

Cisco RAN Management System Installation Guide, Release 5.1 MR

First Published: November 20, 2015

Last Modified: February 15, 2016

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

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

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

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

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

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

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

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

© 2015-2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface xiii

Document Revision History xiii

Objectives xiv

Audience xiv

Conventions xiv

Related Documentation xv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1

Installation Overview 1

Cisco RAN Management System Overview 1

Cisco RMS Deployment Modes 2

All-in-One RMS 3

Distributed RMS 3

Central RMS Node 4

Serving RMS Node 5

Upload RMS Node 5

Installation Flow 6

Installation Image 8

CHAPTER 2

Installation Prerequisites 11

Sample Network Sizes 11

Hardware and Software Requirements 11

Femtocell Access Point Requirement 12

Cisco RMS Hardware and Software Requirements 12

Cisco UCS C240 M3 Server 13

Cisco UCS 5108 Chassis Based Blade Server 13

Cisco UCS B200 M3 Blade Server 13

FAP Gateway Requirements 14
Virtualization Requirements 14
Optimum CPU and Memory Configurations 15
Data Storage for Cisco RMS VMs 15
Central VM 15
Serving VM 16
Upload VM 17
PMG Database VM 19
Device Configurations 19
Access Point Configuration 19
Supported Operating System Services 20
Cisco RMS Port Configuration 20
Cisco UCS Node Configuration 25
Central Node Port Bindings 25
Serving and Upload Node Port Bindings 25
All-in-One Node Port Bindings 26
Cisco ASR 5000 Gateway Configuration 26
NTP Configuration 27
Public Fully Qualified Domain Names 27
RMS System Backup 27

CHAPTER 3 **Installing VMware ESXi and vCenter for Cisco RMS 29**
Prerequisites 29
Configuring Cisco UCS US 240 M3 Server and RAID 30
Installing and Configuring VMware ESXI 5.5.0 31
Installing the VMware vCenter 5.5.0 32
Configuring vCenter 32
Configuring NTP on ESXi Hosts for RMS Servers 33
Installing the OVF Tool 34
Installing the OVF Tool for Red Hat Linux 34
Installing the OVF Tool for Microsoft Windows 35
Configuring SAN for Cisco RMS 36
Creating a SAN LUN 36
Installing FCoE Software Adapter Using VMware ESXi 36
Adding Data Stores to Virtual Machines 37

Adding Central VM Data Stores 37
Adding the DATA Datastore 38
Adding the TX_LOGS Datastore 41
Adding the BACKUP Datastore 45
Validating Central VM Datastore Addition 49
Adding Serving VM Data Stores 50
Adding the SYSTEM_SERVING Datastore 50
Adding Upload VM Data Stores 50
Adding the SYSTEM_UPLOAD Datastore 50
Adding PM_RAW and PM_ARCHIVE Datastores 51
Validating Upload VM Datastore Addition 53
Migrating the Data Stores 53
Initial Migration on One Disk 53

CHAPTER 4 RMS Installation Tasks 55
RMS Installation Procedure 55
Preparing the OVA Descriptor Files 56
Validation of OVA Files 60
Deploying the RMS Virtual Appliance 61
All-in-One RMS Deployment: Example 62
Distributed RMS Deployment: Example 63
RMS Redundant Deployment 66
Deploying an All-In-One Redundant Setup 66
All-In-One Redundant Deployment: Example 70
Migrating from a Non-Redundant All-In-One to a Redundant Setup 72
Deploying the Distributed Redundant Setup 73
Post RMS Redundant Deployment 76
Configuring Serving and Upload Nodes on Different Subnets 76
Configuring Fault Manager Server for Redundant Upload Node 79
Configuring Redundant Serving Nodes 80
Configuring Primary Serving Node or PNR Redundancy 81
Configuring Secondary Serving Node or PNR Redundancy 83
Verifying Secondary Serving Node or PNR Redundancy 85
Configuring the Security Gateway on the ASR 5000 for Redundancy 85

Configuring the Security Gateway on ASR 5000 for Multiple Subnet or Geo-Redundancy 87
Configuring the HNB Gateway for Redundancy 89
Configuring DNS for Redundancy 91
RMS High Availability Deployment 91
Optimizing the Virtual Machines 91
Upgrading the VM Hardware Version 92
Upgrading the VM CPU and Memory Settings 94
Upgrading the Data Storage on Root Partition for Cisco RMS VMs 94
Upgrading the Upload VM Data Sizing 98
RMS Installation Sanity Check 101
Sanity Check for the BAC UI 101
Sanity Check for the DCC UI 102
Verifying Application Processes 102

CHAPTER 5 **Installation Tasks Post-OVA Deployment** 105
HNB Gateway and DHCP Configuration 105
Adding Routes and IPtables for LTE FAP 109
Installing RMS Certificates 109
Auto-Generated CA-Signed RMS Certificates 109
Self-Signed RMS Certificates 112
Self-Signed RMS Certificates in Serving Node 113
Importing Certificates Into Cacerts File 116
Self-Signed RMS Certificates in Upload Node 117
Importing Certificates Into Upload Server Truststore file 120
Enabling Communication for VMs on Different Subnets 121
Configuring Default Routes for Direct TLS Termination at the RMS 122
Post-Installation Configuration of BAC Provisioning Properties 124
PMG Database Installation and Configuration 125
PMG Database Installation Prerequisites 125
PMG Database Installation 126
Schema Creation 126
Map Catalog Creation 128
Load MapInfo Data 129
Grant Access to MapInfo Tables 130

Configuring the Central Node 130
Configuring the PMG Database on the Central Node 130
Area Table Data Population 133
Configuring New Groups and Pools 135
Configuring SNMP Trap Servers with Third-Party NMS 136
Configuring FM, PMG, LUS, and RDU Alarms on Central Node for Third-Party NMS 137
Configuring DPE, CAR, CNR, and AP Alarms on Serving Node for Third-Party NMS 138
Integrating FM, PMG, LUS, and RDU Alarms on Central Node with Prime Central NMS 140
Integrating RMS with Active Prime Central NMS 141
Integrating RMS with Active and DRS on Prime Central NMS 143
Integrating RMS with Two Third-Party Trap Receivers 146
Integrating BAC, PAR, and PNR on Serving Node with Prime Central NMS 147
Integrating Serving Node with Prime Central Active Server 147
Integrating Serving Node with Active and DRS on Prime Central NMS 149
Integrating Serving Node with Two Third-Party Trap Receivers 154
De-Registering RMS with Prime Central Post-Deployment 157
Disabling SNMP Traps Notification to Prime Central NMS Interface 157
Cleaning Up Files On Central Node 158
Cleaning Up Files On Serving Node 158
De-Registering RMS Data Manager from Prime Central 159
Starting Database and Configuration Backups on Central VM 159
Optional Features 160
Default Reserved Mode Setting for Enterprise APs 160
configure_ReservedMode.sh 160
Configuring Linux Administrative Users 161
NTP Servers Configuration 163
Central Node Configuration 163
Serving Node Configuration 164
Upload Node Configuration 164
LDAP Configuration 165
TACACS Configuration 167
Configuring Geographical Identifier SAC 168
Configuring Third-Party Security Gateways on RMS 168
HNB Gateway Configuration for Third-Party SeGW Support 169

CHAPTER 6 Verifying RMS Deployment 171

Verifying Network Connectivity 171

Verifying Network Listeners 172

Log Verification 173

Server Log Verification 173

Application Log Verification 173

Viewing Audited Log Files 174

End-to-End Testing 175

Updating VMware Repository 175

CHAPTER 7 RMS Upgrade 177

Upgrade Flow 177

Pre-Upgrade 179

Pre-Upgrade Tasks for RMS 5.1 MR 179

Pre-Upgrade Tasks for RMS 5.1 MR Hotfix 184

Upgrade 187

Upgrade Prerequisites for RMS 5.1 MR 187

Red Hat Enterprise Linux Upgrade 188

Upgrade Prerequisites for RMS 5.1 MR Hotfix 189

Upgrade from RMS 4.1 to RMS 5.1 MR 189

Upgrading Central Node from RMS 4.1 to RMS 5.1 MR 189

Upgrading Serving Node from RMS 4.1 to RMS 5.1 MR 191

Upgrading Upload Node from RMS 4.1 to RMS 5.1 MR 195

Post RMS 4.1 to RMS 5.1 MR Upgrade Configurations 196

Upgrading from RMS 5.1 to RMS 5.1 MR 199

Upgrading Central Node from RMS 5.1 to RMS 5.1 MR 200

Upgrading Serving Node from RMS 5.1 to RMS 5.1 MR 201

Upgrading Upload Node from RMS 5.1 to RMS 5.1 MR 203

Post RMS 5.1 to RMS 5.1 MR Upgrade Configurations 203

Upgrading from RMS 5.1 MR to RMS 5.1 MR Hotfix 205

Upgrading Central Node from RMS 5.1 MR to RMS 5.1 MR Hotfix 205

Upgrading Serving Node from RMS 5.1 MR to RMS 5.1 MR Hotfix 208

Upgrading Upload Node from RMS 5.1 MR to RMS 5.1 MR Hotfix 210

Post RMS 5.1 MR to RMS 5.1 MR Hotfix Upgrade Configurations 211

Upgrading AP Firmware From Cloud Base 211
Upgrading AP Firmware From RMS 212
Uploading Firmware Files to RMS 212
Initiating Firmware Upgrade on Individual or Bulk FAPs 213
Initiating Firmware Upgrade on Individual FAPs 213
Initiating Firmware Upgrade on Bulk FAPs 215
Disabling Firmware Upgrade on Individual or Bulk FAPs 215
Disabling Firmware Upgrade on Individual FAPs 216
Disabling Firmware Upgrade on Bulk FAPs 217
Upgrading AP Firmware Post RMS 5.1 MR Hotfix Installation 217
Uploading Firmware Files Post RMS 5.1 MR Hotfix Installation 217
Enabling Firmware Upgrade Properties 218
Initiating Firmware Upgrade on Bulk LTE FAPs 219
Verifying Firmware Upgrade on LTE FAPs 220
Disabling Firmware Upgrade on Bulk LTE FAPs 222
Additional Information 222
Post-Upgrade 223
Post RMS 5.1 MR Upgrade Tasks 223
Post RMS 5.1 MR Hotfix Upgrade Task 223
Mapping RMS 4.1 XML Files to RMS 5.1 or 5.1 MR XML Files 223
Merge RMS 4.1 MR XML Files Manually 224
Mapping RMS 5.1 MR XML Files to RMS 5.1 MR Hotfix XML Files 225
Merging RMS 5.1 MR XML Files Manually 225
Record BAC Configuration Template File Details 226
Associate Manually Edited BAC Configuration Template 226
Rollback to RMS, Release 4.1 227
Rollback to RMS, Release 5.1 or 5.1 MR 227
Remove Obsolete Data 228
Basic Sanity Check Post RMS Upgrade 229
Stopping Cron Jobs 230
Starting Cron Jobs 230
Disabling RMS Northbound and Southbound Traffic 231
Enabling RMS Northbound and Southbound Traffic 231

CHAPTER 8 **Troubleshooting** 233

Regeneration of Certificates 233
Certificate Regeneration for DPE 233
Certificate Regeneration for Upload Server 235
Deployment Troubleshooting 238
CAR/PAR Server Not Functioning 238
Unable to Access BAC and DCC UI 239
DCC UI Shows Blank Page After Login 240
DHCP Server Not Functioning 240
DPE Processes are Not Running 242
Connection to Remote Object Unsuccessful 243
VLAN Not Found 244
Unable to Get Live Data in DCC UI 244
Installation Warnings about Removed Parameters 244
Upload Server is Not Up 245
OVA Installation failures 250
250
Update failures in group type, Site - DCC UI throws an error 250
Kernel Panic While Upgrading to RMS, Release 5.1 250
Network Unreachable on Cloning RMS VM 251
Unable to Stop UMT Jobs 252

APPENDIX A **OVA Descriptor File Properties** 255
RMS Network Architecture 255
Virtual Host Network Parameters 256
Virtual Host IP Address Parameters 258
Virtual Machine Parameters 262
HNB Gateway Parameters 263
Auto-Configuration Server Parameters 265
OSS Parameters 265
Administrative User Parameters 268
BAC Parameters 269
Certificate Parameters 270
Deployment Mode Parameters 271
License Parameters 271
Password Parameters 272

Serving Node GUI Parameters 273
DPE CLI Parameters 274
Time Zone Parameter 274

APPENDIX B Examples of OVA Descriptor Files 277
Example of Descriptor File for All-in-One Deployment 277
Example Descriptor File for Distributed Central Node 279
Example Descriptor File for Distributed Serving Node 280
Example Descriptor File for Distributed Upload Node 282
Example Descriptor File for Redundant Serving/Upload Node 283

APPENDIX C Backing Up RMS 285
Full System Backup 285
Back Up System Using VM Snapshot 286
Using VM Snapshot 287
Back Up System Using vApp Cloning 287
Application Data Backup 288
Backup on the Central Node 288
Backup on the Serving Node 291
Backup on the Upload Node 292

APPENDIX D RMS System Rollback 295
Full System Restore 295
Restore from VM Snapshot 295
Restore from vApp Clone 296
Application Data Restore 296
Restore from Central Node 296
296
Restore from Serving Node 299
Restore from Upload Node 302
End-to-End Testing 304

APPENDIX E Glossary 305



Preface

This section describes the objectives, audience, organization, and conventions of the Cisco RAN Management System (RMS) Installation Guide.

- Document Revision History, page xiii
- Objectives, page xiv
- Audience, page xiv
- Conventions, page xiv
- Related Documentation, page xv
- Obtaining Documentation and Submitting a Service Request, page xv

Document Revision History

The Document Revision History table below records technical changes to this guide. The table shows the document revision number for the change, the date of the change, and a brief summary of the change.

Document Number	Date	Change Summary
OL-32397-01	June 23, 2014	Initial version of the document.
	July 8, 2014	Added the following sections: • RMS High Availability Deployment, on page 91 • Configuring SAN for Cisco RMS, on page 36
	February 9, 2015	Fixes to remove non-supported hardware
	February 15, 2016	Updated the "RMS Upgrade" chapter with Release 5.1 MR Hotfix specific updates.

Objectives

This guide provides an overview of the Cisco RAN Management System (RMS) solution and the pre-installation, installation, post-installation, and troubleshooting information for the Cisco RMS installation.

Audience

The primary audience for this guide includes network operations personnel and system administrators. This guide assumes that you are familiar with the following products and topics:

- Basic internetworking terminology and concepts
- Network topology and protocols
- Microsoft Windows 2000, Windows XP, Windows Vista, and Windows 7
- Linux administration
- Red Hat Enterprise Linux Edition, v6.6
- VMware vSphere Standard Edition v5.5

Conventions

This document uses the following conventions:

Convention	Description
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.

Convention	Description
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation

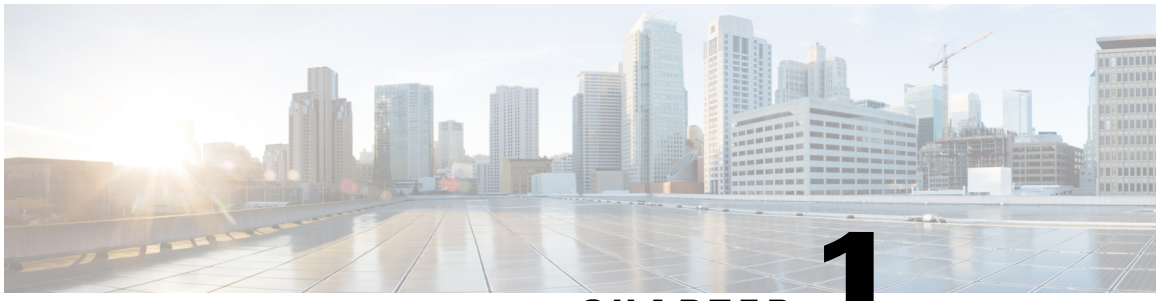
For additional information about the Cisco RAN Management Systems, refer to the following documents:

- *Cisco RAN Management System Administration Guide*
- *Cisco RAN Management System API Guide*
- *Cisco RAN Management System SNMP/MIB Guide*
- *Cisco RAN Management System Release Notes*

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 provides a brief overview of the Cisco RAN Management System (RMS) and explains how to install, configure, upgrade, and troubleshoot RMS installation.

The following sections provide an overview of the Cisco RAN Management System installation process:

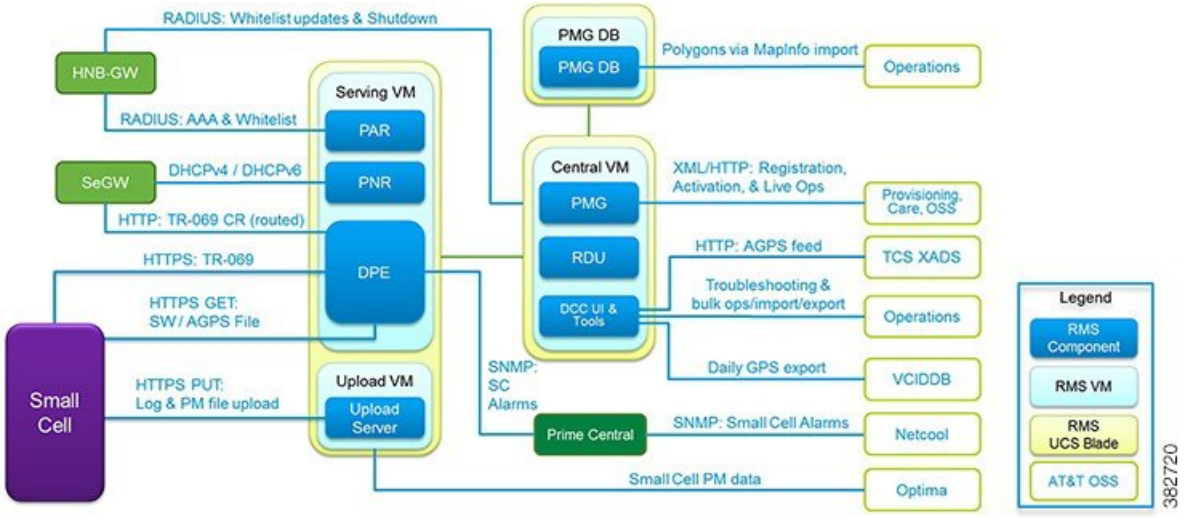
- Cisco RAN Management System Overview, page 1
- Installation Flow, page 6
- Installation Image, page 8

Cisco RAN Management System Overview

The Cisco RAN Management System (RMS) is a standards-based provisioning and management system for HeNB (4G femtocell access point [FAP]). It is designed to provide and support all the operations required to transmit high quality voice and data from Service Provider (SP) mobility users through the SP mobility core. The RMS solution can be implemented through SP-friendly deployment modes that can lower operational costs of femtocell deployments by automating all key activation and management tasks.

The following RMS solution architecture figure illustrates the various servers and their internal and external interfaces for Cisco RMS.

Figure 1: RMS Solution Architecture



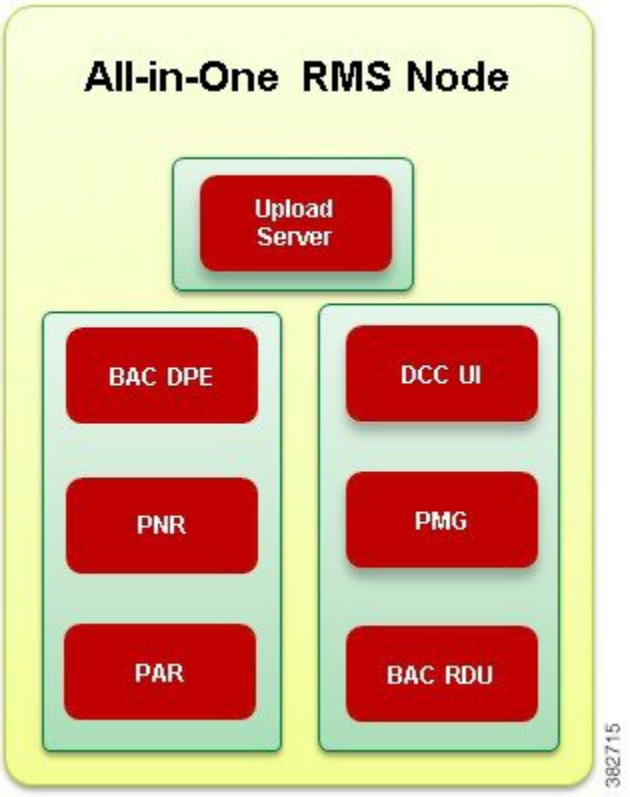
Cisco RMS Deployment Modes

The Cisco RMS solution can be deployed in one of the two RMS deployment modes:

All-in-One RMS

In the All-in-One RMS deployment mode, the Cisco RMS solution is provided on a single host. It supports up to 50,000 FAPs.

Figure 2: All-in-One RMS Node



In an All-In-One RMS node, the Serving Node comprises of the VM combining the BAC DPE, PNR, and PAR components; the Central Node comprises of the VM combining the DCC UI, PMG, and BAC RDU VM components, and the Upload VM comprises of the Upload Server component.

To deploy the All-in-One node, it is mandatory to procure and install VMware with one VMware vCenter per deployment. For more information, see Installing VMware ESXi and vCenter for Cisco RMS, on page 29.

Distributed RMS

In a Distributed RMS deployment mode, the following nodes are deployed:

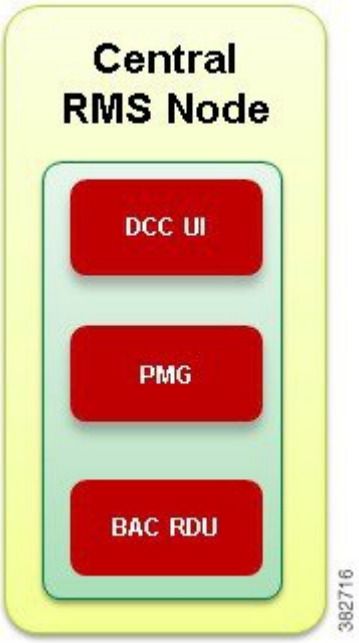
- Central RMS Node, on page 4
- Serving RMS Node, on page 5
- Upload RMS Node, on page 5

In a Distributed deployment mode, up to 2,50,000 APs are supported.

Central RMS Node

On a Central RMS node, the Cisco RMS solution is provided on a separate node. It provides the active-active geographical redundancy option. The Central node can be paired with any number of Serving nodes.

Figure 3: Central RMS Node



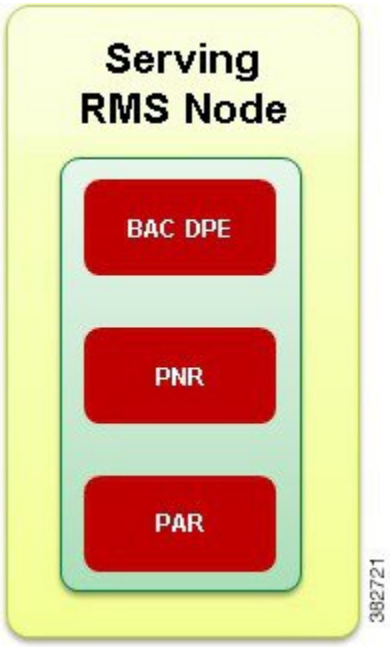
In any of the Cisco RMS deployments, it is mandatory to have at least one Central node.

To deploy the Central node, it is mandatory to procure and install VMware with one VMware vCenter per deployment. For more information, see Installing VMware ESXi and vCenter for Cisco RMS, on page 29

Serving RMS Node

On a Serving RMS node, the Cisco RMS solution is provided on a separate node or host. It supports up to 125,000 FAPs and provides the geographical redundancy with the active-active pair option. The Serving node must be combined with the Central node.

Figure 4: Serving RMS Node



To deploy the Serving node, it is mandatory to procure and install VMware.

In case of serving node deployment failover, the additional Serving nodes can be configured with the same Central Node. To know more about the redundancy deployment option, see RMS Redundant Deployment, on page 66.

Note The RMS node deployments are supported on UCS hardware and use virtual machines (VMs) for performance and security isolation.

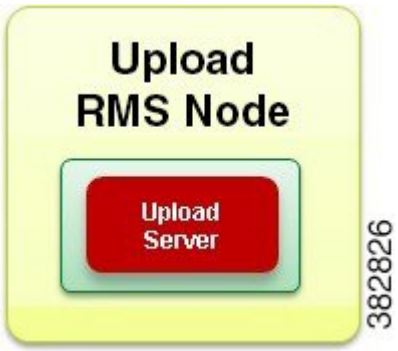
To know how to procure and install VMware on the UCS hardware node, see Installing VMware ESXi and vCenter for Cisco RMS, on page 29

Upload RMS Node

In the Upload RMS node, the Upload Sever is provided on a separate node.

The Upload RMS node must be combined with the Serving node.

Figure 5: Upload RMS Node



Installation Flow

The following table provides the general flow in which to complete the Cisco RAN Management System installation. The table is only a general guideline. Your installation sequence might vary, depending on your specific network requirements.

Before you install Cisco RAN Management System, you need to determine and plan the following:

Step No.	Task	Action	Task Completion: Mandatory or Optional
1	Install Cisco RAN Management System for the first time.	Go to Step 3.	Mandatory
2	Upgrade Cisco RAN Management System from an earlier to the latest release.	Go to Step 11.	Optional
3	Do the following: • Plan on how Cisco RAN Management System installation will fit in your existing network. • Determine the number of femtocell access points (FAPs) that your network should support. • Finalize the RMS deployment based on the network size and APs needed	Ensure that you follow the prerequisites listed in Installation Prerequisites. Then proceed to Step 4.	Mandatory

Step No.	Task	Action	Task Completion: Mandatory or Optional
4	Procure and install the recommended hardware and software that is required for the RMS deployment mode.	Ensure that all the hardware and software listed in Cisco RMS Hardware and Software Requirements, on page 12 are procured and connected. Then proceed to Step 5.	Mandatory
5	Ensure all virtualization requirements for your installation are met.	Follow the recommended virtualization requirements listed in the Virtualization Requirements, on page 14. Then proceed to Step 6.	Mandatory
6	Complete all device configurations.	Complete the device configurations recommended in Device Configurations, on page 19 and proceed to Step 7.	Mandatory
7	Create the configuration file (deployment descriptor).	Prepare and create the Open Virtualization Format (OVF) file as described in Preparing the OVA Descriptor Files, on page 56.	Mandatory
8	Install Cisco RAN Management System.	Complete the appropriate procedures in RMS Installation Tasks, on page 55 and proceed to Step 9.	Mandatory
9	Complete the post-installation activities.	Complete the appropriate procedures in cross-reference in Installation Tasks Post-OVA Deployment, on page 105 and proceed to Step 10.	Mandatory
10	Start using Cisco RAN Management System.	See the *Cisco RAN Management System Administration Guide*.	—

Step No.	Task	Action	Task Completion: Mandatory or Optional
11	Upgrade to the latest Cisco RAN Management System release.	Complete the appropriate procedures in RMS Upgrade, on page 177.	Mandatory
12	Access troubleshooting information for Cisco RAN Management System installation.	Go to Troubleshooting, on page 233 to troubleshoot RMS installation issues.	Optional

Installation Image

The Cisco RAN Management System is packaged in Virtual Machine (VM) images (tar.gz format) that are deployed on the hardware nodes. The deployments supported are.

- Small Scale: Single AP per site
- Large Scale: Distributed with multiple APs per site

For more information about the deployment modes, see Cisco RMS Deployment Modes, on page 2.

To access the image files (OVA), log in to https://software.cisco.com and navigate to **Support > Downloads** to open the Download Software page. Then, navigate to **Products/Wireless/Mobile Internet/Universal Small Cells/Universal Small Cell RAN Management System** to open the page where you can download the required image files.

The available OVA files are listed in the *Release Notes for Cisco RAN Management System* for your specific release.

The RMS image contains the following major components:

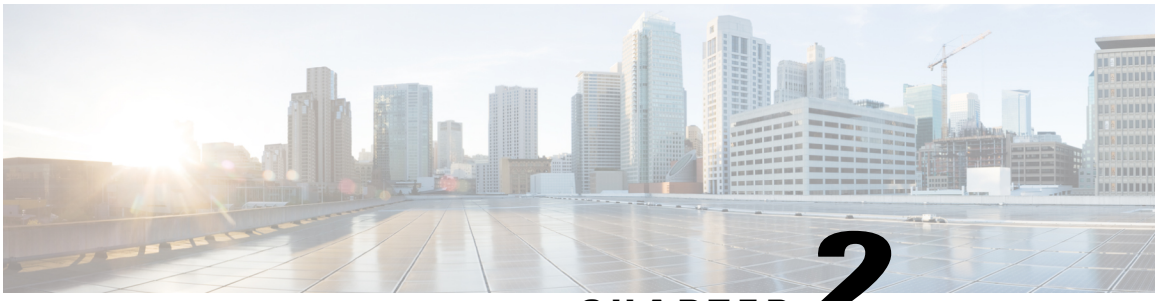
- Provisioning and Management Gateway (PMG) database (DB)
- PMG
- Operational Tools
- Log Upload
- Device Command and Control (DCC) UI
- Broadband Access Center (BAC) Configuration
- BAC
- Prime Network Registrar (PNR)
- Prime Access Registrar (PAR)

For information about the checksum value of the OVA files and the version of major components, see the *Release Notes for Cisco RAN Management System* for your specific release.

After downloading the RMS image files, use these commands to verify the output against the checksums provided in the release notes or checksum files provided in the release folder:

```
$ sha512sum <file-name>
```

```
$ md5sum <file-name>
```



CHAPTER 2

Installation Prerequisites

This chapter provides the network size, hardware and software, and device configuration requirements that must be met before installing the Cisco RAN Management System (RMS).

Note Ensure that all the requirements in the following sections are addressed.

- Sample Network Sizes, page 11
- Hardware and Software Requirements, page 11
- Device Configurations, page 19
- RMS System Backup, page 27

Sample Network Sizes

While planning the network size, you must consider the following:

- Number of femtocell access points (FAPs or APs, used interchangeably in this guide) in your network
- Current network capacity and additional capacity to meet future needs.

For more information about the recommended deployment modes, see Cisco RMS Deployment Modes, on page 2.

Hardware and Software Requirements

These topics describe the FAPs, RMS hardware and software, gateway, and virtualization requirements:

Note Consult with your Cisco account representative for specific hardware and configuration details for your APs, RMS, and gateway units.

Hardware requirements assume that Cisco RMS does not share the hardware with additional applications. (This is the recommended installation.)

Femtocell Access Point Requirement

Cisco RMS supports the FAPs listed in the following table:

Hardware	Band	Power	GPS	Residential/ Enterprise	Access Mode
USC 3330	2 and 5	20 mW	Yes	Residential	Closed
USC 3331	1	20 mW	No	Residential	Closed
USC 3331	2 and 5	20 mW	No	Residential	Closed
USC 5330	1	100 mW	No	Enterprise	Open
USC 5330	2 and 5	100 mW	No	Enterprise	Open
USC 6732 (UMTS)	2 and 5	125 mW	Yes	Enterprise	Open
USC 6732 (LTE)	4, 2, 30, and 5	250 mW	Yes	Enterprise	Open
USC 7330	1	250 mW	No	Enterprise	Open
USC 7330	2 and 5	250 mW	Yes	Enterprise	Open
USC 9330	1	1 W	No	Enterprise	Open
USC 9330	2 and 5	1 W	Yes	Enterprise	Open

For information about the AP configuration, see Access Point Configuration, on page 19.

Cisco RMS Hardware and Software Requirements

Cisco UCS x86 hardware is used for Cisco RAN Management System hardware nodes.

The table below establishes the supported server models that are recommended for the RMS solution.

Supported UCS Hardware	Target RMS Nodes
• Cisco UCS C240 M3 Rack Server • Cisco UCS 5108 Chassis Based Blade Server	All RMS nodes

Cisco UCS C240 M3 Server

The following hardware configuration is used for all RMS nodes:

- Cisco Unified Computing System (UCS) C240 M3 Rack Server
- Rack-mount
- 2 x 2.3 Ghz x 6 Core x86 architecture
- 128 GB RAM
- 12 disks: 4 x 15,000 RPM 300 GB, 8 x 10,000 RPM 300 GB
- RAID array with battery backup and 1 GB cache
- 4 + 1 built-in Ethernet ports
- 2 rack unit (RU)
- Redundant AC power
- Red Hat Enterprise Linux Edition, v6.6
- VMware vSphere Standard Edition v5.5
- VMware vCenter Standard Edition v5.5

Cisco UCS 5108 Chassis Based Blade Server

The following hardware configuration is used for all RMS nodes:

- Cisco UCS 5108 Chassis
- Rack-mount
- 6 rack unit (RU)
- Redundant AC power
- Red Hat Enterprise Linux Edition, v6.6
- VMware vSphere Standard Edition v5.5
- VMware vCenter Standard Edition v5.5
- SAN storage with sufficient disks (see, Data Storage for Cisco RMS VMs, on page 15)

Note The Cisco UCS 5108 Chassis can house up to eight Cisco UCS B200 M3 Blade Servers.

Cisco UCS B200 M3 Blade Server

- Cisco UCS B200 M3 Blade Server
- Rack-mount

- 2 CPUs using 32 GB DIMMs
- 128 GB RAM

Note Ensure that the selected UCS server is physically connected and configured with the appropriate software before proceeding with the Cisco RMS installation.

To install the UCS servers, see the following guides:

- Cisco UCS C240 M3 Server Installation and Service Guide
- Cisco UCS 5108 Server Chassis Installation Guide
- Cisco UCS B200 Blade Server Installation and Service Note

Note The Cisco UCS servers must be pre-configured with standard user account privileges.

FAP Gateway Requirements

The Cisco ASR 5000 Small Cell Gateway serves as the HNB Gateway (HNB-GW) and Security Gateway (SeGW) for the FAP in the Cisco RAN Management System solution.

It is recommended that the hardware node with the Serving VM is co-located with the Cisco ASR 5000 Gateway. The Cisco ASR 5000 Gateway utilizes the Serving VM for DHCP and AAA services. This gateway provides unprecedented scale that can exceed 2,50,000 APs that can be handled by a Serving VM (or redundant pair).

Ensure that the Cisco ASR 5000 Gateway is able to communicate with the Cisco UCS server (on which RMS will be installed) before proceeding with the Cisco RMS installation.

To install the Cisco ASR 5000 Small Cell Gateway, see the Cisco ASR 5000 Installation Guide.

Virtualization Requirements

The Cisco RAN Management System solution that is packaged in Virtual Machine (VM) images (.ova file) requires to be deployed on the Cisco UCS hardware nodes, defined in the Cisco RMS Hardware and Software Requirements, on page 12.

The virtualization framework of the VM enables the resources of a computer to be divided into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and so on.

The benefit of using VMs is load isolation, security isolation, and administration.

- Load isolation ensures that a single service does not take over all the hardware resources and compromise other services.
- Security isolation enables flows between VMs to be routed via a firewall, if desired.
- Administration is simplified by centralizing the VM deployment, and monitoring and allocating the hardware HW resources among the VMs.

Before you deploy the Cisco RAN Management System .ova file:

- Ensure that you install:
  - VMware vSphere Standard Edition v5.5
  - VMware vCenter Standard Edition v5.5

For the procedure to install VMware, see Installing VMware ESXi and vCenter for Cisco RMS, on page 29.

Optimum CPU and Memory Configurations

Following are the optimal values of CPU and memory required for each VM of the All -In-One setup to support from 50,000 and Distributed RMS setup to support from 2,50,000 devices.

Node	vCPU	Memory
All -In-One Setup		
Central Node	8	16 GB
Serving Node		
Upload Node		64 GB
Distributed Setup		
Central Node	16	16 GB
Serving Node	8	
Upload Node	16	64 GB

Data Storage for Cisco RMS VMs

Before installing the VMware, consider the data storage or disk sizing for each of the Cisco RMS VMs.

- Central VM, on page 15
- Serving VM, on page 16
- Upload VM, on page 17

Central VM

The disk-sizing of the Central VM is based on the calculation logic and size for SAN disk space for each RAID set:

LUN Name	Purpose	RAID Set	Min Size	Calculation Logic
DATA	Database	#1	200 GB	In lab tests file size for database is 1 GB for 10,000 devices and 3000 groups, static neighbors if fully populated for each AP, will require an additional database size of around 1.4 GB per 10,000 devices. Considering future expansion plans for 2 million devices and 30% for fragmentation, around 73 GB of disk space will be required; 200GB is the recommended value.
TXN_LOG	Database transaction logs	#2	200 GB	25 MB is seen with residential, but with Metrocell, transaction logs will be very high because of Q-SON. It does not depend on AP deployment population size. 200 GB is recommended.
SYSTEM	OS and application image and application logs	#3	200 GB	Linux and applications need around 16 GB and application logs need 50 GB; Recommended value 200GB considering Ops tools generated logs and reports. It is independent of AP deployment size.
BACKUP	Database backups	#4	250 GB	To maintain minimum four backups for upgrade considerations. 56 GB is the size of the database files for 2 million devices, so minimum required will be approximately 250 GB. For 10,000 devices, approximately 5 GB will be required to maintain four backups. If number of backups needed are more, calculate disk size accordingly.

Serving VM

The disk-sizing of the Serving VM is based on the calculation logic and size for SAN disk space for each RAID set:

LUN Name	Purpose	RAID Set	Min Size	Calculation Logic
SYSTEM	OS and application image and application logs	#1	300 GB	Linux and applications need approximately 16 GB; logs need 10 GB; for backups, swap space and to allow for additional copies for upgrades, 200 GB. It is independent of AP deployment size. 50 GB for PAR and 150 GB for PNR.

Upload VM

The disk-sizing of the Upload VM is based on the following factors:

Sl. No.	Upload VM	Disk Size
1	Approximate size of performance monitoring (PM) statistics file in each log upload	100 KB for Enterprise FAP and 7.5 MB for Residential FAP
2	Number of FAPs per ULS	2,50,000 (50,000 Enterprise + 2,00,000 Residential)
3	Frequency of PM uploads	Once in 15 minutes (4 x 24 = 96 per day) for Enterprise FAPs Once in a day for Residential FAPs

The following disk-sizing of the Upoad VM is based on the calculation logic and size for SAN disk space for each RAID set:

LUN Name	Purpose	RAID Set	Min Size	Calculation Logic
PM_RAW	For storing RAW files	#1	350 GB	Calculation is for 2,50,000 APs with the following assumptions: • For Enterprise 3G FAP PM, size of uploaded file at 15 min sampling frequency and 15 min upload interval is 100 KB • For Residential 3G FAP PM, size of uploaded file at 1 hour sampling frequency and 1 day upload interval is 7.5 MB • ULS has at the most last 2 hours files in raw format. **For a single mode AP:** Disk space required for PM files = (50000*4*2*100)/(1024/1024) + (200000*2*7.5)/(1024*24) = 39 + 122 = 161 GB Additional space for storage of other files like on-demand = 200 GB
PM_ARCHIVE	For storing ARCHIVED files	#2	1000 GB	Considering the compression ratio is down to 15% of total size and ULS starts purging after 60% of disk filled, disk space required by compressed files uploaded in 1 hr = (50000*4*2*100)/(1024/1024) + (200000*2*7.5)/(1024*24))*0.15 = 25 GB To store 24 hrs data, space required = 25*24 = 600 GB = 60% of total disk space Therefore, total disk space for PM files = 1000 GB

LUN Name	Purpose	RAID Set	Min Size	Calculation Logic
SYSTEM	OS and application image and application logs	#3	200 GB	Linux and applications need around 16 GB and logs need 10 GB; for backups, swap space and to allow for additional copies for upgrades, 200 GB. It is independent of AP deployment size.

PMG Database VM

LUN Name	Purpose	RAID Set	Min Size	Calculation Logic
SYSTEM	OS and application image and application logs	#1	50 GB	Linux and Oracle applications need around 25 GB. Considering backups and swap space 50 GB is recommended. It is independent of AP deployment size.

Device Configurations

Before proceeding with the Cisco RAN Management System installation, it is mandatory to complete the following device configurations to enable the various components to communicate with each other and with the Cisco RMS system.

Access Point Configuration

It is mandatory for all small cell access points to have the minimal configuration to contact Cisco RMS within the service provider environment. This enables Cisco RMS to automatically install or upgrade the AP firmware and configure the AP as required for service.

USC 3000, 5000 and 7000 series access points initially connect to the public Ubiquisys cloud service, which configures the enablement data on the AP and then directs them to the service provider Hosted & Managed Services (HMS).

The minimum initial AP configuration includes the following:

- 1 to 3 Network Time Protocol (NTP) server IP addresses or fully qualified domain names (FQDNs). This must be a factory default because the AP has to obtain time in order to perform certificate expiration verification during authentication with servers. HMS will reconfigure the appropriate list of NTP servers on bootstrap.
- Unique AP private key and certificate signed by appropriate Certificate Authority (CA)
- Trust Store configured with public certificate chains of the CA which signs server certificates.

After each Factory recovery, the AP contacts the Ubiquisys cloud service and downloads the following four minimum parameters:

1. RMS public key (certificates)
2. RMS ACS URL
3. Public NTP servers
4. AP software

With these four parameters, the AP validates the RMS certificate, loads the AP software from cloud server, and talks to RMS.

Supported Operating System Services

Only following UNIX services are supported on Cisco RMS. The installer disables all other services.

Node Type	List of Services
RMS Central node	SSH,, HTTPS, NTP, SNMP, SAN, RSYSLOG
RMS Serving node	SSH, HTTPS, NTP, SNMP, SAN, RSYSLOG
RMS Upload Server node	SSH, HTTPS, NTP, SNMP, SAN, RSYSLOG

Cisco RMS Port Configuration

The following table lists the different ports used on the Cisco RMS nodes.

Node Type	Port	Source	Protocol	Usage	

All Server	22	Administrator	SSH	Remote log-in(SSH)
	161	NMS	UDP (SNMP)	SNMP agent used to support get/set
	162	NMS	UDP (SNMP)	SNMP agent to support trap
	123	NTP Server	UDP	NTP for time synchronization
	514	Syslog	UDP	Syslog - used for system logging
	5488	Administrator	TCP	VMware VAMI (Virtual Appliance Management Infrastructure) services
	5489	Administrator	TCP	VMware VAMI (Virtual Appliance Management Infrastructure) services

RMS Central node	8083	OSS	TCP (HTTP)	OSS<->PMG communication
	8084	RDU	TCP	RDU Fault Manager server communication
	443	UI	TCP (HTTPs)	DCC UI
	49187	DPE	TCP	Internal RMS communication - Request coming from DPE
	8090	Administrator	TCP (HTTP)	DHCP administration
	5439	Administrator	TCP	Postgres database port
	1244	RDU/PNR	TCP	DHCP internal communication
	8009	Administrator	TCP	Tomcat AJP connector port
	9006	Administrator	TCP	BAC Tomcat server port
	8015	Administrator	TCP	PNR Tomcat server port
	3799	ASR5K (AAA)	UDP (RADIUS)	RADIUS Change-of-Authorization and Disconnect flows from PMG to ASR5K (Default Port)
	8001	RDU	UDP (SNMP)	SNMP Internal
	49887	RDU	TCP	Listening port (for watchdog) for RDU SNMP Agent
	4698	PMG	TCP	Default listening port for Alarm handler to listen PMG events
	Random	RDU/PNR/Postgres/PMG	TCP/UDP	

				Random ports used by internal processes: java, postmaster, ccmsrv, cnrservagt, ruby, RPCBind, and NFS(Network File system)
RMS Serving node	443	HNB	TCP (HTTPs)	TR-069 management
	7550	HNB	TCP (HTTPS)	Firmware download
	49186	RDU	TCP	RDU<->DPE communication
	2323	DPE	TCP	DPE CLI
	8001	DPE	UDP(SNMP)	SNMP Internal
	7551	DPE/PAR	TCP	DPE authorization service with PAR communication
	Random	DPE/PNR/PAR	TCP/UDP	Random ports used by internal processes: java, arservagt, armcdsvr, cnrservagt, dhcp, cnrsnmp, ccmsrv ,dpe, cnrservagt, and arservagt

RMS Serving Node (PNR)	61610	HNB	UDP (DHCP)	IP address assignment	
	9443	Administrator	TCP (HTTPS)	PNR GUI port	
	1234	RDU/PNR	TCP	DHCP internal communication	
	RMS Serving Node (PAR)	1812	ASR5K (AAA)	UDP (RADIUS)	Authentication and authorization of HNB during Iuh HNB register
1234		RDU	TCP	DHCP internal communication	
647		RMS Serving Node (PAR)	TCP	DHCP failover communication. Only used when redundant RMS Serving instances are used.	
8005		Administrator	TCP	Tomcat server port	
8009		Administrator	TCP	Tomcat AJP connector port	
8443		Administrator	TCP (HTTPS)	PAR GUI port	
RMS Upload Server node	443	HNB	TCP (HTTPS)	PM & PED file upload	
	8082	RDU	TCP	Availability check	
	8082		TCP	North Bound traffic	
	Random	Upload Server	TCP/UDP	Random ports used by internal processes: java, ruby	

Cisco UCS Node Configuration

Each Cisco UCS hardware node has a minimum of 4 +1 Ethernet ports that connect different services to different networks as needed. It is recommended that the following binding of IP addresses to Ethernet ports must be followed:

Central Node Port Bindings

Port	IP Addresses
UCS Management Port	Cisco Integrated Management Controller (CIMC) IP address **Note** CIMC is used to administer Cisco UCS hardware.
Port 1	Hypervisor IP address **Note** Hypervisor access is used to administer VMs via vCenter.
	vCenter IP address
Port 2	Central VM Southbound (SB) IP address
Port 3	Central VM Northbound (NB) IP address

Serving and Upload Node Port Bindings

Port	IP Addresses
UCS Management Port	CIMC IP address
Port 1	Hypervisor IP Address
Port 2	Serving VM north-bound (NB) IP address
	Upload VM NB IP address
Port 3	Serving VM south-bound (SB) IP address
	Upload VM SB IP address

All-in-One Node Port Bindings

Port	IP Addresses
UCS Management Port	CIMC IP address
Port 1	Hypervisor IP Address
	vCenter IP address
Port 2	Central VM SB IP address
	Serving VM NB IP address
	Upload VM NB IP address
Port 3	Serving VM south-bound (SB) IP address
	Upload VM SB IP address
Port 4	Central VM NB IP address

Cisco ASR 5000 Gateway Configuration

The Cisco ASR 5000 Gateway utilizes the Serving VM for DHCP and AAA services. The blade-based architecture of the gateway provides unprecedented scale that can exceed 2,50,000 APs that can be handled by a Serving VM (or redundant pair).

To scale beyond 2,50,000 APs, the ASR 5000 uses several instances of SeGW and HNB-GW within the same Cisco ASR 5000 chassis to direct DHCP and AAA traffic to the correct Serving VM.

- SeGW instances—A separate SeGW instance must be created in the Cisco ASR 5000 for every 2,50,000 APs or every provisioning group (PG) (if smaller PGs are used). Each SeGW instance must:
  - Have a separate public IP address for APs to connect to;
  - Configure DHCP requests to be sent to different set of Serving VMs.

  The SeGW can be co-located with HNB-GW on the same physical ASR 5000 chassis or alternatively SeGW can created on an external ASR 9000 or Cisco 7609 chassis.
- HNB-GW instances—A separate HNB-GW instance must be created in the Cisco ASR 5000 for every 2,50,000 APs or every PG (if smaller PGs are used). Each HNB-GW instance must:
  - Support different private IP addresses for APs to connect via IPSec tunnel
  - Associate with one SeGW context
  - Configure AAA traffic to be sent to different set of Serving VMs
  - Configure AAA traffic to be received from the Central VM (PMG) on a different port or IP

To configure the Cisco ASR 5000 Small Cell Gateway, see the Cisco ASR 5000 System Administration Guide.

NTP Configuration

Network Time Protocol (NTP) synchronization must be configured on all devices in the network as well as on the Cisco UCS servers. The NTP server can be specified during server installation. Failure to organize time synchronization across your network can result in anomalous functioning and results in the Cisco RAN Management System.

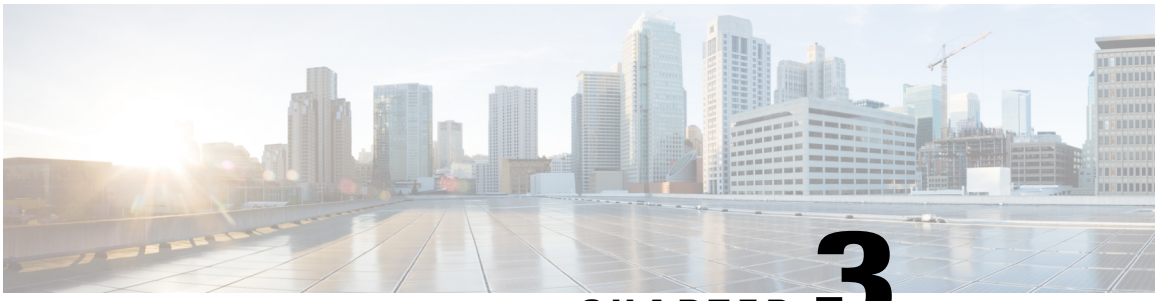
Public Fully Qualified Domain Names

It is recommended to have fully qualified domain name (FQDNs) for all public and private IP addresses because it can simplify IP renumbering. The DNS used by the operator must be configured to resolve these FQDNs to IP addresses of RMS nodes.

