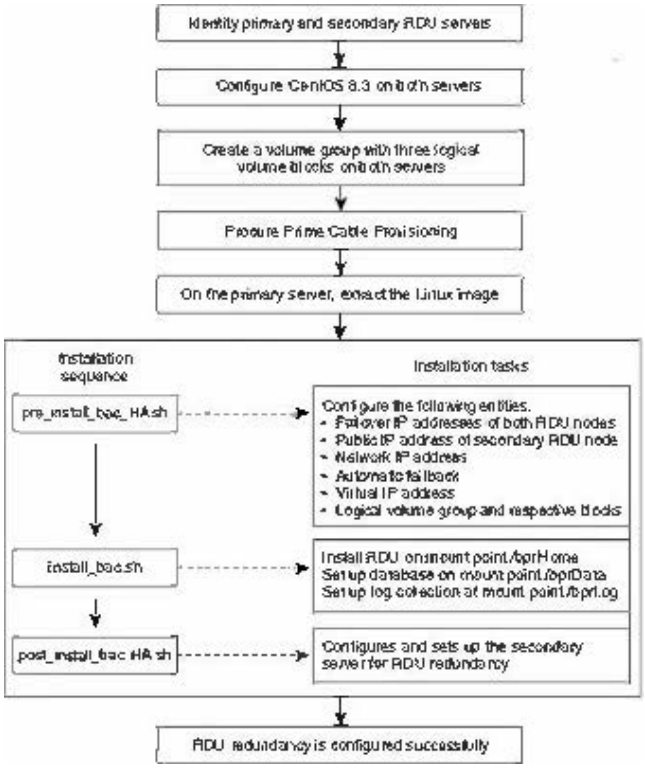
CHAPTER 5

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.

The following figure provides the work flow for RDU redundancy setup.

Figure 8: Work Flow for RDU Redundancy Function Setup



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

- Prerequisites, on page 42
- RDU HA Installation Modes, on page 44
- Common Initial Steps for Configuring RDU HA Nodes, on page 44
- RDU HA Setup in Primary-Secondary Mode, on page 45
- RDU HA Setup in Primary-Only and Secondary-Only Modes, on page 53

• Recovering an Impacted RDU Node Using Recovery Mode, on page 59
• RDU HA Uninstall Scripts, on page 60
• RDU Geo Redundancy, on page 61

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.
- RHEL 8.3 or CentOS 8.3 must be installed on both of these servers.

  Kernel 4.18.0-240 must be installed on both of these servers.
- Network configuration file should contain only the system hostname, not the fully qualified domain name (FQDN).

Caution In the network configuration file, if the system has FQDN name as hostname, it will cause failure in creating DRBD blocks.

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 /bprData, /bprHome, and /bprLog directories are empty.
3. The logical volumes should be of same capacity on both the nodes with a pre-created xfs filesystem.

Requirements for Proper Synchronization between Nodes

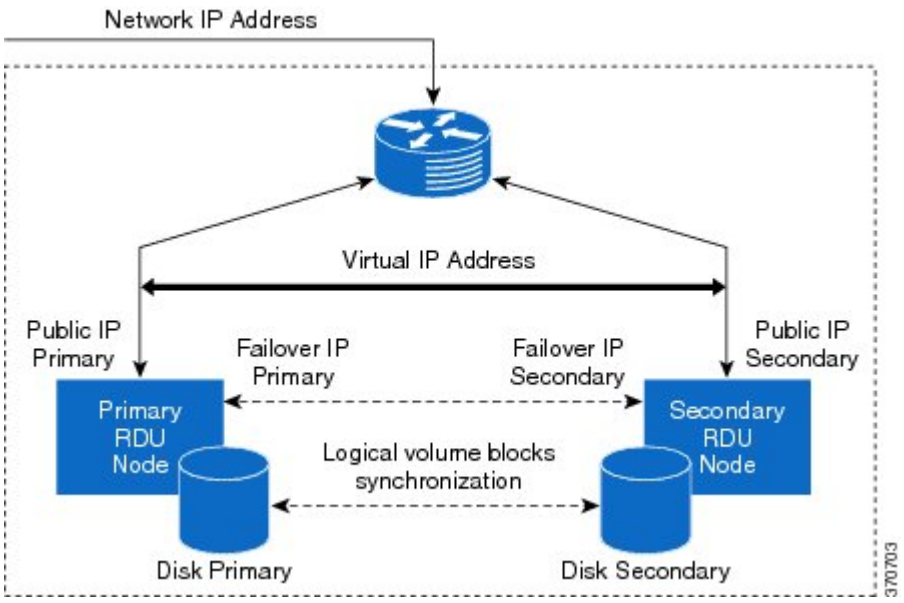
- Identify the virtual IP address that can be used to locate both servers. Ensure that this virtual IP address is not configured for any physical interfaces in the network infrastructure. Also, this virtual IP address must belong to the network cluster in which you configure the primary and secondary RDU nodes.
- In PCP Geo redundancy solution the VIP can be in any subnet
- Identify the network IP addresses for public and private interface to configure dual ring support. For more information on dual ring support, see *Cisco Prime Cable Provisioning User Guide*.
- 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

- To enable RDU HA notifications support, ensure that the SMTP server is configured. For more information on RDU HA notifications, see *Cisco Prime Cable Provisioning User Guide*.
- Both RDU nodes must be configured with Gigabyte network interfaces.

The following figure provides a high level RDU HA setup.

Figure 9: RDU HA Setup



RDU HA Installation Modes

In Prime Cable Provisioning, you can configure RDU HA setup using the following installation modes:

- Primary-Secondary – Used to configure the RDU HA setup with both the primary and secondary nodes available in the network infrastructure.
- Primary Only – Used to create the RDU HA setup only on the primary node. You can deploy the secondary RDU node in future, and configure the RDU HA cluster.
- Secondary Only – Used to create the RDU HA setup only on the secondary node. After the RDU HA setup is created on primary and secondary nodes, you can configure the RDU HA cluster.
- Configure HA – Used to configure the RDU HA cluster if the cluster is HA ready.
- Recovery – Used to recover an impacted (corrupted) RDU node in the HA cluster.

Common Initial Steps for Configuring RDU HA Nodes

The configuration of RDU HA nodes involves some common initial steps, irrespective of the mode of installation. You can perform these initial steps on primary RDU server, secondary RDU server or both the servers, based on the mode of installation. You can then proceed with specific installation steps as defined in other topics.

Procedure

Step 1 Login to the RDU server as root.

Step 2 Modify the config file to disable SELinux using the following command:

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

where, config file controls the state of SELinux on the system. In this file, set the value of SELINUX to disabled.

Step 3 Enter the host details of RDU node using the following command:

```
# vi /etc/hosts
```

The host details involve the public IP addresses, FQDN and short name of primary RDU node.

Step 4 Disable iptables on the RDU node:

```
# systemctl stop firewalld.service
```

Step 5 Verify if the iptables are disabled:

```
# systemctl status firewalld.service
```

Step 6 Reboot the RDU server:

```
# reboot
```

Step 7 Verify if the SELinux is disabled:

```
# /usr/sbin/sestatus
```

RDU HA Setup in Primary-Secondary Mode

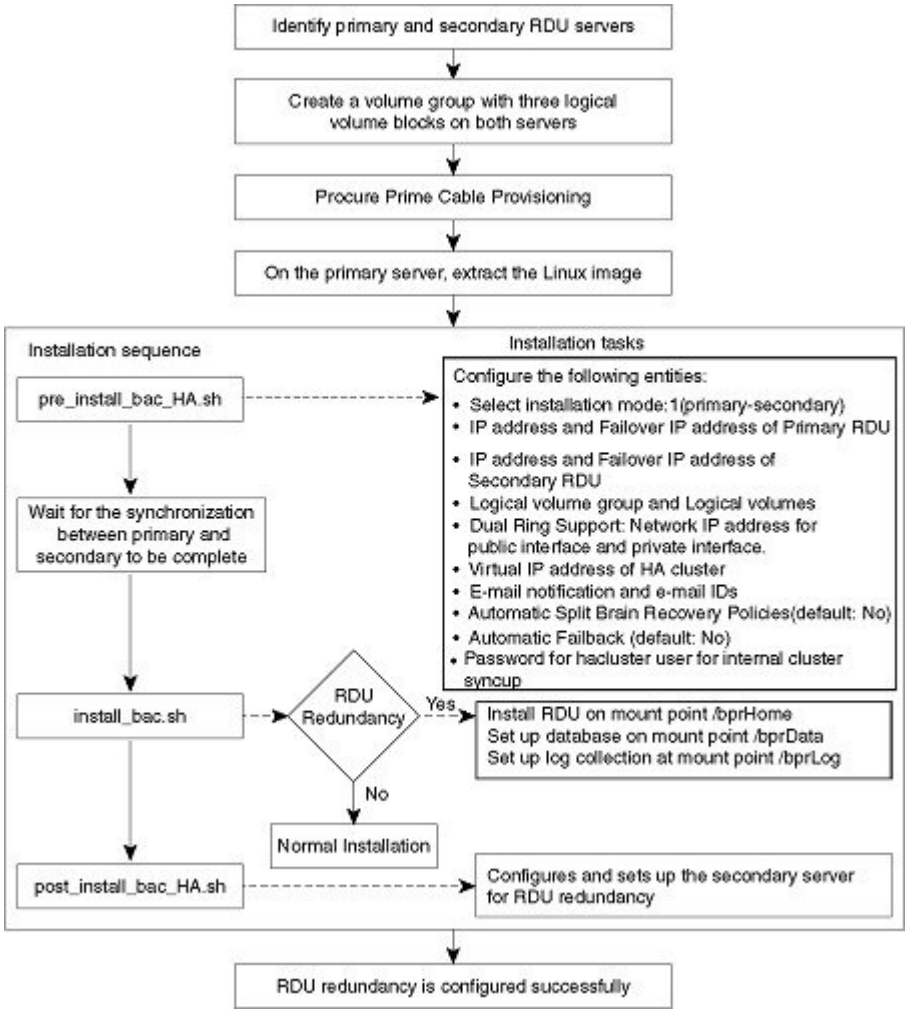
If both primary and secondary RDU nodes are available in the network infrastructure, you can use primary-secondary installation mode to configure HA cluster.