If FQDNs are used to configure target servers on the AP, then server certificates must contain the FQDN to perform appropriate security handshake for TLS.

RMS System Backup

It is recommended to perform a backup of the system before proceeding with the RMS installation. For more details, see RMS Upgrade, on page 177.



CHAPTER 3

Installing VMware ESXi and vCenter for Cisco RMS

This chapter explains how to install the VMware ESXi and vCenter for the Cisco RAN Management System. The following topics are covered in this chapter:

- Prerequisites, page 29
- Configuring Cisco UCS US 240 M3 Server and RAID, page 30
- Installing and Configuring VMware ESXI 5.5.0, page 31
- Configuring vCenter, page 32
- Configuring NTP on ESXi Hosts for RMS Servers, page 33
- Installing the OVF Tool, page 34
- Configuring SAN for Cisco RMS, page 36

Prerequisites

- Rack-mount the Cisco UCS Server and ensure that it is cabled and connected to the network.
- Download VMware ESXi 5.5.0 ISO to the local system
  - File name: VMware-VMvisor-Installer-5.5.0-1331820.x86_64.iso
- Download VMware vCenter 5.5.0 OVA appliance to the local system
  - File name: VMware-vCenter-Server-Appliance-5.5.0.5201-1476389_OVF10.OVA
- Download OVF Tool image to the local system
  - File name: VMware-ovftool-3.0.1-801290-lin.x86_64.bundle
  - File name: VMware-ovftool-3.5.1-1747221-win.x86_64.msi (for Microsoft Windows 64 bit)

Note The OVF Tool image name may change based on the OS version.

- Three set of IP addresses

Note You can download the above-mentioned packages from the VMware website using a valid account.

Configuring Cisco UCS US 240 M3 Server and RAID

Procedure

Step 1 Assign a Cisco Integrated Management Controller (CIMC) Management IP address by physically accessing the Cisco UCS server:

a) Boot up the server and click **F8** to stop the booting.

b) Set the IP address and other configurations as shown in the following figure.



c) Press **F10** to save the configurations and press **Esc** to exit and reboot the server.
The CIMC console can now be accessed via any browser from a system within the same network.

Step 2 Enter the CIMC IP on the browser to access the login page.

Step 3 Enter the default login, Admin, and **password**.

Step 4 Select the **Storage** tab and then click the **Create Virtual Drive from Unused Physical Drives** option to open the dialog box. In the dialog box, four physical drives are shown as available. Configure a single RAID 5.

Note If more number of disks are available, it is recommended that RAID 1 drive be configured with two disks for the VMware ESXi OS and the rest of the disks as a RAID 5 drive for VM Datastore.

Step 5 Choose the Raid Level from the drop-down list, for example, 5.

Step 6 Select the physical drive from the Physical Drives pane, for example, 1.

Step 7 Click **Create Virtual Drive** to create the virtual drive.

Step 8 Next, in the Virtual Drive Info tab, click **Initialize** and **Set as Boot Drive**. This completes the Cisco UCS 240 Server and RAID configuration.

Installing and Configuring VMware ESXI 5.5.0

Procedure

Step 1 Log in to CIMC.

Step 2 Select the **Admin** and **NTP Settings** tabs.

Step 3 Set the available NTP servers and click **Save**.

Note If no NTP servers are available, this step can be skipped. However, these settings help synchronize the VMs with the NTP.

Step 4 Click the **Server** tab and click **Launch KVM Console** from Actions to launch the KVM console.

Step 5 In the KVM Console, click the **Virtual Media** tab and load the downloaded VMware ESXi 5.5.0 ISO image.

Step 6 Click the **KVM** tab and reboot the server. Press **F6** to select the Boot menu.

Step 7 In the Boot menu, select the appropriate image device.

Step 8 Select the ESXi image in the Boot menu to load it.

Step 9 Click **Continue** to Select the operation to perform.

Step 10 Select the available storage.

Step 11 Set the root credential for the ESXi OS and press **F11** to proceed with the installation.

Step 12 Reboot the system after installation and wait to boot the OS completely.

Step 13 Next, set the ESXi OS IP. Press **F2** to customize and select **Configure Management Network**.

Note Set the VLAN ID if any underlying VLAN is configured on the router.

Step 14 Select the IP configuration and set the IP details.

Step 15 Press **Esc** twice and **Y** to save the settings. You should now be able to ping the IP.

Note If required, the DNS server and host name can be set in the same window.

Step 16 Download the vSphere client from http://<esxi-host-Ip> and install it on top of the Windows OS. The installed ESXi can be accessed via the vSphere client.
This completes the VMware ESXi 5.5.0 installation and configuration.

Installing the VMware vCenter 5.5.0

Procedure

Step 1 Log in to the VMware ESXi host via the vSphere client.
Note Skip steps 2 to 4 if no underlying VLAN is available.

Step 2 Select the Configuration tab and select Networking.

Step 3 Select **Properties** and then select **VM Network** in the Properties dialog box and edit.

Step 4 Set the appropriate VLAN ID and click **Save**.

Step 5 Next, go to **File > Deploy OVA Template** and provide the path of the download vCenter 5.5.0 ISO.

Step 6 Provide a vCenter name. The deployment settings summary is displayed in the next window.

Step 7 Start the OVA deployment.

Step 8 Power on the VM and open the console after successful OVA deployment.

Step 9 Log in with the default credentials root/vmware and set the IP address, gateway, and DNS name, and host name.

Step 10 Access the vCenter IP https://<vcenter-Ip:5480> from the browser.

Step 11 Log in with the root/vmware. After log in, accept the license agreement.

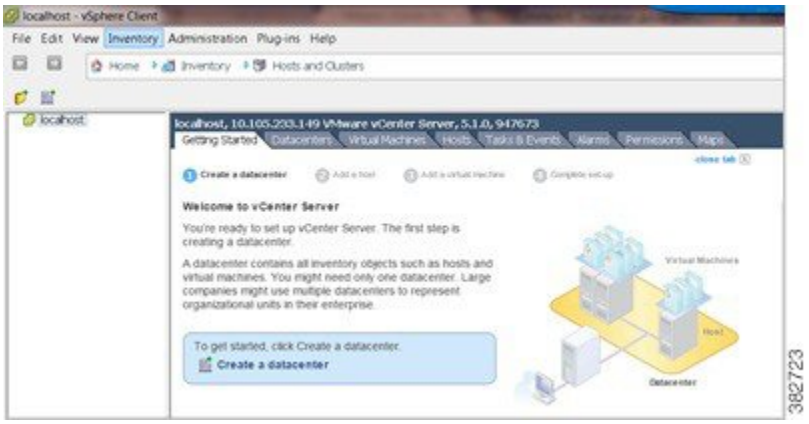
Step 12 Select **Configure with Default Settings** and click **Next** and then **Start**.
Note Use the embedded to store the vCenter inventory, which can handle up to ten hosts and fifty VMs. Usage of an external database like oracle is out of scope.
It takes around 10 to 15 minutes to configure and mount the database. On completion, the summary vCenter displays the summary.

Step 13 Now, access the vCenter via the vSphere client.
This completes the VMware vCenter 5.5.0 installation.

Configuring vCenter

Procedure

Step 1 Log in to the vSphere client.



Step 2 Rename the top level directory and a datacenter.

Step 3 Click **Add Host** and add the same ESXi host in the vCenter inventory list.

Step 4 Enter the host IP address and credentials (same credential set during the ESXi OS installation) in the Connection Settings window.

Step 5 Add the ESXi license key, if any, in the Assign License window.

Step 6 Click **Next**. The configuration summary window is displayed.

Step 7 Click **Finish**. The ESXi host is now added to the vCenter inventory. You can also find the datastore and port group information in the summary window.

Step 8 To add a ESXi host if another VLAN is availabe in your network, follow these steps:

a) Select the ESXi host. Go to the Configuration tab and select **Networking**.

b) Select **Properties** and then click **Add** in the Properties window.

c) Select **Virtual Machine** in the Connection Type window.

d) Provide the VLAN Id

e) Click **Next** and then **Finish**. The second portgroup will be available on the ESXi standard virtual switch.

Note The network names—VM network and VM network 2—can be renamed and used in the ovf descriptor file.

This completes the vCenter configuration for the Cisco RMS installation.

Configuring NTP on ESXi Hosts for RMS Servers

Follow this procedure to configure the NTP server to communicate with all the connected hosts.

Before You Begin

Before configuring the ESXi to an external NTP server, ensure that the ESXi hosts can reach the required NTP server.

Procedure

Step 1 Start the vSphere client.

Step 2 Go to **Inventory > Hosts and Clusters** and select the host.

Step 3 Select the **Configuration** tab.

Step 4 In the Software section of the Configuration tab, select **Time Configuration** to view the time configuration details. If the NTP Client shows "stopped" status, then enable the NTP client by following these steps:

a) Click the **Properties** link (at the top right-hand corner) in the Configuration tab to open the Time Configuration window.
b) Check the **NTP Client Enabled** checkbox.
c) Click **Options** to open the NTP Daemon (ntpd) Options window.
d) Click **Add** to add the NTP server IP address in the Add NTP Server dialog box.
e) Click **OK**.
f) In the NTP Daemon (ntpd) Options window, check the **Restart NTP service to apply changes** checkbox.
g) Click **OK** to apply the changes.
h) Verify that the NTP Client status now is "running".

Installing the OVF Tool

The OVF Tool application is used to deploy virtual appliances on vCenter using CLIs. You can install the OVF Tool for Red Hat Linux and Microsoft Windows as explained in the following procedures:

- Installing the OVF Tool for Red Hat Linux, on page 34
- Installing the OVF Tool for Microsoft Windows, on page 35

Installing the OVF Tool for Red Hat Linux

This procedure installs the OVF Tool for Red Hat Linux on the vCenter VM.

Procedure

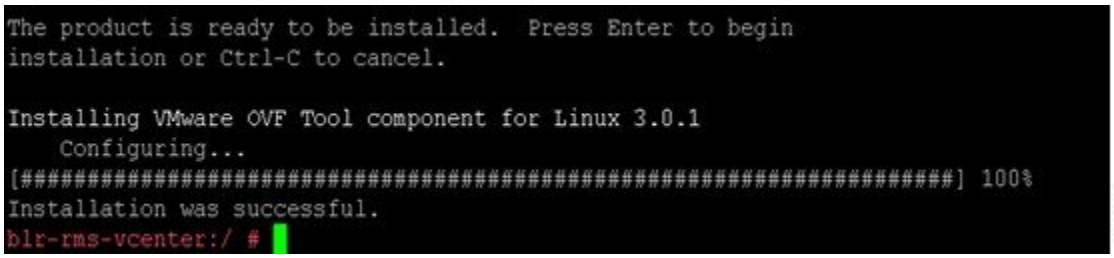
Step 1 Transfer the downloaded VMware-ovftool-3.0.1-801290-lin.x86_64.bundle to the vCenter VM via scp/ftp tools.

Note The OVF Tool image name may change based on the OS version.

Step 2 Check the permission of the file as shown below.

```
localhost:/ # ls -al VMware-ovftool-3.0.1-801290-lin.x86_64.bundle
-rwxr-xr-x 1 root root 36631447 Jul  9  2013 VMware-ovftool-3.0.1-801290-lin.x86_64.bundle
```

Step 3 Execute and follow the on-screen instructions to complete the OVF Tool installation. to complete it.



OVF Tool installation completed.

You can use the following command to deploy OVA.

Example:

```
# ovftool  <location-of-ova-file>  vi://root:<vmware is the id>@<password to log in to
                                vcenter IP>/blr-datacenter/host/<esxihost-ip>
```

Installing the OVF Tool for Microsoft Windows

This procedure installs the OVF Tool for Microsoft Windows 64 bit, on the vCenter VM.

Before You Begin

Procedure

Step 1 Double-click the Windows 64 bit VMware-ovftool-3.5.1-1747221-win.x86_64.msi on your local system to start the installer.
Note The OVF Tool image name may change based on the OS version.

Step 2 In the Welcome screen of the installer, click **Next**.

Step 3 In the License Agreement, read the license agreement and select I agree and click **Next**.

Step 4 Accept the path suggested for the OVF Tool installation or change to a path of your choice and click **Next**.

Step 5 When you have finished choosing your installation options, click **Install**.

Step 6 When the installation is complete, click **Next**.

Step 7 Deselect the **Show the readme file** option if you do not want to view the readme file, and click **Finish** to exit.

Step 8 After installing the OVF Tool on Windows, run the OVF Tool from the DOS prompt.
You should have the OVF Tool folder in your path environment variable to run the OVF Tool from the command line. For instructions on running the utility, go to <datacenter name>/host/<resource pool path>/<vm or vApp name>.

Configuring SAN for Cisco RMS

This section covers the procedure of adding SAN LUN discovery and data stores for RMS hosts on VMware ESXi 5.5.0. It also describes the procedure to associate desired data stores with VMs.

- Creating a SAN LUN, on page 36
- Installing FCoE Software Adapter Using VMware ESXi, on page 36
- Adding Data Stores to Virtual Machines, on page 37
- Migrating the Data Stores, on page 53

Creating a SAN LUN

In the following procedure, Oracle ZFS storage ZS3-2 is used as a reference storage. The actual procedure for creation of logical unit number (LUN) may vary depending on the storage used.

Procedure

Step 1 Log in to the storage using the Oracle ZFS Storage ZS3-2 GUI.

Step 2 Click **Shares**.

Step 3 Click **+LUNs** to open the Create LUN window.

Step 4 Provide the Name, Volume size, and Volume block size. Select the default Target group, Initiator group(s) group and click **Apply**.
New LUN is displayed on the LUN list.

Step 5 Follow steps 1 to 4 to create another LUN.

What to Do Next

To install FCoE Software Adapter, see Installing FCoE Software Adapter Using VMware ESXi, on page 36.

Installing FCoE Software Adapter Using VMware ESXi

Before You Begin

- SAN LUNs should be created based on the SAN requirement (see Creating a SAN LUN, on page 36) and connected via the Fibre Channel over Ethernet (FCoE) to the UCS chassis and hosts with multipaths.
- The LUN is expected to be available on SAN storage as described in Data Storage for Cisco RMS VMs, on page 15. The LUN Size can be different based on the Cisco RMS requirements for the deployment.
- The physical HBA cards should be installed and configured. SAN is attached with the server and LUN shared from storage end.

Procedure

Step 1 Log in to the VMware ESXi host via the vSphere client.

Step 2 Click the **Configuration** tab. In the Hardware area, click **Storage Adapters** to check if the FCoE software adapter is installed. In the Configuration tab, the installed HBA cards (vmhba1,vmhba2) will be visible because there are two physical HBA cards present on the ESXi host. If you do not see the installed HBA cards, refresh the screen to view it.

Step 3 Click **Rescan All** and select the HBA cards one-by-one and the "targets", "devices", and "paths" can be seen.

Step 4 In the Hardware pane, click **Storage**.

Step 5 In the Configuration tab, click **Add Storage** to open the Add Storage wizard.

Step 6 In the Storage Type screen, select the **Disk/LUN** option. Click **Next**.

Step 7 In the Select Disk/LUN screen, select the available FC LUN from the list of available LUNs and click **Next**.

Step 8 In the File System Version screen, select the **VMFS-5** option. Click **Next**.

Step 9 In the Current Disk Layout screen, review the selected disk layout. Click **Next**.

Step 10 In the Properties screen, enter a data store name in the field. For example, SAN-LUN-1. Click **Next**.

Step 11 In the Disk/LUN - Formatting screen, leave the default options as-is and click **Next**.

Step 12 In the Ready to Complete screen, view the summary of the disk layout and click **Finish**.

Step 13 Find the datastore added with the host in the Configuration tab. The added SAN is now ready to use.

Step 14 Repeat steps 4 to 12 to add additional LUNs.

Adding Data Stores to Virtual Machines

Below are the procedures to manually associate datastores to VMs, while OVA installation corresponding SYSTEM data store is provided during installation from the OVA (like SYSTEM_CENTRAL for Central VM, SYSTEM_SERVING for Serving VM, SYSTEM_UPLOAD for Upload VM).

- Adding Central VM Data Stores, on page 37
- Adding Serving VM Data Stores, on page 50
- Adding Upload VM Data Stores, on page 50

Adding Central VM Data Stores

- Adding the DATA Datastore, on page 38
- Adding the TX_LOGS Datastore, on page 41
- Adding the BACKUP Datastore, on page 45
- Validating Central VM Datastore Addition, on page 49

Adding the DATA Datastore

Procedure

Step 1 In the navigation pane, expand **Home > Inventory > Hosts and Clusters** and select the Central node.

Step 2 Right-click on the Central node and click **Edit Settings** to open the Central-Node Virtual Machine Properties dialog box.

Step 3 Click Add in the Hardware tab to open the Add Hardware wizard.

Step 4 In the Device Type screen, select **Hard Disk** from the Choose the type of device you wish to add list. Click **Next**.

Step 5 In the Select a Disk screen, select the **Create a new virtual disk** option. Click **Next**.

Step 6 In the Create a Disk screen, select the disk capacity or memory to be added. For example, 50 GB.

Step 7 Click **Browse** to specify a datastore or datastore cluster to open the Select a datastore or datastore cluster dialog box.

Step 8 In the Select a datastore or datastore cluster dialog box, select DATA datastore and click **Ok** to return to the Create a Disk screen. The selected datastore is displayed in the Specify a datastore or datastore cluster field.

Step 9 Click **Next**.

Step 10 In the Advanced Options screen, leave the default options as-is and click **Next**.

Step 11 In the Ready to Complete screen, the options selected for the hardware are displayed. Click **Finish** to return to the Central-Node Virtual Machine Properties dialog box.

Step 12 Click **Ok**.
For Lab purposes the storage sizes to be chosen for the 'DATA' is 50 GB, for TXN_LOGS is 10 GB and for BACKUPS is 50 GB .

Step 13 In the navigation pane, expand **Home > Inventory > Hosts and Clusters** and select the Central node.

Step 14 Right-click on the Central node and click **Power > Restart Guest** to restart the VM.

Step 15 Log in to the Central node VM and enter sudo mode and trigger its failure. Establish a ssh connection to the VM.

```
ssh 10.32.102.68
```

```
The system responds by connecting the user to the Central VM.
```

Step 16 Use the **sudo** command to gain access to the root user account.

```
sudo su -
```

```
The system responds with a password prompt.
```

Step 17 Check the status of the newly added disk. The disk that is not partitioned is the newly added disk.

```
fdisk -l
```

```
Disk /dev/sda: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0005a3b3

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
```

```
Partition 2 does not end on cylinder boundary.
/dev/sda3              33        6528    52165632   83  Linux

Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdb doesn't contain a valid partition table
```

Step 18 Stop the RDU applications.

```
/etc/init.d/bprAgent stop
BAC Process Watchdog has stopped.
```

Step 19 Format the disk by partitioning the newly added disk.

```
fdisk /dev/sdb
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xcfa0e306.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help): p

Disk /dev/sdc: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xcfa0e306
```

```
   Device Boot      Start         End      Blocks   Id  System

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1305, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-1305, default 1305):
Using default value 1305

Command (m for help): v
Remaining 6757 unallocated 512-byte sectors

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

Step 20 Mark the disk as ext3 type of partition.

```
/sbin/mkfs -t ext3 /dev/sdb1
[root@blr-rms-ha-upload01 files]# /sbin/mkfs -t ext3 /dev/sdb1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
6553600 inodes, 26214055 blocks
1310702 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 26 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

Step 21 Create backup folders for the 'data' partition.

```
mkdir /backups; mkdir /backups/data
The system responds with a command prompt.
```

Step 22 Back up the data.

```
mv /rms/data/ /backups/data/
The system responds with a command prompt.
```

Step 23 Create a new folder for the 'data' partition.

```
cd /rms; mkdir data; chown ciscorms:ciscorms data
The system responds with a command prompt.
```

Step 24 Mount the added partition to the newly added folder.

```
mount /dev/sdb1 /rms/data
The system responds with a command prompt.
```

Step 25 Move the copied folders back for the 'data' partition.

```
cd /backups/data/data; mv pools/ /rms/data/; mv CSCObac /rms/data; mv nwreg2
/rms/data; mv dcc_ui /rms/data
The system responds with a command prompt.
```

Step 26 Edit the fstab file and add the below highlighted text to the end of the file and save it.

```
vi /etc/fstab
#
# /etc/fstab
# Created by anaconda on Fri Apr  4 10:07:01 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=3aa26fdd-1bd8-47cc-bd42-469c01dac313 /                       ext3    defaults
1 1
UUID=ccc74e66-0c8c-4a94-aee0-1eb152502e3f /boot                   ext3    defaults
1 2
UUID=f7d57765-abf4-4699-a0bc-f3175a66470a swap                    swap    defaults
0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/sdb1 /rms/data ext3 rw 0 0
:wq
```

Step 27 Restart the RDU process.

```
/etc/init.d/bprAgent start
BAC Process Watchdog has started.
```

What to Do Next

To add the TX_LOGS datastore, see Adding the TX_LOGS Datastore, on page 41.

Adding the TX_LOGS Datastore

Procedure

Step 1 Repeat Steps 24 to 27 of Adding the DATA Datastore, on page 38 in the for the partitions of 'TX_LOGS'.

Step 2 Log in to the Central node VM and enter sudo mode and trigger its failure. Establish a ssh connection to the VM.

```
ssh 10.32.102.68
```

The system responds by connecting the user to the Central VM.

Step 3 Use the **sudo** command to gain access to the root user account.

```
sudo su -
```

The system responds with a password prompt.

Step 4 Check the status of the newly added disk. The disk that is not partitioned is the newly added disk.

```
fdisk –l
[blr-rms-ha-central03] ~ # fdisk -l

Disk /dev/sda: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0005a3b3

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
/dev/sda3              33        6528    52165632   83  Linux

Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xaf39a885

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1        6527    52428096   83  Linux

Disk /dev/sdc: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdc doesn't contain a valid partition table
```

Step 5 Stop the RDU applications.

```
/etc/init.d/bprAgent stop
BAC Process Watchdog has stopped.
```

Step 6 Format the disk by partitioning the newly added disk.

```
fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xcfa0e306.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
```

```
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help): p

Disk /dev/sdc: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xcfa0e306

   Device Boot      Start         End      Blocks   Id  System

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1305, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-1305, default 1305):
Using default value 1305

Command (m for help): v
Remaining 6757 unallocated 512-byte sectors

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
```

```
Syncing disks.
```

Step 7 Mark the disk as ext3 type of partition.

```
/sbin/mkfs -t ext3 /dev/sdc1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
6553600 inodes, 26214055 blocks
1310702 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 26 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

Step 8 Create backup folders for the 'txn' partition.

```
 mkdir /backups/txn
The system responds with a command prompt.
```

Step 9 Back up the data.

```
 mv /rms/txn/ /backups/txn
The system responds with a command prompt.
```

Step 10 Create a new folder for the ‘txn’ partition.

```
 cd /rms; mkdir txn; chown ciscorms:ciscorms txn
The system responds with a command prompt.
```

Step 11 Mount the added partition to the newly added folder.

```
 mount /dev/sdc1 /rms/txn
The system responds with a command prompt.
```

Step 12 Move the copied folders back for the ‘txn’ partition.

```
 cd /backups/txn/txn; mv CSCObac/ /rms/txn/
The system responds with a command prompt.
```

Step 13 Edit the file fstab and add the below highlighted text at the end of the file and save it.

```
vi /etc/fstab
#
# /etc/fstab
# Created by anaconda on Mon May  5 15:08:38 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
```

```
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=f2fc46ec-f5d7-4223-a1c0-b31476770dc7 /                       ext3    defaults
1 1
UUID=8cb5ee90-63c0-4a00-967d-698644c5aa8c /boot                   ext3    defaults
1 2
UUID=f1a0bf72-0d9e-4032-acd2-392df6eb1329 swap                    swap    defaults
0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/sdb1 /rms/data ext3 rw 0 0
/dev/sdc1 /rms/txn ext3 rw 0 0

:wq
```

Step 14 Restart the RDU process.

```
 /etc/init.d/bprAgent start
BAC Process Watchdog has started.
```

What to Do Next

To add the BACKUP datastore, see Adding the BACKUP Datastore, on page 45.

Adding the BACKUP Datastore

Procedure

Step 1 Repeat Steps 24 to 27 of Adding the DATA Datastore, on page 38 in the for the partitions of 'BACKUPS'.

Step 2 Log in to the Central node VM and enter sudo mode and trigger its failure. Establish a ssh connection to the VM.

```
ssh 10.32.102.68
The system responds by connecting the user to the Central VM.
```

Step 3 Use the **sudo** command to gain access to the root user account.

```
sudo su -
The system responds with a password prompt.
```

Step 4 Check the status of the newly added disk. The disk that is not partitioned is the newly added disk.

```
fdisk -l
[blr-rms-ha-central03] ~ # fdisk -l

Disk /dev/sda: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0005a3b3

   Device Boot      Start         End      Blocks   Id  System
```

```
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
/dev/sda3              33        6528    52165632   83  Linux

Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xaf39a885

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1        6527    52428096   83  Linux

Disk /dev/sdc: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xcfa0e306

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1        1305    10482381   83  Linux

Disk /dev/sdd: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdd doesn't contain a valid partition table
```

Step 5 Stop the RDU applications.

```
/etc/init.d/bprAgent stop
BAC Process Watchdog has stopped.
```

Step 6 Format the disk by partitioning the newly added disk.

```
fdisk /dev/sdd
[blr-rms-ha-central03] ~ # fdisk /dev/sdd
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xf35b26bc.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): m
Command action
   a   toggle a bootable flag
```

```
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help): p

Disk /dev/sdd: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xf35b26bc

   Device Boot      Start         End      Blocks   Id  System

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-6527, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-6527, default 6527):
Using default value 6527

Command (m for help): v
Remaining 1407 unallocated 512-byte sectors

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[blr-rms-ha-central03] ~ # /sbin/mkfs -t ext3 /dev/sdd1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
3276800 inodes, 13107024 blocks
655351 blocks (5.00%) reserved for the super user
```

```
First data block=0
Maximum filesystem blocks=4294967296
400 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 35 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

Step 7 Mark the disk as ext3 type of partition.

```
/sbin/mkfs -t ext3 /dev/sdd1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
6553600 inodes, 26214055 blocks
1310702 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 26 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

Step 8 Create backup folders for the 'backups' partition.

```
 mkdir /backups/backups
The system responds with a command prompt.
```

Step 9 Back up the data.

```
 mv /rms/backups /backups/backups
The system responds with a command prompt.
```

Step 10 Create a new folder for the 'backups' partition.

```
 cd /rms; mkdir backups; chown ciscorms:ciscorms backups
The system responds with a command prompt.
```

Step 11 Mount the added partition to the newly added folder.

```
 mount /dev/sdd1 /rms/backups
The system responds with a command prompt.
```

Step 12 Move the copied folders back for the 'backups' partition.

```
 cd /backups/backups; mv * /rms/backups/
The system responds with a command prompt.
```

Step 13 Edit the file fstab and add the below highlighted text at the end of the file and save it.

```
vi /etc/fstab
#
# /etc/fstab
# Created by anaconda on Mon May  5 15:08:38 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=f2fc46ec-f5d7-4223-a1c0-b31476770dc7 /                       ext3    defaults
1 1
UUID=8cb5ee90-63c0-4a00-967d-698644c5aa8c /boot                   ext3    defaults
1 2
UUID=f1a0bf72-0d9e-4032-acd2-392df6eb1329 swap                    swap    defaults
0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/sdb1 /rms/data ext3 rw 0 0
/dev/sdc1 /rms/txn ext3 rw 0 0
/dev/sdd1 /rms/backups ext3 rw 0 0

:wq
```

Step 14 Restart the RDU process.

```
 /etc/init.d/bprAgent start
BAC Process Watchdog has started.
```

What to Do Next

To add validate the data stores added to the Central VM, see Validating Central VM Datastore Addition, on page 49.

Validating Central VM Datastore Addition

After datastores are added to the host and disks are mounted in the Central VM, validate the added datastores in vSphere client and ssh session on the VM.

Procedure

Step 1 Log in to the vSphere client.

Step 2 In the navigation pane, expand **Home > Inventory > Hosts and Clusters** and select the Central VM.

Step 3 Click the **General** tab to view the datastores associated with the VM, displayed on the screen.

Step 4 Log in to the Central node VM and establish a ssh connection to the VM to see the four disks mounted.

```
[blrrms-central-22] ~ $ mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /rms/data type ext3 (rw)
/dev/sdc1 on /rms/txn type ext3 (rw)
/dev/sdd1 on /rms/backups type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
[blrrms-central-22] ~ $
```

Adding Serving VM Data Stores

Adding the SYSTEM_SERVING Datastore, on page 50

Adding the SYSTEM_SERVING Datastore

In the OVA installation, assign a datastore from the available datastores based on your space requirement for installation. For example, SYSTEM_SERVING.

What to Do Next

To add data stores to the Upload VM, see Adding Upload VM Data Stores, on page 50.

Adding Upload VM Data Stores

- Adding the SYSTEM_UPLOAD Datastore, on page 50
- Adding PM_RAW and PM_ARCHIVE Datastores, on page 51
- Validating Upload VM Datastore Addition, on page 53

Adding the SYSTEM_UPLOAD Datastore

In OVA installation provide SYSTEM_UPLOAD as the datastore for installation.

What to Do Next

To add the PM_RAW and PM_ARCHIVE datastores, see Adding PM_RAW and PM_ARCHIVE Datastores, on page 51.

Adding PM_RAW and PM_ARCHIVE Datastores

Procedure

Step 1 Repeat steps 1 to 14 of Adding the DATA Datastore, on page 38 to add the PM_RAW data store.

Step 2 Repeat steps 1 to 14 of Adding the DATA Datastore, on page 38 to add the PM_ARCHIVE data store.

Step 3 Log in to the Central node VM and establish a ssh connection to the Upload VM using the Upload node hostname.

```
ssh admin1@blr-rms14-upload
The system responds by connecting the user to the upload VM.
```

Step 4 Use the **sudo** command to gain access to the root user account.

```
sudo su -
The system responds with a password prompt.
```

Step 5 Apply **fdisk -l** to display new disk discovered to the system.

Step 6 Apply **fdisk /dev/sdb** to create a new partition on a new disk and save.

```
fdisk /dev/sdb
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-52216, default 1): 1
Last cylinder, +cylinders or +size{K,M,G} (1-52216, default 52216): 52216

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks..
```

Follow the on-screen prompts carefully to avoid errors that may corrupt the entire system.

The cylinder values may vary based on the machine setup.

Step 7 Repeat Step 6 to create partition on the /dev/sdc.

Step 8 Stop the LUS process.

```
god stop UploadServer
Sending 'stop' command
The following watches were affected:
UploadServer
```

Step 9 Create backup folders for the 'files' partition.

```
mkdir -p /backups/uploads
The system responds with a command prompt.

mkdir -p /backups/archives
The system responds with a command prompt.
```

Step 10 Back up the data.

```
 mv/opt/CSCOuls/files/uploads/* /backups/uploads
mv/opt/CSCOuls/files/archives/* /backups/archives
The system responds with a command prompt.
```

Step 11 Create the file system on the new partitions.

```
 mkfs.ext4 -i 4049 /dev/sdb1
The system responds with a command prompt.
```

Step 12 Repeat Step 10 for /dev/sdc1.

Step 13 Mount new partitions under /opt/CSCOuls/files/uploads and /opt/CSCOuls/files/archives directories using the following commands.

```
 mount -t ext4 -o
noatime,data=writeback,commit=120 /dev/sdb1 /opt/CSCOuls/files/uploads/
 mount -t ext4 -o
noatime,data=writeback,commit=120 /dev/sdc1 /opt/CSCOuls/files/archives/

The system responds with a command prompt.
```

Step 14 Edit /etc/fstab and append following entries to make the mount point reboot persistent.

```
/dev/sdb1 /opt/CSCOuls/files/uploads/ ext4 noatime,data=writeback,commit=120 0 0
/dev/sdc1 /opt/CSCOuls/files/archives/ ext4 noatime,data=writeback,commit=120 0 0
```

Step 15 Restore the already backed up data.

```
mv /backups/uploads/* /opt/CSCOuls/files/uploads/
mv /backups/archives/* /opt/CSCOuls/files/archives/
The system responds with a command prompt.
```

Step 16 Check ownership of the /opt/CSCOuls/files/uploads and /opt/CSCOuls/files/archives directory with the following command.

```
ls -l /opt/CSCOuls/files
```

Step 17 Change the ownership of the files/uploads and files/archives directories to ciscorms.

```
 chown -R ciscorms:ciscorms /opt/CSCOuls/files/
The system responds with a command prompt.
```

Step 18 Verify ownership of the mounting directory.

```
ls -al /opt/CSCOuls/files/
total 12
drwxr-xr-x. 7 ciscorms ciscorms 4096 Aug  5 06:03 archives
drwxr-xr-x. 2 ciscorms ciscorms 4096 Jul 25 15:29 conf
drwxr-xr-x. 5 ciscorms ciscorms 4096 Jul 31 17:28 uploads
```

Step 19 Edit the /opt/CSCOuls/conf/UploadServer.properties file.

```
cd /opt/CSCOuls/conf;
sed –i
's/UploadServer.disk.alloc.global.maxgb.*/UploadServer.disk.alloc.global.maxgb=<Max limit>/'

UploadServer.properties;
System returns with command prompt.
```

Replace <Max limit> with the maximum size of partition mounted under /opt/CSCOuls/files/uploads directory.

Step 20 Start the LUS process.

```
god start UploadServer
Sending 'start' command
The following watches were affected:
UploadServer
```

Note For the Upload Server to work properly, both/opt/CSCOuls/files/uploads/and/opt/CSCOuls/files/archives/folders must be on different partitions.

What to Do Next

To add validate the data stores added to the Upload VM, see Validating Upload VM Datastore Addition, on page 53.

Validating Upload VM Datastore Addition

After datastores are added to the host and disks are mounted in the Upload VM, validate the added datastores in vSphere client and ssh session on the VM.

Procedure

Step 1 Log in to the vSphere client.

Step 2 In the navigation pane, expand **Home > Inventory > Hosts and Clusters** and select the Upload VM.

Step 3 Click the **General** tab to view the datastores associated with the VM, displayed on the screen.

Step 4 Log in to the Central node VM and establish a ssh connection to the VM to see the two disks mounted.

Migrating the Data Stores

• Initial Migration on One Disk, on page 53

Initial Migration on One Disk

Procedure

Step 1 Log in to the VMware ESXi host via the vSphere client.

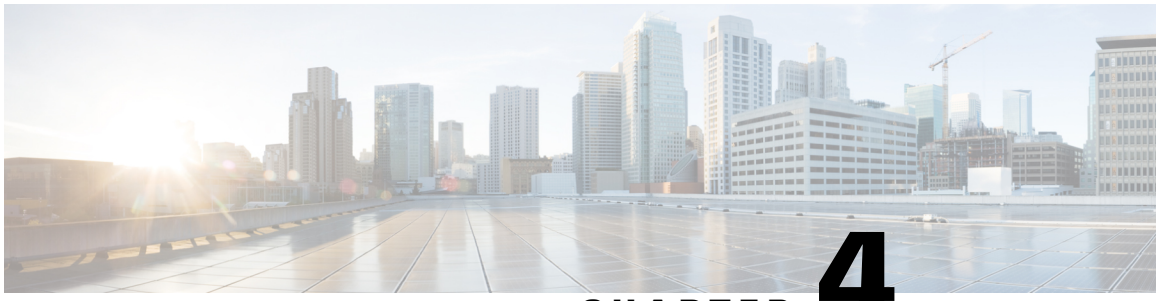
Step 2 In the navigation pane, expand **Home > Inventory > Hosts and Clusters** and select the Central node.

Step 3 Right-click on the Central node and click **Migrate** to open the Migrate Virtual Machine wizard.

Step 4 In the Select Migration Type screen, select the **Change datastore** option. Click **Next**.

Step 5 In the Storage screen, select the required data store. Click **Next**.

Step 6 In the Ready to Complete screen, the options selected for the virtual machine migration are displayed. Click **Finish**.



CHAPTER 4

RMS Installation Tasks

Perform these tasks to install the RMS software.

- RMS Installation Procedure, page 55
- Preparing the OVA Descriptor Files, page 56
- Deploying the RMS Virtual Appliance, page 61
- RMS Redundant Deployment, page 66
- Optimizing the Virtual Machines, page 91
- RMS Installation Sanity Check, page 101

RMS Installation Procedure

The RMS installation procedure is summarized here with links to the specific tasks.

Step No.	Task	Link	Task Completion: Mandatory or Optional
1	Perform all prerequisite installations	Installation Prerequisites, on page 11 and Installing VMware ESXi and vCenter for Cisco RMS, on page 29	Mandatory
2	Create the Open Virtual Application (OVA) descriptor file	Preparing the OVA Descriptor Files, on page 56	Mandatory
3	Deploy the OVA package	Deploying the RMS Virtual Appliance, on page 61	Mandatory
4	Configure redundant Serving nodes	RMS Redundant Deployment, on page 66	Optional

Step No.	Task	Link	Task Completion: Mandatory or Optional
5	Run the configure_PNR_hnbgw.sh and configure_PAR_hnbgw.sh script to configure the HNB gateway properties	HNB Gateway and DHCP Configuration, on page 105	Mandatory if the HNB gateway properties were not included in the OVA descriptor file.
6	Optimize the VMs by upgrading the VM hardware version, upgrading the VM CPU and memory and upgrading the Upload VM data size	Optimizing the Virtual Machines, on page 91	Mandatory
7	Perform a sanity check of the system	RMS Installation Sanity Check, on page 101	Optional but recommended
8	Install RMS Certificates	Installing RMS Certificates, on page 109	Mandatory
9	Configure the default route on the Upload and Serving nodes for TLS termination	Configuring Default Routes for Direct TLS Termination at the RMS, on page 122	Optional
10	Install and configure the PMG database	PMG Database Installation and Configuration, on page 125	Optional Contact Cisco services to deploy PMG DB.
11	Configure the Central node	Configuring the Central Node, on page 130	Mandatory
12	Populate the PMG database	Configuring the Central Node, on page 130	Mandatory
13	Verify the installation	Verifying RMS Deployment, on page 171	Optional but recommended

Preparing the OVA Descriptor Files

The RMS requires Open Virtual Application (OVA) descriptor files, more commonly known as configuration files, that specify the configuration of various system parameters.

The easiest way to create these configuration files is to copy the example OVA descriptor files that are bundled as part of RMS build deliverable itself. The RMS-ALL-In-One-Solution package contains the sample descriptor for all-in-one deployment and the RMS-Distributed-Solution package contains the sample descriptor for distributed deployment. It is recommended to use these sample descriptor files and edit them according to your needs.

Copy the files and rename them as "*.ovftool*" before deploying. You need one configuration file for the all-in-one deployment and three separate files for the distributed deployment.

When you are done creating the configuration files, copy them to the server where vCenter is hosted and the ovftool utility is installed. Alternately, they can be copied to any other server where the ovftool utility tool by VMware is installed. In short, the configuration files must be copied as ".ovftool" to the directory where you can run the VMware **ovftool** command.

The following are mandatory properties that must be provided in the OVA descriptor file. These are the bare minimum properties required for successful RMS installation and operation. If any of these properties are missing or incorrectly formatted, an error is displayed. All other properties are optional and configured automatically with default values.



Note Make sure that all Network 1 (eth0) interfaces (Central, Serving, and Upload nodes) must be in same VLAN.

Only .txt and .xml formats support the copy of OVA descriptor file from desktop to Linux machine. Other formats such as .xlsx and .docx, store some garbage value when we copy to linux and throws an error during installation.

In csv file, if any comma delimiter present between two IPs, for example, **prop:Upload_Node_Gateway=10.5.4.1,10.5.5.1**, the property gets stored in double quotes when copied to Linux machine, **"prop:Upload_Node_Gateway=10.5.4.1,10.5.5.1"**. This will throw an error during deployment.

Table 1: Mandatory Properties for OVA Descriptor File

Property	Description	Valid Values
name	Name of the vApp that is deployed on the host name.	text
datastore	Name of the physical storage to keep the VM files.	text
net:Upload-Node Network 1	VLAN for the connection between the Upload node (NB) and the Central node (SB).	VLAN #
net:Upload-Node Network 2	VLAN for the connection between the Upload node (SB) and the CPE network (FAPs).	VLAN #
net:Central-Node Network 1	VLAN for the connection between the Central node (SB) and Upload Load (NB) or Serving node (NB).	VLAN #
net:Central-Node Network 2	VLAN for the connection between the Central node (NB) and the OSS network.	VLAN #
net:Serving-Node Network 1	VLAN for the connection between the Serving node (NB) and the Central node (SB).	VLAN #
net:Serving-Node Network 2	VLAN for the connection between the Serving node (SoB) and the CPE network (FAPs).	VLAN #

Property	Description	Valid Values
prop:Central_Node_Eth0_Address	IP address of the Southbound VM interface	IPv4 address
prop:Central_Node_Eth0_Subnet	Network mask for the IP subnet of the Southbound VM interface.	Network mask
prop:Central_Node_Eth1_Address	IP address of the Northbound VM interface.	IPv4 address
prop:Central_Node_Eth1_Subnet	Network mask for the IP subnet of the Northbound VM interface.	Network mask
prop:Central_Node_Dns1_Address	IP address of primary DNS server provided by network administrator.	IPv4 address
prop:Central_Node_Dns2_Address	IP address of secondary DNS server provided by network administrator.	IPv4 address
prop:Central_Node_Gateway	IP address of the gateway to the management network for the north bound interface of the Central node. IP address of the gateway from the Northbound interface of the Serving node towards the Central node southbound network and from the Southbound interface of the Serving node towards the CPE.	IPv4 address
prop:Serving_Node_Eth0_Address	IP address of the Northbound VM interface.	IPv4 address
prop:Serving_Node_Eth0_Subnet	Network mask for the IP subnet of the Northbound VM interface.	Network mask
prop:Serving_Node_Eth1_Address	IP address of the Southbound VM interface.	IPv4 address
prop:Serving_Node_Eth1_Subnet	Network mask for the IP subnet of the Southbound VM interface.	Network mask
prop:Serving_Node_Dns1_Address	IP address of primary DNS server provided by network administrator.	IPv4 address
prop:Serving_Node_Dns2_Address	IP address of secondary DNS server provided by network administrator.	IPv4 address

Property	Description	Valid Values
prop:Serving_Node_Gateway	IP address of the gateway to the management network.	comma separated IPv4 addresses of the form [Northbound GW],[Southbound GW] **Note** It is recommended to specify both the gateways.
prop:Upload_Node_Eth0_Address	IP address of the Northbound VM interface.	IPv4 address
prop:Upload_Node_Eth0_Subnet	Network mask for the IP subnet of the Northbound VM interface.	Network mask
prop:Upload_Node_Eth1_Address	IP address of the Southbound VM interface.	IPv4 address
prop:Upload_Node_Eth1_Subnet	Network mask for the IP subnet of the Southbound VM interface.	Network mask
prop:Upload_Node_Dns1_Address	IP address of primary DNS server provided by network administrator.	IPv4 address
prop:Upload_Node_Dns2_Address	IP address of secondary DNS server provided by network administrator.	IPv4 address
prop:Upload_Node_Gateway	IP address of the gateway from Northbound interface of the Upload node for northbound traffic and from Southbound interface of Upload node towards the CPE.	comma separated IPv4 addresses of the form [Northbound GW],[Southbound GW] **Note** It is recommended to specify both the gateways.
prop:Ntp1_Address	Primary NTP server.	IPv4 address
prop:Acs_Virtual_Fqdn	ACS virtual fully qualified domain name (FQDN). Southbound FQDN or IP address of the Serving node. For NAT based deployment, this can be set to public IP/FQDN of the NAT. This is the IP/FQDN which the AP will use to communicate from RMS.	IPv4 address or FQDN value **Note** The recommended value is FQDN. FQDN is required in case of a redundant setup.

Property	Description	Valid Values
prop:Upload_SB_Fqdn	Southbound FQDN or IP address of the Upload node. Specify Upload eth1 address if no fqdn exists. For NAT based deployment, this can be set to public IP/FQDN of the NAT.	IPv4 address or FQDN value **Note** The recommended value is FQDN. FQDN is required in case of a redundant setup.
prop:Central_Hostname	Configured host name of the Central node.	Character string; no periods (.) allowed
prop:Serving_Hostname	Configured host name of the Serving node.	Character string; no periods (.) allowed
prop:Upload_Hostname	Configured host name of the Upload node.	Character string; no periods (.) allowed
diskMode	Logical disk type of the VM.	Thin

Note For third-party SeGW support for allocating inner IPs (tunnel IPs), set the property "prop:Install_Cnr=False" in the descriptor file.

Refer to OVA Descriptor File Properties, on page 255 for a complete description of all required and optional properties for the OVA descriptor files.

Validation of OVA Files

If mandatory properties are missing from a descriptor file, the OVA installer displays an error on the installation console. If mandatory properties are incorrectly configured, an appropriate error is displayed on the installation console and the installation aborts.

An example validation failure message in the ova-first-boot.log is shown here:

```
"Alert!!! Invalid input for Acs_Virtual_Fqdn...Aborting installation..."
```

Log in to the relevant VM using root credentials (default password is Ch@ngeme1) to access the first-boot logs in the case of installation failures.

Wrongly configured properties include invalid IP addresses, invalid FQDN format, and so on. Validations are restricted to format/data-type validations. Incorrect IP addresses/FQDNs (for example, unreachable IPs) are not in the scope of validation.

Deploying the RMS Virtual Appliance

All administrative functions are available through vSphere client. A subset of those functions is available through the vSphere web client. The vSphere client users are virtual infrastructure administrators for specialized functions. The vSphere web client users are virtual infrastructure administrators, help desk, network operations centre operators, and virtual machine owners.

Note All illustrations in this document are from the VMware vSphere client.

Before You Begin

You must be running VMware vSphere version 5.5. There are two ways to access the VMware Vcenter:

- VMware vSphere Client locally installed application
- VMware vSphere Web Client

Note Verify that the sample descriptor file (sample_aio_descr_mandandoptional.txt) has a valid CAR license.

Edit the file using 'vi' editor and ensure that the descriptor property "prop:Car_License_Base" license is not expired.

Example:

```
prop:Car_License_Base=INCREMENT PAR-NG-TPS cisco 7.0 17-may-2015 uncounted
VENDOR_STRING=<count>1</count>
HOSTID=ANY NOTICE="<LicFileID>20150518024936834</LicFileID><LicLineID>1</LicLineID>
<PAK></PAK>" SIGN=753656C69E20
```

As in above example, if the license date has expired then provide a valid CPAR 7.0 license for this property in the .ovftool file (if the property is not present, add the property in the .ovftool file and provide a valid 7.0 license).

Procedure

Step 1 Copy the OVA descriptor configuration files as ".ovftool" to the directory where you can run the VMware ovftool command.

Note If you are running from a Linux server, the .ovftool file should not be in the root directory as it takes precedence over other ".ovftool" files.

While deploying the ova package, the home directory takes the preference over the current directory.

Step 2 **./OVAdeployer.sh** *ova-filepath/ova-file*
vi://*vcenter-user:password@vcenter-host/datacenter-name/***host/***host-folder-if-any/ucs-host*

Example:

```
./OVAdeployer.sh /tmp/RMS-All-In-One-Solution-5.1.1-1H/RMS-All-In-One-Solution-5.1.1-1H.ova

vi://myusername:mypass#1@blr-rms-vcenter1.cisco.com/BLR/host/UCS5K/blrrms-5108-09.cisco.com
./OVAdeployer.sh /tmp/RMS-Distributed-Solution-5.1.1-1H/RMS-Central-Node-5.1.1-1H.ova
```

```
vi://myusername:mypass#1@blr-rms-vcenter1.cisco.com/BLR/host/UCS5K/blrrms-5108-09.cisco.com
```

Note The OVAdeployer.sh tool first validates the OVA descriptor file and then continues to install the RMS. If necessary, get the OVAdeployer.sh tool from the build package and copy it to the directory where the OVA descriptor file is stored.

If the vCenter user or password (or both) is not specified in the command, you are prompted to enter this information on the command line. Enter the user name and password to continue.

All-in-One RMS Deployment: Example

In an all-in-one RMS deployment, all the nodes such as central, serving, and upload are deployed on a single host on the VSphere client.

In an all-in-one RMS deployment, the Serving and Upload nodes should be synchronized with the Central node during first boot up. To synchronize these nodes, add the property "powerOn=False" in the descriptor file (.ovftool).

```
./OVAdeployer.sh
/data/ova/OVA_Files/RMS51/RMS-All-In-One-Solution-5.1.1-1H/RMS-All-In-One-Solution-5.1.1-1H.ova

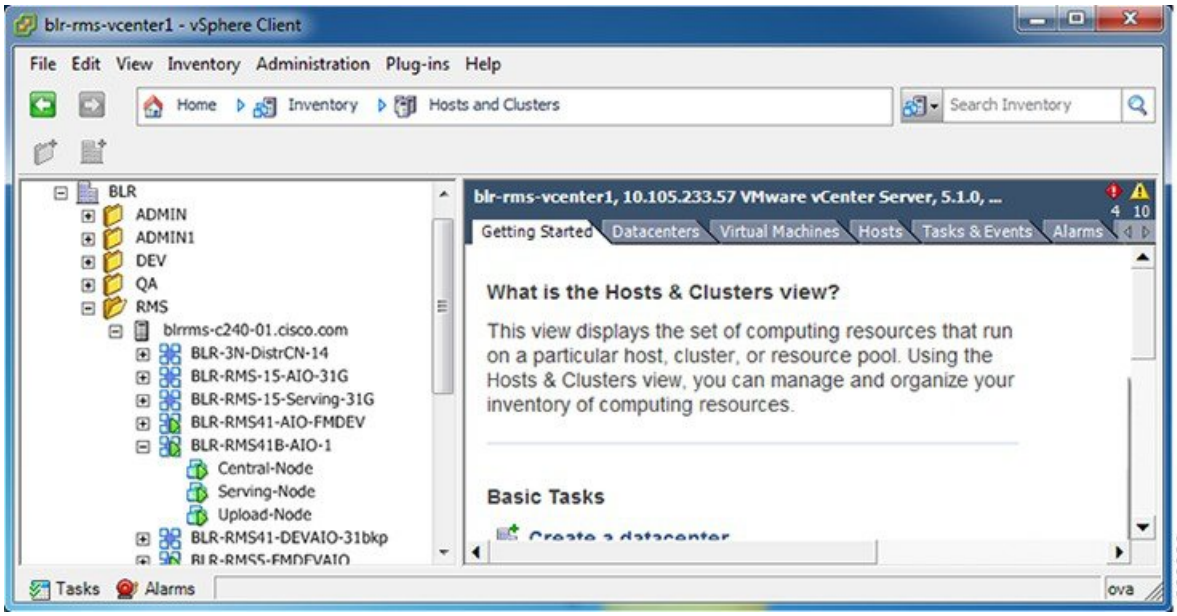
vi://root:vmware@10.105.246.84/HA/host/blrrms-c240-01.cisco.com/

Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are
recommended to
be in same VLAN for AIO/Distributed deployments with an exception for Geo Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
Starting input validation
Checking network configurations in descriptor...
Deploying OVA...
Opening OVA source:
/data/ova/OVA_Files/RMS51/RMS-All-In-One-Solution-5.1.1-1H/RMS-All-In-One-Solution-5.1.1-1H.ova
The manifest does not validate
Opening VI target: vi://root@10.105.246.84:443/HA/host/blrrms-c240-01.cisco.com/
Deploying to VI: vi://root@10.105.246.84:443/HA/host/blrrms-c240-01.cisco.com/
Transfer Completed
Powering on vApp: BLR03-AIO-51H
Completed successfully
Wed 25 Mar 2015 11:00:01 AM IST
OVA deployment took 594 seconds.
```

After OVA installation is completed, power on only the Central VM and wait until the login prompt appears on the VM console. Next, power on the Serving and Upload VMs and wait until the login prompt appears on the VM consoles.

The RMS all-in-one deployment in the vCenter appears similar to this illustration:

Figure 6: RMS All-In-One Deployment



After all hosts are powered on and the login prompt appears on the VM consoles, only then proceed with the configuration changes (example, creating groups, replacing certificates, adding route, and so on). Else, the system bring-up may overwrite your changes.

Note After installation if you see "unix_chkpwd[4773]: password check failed field for user (admin1)" error on the VMware vSphere client console on the Central node, ignore it.

Distributed RMS Deployment: Example

In the distributed deployment, RMS Nodes (Central node, Serving node, and Upload node) are deployed on different hosts on the VSphere client. The RMS nodes must be deployed and powered in the following sequence:

1. Central Node
2. Serving Node
3. Upload Node

Note Power on the Serving and Upload nodes after the Central node applications are up. To confirm this:

1. Log in to the Central node after ten minutes (from the time the nodes are powered on).
2. Switch to root user and look for the following message in the `/root/ova-first-boot.log`.

   `Central-first-boot script execution took [xxx] seconds`
   For example, Central-first-boot script execution took 360 seconds.

The .ovftool files for the distributed deployment differ slightly than that of the all-in-one deployment in terms of virtual host network values as mentioned in Preparing the OVA Descriptor Files, on page 56. Here is an example of the distributed RMS deployment:

Central Node Deployment

```
./OVAdeployer.sh
/data/ova/OVA_Files/RMS51/RMS-Distributed-Solution-5.1.1-1H/RMS-Central-Node-5.1.1-1H.ova
vi://root:vmware@10.105.246.84/HA/host/blrrms-c240-10.cisco.com

Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are
recommended to
be in same VLAN for AIO/Distributed deployments with an exception for Geo Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
Starting input validation
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Deploying OVA...
Opening OVA source:
/data/ova/OVA_Files/RMS51/RMS-Distributed-Solution-5.1.1-1H/RMS-Central-Node-5.1.1-1H.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/blrrms-c240-10.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/blrrms-c240-10.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
Completed successfully
Mon 16 Mar 2015 05:27:48 PM IST
OVA deployment took 155 seconds.
```

Serving Node Deployment

```
./OVAdeployer.sh
/data/ova/OVA_Files/RMS51/RMS-Distributed-Solution-5.1.1-1H/RMS-Serving-Node-5.1.1-1H.ova
vi://root:vmware@10.105.246.84/HA/host/blrrms-c240-10.cisco.com

Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are
recommended to
be in same VLAN for AIO/Distributed deployments with an exception for Geo Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
Starting input validation
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Deploying OVA...
Opening OVA source:
/data/ova/OVA_Files/RMS51/RMS-Distributed-Solution-5.1.1-1H/RMS-Serving-Node-5.1.1-1H.ova
```

```
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/blrrms-c240-10.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/blrrms-c240-10.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
Completed successfully
Mon 16 Mar 2015 05:36:48 PM IST
OVA deployment took 139 seconds.
```

Upload Node Deployment

```
./OVAdeployer.sh
/data/ova/OVA_Files/RMS51/RMS-Distributed-Solution-5.1.1-1H/RMS-Upload-Node-5.1.1-1H.ova
vi://root:vmware@10.105.246.84/HA/host/blrrms-c240-10.cisco.com

Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are
recommended to
be in same VLAN for AIO/Distributed deployments with an exception for Geo

Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
Starting input validation
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Deploying OVA...
Opening OVA source: /data/ova/OVA_Files/RMS51/RMS-Distributed-Solution-5.1.1-1H/RMS-Upload-

Node-5.1.1-1H.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/blrrms-c240-10.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/blrrms-c240-10.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
Completed successfully
Mon 16 Mar 2015 05:39:23 PM IST
OVA deployment took 50 seconds.
```

The RMS distributed deployment in the vSphere appears similar to this illustration:

Figure 7: RMS Distributed Deployment



Note After installation if you see "unix_chkpwd[4773]: password check failed field for user (admin1)" error on the VMware vSphere client console on the Central node, ignore it.

RMS Redundant Deployment

This section describes RMS redundant deployment modes and RMS post deployment configuration procedures.

- Deploying an All-In-One Redundant Setup, on page 66
- Migrating from a Non-Redundant All-In-One to a Redundant Setup, on page 72
- Deploying the Distributed Redundant Setup, on page 73
- Post RMS Redundant Deployment, on page 76

Deploying an All-In-One Redundant Setup

Complete the following steps for the all-in-one redundant deployment:

Before You Begin

Complete the following procedures provided in the *High Availability for Cisco RAN Management Systems* document before performing the following procedure.

- Creating a High Availability Cluster
- Adding Hosts to the High Availability Cluster
- Adding NFS Datastore to the Host
- Adding Network Redundancy for Hosts and Configuring vMotion

Procedure

Step 1 Ensure that you have the relevant sample AIO OVA descriptor (mandatory or mandatory and optional) files from the RMS-Redundant-Solution package.

Step 2 Ensure that you have the relevant installers—OVAdeployer_redundancy.sh and OVAdeployer_redundant_template.sh—for redundant deployment.

Step 3 Copy "sample_aio_descr_mandatory.txt" or "sample_aio_descr_mandandoptional.txt" as ".ovftool" and edit as per setup.
Copy "sample_aio_descr_mandatory.txt" or "sample_aio_descr_mandandoptional.txt" as ".ovftoolhotstandby" and edit as per setup.

Copy ".ovftool, .ovftoolhotstandby, .ovftoolredundantproperties" to the server where the "ovftool" utility is installed.

Step 4 Edit the following descriptors:

- .ovftool—Primary OVF descriptor for the node where all the primary components need to be deployed.
- .ovftoolhotstandby—Hot standby OVF descriptor for the Serving node and Upload node components on hot standby.
- .ovftoolredundantproperties—Priimary and hot standby properties that differ for datastore,vappname for redundant setup.

Note Descriptor file for primary and hot standby remains the same for all-in-one deployment having configured values.

Step 5 Copy the deployment files "OVAdeployer_redundant_template.sh" to "OVAdeployer_redundant.sh" and edit the file that executes redundant deployment.

```
./OVAdeployer_redundancy.sh [complete ova path(Central/Serving/Upload/All-in-one)]
[VCenterURL]
[REDUNDANTDEPPLOYMENT(PRIMARY/HOTSTANDBY)]
```

The example of the above format is given below:

Example:

```
./OVAdeployer_redundancy.sh
/data/ovf/RMS51/HA-AIO-AUG/RMS-Redundant-Solution-5.1.1-199/RMS-Serving-Node-5.1.1-199.ova

vi://rms-qa:cisco123@blr-rms-vcenter2.cisco.com/BLR1/host/HA-AIO-5108-user/blrrms-5108-03-05.cisco.com
 PRIMARY &&
./OVAdeployer_redundancy.sh
/data/ovf/RMS51/HA-AIO-AUG/RMS-Redundant-Solution-5.1.1-199/RMS-Upload-Node-5.1.1-199.ova

vi://rms-qa:cisco123@blr-rms-vcenter2.cisco.com/BLR1/host/HA-AIO-5108-user/blrrms-5108-03-05.cisco.com
 PRIMARY &&
./OVAdeployer_redundancy.sh
/data/ovf/RMS51/HA-AIO-AUG/RMS-Redundant-Solution-5.1.1-199/RMS-Serving-Node-5.1.1-199.ova

vi://rms-qa:cisco123@blr-rms-vcenter2.cisco.com/BLR1/host/HA-AIO-5108-user/blrrms-5108-03-06.cisco.com
 HOTSTANDBY &&
./OVAdeployer_redundancy.sh
/data/ovf/RMS51/HA-AIO-AUG/RMS-Redundant-Solution-5.1.1-199/RMS-Upload-Node-5.1.1-199.ova

vi://rms-qa:cisco123@blr-rms-vcenter2.cisco.com/BLR1/host/HA-AIO-5108-user/blrrms-5108-03-06.cisco.com
 HOTSTANDBY
#EOF-DONT-DELETE
```

Note New parameter PRIMARY/HOTSTANDY must be mentioned at the end of each command.

Step 6 Execute the following command to install the OVA.
Before deployment, ensure that the ".ovftool", ".ovftool_redundancy", and ".ovftoolredundantproperties" are present in the current directory.

Use these commands to change the permission of the script:

Example:
```
chmod +x ./OVAdeployer_redundant.sh;
chmod +x ./OVAdeployer_redundancy.sh
```

Use the following command to deploy the OVA:

Example:
```
./OVAdeployer_redundant.sh
```

Step 7 Detach the CD/DVD drive from the RMS nodes as follows:

a) Log in to the vSphere Web Client and locate the Central node vAPP.
b) In the Getting Started tab, click **Power Off vApp**.
c) After power off, right-click on the Central node VM and click **Edit Settings**.
d) Remove the CD/DVD drive 1 from the Virtual Hardware tab by clicking on the "X" symbol present in the same row.
e) Click **Ok** to finish.
f) Click **Edit Settings** and ensure that the CD/DVD drive 1 is removed.
g) In the Getting Started tab, select the vApp of the VM and click **Power On vApp**.
h) Repeat steps a to g on all the RMS nodes.

Note Ensure all the RMS nodes are up and running before proceeding to Step 8.

Step 8 Run the multi-node script **central-multi-nodes-config.sh** on the Central node from the path `cd /`.
This script takes an input configuration file that must contain the following properties for the redundant Serving and Upload nodes.

Prepare an input configuration file with all the following properties for the redundant Serving and Upload nodes. For example, ovadescrip.txt.

- Central_Node_Eth0_Address
- Central_Node_Eth1_Address
- Serving_Node_Eth0_Address
- Serving_Node_Eth1_Address
- Upload_Node_Eth0_Address
- Upload_Node_Eth1_Address
- Serving_Hostname
- Upload_Hostname
- Acs_Virtual_Fqdn
- Upload_SB_Fqdn

Example:

```
[RMS51G-CENTRAL03] / # ./central-multi-nodes-config.sh ovadescrip.txt
Deployment Descriptor file ovadescrip.txt found, continuing

Central_Node_Eth0_Address=10.1.0.16
Central_Node_Eth1_Address=10.105.246.53
Serving_Node_Eth0_Address=10.4.0.14
Serving_Node_Eth1_Address=10.5.0.23
Upload_Node_Eth0_Address=10.4.0.15
Upload_Node_Eth1_Address=10.5.0.24
Serving_Node_Hostname=RMS51G-SERVING05
Upload_Node_Hostname=RMS51G-UPLOAD05
Upload_SB_Fqdn=femtouls.testlab.com
Acs_Virtual_Fqdn=femtoacs.testlab.com


Verify the input, Press Cntrl-C to exit
Script will start executing in next 15 seconds
...
......10 more seconds to execute
.........5 more seconds to execute
begin configure_iptables
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
end configure_iptables
begin configure_system
end configure_system
begin configure_files
end configure_files
Script execution completed.
Verify entries in following files:
/etc/hosts
/rms/app/rms/conf/uploadServers.xml
```

Step 9 In redundant Serving node, update the following dpe.properties.

Example:

```
[root@setup29-serving2 admin1]# vi /rms/app/CSCObac/dpe/conf/dpe.properties
/server/log/2/level=Info
/server/log/perfstat/enable=enabled
/server/log/trace/dpeext/enable=enabled
/server/log/trace/dpeserver/enable=enabled
/chattyclient/service/enable=disabled

save the file.
restart dpe.
[root@setup29-serving2 admin1]# /etc/init.d/bprAgent restart dpe
```

Step 10 Complete the procedures listed in the Post RMS Redundant Deployment, on page 76 section.

What to Do Next

Complete the "Testing High Availability on the Central Node and vCenter VM" procedure provided in the *High Availability for Cisco RAN Management Systems* document:

All-In-One Redundant Deployment: Example

```
./OVAdeployer_redundant.sh
Starting input validation
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are

recommended to be in same VLAN for AIO/Distributed deployments with an exception for Geo

Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are

recommended to be in same VLAN for AIO/Distributed deployments with an exception for Geo

Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are

recommended to be in same VLAN for AIO/Distributed deployments with an exception for Geo

Redundant Setups...
Reading OVA descriptor from path: ./.ovftool
Converting OVA descriptor to unix format..
Checking deployment type
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are

recommended to be in same VLAN for AIO/Distributed deployments with an exception for Geo

Redundant Setups...
Reading OVA descriptor from path: ./.ovftoolhotstandby
Converting OVA descriptor to unix format..
Checking deployment type
prop:Admin1_Password not provided, will be taking the default value for RMS.
prop:RMS_App_Password not provided, will be taking the default value for RMS.
prop:Root_Password not provided, will be taking the default value for RMS.
Starting OVA installation. Network 1(eth0) interface of Central/Serving/Upload Nodes are

recommended to be in same VLAN for AIO/Distributed deployments with an exception for Geo

Redundant Setups...
Reading OVA descriptor from path: ./.ovftoolhotstandby
Converting OVA descriptor to unix format..
Checking deployment type
Converting OVA descriptor to unix format..
Deploying Central Node OVA...
Opening OVA source: /data/ova/OVA_Files/RMS51/RMS-Redundant-Solution-5.1.0-1G/RMS-Central-

Node-5.1.0-1G.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-

01.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-01.cisco.com
Transfer Completed
Warning:
```

```
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
 - OVF property with key: 'Acs_Virtual_Address' does not exists.
Completed successfully
Mon 02 Mar 2015 06:22:50 PM IST
OVA deployment took 276 seconds.
Converting OVA descriptor to unix format..
Deploying Serving node OVA...
Opening OVA source: /data/ova/OVA_Files/RMS51/RMS-Redundant-Solution-5.1.0-1G/RMS-Serving-

Node-5.1.0-1G.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-

01.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-01.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
 - OVF property with key: 'Acs_Virtual_Address' does not exists.
Completed successfully
Mon 02 Mar 2015 06:26:53 PM IST
OVA deployment took 519 seconds.
Converting OVA descriptor to unix format..
Deploying upload node OVA...
Opening OVA source: /data/ova/OVA_Files/RMS51/RMS-Redundant-Solution-5.1.0-1G/RMS-Upload-

Node-5.1.0-1G.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-

01.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-01.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
 - OVF property with key: 'Acs_Virtual_Address' does not exists.
Completed successfully
Mon 02 Mar 2015 06:28:49 PM IST
OVA deployment took 635 seconds.
Converting OVA descriptor to unix format..
Deploying Secondary Serving node OVA...
Opening OVA source: /data/ova/OVA_Files/RMS51/RMS-Redundant-Solution-5.1.0-1G/RMS-Serving-

Node-5.1.0-1G.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-

10.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-10.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
 - File is missing from the manifest: '.ovf'.
 - OVF property with key: 'Acs_Virtual_Address' does not exists.
Completed successfully
Mon 02 Mar 2015 06:36:16 PM IST
OVA deployment took 1082 seconds.
Converting OVA descriptor to unix format..
Deploying secondary upload node OVA...
Opening OVA source: /data/ova/OVA_Files/RMS51/RMS-Redundant-Solution-5.1.0-1G/RMS-Upload-

Node-5.1.0-1G.ova
The manifest validates
Opening VI target: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-

10.cisco.com
Deploying to VI: vi://root@10.105.246.84:443/HA/host/AIO_REDUNDANCY/blrrms-c240-10.cisco.com
Transfer Completed
Warning:
 - No manifest entry found for: '.ovf'.
```

```
 - File is missing from the manifest: '.ovf'.
 - OVF property with key: 'Acs_Virtual_Address' does not exists.
Completed successfully
Mon 02 Mar 2015 06:38:52 PM IST
OVA deployment took 1238 seconds.
```

Migrating from a Non-Redundant All-In-One to a Redundant Setup

Before You Begin

- ACS URL should mandatorily be an FQDN in an existing all-in-one setup.
- All-in-one installation should exist in the cluster configuration.

Procedure

Step 1 Complete the following procedures provided in the *High Availability for Cisco RAN Management Systems* document:

- Updating Cluster Configuration
- Adding NFS Datastore to the Host
- Adding Network Redundancy for Hosts and Configuring vMotion

Note There will be a downtime on the nodes as the host movement to the cluster will only be possible by powering off the VMs in a host.

Step 2 Add the Southbound IP of the secondary Serving and Upload nodes to the FQDN already in use.

Step 3 Proceed to install the secondary/standby Serving and Upload nodes based on the following procedure: Use the OVAdeployer.sh and the descriptors from the RMS-Distributed-Solution-5.1.0-1x package.

a) Prepare a distributed installation descriptor file for the secondary Serving and Upload nodes separately using the Preparing the OVA Descriptor Files, on page 56 procedure.
b) Proceed with the distributed redundant installation using the Deploying the Distributed Redundant Setup, on page 73 procedure.

Step 4 Complete all the procedures listed in the Post RMS Redundant Deployment, on page 76 section.

Step 5 Complete the following post OVA installation procedures listed in the *High Availability for Cisco RAN Management Systems* document:

- Updating Cluster Configuration
- Migrating Central node to the NFS datastore

Step 6 Verify the high availability on the Central node and vCenter VM in the newly formed setup using the "Testing High Availability on the Central Node and vCenter VM" procedure provided in the *High Availability for Cisco RAN Management Systems* document.

Step 7 Add the appropriate certificates (copy the same dpe.keystore and uls.keystore from primary Serving and Upload nodes) to the newly installed secondary or standby Serving and Upload nodes.

Step 8 Execute the `configure_PNR_hnbgw.sh` and `configure_PAR_hnbgw.sh scripts` from `/rms/ova/scripts/post_install/HNBGW` directory as mentioned in the Installation Tasks Post-OVA

Deployment, on page 105 section to configure the HNB GW details on the secondary or standby PNR and PAR.

Step 9 Verify the provisioning of an existing AP and a newly registered AP with two Serving and Upload nodes on successful completion of the previous steps.

Deploying the Distributed Redundant Setup

To mitigate Serving node and Upload Server Node deployment failover, additional Serving and Upload nodes can be configured with the same Central node.

This procedure describes how to configure additional Serving and Upload nodes with an existing Central node.

Note Redundant deployment does not mandate having both Serving and Upload nodes together. Each redundant node can be deployed individually without having the other node in the setup.

Before You Begin

- It is mandatory for the ACS URL and Upload URL (Upload_SB_Fqdn and Acs_Virtual_Fqdn) to be an FQDN before deploying a distributed redundant setup.
- The ACS and Upload FQDN should be the same on both Serving and Upload nodes respectively. Example, `prop:Acs_Virtual_Fqdn=femtoacs.testlab.com` and `prop:Upload_SB_Fqdn=femtouls.testlab.com`

Procedure

Step 1 Prepare the deployment descriptor (.ovftool file) for any additional Serving nodes as described in Preparing the OVA Descriptor Files, on page 56.
For Serving node redundancy, the descriptor file should have the same provisioning group as the primary Serving node.

For an example on redundant OVA descriptor file, refer to Example Descriptor File for Redundant Serving/Upload Node, on page 283.

The following properties are different in the redundant Serving node and redundant Upload node descriptor files:

Redundant Serving Node:

- name
- Serving_Node_Eth0_Address
- Serving_Node_Eth1_Address
- Serving_Hostname
- Dpe_Cnrquery_Client_Socket_Address (should be same as Serving_Node_Eth0_Address)

- Serving_Node_Eth0_Subnet
- Serving_Node_Eth1_Subnet
- Serving_Node_Gateway
- Upload_Node_Eth0_Address
- Upload_Node_Eth0_Subnet
- Upload_Node_Eth1_Address
- Upload_Node_Eth1_Subnet
- Upload_Node_Dns1_Address
- Upload_Node_Dns2_Address
- Upload_Node_Gateway
- Upload_SB_Fqdn
- Upload_Hostname

Redundant Upload Node:

- name
- Upload_Node_Eth0_Address
- Upload_Node_Eth1_Address
- Upload_Hostname
- Dpe_Cnrquery_Client_Socket_Address (should be same as Serving_Node_Eth0_Address)
- Upload_Node_Eth0_Subnet
- Upload_Node_Eth1_Subnet
- Upload_Node_Gateway
- Serving_Node_Eth0_Address
- Serving_Node_Eth0_Subnet
- Serving_Node_Eth1_Address
- Serving_Node_Eth1_Subnet
- Serving_Node_Dns1_Address
- Serving_Node_Dns2_Address
- Serving_Node_Gateway
- Serving_Hostname

Step 2 Run a multi-node script on the Central node before deploying the redundant Serving node and redundant Upload node.
This script takes an input configuration file that must contain the following properties for the redundant Serving and Upload nodes.

Prepare an input configuration file with all the following properties for the redundant Serving and Upload nodes and name it appropriately. For example, ovadescriptorfile_CN_Config.txt.

- Central_Node_Eth0_Address
- Central_Node_Eth1_Address
- Serving_Node_Eth0_Address
- Serving_Node_Eth1_Address
- Upload_Node_Eth0_Address
- Upload_Node_Eth1_Address
- Serving_Hostname
- Upload_Hostname
- Acs_Virtual_Fqdn
- Upload_SB_Fqdn

Step 3 Copy and upload the above ovf file **ovadescriptorfile_CN_Config.ovf** and save it as .txt (**ovadescriptorfile_CN_Config.txt**) on the Central node at / directory.

Step 4 Take a back up of the **/rms/app/rms/conf/uploadServers.xml** and **/etc/hosts** using these commands:
cp /etc/hosts /etc/hosts_orig

cp /rms/app/rms/conf/uploadServers.xml /rms/app/rms/conf/uploadServers.xml_orig

Step 5 Execute as "root" user the utility shell script (**central-multi-nodes-config.sh**) to configure the network and application properties on the Central node.
The script is located in the / directory. The above copied configuration text file **ovadescriptorfile_CN_Config.txt** should be given as input to the shell script.

Example:
```
./central-multi-nodes-config.sh <deploy-decsr-filename>
```

After execution of the script, a new **fqdn/ip** entry for the new Upload Server node is created in the **/rms/app/rms/conf/uploadServers.xml** file.

Example:
```
[RMS51G-CENTRAL03] / # ./central-multi-nodes-config.sh ovadescrip.txt
Deployment Descriptor file ovadescrip.txt found, continuing

Central_Node_Eth0_Address=10.1.0.16
Central_Node_Eth1_Address=10.105.246.53
Serving_Node_Eth0_Address=10.4.0.14
Serving_Node_Eth1_Address=10.5.0.23
Upload_Node_Eth0_Address=10.4.0.15
Upload_Node_Eth1_Address=10.5.0.24
Serving_Node_Hostname=RMS51G-SERVING05
Upload_Node_Hostname=RMS51G-UPLOAD05
Upload_SB_Fqdn=femtouls.testlab.com
Acs_Virtual_Fqdn=femtoacs03.testlab.com


Verify the input, Press Cntrl-C to exit
Script will start executing in next 15 seconds
...
......10 more seconds to execute
```

```
.........5 more seconds to execute
begin configure_iptables
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
end configure_iptables
begin configure_system
end configure_system
begin configure_files
end configure_files
Script execution completed.
Verify entries in following files:
/etc/hosts
/rms/app/rms/conf/uploadServers.xml
```

Step 6 Create an individual ovf file based on the redundant Serving node or Upload node as described in Step 1 and use the same for deployment. Install additional Serving and Upload nodes as described in Deploying the RMS Virtual Appliance, on page 61.
Complete the following procedures before proceeding to the next step:

- Installing RMS Certificates, on page 109
- Enabling Communication for VMs on Different Subnets, on page 121
- Configuring Default Routes for Direct TLS Termination at the RMS, on page 122

Step 7 Specify route and IPtable configurations to establish a proper inter-node communication after deploying redundant Serving and Upload nodes based on the subnet of the new nodes. For configuring geo-redundant Serving and Upload nodes, see Configuring Serving and Upload Nodes on Different Subnets, on page 76.

Step 8 Configure the Serving node redundancy as described in Configuring Redundant Serving Nodes, on page 80.

Note Redundant Upload node needs no further configuration.

Post RMS Redundant Deployment

This section covers the procedures required to be performed after RMS deployment.

- Configuring Serving and Upload Nodes on Different Subnets, on page 76
- Configuring Fault Manager Server for Central and Upload Nodes on Different Subnets
- Configuring Redundant Serving Nodes, on page 80
- Configuring the Security Gateway on the ASR 5000 for Redundancy, on page 85
- Configuring the HNB Gateway for Redundancy, on page 89
- Configuring DNS for Redundancy, on page 91

Configuring Serving and Upload Nodes on Different Subnets



Note This section is applicable only if the Serving and Upload nodes have eth0 (NB) interface on a different subnet than that of the Central server eth0 IP.

In a multi-site configuration, due to geo-redundancy the Serving and Upload server on site2 (redundant site) can be deployed with eth0/eth1 IPs being on a different subnet compared to the eth0/eth1 IPs of site1 Central, Serving, and Upload servers. In such cases, a post-installation script must be executed on site2 Serving and Upload servers. Follow the procedure to execute this post-installation script.

In a geo-redundant setup, Serving and Upload nodes can be deployed in a different geographical location with IPs (eth0/eth1) in different subnets compared to that of the Central server (eth0/eth1) IP. In such cases, a post-installation script must be executed on the Serving and Upload nodes. Follow this procedure to execute this post-installation script.

Procedure

Step 1 Follow these steps on the Serving node deployed in a different subnet:

a) Post RMS installation, configure appropriate routes on Serving node to communicate with the Central node. For more information, see Enabling Communication for VMs on Different Subnets, on page 121.

Note Start the VM first if the powerOn is set to 'false' in the descriptor file. Else adding routes is not possible.

b) Log in to the Serving node as admin user from the Central node.

c) Switch to root user using the required credentials.

d) Navigate to /rms/ova/scripts/post_install/.

e) Copy the Serving node OVA descriptor to a temporary directory or /home/admin1 and specify the complete path during script execution.

f) Switch back to post_install directory: /rms/ova/scripts/post_install/

g) Run the following commands:

```
chmod +x redundant-serving-config.sh;
    ./redundant-serving-config.sh <diff_subnet_serving_ova_descriptor_filepath>
```

Example:

```
[root@blrrms-serving-19-2 post_install]# ./redundant-serving-config.sh ovftool_serving2
Deployment Descriptor file ovftool_serving2 found, continuing

INFO: Admin1_Username has no value, setting to default

Enter Password for admin user  admin1 on Central Node:
Confirm admin1 Password:
Enter Password for root on Central Node:
Confirm root Password: Function validateinputs starts at  1424262225

INFO: RMS_App_Password has no value, setting to default
INFO: Bac_Provisioning_Group has no value, setting to default
INFO: Ntp2_Address has no value, setting to default
INFO: Ntp3_Address has no value, setting to default
INFO: Ntp4_Address has no value, setting to default
INFO: Ip_Timing_Server_Ip has no value, setting to default
Starting ip input validation
Done ip input validation
Central_Node_Eth0_Address=10.5.1.208
Serving_Node_Eth1_Address=10.5.5.68
Upload_Node_Eth1_Address=10.5.5.69
Upload_SB_Fqdn=femtolus19.testlab.com
Acs_Virtual_Fqdn=femtoacs19.testlab.com

USEACE=
Admin1_Username=admin1
Bac_Provisioning_Group=pg01
Ntp1_Address=10.105.233.60
Ntp2_Address=10.10.10.2
Ntp3_Address=10.10.10.3
Ntp4_Address=10.10.10.4
Ip_Timing_Server_Ip=10.10.10.4
```

```
Verify the input, Press Cntrl-C to exit
Script will start executing in next 15 seconds
...
......10 more seconds to execute
.........5 more seconds to execute
Function configure_dpe_certs starts at  1424262242
Setting RMS CA signed DPE keystore
spawn scp admin1@10.5.1.208:/rms/data/rmsCerts/dpe.keystore
/rms/app/CSCObac/dpe/conf/dpe.keystore
The authenticity of host '10.5.1.208 (10.5.1.208)' can't be established.
RSA key fingerprint is d5:fc:1a:af:c8:e0:f7:3a:10:10:4b:22:b6:3c:f2:95.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.5.1.208' (RSA) to the list of known hosts.
yes
admin1@10.5.1.208's password:
Permission denied, please try again.
admin1@10.5.1.208's password:
dpe.keystore
                                                                                100% 3959
   3.9KB/s   00:00
Performing additional DPE configurations..
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

blrrms-serving-19-2 BAC Device Provisioning Engine


User Access Verification

Password:

blrrms-serving-19-2> enable
Password:
blrrms-serving-19-2# log level 6-info
% OK
.
.
.

File: ../ga_kiwi_scripts/addBacProvisionProperties.kiwi
Finished tests in 13990ms
Total Tests Run    - 16
Total Tests Passed - 16
Total Tests Failed - 0
Output saved in file: /tmp/runkiwi.sh_root/addBacProvisionProperties.out.20150218_1755

_____________________________________________________________________________

Post-processing log for benign error codes:
/tmp/runkiwi.sh_root/addBacProvisionProperties.out.20150218_1755

Revised Test Results
  Total Test Count: 16
      Passed Tests: 16
   Benign Failures: 0
  Suspect Failures: 0

Output saved in file:
/tmp/runkiwi.sh_root/addBacProvisionProperties.out.20150218_1755-filtered
~
[blrrms-central-19] ~ # Done provisioning group configuration
[root@blrrms-serving-19-2 post_install]#
```

Step 2 Follow these steps on the Upload node deployed in a different subnet:

a) Log in to the Upload server (having its IPs in a different subnet) as admin user.

b) Switch to root user using the required credentials.

c) Navigate to /rms/ova/scripts/post_install/.

d) Copy the different subnet Upload server OVA descriptor file to a temporary location or home directory and use this path during script execution.

e) Run the following commands to execute the script:

```
chmod +x redundant-upload-config.sh;
    ./redundant-upload-config.sh <diff_subnet_upload_ova_descriptor_filepath>
```

Example:

```
[root@blr-blrrms-lus-19-2 post_install]# ./redundant-upload-config.sh
/home/admin1/ovftool_upload2
Deployment Descriptor file /home/admin1/ovftool_upload2 found, continuing

INFO: Admin1_Username has no value, setting to default

Enter Password for admin user  admin1 on Central Node:
Confirm admin1 Password: Function validateinputs starts at  1424263071

Starting ip input validation
Done ip input validation
Central_Node_Eth0_Address=10.5.1.208
Upload_Node_Eth0_Address=10.5.4.69
Admin1_Username=admin1

Verify the input, Press Cntrl-C to exit
Script will start executing in next 15 seconds
...
......10 more seconds to execute
.........5 more seconds to execute
Function configure_dpe_certs starts at  1424263088
Setting RMS CA signed LUS keystore
spawn scp admin1@10.5.1.208:/rms/data/rmsCerts/uls.keystore /opt/CSCOuls/conf/uls.keystore
The authenticity of host '10.5.1.208 (10.5.1.208)' can't be established.
RSA key fingerprint is d5:fc:1a:af:c8:e0:f7:3a:10:10:4b:22:b6:3c:f2:95.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.5.1.208' (RSA) to the list of known hosts.
yes
admin1@10.5.1.208's password:
Permission denied, please try again.
admin1@10.5.1.208's password:
uls.keystore
                                                                              100% 3960
   3.9KB/s   00:00
[root@blr-blrrms-lus-19-2 post_install]#
```

Note that the scripts can be rerun if any error is observed. For example, wrong password input for admin user/root.

Configuring Fault Manager Server for Redundant Upload Node

During Central node installation, IPtables for enabling communication between the Central node and Upload server are added for the first upload server (whose IPs are present in the Central node descriptor file). If there are redundant Upload servers, follow these steps on the Central node to manually add IPtable rules to enable communication between the Central node and redundant Upload nodes.

Procedure

Step 1 Log in to the Central node as admin user.

Step 2 Switch to root user.

Step 3 Add the below IPtable entries with the Central node and redundant Upload server IPs to allow communication between them (repeat this step for all the redundant Upload nodes).

```
iptables -A INPUT -p tcp -i eth0 -s <Redundant_Upload_Node_Eth0_Address> -d
<Central_Node_Eth0_Address> --dport 8084 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 -s <Central_Node_Eth0_Address> -d
<Redundant_Upload_Node_Eth0_Address> --sport 8084 -m state --state NEW -j ACCEPT
```

Example:

```
iptables -A INPUT -p tcp -i eth0 -s 10.4.0.12 -d 10.1.0.10 --dport 8084 -m state
--state NEW -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 -s 10.1.0.10 -d 10.4.0.12 --sport 8084 -m state --state
NEW -j ACCEPT
```

Step 4 Save the changes on the Central node by using the following command:

```
service iptables save
```

Step 5 Restart IPtables on the Central node by using the following command:

```
service iptables restart
```

Configuring Redundant Serving Nodes

The RMS Serving nodes are configured as redundant pairs using the **redundant-serving-pnr-config.sh** script.

After the installation of primary and secondary serving node, script will be found under the location `/rms/ova/scripts/redundancy/` for both primary and secondary Serving nodes

The **redundant-serving-pnr-config.sh** script configures the following on the primary and secondary Serving node:

- Deletes any existing IPtable firewall rules for the ports
- Creates or updates the IPtable firewall rules.
- Creates or updates the IPtable firewall rules for the ports 61610 , 61611 , 1234 , and 647.
- Configures PNRs for redundancy.

The following sections describe how to configure and verify redundancy on the primary and secondary Serving node or PNR.

- Configuring Primary Serving Node or PNR Redundancy, on page 81
- Configuring Secondary Serving Node or PNR Redundancy, on page 83
- Verifying Secondary Serving Node or PNR Redundancy, on page 85

Configuring Primary Serving Node or PNR Redundancy

Procedure

Step 1 Log in to the primary Serving Node as 'admin' user.

```
ssh <Primary_Serving_Node_eth0_IP>
```

Step 2 Change to root user: **su-**

Step 3 Navigate to the directory `/rms/ova/scripts/redundancy/`. Update the IP table firewall rules on the primary Serving node to enable the Serving nodes to communicate.

Step 4 Input the values as per the setup details for the Serving nodes as eth0/eth1 IPs and save the file.

```
# Sample Input File for Redundant Serving node configuration

Serving_Node_Primary_Eth0_Address=10.5.1.24
Serving_Node_Secondary_Eth0_Address=10.5.1.20
Serving_Node_Primary_Eth1_Address=10.5.2.24
Serving_Node_Secondary_Eth1_Address=10.5.2.20
```

Step 5 Run the redundancy configuration script, "redundant-serving-pnr-config.sh" as follows:

```
Redundant-serving-pnr-config.sh –i input_file
```

The script prompts the user with the option, “Is the current serving node acting as the primary serving node for RMS Redundancy setup ? [y/n]”. Answer with “y” because the script is executed on the primary Serving node. The script then prompts to specify the 'cnradmin' password.

Example:

```
[root@blrrms-serving-1]#cd /rms/ova/scripts/redundancy/
[root@blrrms-serving-1]#chmod +x redundant-serving-pnr-config.sh
[[root@blrrms-serving-14-2I redundancy]# ./redundant-serving-pnr-config.sh -i
config.redundancy
User : root

Detected RMS Serving Node .
Serving_Node_Primary_Eth0_Address=10.5.1.68
Serving_Node_Primary_Eth1_Address=10.5.2.68
Serving_Node_Secondary_Eth0_Address=10.5.1.72
Serving_Node_Secondary_Eth1_Address=10.5.2.72
Is the current serving node acting as the primary serving node for RMS Redundancy setup ?
[y/n]
y
Configuring Firewall
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Configuring the PNR for Redundancy
Enter cnradmin Password: 109 Ok - resource status is Critical: 1, OK: 8
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd> ################################################################################

nrcmd> #

nrcmd> # csrc_cnr_enable_extpts.nrcmd

nrcmd> # This is a configuration script to be run in Network Registrar's nrcmd.
```

```
nrcmd> # This script enables the CSRC BPR CNR extension points.  It is mandatory that

nrcmd> # this script be run prior to running CSRC BPR.  Modify the reference to

nrcmd> # CSRC_HOME to point to a valid CSRC BPR home directory (don't forget to

nrcmd> # backquote the directory seperators).
.
.
.

nrcmd>
nrcmd> # Display results

nrcmd> extension list
100 Ok - 3 objects found
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
extclientid:
    entry = clientID_trace
    file = libtrace_clientid.so
    init-args =
    init-entry =
    lang = Dex
    name = extclientid
preClientLookup:
    entry = bprClientLookup
    file = libbprextensions.so
    init-args = BPR_HOME=/rms/app/CSCObac,BPR_DATA=/rms/data/CSCObac
    init-entry = bprInit
    lang = Dex
    name = preClientLookup

nrcmd> dhcp listExtensions
100 Ok
post-packet-decode:      1 dexdropras
                         2 extclientid
pre-packet-encode:
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>
nrcmd> # Save

nrcmd> save
100 Ok

nrcmd> 109 Ok - resource status is Critical: 1, OK: 8
100 Ok
109 Ok - resource status is Critical: 1, OK: 8
PNR console output logged in 'pnr-console-out.log' file
Done
```

Configuring Secondary Serving Node or PNR Redundancy

Procedure

Step 1 Log in to the secondary Serving Node as 'admin' user.

```
ssh <Secondary_Serving_Node_eth0_IP>
```

Step 2 Change to root user: **su-**

Step 3 Navigate to the directory `/rms/ova/scripts/redundancy/`. Open and edit the sample input file "config.redundancy".

```
# Sample Input File for Redundant Serving node configuration

Serving_Node_Primary_Eth0_Address=10.5.1.24
Serving_Node_Secondary_Eth0_Address=10.5.1.20
Serving_Node_Primary_Eth1_Address=10.5.2.24
Serving_Node_Secondary_Eth1_Address=10.5.2.20
```

Step 4 Input the values as per the setup details for the Serving nodes as eth0/eth1 IPs and save the file.

Step 5 Run the redundancy configuration script, "redundant-serving-pnr-config.sh" as follows:

```
Redundant-serving-pnr-config.sh –I <input_file>
```

The script prompts the user with the option, “Is the current serving node acting as the primary serving node for RMS Redundancy setup ? [y/n]”. Answer with "n" because the script is executed on the secondary Serving node. The script then prompts to specify the 'cnradmin' password.

Example:

```
[root@blr-rms15-serving redundancy]# ./redundant-serving-pnr-config.sh -i config.redundancy

User : root

Detected RMS Serving Node .
Serving_Node_Primary_Eth0_Address=10.5.1.68
Serving_Node_Primary_Eth1_Address=10.5.2.68
Serving_Node_Secondary_Eth0_Address=10.5.1.72
Serving_Node_Secondary_Eth1_Address=10.5.2.72
Is the current serving node acting as the primary serving node for RMS Redundancy setup ?
[y/n]
n
Configuring Firewall
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Configuring the PNR for Redundancy

Enter cnradmin Password: 109 Ok - resource status is Critical: 1, OK: 8
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd> ################################################################################

nrcmd> #

nrcmd> # csrc_cnr_enable_extpts.nrcmd

nrcmd> # This is a configuration script to be run in Network Registrar's nrcmd.
```

```
nrcmd> # This script enables the CSRC BPR CNR extension points.  It is mandatory that

nrcmd> # this script be run prior to running CSRC BPR.  Modify the reference to

nrcmd> # CSRC_HOME to point to a valid CSRC BPR home directory (don't forget to

nrcmd> # backquote the directory seperators).
.
.
.

nrcmd>
nrcmd> # Display results

nrcmd> extension list
100 Ok - 3 objects found
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
extclientid:
    entry = clientID_trace
    file = libtrace_clientid.so
    init-args =
    init-entry =
    lang = Dex
    name = extclientid
preClientLookup:
    entry = bprClientLookup
    file = libbprextensions.so
    init-args = BPR_HOME=/rms/app/CSCObac,BPR_DATA=/rms/data/CSCObac
    init-entry = bprInit
    lang = Dex
    name = preClientLookup

nrcmd> dhcp listExtensions
100 Ok
post-packet-decode:      1 dexdropras
                         2 extclientid
pre-packet-encode:
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>
nrcmd> # Save

nrcmd> save
100 Ok

nrcmd> 109 Ok - resource status is Critical: 1, OK: 8
100 Ok
109 Ok - resource status is Critical: 1, OK: 8
PNR console output logged in 'pnr-console-out.log' file
Done
```

Verifying Secondary Serving Node or PNR Redundancy

Procedure

Step 1 Log in to the secondary Serving Node as 'admin' user.
```
ssh <Secondary_Serving_Node_eth0_IP>
```

Step 2 Change to root user: **su-**

Step 3 Log in to the PNR prompt using the following command and enter the password when prompted:
/rms/app/nwreg2/local/usrbin/nrcmd -N cnradmin

Step 4 Verify that the primary and secondary Serving nodes are communicating with each other in a redundant setup using the following command.
```
nrcmd> dhcp getRelatedServers
```
In the output, verify that "Communications" is "OK", "State" is "NORMAL", "Partner Role" is "MAIN", and "Partner State" is "NORMAL" in the row where Type is "MAIN".

Output:

```
nrcmd> dhcp getRelatedServers
100 Ok
Type Name Address Requests Communications State Partner
Role Partner State
MAIN -- 10.5.1.24 0 OK NORMAL MAIN
NORMAL
TCP-L blrrms-Serving-02.cisco.com 10.5.1.20,61610 0 NONE listening --
--
```

Step 5 Proceed to execute the **configure_PAR_hnbgw.sh** to configure all the radius clients on the secondary Serving node.

Configuring the Security Gateway on the ASR 5000 for Redundancy

Procedure

Step 1 Log in to the Cisco ASR 5000 that contains the HNB and security gateways.

Step 2 Check the context name for the security gateway: **show context all**.

Step 3 Display the HNB gateway configuration: **show configuration context** *security_gateway_context_name*.
Verify that there are two DHCP server addresses configured. See the highlighted text in the example.

Example:

```
[local]blrrms-xt2-03# show configuration context HNBGW

context HNBGW
  ip pool ipsec range 7.0.1.48 7.0.1.63 public 0 policy allow-static-allocation
  ipsec transform-set ipsec-vmct
  #exit
  ikev2-ikesa transform-set ikesa-vmct
  #exit
  crypto template vmct-asr5k ikev2-dynamic
```

```
  authentication local certificate
  authentication remote certificate
  ikev2-ikesa transform-set list ikesa-vmct
  keepalive interval 120
  payload vmct-sa0 match childsa match ipv4
    ip-address-alloc dynamic
    ipsec transform-set list ipsec-vmct
    tsr start-address 10.5.1.0 end-address 10.5.1.255
  #exit
  nai idr 10.5.1.91 id-type ip-addr
  ikev2-ikesa keepalive-user-activity
  certificate 10-5-1-91
  ca-certificate list ca-cert-name TEF_CPE_SubCA ca-cert-name Ubi_Cisco_Int_ca
#exit
interface Iu-Ps-Cs-H
  ip address 10.5.1.91 255.255.255.0
  ip address 10.5.1.92 255.255.255.0 secondary
  ip address 10.5.1.93 255.255.255.0 secondary
#exit
subscriber default
  dhcp service CNR context HNBGW
  ip context-name HNBGW
  ip address pool name ipsec
exit
radius change-authorize-nas-ip 10.5.1.92 encrypted key
       +A1rxtnjd9vom7g1ugk4buohqxtt073pbivjonsvn3olnz2wsl0sm5
       event-timestamp-window 0 no-reverse-path-forward-check
aaa group default
  radius max-retries 2
  radius max-transmissions 5
  radius timeout 1
  radius attribute nas-ip-address address 10.5.1.92
  radius server 10.5.1.20 encrypted key
     +A3qji4gwxyne5y3s09r8uzi5ot70fbyzzzzgbso92ladvtv7umjcj
     port 1812 priority 2
  radius server 1.4.2.90 encrypted key
     +A1z4194hjj9zvm24t0vdmob18b329iod1jj76kjh1pzsy3w46m9h4
     port 1812 priority 1
#exit
gtpp group default
#exit
gtpu-service GTPU_FAP_1
  bind ipv4-address 10.5.1.93
exit
  dhcp-service CNR
  dhcp client-identifier ike-id
  dhcp server 10.5.1.20
  dhcp server 10.5.1.24
  no dhcp chaddr-validate
  dhcp server selection-algorithm use-all
  dhcp server port 61610
  bind address 10.5.1.92
#exit
dhcp-server-profile CNR
#exit
hnbgw-service HNBGW_1
  sctp bind address 10.5.1.93
  sctp bind port 29169
  associate gtpu-service GTPU_FAP_1
  sctp sack-frequency 5
  sctp sack-period 5
  no sctp connection-timeout
  no ue registration-timeout
  hnb-identity oui discard-leading-char
  hnb-access-mode mismatch-action accept-aaa-value
  radio-network-plmn mcc 116 mnc 116
    rnc-id 116
  security-gateway bind address 10.5.1.91 crypto-template vmct-asr5k context HNBGW
#exit
ip route 0.0.0.0 0.0.0.0 10.5.1.1 Iu-Ps-Cs-H
ip route 10.5.3.128 255.255.255.128 10.5.1.1 Iu-Ps-Cs-H
ip igmp profile default
```

```
  #exit
#exit
end
```

Step 4 If the second DHCP server is not configured, run these commands to configure it:

a) **configure**

b) **context HNBGW**

c) **dhcp-service CNR**

d) **dhcp server** <*dhcp-server-2-IP-Addr* >

e) **dhcp server selection-algorithm use-all**

Verify that the second DHCP server is configured by examining the output from this step.

Note Exit from the config mode and view the DHCP IP.

Example:

```
[local]blrrms-xt2-03# configure
[local]blrrms-xt2-03(config)# context HNBGW
[HNBGW]blrrms-xt2-03(config-ctx)#  dhcp-service CNR
[HNBGW]blrrms-xt2-03(config-dhcp-service)# dhcp server 1.1.1.1
[HNBGW]blrrms-xt2-03(config-dhcp-service)# dhcp server selection-algorithm use-all
```

Step 5 To view the changes, execute the following command:

```
[local]blrrms-xt2-03# show configuration context HNBGW
```

Step 6 Save the changes by executing the following command:

```
[local]blrrms-xt2-03# save config /flash/xt2-03-aug12
```

Note The saved filename can be as per your choice. For example, xt2-03-aug12.

Configuring the Security Gateway on ASR 5000 for Multiple Subnet or Geo-Redundancy

In a different subnet or geo-redundant deployment, it is expected that the Serving and Upload nodes are deployed with IPs on a different subnet. The new subnet therefore needs to be allowed in the IPsec traffic selector on the Security Gateway (SeGW).

In a deployment where the SeGW (ASR 5000) and RMS are on the same subnet, the output of the HNB GW is displayed as follows (the single subnet information is highlighted below):

```
[local]blrrms-xt2-03# show configuration context HNBGW
context HNBGW
ip pool ipsec range 7.0.1.48 7.0.1.63 public 0 policy allow-static-allocation
ipsec transform-set ipsec-vmct
#exit
ikev2-ikesa transform-set ikesa-vmct
#exit
crypto template vmct-asr5k ikev2-dynamic
authentication local certificate
authentication remote certificate
ikev2-ikesa transform-set list ikesa-vmct
keepalive interval 120
payload vmct-sa0 match childsa match ipv4
ip-address-alloc dynamic
ipsec transform-set list ipsec-vmct
tsr start-address 10.5.1.0 end-address 10.5.1.255
#exit
```

Follow the below steps to check and add the different subnet in the IPSec traffic selector of the SeGW (ASR 5000):

Procedure

Step 1 Log in to the Cisco ASR 5000 that contains the HNB and security gateways.

Step 2 Check the context name for the security gateway: **show context all**.

Step 3 Display the HNB gateway configuration: **show configuration context** *security_gateway_context_name*.

Step 4 Update the SeGW (ASR 5000) configuration with the additional subnet using the following command:
tsr start-address <new subnet start IP address> end-address <new subnet end IP address>
Example: For example, .