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 10: 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 Log into the primary and secondary RDU servers as root.

Step 2 Modify the config file to disable SELinux using the following command:

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

where, **config** file controls the state of SELinux on the system. In this file, set the value of SELINUX to disabled.

Step 3 Enter the host details of RDU nodes on both primary and secondary servers using the following command:

```
# vi /etc/hosts
```

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
10.104.182.92 <rdu-primary>.cisco.com <rdu-primary>
10.104.182.93 <rdu-secondary>.cisco.com <rdu-secondary>
```

Note The host details involve the public IP addresses, FQDNs and short names of RDU nodes.

The host details should not involve the failover ip address.

Step 4 Disable ip tables on both the RDU nodes using the following command:

```
# systemctl stop firewalld.service
```

```
# systemctl disable firewalld.service
```

Step 5 Verify if the ip tables are disabled using the following command:

```
# systemctl status firewalld.service
```

Step 6 Reboot both primary and secondary RDU servers using the following command:

```
# reboot
```

Step 7 Verify if the SELinux is disabled using the following command:

```
# /usr/sbin/sestatus
```

Step 8 Perform the steps on both the primary and secondary RDU nodes as described in Common Initial Steps for Configuring RDU HA Nodes, on page 44.

Step 9 Configure the SSH access between primary and secondary RDU nodes and disable the password authentication:

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

```
# ssh-keygen -t rsa -f ~/.ssh/id_rsa -N ""
```

The system generates the SSH keys as follows:

```
Generating public/private rsa key pair.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:WGmpP4lHBg6wyjDPlQ8LFhqdTQ6RqcQQx4eFccKFras root@<rdu primary>
The key's randomart image is:
+---[RSA 2048]----+
|*=O/=            |
| *@O+.   o       |
|=.+o* . =        |
|+*.o * *         |
|..o.. = S        |
|  .    = .       |
| .    . =        |
|E      . .       |
|                 |
+----[SHA256]-----+
```

b. Copy the SSH keys to the secondary RDU node:

 # # ssh-copy-id -i ~/.ssh/id_rsa.pub root@<rdu-primary/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:

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/root/.ssh/id_rsa.pub"
The authenticity of host '<rdu-secondary> (10.65.125.53)' can't be established.
ECDSA key fingerprint is SHA256:C5vHIqW4ZqfBJ2QeNPgm+w1E42/FSxwfbxxCXRL3b60.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
 out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys
root@<rdu-secondary>'s password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@pcp-lnx-23'"
and check to make sure that only the key(s) you wanted were added.
```

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

 # ssh *<target RDU server>* **-- uname -a**

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> 4.18.0-240.22.1.el8_3.x86_64 #1 SMP Thu Apr 8 19:01:30
 UTC 2021
 x86_64 x86_64 x86_64 GNU/Linux
```

Step 10 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 11 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>*

Step 12 Make sure servers have internet connectivity to download packages from CentOS Repo.

Step 13 **Note** For CentOS 8.3, follow the Steps 13 and 14, and for RHEL 8.3, enable the Red Hat subscription on RHEL 8 and then enable a High Availability repository to download the cluster packages from Red Hat.

Configure repository directory in */etc/yum.repos.d* for HA repository.

Copy and save the following as **HA-vault.repo** in */etc/yum.repos.d* :

```
[base-vault]
name=CentOS Linux $releasever - Base
baseurl=http://vault.centos.org/centos/8.3.2011/BaseOS/x86_64/os/
gpgcheck=1
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-centosofficial

[AppStream-vault]
name=CentOS Linux $releasever - AppStream
baseurl=http://vault.centos.org/centos/8.3.2011/AppStream/x86_64/os/
gpgcheck=1
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-centosofficial

[ha-vault]
name=CentOS Linux $releasever - HighAvailability
baseurl=http://vault.centos.org/centos/8.3.2011/HighAvailability/x86_64/os/
gpgcheck=1
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-centosofficial
```

Step 14 **Note** For Geo setup in RHEL 8.3, RHEL EPEL repository should be enabled to install the frr package.

Configure the repository for Geo setup.

Copy and save the following as **frr-7.repo** in */etc/yum.repos.d* :

```
[frr]
name=FRRouting 7.x Packages for Enterprise Linux 8 - $basearch
```

```
baseurl=https://rpm.frrouting.org/repo/el8/frr7
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-FRR

[frr-RPKI]
name=FRRouting 7.x Packages with RPKI for Enterprise Linux 8 - $basearch
baseurl=https://rpm.frrouting.org/repo/el8/frr-rpki
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-FRR

[frr-extras]
name=FRRouting Dependencies for Enterprise Linux 8 - $basearch
baseurl=https://rpm.frrouting.org/repo/el8/extras
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-FRR
```

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 4: RDU Two Node Failover Pair Setup

Sequence	Installation Scripts	Description
1	pre_install_bac_HA.sh	Used to configure the following entities: • Installation mode: 1 (primary-secondary) • Logical volume group and logical volumes • Failover IP addresses of both the RDU nodes • Network IP address • Dual ring support; Network IP addresses for public and private interfaces • Automatic failback • RDU HA notifications; Email addresses of the recipients to receive RDU HA cluster notifications • Virtual IP address • Secondary RDU server public IP address • Automatic split brain recovery • Utilities required for RDU redundancy function setup. • Password for hacluster user.

Sequence	Installation Scripts	Description
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:

```
gunzip -d BAC_63_LinuxK9.gtar.gz
```

```
gtar -xzvf BAC_63_LinuxK9.gtar
```

The utility creates the BAC_63_LinuxK9 directory into which the installation program is extracted.

Step 3 Run the preinstallation script using the following command:

```
# sh pre_install_bac_HA.sh
```

Step 4 Select the installation mode **1 (primary-secondary)** to configure the RDU HA cluster with both primary and secondary nodes available in the network infrastructure.

Step 5 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 6 Enter the name of the logical volume group. For example, VGBPR.

Step 7 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 8 Enter the network IP address of the subnet under which both the RDU cluster nodes exist.

Step 9 Enter the network IP addresses for both public and private interfaces of the RDU cluster nodes. The Network IP address (public) is configured for the network ring on public interface, and the Network IP address (private) is configured for the network ring on private interface. For more information on dual ring configuration, see *Cisco Prime Cable Provisioning User Guide*.

Step 10 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.

- For PCP Geo redundancy solution the CIDR value of VIP should be 32.

Step 11 For PCP Geo redundancy solution (i.e if both the servers are on different subnet) enter "**y**" to advertise VIP using frr, else enter "**n**" .

- If VIP advertisement through frr is enabled then enter the interface through which you want to advertise the VIP, by default it is ens, make sure this interface name is same on both primary and secondary servers, also make sure this interface is connected to the ingress router where route injection is done.
- If VIP advertisement through frr is disabled then enter the CIDR value for VIP.

Step 12 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 13 Enter valid password to set and authenticate hacluster user, for internal communication between cluster servers.

Step 14 Enter **n** to disable RDU HA email notifications, the default value is **y**.

To configure email notifications, you must:

a. configure the following properties in */etc/postfix/main.cf* file:

- relay_domains = <*SMTP_IPaddress*> or <*Domain_name_address*>
- relayhost = <*SMTP_IPaddress*> or <*Domain_name_address*>

b. enter the email addresses of the recipients to receive the HA cluster notifications. The email addresses of multiple recipients are configured using comma separated list.

Note You can also enter a valid email alias to trigger RDU HA email notifications to a dedicated group of recipients.

The email notifications are triggered for the following events:

- Primary or secondary RDU node changes its state during the failover or failback occurrence
- CRM resources become unresponsive or changes its state
- Split brain occurrence

Step 15 Enter **y** to enable the automatic split brain recovery. For information on split brain recovery policies, see Cisco prime Cable Provisioning User Guide.

Note Even though both automatic failback and automatic split brain recovery are enabled, some of the data may be discarded to ensure automatic recovery from the split brain situation.

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 16 Install RDU on the synchronized logical volumes; **LVBPRHOME**, **LVBPRDATA**, and **LVBPRDBLOG**. For details, see Installing the RDU in Interactive Mode, on page 21.

Step 17 Run the post-installation script available under **BAC_63_LinuxK9** directory:

```
# sh post_install_bac_HA.sh
```

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

RDU HA Setup in Primary-Only and Secondary-Only Modes

Prime Cable Provisioning provides you the flexibility to first deploy the primary RDU node with HA setup ready, and later deploy the secondary RDU node and create the RDU HA cluster.

To configure the RDU HA setup using primary only and secondary only modes, you must perform the following tasks sequentially:

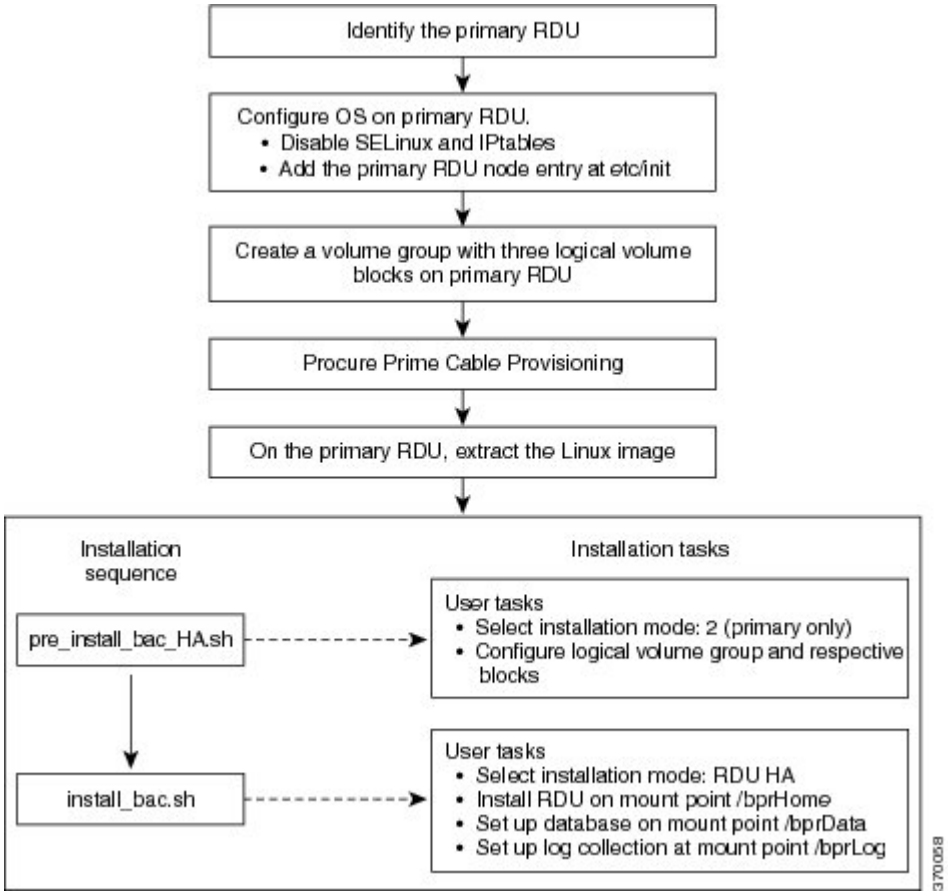
1. Create RDU HA setup on the primary node.
2. Create RDU HA setup on the secondary node.
3. Configure the cluster for HA.

Configuring RDU Node in Primary-Only Mode

The primary only installation mode helps you to create the HA setup on the primary RDU node. You can deploy the secondary RDU node at a later stage, and configure the HA setup without impacting the primary node configuration.

The following figure provides the workflow to create the HA setup on primary RDU node.

Figure 11: RDU HA Setup on Primary Node



To create the HA setup on primary RDU node:

Procedure

Step 1 Perform the steps on the primary RDU node as described in Common Initial Steps for Configuring RDU HA Nodes, on page 44.

Step 2 Extract the installation package:

```
gtar -xzvpf BAC_63_LinuxK9.gtar
```

The utility creates the BAC_63_LinuxK9 directory into which the installation program is extracted.

Step 3 Run the preinstallation script:

```
# sh pre_install_bac_HA.sh
```

Step 4 Select the installation mode as **2** (primary only).

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.

The preinstallation script performs the following automated operations on both primary RDU nodes:

- Installs the utilities for RDU redundancy setup, and stops them.
- Removes chkconfig entries for configuring the utilities.
- Formats all the LVBs using ext4.

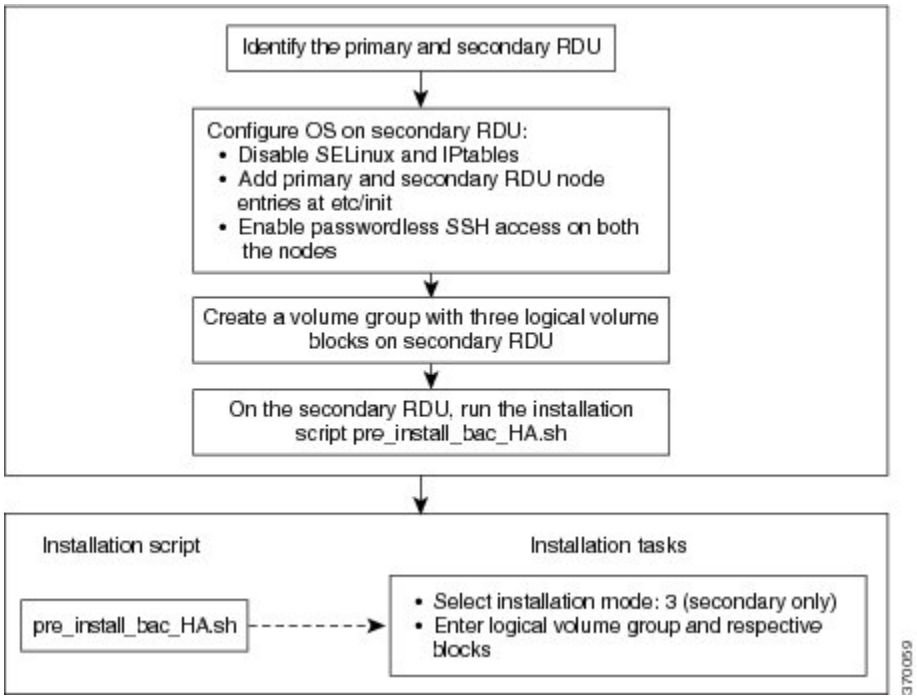
Step 7 Install RDU on the synchronized logical volumes - **LVBPRHOME**, **LVBPRDATA**, and **LVBPRDBLOG**. For details, see Installing the RDU in Interactive Mode, on page 21.

Configuring RDU Node in Secondary-Only Mode

The secondary-only installation mode helps you to create the HA setup on secondary RDU node. You can proceed with this installation mode if you have identified the primary node and it meets the prerequisites. The secondary RDU node is deployed to configure the RDU two node failover pair.

The following figure provides the workflow to create the HA setup on secondary RDU node.

Figure 12: RDU HA Setup on Secondary Node



To create the HA setup on secondary RDU node:

Procedure

Step 1 Check whether the primary RDU node is already identified and it meets the prerequisites.

Step 2 Perform the steps on the secondary RDU node as described in Common Initial Steps for Configuring RDU HA Nodes, on page 44.

Step 3 Configure the SSH access between primary and secondary RDU nodes and disable the password authentication:

- Create the SSH keys, on the secondary RDU node, :

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

- Copy the SSH keys to the primary RDU node:

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

  `# scp -r ~/.ssh <rdu-primary>:`

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

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

 # /usr/sbin/sestatus

Step 4 Verify if the SSH access is available without password authentication, on the primary and secondary RDUs:

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

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

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