```
tsr start-address 10.5.4.0 end-address 10.5.4.255
[local]blrrms-xt2-19# configure
[local]blrrms-xt2-19(config)# context HNBGW
[HNBGW]blrrms-xt2-19(config-ctx)# crypto template vmct-asr5k ikev2-dynamic
[HNBGW]blrrms-xt2-19(cfg-crypto-tmpl-ikev2-tunnel)# payload vmct-sa0 match childsa match
ipv4
[HNBGW]blrrms-xt2-19(cfg-crypto-tmpl-ikev2-tunnel-payload)# tsr start-address 10.5.4.0
end-address 10.5.4.255
[HNBGW]blrrms-xt2-19(cfg-crypto-tmpl-ikev2-tunnel-payload)# exit
[HNBGW]blrrms-xt2-19(cfg-crypto-tmpl-ikev2-tunnel)# exit
[HNBGW]blrrms-xt2-19(config-ctx)# exit
[HNBGW]blrrms-xt2-19(config)# exit
[local]blrrms-xt2-19# save config /flash/xt2-03-aug12
Are you sure? [Yes|No]: yes
[local]blrrms-xt2-19#
```

Step 5 Verify the updated SeGW configuration using the command:
show configuration context *security_gateway_context_name*
The updated output is highlighted below:

```
[local]blrrms-xt2-03# show configuration context HNBGW
config
context HNBGW
ip pool ipsec range 7.0.1.48 7.0.1.63 public 0 policy allow-static-allocation
ipsec transform-set ipsec-vmct
#exit
ikev2-ikesa transform-set ikesa-vmct
#exit
crypto template vmct-asr5k ikev2-dynamic
authentication local certificate
authentication remote certificate
ikev2-ikesa transform-set list ikesa-vmct
keepalive interval 120
payload vmct-sa0 match childsa match ipv4
ip-address-alloc dynamic
ipsec transform-set list ipsec-vmct
tsr start-address 10.5.1.0 end-address 10.5.1.255
tsr start-address 10.5.4.0 end-address 10.5.4.255
#exit
```

Configuring the HNB Gateway for Redundancy

Procedure

Step 1 Log in to the HNB gateway.

Step 2 Display the configuration context of the HNB gateway so that you can verify the radius information: **show configuration context** *HNBGW_context_name*

If the radius parameters are not configured as shown in this example, configure them as in this procedure.

Example:

```
[local]blrrms-xt2-03# show configuration context HNBGW

  context HNBGW
    ip pool ipsec range 7.0.1.48 7.0.1.63 public 0 policy allow-static-allocation
    ipsec transform-set ipsec-vmct
    #exit
    ikev2-ikesa transform-set ikesa-vmct
    #exit
    crypto template vmct-asr5k ikev2-dynamic
      authentication local certificate
      authentication remote certificate
      ikev2-ikesa transform-set list ikesa-vmct
      keepalive interval 120
      payload vmct-sa0 match childsa match ipv4
        ip-address-alloc dynamic
        ipsec transform-set list ipsec-vmct
        tsr start-address 10.5.1.0 end-address 10.5.1.255
      #exit
      nai idr 10.5.1.91 id-type ip-addr
      ikev2-ikesa keepalive-user-activity
      certificate 10-5-1-91
      ca-certificate list ca-cert-name TEF_CPE_SubCA ca-cert-name Ubi_Cisco_Int_ca
    #exit
    interface Iu-Ps-Cs-H
      ip address 10.5.1.91 255.255.255.0
      ip address 10.5.1.92 255.255.255.0 secondary
      ip address 10.5.1.93 255.255.255.0 secondary
    #exit
    subscriber default
      dhcp service CNR context HNBGW
      ip context-name HNBGW
      ip address pool name ipsec
    exit
    radius change-authorize-nas-ip 10.5.1.92 encrypted key
                +A1rxtnjd9vom7g1ugk4buohqxtt073pbivjonsvn3olnz2wsl0sm5
                event-timestamp-window 0 no-reverse-path-forward-check
    aaa group default
      radius max-retries 2
      radius max-transmissions 5
      radius timeout 1
      radius attribute nas-ip-address address 10.5.1.92
      radius server 10.5.1.20 encrypted key
+A3qji4gwxyne5y3s09r8uzi5ot70fbyzzzzgbso92ladvtv7umjcj
                port 1812 priority 2
      radius server 1.4.2.90 encrypted key
+A1z4194hjj9zvm24t0vdmob18b329iod1jj76kjh1pzsy3w46m9h4
                port 1812 priority 1
    #exit
    gtpp group default
    #exit
    gtpu-service GTPU_FAP_1
      bind ipv4-address 10.5.1.93
```

```
    exit
    dhcp-service CNR
      dhcp client-identifier ike-id
      dhcp server 10.5.1.20
      dhcp server 10.5.1.24
      no dhcp chaddr-validate
      dhcp server selection-algorithm use-all
      dhcp server port 61610
      bind address 10.5.1.92
    #exit
    dhcp-server-profile CNR
    #exit
    hnbgw-service HNBGW_1
      sctp bind address 10.5.1.93
      sctp bind port 29169
      associate gtpu-service GTPU_FAP_1
      sctp sack-frequency 5
      sctp sack-period 5
      no sctp connection-timeout
      no ue registration-timeout
      hnb-identity oui discard-leading-char
      hnb-access-mode mismatch-action accept-aaa-value
      radio-network-plmn mcc 116 mnc 116
        rnc-id 116
      security-gateway bind address 10.5.1.91 crypto-template vmct-asr5k context HNBGW
    #exit
    ip route 0.0.0.0 0.0.0.0 10.5.1.1 Iu-Ps-Cs-H
    ip route 10.5.3.128 255.255.255.128 10.5.1.1 Iu-Ps-Cs-H
    ip igmp profile default
    #exit
  #exit
end
```

Step 3 If the radius server configuration is not as shown in the above example, perform the following configuration:

a) **configure**

b) **context** *HNBGW_context_name*

c) **radius server** *radius-server-ip-address* **key secret port 1812 priority 2**

Note When two radius servers are configured, one server is assigned Priority 1 and the other server is assigned Priority 2. If radius server entries are already configured, check their priorities. Else, assign new server priorities.

Example:

```
[local]blrrms-xt2-03# configure
[local]blrrms-xt2-03(config)# context HNBGW
[HNBGW]blrrms-xt2-03(config-ctx)# radius server 10.5.1.20 key secret port 1812 priority 2

radius server 10.5.1.20 encrypted key +A3qji4gwxyne5y3s09r8uzi5ot70fbyzzzzgbso92ladvtv7umjcj

        port 1812 priority 2
```

Step 4 If the configuration of the radius server is not correct, delete it: **no radius server** *radius-server-id-address*

Example:

```
[HNBGW]blrrms-xt2-03(config-ctx)# no radius server 10.5.1.20
```

Step 5 Configure the radius maximum retries and time out settings:

a) **configure**

b) **context** *hnbgw_context_name*

c) **radius max-retries 2**

d) **radius timeout 1**

After configuring the radius settings, verify that they are correct as in the example.

Example:

```
[local]blrrms-xt2-03# configure
[local]blrrms-xt2-03(config)# context HNBGW
[HNBGW]blrrms-xt2-03(config-ctx)# radius max-retries 2
[HNBGW]blrrms-xt2-03(config-ctx)# radius timeout 1

radius max-retries 2
   radius max-transmissions 5
   radius timeout 1
```

After the configuration is complete, the HNB GW sends access request thrice to the primary PAR with a one-second time delay between the two requests.

Configuring DNS for Redundancy

Configure the DNS with the newly added redundant configuration for the Serving and Upload nodes.

RMS High Availability Deployment

The high availability feature for Cisco RMS is designed to ensure continued operation of Cisco RMS sites in case of network failures. High availability provides a redundant setup that is activated automatically or manually when an active Central node or Provisioning and Management Gateway (PMG) database (DB) fails at one RMS site. This setup ensures that the Central node and PMG DB are connected at all times.

To implement high availability you will need an RMS site 1 as primary Central node, Serving node, and Upload node and RMS site 2 with redundant Serving node and Upload node.

To know more about high availability and configure it for Cisco RMS, see the following sections of the *High Availability for Cisco RAN Management Systems* document.

- Configuring High Availability for the Central Node
- Configuring High Availability for VMware vCenter in RMS Distributed Setup
- Configuring High Availability for VMware vCenter in RMS All-In-One Setup
- Configuring High Availability for the PMG DB

Optimizing the Virtual Machines

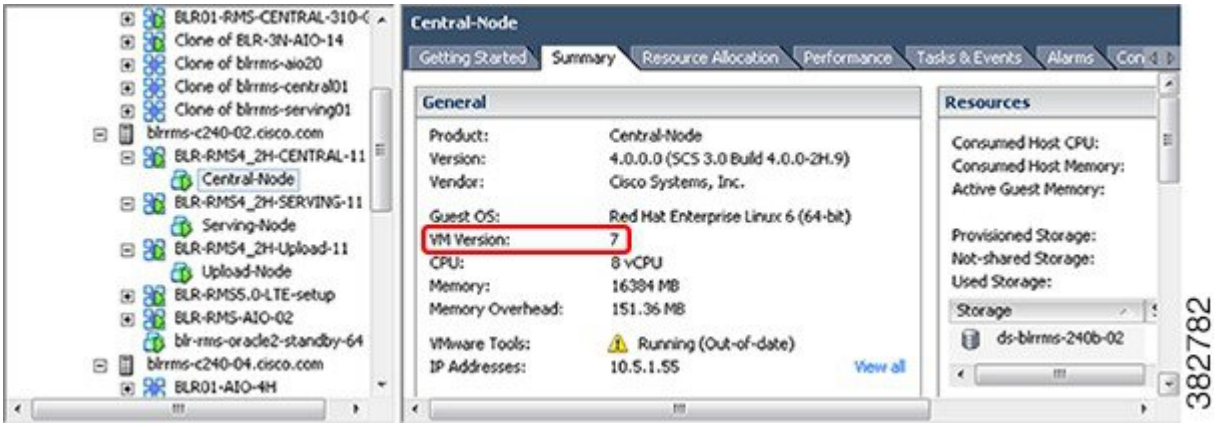
To run the RMS software, you need to verify that the VMs that you are running are up-to-date and configured optimally. Use these tasks to optimize your VMs.

Upgrading the VM Hardware Version

To have better performance parameter options available (for example, more virtual CPU and memory), the VMware hardware version needs to be upgraded to version 8 or above. You can upgrade the version using the vSphere client .

Note Prior to the VM hardware upgrade, make a note of the current hardware version from vSphere client.

Figure 8: VMware Hardware Version

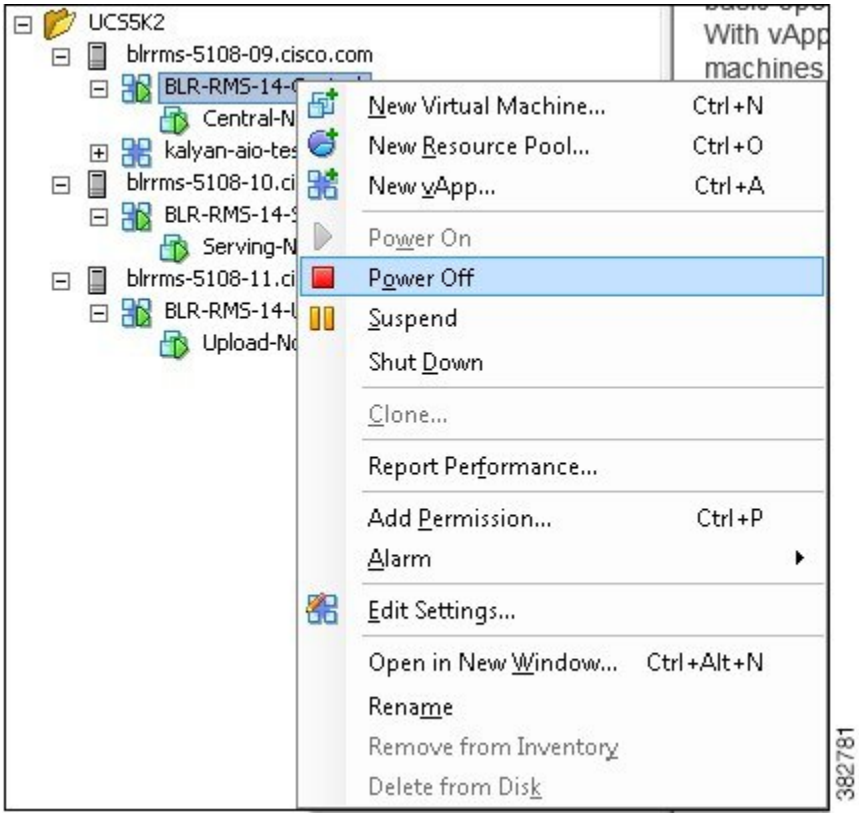


Procedure

Step 1 Start the vSphere client.

Step 2 Right-click the vApp for one of the RMS nodes and select **Power Off**.

Figure 9: Power Off the vApp



Step 3 Right-click the virtual machine for the RMS node (central, serving, upload) and select **Upgrade Virtual Hardware**.
The software upgrades the virtual machine hardware to the latest supported version.

Note The **Upgrade Virtual Hardware** option appears only if the virtual hardware on the virtual machine is not the latest supported version.

Step 4 Click **Yes** in the **Confirm Virtual Machine Upgrade** screen to continue with the virtual hardware upgrade.

Step 5 Verify that the upgraded version is displayed in the Summary screen of the vSphere client.

Step 6 Repeat this procedure for all remaining VMs, such as central, serving and upload so that all three VMs are upgraded to the latest hardware version.

Step 7 Right-click the respective vApp of the RMS nodes and select **Power On**.

Step 8 Make sure that all VMs are completely up with their new installation configurations.

Upgrading the VM CPU and Memory Settings

Before You Begin

Upgrade the VM hardware version as described in Upgrading the VM Hardware Version, on page 92.

Note Upgrade the CPU/Memory settings of the required RMS VMs using the below procedure to match the configurations defined in the section Optimum CPU and Memory Configurations, on page 15

Procedure

Step 1 Start the VMware vSphere web client.

Step 2 Right-click the vApp for one of the RMS nodes from the left panel and select **Power Off**.

Step 3 Right-click the virtual machine for a RMS node (central, serving, upload) and select **Edit Settings**.

Step 4 Select the **Virtual Hardware** tab. Click or Expand **Memory** in the Virtual Hardware on the left pane of the screen and update the RAM.

Step 5 Click the **Virtual Hardware** tab and update the Number of CPUs.

Step 6 Click **OK**.

Step 7 Right-click the vApp and select **Power On**.

Step 8 Repeat this procedure for all remaining VMs (central, serving, and upload).

Upgrading the Data Storage on Root Partition for Cisco RMS VMs

This procedure describes how to increase the disk space on the root partition. In the example illustrated below the disk partition is increased from 50 GB to 100 GB. Choose the new size (SYSTEM PARTITION) based on the value provided in Data Storage for Cisco RMS VMs, on page 15.

Procedure

Step 1 Log in to the VM and launch the console. Check the size of the existing partition.

```
# df -h
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              49G  8.5G   39G  19% /
```

```
tmpfs                 7.8G     0  7.8G   0% /dev/shm
/dev/sda1             124M   25M   94M  21% /boot
```

Step 2 Take a clone of the system (see Back Up System Using vApp Cloning, on page 287).

Step 3 Check the current root disk (`/dev/sda`) size using the following command.

```
# fdisk -l
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # fdisk -l

Disk /dev/sda: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00058cff

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
/dev/sda3              33        6528    52165632   83  Linux
[BLR17-Central-41N] /home/admin1 #
```

Step 4 Power down the VM. Select the VM and click **Power off the Virtual Machine**.

Step 5 Select the respective VM from the vCenter inventory list, right-click and click **Edit Settings**. Under the Virtual Hardware tab select Hard disk 1 and increase the size of the disk to desired size. Click **OK**.

Step 6 Power on the VM. Select the VM and click **Power off the Virtual Machine**.

Step 7 Log in to the VM and switch to root user.

```
$ su
```

Output:

Example:

```
[BLR17-Central-41N] ~ $ su
Password:
[BLR17-Central-41N] /home/admin1 #
```

Step 8 Verify the updated root disk (`/dev/sda`) size using the following command.

```
# fdisk -l
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # fdisk -l

Disk /dev/sda: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00058cff

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
```

```
/dev/sda3              33        6528    52165632   83  Linux
[BLR17-Central-41N] /home/admin1 #
```

Step 9 Use the **fdisk /dev/sda** command and enter option `p` to view the current partitions on `/dev/sda`. Note the start and end cylinder number for `/dev/sda3` (`/dev/sda3` is the root file system that can be verified using the **df -h** command). Enter option `d` and `3` (as root FS is sda3) to delete root FS temporarily. Enter option`p` to confirm that the partition has been deleted.

```
# fdisk  /dev/sda
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # fdisk  /dev/sda

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): p

Disk /dev/sda: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00058cff

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.
/dev/sda3              33        6528    52165632   83  Linux

Command (m for help): d
Partition number (1-4): 3


Command (m for help): p

Disk /dev/sda: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00058cff

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          17      131072   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              17          33      131072   82  Linux swap / Solaris
Partition 2 does not end on cylinder boundary.

Command (m for help):
```

Step 10 Enter options `n`, `p`, and `3` in order when prompted (to create a new primary partition on `/dev/sda3`). Note that the start cylinder number will be same as noted in Step 9, press Enter. Only the last cylinder number should be greater than the earlier number noted in Step 9. Press Enter. Enter option `w` to save the settings.

Example:

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (33-13054, default 33):
```

```
Using default value 33
Last cylinder, +cylinders or +size{K,M,G} (33-13054, default 13054):
Using default value 13054

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[BLR17-Central-41N] /home/admin1 #
```

Step 11 Reboot the system.

```
# reboot
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # reboot
Broadcast message from admin1@BLR17-Central-41N
        (/dev/pts/0) at 3:47 ...
The system is going down for reboot NOW!
[BLR17-Central-41N] /home/admin1 #
```

Step 12 Login to the system and switch to root user.

```
$ su
```

Output:

Example:

```
[BLR17-Central-41N] ~ $ su
Password:
[BLR17-Central-41N] /home/admin1 #
```

Step 13 Enable the new disk size by using the following command.

```
# resize2fs /dev/sda3
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # resize2fs /dev/sda3
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/sda3 is mounted on /; on-line resizing required
old desc_blocks = 4, new_desc_blocks = 7
Performing an on-line resize of /dev/sda3 to 26148271 (4k) blocks.
The filesystem on /dev/sda3 is now 26148271 blocks long.

[BLR17-Central-41N] /home/admin1 #
```

Step 14 Verify the new size using the following command.

```
# df -h
```

Output:

Example:

```
[BLR17-Central-41N] /home/admin1 # df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              99G  8.5G   85G  10% /
tmpfs                 7.8G     0  7.8G   0% /dev/shm
/dev/sda1             124M   25M   94M  21% /boot
```

```
[BLR17-Central-41N] /home/admin1 #
```

Upgrading the Upload VM Data Sizing

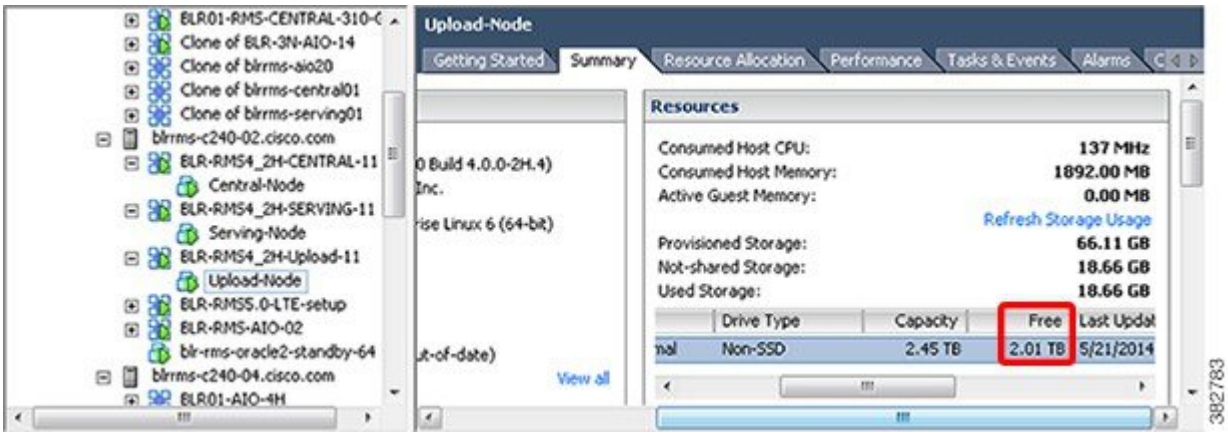
Note Refer to Virtualization Requirements, on page 14 for more information on data sizing.

Procedure

Step 1 Log in to the VMware vSphere web client and connect to a specific vCenter server.

Step 2 Select the Upload VM and click the **Summary** tab and view the available free disk space in Virtual Hardware > Location. Make sure that there is sufficient disk space available to make a change to the configuration.

Figure 10: Upload Node Summary Tab



Step 3 Right-click the RMS upload virtual machine and select **Power** followed by **Shut Down Guest**.

Step 4 Right-click again the RMS upload virtual machine and select **Edit Settings**.

Step 5 In the Edit Settings page, click **New Device** and select **New Hard Disk** or **Existing Hard Disk** to add or select a new hard disk.

Step 6 Select one of the data stores based on the disk size needed, give the required disk size as input and create a new hard disk.

Step 7 Click **OK**.

Step 8 Repeat steps 5 and 7 for **Hard disk 2**.

Step 9 Right-click the VM and select **Power** followed by **Power On**.

Step 10 Log in to the Upload node.

a) Log in to the Central node VM using the central node eth1 address.

b) ssh to the Upload VM using the upload node hostname.

Example:

```
ssh admin1@blr-rms14-upload
```

Step 11 Check the effective disk space after expanding: **fdisk -l**.

Step 12 Apply **fdisk** on expanded disk and create the new partition on the disk and save.

```
fdisk /dev/sdb
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-52216, default 1): 1
Last cylinder, +cylinders or +size{K,M,G} (1-52216, default 52216): 52216

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks..
```

Follow the on-screen prompts carefully to avoid errors that may corrupt the entire system.

The cylinder values may vary based on the machine setup.

Step 13 Repeat Step 11 to create partition on another disk.

Step 14 Stop the LUS process.

Example:

```
 god stop UploadServer
Sending 'stop' command
The following watches were affected:
UploadServer
```

Step 15 Create backup folders for the 'files' partition.

Example:

```
 mkdir -p /backups/uploads
The system responds with a command prompt.

mkdir –p /backups/archives
The system responds with a command prompt.
```

Step 16 Back up the data.

Example:

```
 mv/opt/CSCOuls/files/uploads/* /backups/uploads
mv/opt/CSCOuls/files/archives/* /backups/archives
The system responds with a command prompt.
```

Step 17 Create the file system on the expanded partitions.

Example:

```
mkfs.ext4 -i 4096 /dev/sdb1
The system responds with a command prompt.
```

Step 18 Repeat Step 16 for other partitions.

Step 19 Mount expanded partitions under /opt/CSCOuls/files/uploads and /opt/CSCOuls/files/archives directories using the following commands.

```
 mount -t ext4 -o
noatime,data=writeback,commit=120 /dev/sdb1 /opt/CSCOuls/files/uploads/
 mount -t ext4 -o
noatime,data=writeback,commit=120 /dev/sdc1 /opt/CSCOuls/files/archives/

The system responds with a command prompt.
```

Step 20 Edit /etc/fstab and append following entries to make the mount point reboot persistent.

```
/dev/sdb1 /opt/CSCOuls/files/uploads/ ext4 noatime,data=writeback,commit=120 0 0
/dev/sdc1 /opt/CSCOuls/files/archives/ ext4 noatime,data=writeback,commit=120 0 0
```

Step 21 Restore the already backed up data.

```
mv /backups/uploads/* /opt/CSCOuls/files/uploads/
mv /backups/archives/* /opt/CSCOuls/files/archives/
The system responds with a command prompt.
```

Step 22 Check ownership of the /opt/CSCOuls/files/uploads and /opt/CSCOuls/files/archives directory with the following command.

```
ls -l /opt/CSCOuls/files
```

Step 23 Change the ownership of the files/uploads and files/archives directories to ciscorms.

```
 chown -R ciscorms:ciscorms /opt/CSCOuls/files/
The system responds with a command prompt.
```

Step 24 Verify ownership of the mounting directory.

```
ls -al /opt/CSCOuls/files/
total 12
drwxr-xr-x. 7 ciscorms ciscorms 4096 Aug  5 06:03 archives
drwxr-xr-x. 2 ciscorms ciscorms 4096 Jul 25 15:29 conf
drwxr-xr-x. 5 ciscorms ciscorms 4096 Jul 31 17:28 uploads
```

Step 25 Edit the /opt/CSCOuls/conf/UploadServer.properties file.

```
cd /opt/CSCOuls/conf;
sed –i
's/UploadServer.disk.alloc.global.maxgb.*/UploadServer.disk.alloc.global.maxgb=<Max limit>/'

UploadServer.properties;
System returns with command prompt.
```

Replace <Max limit> with the maximum size of partition mounted under /opt/CSCOuls/files/uploads.

Step 26 Start the LUS process.

```
god start UploadServer
Sending 'start' command
The following watches were affected:
UploadServer
```

Note For the Upload Server to work properly, both/opt/CSCOuls/files/uploads/and/opt/CSCOuls/files/archives/folders must be on different partitions.

RMS Installation Sanity Check

Note Verify that there are no install related errors or exceptions in the ova-first-boot.log present in "/root" directory. Proceed with the following procedures only after confirming from the logs that the installation of all the RMS nodes is successful.

Sanity Check for the BAC UI

Following the installation, perform this procedure to ensure that all connections are established.

Note The default user name is bacadmin. The password is as specified in the OVA descriptor file (prop:RMS_App_Password). The default password is Rmsuser@1.

Procedure

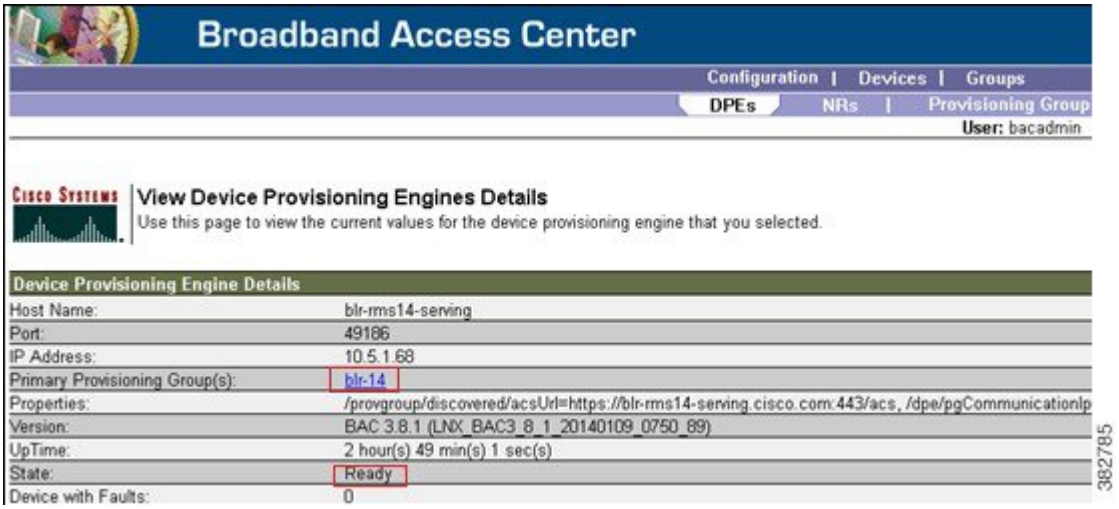
Step 1 Log in to BAC UI using the URL `https://<central-node-north-bound-IP>/adminui`.

Step 2 Click on **Servers**.

Step 3 Click the tabs at the top of the display to verify that all components are populated:

- DPEs—Should display respective serving node name given in the descriptor file used for deployment. Click on the serving node name. The display should indicate that this serving node is in the **Ready** state.

Figure 11: BAC: View Device Provisioning Engines Details



- NRs—Should display the NR (same as serving node name) given in the descriptor file used for deployment. Click on the NR name. The display should indicate that this node is in the **Ready** state.
- Provisioning Groups—Should display the respective provisioning group name given in the descriptor file used for deployment. Click on the Provisioning group name. The display should indicate the ACS URL pointing to the value of the property, "prop: Acs_Virtual_Fqdn" that you specified in the descriptor file.
- RDU—Should display the RDU in the **Ready** state.

If all of these screens display correctly as described, the BAC UI is communicating correctly.

Sanity Check for the DCC UI



Note Before using the username, pmguser or pmgadmin, through the DCC UI to communicate with PMG, ensure that you change their default password.

Following the installation, perform this procedure to ensure that all connections are established.

Procedure

Step 1 Log in to DCC UI using the URL https://[central-node-northbound-IP]/dcc_ui.
The default username is dccadmin. The password is as specified in the OVA descriptor file (prop:RMS_App_Password). The default password is Rmsuser@1.

Step 2 Click the Groups and IDs tab and verify that the Group Types table shows Area, Enterprise, FemtoGateway, HeNBGW,LTESecGateway, RFProfile, RFProfile-LTE, Region, Site, SubSite, and UMTSSecGateway and the ID Pool Type table shows CELL-POOL, SAI-POOL, and LTE-CELL-POOL.

Verifying Application Processes

Verify the RMS virtual appliance deployment by logging onto each of the virtual servers for the Central, Serving and Upload nodes. Note that these processes and network listeners are available for each of the servers:

Procedure

Step 1 Log in to the Central node as a root user.

Step 2 Run: **service bprAgent status**
In the output, note that these processes are running:

```
[rtpfga-s1-central1] ~ # service bprAgent status
```

```
BAC Process Watchdog is running
Process [snmpAgent] is running
Process [rdu] is running
Process [tomcat] is running
```

Step 3 Run: **/rms/app/nwreg2/regional/usrbin/cnr_status**

Note This step is not applicable in a third-party SeGW RMS deployment.

```
[rtpfga-ova-central06] ~ # /rms/app/nwreg2/regional/usrbin/cnr_status
Server Agent running (pid: 4564)
CCM Server running (pid: 4567)
WEB Server running (pid: 4568)
RIC Server Running (pid:v4569)
```

Step 4 Login to the Serving node and run the command as root user.

Step 5 Run: **service bprAgent status**

```
 [rtpfga-s1-serving1] ~ # service bprAgent status

BAC Process Watchdog is running.
Process [snmpAgent] is running.
Process [dpe] is running.
Process [cli] is running.
```

Step 6 Run: **/rms/app/nwreg2/local/usrbin/cnr_status**

Note This step is not applicable in a third-party SeGW RMS deployment.

```
[rtpfga-s1-serving1] ~ # /rms/app/nwreg2/local/usrbin/cnr_status

DHCP server running (pid: 16805)
Server Agent running (pid: 16801)
CCM Server running (pid: 16804)
WEB Server running (pid: 16806)
CNRSNMP server running (pid: 16808)
RIC Server Running (pid: 16807)
TFTP Server is not running
DNS Server is not running
DNS Caching Server is not running
```

Step 7 Run: **/rms/app/CSCOar/usrbin/arstatus**

```
[root@rms-aio-serving ~]# /rms/app/CSCOar/usrbin/arstatus

Cisco Prime AR RADIUS server running (pid: 24272)
Cisco Prime AR Server Agent running (pid: 24232)
Cisco Prime AR MCD lock manager running (pid: 24236)
Cisco Prime AR MCD server running (pid: 24271)
Cisco Prime AR GUI running (pid: 24273)
[root@rms-aio-serving ~]#
```

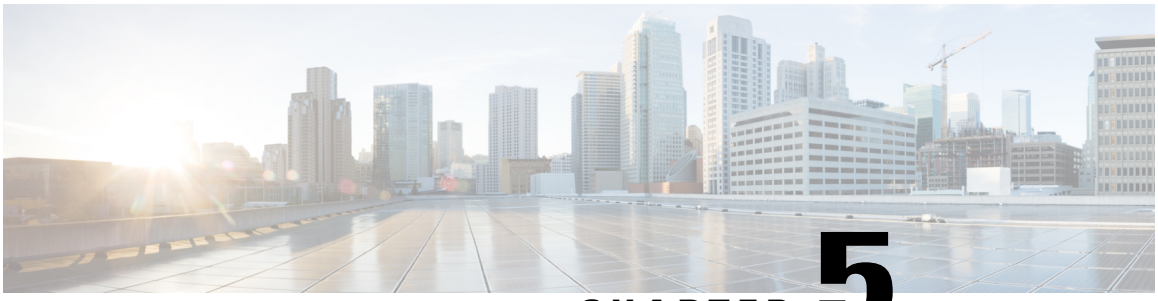
Step 8 Login to the Upload node and run the command as root user.

Step 9 Run: **service god status**

```
[rtpfga-s1-upload1] ~ # service god status

UploadServer: up
```

Note If the above status of UploadServer is not up (start or unmonitor state), see Upload Server is Not Up, on page 245 for details.



CHAPTER 5

Installation Tasks Post-OVA Deployment

Perform these tasks after deploying the OVA descriptor files.

- HNB Gateway and DHCP Configuration, page 105
- Adding Routes and IPtables for LTE FAP, page 109
- Installing RMS Certificates, page 109
- Enabling Communication for VMs on Different Subnets, page 121
- Configuring Default Routes for Direct TLS Termination at the RMS, page 122
- Post-Installation Configuration of BAC Provisioning Properties , page 124
- PMG Database Installation and Configuration, page 125
- Configuring New Groups and Pools, page 135
- Configuring SNMP Trap Servers with Third-Party NMS, page 136
- Integrating FM, PMG, LUS, and RDU Alarms on Central Node with Prime Central NMS, page 140
- Integrating BAC, PAR, and PNR on Serving Node with Prime Central NMS, page 147
- De-Registering RMS with Prime Central Post-Deployment, page 157
- Starting Database and Configuration Backups on Central VM , page 159
- Optional Features, page 160

HNB Gateway and DHCP Configuration

Follow this procedure only in the following scenarios:

- When PNR and PAR details are not provided during installation in the descriptor file and you want to create the first instance of PNR (scope/lease) and PAR (Radius clients).
- To declare multiple PNR/PAR details.

Note Skip this procedure if PNR and PAR details are already provided in the descriptor file during installation.

Use the following scripts available in `/rms/ova/scripts/post_install/HNBGW` to configure PAR and PNR with the HNB Gateway information on the RMS Serving nodes.

- configure_PNR_hnbgw.sh: This script creates a scope and lease list in the Serving node with the details provided in the input configuration file.

Note Ensure that the Lease Time on the client (SeGW configuration) is set to 86400 seconds.

Sample Input File for HNB GW configuration:

```
#CNR properties
Cnr_Femto_Scope=femto-scope2
Asr5k_Dhcp_Address= Asr5k_Dhcp_Address
Dhcp_Pool_Network= Asr5k_Pool network
Dhcp_Pool_Subnet= DHCP Subnet
Dhcp_Pool_FirstAddress= DHCP Pool First address
Dhcp_Pool_LastAddress= DHCP Pool last address
Central_Node_Eth1_Address=North Bound central Node address

#CAR properties
Car_HNBGW_Name=ASR5K2
radius_shared_secret=secret

#Common Properties for CAR and CNR
Asr5k_Radius_Address=
Serving_Node_NB_Gateway=
Serving_Node_Eth0_Address= North Bound address
```

Usage:

```
configure_PNR_hnbgw.sh [ -i <config_file> ] [-h] [--help]
```

Example:

```
./configure_PNR_hnbgw.sh -i HNBGW-CONFIG
User : root

Detected RMS Serving Node .
*******************Post-installation script to configure HNB-GW with
RMS*******************************
Is the current Serving node part of Distributed RMS deployment mode ? [y/n Note:
y=Distributed n=AIO]
n
Enter cnradmin Password:



[default cnr admin password is Rmsuser@1]

Following are the already configured femto scopes in CNR :
100 Ok - 2 objects found
Name                              Subnet               Policy
----                              ------               ------
dummy-scope                       10.10.10.1/32        default
femto-scope                       10.10.10.1/32        default
100 Ok

 NOTE : Please make sure that the above CNR/PNR scope(s) name and DHCP IP range/subnet
 don't overlap with the values of the input file.

Do you want to continue [y/n] :y
Configuring CNR
100 Ok
.
```

```
.
.
nrcmd> dhcp listExtensions
100 Ok
post-packet-decode:      1 dexdropras
                         2 extclientid
pre-packet-encode:
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>
nrcmd> # Save

nrcmd> save
100 Ok

nrcmd> 100 Ok
100 Ok - 4 objects found
Name                            Subnet               Policy
----                            ------               ------
dummy-scope                     10.10.10.1/32        default
dummyfemto-scope2               10.5.1.187/32        default
femto-scope                     10.10.10.1/32        default
femto-scope2                    7.0.2.96/28          default
100 Ok
Setting firewall for CNR DHCP....
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Enter yes To Configure the value of the Asr5k_Radius_CoA_Port. Enter no to use the
default value
no
Configuring the Default Asr5k_Radius_CoA_Port 3799 on RMS Central Node

Enter the RMS Central Node admin Username: admin1

Enter the RMS Central Node admin Password:
Validating Admin_Username and Admin_Password
Enter the value of Root_Password: Validating password
 Central Node : 10.5.1.220
spawn ssh admin1@10.5.1.220
admin1@10.5.1.220's password:
Last login: Fri Aug  7 08:54:48 2015 from blrrms-serving-22-sree
This system is restricted for authorized users and
for legitimate business purposes only. The actual or attempted
unauthorized access, use, or modification of this system is
strictly prohibited Unauthorized users are subject to
Company disciplinary proceedings and/or criminal and civil
penalties under state, federal, or other applicable domestic
and foreign laws. The use of this system may be monitored and
recorded for administrative and security reasons.
[blrrms-central-22-sree] ~ $ su -
Password:
[blrrms-central-22-sree] ~ # iptables -A OUTPUT -s 10.5.1.220 -d 10.5.1.187 -p udp -m
 udp --dport 3799 -m state --state NEW -j ACCEPT
[blrrms-central-22-sree] ~ # iptables -A OUTPUT -s 10.105.233.92 -d 10.5.1.187 -p udp
 -m udp --dport 3799 -m state --state NEW -j ACCEPT ; service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
[blrrms-central-22-sree] ~ # exit
logout
[blrrms-central-22-sree] ~ $ exit
logout
Connection to 10.5.1.220 closed.
```

- configure_PAR_hnbgw.sh: This script creates Radius clients in the Serving node with the details provided in the input configuration file.

  Usage:

  ```
  configure_PAR_hnbgw.sh [ -i <config_file> ] [-h] [--help]
  ```

  Example:

  ```
  ./configure_PAR_hnbgw.sh -i HNBGW-CONFIG
  User : root

  Detected RMS Serving Node .
  ******************Post-installation script to configure HNBGW with RMS
  CAR*****************************
  Enter car admin Password:

  [default car admin password is Rmsuser@1]

  Configuring CAR....
  Setting firewall for CAR Radius
  iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
  *******Done************
  ```

Before You Begin

- 'root' privilege is a mandatory to execute the scripts.
- Scripts should be executed from the RMS Serving node.
- Prepare the input configuration file "hnbgw_config" with the required HNB GW and related DHCP information.

Procedure

Execute the scripts based on the deployment mode by providing the config file input.

Note
- Execute the configure_PAR_hnbgw.sh script only if the Radius client is not created with the new ASR 5000 IP address(Asr5k_Radius_Address).
- Add proper routes on the RMS Serving node to ensure that the Cisco RMS and ASR 5000 router are reachable. Ping to manually check reachability.

RMS AIO (All-In-One) Mode Deployment :

Execute the following scripts on the Serving node:

```
./configure_PNR_hnbgw.sh -i hnbgw_config
./configure_PAR_hnbgw.sh -i hnbgw_config
```

RMS Distributed Mode Deployment:

Execute the following scripts on the Serving node:

```
./configure_PNR_hnbgw.sh -i hnbgw_config
./configure_PAR_hnbgw.sh -i hnbgw_config
```

RMS Distributed Mode Deployment (Redundancy):

Execute the following scripts on the primary Serving node first and then execute the script on the secondary Serving node:

Note For secondary Serving node, modify the config file hnbgw_config with secondary Serving node details (attributes - Serving_Node_NB_Gateway,Serving_Node_Eth0_Address) and then execute the script.

```
./configure_PNR_hnbgw.sh -i hnbgw_config
./configure_PAR_hnbgw.sh -i hnbgw_config
```

Configure the new security Gateway on the ASR 5000 router as described in the Configuring the Security Gateway on the ASR 5000 for Redundancy, on page 85.

Configure the new HNB GW for redundancy as described in Configuring the HNB Gateway for Redundancy, on page 89.

Adding Routes and IPtables for LTE FAP

To get LiveData to work on the LTE FAP, add the route for the inner IP address and IPtables using the Serving node, eth0 gateway.

Example for Adding Routes:

```
route add -net 10.30.10.128/25 gw 10.10.31.102
```

In the above example, 10.30.10.128/25 is the FAP subnet, 10.10.31.102 is the gateway of Serving node NB interface that connects or routes to the HeNBGW.

Example for Adding IPtables:

```
iptables -A OUTPUT -p tcp -s 10.10.31.102 -d 10.30.10.128/25 --dport 7547 -m state --state
 NEW -j ACCEPT
service iptables save
```

In the above example, 10.10.31.102 is the Serving node eth0 address and 10.30.10.128/25 is the FAP subnet.

Installing RMS Certificates

Following are the two types of certificates are supported. Use one of the options, depending on the availability of your signing authority:

- Auto-generated CA signed RMS certificates – If you do not have your own signing authority (CA) defined
- Self-signed RMS certificates(for manual signing purpose) – If you have your own signing authority (CA) defined

Auto-Generated CA-Signed RMS Certificates

The RMS supports auto-generated CA-signed RMS certificates as part of the installation to avoid manual signing overhead. Based on the optional inputs in the OVA descriptor file, the RMS installation generates the customer specific *Root CA* and *Intermediate CA*, and subsequently signs the RMS (DPE and ULS) certificates using these generated CAs. If these properties are not specified in the OVA descriptor file, the default values are used.

Table 2: Optional Certificate Properties in OVA Descriptor File

Property	Default Value
prop:Cert_C	US
prop:Cert_ST	NC
prop:Cert_L	RTP
prop:Cert_O	Cisco Systems, Inc.
prop:Cert_OU	MITG

The signed RMS certificates are located at the following destination by default:

- DPE—`/rms/app/CSCObac/dpe/conf/dpe.keystore`
- ULS—`/opt/CSCOuls/conf/uls.keystore`

The following example shows how to verify the contents of keystore, for example, dpe.keystore:

Note The keystore password is Rmsuser@1

```
[root@blrrms-serving-08 ~]# keytool -keystore /rms/app/CSCObac/dpe/conf/dpe.keystore -list
 -v

Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: dpe-key
Creation date: May 19, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 3
Certificate[1]:
Owner: CN=10.5.2.44, OU=POC, O=Cisco Systems, ST=NC, C=US
Issuer: CN="Cisco Systems, Inc. POC Int", O=Cisco
Serial number: 1
Valid from: Mon May 19 17:24:31 UTC 2014 until: Tue May 19 17:24:31 UTC 2015
Certificate fingerprints:
         MD5:  C7:9D:E1:A1:E9:2D:4C:ED:EE:3E:DA:4B:68:B3:0D:0D
         SHA1: D9:55:3E:6E:29:29:B4:56:D6:1F:FB:03:43:30:8C:14:78:49:A4:B8
         Signature algorithm name: SHA256withRSA
         Version: 3
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DC AB 02 FA 9A B2 5F 60   15 54 BE 9E 3B ED E7 B3  ......_`.T..;...
0010: AB 08 A5 68                                        ...h
]
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  ipsecEndSystem
```

```
  ipsecTunnel
  ipsecUser
]
#3: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 43 0C 3F CF E2 B7 67 92   17 61 29 3F 8D 62 AE 94  C.?...g..a)?.b..
0010: F5 6A 5D 30                                        .j]0
]
]
Certificate[2]:
Owner: CN="Cisco Systems, Inc. POC Int", O=Cisco
Issuer: CN="Cisco Systems, Inc. POC Root", O=Cisco
Serial number: 1
Valid from: Mon May 19 17:24:31 UTC 2014 until: Thu May 13 17:24:31 UTC 2038
Certificate fingerprints:
         MD5:  53:7E:60:5A:20:1A:D3:99:66:F4:44:F8:1D:F9:EE:52
         SHA1: 5F:6A:8B:48:22:5F:7B:DE:4F:FC:CF:1D:41:96:64:0E:CD:3A:0C:C8
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:0
]
#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 43 0C 3F CF E2 B7 67 92   17 61 29 3F 8D 62 AE 94  C.?...g..a)?.b..
0010: F5 6A 5D 30                                        .j]0
]
]
#4: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 1F E2 47 CF DE D5 96 E5   15 09 65 5B F5 AC 32 FE  ..G.......e[..2.
0010: CE 3F AE 87                                        .?..
]

]
Certificate[3]:
Owner: CN="Cisco Systems, Inc. POC Root", O=Cisco
Issuer: CN="Cisco Systems, Inc. POC Root", O=Cisco
Serial number: e8c6b76de63cd977
Valid from: Mon May 19 17:24:30 UTC 2014 until: Fri May 13 17:24:30 UTC 2039
Certificate fingerprints:
         MD5:  15:F9:CF:E7:3F:DC:22:49:17:F1:AC:FB:C2:7A:EB:59
         SHA1: 3A:97:24:C2:A2:B3:73:39:0E:49:B2:3D:22:85:C7:C0:D8:63:E2:81
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]
```

```
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1F E2 47 CF DE D5 96 E5   15 09 65 5B F5 AC 32 FE  ..G.......e[..2.
0010: CE 3F AE 87                                        .?..
]
]
*******************************************
*******************************************
```

You must manually update the certificates to the ZDS server, as described in this procedure.

Procedure

Step 1 Locate the RMS CA chain at following location in the central node:
`/rms/data/rmsCerts/ZDS_Upload.tar.gz`
The ZDS_Upload.tar.gz file contains the following certificate files:

- hms_server_cert.pem
- download_server_cert.pem
- pm_server_cert.pem
- ped_server_cert.pem

Step 2 Upload the ZDS_Upload.tar.gz file to the ZDS.

Self-Signed RMS Certificates

Before installing the certificates, create the security files on the Serving node and the Upload node. Each of these nodes includes the unique keystore and csr files that are created during the deployment process. Procedure for creating security files:

Procedure

Step 1 Locate each of the following Certificate Request files.

- Serving Node: `/rms/app/CSCObac/dpe/conf/self_signed/dpe.csr`
- Upload Node :`/opt/CSCOuls/conf/self_signed/uls.csr`

Step 2 Sign them using your relevant certificate authority.
After the CSR is signed, you will get three files: client-ca.cer, server-ca.cer, and root-ca.cer.

Self-Signed RMS Certificates in Serving Node

Procedure

Step 1 Import the following three certificates (client-ca.cer, server-ca.cer, and root-ca.cer) into the keystore after getting the csr signed by the signing tool to complete the security configuration for the Serving Node:

a) Log in to the Serving node and then switch to root user:**su -**

b) Place the certificates (client-ca.cer, server-ca.cer, and root-ca.cer) into the `/rms/app/CSCObac/dpe/conf/self_signed` folder.

c) Run the following commands in`/rms/app/CSCObac/dpe/conf/self_signed`:

Note The default password for `/rms/app/cscobac/jre/lib/security/cacerts` is "changeit".