```
Linux <target RDU server> 3.10.0-693.11.6.x86_64 #1 SNP Wed Jun 13 18:24:36 EDT
2012
x86_64 x86_64 x86_64 GNU/Linux
```

Step 5 Extract the installation package:

gtar -xzvpf BAC_63_LinuxK9.gtar.gz

The utility creates the BAC_63_LinuxK9 directory into which the installation program is extracted.

Step 6 Run the preinstallation script:

 # sh pre_install_bac_HA.sh

Step 7 Select the installation mode as **3** (secondary only).

Step 8 Enter the name of the logical volume group. For example, VGBPR.

Step 9 Enter the name of the logical volume blocks 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.

Note In case of *secondary only* installation, the preinstallation script restricts mounting of LVBs on home, data, and DBlog directories.

The preinstallation script performs the following automated operations on secondary RDU node:

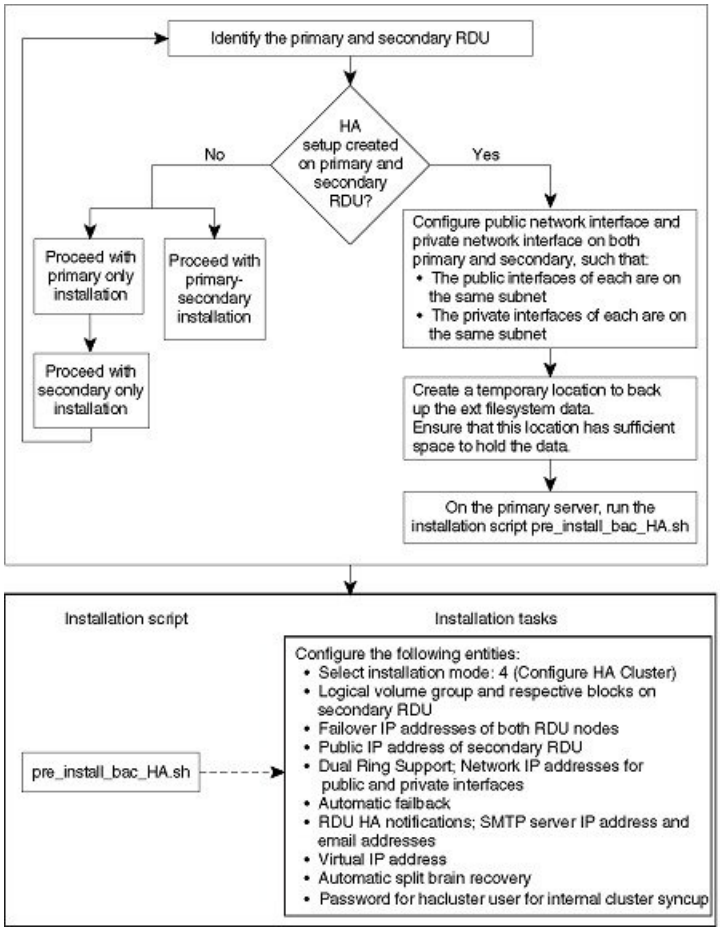
- Installs the utilities for RDU redundancy setup.
- Creates the required resources for synchronizing the block devices.
- Adds the chkconfig entries for configuring the utilities.
- Formats all the LVBs using xfs only on secondary node.

Configuring HA Cluster from an RDU HA Ready Installation

If the installation is HA Ready (the primary server is successfully set up with the Primary Only mode), you can configure the HA cluster. You can run the installation script *pre_install_HA_bac.sh* and choose the installation mode **4 (configure HA)** to configure the required resources and synchronize the primary and secondary RDU nodes.

The following figure provides the workflow for configuring the RDU two node failover pair.

Figure 13: Configure HA Cluster



To configure the HA cluster:

Procedure

Step 1 Check whether the RDU HA setup is created on primary RDU using the primary-only mode. For information on how to create the HA setup, see Configuring RDU Node in Primary-Only Mode, on page 53.

Step 2 Check whether both the nodes (primary and secondary) have one public network interface each, configured in the same subnet; and one private network interface each, configured in the same subnet (different from the previous subnet).

Step 3 Create a temporary location on the primary RDU where you can back up the xfs filesystem data. Ensure that the appropriate space is available in the temporary location to store the existing file system data.

Note When you configure the RDU HA cluster, the xfs filesystem on primary RDU server is overwritten with DRBD filesystem. The installation mode **4 (configure HA)** facilitates you to back up the xfs filesystem data and store it in a temporary location. This data is further restored after the DRBD filesystem is created on primary RDU server.

Step 4 Log into the primary RDU node as root, and run the installation script *pre_install_bac_HA.sh*.

Step 5 Select the installation mode **4 (configure HA)**.

Step 6 Enter the temporary location to back up the xfs filesystem data.

Step 7 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 server - Public IP address that is used for external communication.

Step 8 Enter the name of the logical volume group. For example, VGBPR.

Step 9 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 10 Enter the network IP address for both public and private interfaces of the RDU cluster nodes. The Network IP address (public) is configured for the network ring on public interface, and the Network IP address (private) is configured for the network ring on private interface. For more information on dual ring configuration, see Cisco Prime Cable Provisioning User Guide.

Step 11 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 12 Enter **y** to enable RDU HA email notifications. To configure email notifications, you must:

- Configure the following properties in */etc/postfix/main.cf* file:
  - relay_domains = <*SMTP_IPaddress*> or <*Domain_name_address*>
  - relayhost = <*SMTP_IPaddress*> or <*Domain_name_address*>
- Enter the email addresses of the recipients to receive the HA cluster notifications. The email addresses of multiple recipients are configured using comma separated list.

  Note You can also enter a valid email alias to trigger RDU HA email notifications to a dedicated group of recipients.

The email notifications are triggered for the following events:

- Primary or Secondary RDU node changes its state during the failover or failback occurrence
- CRM resources become unresponsive or changes its state
- Split brain occurrence

Step 13 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.

Step 14 Enter **y** to enable the automatic split brain recovery. For information on split brain recovery policies, see *Cisco Prime Cable Provisioning User Guide*.

The *pre_install_bac_HA.sh* 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.
- Adds the chkconfig entries for configuring the utilities.

Step 15 Enter valid password to set and authenticate hacluster user. For internal communication between cluster servers.

Step 16 Run the post-installation script available under **BAC_63_LinuxK9** directory:

```
# sh post_install_bac_HA.sh
```

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

Recovering an Impacted RDU Node Using Recovery Mode

If any of the RDU nodes in the HA cluster gets corrupted, you can recover the impacted RDU node using the recovery mode. The recovery mode facilitates you to synchronize the impacted RDU node with the active RDU node, and restore the corrupted filesystem data.

To recover the impacted RDU node:

Procedure

Step 1 Ensure the following:

- The impacted RDU node conforms to the required prerequisites and that the initial configuration is set up. For details, see Prerequisites, on page 42 and Common Initial Steps for Configuring RDU HA Nodes, on page 44.
- SSH is also configured on the impacted node, with password authentication disabled.
- The public network interface and the private network interface of the impacted node are configured with the same IP address as before.

Step 2 Log into the impacted RDU node as root, and run the installation script *pre_install_bac_HA.sh*.

Step 3 Select the recovery mode **5**.

Step 4 Enter the public IP address of the active RDU node.

Step 5 Enter the name of the logical volume group.

Step 6 Enter the name of the logical volumes created on /bprHome, /bprData, and /bprLog directories.

Once the synchronization of the filesystem is completed, the impacted RDU node gets reconnected to the RDU HA cluster.

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 5: Uninstall RDU HA Setup

Sequence	Uninstall Scripts	Description
1	uninstall_bac.sh	Used to unistall the RDU component from the logical volume blocks; /bprHome, /bprData, and /bprLog. For details, see Uninstalling Prime Cable Provisioning, on page 38.
2	uninstall_bac_HA.sh	Used to remove the utilities installed for RDU redundancy function. Remove VIP from primary server after successful completion of uninstall_bac_HA.sh using the following command. *ip -f inet addr del VIP/CIDR value brd netmask value dev interface name* *ex: ip -f inet addr del 10.10.2.1/32 brd 255.255.255.255 dev lo*

Note In the RDU HA cluster:

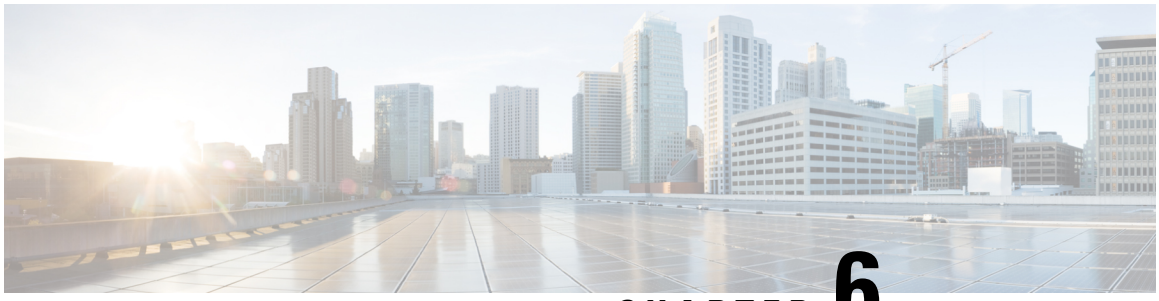
- If you want to uninstall the RDU HA setup created only on the primary RDU node, run the uninstall_bac.sh and uninstall_bac_HA.sh sequentially on the primary RDU node as described in Table 5: Uninstall RDU HA Setup, on page 60.
- If you want to uninstall the RDU HA setup created only on the secondary RDU node, run the uninstall_bac_HA.sh on the secondary RDU server.

RDU Geo Redundancy

RDU Geo Redundancy is an enhanced feature of RDU HA supported on RHEL 8.3 or CentOS 8.3 with kernel(4.18.0-240) (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 41



CHAPTER 6

Upgrading Prime Cable Provisioning

Prime Cable Provisioning 6.3 can be upgraded from PCP 5.x/6.x. Prime Cable Provisioning 6.3 supports only 64-bit servers. If you are running any earlier 5.x version of Prime Cable Provisioning on 32-bit servers, you should first upgrade to 64-bit servers and then upgrade to Prime Cable Provisioning 6.3.

All components of Prime Cable Provisioning 5.x/6.x can be upgraded to Prime Cable Provisioning 6.3. You need to migrate the database, if you upgrade to Prime Cable Provisioning 6.3 from Prime Cable Provisioning 5.x.

See Cisco Prime Cable Provisioning Upgrade Matrix for more details.

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 PCP 5.x/6.x to Prime Cable Provisioning 6.3, on page 63
- **eRouter Migration tool** , on page 83

Upgrade Cisco PCP 5.x/6.x to Prime Cable Provisioning 6.3

You can upgrade all components of Cisco PCP 5.x/6.x by running the Prime Cable Provisioning 6.3 installer. The installer automatically upgrades the installed components to Prime Cable Provisioning 6.3. 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 5.x/6.x RDU database and verify the same.
- Install the Prime Cable Provisioning 6.3 RDU. After the fresh installation, you need to migrate the database either using the migration tool or the migration script.
- Auto-upgrade is not supported for KDC on Linux. Though you can manually upgrade KDC, we recommend fresh installation to avoid any installation issues.
- You can upgrade RDU, DPE, CPNR-EP and PWS from Cisco PCP 5.x or above to Prime Cable Provisioning 6.3 .
- 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 10.x or above, and then upgrade the Prime Network Registrar Extension Points to Prime Cable Provisioning 6.3. For the Prime Network

Registrar upgrade to 10.x see the *Cisco Prime Network Registrar 11.x Installation Guide* and for the extension points upgrade, see Upgrading Cisco Prime Network Registrar Extensions, on page 79.

The following table represents the components that can be upgraded from the previous versions to Prime Cable Provisioning 6.3.

Components	6.x	5.x
RDU	Y (After upgrade, migrate the database)	Y (After upgrade, migrate the database)
RDU HA	Y	Y
PWS	Y	Y
DPE	Y	Y
CPNR Extension point	Y	Y
KDC	Y	Y

See Cisco Prime Cable Provisioning Compatibility Matrix for more details about which components can be auto-upgraded to Prime Cable Provisioning 6.3 and which need fresh installation.

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

About Backward Compatibility

Prime Cable Provisioning 6.3 RDU can interoperate with 5.x, 6.x versions of Provisioning Group components (DPE and PNR EP).

Note In Prime Cable Provisioning 6.3, to avoid the java secure mode communication issue during interoperability (DPE in 5.x and RDU 6.3) follow the below steps:

1. After upgrading the RDU to PCP 6.3, edit the following properties in $BPR_HOME/jre/lib/security/java.security file .

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

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

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

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

2. Add the following properties in the *BPR_HOME/rdu/conf/rdu.properties* file:

```
/ssl/cipher/all=disabled
/ssl/cipher/customList=SSL_RSA_WITH_RC4_128_MD5,TLS_RSA_WITH_AES_256_CBC_SHA256
```

3. Restart the RDU and DPE, and start testing for InterOperability in secure mode.

After upgrading DPE, PNR EP, PWS to 6.3, add the content removed in *Step 1* back to the *java.security* file and remove the properties added in *Step 2*. Then the PCP components in secure mode will use the strong ciphers supported by PCP, see Ciphers Supported for Secure Communication Section of Cisco Prime Cable Provisioning User Guide.

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

Note

- In Prime Cable Provisioning 6.3, the RDU user configuration overrides RADIUS user configuration for authorization. This is done to support backward compatibility of existing RADIUS users. After migrating from an earlier version to Prime Cable Provisioning 6.3, all existing RADIUS users are migrated as local users in RDU. So it is advised that you delete all the existing duplicate RADIUS users once the RADIUS users are configured with the appropriate Cisco AV Pairs.
  - Existing read-only and read-write users would be mapped to new ReadOnly and ReadWrite users.
  - Default out of the box (OOTB) admin user will be mapped to Admin role.
  - Radius users will be migrated as local RDU users.
- Prime Cable Provisioning provides multivendor support through Option 43 and its suboptions. When using this option, ensure that you modify templates used in earlier releases to be compatible with the template grammar that Prime Cable Provisioning 6.3 uses.
- You must upgrade the existing API client libraries (.jar files) to Prime Cable Provisioning 6.3. 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 85.

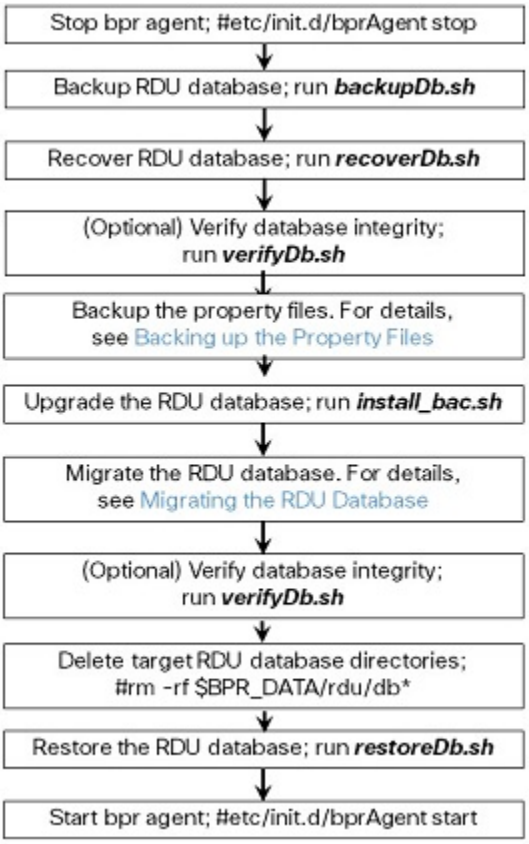
Database Migration

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

1. Backing Up the RDU Database
2. Recovering the Backed Up RDU Database
3. Verify Database Integrity of Cisco PCP 5.x/6.x
4. Backing up the Property Files
5. Upgrading RDU from Cisco PCP 5.x/6.x to PCP 6.3
6. Migrating the RDU Database
7. Verifying Database Integrity of Prime Cable Provisioning 6.3

The following figure describes the workflow for database migration.

Figure 14: Database Migration



Backing Up the RDU Database

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

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

Note We recommend that you use the throttle option always since it is not an I/O intensive operation. The throttle option is supported in Prime Cable Provisioning 6.3.

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 PCP 5.x

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

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

Note To verify the database before migration, use the **verifyDb.sh** tool from the Cisco PCP 5.x installation corresponding to the version of the database. You cannot verify a non-migrated database with the Prime Cable Provisioning 6.3 version of **verifyDb.sh**.

For example, enter:

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

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

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

Backing up the Property Files

If you have customized any of the property files during your current installation (BAC 4.2.x, PCP 5.x/6.x), you will need to first back them up and then copy them manually to the Prime Cable Provisioning 6.3 database.

To back up the property files:

Procedure

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

```
# systemctl stop bpragent
```

Step 2 Back up the following files.

- files under *<BAC_HOME>/rdu/conf/*
  - *rdu.properties*
  - *adminui.properties*
  - Other xml files and dtd files
    - /opt/CSCObac/rdu/conf/CABLEHOME_OptionDesc.dtd
    - /opt/CSCObac/rdu/conf/PKTCBL_OptionDesc.dtd
    - /opt/CSCObac/rdu/conf/DOCSIS_OptionDesc.dtd
    - /opt/CSCObac/rdu/conf/log4j.xml
    - /opt/CSCObac/rdu/conf/PKTCBL_OptionDesc.xml
    - /opt/CSCObac/rdu/conf/CABLEHOME_OptionDesc.xml
    - /opt/CSCObac/rdu/conf/DOCSIS_OptionDesc.xml
    - /opt/CSCObac/rdu/conf/AuditLog.properties
- the MIB files under *$BAC_HOME/rdu/mibs/*
- the *.xml files under *$BAC_HOME/snmp/conf/*

In addition to the above files when you upgrade from Cisco BAC 4.2.x, PCP 5.x/6.x to PCP 6.3, 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 PCP 5.x/6.x to PCP 6.3

Use this procedure to upgrade the RDU of Cisco PCP 5.x/6.x to PCP 6.3:

Note See Cisco Prime Cable Provisioning Upgrade Matrix for details about which components can be auto-upgraded to Prime Cable Provisioning 6.3 and which need fresh installation.

Procedure

Step 1 Unpack the Prime Cable Provisioning 6.3 install package with .gtar extension using the following command:

On Linux:

```
gtar -zxpf BAC_63_LinuxK9.gtar.gz
```

Step 2 To start the upgrade process for RDU, select the RDU component after running the install script of Prime Cable Provisioning 6.3 using the following command:

On Linux:

```
# <install-path>/BAC_63_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 package.

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

The installation program will take the required backup, and remove Cisco PCP RDU. The installation program also prompts you to proceed with the installation of Prime Cable Provisioning 6.3 RDU. To continue with the installation see, Installing the RDU in Interactive Mode, on page 21.

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

Step 6 To verify if the output information indicates Prime Cable Provisioning 6.3, enter:

On Linux:

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

Upgrading PCP along with HA

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

- Geo HA is available only from 5.2.x. Fresh Installation of PCP 6.3 Geo and Local HA setup works only on RHEL / CENTOS 8.3 (kernel - 4.18.0-240). Upgrading Geo and Local HA setup to PCP 6.3 works on RHEL / CENTOS 7.4 (kernel - 3.10.0-693.11.6).

Note If you are upgrading to 6.3 version, then you must upgrade the OS to RHEL/CENTOS 7.4 with kernel (3.10.0-693.11.6) or RHEL/CENTOS 8.3 with kernel (4.18.0-240).

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 71 or Upgrading PCP along with HA - Procedure 2, on page 72.

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

- Upgrading from PCP 5.x/5.2.x/5.3.x/6.x RDU to 6.3 RDU Local / Geo HA Cluster.

- Upgrading from PCP 5.x/5.2.x/5.3.x/6.x RDU Local HA Cluster to 6.3 RDU Local HA Cluster with OS Upgrade
- Upgrading from PCP 5.x/5.2.x/5.3.x/6.x RDU Local HA Cluster to 6.3 RDU GEO HA Cluster.

If you are upgrading from any one of the scenario mentioned below, please follow the steps mentioned in Upgrading PCP along with HA - Procedure 3, on page 72.

Note Below scenarios does not require OS upgrade.

- Upgrading from PCP 6.1/6.1.x/6.2 RDU GEO HA Cluster to 6.3 RDU GEO HA Cluster.
- Upgrading from PCP 6.1/6.1.x/6.2 RDU Local HA Cluster to 6.3 RDU Local HA Cluster.
- Upgrading from PCP 6.1/6.1.x/6.2 RDU Local HA Cluster to 6.3 RDU GEO HA Cluster.

Upgrading PCP along with HA - Procedure 1

Procedure

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

Step 2 Upgrade the OS to RHEL/CENTOS 7.4 (kernel - 3.10.0-693.11.6) or RHEL/CENTOS 8.3 (kernel - 4.18.0-240) on primary node.

Step 3 Run the pre-installation script on the primary node and select option 2. For details, see: Configuring RDU Node in Primary-Only Mode, on page 53.

Step 4 Install RDU on the synchronized logical volumes; **LVBPRHOME**, **LVBPRDATA**, and **LVBPRDBLOG**. For details, see Installing the RDU in Interactive Mode, on page 21.

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

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

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

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

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

Step 9 Upgrade the OS to RHEL/CentOS 8.3 on the secondary node.

Step 10 Run the pre-installation script on the secondary node and select option 3. For details, see: Configuring RDU Node in Secondary-Only Mode, on page 55.

Step 11 Run the pre-installation script on the primary node and select option 4. For details, see: Configuring HA Cluster from an RDU HA Ready Installation, on page 57.

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

Step 12 Run the post-installation script available under **BAC_63_LinuxK9** directory:

```
# sh post_install_bac_HA.sh
```

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

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

Upgrading PCP along with HA - Procedure 2

Procedure

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

Step 2 Upgrade the OS to RHEL/CENTOS 7.4 (kernel - 3.10.0-693.11.6) or RHEL/CENTOS 8.3 (kernel - 4.18.0-240) on secondary node.

Step 3 Run the pre-installation script on the secondary node and select option 3. For details, see: Configuring RDU Node in Secondary-Only Mode, on page 55.

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

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

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

Step 7 Move the DB Backup to some common repository.

Step 8 Upgrade the OS to RHEL/CentOS 8.3 on the primary node.

Step 9 Run the pre-installation script on the primary node and select option 1. For details, see: Setting Up RDU Two Node Failover Pair, on page 50.

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

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

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

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

Upgrading PCP along with HA - Procedure 3

Procedure

Step 1 Turn the secondary RDU to standby mode, so that the VIP will be reachable through the primary RDU node. using the command: `/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh secondary on`

Step 2 Enable the firewall, so that the DPE and CNR-EP will not reach the VIP on the primary node.

Step 3 Stop the bprAgent using the command: `/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh stop res_bprAgent_1`

Step 4 Back up the RDU database and property files as described in section Backing Up the RDU Database and Backing up the Property Files.

Step 5 Move the DB Backup to some common repository.

Step 6 Delete the bprAgent resources using the command: `pcs resource delete res_bprAgent_1`

Step 7 Start the upgrade process for RDU `/BAC_63_Linux/install_bac.sh`

Step 8 Move the DB Backup from common repository to primary node and migrate the DB and restore the same, as described in Database Migration, on page 66 section.

Step 9 Turn off the secondary RDU to standby mode using the command:
`/bprHome/CSCObac/agent/HA/bin/standby_ha_switch.sh secondary off`

Step 10 Run the post-installation script available under **BAC_63_LinuxK9** directory on the primary node: `./post_install_bac_HA.sh`. The post-installation script performs the automated configuration tasks required for RDU redundancy function setup.

Step 11 Command is not Mandatary if bpragent service running:
`/bprHome/CSCObac/agent/HA/bin/manage_ha_resources.sh start res_bprAgent_1`

Step 12 Disable the firewall, so that the DPE and CNR-EP can reach the VIP.

Migrating the RDU Database

After you perform the sequence of steps (steps 1 to 5) as explained in Database Migration section , use the migration script (**migrateDb.sh**) for migrating the RDU database to Prime Cable Provisioning 6.3.

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

- Cisco BAC 4.2.x/ PCP 5.x/6.x on Linux to PCP 6.3 on Linux, use the migration script (**migrateDb.sh**) only.

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

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

Note In Prime Cable Provisioning 6.3 migration, migrateDB script does not migrate all the custom files from MIBs directory. It migrates only the MIB files that are mentioned in the rdu.properties. If the mibList property is not defined in rdu.properties, then it uses the MIB file names from the System Default Configuration and migrate those files to the database.

Table 6: migrateDb.sh Options

Argument	Description	Required	Optional	Default
-dbdir *dir*	Specifies the location of the database backup that is to be migrated.	✓		None
-dblogdir *dir*	Specifies the location of the database logs that are to be migrated.		✓	The directory that the -dbdir option specifies

Argument	Description	Required	Optional	Default
-cachesize *value*	Specifies, in MB, the size of the memory cache. If you use this parameter, you must not exceed the 100-MB limit, unless you reduce the value of the **-Xmx** variable in the migrateDb.sh script by double the increase in the cache size. For example, if you set cache size to 200 MB, you must reduce the value of **-Xmx** to: (200-100)*2 = 200 MB		✓	100 MB
-help	Specifies usage for the tool		✓	

Migrating to Prime Cable Provisioning 6.3 Using In-line Migration Script

Migrating the RDU database to Prime Cable Provisioning 6.3, using the in-line migration script - **migrateDb.sh**, consists of five main steps:

1. Install/ Upgrade the Prime Cable Provisioning 6.3 RDU.
2. Stop the bprAgent.
3. Run the **migrateDb.sh** script (which is located under *$BPR_HOME/migration*) on the backed up database.
4. Restore the migrated database.
5. Start the bprAgent. After the migration is complete, a message is displayed indicating the same. You cannot launch the Admin UI until this step is completed.

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

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

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

The following table describes the process of migration from Cisco BAC 4.2.x/ PCP 5.x/6.x Linux to Prime Cable Provisioning 6.3 Linux using examples that assume that:

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

- The migration from Cisco BAC 4.2.x/ PCP 5.x/6.x to 6.3 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 7: RDU Migration Workflow from Cisco BAC 4.2.x/ PCP 5.x/6.x Linux to Cisco Prime Cable Provisioning 6.3 Linux

Step	Task	See
1	Stop the *bprAgent* using the following command: `# systemctl stop bpragent`	

2	Run PCP 6.3 migrateDb.sh on the backed up database. The migrateDb.sh script resides in the $BPR_HOME/migration directory.
	For example:
	`# $BPR_HOME/migration/migrateDb.sh -dbdir`
	`/var/backup/rdu-backup-20130829-031028`
	-dbdir—Specifies the location of the database backup that is to be migrated; in this case, */var/backup*.	

3	Observe the migration progress using the *migration.log* file. For example: `# tail -f /var/backup/rdu-backup-20130829-031028/migration.log`	
4	Verify if the migration is complete using the migration.log file. If you find any warnings or notices, use the grep command-line tool to search them. For example: `# tail /var/backup/rdu-backup-20130829-031028/migration.log`	Cisco Prime Cable Provisioning User Guide

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

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

Step	Task	See

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

8	Start the *bprAgent* using the following command: `# systemctl start bpragent` This also starts the RDU process. Check the rdu.log file for messages on successful initialization, which also indicate that RDU will be up and running.	Cisco Prime Cable Provisioning User Guide
9	Also, you can check if the *$BPR_DATA/rdu/db/DB_VERSION* file indicates the database version as 6.3.	Cisco Prime Cable Provisioning User Guide
	Note Migration preserves the device record revision numbers used in DPE synchronization. As a result, DPE repopulation is not triggered after the RDU database upgrade, ensuring the least disruption until you upgrade the specific DPE.	
10	Verify the RDU operations by logging into the Admin UI. From **Servers > RDU**, you can check if the RDU version is 6.3 and if the device count statistics is correct (same number of devices as before and all the devices are in the same state as they were earlier)	Cisco Prime Cable Provisioning User Guide

About Migration Performance

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

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

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

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

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

Migration of Duplicate Class of Service and Node Name

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

- Class of Service—{*Technology_Name*}_{*Original_ClassOfService_Name*}
- Nodes—{*Node_Type*}_{*Node_Name*}

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

RDU Extension Migration

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

Enabling Password Encryption

Prime Cable Provisioning uses SHA1 digest algorithm for password encryption. However, when you migrate from Cisco BAC 4.2.x/ PCP 5.x to PCP 6.3, it continues to use the encryption algorithms used in Cisco BAC 4.2.x/ PCP 5.x. After successful migration, you can enable SHA1 digest algorithm for password encryption using the script **passwordEncryption.sh** available in *BPR_HOME/rdu/bin*.