1 **/rms/app/CSCObac/jre/bin/keytool -import -alias server-ca -file [server-ca.cer] -keystore /rms/app/CSCObac/jre/lib/security/cacerts**

Sample Output

```
[root@blrrms-serving-22 self_signed]# /rms/app/CSCObac/jre/bin/keytool -import -alias
 server-ca
                        -file server-ca.cer -keystore
/rms/app/CSCObac/jre/lib/security/cacerts
Enter keystore password:
Owner: CN=rtp Femtocell CA, O=Cisco
Issuer: CN=Cisco Root CA M1, O=Cisco
Serial number: 610420e200000000000b
Valid from: Sat May 26 01:04:27 IST 2012 until: Wed May 26 01:14:27 IST 2032
Certificate fingerprints:
         MD5:  AF:0C:A0:D3:74:18:FE:16:A4:CA:87:13:A8:A4:9F:A1
         SHA1: F6:CD:63:A8:B9:58:FE:7A:5A:61:18:E4:13:C8:DF:80:8E:F5:1D:A9
         SHA256: 81:38:8F:06:7E:B6:13:87:90:D6:8B:72:A3:40:03:92:A4:8B:94
                  :33:B8:3A:DD:2C:DE:8F:42:76:68:65:6B:DC
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 0A 00 53 00 75 00 62   00 43 00 41              ...S.u.b.C.A


#2: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                           ...


#3: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   accessLocation: URIName: http://www.cisco.com/security/pki/certs/crcam1.cer
]
```

```
]

#4: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A6 03 1D 7F CA BD B2 91   40 C6 CB 82 36 1F 6B 98  ........@...6.k.
0010: 8F DD BC 29                                        ...)
]
]

#5: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:0
]

#6: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
     [URIName: http://www.cisco.com/security/pki/crl/crcam1.crl]
]]

#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.3.6.1.4.1.9.21.1.16.0]
[PolicyQualifierInfo: [
  qualifierID: 1.3.6.1.5.5.7.2.1
  qualifier: 0000: 16 35 68 74 74 70 3A 2F   2F 77 77 77 2E 63 69 73  .5http://www.cis
0010: 63 6F 2E 63 6F 6D 2F 73   65 63 75 72 69 74 79 2F  co.com/security/
0020: 70 6B 69 2F 70 6F 6C 69   63 69 65 73 2F 69 6E 64  pki/policies/ind
0030: 65 78 2E 68 74 6D 6C                               ex.html

]]  ]
]

#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  ipsecEndSystem
  ipsecTunnel
  ipsecUser
  1.3.6.1.4.1.311.10.3.1
  1.3.6.1.4.1.311.20.2.1
  1.3.6.1.4.1.311.21.6
]

#9: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#10: ObjectId: 2.5.29.14 Criticality=false
```

```
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5B F4 8C 42 FE DD 95 41   A0 E8 C2 45 12 73 1B 68  [..B...A...E.s.h
0010: 42 6C 0D EF                                        Bl..
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

2 **/rms/app/CSCObac/jre/bin/keytool -import -alias root-ca -file [root-ca.cer] -keystore /rms/app/CSCObac/jre/lib/security/cacerts**

Note The default password for `/rms/app/cscobac/jre/lib/security/cacerts` is "changeit".

Sample Output

```
[root@blrrms-serving-22 self_signed]# /rms/app/CSCObac/jre/bin/keytool -import -alias
 root-ca
                       -file root-ca.cer -keystore
/rms/app/CSCObac/jre/lib/security/cacerts
Enter keystore password:
Owner: CN=Cisco Root CA M1, O=Cisco
Issuer: CN=Cisco Root CA M1, O=Cisco
Serial number: 2ed20e7347d333834b4fdd0dd7b6967e
Valid from: Wed Nov 19 03:20:24 IST 2008 until: Sat Nov 19 03:29:46 IST 2033
Certificate fingerprints:
         MD5:  F0:F2:85:50:B0:B8:39:4B:32:7B:B8:47:2F:D1:B8:07
         SHA1: 45:AD:6B:B4:99:01:1B:B4:E8:4E:84:31:6A:81:C2:7D:89:EE:5C:E7
         SHA256: 70:5E:AA:FC:3F:F4:88:03:00:17:D5:98:32:60:3E
                   :EF:AD:51:41:71:B5:83:80:86:75:F4:5C:19:0E:63:78:F8
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                           ...


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
```

```
0000: A6 03 1D 7F CA BD B2 91   40 C6 CB 82 36 1F 6B 98  ........@...6.k.
0010: 8F DD BC 29                                        ...)
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

d) Import the certificate reply into the DPE keystore:
· **/rms/app/CSCObac/jre/bin/keytool -import -trustcacerts -file [client-ca.cer] -keystore /rms/app/CSCObac/dpe/conf/self_signed/dpe.keystore -alias dpe-key**

Note The password for the client certificate installation is specified in the OVA descriptor file (prop:RMS_App_Password). The default value is Rmsuser@1.

Sample Output

```
[root@blrrms-serving-22 self_signed]# /rms/app/CSCObac/jre/bin/keytool -import
-trustcacerts -file client-ca.cer -keystore
/rms/app/CSCObac/dpe/conf/self_signed/dpe.keystore -alias dpe-key
Enter keystore password:
Certificate reply was installed in keystore
```

Step 2 Run the following commands to take the backup of existing certificates and copy the new certificates:

a) cd /rms/app/CSCObac/dpe/conf
b) mv dpe.keystore dpe.keystore_org
c) cp self_signed/dpe.keystore .
d) chown bacservice:bacservice dpe.keystore
e) chmod 640 dpe.keystore
f) /etc/init.d/bprAgent restart dpe

Step 3 Verify the automatic installation of the Ubiquisys CA certificates to the cacerts file on the DPE by running these commands:

- **/rms/app/CSCObac/jre/bin/keytool -keystore /rms/app/CSCObac/jre/lib/security/cacerts -alias UbiClientCa -list -v**
- **/rms/app/CSCObac/jre/bin/keytool -keystore /rms/app/CSCObac/jre/lib/security/cacerts -alias UbiRootCa -list -v**

Note The default password for `/rms/app/cscobac/jre/lib/secutiry/cacerts` is changeit.

What to Do Next

If there are issues during the certificate generation process, refer to Regeneration of Certificates, on page 233.

Importing Certificates Into Cacerts File

If a certificate signed by a Certificate Authority that is not included in the Java cacerts file by default is used, then it is mandatory to complete the following configuration:

Procedure

Step 1 Log in to the Serving node as a root user and navigate to `/rms/app/CSCObac/jre/lib/security` directory.

Step 2 Import the intermediate or root certificate (or both) into the cacerts file using the below command:
`keytool -import -alias <alias> -keystore cacerts -trustcacerts -file <certificate_filename>`

Step 3 Provide a valid RMS_App_Password when prompted to import the certificate into the cacerts file.

Self-Signed RMS Certificates in Upload Node

Procedure

Step 1 Import the following three certificates (client-ca.cer, server-ca.cer, and root-ca.cer) into the keystore after getting the csr signed by the signing tool to complete the security configuration for the Upload Node:

a) Log in to the Upload node and switch to root user: **su -**

b) Place the certificates (client-ca.cer, server-ca.cer, and root-ca.cer) in the `/opt/CSCOuls/conf/self_signed` folder.

c) Run the following commands in `/opt/CSCOuls/conf/self_signed`:

1 **keytool -importcert -keystore uls.keystore -alias root-ca -file [root-ca.cer]**

Note The password for the keystore is specified in the OVA descriptor file (prop:RMS_App_Password). The default value is Rmsuser@1.

Sample Output

```
[root@blr-blrrms-lus2-22 self_signed]# keytool -importcert -keystore uls.keystore
                                        -alias root-ca -file root-ca.cer
Enter keystore password:
Owner: CN=Cisco Root CA M1, O=Cisco
Issuer: CN=Cisco Root CA M1, O=Cisco
Serial number: 2ed20e7347d333834b4fdd0dd7b6967e
Valid from: Wed Nov 19 03:20:24 IST 2008 until: Sat Nov 19 03:29:46 IST 2033
Certificate fingerprints:
         MD5:  F0:F2:85:50:B0:B8:39:4B:32:7B:B8:47:2F:D1:B8:07
         SHA1: 45:AD:6B:B4:99:01:1B:B4:E8:4E:84:31:6A:81:C2:7D:89:EE:5C:E7
         SHA256: 70:5E:AA:FC:3F:F4:88:03:00:17:D5:98:32:60:3E:EF:AD:51:41:71:
                   B5:83:80:86:75:F4:5C:19:0E:63:78:F8
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                           ...


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
```

```
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A6 03 1D 7F CA BD B2 91   40 C6 CB 82 36 1F 6B 98  ........@...6.k.
0010: 8F DD BC 29                                        ...)
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

2 **keytool -importcert -keystore uls.keystore -alias server-ca -file [server-ca.cer]**

Note The password for the keystore is specified in the OVA descriptor file (prop:RMS_App_Password). The default value is Rmsuser@1.

Sample Output

```
[root@blr-blrrms-lus2-22 self_signed]# keytool -importcert -keystore uls.keystore
                                        -alias server-ca -file server-ca.cer
Enter keystore password:
Owner: CN=rtp Femtocell CA, O=Cisco
Issuer: CN=Cisco Root CA M1, O=Cisco
Serial number: 610420e200000000000b
Valid from: Sat May 26 01:04:27 IST 2012 until: Wed May 26 01:14:27 IST 2032
Certificate fingerprints:
         MD5:  AF:0C:A0:D3:74:18:FE:16:A4:CA:87:13:A8:A4:9F:A1
         SHA1: F6:CD:63:A8:B9:58:FE:7A:5A:61:18:E4:13:C8:DF:80:8E:F5:1D:A9
         SHA256: 81:38:8F:06:7E:B6:13:87:90:D6:8B:72:A3
                     :40:03:92:A4:8B:94:33:B8:3A:DD:2C:DE:8F:42:76:68:65:6B:DC
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 0A 00 53 00 75 00 62   00 43 00 41              ...S.u.b.C.A


#2: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                           ...


#3: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
```

```
  [
   accessMethod: caIssuers
   accessLocation: URIName: http://www.cisco.com/security/pki/certs/crcam1.cer
]
]

#4: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A6 03 1D 7F CA BD B2 91   40 C6 CB 82 36 1F 6B 98  ........@...6.k.
0010: 8F DD BC 29                                        ...)
]
]

#5: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:0
]

#6: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
     [URIName: http://www.cisco.com/security/pki/crl/crcam1.crl]
]]

#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.3.6.1.4.1.9.21.1.16.0]
[PolicyQualifierInfo: [
  qualifierID: 1.3.6.1.5.5.7.2.1
  qualifier: 0000: 16 35 68 74 74 70 3A 2F   2F 77 77 77 2E 63 69 73  .5http://www.cis
0010: 63 6F 2E 63 6F 6D 2F 73   65 63 75 72 69 74 79 2F  co.com/security/
0020: 70 6B 69 2F 70 6F 6C 69   63 69 65 73 2F 69 6E 64  pki/policies/ind
0030: 65 78 2E 68 74 6D 6C                               ex.html

]]  ]
]

#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  ipsecEndSystem
  ipsecTunnel
  ipsecUser
  1.3.6.1.4.1.311.10.3.1
  1.3.6.1.4.1.311.20.2.1
  1.3.6.1.4.1.311.21.6
]

#9: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
```

```
  Crl_Sign
]

#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 5B F4 8C 42 FE DD 95 41   A0 E8 C2 45 12 73 1B 68  [..B...A...E.s.h
0010: 42 6C 0D EF                                        Bl..
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

3 **keytool -importcert -keystore uls.keystore -alias uls-key -file [client-ca.cer]**

Note The password for keystore is specified in the OVA descriptor file (prop:RMS_App_Password). The default value is Rmsuser@1.

Sample Output

```
[root@blr-blrrms-lus2-22 self_signed]# keytool -importcert -keystore uls.keystore
-alias uls-key -file client-ca.cer
Enter keystore password:
Certificate reply was installed in keystore
```

Step 2 Run the following commands to take the backup of existing certificates and copy the new certificates:

a) cd /opt/CSCOuls/conf
b) mv uls.keystore uls.keystore_org
c) cp self_signed/uls.keystore .
d) chown ciscorms:ciscorms uls.keystore
e) chmod 640 uls.keystore
f) service god restart

Step 3 Run these commands to verify that the Ubiquisys CA certificates were placed in the Upload node truststore:

- **keytool -keystore /opt/CSCOuls/conf/uls.truststore -alias UbiClientCa -list -v**
- **keytool -keystore /opt/CSCOuls/conf/uls.truststore -alias UbiRootCa -list -v**

Note The password for uls.truststore is Ch@ngeme1.

What to Do Next

If there are issues during the certificate generation process, refer to Regeneration of Certificates, on page 233.

Importing Certificates Into Upload Server Truststore file

If a certificate signed by a Certificate Authority that is not included in the uls.truststore file by default is used, then it is mandatory to complete the following configuration:

Procedure

Step 1 Login to the Upload node as a root user and navigate to the `/opt/CSCOuls/conf` directory.

Step 2 Import the intermediate or root certificate (or both) into the uls.truststore file using the below command:
```
keytool -import -alias <alias> -keystore uls.truststore -trustcacerts -file
<certificate_filename>
```

Step 3 Provide a valid RMS_App_Password when prompted to import the certificate into the uls.truststore file.

Enabling Communication for VMs on Different Subnets

As part of RMS deployment there could be a situation wherein the Serving/Upload nodes with eth0 IP are in a different subnet compared to that of the Central node. This is also applicable if redundant Serving/Upload nodes have eth0 IP on a different subnet than that of the Central node.

In such a situation, based on the subnets, routing tables need to be manually added on each node so as to ensure communication between all nodes.

Perform the following procedure to add routing tables.



Note Follow these steps on the VM console on each RMS node.

Procedure

Step 1 Central Node:
This route addition ensures that Central node can communicate successfully with Serving and Upload nodes present in different subnets.

```
route add –net  <subnet of Serving/Upload Node eth0 IP>  netmask  <netmask IP> gw
<gateway for Central Node eth0 IP>
```
For example: route add -net 10.5.4.0 netmask 255.255.255.0 gw 10.5.1.1

Step 2 Serving Node, Upload Node:
These route additions ensure Serving and Upload node communication with other nodes on different subnets.

a) Serving Node:
```
route add –net  <subnet of Serving/Upload Node eth0 IP>  netmask  <netmask IP> gw
<gateway for Serving Node eth0 IP>
```
For example: route add -net 10.5.4.0 netmask 255.255.255.0 gw 10.5.1.1

b) Upload Node:
```
route add –net  <subnet of Serving/Upload Node eth0 IP>  netmask  <netmask IP> gw
<gateway for Upload  Node eth0 IP>
```

For example: route add -net 10.5.4.0 netmask 255.255.255.0 gw 10.5.1.1

Step 3 Repeat Step 2 for other Serving and Upload nodes.

Step 4 Include the entry <destination subnet/netmask number> via <gw IP> in the `/etc/sysconfig/network-scripts/route-eth0` file to make the added routes permanent. If the file is not present, create it. For example: 10.5.4.0/24 via 10.1.0.1

Configuring Default Routes for Direct TLS Termination at the RMS

Because transport layer security (TLS) termination is done at the RMS node, the default route on the Upload and Serving nodes must point to the southbound gateway to allow direct device communication with these nodes.

Note If the Northbound and Southbound gateways are already configured in the descriptor file, as shown in the example, then this section can be skipped.

- prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1
- prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1

Procedure

Step 1 Log in to the Serving node and run the following command: **netstat –nr**

Example:

```
netstat –nr

Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.81.254.202   10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.105.233.81   10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.10.10.4      10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
64.102.6.247    10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.5.1.9        10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.5.1.8        10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.105.233.60   10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
7.0.1.176       10.5.1.1        255.255.255.240 UG        0 0          0 eth0
10.5.1.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.5.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth1
0.0.0.0         10.5.1.1        0.0.0.0         UG        0 0          0 eth0
```

Step 2 Use the below procedure to set the southbound gateway as the default gateway on the Serving node:

- To make the route settings temporary, execute the following commands on the Serving node:
  - Delete the northbound gateway IP address using the following command. For example,**route delete -net 0.0.0.0 netmask 0.0.0.0 gw 10.5.1.1**

- Add the southbound gateway IP address using the following command. For example,**route add -net 0.0.0.0 netmask 0.0.0.0 gw 10.5.2.1**

- To make the route settings default or permanent, execute the following command on the Serving node: **/opt/vmware/share/vami/vami_config_net**

Example:

```
/opt/vmware/share/vami/vami_config_net

Main Menu

0)      Show Current Configuration (scroll with Shift-PgUp/PgDown)
1)      Exit this program
2)      Default Gateway
3)      Hostname
4)      DNS
5)      Proxy Server
6)      IP Address Allocation for eth0
7)      IP Address Allocation for eth1
Enter a menu number [0]: 2

Warning: if any of the interfaces for this VM use DHCP,
the Hostname, DNS, and Gateway parameters will be
overwritten by information from the DHCP server.

Type Ctrl-C to go back to the Main Menu

0)      eth0
1)      eth1
Choose the interface to associate with default gateway [0]: 1
Note: Provide the southbound gateway IP address as highlighted below
Gateway will be associated with eth1
IPv4 Default Gateway [10.5.1.1]: 10.5.2.1


Reconfiguring eth1...
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
RTNETLINK answers: File exists
Network parameters successfully changed to requested values

Main Menu

0)      Show Current Configuration (scroll with Shift-PgUp/PgDown)
1)      Exit this program
2)      Default Gateway
3)      Hostname
4)      DNS
5)      Proxy Server
6)      IP Address Allocation for eth0
7)      IP Address Allocation for eth1
Enter a menu number [0]: 1
```

Step 3 Verify that the southbound gateway IP address was added: **netstat –nr**

Example:

```
netstat –nr

Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.81.254.202   10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.105.233.81   10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.10.10.4      10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
64.102.6.247    10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.5.1.9        10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.5.1.8        10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
10.105.233.60   10.5.1.1        255.255.255.255 UGH       0 0          0 eth0
7.0.1.176       10.5.1.1        255.255.255.240 UG        0 0          0 eth0
10.5.1.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.5.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth1
0.0.0.0         10.5.2.1        0.0.0.0         UG        0 0          0 eth1
```

Step 4 To add the southbound gateway IP address from the Upload node, repeat Steps 1 to 3 on the Upload node.

Post-Installation Configuration of BAC Provisioning Properties

The establishment of a connection between the Serving node and Central node can fail during the installation due to network latency in SSH or because the Southbound IP of the Central node and Northbound IP of the Serving node are in different subnets. As a result, BAC Provisioning properties such as upload and ACS URLs are not added. If this occurs, you must configure the BAC provisioning properties after establishing connectivity between the Central node and Serving node after the installation. RMS provides a script for this purpose. To add the BAC provisioning properties, perform this procedure:

Procedure

Step 1 Log in to the central node

Step 2 Switch to root user using **su -**.

Step 3 Change to directory `/rms/ova/scripts/post_install` and run the script **configure_bacproperies.sh**. The script will require a descriptor file as an input.
Run the commands:

cd /rms/ova/scripts/post_install

./configure_bacproperies.sh deploy-descr-filename.

Sample Output

```
File: /rms/ova/scripts/post_install/addBacProvisionProperties.kiwi
Finished tests in 244ms
Total Tests Run    - 14
Total Tests Passed - 14
Total Tests Failed - 0
Output saved in file: /tmp/runkiwi.sh_admin1/addBacProvisionProperties.out.20141203_0838

_____________________________________________________________________________
Post-processing log for benign error codes:
/tmp/runkiwi.sh_admin1/addBacProvisionProperties.out.20141203_0838
```

```
Revised Test Results
  Total Test Count: 14
      Passed Tests: 14
   Benign Failures: 0
  Suspect Failures: 0

Output saved in file:
/tmp/runkiwi.sh_admin1/addBacProvisionProperties.out.20141203_0838-filtered
/rms/ova/scripts/post_install /home/admin1
*******Done************
```

Step 4 After executing the scripts successfully, the BAC properties are added in the BACAdmin UI. To verify the properties that are added:

a) Log in to BAC UI using the URL `https://<central-node-north-bound-IP>/adminui`
b) Click on **Servers**.
c) Click the **Provisioning Group** tab at the top of the display to verify that all the properties such as ACS URL, Upload URL , NTP addresses, and Ip Timing_Server IP properties are added.

PMG Database Installation and Configuration

PMG Database Installation Prerequisites

1 The minimum hardware requirements for the Linux server should be as per Oracle 11gR2 documentation. In addition, 4 GB disc space is required for PMG DB data files.
Following are the recommendations for VM:

- Red Hat Enterprise Linux Server (release v6.6)
- Memory: 8 GB
- Disk Space: 50 GB
- CPU: 8 vCPU

2 Ensure that the Oracle installation directory (for example, /u01/app/oracle) is owned by the Oracle OS root user. For example,

```
# chown -R oracle:oinstall /u01/app/oracle
```

3 Ensure Oracle 11gR2 is installed with database name=PMGDB and ORACLE_SID=PMGDB and running on the Oracle installation VM.

Following are the recommendation for database initialization parameters::

- memory_max_target: 3200 MB
- memory_target: 3200 MB
- No. of Processes: 150 (Default value)
- No. of sessions: 248 (Default value)

4 ORACLE_HOME environment variable is created and $ORACLE_HOME/bin is in the system path.

```
# echo $ORACLE_HOME
/u01/app/oracle/product/11.2.0/dbhome_1
#echo $PATH
/u01/app/oracle/product/11.2.0/dbhome_1/bin:/usr/lib64/qt-3.3/bin:
   /usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/oracle/bin
```

5 To populate Mapinfo data from the Mapinfo files:

a Ensure that third party tools “EZLoader” and Oracle client (with Administrator option selected in Installation Types) are installed with Windows operating system.

b Tnsnames.ora has PMGDB server entry.
For example, in the file, `c:\oracle\product\10.2.0\client_3\NETWORK\ADMIN\tnsnames.ora`, the following entry should be present.

```
PMGDB =
  (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)(HOST = <PMGDB Server IP>)(PORT = <PMGDB server oracle
 application port>))
    )
    (CONNECT_DATA =
      (SID = PMGDB)
      (SERVER = DEDICATED)
    )
)
```

c Download the MapInfo files generated by the third party tool.

d Ensure correct IPTable entiries are added on the PMGDB server to allow communication between EZLoader application and Oracle application on the PMGDB server.

Note Perform the following procedures as an 'oracle' user.

PMG Database Installation

Schema Creation

Procedure

Step 1 Download the .gz file `RMS-PMGDB-<RMS build num>.tar.gz` from the release folder to desktop.

Step 2 Log in to the database VM.

Step 3 Copy the downloaded `RMS-PMGDB-<RMS build num>.tar.gz` file from the desktop to the Oracle user home directory (example, `/home/oracle`) on PMGDB server as oracle user.

Step 4 Login to the PMGDB server as oracle user. In the home directory (example, `/home/oracle`), unzip and untar the `RMS-PMGDB-<RMS build num>.tar.gz` file.

```
# gunzip RMS-PMGDB-<RMS build num>.tar
# tar -xvf RMS-PMGDB-<RMS build num>.tar
```

Step 5 Go to PMGDB installation base directory `~/pmgdb_install/`.
Run install script and provide input as prompted. `# ./install_pmgdb.sh` **Input Parameters Required:**

1 Full filepath and name of data file PMGDB tablespace.
2 Full filepath and name of data file MAPINFO tablespace.
3 Password for database user PMGDBADMIN.
4 Password for database user PMGUSER.
5 Password for database user PMGDB_READ.
6 Password for database user MAPINFO.

Password Validation:

- If password value for any database user provided is blank, respective username (e.g. PMGDBADMIN) will be used as default value.
- The script does not validate password values against any password policy as password policy can vary based on the Oracle password policy configured.
- Following is the sample output for reference:

  Note In the output, the system prompts you to change the file name if the file name already exists. Change the file name. Example: pmgdb1_ts.dbf

```
[oracle@blr-rms-oracle2 pmgdb_install]$ ./install_pmgdb.sh
The script will get executed on database instance PMGDB
Enter PMGDB tablespace filename with filepath
(e.g. /u01/app/oracle/oradata/PMGDB/pmgdb_ts.dbf):
/u01/app/oracle/oradata/PMGDB/pmgdb_ts.dbf
File already exists, enter a new file name
[oracle@blr-rms-oracle2 pmgdb_install]$ ./install_pmgdb.sh
The script will get executed on database instance PMGDB
Enter PMGDB tablespace filename with filepath
(e.g. /u01/app/oracle/oradata/PMGDB/pmgdb_ts.dbf):
/u01/app/oracle/oradata/PMGDB/test_pmgdb_ts.dbf
You have entered /u01/app/oracle/oradata/PMGDB/test_pmgdb_ts.dbf
as PMGDB table space.
 Do you want to continue[y/n]y
filepath entered is  /u01/app/oracle/oradata/PMGDB/test_pmgdb_ts.dbf
Enter MAPINFO tablespace filename with filepath
(e.g. /u01/app/oracle/oradata/PMGDB/mapinfo_ts.dbf):
/u01/app/oracle/oradata/PMGDB/test_mapinfo_ts.dbf
You have entered  /u01/app/oracle/oradata/PMGDB/test_mapinfo_ts.dbf as MAPINFO  table
 space.
 Do you want to continue[y/n]y
filepath entered is  /u01/app/oracle/oradata/PMGDB/test_mapinfo_ts.dbf
Enter password for user PMGDBADMIN :
Confirm Password:
Enter password for user PMGUSER :
Confirm Password:
Enter password for user PMGDB_READ :
Confirm Password:
Enter password for user MAPINFO :
Confirm Password:
****************************************************************
*Connecting to database PMGDB

Script execution completed , verifying...
****************************************************************
   No errors, Installation completed successfully!
   Main log file created is /u01/oracle/pmgdb_install/pmgdb_install.log
```

```
   Schema log file created is /u01/oracle/pmgdb_install/sql/create_schema.log
*****************************************************************
```

Step 6 On successful completion, the script creates schema on the PMGDB database instance.

Step 7 If the script output displays an error, "`Errors may have occurred during installation`", see the following log files to find out the errors:

a) `~/pmgdb_install/pmgdb_install.log`

b) `~/pmgdb_install/sql/create_schema.log`

Correct the reported errors and recreate schema.

Map Catalog Creation



Note Creation of Map Catalog is needed only for fresh installation of PMG DB.

Procedure

Step 1 Ensure that the MapInfo files are downloaded and extracted on your computer. (See PMG Database Installation Prerequisites, on page 125).

Step 2 Go to `C:/ezldr/EazyLoader.exe`, and double-click “EazyLoader.exe” to open the MapInfo EasyLoader window to load the data.

Step 3 Click **Oracle Spatial** and log in to the PMGDB using **MAPINFO** as the user id and password (which was provided during Schema creation), and server name as tnsname given in tnsnames.ora (example, **PMGDB**).

Step 4 Click **Source Tables** to load MapInfo TAB file from the extracted location, for example, "C:\ezldr\FemtoData\v72\counties_gdt73.TAB”.

Step 5 Click **Map Catalog** to create the map catalog. A system message “A Map Catalog was successfully created.” is displayed on successful creation. Click **OK**.

Step 6 Click **Options** and verify that the following check boxes are checked in Server Table Processing:

- Create Primary Key
- Create Spatial Index

Step 7 Click **Close** to close the MapInfo EasyLoader window.

Load MapInfo Data

Procedure

Step 1 Ensure that the MapInfo files are downloaded and extracted on your computer.

Step 2 Log in to the Central Node as an admin user.

Step 3 Download and ftp the following file on your laptop under EzLoader folder (for example, C:\ezldr).
/rms/app/ops-tools/public/batch-files/loadRevision.bat

Step 4 Open windows command line tool, change the directory to EZLoader folder and run the bat file.
loadRevision.bat [mapinfo-revisionnumber] [input file path] [MAPINFO user password]
where

mapinfo-revisionnumber is the revision number of the MapInfo files that are downloaded.

input file path is the base path where downloaded MapInfo files are extracted, that is, where the directory with the name "v<mapinfo-revisionnumber>" like v73 is located after extraction.

MAPINFO user password is the password given to the MAPINFO user during the schema creation. If no input is given then default password is same as username, that is, MAPINFO.

```
C:\>
C:\>cd ezldr
c:\ezldr>loadRevision.bat 73 c:\ezldr\FemtoData MAPINFO

c:\ezldr>echo off
Command Line Parameters:
   revision ID = "73"
          path = "c:\ezldr\FemtoData"
          mapinfo password = "<Not Displayed>"
-------
Note:
MAPINFO_MAPCATALAOG should be present in the database. If not, EasyLoader GUI can
be used to create it.
-------
Calling easyloader...
Logs are created under EasyLoader.log
Done.

C:\ezldr>
```

Example:
loadRevision.bat 73 c:\ezldr\FemtoData MAPINFO

Note
1. MAPINFO_MAPCATALOG should be present in the database. If not, to create it and load the Mapinfo data again, see the Map Catalog Creation, on page 128.
2. Logs are created in a file *EasyLoader.log* under current directory (for example, C:\ezldr). Verify the logs if the table does not get created in the database.
3. Multiple revision tables can exist in the database. For example, COUNTIES_GDT72, COUNTIES_GDT73, and so on.

Step 5 Log in to PMGDB as MAPINFO user from sqlplus client and verify the tables are created and data is uploaded.

Grant Access to MapInfo Tables

Procedure

Step 1 Log in to the PMGDB server as an oracle user.

Step 2 Go to PMGDB installation base directory " ~/pmgdb_install/".

Step 3 Run grant script.
./grant_mapinfo.sh

Following is the sample output of the Grant access script for reference:

```
[oracle@blr-rms-oracle2 pmgdb_install]$ ./grant_mapinfo.sh

The script will get executed on database instance PMGDB


****************************************************************

Connecting to database PMGDB

Script execution completed , verifying...
****************************************************************

No errors, Executing grants completed successfully!

Log file created is /u01/oracle/pmgdb_install/grant_mapinfo.log
****************************************************************
[oracle@blr-rms-oracle2 pmgdb_install]$
```

Step 4 Verify ~/pmgdb_install/grant_mapinfo.log.

Configuring the Central Node

Configuring the PMG Database on the Central Node

Before You Begin

Verify that the PMG database is installed. If not install it as described in PMG Database Installation and Configuration, on page 125.

Procedure

Step 1 Log in to the Central node as admin user.

```
[rms-aio-central] ~ $ pwd
/home/admin1
```

Step 2 Change from Admin user to root user.

```
[rms-aio-central] ~ $ su -
Password:
```

Step 3 Check the current directory and the user.

```
[rms-aio-central] ~ # pwd
/root
[rms-aio-central] ~ # whoami
root
```

Step 4 Change to install directory `/rms/ova/scripts/post_install`

```
# cd /rms/ova/scripts/post_install
```

Step 5 Execute the configure script, **pmgdb_configure.sh** with valid input. The input values are:
Pmgdb_Enabled -> To enable pmgdb set it to “true”

Pmgdb_Primary_Dbserver_Address -> PMG DB primary server ip address for example, 10.105.233.66

Pmgdb_Primary_Dbserver_Port -> PMG DB primary server port for example, 1521

Pmgdb_Standby1_Dbserver_Address -> PMG DB standby 1 server (hot standby) IP address. For example, **10.105.242.64**. Optional, if not specified, connection failover to hot standby database will not be available. To enable the failover feature later, script has to be executed again.

Pmgdb_Standby1_Dbserver_Port -> PMG DB standby 1 server (hot standby) port. For example, **1521**. Do not specify this property if previous property is not specified.

Pmgdb_Standby2_Dbserver_Address -> PMG DB standby 2 server (cold standby) IP address. For example, **10.105.242.64**. Optional, if not specified, connection failover to cold standby database will not be available. To enable the failover feature later, script has to be executed again.

Pmgdb_Standby2_Dbserver_Port -> PMG DB standby 2 server (cold standby) port. For example, **1521**. Do not specify this property if previous property is not specified.

Enter DbUser PMGUSER Password -> Is prompted. Provide Password of the database user "PMGUSER". Also, provide the same password when prompted for confirmation of password.

Usage:

pmgdb_configure.sh <Pmgdb_enabled> <Pmgdb_Dbserver_Address> <Pmgdb_Dbserver_Port>

[<Pmgdb_Stby1_Dbserver_Address>] [<Pmgdb_Stby1_Dbserver_Port>] [<Pmgdb_Stby2_Dbserver_Address>]

[<Pmgdb_Stby2_Dbserver_Port>]

Example:
Following is an example where three PMGDB Servers (Primary, Hot Standby and Cold Standby) are used:

```
[rms-distr-central] /rms/app/rms/install # ./pmgdb_configure.sh true 10.105.242.63 1521
10.105.233.64 1521
10.105.233.63 1521

Executing as root user


Enter DbUser PMGUSER Password:
Confirm Password: Central_Node_Eth0_Address 10.5.4.35
Central_Node_Eth1_Address 10.105.242.86
Script input:

Pmgdb_Enabled=true
```

```
Pmgdb_Prim_Dbserver_Address=10.105.242.63
Pmgdb_Prim_Dbserver_Port=1521
Pmgdb_Stby1_Dbserver_Address=10.105.233.64
Pmgdb_Stby1_Dbserver_Port=1521
Pmgdb_Stby2_Dbserver_Address=10.105.233.63
Pmgdb_Stby2_Dbserver_Port=1521
 Executing in 10 sec, enter <cntrl-C> to exit
.....
....
...
..
.
Start configure dcc props
dcc.properties already exists in conf dir
END configure dcc props
Start configure pmgdb props
pmgdb.properties already exists in conf dir
Changed jdbc url to jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
(HOST=10.105.242.63)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=10.105.233.64)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)
(HOST=10.105.233.63)(PORT=1521))(FAILOVER=on)
(LOAD_BALANCE=off))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=PMGDB_PRIMARY)))
End configure pmgdb props
Configuring iptables for Primary server
Start configure_iptables
Removing old entries first, may show error if rule does not exist
Removing done, add rules
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
end configure_iptables
Configuring iptables for Standby server
Start configure_iptables
Removing old entries first, may show error if rule does not exist
Removing done, add rules
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
end configure_iptables
Configuring iptables for Standby server
Start configure_iptables
Removing old entries first, may show error if rule does not exist
Removing done, add rules
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
end configure_iptables
Done PmgDb configuration
[rms-distr-central] /rms/app/rms/install #
```

Step 6 Restart PMG application as a root user if the configuration is successful.

```
# service god stop


# service god start
```

Step 7 Verify that PMG DB server is connected. Change to user **ciscorms** and run the OpsTools script: getAreas.sh. If the PmgDB configuration is successful, the script runs successfully without any errors.

```
# su - ciscorms
# getAreas.sh -key 100

[rms-aio-central] /rms/app/rms/install # su -
[rms-aio-central] ~ # su - ciscorms
[rms-aio-central] ~ $ getAreas.sh -key 100
Config files script-props/private/GetAreas.properties or
script-props/public/GetAreas.properties
     not found. Continuing with default settings.
Execution parameters:
key=100
GetAreas processing can take some time please do not terminate.
Received areas, total areas 0
Writing to file: /users/ciscorms/getAreas.csv
The report captured in csv file: /users/ciscorms/getAreas.csv
```

```
**** GetAreas End Script ***
[rms-aio-central] ~ $
```

Step 8 In case of an error, do the following:

a) Verify that pmgdb.enabled=true in **/rms/app/rms/conf/dcc.properties**.

b) In **/rms/app/rms/conf/pmgdb.properties**, verify `pmgdb.tomcat.jdbc.pool.jdbcUrl property` and edit the values if necessary:

```
pmgdb.tomcat.jdbc.pool.jdbcUrl=jdbc:oracle:thin:@
(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=DBSERVER1)
(PORT=DBPORT1))(ADDRESS=(PROTOCOL=TCP)(HOST=DBSERVER2)(PORT=DBPORT2))
(ADDRESS=(PROTOCOL=TCP)(HOST=DBSERVER3)(PORT=DBPORT3))
(FAILOVER=on)(LOAD_BALANCE=off))(CONNECT_DATA=(SERVER=DEDICATED)
(SERVICE_NAME=PMGDB_PRIMARY)))
```

c) If pmgdb.tomcat.jdbc.pool.jdbcUrl property is edited, restart the PMG and run getAreas.sh again.

Note If a wrong password was given during "pmgdb_configure.sh" script execution., the script can be re-executed with the correct password following "Configuring the PMG Database on the Central Node". Restart the PMG and run getAreas.sh again after the script execution.

Step 9 If you can still not connect, check the IPtables entries for the database server.

```
# iptables -S
```

Area Table Data Population

After the PMG database installation, the Area table which is used to lookup polygons is empty. It needs to be populated from the MapInfo table. This task describes how to use the script, **updatePolygon.sh** to populate the data.

Procedure

Step 1 Log in to Central node as admin user.

```
[rms-aio-central] ~ $ pwd
/home/admin1
```

Step 2 Change from Admin user to Root user.

```
[rms-aio-central] ~ $ su -
Password:
```

Step 3 Check the current directory and the user.

```
[rms-aio-central] ~ # pwd
/root
[rms-aio-central] ~ # whoami
root
```

Step 4 If the PMG database configuration is not done, configure the PMG database on the Central node as described in Configuring the PMG Database on the Central Node, on page 130.

Step 5 Change to user **ciscorms**.

```
# su - ciscorms
```

Step 6 Run the **updatePolygons.sh** script with mapinfo revision number as input.
For example,

```
# updatePolygons.sh -rev 73
```

The -help option can be used to display script usage:

```
# updatePolygons.sh -help
```

```
[rms-aio-central] ~ $ updatePolygons.sh -rev 73
Config files script-props/private/UpdatePolygons.properties or
script-props/public/UpdatePolygons.properties not found. Continuing with default settings.
Execution parameters:
rev=72
Source table is mapinfo.counties_gdt73
Initializing PMG DB
Update Polygon processing can take some time please do not terminate.
Updated Polygon in PmgDB Change Id:1
**** UpdatePolygons End Script ***
```

Step 7 Verify that the Area table is populated with data.

Step 8 Run the command to connect to SQL:**sqlplus PMGUSER/<PMGUSER password>** on PMGDB server.
Sample Output

```
SQL>
```

Step 9 Run the SQL command as PMGUSER on the PMG database server: **SQL> select count(*) from area;**
Sample Output

```
COUNT(*)
----------
3232
```

Step 10 To register from DCC UI with Lattitude, Longitude coordinates, an Area group with name as valid area key needs to be created.
For example, for "New York" county, where lat= 40.714623 and long= -74.006605, Area group with name "36061" should be created where 36061 is area_key for New York county.
This can be done by running the Operational Tools script **updatePolygonsInPmg.sh** as ciscorms user where it creates all the area groups corresponding to the area_keys present in the Area table.

For example:

```
# updatePolygonsInPmg.sh -changeid <changeid of update transaction>
```

The change ID of update transaction can be found in logs of **updatePolygons.sh** when it is run to update Area table from mapinfo table. (See the output for Step 6, highlighted to obtain the Change ID value.) When Area table is populated with the data after first time installation of PMG database, **updatePolygonsInPmg.sh** can be run with other optimization options such as multiple threads, and so on.

For more information on usage, see *Operational Tools* in the *Cisco RAN Management System Administration Guide*.

The newly created area group properties are fetched from the DefaultArea properties. The group specific details are to be modified through DCC UI, either from GUI or by exporting/importing csv files.

Note DCC UI may have performance issues when a large number of groups are created.

Alternate way to create area groups is by creating them manually through the DCC UI. That is, exporting existing area in csv, changing the name as valid area_key along with other property values, and importing them back to the DCC UI.

The valid areas (counties) and area_keys can be queried from the PMG database or OpsTools Script. Use **getAreas.sh** with the **-all** option.

From SQL prompt, run the below SQL command as PMGUSER on PMGDB server:

```
SELECT area_key, area_name, area_region
FROM AREA
WHERE STATUS = 'A'
ORDER BY area_key;
```

From OpsTools script:

```
# getAreas.sh –all
```

```
[rms-aio-central] ~ $ getAreas.sh -all
Config files script-props/private/GetAreas.properties or
script-props/public/GetAreas.properties not found. Continuing with default settings.
Execution parameters:
all
GetAreas processing can take some time please do not terminate.
Received areas, total areas 3232
Writing to file: /users/ciscorms/getAreas.csv
The report captured in csv file: /users/ciscorms/getAreas.csv
**** GetAreas End Script ***
[rms-aio-central] ~ $
```

Note If no data is retrieved by the SQL query or the OpsTools script, Area table may be empty. Ensure that you follow the steps in PMG Database Installation and Configuration, on page 125 and contact the next level of support.

Configuring New Groups and Pools

The default groups and pools cannot be used post installation. You must create new groups and pools. You can recreate your groups and pools using a previously exported csv file. Alternatively, you can create completely new groups and pools as required. For more information, refer to recommended order for working with pools and groups as described in the in the *Cisco RAN Management System Administration Guide*.

Note Default groups and pools are available for reference after deployment. Use these as examples to create new groups and pools.

Only for Enterprise support, you need to configure Enterprise and Site groups.

Ensure that you add the following groups and pools before registering a device in the sequence shown as follows: CELL-POOL, SAI-POOL, LTE-CELL-POOL, Area, Enterprise, FemtoGateway, HeNBGW, LTESecGateway, RFProfile, RFProfile-LTE, Region, Site, SubSite, and UMTSSecGateway.

Note Provide the FC-PROV-GRP-NAME property in the femtogateway with the provisioning group name, "Bac_Provisioning_Group" that is provided during the deployment in the OVA descriptor file. The default value for the Bac_Provisioning_Group property is pg01.

Configuring SNMP Trap Servers with Third-Party NMS

In the Cisco RMS solution architecture, the Centralized Fault Management (FM) Framework feature provides a uniform interface to network management systems (NMS) for fault management. This feature supports the Cisco-EPM-NOTIFICATION-MIB that notifies the RMS components (PMG, log upload server [LUS]) alarms to the Prime Central NMS through the through SNMPv2c interface.

The Centralized FM framework feature consists of

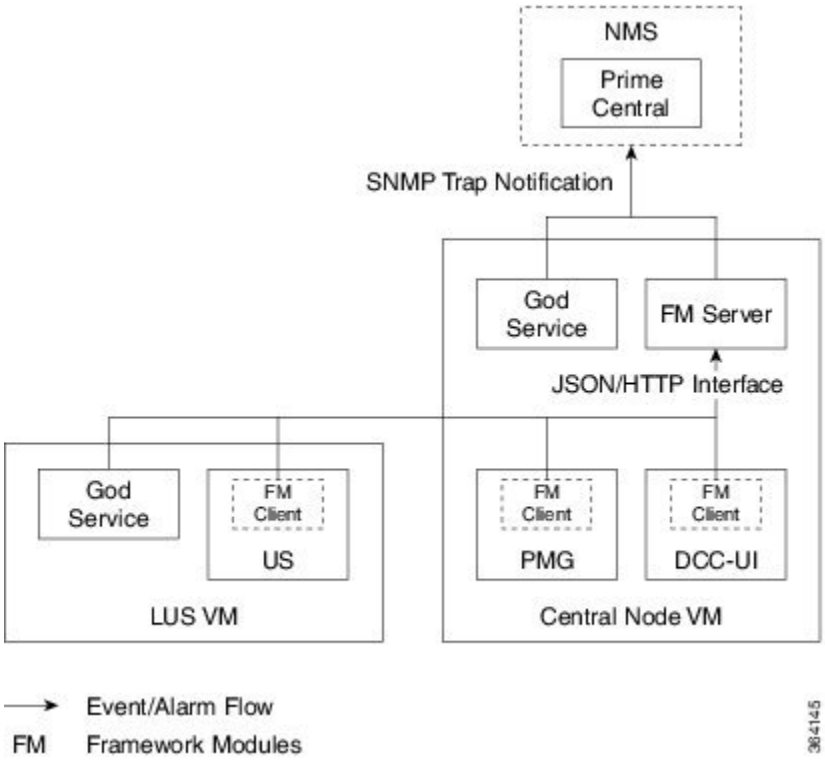
- FM server module—This module receives alarm notifications from the ULS and the PMG application servers through JSON over HTTP interface. The module then transforms the received alarm information into a Cisco-EPM-NOTIFICATION-MIB specification and notifies it as an SNMv2cP trap to the Prime Central NMS.
- FM client module—This module provides a set of generic APIs to raise and clear alarms and enable the integration with the Cisco RMS components.

  The FM server application is built as an rpm package for installation. The maven rpm specification in pom.xml is used to specify the directory structure on the target platform (similar to other applications on the Central node), when the application is installed.

  The FM client library is integrated with each RMS component application such as PMG, LUS applications.

The following figure depicts the positioning of the Centralized Fault Management Framework feature-specific functions in the Cisco RMS solution architecture.

Figure 12: Centralized Fault Management Framework in Cisco RMS Solution Architecture



Configuring FM, PMG, LUS, and RDU Alarms on Central Node for Third-Party NMS

Procedure

Step 1 Log in to the Central node.

Step 2 Switch to root user: **su –**

Step 3 Enable SNMP on the Central node

```
ovfenv -f /rms/ovf-env.xml -k Snmptrap_Enable -v True
```

Step 4 Navigate to the following directory: `cd /rms/ova/scripts/post_install/`

Step 5 Run the **configure_fm_server.sh** script.

Example:

```
 [rms-central-blr01] ~ $ su
Password: ***********
[rms-central-blr01] /rms/ova/scripts/post_install # ovfenv -f /rms/ovf-env.xml -k
Snmptrap_Enable -v True
[rms-central-blr01] /home/admin1 # cd /rms/ova/scripts/post_install/
```

```
[rms-central-blr01] /rms/ova/scripts/post_install # ./configure_fm_server.sh
******************Script to configure NMS interface details for
FM-Server*******************************
RMS FM Framework requires the NMS manager interface details...
Enter number of SNMP managers to be configured (0 to disable SNMP traps/1/2/3)
1
Enter details for NMS-1
Enter NMS manager interface IP address
10.105.242.54
Enter NMS manager SNMP trap version(v1/v2c)
v2c
Enter NMS manager interface port number(162/1162)
162
Enter the SNMP trap community for the NMS
public
Entering update_BACSnmpDetails()
OK
Please restart [stop and start] SNMP agent.
Process [snmpAgent] has been restarted.

Exiting update_BACSnmpDetails()
RMS was not configured for sending SNMP traps, skipping the deletion of earlier added iptable
 rules.
Assigning the variables for FMServer.properties update
Setting firewall for fm_server....
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Is the specified NMS, Prime Central SNMP Trap Host? [ 10.105.242.54 ] Specify [y]es / [n]o
 [y]?
n
 Exiting without Prime Central Integration
[rms-central-blr01] /rms/ova/scripts/post_install #
```

Configuring DPE, CAR, CNR, and AP Alarms on Serving Node for Third-Party NMS

Procedure

Step 1 Log in to the Serving node.

Step 2 Switch to root user: **su –**

Step 3 Change the directory: `cd /rms/ova/scripts/post_install`

Step 4 Navigate to the following directory: `cd /rms/ova/scripts/post_install/`

Step 5 Run the **./configuresnmpservingnode.sh**script.