Verifying Database Integrity of Prime Cable Provisioning 6.3

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

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

For example, enter:

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

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

Note You cannot verify a non-migrated database with the Prime Cable Provisioning 6.3 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 PCP 5.x or above to Prime Cable Provisioning 6.3. This reduces the time required for the synchronization with RDU while porting all the devices to the new DPE.

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

Procedure

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

a) Stop the Cisco PCP 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 PCP DPE server.

b) Copy the created database tar to the Cisco PCP 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 PCP DPE.

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

Upgrading DPE from Cisco PCP 5.x/6.x to PCP 6.3

Use this procedure to upgrade the DPE of Cisco PCP 5.x/6.x to PCP 6.3:

Procedure

Step 1 Unpack the Prime Cable Provisioning 6.3 install package with .gtar extension using the following command:

On Linux:

```
gtar -zxpf BAC_63_LinuxK9.gtar.gz
```

Step 2 To start the upgrade process for DPE, select the DPE component after running the install script of Prime Cable Provisioning 6.3 using the following command:

On Linux:

```
# <install-path>/BAC_63_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 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/6.x DPE. The installation program also prompts you to proceed with the installation of Prime Cable Provisioning 6.3 DPE. To continue with the installation see, Installing DPE in Interactive Mode, on page 27.

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

Step 6 To verify if the output information indicates Prime Cable Provisioning 6.3, enter:

On Linux:

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

DPE Rollback

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

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

Procedure

Step 1 Uninstall PCP 6.2 DPE, as described in the section Uninstalling Prime Cable Provisioning, on page 38

Step 2 Install the DPE version that you used for rollback, as described in the section Installing Prime Cable Provisioning, on page 19.

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 command:

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

The Prime Network Registrar extensions can be upgraded from Cisco PCP 5.x/PCP 6.x version to Prime Cable Provisioning 6.3 version.

Upgrading Prime Network Registrar-EP from Cisco PCP 5.x/6.x to PCP 6.3

Use this procedure to upgrade the Prime Network Registrar extension points of Cisco PCP 5.x/6.x to PCP 6.3:

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

- PCP 6.3 RDU is compatible with Cisco PCP 5.x/6.x CNR EP. See Cisco Prime Cable Provisioning Compatibility Matrix for more details.
- PCP 6.3 does not support 32-bit CNR EP.

Procedure

Step 1 Back up the file:

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

Step 2 Unpack the Prime Cable Provisioning 6.3 install package with .gtar extension using the following command:

On Linux:

```
gtar -zxpf BAC_63_LinuxK9.gtar.gz
```

Step 3 To start the upgrade process for Prime Network Registrar extensions, select the CPNR-EP component after running the install script of Prime Cable Provisioning 6.3 version using the following command:

On Linux:

```
# <install-path>/BAC_63_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 PCP 5.x package.

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

The installation program removes the Cisco PCP 5.x/PCP 6.x package, and prompts you to proceed with Prime Cable Provisioning 6.3 installation. To continue with the installation, see Installing Prime Network Registrar Extension Points in Interactive Mode, on page 29.

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

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

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

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

Step 8 To verify if the output information indicates Prime Cable Provisioning 6.3, enter:

On Linux:

```
# rpm -qa CSCObac
```

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

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

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

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

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

Enabling eRouter Capabilities

Procedure

	Command or Action	Purpose
Step 1	Enable eRouter1.0 IPv4 registered capability in CNR using the script /opt/CSCObac/cnr_ep/bin/changeNRProperties.sh **Example:** `./changeNRProperties.sh -ee "enabled"`	
Step 2	Enable eRouter1.0 IPv6 registered capability in CNR using the script /opt/CSCObac/cnr_ep/bin/changeNRProperties.sh **Example:** `./changeNRProperties.sh -eev6 "enabled"`	
Step 3	Run the script /opt/CSCObac/cnr_ep/bin/changeNRProperties.sh with option -edns to initialize the /eRouter/dns/server property with the DNS Server details. The DNS Server can be a single IP Address or a list of comma separated IP addresses. This will ensure that "domain-name-servers" mandatory Option is sent from PCP during the eRouter provisioning process.	

	Command or Action	Purpose

	Example:
	`./changeNRProperties.sh -edns DNS-Server-IP`
	`./changeNRProperties.sh -edns 192.168.4.3`
	`./changeNRProperties.sh -edns 192.168.4.3,192.168.5.2,192.168.3.1`	

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

Upgrading KDC from Cisco PCP 5.x/6.x to Prime Cable Provisioning 6.3

Prime Cable Provisioning does not support automatic upgrade for KDC on Linux. We recommend fresh installation of Prime Cable Provisioning 6.3 KDC. Here is the manual procedure to upgrade the KDC of Cisco PCP 5.x to Prime Cable Provisioning 6.3:

Procedure

Step 1 Back up the following files:

- All certificates from `<BPR_HOME>/kdc/<Operating_System>/packetcable/certificates` directory.
- KDC_private_key.pkcs8 from `<BPR_HOME>/kdc/OS/` directory.
- bacckdc.license from `<BPR_HOME>/kdc` directory.

Step 2 Uninstall the 5.x KDC.

Step 3 Install the Prime Cable Provisioning 6.3 KDC. See Installing KDC in Interactive Mode, on page 34.

Step 4 After the upgrade is complete, restore:

- All certificates to `<BPR_HOME>/kdc/<Operating_System>/packetcable/certificates` directory.
- KDC_private_key.pkcs8 to `<BPR_HOME>/kdc/OS/` directory.
- bacckdc.license to `<BPR_HOME>/kdc` directory.

eRouter Migration tool

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

- Configuration > Defaults > eRouter Defaults > Click the Enabled radio button of the eRouter Feature.
- Enable the IPv4 - ERouter 1.0 , IPv6 - ERouter 1.0 capability in the provisioning group details page.

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

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

Parameters

-cachesize	An optional parameter that specifies cache size in MB. The default cache size is 100MB.
-dbdir	An optional parameter to specify the database directory path. If not specified, RDU database will be used by default.
-dblogdir	An optional parameter for database log directory path, if **-dbdir** is used. If not specified the directory specified with - **dbdir** option is used by default.
-detecterouterdevices	An optional parameter for directory path to write MAC/DUID address. If specified, tool will find MAC address of the device which are detected as computer and write to a file in the specified directory. If MAC address is not available, it will print DUID address to a file.
-inputmacfile	An optional parameter to read MAC address. If specified, tool reads MAC address from this file for migration and convert as eRouter. Cannot be used with - **detecterouterdevices** or **-inputduidfile** option.
-inputduidfile	An optional parameter to read DUID address. If specified, tool reads the DUID address from this file for migration and converts it as eRouter. Cannot be used with - **detecterouterdevices** or - **inputmacfile** option.

SAMPLE USAGE:

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

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

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

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

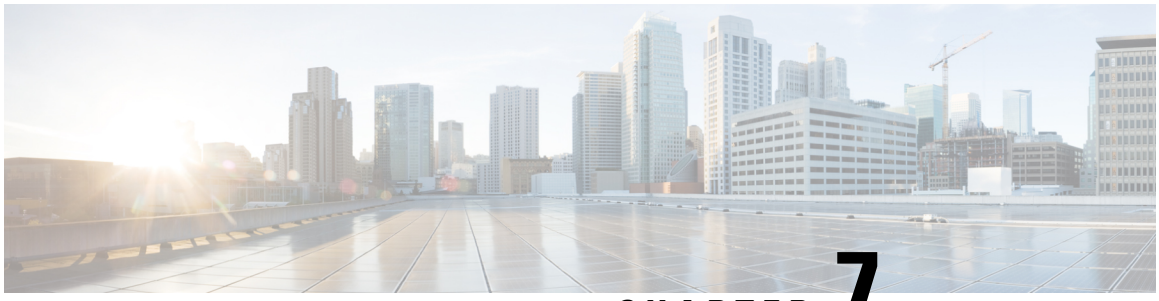
   If MAC address does not exist for the device, DUID will be written to the file `<dir_to_write_address>/eRouterDevicesDUID`.

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

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

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

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



CHAPTER 7

Next Steps

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

- Licensing Prime Cable Provisioning, on page 85
- Cisco Prime Network Registrar Configurations, on page 89
- Setting Up a Device Provisioning Engine, on page 91

Licensing Prime Cable Provisioning

To access this release, you must procure a new license of Prime Cable Provisioning 6.0.

Note You need to get the permanent or evaluation license of 6.0 to upgrade from 5.0/5.1/5.2/5.3/5.3.x to 6.x.

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 5.x, 6.x, 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.