Example:

```
 [root@rms-Serving-blr01 ~]# cd /rms/ova/scripts/post_install/
[root@rms-Serving-blr01 post_install]#
[root@rms-Serving-blr01 post_install]# ./configuresnmpservingnode.sh
******************Post-installation script to configure SNMP on RMS Serving
Node*****************************

MENU
1 - Configure SNMP Servers
2 - Configure SNMPTrap Servers

0 - exit program
Enter selection: 2
```

```
Enter the value of Snmptrap_Community
public
Enter the value of Snmptrap1_Address
10.105.242.54
Is the specified Snmptrap1_Address, Prime Central SNMP Trap Host? [ 10.105.242.54 ] Specify
 [y]es / [n]o [y]?
n
WARNING!!! Script is running without Prime Central Integration
 Enter the value of SNMP Snmptrap1 port [1162]: 162
Enter default value 12.12.12.12,if  Snmptrap2_Address is not available
12.12.12.12
 Enter the value of SNMP Snmptrap2 port [1162]: 162
Enter the value of RMS_App_Password from OVA descriptor(Enter default RMS_App_Password if
not present in descriptor)
**********
OK
Please restart [stop and start] SNMP agent.
SIOCADDRT: File exists
SIOCADDRT: File exists
Starting snmpd:
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
rms-Serving-blr01 BAC Device Provisioning Engine
User Access Verification
Password:
rms-Serving-blr01> enable
Password:
rms-Serving-blr01# dpe reload
Process [dpe] has been restarted.
Connection closed by foreign host.
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Stopping snmpd:                                            [  OK  ]
Configuring CAR Server..
200 OK
Waiting for these processes to die (this may take some time):
Cisco Prime AR RADIUS server running       (pid: 1758)
Cisco Prime AR Server Agent running        (pid: 1700)
Cisco Prime AR MCD lock manager running    (pid: 1704)
Cisco Prime AR MCD server running          (pid: 1711)
Cisco Prime AR GUI running                 (pid: 1715)
4 processes left.3 processes left.............2 processes left.k0 processes left

Cisco Prime Access Registrar Server Agent shutdown complete.
Starting Cisco Prime Access Registrar Server Agent...completed.
Done CAR Extension point configuration
Configuring CNR Server..
100 Ok
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd>
trap-recipient 10.105.242.54 create ip-addr=10.105.242.54 port-number=162 community=public
314 Duplicate object - trap-recipient 10.105.242.54 create ip-addr=10.105.242.54
port-number=162 community=public

nrcmd>
trap-recipient 12.12.12.12 create ip-addr=12.12.12.12 port-number=162 community=public
314 Duplicate object - trap-recipient 12.12.12.12 create ip-addr=12.12.12.12 port-number=162
 community=public
```

```
nrcmd>
dhcp set traps-enabled=all
100 Ok
traps-enabled=all

nrcmd>
snmp stop
100 Ok

nrcmd>
snmp start
100 Ok

nrcmd>
save
100 Ok

nrcmd>
server dhcp reload
100 Ok

nrcmd>
exit
# Stopping Network Registrar Local Server Agent
INFO: waiting for Network Registrar Local Server Agent to exit ...
INFO: waiting for Network Registrar Local Server Agent to exit ...
INFO: waiting for Network Registrar Local Server Agent to exit ...
# Starting Network Registrar Local Server Agent
Done CNR Extension point configuration
Process [snmpAgent] has been restarted.

configured Snmp Trap Servers Successfully

MENU
1 - Configure SNMP Servers
2 - Configure SNMPTrap Servers

0 - exit program

Enter selection: 0
```

Integrating FM, PMG, LUS, and RDU Alarms on Central Node with Prime Central NMS

The 'configure_fm_server.sh' script is used to integrate Cisco RMS with the Prime Central NMS for fault notification. This script allows the registration of the Domain Manager (DM) for RMS in the Prime Central NMS. Prime Central allows the receipt of SNMP traps from RMS only if DM registration for RMS is completed.

The 'configure_fm_server.sh' script

- Accepts the following NMS interface details and updates the FMServer.properties file (for FM Server) and `/etc/snmp/snmpd.conf` (for snmp).
- Adds the IPtable rules to allow the SNMP traps to be notified to the specified NMS interfaces.
    - NMS interface IP address,
    - Port number (162 or 1162)
    - Community string

- Supported SNMP version (v1 or v2c)

Subsequently, during deployment the script prompts you to specify whether one of the configured NMS is Prime Central. If it is Prime Central, the script accepts the Prime Central database server details such as, Prime Central DB server IP, DB server listening port, DB user credentials (user-ID and password), and registers the Domain Manger for RMS in Prime Central.

Perform the following procedures in the following sections to integrate active Prime Central NMS, active and Disaster Recovery Prime Central NMS, and configure two third-party trap receivers.

Integrating RMS with Active Prime Central NMS

Only active Prime Central mode is used to integrate Cisco RMS with one Prime Central NMS for fault notification.

Procedure

Step 1 Log in to the Central node.

Step 2 Switch to root user: **su -**

Step 3 Navigate to the following directory: `cd /rms/ova/scripts/post_install/`

Step 4 Run the **configure_fm_server.sh** script.

Example:

```
[blrrms-central-14-2I] ~ # su
[blrrms-central-14-2I] ~ # cd /rms/ova/scripts/post_install/
[blrrms-central-14-2I] /rms/ova/scripts/post_install # ./configure_fm_server.sh
******************Script to configure NMS interface details for
FM-Server*******************************
RMS FM Framework requires the NMS manager interface details...
To Integrate only one Active PC : 1
To Integrate both PC Active and DR mode : 2
Enter number of SNMP managers to be configured (0 to disable SNMP traps/1/2/3)
//select the option 1 for configuring only Active PC
1
Enter details for NMS-1
Enter NMS manager interface IP address
10.105.242.19
Enter NMS manager SNMP trap version(v1/v2c)
v2c
Enter NMS manager interface port number(162/1162)
1162
Enter the SNMP trap community for the NMS
public
Entering update_BACSnmpDetails()
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
Process [snmpAgent] has been restarted.

Exiting update_BACSnmpDetails()
Deleting the iptable rules, added for the earlier configured NMS...
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Assigning the variables for FMServer.properties update
Setting firewall for fm_server....
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

Is the specified NMS, Prime Central SNMP Trap Host? [ 10.105.242.19 ] Specify [y]es / [n]o
 [y]?
```

```
Y
Enter the Prime Central Server hostname as fully qualified domain name (FQDN) :
prime-central-fm3.cisco.com
   Enter the Prime Central root password :
   Select mode - Active(a) or DR(d) [a]: a
spawn ssh root@10.105.242.19
The authenticity of host '10.105.242.19 (10.105.242.19)' can't be established.
RSA key fingerprint is 68:32:c3:0a:b0:ee:c9:2f:c5:35:ff:cb:41:e9:d9:7a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.105.242.19' (RSA) to the list of known hosts.
yes
root@10.105.242.19's password:
Permission denied, please try again.
root@10.105.242.19's password:
Last login: Fri Jul 24 01:44:53 2015 from 10.196.85.22
[root@prime-central-fm3 ~]# sed -i /10.105.233.84/d /etc/hosts
[root@prime-central-fm3 ~]# sed -i /blrrms-central-14-2I/d /etc/hosts
[root@prime-central-fm3 ~]# echo 10.105.233.84     blrrms-central-14-2I >> /etc/hosts
[root@prime-central-fm3 ~]# exit
logout
Connection to 10.105.242.19 closed.
   Enter the Prime Central Database Server IP Address [10.105.242.19]:
   Enter the Prime Central database name (sid) [primedb]:
   Enter the Prime Central database port [1521]:
   Enter the Prime Central database user [primedba]:
   Enter the Prime Central database password :



********* Running DMIntegrator on blrrms-central-14-2I at Tue Sep 15 10:33:35 IST 2015
**********

 Invoking /rms/app/CSCObac/prime_integrator/DMIntegrator.sh with [PROPFILE: DMIntegrator.prop]
 [SERVER: 10.105.242.19] [SID: primedb] [USER: primedba] [PORT: 1521] [ID: ]

- Initializing
         - Checking property file
         - Validating Java
         - Setting ENVIRONMENT
         - DM install location: /rms/app/fm_server
         - User Home Direcory: /root
         - Extracting DMIntegrator.tar
         - Setting Java Path
         - JAVA BIN : /usr/java/default/bin/java -classpath
/rms/app/fm_server/prime_integrator/DMIntegrator/lib/*:/rms/app/fm_server/prime_integrator/DMIntegrator/lib

- Creating Data Source
         - Encrypting DB Passwd
         - Created /rms/app/fm_server/prime_integrator/datasource.properties
         - PRIME_DBSOURCE : /rms/app/fm_server/prime_integrator/datasource.properties
- Checking DB connection parameters
- Insert/Update DM Data in Suite DB
         - dmid.xml not found. Inserting
         - Regular case
         - Inserted with ID : rms://rms:15
- Setting up SSH on the DM
         - Setting SSH Keys
         - Copying /usr/bin/scp
         - Modifying /rms/app/fm_server/prime_local/prime_secured/ssh_config
         - file transfer test successful
- Adding Prime Central server into pc.xml
- Running DMSwitchToSuite.sh
         - /DMSwitchToSuite.sh doesn't exist. Skipping

The Integration process completed. Check the DMIntegrator.log for any additional details

Prime Central integration is successful.
*********Done************
```

Integrating RMS with Active and DRS on Prime Central NMS

Active and Disaster Recovery Server (DRS) is used to integrate Cisco RMS with two Prime Central NMS for fault notification.

Procedure

Step 1 Log in to the Central node.

Step 2 Switch to root user: **su -**

Step 3 Navigate to the following directory: `cd /rms/ova/scripts/post_install/`

Step 4 Run the **configure_fm_server.sh** script.

Example:

```
[blrrms-central-14-2I] /rms/ova/scripts/post_install # ./configure_fm_server.sh
******************Script to configure NMS interface details for
FM-Server*****************************
RMS FM Framework requires the NMS manager interface details...
To Integrate only one Active PC : 1
To Integrate both PC Active and DR mode : 2
Enter number of SNMP managers to be configured (0 to disable SNMP traps/1/2/3)
2
Enter details for NMS-1
Enter NMS manager interface IP address
10.105.242.19
Enter NMS manager SNMP trap version(v1/v2c)
v2c
Enter NMS manager interface port number(162/1162)
1162
Enter the SNMP trap community for the NMS
public
Enter details for NMS-2
Enter NMS manager interface IP address
10.105.242.36
Enter NMS manager SNMP trap version(v1/v2c)
v2c
Enter NMS manager interface port number(162/1162)
1162
Enter the SNMP trap community for the NMS
public
Entering update_BACSnmpDetails()
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
Process [snmpAgent] has been restarted.

Exiting update_BACSnmpDetails()
Deleting the iptable rules, added for the earlier configured NMS...
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Assigning the variables for FMServer.properties update
Setting firewall for fm_server....
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

Is the specified NMS, Prime Central SNMP Trap Host? [ 10.105.242.19 ] Specify [y]es / [n]o
 [y]?
y
 Enter the Prime Central Server hostname as fully qualified domain name (FQDN) :
prime-central-fm3.cisco.com
   Enter the Prime Central root password :
   Select mode - Active(a) or DR(d) [a]: a
spawn ssh root@10.105.242.19
```

```
root@10.105.242.19's password:
Last login: Fri Jul 24 01:46:17 2015 from 10.105.233.84
[root@prime-central-fm3 ~]# sed -i /10.105.233.84/d /etc/hosts
[root@prime-central-fm3 ~]# sed -i /blrrms-central-14-2I/d /etc/hosts
[root@prime-central-fm3 ~]# echo 10.105.233.84     blrrms-central-14-2I >> /etc/hosts
[root@prime-central-fm3 ~]# exit
logout
Connection to 10.105.242.19 closed.
   Enter the Prime Central Database Server IP Address [10.105.242.19]:
   Enter the Prime Central database name (sid) [primedb]:
   Enter the Prime Central database port [1521]:
   Enter the Prime Central database user [primedba]:
   Enter the Prime Central database password :



********* Running DMIntegrator on blrrms-central-14-2I at Tue Sep 15 11:18:23 IST 2015
**********

 Invoking /rms/app/CSCObac/prime_integrator/DMIntegrator.sh with [PROPFILE: DMIntegrator.prop]
 [SERVER: 10.105.242.19] [SID: primedb] [USER: primedba] [PORT: 1521] [ID: ]

- Initializing
         - Checking property file
         - Validating Java
         - Setting ENVIRONMENT
         - DM install location: /rms/app/fm_server
         - User Home Direcory: /root
         - Extracting DMIntegrator.tar
         - Setting Java Path
         - JAVA BIN : /usr/java/default/bin/java -classpath
/rms/app/fm_server/prime_integrator/DMIntegrator/lib/*:/rms/app/fm_server/prime_integrator/DMIntegrator/lib

- Creating Data Source
         - Encrypting DB Passwd
         - Created /rms/app/fm_server/prime_integrator/datasource.properties
         - PRIME_DBSOURCE : /rms/app/fm_server/prime_integrator/datasource.properties
- Checking DB connection parameters
- Insert/Update DM Data in Suite DB
         - dmid.xml not found. Inserting
         - Regular case
         - Inserted with ID : rms://rms:16
- Setting up SSH on the DM
         - Setting SSH Keys
         - Copying /usr/bin/scp
         - Modifying /rms/app/fm_server/prime_local/prime_secured/ssh_config
         - file transfer test successful
- Adding Prime Central server into pc.xml
- Running DMSwitchToSuite.sh
         - /DMSwitchToSuite.sh doesn't exist. Skipping

The Integration process completed. Check the DMIntegrator.log for any additional details

Prime Central integration is successful.
Is the specified NMS, Prime Central SNMP Trap Host? [ 10.105.242.36 ] Specify [y]es / [n]o
 [y]?
y
 Enter the Prime Central Server hostname as fully qualified domain name (FQDN) :
blr-primecentral-FM2.cisco.com
   Enter the Prime Central root password :
   Select mode - Active(a) or DR(d) [a]: d
spawn ssh root@10.105.242.36
WARNING: DSA key found for host 10.105.242.36
in /root/.ssh/known_hosts:4
DSA key fingerprint d5:b1:ef:3c:11:b9:35:75:cc:a2:d3:f3:52:56:76:32.
+--[ DSA 1024]----+
|             .  oo|
|            . oE.O|
|           . ooo*+|
|          .  o.o++|
|         S    .+= |
|              o...|
```

```
|             +. |
|               . |
|                 |
+-----------------+

The authenticity of host '10.105.242.36 (10.105.242.36)' can't be established
but keys of different type are already known for this host.
RSA key fingerprint is a5:1f:11:9e:2d:01:15:1a:38:4b:d0:5f:17:f6:56:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.105.242.36' (RSA) to the list of known hosts.
yes
root@10.105.242.36's password:
Permission denied, please try again.
root@10.105.242.36's password:
Last login: Fri Jul 24 04:17:42 2015 from 10.196.85.22
[root@blr-primecentral-FM2 ~]# sed -i /10.105.233.84/d /etc/hosts
[root@blr-primecentral-FM2 ~]# sed -i /blrrms-central-14-2I/d /etc/hosts
[root@blr-primecentral-FM2 ~]# echo 10.105.233.84     blrrms-central-14-2I >> /etc/hosts
[root@blr-primecentral-FM2 ~]# exit
logout
Connection to 10.105.242.36 closed.
   Enter the Prime Central Domain Manager (DM) Id [1]: 16
   Enter the Prime Central Database Server IP Address [10.105.242.36]:
   Enter the Prime Central database name (sid) [primedb]:
   Enter the Prime Central database port [1521]:
   Enter the Prime Central database user [primedba]:
   Enter the Prime Central database password :


********* Running DMIntegrator on blrrms-central-14-2I at Tue Sep 15 12:20:05 IST 2015
**********

 Invoking /rms/app/CSCObac/prime_integrator/DMIntegrator.sh with [PROPFILE: DMIntegrator.prop]
 [SERVER: 10.105.242.36] [SID: primedb] [USER: primedba] [PORT: 1521] [ID: 16]

- Initializing
         - Checking property file
         - Validating Java
         - Setting ENVIRONMENT
         - DM install location: /rms/app/fm_server
         - User Home Direcory: /root
         - Extracting DMIntegrator.tar
         - Setting Java Path
         - JAVA BIN : /usr/java/default/bin/java -classpath
/rms/app/fm_server/prime_integrator/DMIntegrator/lib/*:/rms/app/fm_server/prime_integrator/DMIntegrator/lib

- Creating Data Source
         - Encrypting DB Passwd
         - Created /rms/app/fm_server/prime_integrator/datasource.properties
         - PRIME_DBSOURCE : /rms/app/fm_server/prime_integrator/datasource.properties
- Checking DB connection parameters
- Checking if ID is valid
- Insert/Update DM Data in Suite DB
         - dmid.xml not found. Inserting
         - Disaster Recovery case
         - Inserted with ID : rms://rms:16
- Setting up SSH on the DM
         - Setting SSH Keys
         - Copying /usr/bin/scp
         - Modifying /rms/app/fm_server/prime_local/prime_secured/ssh_config
         - file transfer test successful
- Adding Prime Central server into pc.xml
- Running DMSwitchToSuite.sh
         - /DMSwitchToSuite.sh doesn't exist. Skipping

The Integration process completed. Check the DMIntegrator.log for any additional details

Prime Central integration is successful.
*********Done************
```

Integrating RMS with Two Third-Party Trap Receivers

Two third-party trap receivers are used to integrate Cisco RMS for fault notification.

Procedure

Step 1 Log in to the Central node.

Step 2 Switch to root user: **su -**

Step 3 Navigate to the following directory: `cd /rms/ova/scripts/post_install/`

Step 4 Run the **configure_fm_server.sh** script.

Example:

```
[blrrms-central-14-2I] /rms/ova/scripts/post_install # ./configure_fm_server.sh
******************Script to configure NMS interface details for
FM-Server*******************************
RMS FM Framework requires the NMS manager interface details...
To Integrate only one Active PC : 1
To Integrate both PC Active and DR mode : 2
Enter number of SNMP managers to be configured (0 to disable SNMP traps/1/2/3)
2
Enter details for NMS-1
Enter NMS manager interface IP address
10.105.242.30
Enter NMS manager SNMP trap version(v1/v2c)
v2c
Enter NMS manager interface port number(162/1162)
1162
Enter the SNMP trap community for the NMS
public
Enter details for NMS-2
Enter NMS manager interface IP address
10.105.242.78
Enter NMS manager SNMP trap version(v1/v2c)
v2c
Enter NMS manager interface port number(162/1162)
1162
Enter the SNMP trap community for the NMS
public
Entering update_BACSnmpDetails()
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
Process [snmpAgent] has been restarted.

Exiting update_BACSnmpDetails()
Deleting the iptable rules, added for the earlier configured NMS...
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Assigning the variables for FMServer.properties update
Setting firewall for fm_server....
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

Is the specified NMS, Prime Central SNMP Trap Host? [ 10.105.242.30 ] Specify [y]es / [n]o
 [y]?
n
Is the specified NMS, Prime Central SNMP Trap Host? [ 10.105.242.78 ] Specify [y]es / [n]o
 [y]?
n
*********Done************
[blrrms-central-14-2I] /rms/ova/scripts/post_install #
```

Integrating BAC, PAR, and PNR on Serving Node with Prime Central NMS

To integrate BAC, PAR, and PNR on the Serving node with Prime Central active server, configure active Prime Central NMS, active and Disaster Recovery Prime Central NMS, and configure two third-party trap receivers.

Integrating Serving Node with Prime Central Active Server

Procedure

Step 1 Log in to the Serving node.

Step 2 Switch to root user: **su -**

Step 3 Change the directory: `cd /rms/ova/scripts/post_install`

Step 4 Navigate to the following directory: `cd /rms/ova/scripts/post_install/`

Step 5 Run the **./configuresnmpservingnode.sh script.**script.

Example:

```
[admin1@rms-Serving-blr01 ~]$ su
Password:
[root@rms-Serving-blr01 admin1]# cd /rms/ova/scripts/post_install/
[root@rms-Serving-blr01 post_install]# ./configuresnmpservingnode.sh
******************Post-installation script to configure SNMP on RMS Serving
Node*****************************

MENU
1 - Configure SNMP Servers
2 - Configure SNMPTrap Servers

0 - exit program

Enter selection: 2

Enter the value of Snmptrap_Community
public
Enter the value of Snmptrap1_Address
10.105.242.36
Is the specified Snmptrap1_Address, Prime Central (Active) SNMP Trap Host? [ 10.105.242.36
 ] Specify [y]es / [n]o [y]?
y
   Enter the Prime Central (Active) Server hostname as fully qualified domain name (FQDN)
:
blr-primecentral-FM2.cisco.com
   Enter the Prime Central (Active) root password :
 Enter the value of SNMP Snmptrap1 port [1162]: 1162
Enter default value 12.12.12.12,if  Snmptrap2_Address is not available
12.12.12.12
 Enter the value of SNMP Snmptrap2 port [1162]: 162
Enter the value of RMS_App_Password from OVA descriptor(Enter default RMS_App_Password if
not present in descriptor)
OK
Please restart [stop and start] SNMP agent.
SIOCADDRT: File exists
```

```
Starting snmpd:
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

rms-Serving-blr01 BAC Device Provisioning Engine


User Access Verification

Password:

rms-Serving-blr01> enable
Password:
rms-Serving-blr01# dpe reload
Connection closed by foreign host.
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
spawn ssh root@10.105.242.36
The authenticity of host '10.105.242.36 (10.105.242.36)' can't be established.
RSA key fingerprint is a5:1f:11:9e:2d:01:15:1a:38:4b:d0:5f:17:f6:56:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.105.242.36' (RSA) to the list of known hosts.
yes
root@10.105.242.36's password:
Last login: Thu Jun 18 11:34:45 2015 from 10.78.184.154
[root@blr-primecentral-FM2 ~]# sed -i /10.5.1.16/d /etc/hosts
[root@blr-primecentral-FM2 ~]# sed -i /rms-Serving-blr01/d /etc/hosts
[root@blr-primecentral-FM2 ~]# echo 10.5.1.16     rms-Serving-blr01 >> /etc/hosts
[root@blr-primecentral-FM2 ~]# exit
logout
Connection to 10.105.242.36 closed.
Integrating BAC with Prime Central (Active). Are you sure? (y/n) [n]: y
   Select mode - Active(a) or DR(d) [a]: a
   Enter the Prime Central Database Server IP Address [10.5.1.16]: 10.105.242.36
   Enter the Prime Central database name (sid) [primedb]: primedb
   Enter the Prime Central database port [1521]: 1521
   Enter the Prime Central database user [primedba]: primedba
   Enter the Prime Central database password :
   Enter the Prime Central SNMP Trap Host IP address [10.105.242.36]: 10.105.242.36
   Enter the Prime Central SNMP Trap port [1162]: 1162



********* Running DMIntegrator on rms-Serving-blr01 at Thu Jun 18 11:44:35 IST 2015
**********

 Invoking ./DMIntegrator.sh with [PROPFILE: DMIntegrator.prop] [SERVER: 10.105.242.36] [SID:
 primedb] [USER: primedba] [PORT: 1521] [ID: ]

.
.
.
.
configured Snmp Trap Servers Successfully

MENU
1 - Configure SNMP Servers
2 - Configure SNMPTrap Servers

0 - exit program

Enter selection:
```

Note In the above script output, make a note of the DM ID value (*Inserted with ID : bac://bac:34*) and the same DM ID value should be used for Prime Central Disaster Recovery Server integration.

Integrating Serving Node with Active and DRS on Prime Central NMS

Active and Disaster Recovery Server (DRS) is used to integrate Cisco RMS with two Prime Central NMS for fault notification.

Procedure

Step 1 Log in to the Serving node.

Step 2 Switch to root user: **su -**

Step 3 Navigate to the following directory: `cd /rms/ova/scripts/post_install`

Step 4 Run the **./configuresnmpservingnode.sh** script.

Example:

```
[root@blrrms-serving-14-2I post_install]# ./configuresnmpservingnode.sh s
******************Post-installation script to configure SNMP on RMS Serving
Node*****************************

MENU
1 - Configure SNMPTrap Servers

0 - exit program

Enter selection: 1

SUBMENU
=======
1 - To Integrate only one SNMP trap receiver [PC(Active)/third party trap receiver]
2 - To Integrate two SNMP trap receivers, following combinations are suppotred
  - [ a) both Active and DR mode PCs, b) Two third party trap receivers ]
Enter number of SNMP managers to be configured (0-to disable SNMP traps/1/2/CTRL+C to exit)
2
Enter the value of Snmptrap_Community
public
Enter the value of Snmptrap1_Address
10.105.242.19
Is the specified SNMP Trap Receiver Address, Prime Central SNMP Trap Host? [ 10.105.242.19
 ] Specify [y]es / [n]o [y]?
y
   Enter the Prime Central Server hostname as fully qualified domain name (FQDN) :
prime-central-fm3.cisco.com
   Enter the Prime Central root password :
 Enter the value of SNMP Snmptrap1 port [1162]:
Enter the value of Snmptrap2_Address
10.105.242.36
Is the specified SNMP Trap Receiver Address, Prime Central SNMP Trap Host? [ 10.105.242.36
 ] Specify [y]es / [n]o [y]?
y
   Enter the Prime Central Server hostname as fully qualified domain name (FQDN) :
blr-primecentral-FM2.cisco.com
   Enter the Prime Central root password :
 Enter the value of SNMP Snmptrap2 port [1162]:
Enter the value of RMS_App_Password from OVA descriptor(Enter default RMS_App_Password if
not present in descriptor)
Connection closed by foreign host.
Please try again with correct RMS_App_Password
```

```
Connection closed by foreign host.
SIOCDELRT: No such process
SIOCDELRT: No such process
sed: -e expression #1, char 42: Invalid preceding regular expression
sed: -e expression #1, char 34: Invalid preceding regular expression
OK
Please restart [stop and start] SNMP agent.
sed: -e expression #1, char 34: Invalid preceding regular expression
OK
Please restart [stop and start] SNMP agent.
Removing old iptable rules
iptables: Bad rule (does a matching rule exist in that chain?).
iptables: Bad rule (does a matching rule exist in that chain?).
Removing old iptable rules Done.
SIOCADDRT: File exists
SIOCADDRT: File exists
Starting snmpd:
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

blr-rms15-serving BAC Device Provisioning Engine


User Access Verification

Password:

blr-rms15-serving> enable
Password:
blr-rms15-serving# dpe reload
Process [dpe] has been restarted.

Connection closed by foreign host.
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
spawn ssh root@10.105.242.19
root@10.105.242.19's password:
Last login: Fri Jul 24 05:32:04 2015 from 10.5.1.72
[root@prime-central-fm3 ~]# sed -i /10.5.1.72/d /etc/hosts
[root@prime-central-fm3 ~]# sed -i /blr-rms15-serving/d /etc/hosts
[root@prime-central-fm3 ~]# echo 10.5.1.72     blr-rms15-serving >> /etc/hosts
[root@prime-central-fm3 ~]# exit
logout
Connection to 10.105.242.19 closed.
Integrating BAC with Prime Central. Are you sure? (y/n) [n]: y
   Select mode - Active(a) or DR(d) [a]: a
   Enter the Prime Central Database Server IP Address [10.5.1.72]: 10.105.242.19
   Enter the Prime Central database name (sid) [primedb]:
   Enter the Prime Central database port [1521]:
   Enter the Prime Central database user [primedba]:
   Enter the Prime Central database password :
   Enter the Prime Central SNMP Trap Host IP address [10.105.242.19]:
   Enter the Prime Central SNMP Trap port [1162]:



********* Running DMIntegrator on blr-rms15-serving at Tue Sep 15 14:51:27 IST 2015
**********

 Invoking ./DMIntegrator.sh with [PROPFILE: DMIntegrator.prop] [SERVER: 10.105.242.19] [SID:
 primedb] [USER: primedba] [PORT: 1521] [ID: ]

- Initializing
         - Checking property file
         - Validating Java
         - Setting ENVIRONMENT
         - DM install location: /rms/app/CSCObac
```

```
        - User Home Direcory: /root
        - Extracting DMIntegrator.tar
        - Setting Java Path
        - JAVA BIN : /rms/app/CSCObac/jre/bin/java -classpath
/rms/app/CSCObac/prime_integrator/DMIntegrator/lib/*:/rms/app/CSCObac/prime_integrator/DMIntegrator/lib

- Creating Data Source
        - Encrypting DB Passwd
        - Created /rms/app/CSCObac/prime_integrator/datasource.properties
        - PRIME_DBSOURCE : /rms/app/CSCObac/prime_integrator/datasource.properties
- Checking DB connection parameters
- Insert/Update DM Data in Suite DB
        - dmid.xml not found. Inserting
        - Regular case
        - Inserted with ID : bac://bac:19
- Setting up SSH on the DM
        - Setting SSH Keys
        - Copying /usr/bin/scp
        - Modifying /rms/app/CSCObac/prime_local/prime_secured/ssh_config
        - file transfer test successful
- Adding Prime Central server into pc.xml
- Running DMSwitchToSuite.sh
        - /DMSwitchToSuite.sh doesn't exist. Skipping

The Integration process completed. Check the DMIntegrator.log for any additional details

Updating trap host and port
Process [snmpAgent] has been restarted.

Prime Central integration is successful.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
spawn ssh root@10.105.242.36
root@10.105.242.36's password:
Last login: Fri Jul 24 06:34:18 2015 from 10.5.1.72
[root@blr-primecentral-FM2 ~]# sed -i /10.5.1.72/d /etc/hosts
[root@blr-primecentral-FM2 ~]# sed -i /blr-rms15-serving/d /etc/hosts
[root@blr-primecentral-FM2 ~]# echo 10.5.1.72     blr-rms15-serving >> /etc/hosts
[root@blr-primecentral-FM2 ~]# exit
logout
Connection to 10.105.242.36 closed.
Integrating BAC with Prime Central. Are you sure? (y/n) [n]: y
   Select mode - Active(a) or DR(d) [a]: d
   Enter the Prime Central Database Server IP Address [10.5.1.72]: 10.105.242.36
   Enter the Prime Central database name (sid) [primedb]:
   Enter the Prime Central database port [1521]:
   Enter the Prime Central database user [primedba]:
   Enter the Prime Central database password :
   Enter the Prime Central SNMP Trap Host IP address [10.105.242.36]:
   Enter the Prime Central SNMP Trap port [1162]:
   Enter the Prime Central Domain Manager (DM) Id [1]: 19



********* Running DMIntegrator on blr-rms15-serving at Tue Sep 15 14:56:13 IST 2015
***********

 Invoking ./DMIntegrator.sh with [PROPFILE: DMIntegrator.prop] [SERVER: 10.105.242.36] [SID:
 primedb] [USER: primedba] [PORT: 1521] [ID: 19]

- Initializing
        - Checking property file
        - Validating Java
        - Setting ENVIRONMENT
        - DM install location: /rms/app/CSCObac
        - User Home Direcory: /root
        - Extracting DMIntegrator.tar
        - Setting Java Path
        - JAVA BIN : /rms/app/CSCObac/jre/bin/java -classpath
/rms/app/CSCObac/prime_integrator/DMIntegrator/lib/*:/rms/app/CSCObac/prime_integrator/DMIntegrator/lib

- Creating Data Source
```

```
         - Encrypting DB Passwd
         - Created /rms/app/CSCObac/prime_integrator/datasource.properties
         - PRIME_DBSOURCE : /rms/app/CSCObac/prime_integrator/datasource.properties
- Checking DB connection parameters
- Checking if ID is valid
- Insert/Update DM Data in Suite DB
         - dmid.xml not found. Inserting
         - Disaster Recovery case
         - Inserted with ID : bac://bac:19
- Setting up SSH on the DM
         - Setting SSH Keys
         - Copying /usr/bin/scp
         - Modifying /rms/app/CSCObac/prime_local/prime_secured/ssh_config
         - file transfer test successful
- Adding Prime Central server into pc.xml
- Running DMSwitchToSuite.sh
         - /DMSwitchToSuite.sh doesn't exist. Skipping

The Integration process completed. Check the DMIntegrator.log for any additional details

Updating trap host and port
Process [snmpAgent] has been restarted.

Prime Central integration is successful.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Stopping snmpd:                                            [  OK  ]
Cisco Prime Access Registrar Server Agent is not running, Skipping the CAR Server SNMP
Configuration ...
Configuring CNR Server..
109 Ok - resource status is Critical: 1, OK: 8
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd>
trap-recipient 10.105.242.19 create ip-addr=10.105.242.19 port-number=1162 community=public
100 Ok
10.105.242.19:
    agent-addr =
    community = public
    ip-addr = 10.105.242.19
    ip6address =
    port-number = 1162
    tenant-id = 0  tag: core
    v6-port-number = [default=162]

nrcmd>
dhcp set traps-enabled=all
100 Ok
traps-enabled=all

nrcmd>
snmp stop
100 Ok

nrcmd>
snmp start
100 Ok

nrcmd>
save
100 Ok

nrcmd>
server dhcp reload
```

```
100 Ok

nrcmd>
exit
109 Ok - resource status is Critical: 1, OK: 8
109 Ok - resource status is Critical: 1, OK: 8
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd>
trap-recipient 10.105.242.36 create ip-addr=10.105.242.36 port-number=1162 community=public
100 Ok
10.105.242.36:
    agent-addr =
    community = public
    ip-addr = 10.105.242.36
    ip6address =
    port-number = 1162
    tenant-id = 0  tag: core
    v6-port-number = [default=162]

nrcmd>
dhcp set traps-enabled=all
100 Ok
traps-enabled=all

nrcmd>
snmp stop
100 Ok

nrcmd>
snmp start
100 Ok

nrcmd>
save
100 Ok

nrcmd>
server dhcp reload
100 Ok

nrcmd>
exit
109 Ok - resource status is Critical: 1, OK: 8
# Stopping Network Registrar Local Server Agent
INFO: waiting for Network Registrar Local Server Agent to exit ...
INFO: waiting for Network Registrar Local Server Agent to exit ...
INFO: waiting for Network Registrar Local Server Agent to exit ...
# Starting Network Registrar Local Server Agent
Done CNR Extension point configuration
Process [snmpAgent] has been restarted.




configured Snmp Trap Servers Successfully

MENU
1 - Configure SNMPTrap Servers

0 - exit program
```

```
Enter selection:
```

Integrating Serving Node with Two Third-Party Trap Receivers

Two third-party trap receivers are used to integrate Cisco RMS for fault notification.

Procedure

Step 1 Log in to the Serving node.

Step 2 Switch to root user: **su -**

Step 3 Navigate to the following directory: `cd /rms/ova/scripts/post_install`

Step 4 Run the **./configuresnmpservingnode.sh** script.

Example:

```
[root@blrrms-serving-14-2I admin1]# cd /rms/ova/scripts/post_install/
[root@blrrms-serving-14-2I post_install]# ./configuresnmpservingnode.sh
******************Post-installation script to configure SNMP on RMS Serving
Node*******************************

MENU
1 - Configure SNMPTrap Servers

0 - exit program

Enter selection: 1

SUBMENU
=======
1 - To Integrate only one SNMP trap receiver [PC(Active)/third party trap receiver]
2 - To Integrate two SNMP trap receivers, following combinations are suppotred
  - [ a) both Active and DR mode PCs, b) Two third party trap receivers ]
Enter number of SNMP managers to be configured (0-to disable SNMP traps/1/2/CTRL+C to exit)
2
Enter the value of Snmptrap_Community
public
Enter the value of Snmptrap1_Address
10.105.242.64
Is the specified SNMP Trap Receiver Address, Prime Central SNMP Trap Host? [ 10.105.242.64
 ] Specify [y]es / [n]o [y]?
n
WARNING!!! Script is running without Prime Central Integration
 Enter the value of SNMP Snmptrap1 port [1162]: 162
Enter the value of Snmptrap2_Address
10.105.242.17
Is the specified SNMP Trap Receiver Address, Prime Central SNMP Trap Host? [ 10.105.242.17
 ] Specify [y]es / [n]o [y]?
n
WARNING!!! Script is running without Prime Central Integration
 Enter the value of SNMP Snmptrap2 port [1162]: 162
Enter the value of RMS_App_Password from OVA descriptor(Enter default RMS_App_Password if
not present in descriptor)
Connection closed by foreign host.
Please try again with correct RMS_App_Password
Connection closed by foreign host.
Please try again with correct RMS_App_Password
Connection closed by foreign host.
Please try again with correct RMS_App_Password
Connection closed by foreign host.
SIOCDELRT: No such process
```

```
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
Removing old iptable rules
iptables: Bad rule (does a matching rule exist in that chain?).
Removing old iptable rules Done.
Starting snmpd:
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

blrrms-serving-14-2I BAC Device Provisioning Engine


User Access Verification

Password:

blrrms-serving-14-2I> enable
Password:
blrrms-serving-14-2I# dpe reload
Connection closed by foreign host.
OK
Please restart [stop and start] SNMP agent.
OK
Please restart [stop and start] SNMP agent.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Stopping snmpd:                                            [  OK  ]
Configuring CAR Server..
200 OK
Waiting for these processes to die (this may take some time):
Cisco Prime AR RADIUS server running       (pid: 1840)
Cisco Prime AR Server Agent running        (pid: 1782)
Cisco Prime AR MCD lock manager running    (pid: 1785)
Cisco Prime AR MCD server running          (pid: 1793)
Cisco Prime AR GUI running                 (pid: 1797)
4 processes left.3 processes left.............k0 processes left

Cisco Prime Access Registrar Server Agent shutdown complete.
Starting Cisco Prime Access Registrar Server Agent...........Restarting...
Waiting for these processes to die (this may take some time):
Cisco Prime AR RADIUS server terminated    (pid: )
Cisco Prime AR Server Agent running        (pid: 5298)
Cisco Prime AR MCD lock manager running    (pid: 5302)
Cisco Prime AR MCD server running          (pid: 5593)
Cisco Prime AR GUI running                 (pid: 5313)
SNMP Master Agent running                (pid: 5312)
4 processes left.2 processes left.............k0 processes left

Cisco Prime Access Registrar Server Agent shutdown complete.
Starting Cisco Prime Access Registrar Server Agent...completed.
Done CAR Extension point configuration
Configuring CNR Server..
109 Ok - resource status is Critical: 1, OK: 8
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd>
trap-recipient 10.105.242.64 create ip-addr=10.105.242.64 port-number=162 community=public
100 Ok
10.105.242.64:
    agent-addr =
    community = public
```

```
    ip-addr = 10.105.242.64
    ip6address =
    port-number = 162
    tenant-id = 0  tag: core
    v6-port-number = [default=162]

nrcmd>
dhcp set traps-enabled=all
100 Ok
traps-enabled=all

nrcmd>
snmp stop
100 Ok

nrcmd>
snmp start
100 Ok

nrcmd>
save
100 Ok

nrcmd>
server dhcp reload
100 Ok

nrcmd>
exit
109 Ok - resource status is Critical: 1, OK: 8
109 Ok - resource status is Critical: 1, OK: 8
session:
    cluster = localhost
    current-view = Default
    current-vpn = global
    default-format = user
    dhcp-edit-mode = synchronous
    dns-edit-mode = synchronous
    groups = superuser
    roles = superuser
    user-name = cnradmin
    visibility = 5
nrcmd>
trap-recipient 10.105.242.17 create ip-addr=10.105.242.17 port-number=162 community=public
100 Ok
10.105.242.17:
    agent-addr =
    community = public
    ip-addr = 10.105.242.17
    ip6address =
    port-number = 162
    tenant-id = 0  tag: core
    v6-port-number = [default=162]

nrcmd>
dhcp set traps-enabled=all
100 Ok
traps-enabled=all

nrcmd>
snmp stop
100 Ok

nrcmd>
snmp start
100 Ok

nrcmd>
save
100 Ok

nrcmd>
```

```
server dhcp reload
100 Ok

nrcmd>
exit
109 Ok - resource status is Critical: 1, OK: 8
# Stopping Network Registrar Local Server Agent
INFO: waiting for Network Registrar Local Server Agent to exit ...
INFO: waiting for Network Registrar Local Server Agent to exit ...
INFO: waiting for Network Registrar Local Server Agent to exit ...
# Starting Network Registrar Local Server Agent
Done CNR Extension point configuration
Process [snmpAgent] has been restarted.



configured Snmp Trap Servers Successfully

MENU
1 - Configure SNMPTrap Servers

0 - exit program

Enter selection:
```

De-Registering RMS with Prime Central Post-Deployment

To re-run the Cisco RMS integration with Prime Central on the Central and Serving nodes, complete the procedures listed in this section before the integration. It is mandatory to de-register Cisco RMS with Prime Central NMS before the rerun:

- Disabling SNMP Traps Notification to Prime Central NMS Interface, on page 157
- Cleaning Up Files On Central Node, on page 158
- Cleaning Up Files On Serving Node, on page 158
- De-Registering RMS Data Manager from Prime Central, on page 159

Disabling SNMP Traps Notification to Prime Central NMS Interface

Follow these steps to disable SNMP traps notifications to the Prime Central NMS interface on the Cisco RMS Central node

Procedure

Step 1 Log in to the Central node and run the following commands.

Example:

```
[rms-aio-central]cd /rms/ova/scripts/post_install
./configure_fm_server.sh
```

Step 2 Enter the number of SNMP managers to be configured as ' 0 ' to de-register the Prime Central NMS interface. This disables the SNMP trap notification. The script execution output log is displayed as follows

Example:

```
[rms-aio-central] /rms/ova/scripts/post_install # ./configure_fm_server.sh
********************Script to configure NMS interface details for
FM-Server*******************************
RMS FM Framework requires the NMS manager interface details...
Enter number of SNMP managers to be configured (0 to disable SNMP traps/1/2/3)
0
Disabling SNMP traps from RMS
Deleting the iptable rules, added for the earlier configured NMS...
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
*********Done************
[rms-aio-central] /rms/ova/scripts/post_install #
```

Cleaning Up Files On Central Node

To clean up the files on the Central node, which was generated from the earlier Prime Central integration procedure, complete these steps:

Procedure

Step 1 Log in to the Central node as root user.

Step 2 Navigate to the `/rms/app/fm_server/prime_integrator` directory.

Step 3 Enter the following command:

```
rm –rf DMIntegrator.log DMIntegrator.prop datasource.properties dbpasswd.pwd dmid.xml jms.log
 pc.xml
```

Step 4 Enter `/rms/app/CSCObac/snmp/bin/snmpAgentCfgUtil.sh` and delete host <rms-aio-central>; ' rms-aio-central' is the host name of the RMS Central node.

Cleaning Up Files On Serving Node

To clean up the files on the Serving node, which was generated from the earlier Prime Central integration procedure, complete these steps.

Procedure

Step 1 Log in to the Central node as root user.

Step 2 Navigate to the `cd /rms/app/CSCObac/prime_integrator/` directory.

Step 3 Enter the following command:

```
Enter rm –rf DMIntegrator.log DMIntegrator.prop datasource.properties dbpasswd.pwd dmid.xml
 jms.log pc.xml.
```

Step 4 Enter `/rms/app/CSCObac/snmp/bin/snmpAgentCfgUtil.sh` and delete host <host name>.

Step 5 Restart the SnmpAgent.

De-Registering RMS Data Manager from Prime Central

De-register RMS Data Manager from Prime Central, which was used to integrate RMS with Prime Central earlier.

Procedure

Step 1 Log in to the Prime Central server using ssh with 'root' user ID and password.

Step 2 Switch to: **su - primeusr**.

Step 3 Execute the **list** command to find the ID value assigned to the RMS host (Central node host name).

Step 4 Enter **cd ~/install/scripts**.

Step 5 Enter **./dmRemoveUtil**.
When prompted, enter the Central administrator user ID and password and the RMS ID value, which is described in Step 3.

Step 6 Enter **itgctl stop** and **itgctl start**.

Step 7 Log out from the Prime Central server.

Starting Database and Configuration Backups on Central VM

Set the cron job to take periodic backup of the configurations and databases. Specify the hour of day with inputs for number of days of retention of backups and postgress DB password. Follow this procedure to set the cron job.

Procedure

Step 1 Log in to the Central node as root user.

Step 2 Edit the cron tab using the following commands:

```
export EDITOR=vi;
crontab -e
```

Step 3 Set and save the cron job for creating the backup of the configurations, RDU, and postgres databases.

```
<minute> <hour> * * * /rms/ova/scripts/redundancy/backup_central_vm.cron.hourly <number of
 days of backup retention> <Postgress DB password>
```

Note <Postgress DB password> is the value of the RMS_App_Password property provided during RMS installation.

Example:

```
0 6 * * * /rms/ova/scripts/redundancy/backup_central_vm.cron.hourly 3 Rmsuser@1
```

Step 4 View the content of the cron tab using the **crontab -l** command.

Example:

```
[blr-rms19-central] /home/admin1 # crontab -l
0 6 * * * /rms/ova/scripts/redundancy/backup_central_vm.cron.hourly 3 Rmsuser@1
[blr-rms19-central] /home/admin1 #
```

Step 5 Check for the backup file at the location `/rms/backups/` after the hour of day specified in the cron job. Sample filename is "centralVmBackup_2014-06-25-16-00.tar.gz".

Note The cron jobs for all users must be backed up to be restored later across all the Central nodes during disaster recovery.

Optional Features

Following sections explain how to configure the optional features:

Default Reserved Mode Setting for Enterprise APs

To enable the default reserved mode settings for an enterprise AP by default, run configure_ReservedMode.sh.

configure_ReservedMode.sh

Note Run the script using the *-h* option to check the feature getting enabled with this script.

This tool enables the `Set default Reserved-mode setting to True for Enterprise APs` configuration in RMS.

The script is present in the `/rms/ova/scripts/post_install` path. To execute the script, log in as 'root' user navigate to the path and execute configure_ReservedMode.sh.

Sample Output

```
[RMS51G-CENTRAL03] /rms/ova/scripts/post_install # ./configure_ReservedMode.sh
*************Enabling the following configurations in RMS*********************************
*************Setting default Reserved-mode setting to True for Enterprise APs*************
*************Applying screen configurations*******************
*************Executing kiwis*******************
/rms/app/baseconfig/bin /rms/ova/scripts/post_install
/rms/app/baseconfig/bin /rms/app/baseconfig/bin

Running 'apiscripter.sh /rms/app/baseconfig/ga_kiwi_scripts/custom1/setDefResMode.kiwi'...
.
.
.
.
.
.
The following tasks were affected:
AlarmHandler
/etc/init.d /rms/ova/scripts/post_install
Process [tomcat] has been restarted. Encountered an error while stopping.

/rms/ova/scripts/post_install
*************************Done***********************************
```

The following procedure is the workaround if the PMG server status is in an unmonitored state.

Procedure

Step 1 Check if the PMGServer status is up. To do this:

a) Log in to RMS Central node as root login.

b) Check PMGServer status by executing the following command.

Example:

```
[rms-aio-central] /home/admin1 # god status PMGServer
PMGServer: up
```

Note If the PMGServer status is up as shown in Step 1b, skip Step 2. If the PMGServer status shows as "unmonitored" in Step 1b, then proceed to Step 2.

Step 2 If the PMGServer status is unmonitored, run the following command.

Example:

```
god start PMGServer
Sending 'start' command

The following watches were affected:
PMGServer

check the status PMGServer should be up and running after sometime

[rms-aio-central] /home/admin1 # god status PMGServer
PMGServer: up
```

Configuring Linux Administrative Users

By default **admin1** user is provided with RMS deployment. Use the following steps post installation in the Central, Serving, and Upload node to add additional administrative users or to change the passwords of existing administrative users.

Note Changing the root user password is not supported with this post install script.

Use the following steps to configure users on the Central, Serving, or Upload nodes:

Procedure

Step 1 Log in to the **Central node**.

Step 2 ssh to the Serving or Upload node as required
This step is required to configure users on either the Serving or Upload node only.

Step 3 Switch to root user: **su -**

Step 4 Change the directory: `cd /rms/ova/scripts/post_install`

Step 5 Run the configuration script: `./configureusers.sh`

The script prompts you for the first name, last name username, password to be configured for adding user or changing password of existing user, as shown in this example.

Note Bad Password should be considered as warning. If the password given does not adhere to the Password Policy, an error is displayed after typing the wrong password in the password prompt. The password should be mixed case, alphanumeric, 8 to 127 characters long, should contain one of the special characters(*,@,#), and no spaces. In case of a wrong password, try again with a valid password.

Example:

```
[blrrms-central-22-sree] /rms/ova/scripts/post_install # ./configureusers.sh

MENU
1 - Add linux admin
2 - Modify existing linux admin password

0 - exit program

Enter selection: 1

Enter users FirstName
admin
Enter users LastName
admin1
Enter the username
test
adding user test to users
Enter the password
Changing password for user test.
New password: Retype new password: passwd: all authentication tokens updated successfully.

MENU
1 - Add linux admin
2 - Modify existing linux admin password

0 - exit program

Enter selection: 0

[blrrms-central-22-sree] /rms/ova/scripts/post_install #
```

NTP Servers Configuration

Note

- Follow these steps to configure NTP servers only for RMS.
- NTP addresses can be configured using scripts. For configuring FAP NTP servers, see the *Cisco RAN Management System Administration Guide*.
- If the ESXi host is unable to synchronize with an external NTP Server due to network configuration constraints, use the following steps to configure the NTP Server IP on the RMS nodes.

  The VMware Level checkbox for enabling synchronization with external NTP Server should be unchecked.
- For Server level NTP configuration, ensure that the NTP Server is reachable from every RMS Node (Central/Serving/Upload).

  Routes should be added to establish connectivity.

Following steps explain how to configure the NTP servers:

Central Node Configuration

Use the following steps post installation in the RMS deployment to configure the NTP servers on the Central node or to modify NTP IP address details if they exist in the descriptor file:

Procedure

Step 1 Log in to the **Central node**

Step 2 Switch to root user: **su -**

Step 3 Locate the script `configurentpcentralnode.sh` in the `/rms/ova/scripts/post_install` directory.

Step 4 Change the directory: `cd /rms/ova/scripts/post_install`

Step 5 Run the configuration script: `./configurentpcentralnode.sh`

The script prompts you for the NTP Servers to be configured, as shown in this example.

```
[blrrms-central-14-2I] /rms/ova/scripts/post_install # ./configurentpcentralnode.sh
********************Post-installation script to configure NTP Servers on RMS Central
Node*****************************
To configure NTP Servers Enter yes or no to Exit.
yes
Enter the value of Ntp1_Address
10.105.233.60
Enter the value of Ntp2_Address
4.4.4.4
Configuring NTP servers
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]


iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
```

```
NTP Servers configured Successfully
[blrrms-central-14-2I] /rms/ova/scripts/post_install #
```

Serving Node Configuration

Use the following steps post installation in the RMS deployment to configure the NTP servers in Serving Node:

Procedure

Step 1 Log in to the **Central node**

Step 2 ssh to Serving node

Step 3 Switch to root user: **su -**

Step 4 Locate the script `configurentpservingnode.sh` in the `/rms/ova/scripts/post_install` directory.