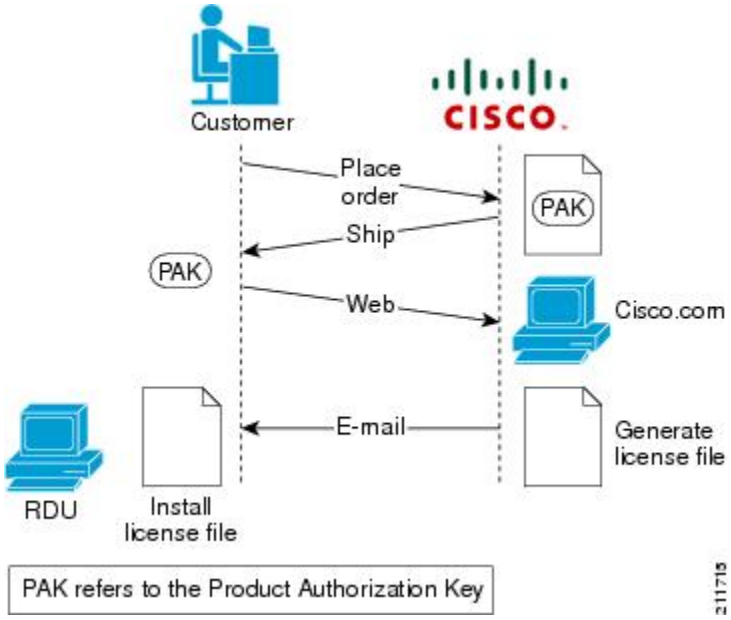
The DPE license is either included in a single license file along with the Service License or it is a separate license file by itself. The DPE is licensed only when you install this license file from the Admin UI.

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 15: 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 88.

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 88.

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 username and password.

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 90

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 85.

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:

```
# <BPR_HOME>/cli/bin/startCLI.sh
```

After you access the CLI, you must enter the DPE credentials to continue.

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.**

a. To change the login password:

1. Access the DPE in the privileged mode.
2. At the prompt, enter the **password** command.

   For example:

   ```
   bac_dpe# password
   ```

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

   For example:

   ```
   New password: <password1>
   Retype new password: <password1>
   Password changed successfully.
   ```

b. To change the privileged mode password:

1. Access the DPE in the privileged mode. You must have the PRIV_DPE_UPDATE privilege to run this command.
2. 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# BPR_HOME/agent/bin/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 92.

After the successful configuration of the DPE, the configured DPE must appear under the Servers page 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.pcnet.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: /pktcbl/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: /pktcbl/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).

Tip dpe.properties: to turn SNMPv3 cloning off, use /pktcbl/snmp/keyMaterial= ; to turn it on, use /pktcbl/snm
example, /pktcbl/snmp/keyMaterial=31:32:33:34:
35:36:37:38:39:30:31:32:33:34:35:36:37:38:39:30:31:32:33:34:35:36:37:38:39:30:31:32:33:34:35:36:37:38

For example:

```
bac_dpe# service packetcable 1 snmp key-material password4
% OK (Requires DPE restart "> dpe reload")
```

Step 6 Enter this command to enable the PacketCable voice technology.

```
bac_dpe# service packetcable 1 enable true
```

You can disable voice technology by entering **service packetcable 1 enable false**.

Tip dpe.properties: /pktcbl/enable=enabled

For example:

```
bac_dpe# service packetcable 1 enable true
% OK (Requires DPE restart "> dpe reload")
```

Step 7 Run the **dpe reload** command.

For example:

```
bac_dpe# dpe reload
Process [dpe] has been restarted.
```

Controls Available

The commands described in this section provide additional configuration settings.

- **service packetcable 1 registration encryption enable**—This command optionally enables encryption of the MTA configuration file.

Tip dpe.properties: /pktcbl/regsvr/configEncrypt=1

- **no service packetcable 1 registration encryption enable**—This command optionally disables encryption of the MTA configuration file.

Tip dpe.properties: /pktcbl/regsvr/configEncrypt=0

- **service packetcable 1 snmp timeout** *timeout*—This command dynamically sets the number of seconds that the DPE waits for a response to an SNMPv3 SET operation. The timeout is expressed in seconds and the default value is 10 seconds.

Tip dpe.properties: /pktcbl/snmp/timeout=1 and /pktcbl/snmp/timeout=10

INDEX

A

adding components 38
Admin UI 1
  login password 1
  login username 1
audience vii
available disk space 11
  data directory 11

B

bacckdc.license 89

C

checklist 11
  installing 11
commands 19, 36
  Prime Cable Provisioning:pkgask (noninteractive) 36
  UNIX 19
    tar 19
Common Steps 20
components:adding to install 38
configuration 33, 93, 95
  DPE 93, 95
    for data 93
    for voice technology (PacketCable) 95
  Network Registrar extensions 33
    validating 33
Configuring 34
  CPNR-EP Properties File 34
Crypto libraries 34

D

data directory 11
database logs directory 11
DHCP 89
  configuring for Network Registrar 89
  reload 89
directories 11
  data 11
  database logs 11
directories *(continued)*
  default location 11
    database logs 11
    home 11
    Network Registrar extensions 11
  disk space 11
    data 11
    home 11
  home 11
DNS 89
  enabling a spoofing server 89
  reload 89
DPE 91–93, 95, 97
  about 91
  configuring 93, 95, 97
    for data 93
    for voice technology 95
  dpe.properties file 95
  dpe.properties file:/pktcbl/enable 95
  dpe.properties file:/pktcbl/regsvr/configEncrypt=0 97
  dpe.properties file:/pktcbl/regsvr/configEncrypt=1 97
  dpe.properties file:/pktcbl/regsvr/KDCServiceKey 95
  dpe.properties file:/pktcbl/regsvr/policyPrivacy 95
  dpe.properties file:/pktcbl/snmp/keyMaterial 95
  dpe.properties file:/pktcbl/snmp/timeout=1 97
  dpe.properties file:/pktcbl/snmp/timeout=10 97
  dpe.properties file:/server/provFQDNs 95
  logging in 92
DPE Cache 77, 79
  backup tool 77, 79

G

generate 36
  response file 36

H

home directory 11

I

installation 10–11
  checklist 11

installation *(continued)*
directories 11
data 11
database logs 11
home 11
requirements 10
Network Registrar 10
Installation 7, 16
Requirements 7
worksheet 16
installation checklist 11
installing 16, 21, 24, 27, 29, 34, 36
components 34
components interactive 21, 24, 27
PWS 24
RDU 21
REST PWS 27
components, interactive 27, 29
DPE 27
Network Registrar extensions 29
components, noninteractive 36
initial steps 16
pkgask install 36
components (noninteractive) 36
pkgask install (noninteractive) 36
Installing 19
initial steps 19
interactive 34
KDC 34
interactive installation 19, 24, 27, 29, 34
components 24, 27, 29, 34
DPE 27
Network Registrar extensions 29
PWS 24
REST PWS 27
initial steps 19
KDC 34
interactive installation components 21
RDU 21

K

KDC 34, 85
FQDN 34
interactive installation 34
interface address 34
Kerberos realm 34
KeyGen tool 34
license 85
service key 34
on DPE 34
on KDC 34

L

large file support 9
linux 9
license file 1, 11
licensing 85, 88–89
DPE 85
about 85
installing license 85
KDC 85, 89
about 85
bacckdc.license 89
installing license 89
license file 85, 88
about 85
installing 88
listening port 11
about 11
default number 11
logical volume blocks 42
logical volume group 42

M

migrateDb.sh tool 73
arguments 73
using 73

N

Network Registrar 1, 10–11, 33, 38, 79, 90
about 1
clusters 1
local 1
regional 1
default location 11
installing extensions 1, 10, 33
requirements 10
tasks 1
validating 33
license key 1
nrcmd CLI 90
uninstalling 38
upgrading 79
Network Registrar:installing extensions:configuring 32
Network Registrar:reloading server 32
Network Registrar:web UI:login username 32
noninteractive installation 36–37
about 36
installing using response file 37
nrcmd CLI 90

O

obtain license 86

operating system 7
requirements 7
overview 1

P

PacketCable 95
configuring DPE 95
post-uninstallation task 39
product documentation vii
PWS 24
interactive installation 24

R

RDU 11, 21, 38, 73, 77
interactive installation 21
listening port 11
migrating database 73, 77
using migrateDb.sh tool 73
verifying integrity 77
RDU agent 38
shared secret 11
RDU Redundancy 42, 46, 50, 53, 55, 57, 59–60
configure HA mode 57
HA Setup 46
install_bac.sh 50
installation scripts 50
logical volume manager 42
miscellaneous requirements 42
post_install_bac_HA.sh 50
pre_install_bac_HA.sh 50
prerequisites 42
primary server 46
primary-only mode 53
recovery mode 59
redundancy requirements 42
secondary server 46
secondary-only mode 55
SSH keys 46
Two Node Failover Pair 50
uninstall 60
utility requirements 42
recovering 66
RDU database 66
requirements 7–8, 10
hardware 8
Network Registrar 10
requirements *(continued)*
patches 7
Requirements 9
Database 9
REST PWS 27
interactive installation 27

S

scope selection tag 90
shared secret 11
SSL libraries 34
Supports 63
64-bit servers 63
inline migration 63

T

Tomcat process 38
detecting 38
tool 73
migrateDb.sh 73

U

uninstall 38
uninstall_bac_HA.sh 60
uninstallation 38–39
post-uninstallation task 39
uninstalling 38
upgrade 69, 78, 80, 82
CPNR-EP 80
DPE 69, 78
KDC 82
Upgrade requirements 63
upgrading 66, 73, 77, 79
components 79
Network Registrar extensions 79
migrating RDU database 73, 77
using migrateDb.sh 73
verifying database integrity 77
RDU migration 66, 73

V

verify 66
database integrity 66