Step 5 Change the directory: `cd /rms/ova/scripts/post_install`

Step 6 Run the configuration script: `./configurentpservingnode.sh`

The script prompts you for NTP Servers address as shown in this example.

```
[root@blrrms-serving-14-2I post_install]# ./configurentpservingnode.sh
*******************Post-installation script to configure NTP Server on RMS Serving
Node*******************************
To configure NTP Servers Enter yes or no to Exit.
yes
Enter the value of Ntp1_Address
10.105.233.60
Enter the value of Ntp2_Address
10.105.244.24
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]


Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
NTP Servers configured Successfully
[root@blrrms-serving-14-2I post_install]#
```

Upload Node Configuration

Use the following steps post installation in the RMS deployment to configure the NTP servers in Upload Node:

Procedure

Step 1 Log in to the **Central node**.

Step 2 ssh to Upload node

Step 3 Switch to root user: **su -**

Step 4 Locate the script `configurentploguploadnode.sh` in the `/rms/ova/scripts/post_install` directory.

Step 5 Change the directory: `cd /rms/ova/scripts/post_install`

Step 6 Run the configuration script: `./configurentploguploadnode.sh`

The script prompts you for NTP Servers address as shown in this example.

```
[root@blrrms-upload-14-2I post_install]# ./configurentploguploadnode.sh
******************Post-installation script to configure NTP on RMS Log Upload
Node*****************************
To configure NTP Servers Enter yes or no to Exit.
yes
Enter the value of Ntp1_Address
10.105.233.60
Enter the value of Ntp2_Address
10.105.244.24
Usage: grep [OPTION]... PATTERN [FILE]...
Try `grep --help' for more information.
Usage: grep [OPTION]... PATTERN [FILE]...
Try `grep --help' for more information.
Usage: grep [OPTION]... PATTERN [FILE]...
Try `grep --help' for more information.


iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
Shutting down ntpd: [ OK ]
Starting ntpd: [ OK ]
NTP Servers configured Successfully
[root@blrrms-upload-14-2I post_install]#
```

LDAP Configuration

Procedure

Step 1 Log in to RDU central node using the command **ssh admin1@<RDU_central_node_ipaddress>**

```
The system responds with a command prompt.
```

Step 2 Change in to root user and enter the root password, using the command: **su -l root**

Step 3 Check the required rpm packages available in central node by using the command:

```
pam_ldap-185-11.el6.x86_64
nscd-2.12-1.107.el6.x86_64
nfs-utils-1.2.3-7.el6.x86_64
autofs-5.0.5-73.el6.x86_64
readline-6.0-4.el6.i686
sqlite-3.6.20-1.el6.i686
nss-softokn-3.12.9-11.el6.i686
nss-3.14.0.0-12.el6.x86_64
openldap-2.4.23-31.el6.x86_64
nss-pam-ldapd-0.7.5-18.el6.x86_64
ypbind-1.20.4-29.el6.x86_64
```

Following is the output:

```
pam_ldap-185-11.el6.x86_64
nscd-2.12-1.25.el6.x86_64
nfs-utils-1.2.3-7.el6.x86_64
autofs-5.0.5-31.el6.x86_64
NetworkManager-0.8.1-9.el6.x86_64
readline-6.0-3.el6.i686
sqlite-3.6.20-1.el6.i686
nss-softokn-3.12.9-3.el6.i686
nss-3.12.9-9.el6.i686
openldap-2.4.23-15.el6.i686
```

```
nss-pam-ldapd-0.7.5-7.el6.x86_64
```

Step 4 Do a checksum on the file and verify with the checksum below, by using the command:**md5sum /lib/security/pam_ldap.so**

Note Checksum value should match with the given output.

```
9903cf75a39d1d9153a8d1adc33b0fba  /lib/security/pam_ldap.so
```

Step 5 Edit the nssswitch.conf file, by using the command: **vi /etc/nsswitch.conf** and edit the following: Password: files ldap; Shadow: files ldap; Group: files ldap.

Step 6 Run authconfig-tui, by using the command: **authconfig-tui**
Select:

- Cache Information
- Use LDAP
- Use MD5 Passwords
- Use Shadow Passwords
- Use LDAP Authentication
- Local authorization is sufficient

Step 7 Configure LDAP Settings, by selecting **Next**, and entering the below command:

```
LDAP Configuration
ldap://ldap.cisco.com:389/
OU=active,OU=employees,OU=people,O=cisco.com
```

Note This LDAP configuration varies based on the customer set-up.

Step 8 Restart the services after the configuration changes, by selecting **Ok**.

```
Service nfs start
Service autofs start
Service NetworkManager start
```

Note This LDAP configuration should be modified based on the customer set-up.

Step 9 Enable LDAP configuration at dcc.properties by using the command **vi /rms/app/rms/conf/dcc.properties**. Modify:

```
# PAM configuration
pam.service.enabled=true
pam.service=login
```

Step 10 Restart RDU by using the command **/etc/init.d/bprAgent restart**.

Step 11 Log in to the DCCUI via **dccadmin**.

Step 12 Add user name and enable External authentication.

Note To be LDAP authenticated, the user must be selected as **Externally Authenticated** in DCCUI.

Step 13 Create a UNIX user account on Central VM to match the account on LDAP server before trying to authenticate the user via DCC UI by using the command: **/usr/sbin/useradd <username>**

Step 14 Ensure that the username is correct on LDAP server, DCC UI and Central VM.

Note RMS does not apply the password policy for remote users. This is because LDAP servers manage their login information and passwords.

Step 15 Update IPtables with required LDAP ports.

TACACS Configuration

Use this task to integrate the PAM_TAC library on the Central Node.

Procedure

Step 1 **ssh admin1@***RDU_central_node_ipaddress*.
Logs on to RDU Central Node.

Following is the output:
```
The system responds with a command prompt.
```

Step 2 **su -l root**
Changes to root user.

Step 3 **vi /etc/pam.d/tacacs**
Creates the TAC configuration file for PAM on the Central Node. Add the following to the TACACS file:

```
#%PAM-1.0
auth       sufficient   /lib/security/pam_tacplus.so debug server=<tacacs server ip >
secret=<tacacs server secret> encrypt
account    sufficient   /lib/security/pam_tacplus.so debug server==<tacacs server ip >
secret=<tacacs server secret> encrypt service=shell protocol=ssh
session    sufficient   /lib/security/pam_tacplus.so debug server==<tacacs server ip >
secret=<tacacs server secret> encrypt service=shell protocol=ssh
```

Example:

```
#%PAM-1.0
auth       sufficient   /lib/security/pam_tacplus.so debug server=10.105.242.54
secret=cisco123 encrypt
account    sufficient   /lib/security/pam_tacplus.so debug server=10.105.242.54
secret=cisco123 encrypt service=shell protocol=ssh
session    sufficient   /lib/security/pam_tacplus.so debug server=10.105.242.54
secret=cisco123 encrypt service=shell protocol=ssh
```

Step 4 **vi /etc/pam.d/sshd**
Inserts the TACACS entry in the sshd PAM file. Add the following:

```
auth       include      tacacs
```

Step 5 **vi /rms/app/rms/conf/dcc.properties**
Enables the PAM service at dcc.properties, for the DCC UI configuration. Additionally, modify the following:

```
# PAM configuration
pam.service.enabled=true
pam.service=tacacs
```

Step 6 **/etc/init.d/bprAgent restart**
Restarts the RDU.

Step 7 Log in to DCC UI via the **dccadmin**.

Step 8 Add the user name and enable External authentication by checking the **External authentication** check box.
Note To be TACACS authenticated, the user must be selected as **Externally Authenticated** in DCCUI.

Step 9 **/usr/sbin/useradd** *username*
Creates a UNIX user account on the Central VM to match the account on TACACS+ server. Do this before trying to authenticate the user via the DCC UI.

Following is the output:
```
The system responds with a command prompt.
```

Step 10 Ensure that the username is correct on TACACS+ server, DCC UI and Central VM.
Note The password policy does not apply to non-local users that authentication servers such as TACACS server manage their login information and passwords.

Step 11 Update IPtables with required TACACS ports.

Configuring Geographical Identifier SAC

To configure Geographical Identifier SAC on the deployed system, run the **configure_Insee_RF_AlarmsProfile.sh script**.

For more details on the location and usage of this script, see the "Configuring Geographical Identifier" section of the *Cisco RAN Management System Administration Guide*.

Configuring Third-Party Security Gateways on RMS



Note Perform this procedure only when you want to enable third-party SeGW on the already-installed RMS.

Procedure

Step 1 Deploy RMS (AIO or Distributed).

Step 2 On the Serving node, execute the `/rms/ova/scripts/post_install/SecGW/disable_PNR.sh` script. Repeat this step for all Serving nodes in case of a redundant setup.

Step 3 Follow this step *only* if the .ovftool does not have the PAR details in the descriptor file during deployment. If the .ovftool has the PAR details in the descriptor file, proceed to Step 4:
Execute the `/rms/ova/scripts/post_install/HNBGW/configure_PAR_hnbgw.sh` script.

The **configure_PAR_hnbgw.sh** script creates Radius clients on the Serving node with the details provided in the input configuration file.

```
configure_PAR_hnbgw.sh [ -i config_file ] [-h] [--help]
```

Step 4 Add iptables entry.
```
“iptables -A OUTPUT -s <ServingNode_NB_IP> -d <DHCP_POOL_Network/Subnet> -p tcp --dport 7547
 -j
ACCEPT”
```

Example:

```
iptables -A OUTPUT -s 10.5.1.209 -d 7.0.2.48/28 -p tcp --dport 7547 -j ACCEPT
```

Here 10.5.1.209 is the ServingNode_NB_IP and 7.0.2.48/28 is the DHCP_POOL_Network/Subnet configured in the SecGW or in the third party DHCP server.

Step 5 Add permanent route entry for the IPSec pool as defined in the third-party SeGW.

```
route add -net DHCP_POOL_Network/Subnet gw SN_eth0_NB_Gateway
```

Example:

```
route add -net 7.0.5.224/28 gw 10.5.1.1
```

HNB Gateway Configuration for Third-Party SeGW Support

Note This procedure is applicable only when RMS is installed with Install_Cnr=false.

Procedure

Step 1 Execute the `/rms/ova/scripts/post_install/HNBGW/configure_PAR_hnbgw.sh` script. The **configure_PAR_hnbgw.sh script** creates Radius clients on the Serving node with the details provided in the input configuration file.

```
configure_PAR_hnbgw.sh [ -i config_file ] [-h] [--help]
```

Note
- Perform this step on the Serving node only if the .ovftool does not have the PAR details in the descriptor file during deployment.
- If the .ovftool has the PAR details in the descriptor file, proceed to Step 2.

Step 2 Add IPtables entry.

```
iptables -A OUTPUT -s ServingNode_NB_IP -d DHCP_POOL_Network/Subnet -p tcp --dport
7547
-j
ACCEPT"
```

Example:

```
iptables -A OUTPUT -s 10.5.1.209 -d 7.0.2.48/28 -p tcp --dport 7547 -j ACCEPT
Here 10.5.1.209 is the ServingNode_NB_IP and 7.0.2.48/28 is the DHCP_POOL_Network/Subnet
configured
in the SecGW or in the third party DHCP server.
```

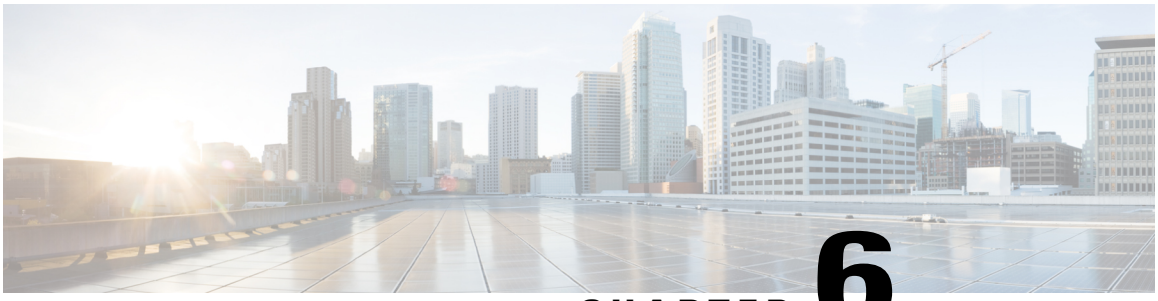
Step 3 Save IPtables and restart IPtables.

```
service iptables save
service iptables restart
```

Step 4 Add permanent route entry for the IPSec pool as defined in the third-party SeGW.

```
route add -net DHCP_POOL_Network/Subnet gw SN_eth0_NB_Gateway
```

Note Repeat this step for all Serving nodes in a redundant setup.



CHAPTER 6

Verifying RMS Deployment

Verify if all the RMS Virtual hosts have the required network connectivity.

- Verifying Network Connectivity, page 171
- Verifying Network Listeners, page 172
- Log Verification, page 173
- End-to-End Testing, page 175

Verifying Network Connectivity

Procedure

Step 1 Verify if the RMS Virtual host has network connectivity from the Central Node, using the following steps:

a) Ping the gateway. (prop:vami.gateway.Central-Node or prop:Central_Node_Gateway).

b) Ping the DNS servers. (prop:vami.DNS.Central-Node or prop:Central_Node_Dns1_Address & prop:Central_Node_Dns2_Address).

c) Ping the NTP servers. (prop:Ntp1_Address, prop:Ntp2_Address, prop:Ntp3_Address & prop:Ntp4_Address).

Step 2 Verify if the RMS Virtual host has network connectivity from the Serving Node, using the following steps:

a) Ping the gateway. (prop:vami.gateway.Serving-Node or prop:Serving_Node_Gateway).

b) Ping the DNS servers. (prop:vami.DNS.Serving-Node or prop:Serving_Node_Dns1_Address & prop:Serving_Node_Dns2_Address).

c) Ping the NTP servers. (prop:Ntp1_Address, prop:Ntp2_Address, prop:Ntp3_Address & prop:Ntp4_Address).

Step 3 Verify if the RMS Virtual host has network connectivity from the Upload Node, using the following steps:

a) Ping the gateway. (prop:vami.gateway.Upload-Node or prop:Upload_Node_Gateway).

b) Ping the DNS servers. (prop:vami.DNS.Upload-Node or prop:Upload_Node_Dns1_Address & prop:Upload_Node_Dns2_Address).

c) Ping the NTP servers. (prop:Ntp1_Address, prop:Ntp2_Address, prop:Ntp3_Address & prop:Ntp4_Address).

Step 4 Perform the additional network connectivity testing on each of the nodes, for the following optional services:

a) Ping the Syslog servers (Optional).

b) Ping the SNMP servers (Optional).
c) Ping the SNMP trap servers (Optional).

Verifying Network Listeners

Verify that the RMS virtual hosts have opened the required network listeners. If the Upload server process is not up, for more details see Upload Server is Not Up, on page 245.

RMS Node	Component	Network Listener
Central Node	BAC RDU	• netstat -an | grep 443 • netstat -an | grep 8005 • netstat -an | grep 8083 • netstat -an | grep 49187 • netstat -an | grep 8090
Serving Node	Cisco Prime Access Registrar (PAR)	• netstat -an | grep 1812 • netstat -an | grep 8443 • netstat -an | grep 8005
	Cisco Prime Network Registrar (PNR)	• netstat -an | grep 61610
	BAC DPE	• netstat -an | grep 2323 • netstat -an | grep 49186
Upload Node	Upload Server	• netstat -an |grep 8082 • netstat -an |grep 443

Log Verification

Server Log Verification

Post installation, the following server logs *should* be checked for verification of clean server start-up.

- **Central Virtual Machine (VM):**
  - /rms/data/CSCObac/agent/logs/snmpAgent_console.log
  - /rms/data/CSCObac/agent/logs/tomcat_console.log
  - /rms/data/dcc_ui/postgres/dbbase/pgstartup.log
  - /rms/log/pmg/PMGServer.console.log
  - /rms/data/nwreg2/regional/logs/install_cnr_log
  - /rms/log/dcc_ui/ui-debug.log
- **Serving VM:** /rms/data/nwreg2/local/logs/install_cnr_log



Note Any errors in the above log files *at the time of application deployment* need to be notified to the operation support team.

Application Log Verification

Application level logs can be referred to in case of facing application-level usage issues:

RMS Node	Component	Log Name
Central VM	DCC_UI	/rms/log/dcc_ui/ui-audit.log /rms/log/dcc_ui/ui-debug.log
	PMG	/rms/log/pmg/pmg-debug.log /rms/log/pmg/pmg-audit.log
	BAC/RDU	/rms/data/CSCObac/rdu/logs/audit.log /rms/data/CSCObac/rdu/logs/rdu.log
Serving VM	PNR	/rms/data/nwreg2/local/logs/ name_dhcp_1_log

	PAR	/rms/app/CSCOar/logs/name_radius_1_log Or /rms/app/CSCOar/logs/name_radius_1_trace
	DPE	/rms/data/CSCObac/dpe/logs/dpe.log
Upload Server VM		/opt/CSCOuls/logs/*.log (uls.log, sb-events.log, nb-events.log)

Viewing Audited Log Files

The Linux auditd service is used in ova install scripts to audit changes to most of the configurations and properties files. You can view any of the audited log files. All files or directories that are eligible for auditing are listed in the audit.rules file located in /etc/audit/. For each audited file or directory, there is a rule in audit.rules of the following syntax: **-w** {*filename_and_path* | *directory_name*} **-p wa -k** *key*

Use one of these commands to search on the logs:

- **ausearch -f** {*filename_and_path* | *directory_name*} **-i**
- **ausearch -k** *key* **-i**

Here is sample output from the search:

```
Output
[rms-aio-central] /home/admin1 # ausearch -k PMGServer.properties -i
Warning - freq is non-zero and incremental flushing not selected.
----
type=CONFIG_CHANGE msg=audit(09/26/14 13:59:23.508:33) : auid=unset ses=unset
subj=system_u:system_r:auditctl_t:s0 op="add rule" key=PMGServer.properties list=exit res=1
----
type=PATH msg=audit(09/26/14 14:02:38.761:155) : item=0
name=/rms/app/pmg/conf/PMGServer.properties
inode=2761390 dev=08:03 mode=file,644 ouid=ciscorms ogid=ciscorms rdev=00:00
obj=system_u:object_r:default_t:s0
type=CWD msg=audit(09/26/14 14:02:38.761:155) :  cwd=/
type=SYSCALL msg=audit(09/26/14 14:02:38.761:155) : arch=x86_64 syscall=open success=yes
exit=3
a0=1b4d8d0 a1=241 a2=1b6 a3=fffffffffffffff0 items=1 ppid=1457 pid=4310 auid=unset uid=root

gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset

comm=central-first-b exe=/bin/bash subj=system_u:system_r:initrc_t:s0 key=PMGServer.properties
```

From the sample output, the note the following:

- audit(09/26/14 14:02:38.761:155) : represents the audit log time.
- uid=root :represents the user id performing the operation
- exe=/bin/bash : exe represents the command modifying the operation (bash script, grep or vi etc)
- comm=central-first-b : represents the script name or linux command (grep,vi etc).

End-to-End Testing

Perform the following processes for end-to-end testing of the Small Cell device:

Procedure

Step 1 Register a Small Cell Device.
Step 2 Power on the Small Cell Device.
Step 3 Verify NTP Signal.
Step 4 Verify TR-069 Inform.
Step 5 Verify Discovered Parameters.
Step 6 Verify Class of Service selection.
Step 7 Perform Firmware Upgrade.
Step 8 Verify Updated Discovered Parameters.
Step 9 Verify Configuration Synchronization.
Step 10 Activate the Small Cell Device.
Step 11 Verify IPSec Connection.
Step 12 Verify Connection Request.
Step 13 Verify Live Data Retrieval.
Step 14 Verify HNB-GW Connection.
Step 15 Verify Radio is Activated.
Step 16 Verify User Equipment can Camp.
Step 17 Place First Call.
Step 18 Verify Remote Reboot.
Step 19 Verify On-Demand Log Upload.

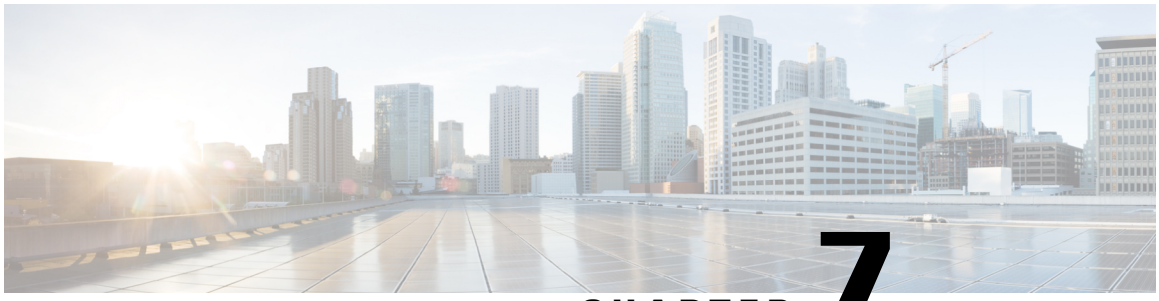
Updating VMware Repository

All the system updates for the VMware Studio and the VMware vCenter are stored on the Update Repository, and can be accessed either online through Cisco DMZ or Offline (delivered to the Customer through Services team or DVD).

Perform the following procedures to apply updates on the RMS nodes:

Procedure

Step 1 Disable the network interfaces for each virtual machine.
Step 2 Create a snapshot of each virtual machine.
Step 3 Mount the Update ISO on the vCenter server.
Step 4 Perform a check for new software availability.
Step 5 Install updates using the vSphere Console.
Step 6 Perform system tests to verify that the updated software features are operating properly.
Step 7 Enable network interfaces for each virtual machine in the appliance.
Step 8 Perform end-to-end testing.



CHAPTER 7

RMS Upgrade

This chapter describes the pre-upgrade, upgrade, and post-upgrade tasks for Cisco RMS.

- Upgrade Flow, page 177
- Pre-Upgrade, page 179
- Upgrade, page 187
- Post-Upgrade, page 223
- Mapping RMS 4.1 XML Files to RMS 5.1 or 5.1 MR XML Files, page 223
- Mapping RMS 5.1 MR XML Files to RMS 5.1 MR Hotfix XML Files, page 225
- Record BAC Configuration Template File Details, page 226
- Associate Manually Edited BAC Configuration Template , page 226
- Rollback to RMS, Release 4.1, page 227
- Rollback to RMS, Release 5.1 or 5.1 MR, page 227
- Remove Obsolete Data , page 228
- Basic Sanity Check Post RMS Upgrade, page 229
- Stopping Cron Jobs, page 230
- Starting Cron Jobs, page 230
- Disabling RMS Northbound and Southbound Traffic, page 231
- Enabling RMS Northbound and Southbound Traffic, page 231

Upgrade Flow

The following table provides the general flow required to complete RMS upgrade. Before upgrade, determine and plan for the following maintenance windows and activities:

Sl. No.	Maintenance Window		Section		Service Impact
1	Pre-Upgrade, on page 179		Pre-Upgrade Tasks for RMS 5.1 MR, on page 179	Pre-Upgrade Tasks for RMS 5.1 MR Hotfix, on page 184	Partial
2	Upgrade, on page 187	**RMS4.1 to RMS5.1 MR Upgrade**	**RMS5.1 to RMS5.1 MR Upgrade**	**RMS5.1 MR to RMS5.1 MR Hotfix Upgrade**	
		Upgrade Prerequisites for RMS 5.1 MR, on page 187		Upgrade Prerequisites for RMS 5.1 MR Hotfix, on page 189	Complete
		Upgrading Central Node from RMS 4.1 to RMS 5.1 MR, on page 189	Upgrading Central Node from RMS 5.1 to RMS 5.1 MR, on page 200	Upgrading Central Node from RMS 5.1 MR to RMS 5.1 MR Hotfix, on page 205	
		Upgrading Serving Node from RMS 4.1 to RMS 5.1 MR, on page 191	Upgrading Serving Node from RMS 5.1 to RMS 5.1 MR, on page 201	Upgrading Serving Node from RMS 5.1 MR to RMS 5.1 MR Hotfix, on page 208	
		Upgrading Upload Node from RMS 4.1 to RMS 5.1 MR, on page 195	Upgrading Upload Node from RMS 5.1 to RMS 5.1 MR, on page 203	Upgrading Upload Node from RMS 5.1 MR to RMS 5.1 MR Hotfix, on page 210	
		Post RMS 4.1 to RMS 5.1 MR Upgrade Configurations, on page 196	Post RMS 5.1 to RMS 5.1 MR Upgrade Configurations, on page 203	Post RMS 5.1 MR to RMS 5.1 MR Hotfix Upgrade Configurations, on page 211	
3	Post-Upgrade, on page 223	Post RMS 5.1 MR Upgrade Tasks, on page 223		Post RMS 5.1 MR Hotfix Upgrade Task, on page 223	—

Pre-Upgrade

Pre-Upgrade Tasks for RMS 5.1 MR

1. Stop the RMS Northbound and Southbound traffic. For more information, see Disabling RMS Northbound and Southbound Traffic, on page 231.
2. Ensure cron jobs are not running while upgrading the system. For more information, see Stopping Cron Jobs, on page 230.

   The following service-impacting tasks should be carried out during the pre-upgrade maintenance window.
3. Ensure that the CAR license on all the Serving nodes is valid. Verify if both the `/rms/app/CSCOar/license/CSCOar.lic` and `/home/CSCOar.lic` files of the Serving node have the same valid license. Else, update a valid 6.0 license before proceeding with the upgrade, see CAR/PAR Server Not Functioning , on page 238.
4. Ensure that there are no UMT jobs running. Log in to the DCC UI and navigate to the Upgrade Monitor tab. Click on the jobs in the "In Progress" tab and select **Stop Monitoring**. In case of any issues, see Unable to Stop UMT Jobs, on page 252.
5. Ensure that the total disk space utilization is not exceeding 50 GB. Else, follow Remove Obsolete Data , on page 228.
6. Clone the system, see Back Up System Using vApp Cloning, on page 287.
7. Ensure that the existing hardware supports RMS 5.1 MR. Before proceeding with the upgrade, see Cisco RMS Hardware and Software Requirements, on page 12.
8. Ensure that the Central node VM CPU and memory is as suggested in the Optimum CPU and Memory Configurations, on page 15. For more information, see Upgrading the VM CPU and Memory Settings, on page 94.

Note From the vSphere Web Client, navigate to the Host > Summary > STORAGE > FREE/USED/CAPACITY to ensure that the data store has 200 GB free space to extend the root partition from 50 GB to 200 GB.

If root partition (*/dev/sda3*) is not the final partition of the system, then follow the *Method of Procedure for Increasing Root Partition* document and proceed to Step 10; else proceed to the next step (Step 9).

To confirm the root partition, look for existing partitions that have higher than 3 sda partitions (like `/dev/sda4` or `/dev/sda5`) in the **df -h** command output on each RMS node. These additional partitions on `/dev/sda` must be moved to new disks to establish `/dev/sda3` as the final partition.

Enter:

```
df –h
```

Output:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              49G   38G  8.9G  81% /
tmpfs                 7.8G     0  7.8G   0% /dev/shm
/dev/sda1             124M   28M   91M  24% /boot
/dev/sda5             9.9G  155M  9.2G   2% /rms/txn
/dev/sdb1              19G  5.3G   13G  30% /rms/data
/dev/sdc1              19G  3.1G   15G  18% /rms/backups
```

9 Follow the Upgrading the Data Storage on Root Partition for Cisco RMS VMs, on page 94 to increase the data storage or disk size.

10 Delete the clone taken as part of Step 6 and take a fresh clone of the system with increased data storage, see Back Up System Using vApp Cloning, on page 287.

Note This clone is used for rollback; ensure that there are no modifications after the system is cloned.

11 If the upgrade path is RMS5.1 to RMS5.1MR, then ensure that there are no LTE APs present. If present, manually delete the APs before the upgrade.

12 Detach the CD/DVD drive from the RMS nodes as follows:

- **a** Log in to the vSphere Web Client and locate the Central node vAPP.
- **b** In the Getting Started tab, click **Power Off vApp**.
- **c** After power off, right-click on the Central node VM and click **Edit Settings**.
- **d** Remove the CD/DVD drive 1 from the Virtual Hardware tab by clicking on the "X" symbol present in the same row.
- **e** Click **Ok** to finish.
- **f** Click **Edit Settings** and ensure that the CD/DVD drive 1 is removed.
- **g** In the Getting Started tab, select the vApp of the VM and click **Power On vApp**.
- **h** Repeat steps a to g on all the RMS nodes.

13 Start the RMS Northbound and Southbound traffic. For more information, see Enabling RMS Northbound and Southbound Traffic, on page 231.

Note The Southbound interface is enabled automatically as part of step12.

14 Start the cron jobs. For more information, see Starting Cron Jobs, on page 230.

The following tasks are not service impacting and can be performed outside the maintenance window.

15 Ensure that the manually added routes are made permanent on all the nodes. Else, follow Enabling Communication for VMs on Different Subnets, on page 121.

16 Ensure that a backup of ovfEnv.xml is taken from `/opt/vmware/etc/vami/` directory on all the nodes.

17 Manually append the Central server "hostname" and "eth0 IP" to the existing `/etc/hosts` file of the Serving and Upload nodes.

Input:
```
<Central node eth0 IP> <Central node host name>
```

Sample Output:
```
10.5.1.208  blr-rms19-central
```

18 Download and untar the "RHEL6.7-tar.gz" package.

```
tar -zxvf RHEL6.7-tar.gz
```

19 Move the "rhel-server-6.7-x86_64-dvd.iso" file on all the RMS nodes "/" directory.

20 Download the RMS upgrade package and copy it to the `admin` directory of all the RMS nodes.

21 (For Hotfix only) Apply the Red Hat Enterprise Linux 6.7 security vulnerability patch on RMS. To do this, see the *Method of Procedure to Apply Red Hat Enterprise Linux 6.7 Security Patch on Cisco RMS*.

22 Ensure that the RMS_App_Password is known before starting the upgrade.

23 Ensure that the "password" property value in the `/rms/app/BACCTools/conf/APIScripter.arguments` file of the Central node contains the same property password as the "bacadmin" user password of RMS 4.1 or RMS 5.1. If these are not in sync, then change the password in the file to match the "bacadmin" user password.

24 Record (make a note in a file on the local machine) the local verification (LV) related properties present in the class of service level on the BAC UI.

Identify the LV related properties from the activated-BV3.4.4.0, activated-BV3.5.11.0, baseline-BV3.4.4.0, and baseline-BV3.5.11.0.

25 If applicable, take a backup (that is, save to the local machine) of the configuration template mapping that has been manually changed or associated with a CoS of the device

26 Record the manually customized default configuration template as described in Record BAC Configuration Template File Details, on page 226.

27 Manually back up the RF profile group instances using the Export option in the DCC UI, see "Exporting Information about a Group or ID Pool Instance" section in the *Cisco RAN Management System Administration Guide* for steps to export and revert RF profiles post upgrade to RMS 5.1 MR. This would be required because the property values may be reset as per the latest RFprofile version.

28 If applicable (when the default DN prefix is changed) take a backup of the DN Prefix format configured in DCC UI > Configurations > DN Prefix tab to apply the same configurations post-upgrade.

29 Take a screen-shot of the DCC > Groups and IDs > Group Types/ID Pool Types tab and identify the manual associations of the Group Types/ID Pool Types. For information on default associations, see the following tables:

Note The 'AlarmsProfile' GroupType mentioned in the following table will be seen only on systems where the INSEE-SAC feature is enabled.

a If the upgrade path is from RMS, Release 4.1 to RMS, Release 5.1 MR, refer to the following default GroupType/IDPoolType associations to identify the manual changes.

Group Type Name	Associated ID Pool Types	Associated Group Types
Area	SAI-POOL	FemtoGateway
Enterprise	—	Site
FemtoGateway	CELL-POOL	—
RFProfile	—	—
Site	—	Area Enterprise FemtoGateway
AlarmsProfile	—	—

ID Pool Type Name	Associated Group Type
CELL-POOL	FemtoGateway
SAI-POOL	Area

b If the upgrade path is from RMS, Release 5.1 to RMS, Release 5.1 MR, refer to the following default GroupType/IDPoolType associations to identify the manual changes.

Group Type Name	Associated ID Pool Types	Associated Group Types
Area	SAI-POOL	HeNB-GW FemtoGateway Region
Enterprise	—	Site
FemtoGateway	CELL-POOL	UMTSSecGateway
HeNBGW	—	LTESecGateway
LTESecteway	—	—

Group Type Name	Associated ID Pool Types	Associated Group Types
RFProfile	—	—
RFProfile-LTE	—	—
Region	LTE-CELL-POOL	—
Site	—	Area Enterprise FemtoGateway SubSite
Subsite	—	Site
UMTSSecGateway	—	—
AlarmsProfile	—	—

ID Pool Type Name	Associated Group Type
CELL-POOL	FemtoGateway
LTE-CELL-POOL	Region
SAI-POOL	Area

30 Ensure that groups with the same name do not exist, before the upgrade. For example, consider two group types - Area and FemtoGateway. These group types should not have the same group name across both the group types, like "New" under Area Group Type and under Femtogateway group type.

31 If the upgrade path is from RMS 4.1 to RMS 5.1 MR, ensure that the PAR on the Serving node is upgraded to version 6.1.2.3.

Input:
```
rpm -qa |grep CPAR
```

Sample Output:
```
CPAR-6.1.2.3-1.noarch
```

32 Identify and note the changes made in the xml files (pmg-profile/DCC UI xml files) by comparing the xml files present in `/rms/app/rms/conf` and the corresponding default files to merge the changes, post-upgrade. The list of RMS 4.1 xml files are as follows:

- sdm-register-residential-screen-setup.xml
- sdm-register-enterprise-screen-setup.xml
- sdm-update-residential-screen-setup.xml

- sdm-update-enterprise-screen-setup.xml
- sdm-static-neighbors-filter-screen-setup.xml
- sdm-inter-rat-static-neighbors.xml
- sdm-inter-freq-static-neighbors.xml
- deviceParamsDisplayConfig.xml
- bgmt-add-group-screen-setup-Area.xml
- bgmt-add-group-screen-setup-FemtoGateway.xml
- bgmt-add-group-screen-setup-RFProfile.xml
- bgmt-add-group-screen-setup-AlarmsProfile.xml
- bgmt-add-group-screen-setup-Site.xml
- bgmt-add-group-screen-setup-Enterprise.xml
- bgmt-add-pool-screen-setup-CELL-POOL.xml
- bgmt-add-pool-screen-setup-SAI-POOL.xml
- pmg-profile.xml

33 Ensure that all the processes are up and running on the Central, Serving, and Upload nodes, see RMS Installation Sanity Check, on page 101.

Pre-Upgrade Tasks for RMS 5.1 MR Hotfix

1 Ensure that the CAR license on all the Serving nodes is valid. Verify if both the `/rms/app/CSCOar/license/CSCOar.lic` and `/home/CSCOar.lic` files of the Serving node have the same valid license. Else, update a valid 6.0 license before proceeding with the upgrade, see CAR/PAR Server Not Functioning , on page 238.

2 Verify that the ovfEnv.xml present in the `/opt/vmware/etc/vami/` directory on all the RMS nodes and is not empty as shown in the following example.

Example:

```
central] ~ # ls -l /opt/vmware/etc/vami/
total 12
drwxr-xr-x. 2 root root 4096 Jun 12 2015 flags
lrwxrwxrwx. 1 root root 16 Feb 4 06:10 ovfEnv.xml -> /rms/ovf-env.xml
-r--r--r--. 1 root root 166 Feb 23 2012 vami.xml
-rw-r--r--. 1 root root 128 Jun 12 2015 vami_ovf_info.xml
[central] ~ #
```

If the file is empty, add the following line to the file:

```
<Environment
>
</Environment>
```

Example:

```
[central] ~ # cat /opt/vmware/etc/vami/ovfEnv.xml
<Environment
>
```

```
</Environment>
[central] ~ #
```

Ensure that a backup of the ovfEnv.xml file is taken from `/opt/vmware/etc/vami/` directory on all the nodes.

3 Before applying the hotfix, export GlobalRegion and GlobalUMTSSecGateway groups through DCC UI.

4 Ensure that there is no live data set for these parameters on LTE APs:

- Device.Services.FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IntraFreq.X_CISCO_COM_OpenPciListStart
- Device.Services.FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IntraFreq.X_CISCO_COM_OpenPciListRange
- Device.Services.FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.InterFreq.Carrier.{i}.X_CISCO_COM_OpenPciListStart
- Device.Services.FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.InterFreq.Carrier.{i}.X_CISCO_COM_OpenPciListRange

If the live data is set for these parameters, log in to the DCC UI and in the Perform tab, go to Set Modified Live Data > X_CISCO_COM_OpenPciListStart and click Restore to Default to remove it.

5 Ensure that the FIRMWARE-UPGRADE-LTE-ENABLE, FIRMWARE-UPGRADE-LTE-VERSION, and FIRMWARE-UPGRADE-LTE-IMAGE properties are not present at the device or hierarchical group levels following the below procedure:

a Log in to the Central Node console as an admin or ciscorms user.

b Prepare a configuration file with the node property and property hierarchy content.

```
DeviceParameter, DeviceDetailsKeys.DEVICE_ID, EID
NodeProperty{Area}, Name, Area
NodeProperty{Enterprise}, Name, Enterprise
NodeProperty{Site}, Name, Site
NodeProperty{HeNBGW}, Name, HeNBGW
NodeProperty{LTESecGateway}, Name, LTESecGateway
NodeProperty{RFProfile}, Name, RFProfile
PropertyHierarchy, FIRMWARE-UPGRADE-LTE-ENABLE, Enabled
PropertyHierarchy, FIRMWARE-UPGRADE-LTE-VERSION, Version
PropertyHierarchy, FIRMWARE-UPGRADE-LTE-IMAGE, Image
```

In the following example, 'gddt.conf' is the configuration file created to run the getDeviceData.sh tool.

Example:

```
[central] ~ $ cat gddt.conf
DeviceParameter, DeviceDetailsKeys.DEVICE_ID, EID
NodeProperty{Area}, Name, Area
NodeProperty{Enterprise}, Name, Enterprise
NodeProperty{Site}, Name, Site
NodeProperty{HeNBGW}, Name, HeNBGW
NodeProperty{LTESecGateway}, Name, LTESecGateway
NodeProperty{RFProfile}, Name, RFProfile
PropertyHierarchy, FIRMWARE-UPGRADE-LTE-ENABLE, Enabled
PropertyHierarchy, FIRMWARE-UPGRADE-LTE-VERSION, Version
PropertyHierarchy, FIRMWARE-UPGRADE-LTE-IMAGE, Image
[central] ~ $
```

c Create a text file with the following content:

```
activated-DSV4.0.0T.0
baseline-DSV4.0.0T.0
```

Note This file must contain only the above two CoS values. For more details on get device data, refer to the "getDeviceData.sh" section of the "Operational Tools" chapter in the *Cisco RAN Management System Administration Guide*.

Example:

```
[central] ~ $ cat text
activated-DSV4.0.0T.0
baseline-DSV4.0.0T.0
[central] ~ $
```

d Execute the getDeviceData.sh tool using the below command:

getDeviceData.sh -config <Path and name of the config file created> -idfile <Path and name of the idfile created>

Example:

```
[central] ~ $ getDeviceData.sh -config gddt.conf -idfile text.txt -type cos
Initializing RDU client...
ok
 number of devices: 2

Execution parameters:
 -outdir /rms/ops/GetDeviceData-20160119-101718
 -config /rms/ops/GetDeviceData-20160119-101718/gddt.conf
 -idfile /home/admin1/text.txt
 -rate 1000/min
 -timeout 60000
 -liveThreads 100

Retrieving all global data
Retrieving all Node properties...
Processing node type [AdditionalConfig]...
1 node objects of type [AdditionalConfig] retrieved
Processing node type [Area]...
3 node objects of type [Area] retrieved
Processing node type [CELL-POOL]...
1 node objects of type [CELL-POOL] retrieved
.
.
.
Processing node type [UMTSSecGateway]...
3 node objects of type [UMTSSecGateway] retrieved
Processing node type [system]...
1 node objects of type [system] retrieved
Retrieved all 55 node objects

Retrieving all Class of Service properties...
28 Class Of Service objects retrieved

Retrieving all ProvGroup properties...
1 ProvGroup objects retrieved

Retrieving all property defaults...ok

Done retrieving all global data in 0.307 sec

Retrieving device data
 * max rate of get live data requests - 1000/min
 * number of liveThreads - 100
 * timeout for get live data operations - 60000 msec
 * output to [/rms/ops/GetDeviceData-20160119-101718/device-data.csv]
 * errors to [/rms/ops/GetDeviceData-20160119-101718/logs/error.log]
 * audits to [/rms/ops/GetDeviceData-20160119-101718/logs/audit.log]
 * debug messages to [/rms/ops/GetDeviceData-20160119-101718/logs/debug.log]

Done exporting data to id file 0.021 sec

Processed 2 devices. Rate: 1061/min. Errors: 0.  Warnings: 0.
```

```
Completed processing 2 devices.
Data retrieval completed in 0 sec
Done.
[central] ~ $
```

Note Ensure that there are no errors as shown (see highlighted text) in the example.

e Open the **device-data.csv'** file from the output directory (as shown in the example in the earlier step) and verify that the FIRMWARE-UPGRADE-LTE-ENABLE, FIRMWARE-UPGRADE-LTE-VERSION, and FIRMWARE-UPGRADE-LTE-IMAGE properties are not populated.

Example:

```
[central] ~ $ cat /rms/ops/GetDeviceData-20160119-101718/device-data.csv
EID,Area,Enterprise,Site,HeNBGW,LTESecGateway,RFProfile,Enabled,Version,Image
001B67-352639054083976,Area,Enterprise,Site,HeNBGW-1,LTESECGW-1,,true,,
001B67-352639054084560,Area,Enterprise,Site,HeNBGW-1,LTESECGW-1,,false,
DSV4.0.6T.130116,DSV4.0.6T.130116_SCF.xml
[central] ~ $
```

Note

- Ensure that there are no values populated for Enabled, Version, and Image columns.
- If there are values populated for Enabled, Version, and Image columns as shown in the example, note-down the APs for which the values are populated and the groups that are associated with the those APs.
- Verify the level at which the properties are present and make a note of it.

6 Identify and note the changes made in the XML files (pmg-profile/DCC UI xml files) by comparing the xml files present in /rms/app/rms/conf and the corresponding default files to merge the changes, post-upgrade. The list of RMS 5.1 MR XML files are as follows:

- pmg-profile.xml
- bgmt-add-group-screen-setup-Area-MIXED.xml
- bgmt-add-group-screen-setup-Region.xml
- bgmt-add-group-screen-setup-Area.xml
- bgmt-add-group-screen-setup-Area-LTE.xml

7 Ensure that all the LTE APs on the system are up with live data to perform firmware upgrade.

8 Ensure that the RMS_App_Password is noted before the upgrade.

Upgrade

Upgrade Prerequisites for RMS 5.1 MR

Follow the below procedures during the upgrade maintenance window.

1. Stop the RMS Northbound and Southbound traffic. For more information, see Disabling RMS Northbound and Southbound Traffic, on page 231.
2. Ensure that cron jobs are not running while upgrading the system. For more information, see Stopping Cron Jobs, on page 230.
3. Ensure that the total disk space utilization is not exceeding 50 GB by using the **df -h** command on all the RMS Nodes.

   Example:

```
[rms-distr-central] ~ $ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              49G   38G  8.9G  81% /
tmpfs                 7.8G     0  7.8G   0% /dev/shm
/dev/sda1             124M   28M   91M  24% /boot
/dev/sda5             9.9G  155M  9.2G   2% /rms/txn
/dev/sdb1              19G  5.3G   13G  30% /rms/data
/dev/sdc1              19G  3.1G   15G  18% /rms/backups
[rms-distr-central] ~ $
```

   Else, follow Remove Obsolete Data , on page 228.

Red Hat Enterprise Linux Upgrade

1. Follow the RHEL 6.7 upgrade MOP to upgrade RHEL on all the RMS nodes. Cloning the RMS VMs (mentioned in "5.1.2 Clone the System" section of the MOP) before the RHEL upgrade is optional (it increases the maintenance window duration) because the clone is already taken in the pre-upgrade maintenance window, which is used for rollback.
2. Ensure that the RHEL is upgraded to v6.7. As a root user verify the output of the below command on the nodes:

   Input:

```
cat /etc/redhat-release
```

   Sample Output:

```
Red Hat Enterprise Linux Server release 6.7(Santiago)
```

3. For an upgrade from RMS4.1 to RMS5.1MR, verify that the postgresql is listening on 5435 port of the Central node.

   Input:

```
netstat -na |grep 5435 |grep LISTEN
```

   Sample Output:

```
tcp        0      0 127.0.0.1:5435          0.0.0.0:*
LISTEN
unix  2      [ ACC ]     STREAM     LISTENING     12891
/tmp/.s.PGSQL.5435
```

   The postgresql port should be listening to port 5435 before upgrade. If it is not listening, change the postgres port setting as follows:

   - i. Log in to the Central node as root user.
   - ii. Change the port to 5435:

     Input:

```
sed -i 's/PGPORT=5432/PGPORT=5435/' /etc/rc.d/init.d/postgresql
```

     Sample output:

```
The system responds with the command prompt
```

- iii. Reboot the Central VM and repeat this step on the cold standby Central node in case of high availability setup.

4 Ensure that all the processes are up and running on the Central, Serving, and Upload nodes before performing the upgrade, see Verifying Application Processes, on page 102.

Note After RHEL upgrade on all the RMS nodes, proceed with the RMS upgrade on each of the nodes.

Upgrade Prerequisites for RMS 5.1 MR Hotfix

Follow the below procedures during the upgrade maintenance window.

1 Ensure that the total disk space utilization is not exceeding 50 GB. Else, follow Remove Obsolete Data , on page 228.

2 Clone the system, see Back Up System Using vApp Cloning, on page 287.

3 Ensure that all the RMS nodes are reachable via **ssh**. Else, follow Network Unreachable on Cloning RMS VM , on page 251.

4 Apply the Red Hat Enterprise Linux 6.7 security vulnerability patch on RMS. To do this, see the *Method of Procedure to Apply Red Hat Enterprise Linux 6.7 Security Patch on Cisco RMS*.

5 Stop the RMS Northbound and Southbound traffic. For more information, see Disabling RMS Northbound and Southbound Traffic, on page 231.

6 Ensure cron jobs are not running while upgrading the system. For more information, see Stopping Cron Jobs, on page 230.

After completing the prerequisites, proceed Upgrading from RMS 5.1 MR to RMS 5.1 MR Hotfix, on page 205 on each of the nodes.

Upgrade from RMS 4.1 to RMS 5.1 MR

Upgrading Central Node from RMS 4.1 to RMS 5.1 MR

Procedure

Step 1 Log in to the Central node as root user.

Step 2 Move the **RMS-UPGRADE-5.1.1-x.tar.gz** file from the `admin` directory to the `/rms` directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.1-x.tar.gz -C /rms**

- i. As a root user stop the IGS from the Central node:
  `/rms/app/baseconfig/bin/runkiwi.sh /rms/upgrade/confFiles/kiwis/stopigs.kiwi`
- ii. Stop the DPE process on all the Serving nodes:
  `/etc/init.d/bprAgent stop dpe`
- iii. Using BAC UI manually, set the recorded LV related properties from the Class of Service level (in Pre-Upgrade Tasks) at the provisioning group level (Servers > Provisioning Groups).
- iv. As a root user, start the IGS on the Central node:
  `/rms/app/baseconfig/bin/runkiwi.sh /rms/upgrade/confFiles/kiwis/startigs.kiwi`

d) **/rms/upgrade/upgrade_rms.sh**

In the output, when you are prompted to proceed with the upgrade, enter a response and wait for the upgrade to complete with a completed message on the console.

Sample Output:

```
[BLR17-Central-41N] / # /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Central-Node
INFO - Detected RMS4.1 setup
INFO - Upgrading the current RMS installation to 5.1.1.0 MR. Do you want to proceed? (y/n)
:
y
INFO - Stopping applications on Central Node
INFO - Stopping bprAgent ..
INFO - BAC stopped successfully
INFO - Stopping PMG and AlarmHandler ..
INFO - Taking RMS Central Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/centralBackUpFileList
INFO - Filebackup tar is present at path : /rmsbackupfiles/rdubackup/rms-central.tar
INFO -
INFO - Starting RPM Upgrade ..
...
...
INFO - Disabling ETH0 gateway in central node ifcfg-eth0
INFO - Changing Postgres port from 5435 to 5439 and AlarmHandler port from 4678 to 4698
INFO - Restoring the DCC-UI DB ..
INFO - Executing /rmsbackupfiles/dccuiDbBackup/dbbackup.sql in dcc
INFO - Restarting applications on Central Node
INFO - Restarting bprAgent ...
INFO - BAC is running
INFO - Restarting PMG and Alarmhandler..
INFO - Disabling the unnecessary TCP/IP Services
INFO - Finished upgrading RMS Central Node .
[BLR17-Central-41N] / #
```

Step 4 Repeat Steps 3a to 3d on the cold standby Central node in case of a high availability setup.

Step 5 Restore the value of the property "sdm.logupload.ondemand.nbpassword" in the `/rms/app/CSCObac/rdu/tomcat/webapps/dcc_ui/sdm/plugin-config.properties` file as in the `/rmsbackupfiles/plugin-config.properties` file of the Central node.

Upgrading Serving Node from RMS 4.1 to RMS 5.1 MR

Procedure

Step 1 Log in to the Serving node as root user.

Step 2 Move the **RMS-UPGRADE-5.1.1-x.tar.gz** file from the `admin` directory to the `/rms` directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.1-x.tar.gz -C /rms**

Note After untarring the RMS upgrade package, verify that the license present in `/rms/upgrade/confFiles/license/CSCOar.lic.70` is a valid 7.0 PAR license. Else, edit the file by providing a valid value using 'vi' editor to update the valid license, see CAR/PAR Server Not Functioning , on page 238.

d) **/rms/upgrade/upgrade_rms.sh**

Note
- In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.
- Provide the PNR/PAR password (RMS_App_Password of RMS, Release 4.1) when prompted and wait for the upgrade to complete with a completed message on the console.

Sample Output:

```
[root@BLR17-Serving-41N /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Serving-Node
INFO - Detected RMS4.1 setup
INFO - Upgrading the current RMS installation to 5.1.1.0 MR. Do you want to proceed? (y/n)
:
y
INFO - Stopping applications on Serving Node
INFO - Stopping bprAgent ..
INFO - BAC stopped successfully
INFO - Disabling the PNR extension points
Enter cnradmin Password:
INFO - Stopping PNR ..
INFO -
INFO - Stopping CAR ..
INFO - Taking RMS Serving Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/servingBackUpFileList
INFO - Copying the DHCP files ..
INFO - Files are being moved to backup directory
INFO - Copying the DHCP files done
INFO - Filebackup tar is present at path : /rms-serving.tar
INFO -
INFO - Starting RPM Upgrade ..
INFO -
INFO - Upgrading the BAC on RMS Serving Node ....
INFO -
INFO - Enabling the PNR extensions
```

```
INFO -
INFO - Starting bprAgent ..
INFO -
INFO - Starting PNR ..
INFO -
INFO - Starting CAR ..
INFO -
Enter caradmin Password:
INFO - Executing configARExtension.sh ..
INFO - Executing runCopyCarFile.sh ..
INFO - Restarting bprAgent ..
/usr/java /rms
/rms
INFO - Upgrading PNR-local ...
INFO -
...
INFO -
INFO - Restoring the Serving certs :
INFO - Disabling the unnecessary TCP/IP Services
INFO - Finished upgrading RMS Serving Node .
[root@BLR17-Serving-41N /]#
```

Step 4 Repeat steps 3a to 3d on the redundant Serving node in case of a redundant setup.

Step 5 If the Serving nodes have redundancy configured on the system, then in the "iptables", change the protocol of the "647" port from "udp" to "tcp":

a) On the primary Serving node, run the following commands:

- i. Verify the protocol of the port '647'.

```
.iptables -S |grep 647
```

Example:

```
• -A INPUT -s serving-node-2-eth0-address/netmask -d
serving-node-1-eth0-address/netmask -i eth0 -p udp -m udp --dport 647
-m state --state NEW -j ACCEPT
• -A OUTPUT -s serving-node-1-eth0-address/netmask -d
serving-node-2-eth0-address/netmask -o eth0 -p udp -m udp --dport 647
-m state --state NEW -j ACCEPT
```

- ii. Remove the existing firewall for the port “647” on udp protocol.

  - `iptables -D INPUT -s serving-node-2-eth0-address/netmask -d serving-node-1-eth0-address/netmask -i eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT`
  - `iptables -D OUTPUT -s serving-node-1-eth0-address/netmask -d serving-node-2-eth0-address/netmask -o eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT`

- iii. Add the IPtable for the port “647” on tcp protocol.

- iptables -A INPUT -s **serving-node-2-eth0-address/netmask** -d **serving-node-1-eth0-address/netmask** -i eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- iptables -A OUTPUT -s **serving-node-1-eth0-address/netmask** -d **serving-node-2-eth0-address/netmask** -o eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- service iptables save

Example:

- iptables -D INPUT -s 10.5.4.48/32 -d 10.5.4.45/32 -i eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT
- iptables -D OUTPUT -s 10.5.4.45/32 -d 10.5.4.48/32 -o eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT
- iptables -A INPUT -s 10.5.4.48/32 -d 10.5.4.45/32 -i eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- iptables -A OUTPUT -s 10.5.4.45/32 -d 10.5.4.48/32 -o eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- service iptables save

b) On the secondary Serving node, run the following commands:

- i. Remove the existing firewall for the port "647" on udp protocol.
  - iptables -D INPUT -s **serving-node-1-eth0-address/netmask** -d **serving-node-2-eth0-address/netmask** -i eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT
  - iptables -D OUTPUT -s **serving-node-2-eth0-address/netmask** -d **serving-node-1-eth0-address/netmask** -o eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT
- ii. Add the IPtable for the port “647” on tcp protocol.

- iptables -A INPUT -s **serving-node-1-eth0-address/netmask** -d **serving-node-2-eth0-address/netmask** -i eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- iptables -A OUTPUT -s **serving-node-2-eth0-address/netmask** -d **serving-node-1-eth0-address/netmask** -o eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- service iptables save

Example:

- iptables -D INPUT -s 10.5.4.45/32 -d 10.5.4.48/32 -i eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT
- iptables -D OUTPUT -s 10.5.4.48/32 -d 10.5.4.45/32 -o eth0 -p udp -m udp --dport 647 -m state --state NEW -j ACCEPT
- iptables -A INPUT -s 10.5.4.45/32 -d 10.5.4.48/32 -i eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- iptables -A OUTPUT -s 10.5.4.48/32 -d 10.5.4.45/32 -o eth0 -p tcp -m tcp --dport 647 -m state --state NEW -j ACCEPT
- service iptables save

c) Change the PNR product version on the cluster configuration on the primary Serving node by following these steps as a root user:

- **/rms/app/nwreg2/local/usrbin/nrcmd -N cnradmin**

  Note When prompted, enter the RMS_App_Password password as set in RMS, Release 4.1.
- **cluster Backup-cluster set product-version=8.3**
- **save**
- **dhcp reload**
- **exit**

Example:

```
[root@serving-1-41 admin1]# /rms/app/nwreg2/local/usrbin/nrcmd -N cnradmin
password:
100 Ok
session:
cluster = localhost
current-view = Default
current-vpn = global
default-format = user
dhcp-edit-mode = synchronous
dns-edit-mode = synchronous
groups = superuser
roles = superuser
user-name = cnradmin
visibility = 5
nrcmd> cluster Backup-cluster set product-version=8.3
100 Ok
```

```
nrcmd> save
100 Ok
nrcmd> dhcp reload
100 Ok
nrcmd> exit
[root@serving-1-41 admin1]#
```

Upgrading Upload Node from RMS 4.1 to RMS 5.1 MR

Procedure

Step 1 Log in to the Upload node as root user.

Step 2 Move the **RMS-UPGRADE-5.1.1-x.tar.gz** file from the `admin` directory to the **`/rms`** directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar –zxvf /rms/RMS-UPGRADE-5.1.1-x.tar.gz –C /rms**

d) **/rms/upgrade/upgrade_rms.sh**

Note

- In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.
- Provide the valid keystore password (RMS_App_Password for RMS, Release 4.1) when prompted and wait for the upgrade to complete with a completed message on the console.

Sample Output:

```
[root@BLR17-Upload-41N /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Upload-Node
INFO - Detected RMS4.1 setup
INFO - Upgrading the current RMS installation to 5.1.1.0 MR. Do you want to proceed? (y/n)
:
y
INFO - Stopping applications on Upload Node
INFO - Stopping Upload Server ..
INFO - Taking RMS Upload Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/uploadBackUpFileList
tar: Removing leading `/' from member names
INFO - Filebackup tar is present at path : /rms-upload.tar
INFO -
INFO - Starting RPM Upgrade ..
...
INFO - Restoring the Upload certs :
INFO - Restarting the audit service
Enter Keystore Password: INFO - Restarting Upload Server
INFO - Disabling the unnecessary TCP/IP Services
INFO - Finished upgrading RMS Upload Node .
```

```
[root@BLR17-Upload-41N /]#
```

Step 4 Repeat Steps 3a to 3d on the redundant Upload node in case of a redundant setup.

Post RMS 4.1 to RMS 5.1 MR Upgrade Configurations

1. If the **pmg-profile.xml** file was changed manually before the upgrade, these changes or customizations have to be manually merged post-upgrade. Follow the below procedure to merge the **pmg-profile.xml**:

   a. Copy the **pmg-profile.xml** file from `/rms/app/rms/doc/pmg` to `/rms/app/rms/conf`; change the owner or permission of the file to "ciscorms" and merge the changes as identified in Step 31 of the Pre-Upgrade Tasks for RMS 5.1 MR, on page 179.

   b. Validate the modified **pmg-profile.xml** file against the latest pmg-profile schema file (XSD file) using the below command:
   `xmllint --noout --schema <xsdpath> <xmlpath>`

   <xsdpath> is the complete path to the latest pmg-profile schema file (XSD file). In RMS 5.1 MR the XSD is present in `/rms/app/rms/doc/pmg/pmg-profile-v2_0_0.xsd` on the Central node.

   <xmlpath> is the complete path to the modified pmg-profile.xml (`/rms/app/rms/conf/pmg-profile.xml`).

   Example:
   ```
   [blr-central-41] ~ # xmllint --noout --schema
   /rms/app/rms/doc/pmg/pmg-profile-v2_0_0.xsd /rms/app/rms/conf/pmg-profile.xml
   /rms/app/rms/conf/pmg-profile.xml validates
   [blr-central-41] ~ #
   ```

   c. After the **pmg-profile.xml** file is modified and validated, then restart the pmg process as a 'root' user using the below command:
   ```
   # god restart PMGServer
   ```

   Example:
   ```
   [blr-central-41] ~ # god restart PMGServer
   Sending 'restart' command
   The following watches were affected:
   PMGServer
   [blr-central-41] ~ #
   ```

   d. After restarting the PMGServer, ensure that the process is up before proceeding further. Use the following command to verify that the PMG server is listening on the port 8083.

   Example:
   ```
   [blr-central-41] ~ # netstat -an|grep 8083
   tcp 0 0 0.0.0.0:8083 0.0.0.0:* LISTEN
   [blr-central-41] ~ #
   ```

2. Follow these steps to configure the RMS 5.1 MR version features:

   a. Log in to the Central node as a root user and follow this procedure to disable the "Instruction Generation Service".

   Run the following command as 'root' user to stop "Instruction Generation Service" and proceed to the next step to configure groups and pools.

   ```
   /rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/stopigs.kiwi
   ```

Note Clear browser cache and cookies before accessing the DCC UI.

b If any changes related to group and pool associations were made to the default existing Group Types and ID Pool Types before upgrade (that is, DCC > Groups and IDs > Group Types/ID Pool Types), then update the same group or pool associations after the upgrade (for example, if Area group type was modified and associated with the Alarms Profile group type or any new group type). Refer to the following default RMS 5.1 MR GroupType/IDPoolType associations:

Group Type Name	Associated ID Pool Types	Associated Group Types
Area	SAI-POOL	HeNB-GW FemtoGateway Region
Enterprise	—	Site
FemtoGateway	CELL-POOL	UMTSSecGateway
HeNBGW	—	LTESecGateway
LTESecteway	—	—
RFProfile	—	—
RFProfile-LTE	—	—
Region	LTE-CELL-POOL	—
Site	—	Area Enterprise FemtoGateway SubSite
Subsite	—	Site
UMTSSecGateway	—	—
AlarmsProfile	—	—

ID Pool Type Name	Associated Group Type
CELL-POOL	FemtoGateway
LTE-CELL-POOL	Region

ID Pool Type Name	Associated Group Type
SAI-POOL	Area

c Migrate the existing groups to the new group architecture.

To migrate the groups, follow this procedure:

- i. Log in to DCC UI and go to Groups and IDs screen. Update the mandatory properties in the GlobalRegion and GlobalUMTSSecGateway groups of Region and UMTSSecGateway GroupType.
  - On GlobalRegion group instance of the Region GroupType, update the ID Pools, PLMNID, FC-LTE-PLMN-LIST, IU-PLMNID property values appropriately.
  - On GlobalUMTSSecGateway group instance of the UMTSSecGateway GroupType update the IPSEC Server Host 1 property value appropriately.

- ii. Log in to the Central Node as 'admin' user and export all existing Areas by using the following opstool command:
  `bulkimportexport.sh -ops export -type Area -outdir /home/admin1`
  This command exports all Areas to a file, for example,
  `BulkImportExport-20141107-095929/GroupsAndIds_export_Area_AllGroups__2014-1107_09_59_30.csv`
  .

  Note Edit the csv file using the 'vi' editor and remove the "DefaultArea" entry before proceeding to the next step.

- iii. Import all the areas exported in sub-step ii, associating the GlobalRegion and DefaultHeNBGW to each area by using the following command:

  ```
  bulkimportexport.sh -ops import -type Area –csvfile
  /home/admin1/BulkImportExport-20141107-095929/GroupsAndIds_export_Area_AllGroups__2014-11-07_09_59_30.csv

  -defaultLinkedGroups
  "{name:GlobalRegion,type:Region},{name:DefaultHeNBGW,type:HeNBGW}"
  ```
  This command associates all the existing areas to GlobalRegion and DefaultHeNBGW.

- iv. Export all existing FemtoGateways by using the following command:
  `bulkimportexport.sh -ops export -type FemtoGateway -outdir /home/admin1`
  This command exports all FemtoGateways to a file, for example,
  `BulkImportExport-20141107-095929/GroupsAndIds_export_FemtoGateway_AllGroups__2014-11-07_09_59_30.csv.`

  Note Edit the csv file using the 'vi' and remove the "DefaultFGW" entry before proceeding to the next step.

- v. Import all the FemtoGateways exported in sub-step iv, associating the GlobalUMTSSecGateway to each FemtoGateway using the following command:

  ```
  bulkimportexport.sh -ops import -type FemtoGateway –csvfile
  /home/admin1/BulkImportExport-20141107-095929/GroupsAndIds_export_FemtoGateway_AllGroups__2014-11-07_09_59_30.csv

  -defaultLinkedGroups "{name:GlobalUMTSSecGateway,type:UMTSSecGateway}"
  ```
  This command associates all the existing FemtoGateways to GlobalUMTSSecGateway.

- vi. The Configuration templates in BAC are automatically replaced with respective RMS 5.1 MR versions during upgrade. Manually customize the replaced configuration template as described in Associate Manually Edited BAC Configuration Template , on page 226.
- vii. Manually update the RF profile property value (if required) as per the previously exported csv file (in RMS 4.1) and provide appropriate values for the empty fields. For more information, see the "Updating a Group Type, Group Instance, ID Pool Type, or ID Pool Instance" section of the *Cisco RAN Management System Administration Guide*.
- viii. The DN prefix format configured in DCC UI > Configurations > DN Prefix are automatically replaced with the respective RMS 5.1 MR versions. If required, manually reconfigure the format as in RMS, Release 4.1.
- ix. The LTE-related mandatory properties are without values on the existing Area that are created in RMS 4.1. Enter default values for mandatory properties via DCC UI; default values can be referenced from tooltip present for each property.
- x. Enable the “Instruction Generation Service” by following the below procedure:

  Log in as 'root' user and run the following command to start “Instruction Generation Service”.
  `/rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/startigs.kiwi`

d On the Central node, if sslProtocol="TLS" in the `/rms/app/CSCObac/rdu/tomcat/conf/server.xml` file, then log in as 'root' user and change it to sslProtocols="TLSv1.2,TLSv1.1,TLSv1" and restart the tomcat process using the below command.
`/etc/init.d/bprAgent restart tomcat`

Example:

```
[Central] ~ # /etc/init.d/bprAgent restart tomcat
Process [tomcat] has been restarted. Encountered an error while stopping.

[Central] ~ # /etc/init.d/bprAgent status tomcat
BAC Process Watchdog is running.
Process [tomcat] is running.

[Central] ~ #
```

e Start the RMS Northbound traffic and Southbound traffic. For more information, see Enabling RMS Northbound and Southbound Traffic, on page 231.

f Start the cron jobs. For more information, see Starting Cron Jobs, on page 230.

3 Ensure that all the processes are up after the upgrade, see RMS Installation Sanity Check, on page 101.

What to Do Next

To know more about customizing the RMS system and post-upgrade activities, see Post RMS 5.1 MR Upgrade Tasks, on page 223 and Additional Information, on page 222.

Upgrading from RMS 5.1 to RMS 5.1 MR

Ensure that all the RMS nodes are reachable via **ssh**. Else, follow Network Unreachable on Cloning RMS VM , on page 251.

Upgrading Central Node from RMS 5.1 to RMS 5.1 MR

Procedure

Step 1 Log in to the Central node as 'root' user.

Step 2 Move the **RMS-UPGRADE-5.1.1-x.tar.gz** file from the `admin` directory to the `/rms` directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as 'root' user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.1-x.tar.gz -C /rms**

- i. As a root user stop the IGS from the Central node:
  `/rms/app/baseconfig/bin/runkiwi.sh /rms/upgrade/confFiles/kiwis/stopigs.kiwi`
- ii. Stop the DPE process on all the Serving nodes:
  `/etc/init.d/bprAgent stop dpe`
- iii. Using BAC UI manually, set the recorded LV related properties from the Class of Service level (in Pre-Upgrade Tasks) at the provisioning group level (Servers > Provisioning Groups).
- iv. Provide the appropriate value of IPSEC Server Host 1 and IPSEC Server Host 2 at the FemtoGateway Group Instances.
- v. As a root user, start the IGS on the Central node:
  `/rms/app/baseconfig/bin/runkiwi.sh /rms/upgrade/confFiles/kiwis/startigs.kiwi`

d) **/rms/upgrade/upgrade_rms.sh**

In the output, when you are prompted to proceed with the upgrade, enter a response and wait for the upgrade to complete with a completed message on the console.

Sample Output:

```
[BLR17-Central-41N] / # /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Central-Node
INFO - Detected RMS5.1.0-2I setup
INFO - Upgrading the current RMS installation to 5.1.1.0 MR. Do you want to proceed? (y/n)
:
y
INFO - Stopping applications on Central Node
INFO - Stopping bprAgent ..
INFO - BAC stopped successfully
INFO - Stopping PMG and AlarmHandler ..
INFO - Taking RMS Central Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/centralBackUpFileList
INFO - Filebackup tar is present at path : /rmsbackupfiles/rdubackup/rms-central.tar
INFO -
INFO - Starting RPM Upgrade ..
...
...
INFO - Disabling ETH0 gateway in central node ifcfg-eth0
```

```
INFO - Changing Postgres port from 5435 to 5439 and AlarmHandler port from 4678 to 4698
INFO - Restoring the DCC-UI DB ..
INFO - Executing /rmsbackupfiles/dccuiDbBackup/dbbackup.sql in dcc
INFO - Restarting applications on Central Node
INFO - Restarting bprAgent ...
INFO - BAC is running
INFO - Restarting PMG and Alarmhandler..
INFO - Disabling the unnecessary TCP/IP Services
INFO - Finished upgrading RMS Central Node .
[BLR17-Central-41N] / #
```

Note The following error, which has no impact to the system in the upgrade-debug.log, can be ignored:
`ERROR: column "password_lifetime" of relation "role_names" already exists`

Step 4 Repeat Steps 3a to 3d on the cold standby Central node in case of a high availability setup.

Step 5 Restore the value of the property "sdm.logupload.ondemand.nbpassword" in the `/rms/app/CSCObac/rdu/tomcat/webapps/dcc_ui/sdm/plugin-config.properties` file as in the `/rmsbackupfiles/plugin-config.properties` file.

Upgrading Serving Node from RMS 5.1 to RMS 5.1 MR

Procedure

Step 1 Log in to the Serving node as root user.

Step 2 Move the **RMS-UPGRADE-5.1.1-x.tar.gz** file from the `admin` directory to the `/rms` directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.1-x.tar.gz -C /rms**

Note After untarring the RMS upgrade package, verify that the license present in `/rms/upgrade/confFiles/license/CSCOar.lic.70` is a valid 7.0 PAR license. Else, edit the file by providing a valid value using 'vi' editor to update the valid license, see CAR/PAR Server Not Functioning , on page 238.

d) **/rms/upgrade/upgrade_rms.sh**

Note
- In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.
- Provide the PNR/PAR password (RMS_App_Password of RMS, Release 4.1) when prompted and wait for the upgrade to complete with a completed message on the console.

Sample Output:

```
[root@BLR17-Serving-41N /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Serving-Node
INFO - Detected RMS5.1.0-2I setup
INFO - Upgrading the current RMS installation to 5.1.1.0 MR. Do you want to proceed? (y/n)
:
```

```
y
INFO - Stopping applications on Serving Node
INFO - Stopping bprAgent ..
INFO - BAC stopped successfully
INFO - Disabling the PNR extension points
Enter cnradmin Password:
INFO - Stopping PNR ..
INFO -
INFO - Stopping CAR ..
INFO - Taking RMS Serving Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/servingBackUpFileList
INFO - Copying the DHCP files ..
INFO - Files are being moved to backup directory
INFO - Copying the DHCP files done
INFO - Filebackup tar is present at path : /rms-serving.tar
INFO -
INFO - Starting RPM Upgrade ..
INFO -
INFO - Upgrading the BAC on RMS Serving Node ....
INFO -
INFO - Enabling the PNR extensions
INFO -
INFO - Starting bprAgent ..
INFO -
INFO - Starting PNR ..
INFO -
INFO - Starting CAR ..
INFO -
Enter caradmin Password:
INFO - Executing configARExtension.sh ..
INFO - Executing runCopyCarFile.sh ..
INFO - Restarting bprAgent ..
/usr/java /rms
/rms
INFO - Upgrading PNR-local ...
INFO -
...
INFO -
INFO - Restoring the Serving certs :
INFO - Disabling the unnecessary TCP/IP Services
INFO - Finished upgrading RMS Serving Node .
[root@BLR17-Serving-41N /]#
```

Step 4 Repeat steps 3a to 3d on the redundant Serving node in case of a redundant setup.

Upgrading Upload Node from RMS 5.1 to RMS 5.1 MR

Procedure

Step 1 Log in to the Upload node as 'root' user.

Step 2 Move the **RMS-UPGRADE-5.1.1-x.tar.gz** file from the `admin` directory to the **`/rms`** directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as 'root' user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar –zxvf /rms/RMS-UPGRADE-5.1.1-x.tar.gz –C /rms**

d) **/rms/upgrade/upgrade_rms.sh**

Note In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.

Sample Output:

```
[root@BLR17-Upload-41N /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Upload-Node
INFO - Detected RMS5.1.0-2I setup
INFO - Upgrading the current RMS installation to 5.1.1.0 MR. Do you want to proceed? (y/n)
:
y
INFO - Stopping applications on Upload Node
INFO - Stopping Upload Server ..
INFO - Taking RMS Upload Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/uploadBackUpFileList
tar: Removing leading `/' from member names
INFO - Filebackup tar is present at path : /rms-upload.tar
INFO -
INFO - Starting RPM Upgrade ..
...
INFO - Restoring the Upload certs :
INFO - Restarting the audit service
INFO - Disabling the unnecessary TCP/IP Services
INFO - Finished upgrading RMS Upload Node .
[root@BLR17-Upload-41N /]#
```

Step 4 Repeat Steps 3a to 3d on the redundant Upload node in case of a redundant setup.

Post RMS 5.1 to RMS 5.1 MR Upgrade Configurations

1 If the **pmg-profile.xml** file was changed manually before the upgrade, these changes or customizations have to be manually merged post-upgrade. Follow the below procedure to merge the **pmg-profile.xml**:

a. Copy the **pmg-profile.xml** file from `/rms/app/rms/doc/pmg` to `/rms/app/rms/conf`; change the permission of the file to “ciscorms” and merge the changes as identified in Step 31 of the Pre-Upgrade Tasks for RMS 5.1 MR, on page 179.

b. Validate the modified **pmg-profile.xml** file against the latest pmg-profile schema file (XSD file) using the below command:

```
xmllint --noout --schema <xsdpath> <xmlpath>
```

<xsdpath> is the complete path to the latest pmg-profile schema file (XSD file). In RMS 5.1 MR the XSD is present in `/rms/app/rms/doc/pmg/pmg-profile-v2_0_0.xsd` on the Central node.

<xmlpath> is the complete path to the modified pmg-profile.xml (`/rms/app/rms/conf/pmg-profile.xml`).

Example:

```
[blr-central-41] ~ # xmllint --noout --schema
/rms/app/rms/doc/pmg/pmg-profile-v2_0_0.xsd /rms/app/rms/conf/pmg-profile.xml
/rms/app/rms/conf/pmg-profile.xml validates
[blr-central-41] ~ #
```

c. After the **pmg-profile.xml** file is modified and validated, then restart the pmg process as a 'root' user using the below command:

```
# god restart PMGServer
```

Example:

```
[blr-central-41] ~ # god restart PMGServer
Sending 'restart' command
The following watches were affected:
PMGServer
[blr-central-41] ~ #
```

d. After restarting the PMGServer, ensure that the process is up before proceeding further. Use the following command to verify that the PMG server is listening on the port 8083.

Example:

```
[blr-central-41] ~ # netstat -an|grep 8083
tcp 0 0 0.0.0.0:8083 0.0.0.0:* LISTEN
[blr-central-41] ~ #
```

2. Disable the “Instruction Generation Service” using the following procedure.

   Run the following command as 'root' user to stop “Instruction Generation Service”.

   ```
   /rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/stopigs.kiwi
   ```

3. The Configuration templates in BAC are automatically replaced with respective RMS 5.1 MR versions during upgrade. Manually customize the replaced configuration template as described in Associate Manually Edited BAC Configuration Template , on page 226.

4. Manually update the RF profile property value (if required) as per the previously exported csv file (in RMS 5.1) and provide appropriate values for the empty fields. For more information, see the "Updating a Group Type, Group Instance, ID Pool Type, or ID Pool Instance" section of the *Cisco RAN Management System Administration Guide*.

5. The DN prefix format configured in DCC UI > Configurations > DN Prefix are automatically replaced with the respective RMS 5.1 MR versions. If required, manually reconfigure the format as in RMS, Release 5.1.

6. On the GlobalUMTSSecGateway group instance of the UMTSSecGateway GroupType, update the IPSec Server Host 1 and IPSec Server Host 2 property value appropriately.

7 On the Central node, if sslProtocol="TLS" in the `/rms/app/CSCObac/rdu/tomcat/conf/server.xml` file, then log in as 'root' user and change it to sslProtocols="TLSv1.2,TLSv1.1,TLSv1" and restart the tomcat process using the below command.
`/etc/init.d/bprAgent restart tomcat`

Example:

```
[Central] ~ # /etc/init.d/bprAgent restart tomcat
Process [tomcat] has been restarted. Encountered an error while stopping.

[Central] ~ # /etc/init.d/bprAgent status tomcat
BAC Process Watchdog is running.
Process [tomcat] is running.

[Central] ~ #
```

8 Enable the “Instruction Generation Service” by following the below procedure:

Run the following command as 'root' user to start the “Instruction Generation Service”.

```
/rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/startigs.kiwi
```

9 Start the RMS Northbound traffic and Southbound traffic. For more information, see Enabling RMS Northbound and Southbound Traffic, on page 231.

10 Start the cron jobs. For more information, see Starting Cron Jobs, on page 230.

11 Ensure that all the processes are up after the upgrade, see RMS Installation Sanity Check, on page 101.

What to Do Next

To know more about customizing the RMS system and post-upgrade activities, see Post RMS 5.1 MR Upgrade Tasks, on page 223 and Additional Information, on page 222.

Upgrading from RMS 5.1 MR to RMS 5.1 MR Hotfix

Upgrading Central Node from RMS 5.1 MR to RMS 5.1 MR Hotfix

Procedure

Step 1 Log in to the Central node as 'root' user.

Step 2 Move the **RMS-UPGRADE-5.1.2-x-HOTFIX01.tar.gz** file from the `admin` directory to the `/rms` directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.2-x-HOTFIX01.tar.gz -C /rms**

d) **/rms/upgrade/upgrade_rms.sh**

Note In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.

Sample Output:

```
[root@blr-rms15-serving rms]# cd /
[root@blr-rms15-serving /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
```

```
INFO - Central-Node
INFO - Detected RMS5.1.1-253 setup .
INFO - Applying the 5.1.2.0 HOTFIX . Do you want to proceed? (y/n) :
y
INFO - Stopping applications on Central Node
INFO - Stopping bprAgent ..
INFO - BAC stopped successfully
INFO - Stopping PMG and AlarmHandler ..
INFO - Taking RMS Central Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/centralBackUpFileList
INFO - Filebackup tar is present at path : /rmsbackupfiles/rdubackup/rms-central.tar
INFO -
INFO - Starting RPM Upgrade ..
INFO -  /usr/java/jre1.6.0_45 already installed.So skipping JRE upgrade
INFO - Upgrading jre to 1.7...
INFO - Restarting the bprAgent ..
INFO - Upgrading BASELINE CONFIG ...
INFO - BAC-CONFIG upgraded to /rms/upgrade/rpms/CSCOrms-baseline-config-ga-5.1.2-45.noarch.rpm
INFO - Upgrading OPS-TOOLS ...
INFO - OPS-TOOLS upgraded to /rms/upgrade/rpms/CSCOrms-ops-tools-ga-5.1.2-45.noarch.rpm
INFO - Upgrading PMG ...
INFO - PMG upgraded to /rms/upgrade/rpms/CSCOrms-pmg-ga-5.1.2-45.noarch.rpm
INFO -
INFO - Upgrading DCC-UI ...
INFO - DCC-UI upgraded to /rms/upgrade/rpms/CSCOrms-dcc-ui-ga-5.1.2-45.noarch.rpm
INFO - Changing Postgres port from 5435 to 5439 and AlarmHandler port from 4678 to 4698
INFO - /rms/.upgrade-sqls is not present.Its a first time upgrade. intra-upgrade.sql present
 in upgrade tar will be executed
INFO - Restarting applications on Central Node
INFO - Restarting bprAgent ...
INFO - BAC is running
INFO - Restarting PMG and Alarmhandler..
INFO - Disabling the unnecessary TCP/IP Services
INFO - Going for sleep for 60s..to make NTP server up
INFO - Going for sleep for 3 min to make pmg up and working
2016-02-05 11:10:23 [INFO] (upgrade_rms.sh) - Finished upgrading RMS Central Node
```

Note If this error message is seen in the output—"Hence operator has to manually import the Area and Region group file located at `/tmp/GroupsAndIds_export_Region_DefaultRegion_properties_AfterMigration.csv` "—follow these steps. Else proceed to the Upgrading Serving Node from RMS 5.1 MR to RMS 5.1 MR Hotfix, on page 208 procedure.

1 If the **pmg-profile.xml** file was changed manually before the upgrade, these changes or customizations have to be manually merged post-upgrade. Follow the below procedure to merge the **pmg-profile.xml**:

a Copy the **pmg-profile.xml** file from `/rms/app/rms/doc/pmg` to `/rms/app/rms/conf`; change the owner or permission of the file to "ciscorms" and merge the changes as identified in Step 31 of the Pre-Upgrade Tasks for RMS 5.1 MR, on page 179.

Note
- Ensure that the following property expressions in the pmg-profile.xml file are aligned with the property expressions of the XML file in the hotfix:
  - FC-LTE-INTRA-FREQ-PMAX
  - FC-LTE-NEIGHBOR-LTECELL-\d{1,2}-X2-CONNECTION-STATUS
  - FC-LTE-NEIGHBOR-LTECELL-\d{1,2}-X2-HO-STATUS
- Ensure that the FC-LTE-CARRIER-i-OPENPCILISTSTARTFC-LTE-CARRIER-i-OPENPCILISTRANGE property is not copied or merged with the pmg-profile.xml file in the `/rms/app/rms/conf` directory.

b Validate the modified **pmg-profile.xml** file against the latest pmg-profile schema file (XSD file) using the below command:

`xmllint --noout --schema <xsdpath> <xmlpath>`

<xsdpath> is the complete path to the latest pmg-profile schema file (XSD file). In RMS 5.1 MR the XSD is present in `/rms/app/rms/doc/pmg/pmg-profile-v2_0_0.xsd` on the Central node.

<xmlpath> is the complete path to the modified pmg-profile.xml (`/rms/app/rms/conf/pmg-profile.xml`).

Example:

```
[blr-central-41] ~ # xmllint --noout --schema
/rms/app/rms/doc/pmg/pmg-profile-v2_0_0.xsd /rms/app/rms/conf/pmg-profile.xml
/rms/app/rms/conf/pmg-profile.xml validates
[blr-central-41] ~ #
```

c After the **pmg-profile.xml** file is modified and validated, then restart the pmg process as a 'root' user using the below command:

```
# god restart PMGServer
```

Example:

```
[blr-central-41] ~ # god restart PMGServer
Sending 'restart' command
The following watches were affected:
PMGServer
[blr-central-41] ~ #
```

d After restarting the PMGServer, ensure that the process is up before proceeding further. Use the following command to verify that the PMG server is listening on the port 8083.

Example:

```
[blr-central-41] ~ # netstat -an|grep 8083
```

```
tcp 0 0 0.0.0.0:8083 0.0.0.0:* LISTEN
[blr-central-41] ~ #
```

2 Log in to the Central node as a root user and follow this procedure to disable the “Instruction Generation Service”.

Run the following command as 'root' user to stop “Instruction Generation Service” and proceed to the next step to configure groups and pools.

```
/rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/stopigs.kiwi
```

Note Clear browser cache and cookies before accessing the DCC UI.

3 Execute the following command to update the Area.

```
su -c " bulkimportexport.sh -ops import -type Area -csv file
/tmp/GroupsAndIds_export_Area_DefaultArea_properties_AfterMigration.csv" ciscorms
```

4 Execute the following command to update Region groups.

```
su -c " bulkimportexport.sh -ops import -type Region -csv file
/tmp/GroupsAndIds_export_Region_DefaultRegion_properties_AfterMigration.csv" ciscorms
```

5 Enable the “Instruction Generation Service” by following the below procedure:

Log in as 'root' user and run the following command to start “Instruction Generation Service”.

```
/rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/startigs.kiwi
```

Upgrading Serving Node from RMS 5.1 MR to RMS 5.1 MR Hotfix

Procedure

Step 1 Log in to the Serving node as root user.

Step 2 Move the **RMS-UPGRADE-5.1.2-x-HOTFIX01.tar.gz** file from the `admin` directory to the `/rms` directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.2-x-HOTFIX01.tar.gz -C /rms**

d) **/rms/upgrade/upgrade_rms.sh**

Note
- In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.
- Provide the PNR/PAR password (RMS_App_Password) when prompted and wait for the upgrade to complete with a completed message on the console.

Sample Output:

```
[root@blr-rms15-serving rms]# cd /
[root@blr-rms15-serving /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Serving-Node
INFO - Detected RMS5.1.1-253 setup .
```

```
INFO - Applying the 5.1.2.0 HOTFIX . Do you want to proceed? (y/n) :
y
INFO - Stopping applications on Serving Node
INFO - Stopping bprAgent ..
INFO - BAC stopped successfully
INFO - Disabling the PNR extension points
Enter cnradmin Password: 401 Login Failure - cluster localhost: no nrcmd permissions
Enter cnradmin Password:
INFO - Stopping PNR ..
INFO -
INFO - Stopping CAR ..
INFO - Taking RMS Serving Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/servingBackUpFileList
/bin/cp: cannot stat `/rms/app/nwreg2/local/extensions/dhcp/dex//*': No such file or directory
INFO - Copying the DHCP files ..
INFO - DHCP files are already moved to the backup directory
INFO - dpeext.jar already moved to the backup directory
INFO - Copying the DHCP files done
INFO - Filebackup tar is present at path : /rms-serving.tar
INFO -
INFO - Starting RPM Upgrade ..
cp: cannot stat `/rmsbackupfiles/dpebackup/*': No such file or directory
INFO -
INFO - Enabling the PNR extensions
INFO -
INFO - Starting bprAgent ..
INFO -
INFO - Starting PNR ..
INFO -
INFO - Starting  CAR ..
INFO -
Enter car admin Password:
INFO - Executing configARExtension.sh ..
INFO - Executing runCopyCarFile.sh ..

INFO - Restarting  bprAgent ..

cp: cannot stat `/rmsbackupfiles/dpebackup/*.so': No such file or directory
INFO -
INFO - Restarting PNR ..
cp: cannot stat `/rmsbackupfiles/dpebackup/dpeext.jar': No such file or directory
INFO -
INFO - Restarting  CAR ..
INFO - Restoring the Serving certs :
INFO - Disabling the unnecessary TCP/IP Services
INFO - Going for sleep for 60s..to make NTP server up
INFO - Finished upgrading RMS Serving Node .
```

Upgrading Upload Node from RMS 5.1 MR to RMS 5.1 MR Hotfix

Procedure

Step 1 Log in to the Upload node as 'root' user.

Step 2 Move the **RMS-UPGRADE-5.1.2-x-HOTFIX01.tar.gz** file from the `admin` directory to the **`/rms`** directory.

Note The "x" in the upgrade image represents the target upgrade load number.

Step 3 Execute the following commands as root user to perform the upgrade:

a) **cd /**

b) **rm -rf /rms/upgrade**

c) **tar -zxvf /rms/RMS-UPGRADE-5.1.2-x-HOTFIX01.tar.gz -C /rms**

d) **/rms/upgrade/upgrade_rms.sh**

Note In the output, when you are prompted to proceed with the upgrade, enter the response as 'y'.

Sample Output:

```
[root@blr-rms15-upload /]# /rms/upgrade/upgrade_rms.sh
INFO - Detecting the RMS Node ..
INFO - Upload-Node
INFO - Detected RMS5.1.1-253 setup .
INFO - Applying the 5.1.2.0 HOTFIX . Do you want to proceed? (y/n) :
y
INFO - Stopping applications on Upload Node
INFO - Stopping Upload Server ..
INFO - Taking RMS Upload Node file backup as per the configuration in the
file:/rms/upgrade/backupfilelist/uploadBackUpFileList
/rms/upgrade/upgrade_rms.sh: line 1416: /bin/cp: Argument list too long
tar: Removing leading `/' from member names
INFO - Filebackup tar is present at path : /rms-upload.tar
INFO -
INFO - Starting RPM Upgrade ..
INFO - Upgrading jre to 1.7...
INFO - Restoring the Upload certs
Enter Keystore Password: INFO - Restarting Upload Server
INFO - Disabling the unnecessary TCP/IP Services
INFO - Going for sleep for 60s..to make NTP server up
INFO - Finished upgrading RMS Upload Node .
```

What to Do Next

1. Start the cron jobs. For more information, see Starting Cron Jobs, on page 230.
2. Start the RMS Northbound traffic and Southbound traffic. For more information, see Enabling RMS Northbound and Southbound Traffic, on page 231.

Post RMS 5.1 MR to RMS 5.1 MR Hotfix Upgrade Configurations

1 Log in to the Central node as a root user and follow this procedure to disable the “Instruction Generation Service”.

Run the following command as 'root' user to stop “Instruction Generation Service” and proceed to the next step to configure groups and pools.

```
/rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/stopigs.kiwi
```

Note Clear browser cache and cookies before accessing the DCC UI.

2 Import the GlobalUMTSSecGateway group file that was exported before upgrade. For more information, see Pre-Upgrade Tasks for RMS 5.1 MR Hotfix, on page 184.

3 Edit the exported GlobalRegion group file and remove FC-QOS-LIST, FC-INTRA-PCILIST-START and FC-INTRA-PCILIST-RANGE properties and corresponding values from the file and then import.

4 Enable the “Instruction Generation Service” by following the below procedure:

Log in as 'root' user and run the following command to start “Instruction Generation Service”.

```
/rms/app/baseconfig/bin/runkiwi.sh /rms/ova/scripts/post_install/startigs.kiwi
```

What to Do Next

Proceed to the Upgrading AP Firmware Post RMS 5.1 MR Hotfix Installation, on page 217 procedure.

Upgrading AP Firmware From Cloud Base

The following procedure enables bulk APs (that have established IPsec tunnel) to contact the CloudBase. This is achieved by issuing the Factory Recovery from Cisco RMS to the bulk devices and thus upgrading the bulk APs to the latest Firmware.

Before You Begin

Ensure that the AP profiles in the CloudBase have the latest AP firmware version. To set the latest version of Firmware in CloudBase, see http://www.cisco.com/c/en/us/support/wireless/3g-small-cell/products-maintenance-guides-list.html.

Procedure

Step 1 Log in to the RMS Central node as admin user.

Example:

```
ssh <admin_User_name>@Central_Server_eth1_IP
```

Note The *admin_User_name* must be part of the ciscorms group; run **id admin_User_name** to verify the user name.

Step 2 Create a folder `CloudBaseUpgrade` in the home directory.

Example:
```
mkdir –p  $HOME/CloudBaseUpgrade
```

Step 3 Go to the newly created folder `CloudBaseUpgrade`.

Example:
```
cd $HOME/CloudBaseUpgrade
```

Step 4 Create a new text file using the text editor and enter the list of AP EIDs that need to be upgraded via the CloudBase. Save the file as CloudBaseUpgradeEID.txt.

Example:
```
vi CloudBaseUpgradeEID.txt
001B67-111213131313131
001B67-213321431414141
001B67-424672467452567
```

Step 5 Run **massFactoryRestore.sh** to trigger factory recovery for the list of EIDs mentioned in the previous step. For information on how to execute **massFactoryRestore.sh**, see massFactoryRestore.sh.

Example:
```
massFactoryRestore.sh –idfile CloudBaseUpgradeEID.txt –type devices –rate 1
```

Note The rate value should not be more than 1.

Step 6 Run **GetDeviceData.sh** (see, getDeviceData.sh) to find list of APs mentioned in the CloudBaseUpgradeEID.txt that have been upgraded with the latest firmware.

Note If APs have not contacted RMS then the firmware of these APs may not show the latest version.

Single APs can also be upgraded to the latest firmware from the CloudBase. To perform an upgrade, initiate factory recovery from DCC UI for individual APs. For more information, see Resetting a Device.

Upgrading AP Firmware From RMS

The following procedure enables single or bulk APs (that have established IPsec tunnel) to download firmware files from RMS, thereby, upgrading the single or bulk APs to the latest firmware.

Uploading Firmware Files to RMS

Procedure

Step 1 Download the AP software files by following the instructions provided at this link: http://www.cisco.com/c/dam/en/us/td/docs/wireless/asr_5000/smallcell/USC_Software_Docs/R35_MR/References/USC-44-45-001_Downloading_Software_from_CloudBase.pdf.

Step 2 Save the available firmware files to your desktop or machine that is used to access the BAC UI. Save the files in the format <AP Software Version>_<filename>. For example, if AP needs to upgrade to software version BV3.5.11.5, then save the five files in the format given below.

- BV3.5.11.5_SCF.sig

- BV3.5.11.5_SCF.xml
- BV3.5.11.5_rootfs.bin
- BV3.5.11.5_standard-kernel.bin
- BV3.5.11.5_ubiqfs.bin

Step 3 Log in to the BAC UI using 'bacadmin' credentials.

Example:
`https://<CentralNode _eth1_IPAddress>/adminui/`

a) Select the **Configuration** option on the BAC UI landing page.
b) Click the **Files** tab.
c) In the Files tab, click **Add** to open the Add Files page.
d) From the File Type drop-down list, select the **Firmware File**.
e) Click **Browse** to browse and select the firmware file saved locally as described in Step 2. For example, BV3.5.11.5_SCF.sig.
f) Enter the File Name of the file selected in the previous step. The filename should reflect the selected firmware file name. For example, BV3.5.11.5_SCF.sig.

Step 4 Repeat Step 3 for the remaining four files: BV3.5.11.5_SCF.xml, BV3.5.11.5_rootfs.bin, BV3.5.11.5_standard-kernel.bin, and BV3.5.11.5_ubiqfs.bin.

Initiating Firmware Upgrade on Individual or Bulk FAPs

The following procedures describe how to Initiate firmware upgrade on individual or bulk of FAPs in a controlled manner to ensure that the system is not overloaded.

Note Ensure that the firmware upgrade related custom properties are not enabled at any Group, Class of Service, Provisioning Group, and CWMP Defaults level.

Initiating Firmware Upgrade on Individual FAPs

Post the update API xml from the OSS to initiate firmware upgrade on a single FAP. This sets the firmware upgrade related custom properties at the device level on the BAC and initiates the connection request on the device. On receiving the connection request from the device, BAC initiates the firmware download by comparing the software version of FAP on the device with the properties set via xml. Sample xml is shown below:

For UMTS Device: XML Format

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>UMTS Device EID</EID>
```

```
<Updates>
<Parameters>
<Parameter>
<Name>FIRMWARE-UPGRADE-ENABLE</Name>
<Value>true</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-VERSION</Name>
<Value>UMTS Firmware version</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-IMAGE</Name>
<Value>UMTS Firmware version_SCF.xml</Value>
</Parameter>
</Parameters>
</Updates>
</Update>
```

Example:

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>001B67-357539015675404</EID>
<Updates>
<Parameters>
<Parameter>
<Name>FIRMWARE-UPGRADE-ENABLE</Name>
<Value>true</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-VERSION</Name>
<Value>BV3.5.11.5</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-IMAGE</Name>
<Value>BV3.5.11.5_SCF.xml</Value>
</Parameter>
</Parameters>
</Updates>
</Update>
```

For LTE Device: XML Format

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>LTE Device EID</EID>
<Updates>
<Parameters>
<Parameter>
<Name>FIRMWARE-UPGRADE-LTE-ENABLE</Name>
<Value>true</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-LTE-VERSION</Name>
<Value>LTE Firmware version</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-LTE-IMAGE</Name>
<Value>LTE Firmware version_SCF.xml</Value>
</Parameter>
</Parameters>
</Updates>
</Update>
```

Example:

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>001B67-352639054084354</EID>
<Updates>
<Parameters>
<Parameter>
<Name>FIRMWARE-UPGRADE-LTE-ENABLE</Name>
<Value>true</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-LTE-VERSION</Name>
<Value>DSV4.0.3T.9335</Value>
</Parameter>
<Parameter>
<Name>FIRMWARE-UPGRADE-LTE-IMAGE</Name>
<Value>DSV4.0.3T.9335_SCF.xml</Value>
</Parameter>
</Parameters>
</Updates>
</Update>
```

Note For any device if the connection request fails, firmware upgrade is initiated on that device after it connects with an inform having 0 BOOTSTRAP/1 BOOT/2 PERIODIC/6 CONNECTION REQUEST event codes.

Initiating Firmware Upgrade on Bulk FAPs

Continuously post the xml given in Initiating Firmware Upgrade on Individual FAPs , on page 213 to initiate bulk AP upgrades for a selected set of a devices at a uniform rate of two per second from the OSS for the allowed number of hours in the day. Use the `GetDeviceData` script to monitor the status of the firmware upgrade and analyze the GetDeviceData report for device software versions at the end of the day.

Ensure that there is at least an hour gap after the firmware upgrade initiation and firmware upgrade completion before running the `GetDeviceData` script.

Note Until the firmware upgrade gets disabled (as mentioned in Disabling Firmware Upgrade on Individual or Bulk FAPs , on page 215), if any FAP (for which firmware upgrade custom properties are set in BAC) gets a different firmware version from CloudBase after Factory Recovery, then its firmware version changes based on the settings provided at the device level on BAC (when it contacts RMS).

Disabling Firmware Upgrade on Individual or Bulk FAPs

The following procedures describe how to disable firmware upgrade on individual or bulk of FAPs in a controlled manner to ensure that the system is not overloaded.

Disabling Firmware Upgrade on Individual FAPs

Post the update API xml from the OSS to disable firmware upgrade on a single FAP (after it is moved to the intended software) to remove firmware upgrade related custom properties at the device level on the BAC. Sample xml is shown below

For UMTS Device: XML Format

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>UMTS Device EID</EID>
<Removals>
<ParameterNames>
<Name>FIRMWARE-UPGRADE-ENABLE</Name>
<Name>FIRMWARE-UPGRADE-VERSION</Name>
<Name>FIRMWARE-UPGRADE-IMAGE</Name>
</ParameterNames>
</Removals>
</Update>
```

Example:

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>001B67-357539015675404</EID>
<Removals>
<ParameterNames>
<Name>FIRMWARE-UPGRADE-ENABLE</Name>
<Name>FIRMWARE-UPGRADE-VERSION</Name>
<Name>FIRMWARE-UPGRADE-IMAGE</Name>
</ParameterNames>
</Removals>
</Update>
```

For LTE Device: XML Format

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>LTE Device EID</EID>
<Removals>
<ParameterNames>
<Name>FIRMWARE-UPGRADE-LTE-ENABLE</Name>
<Name>FIRMWARE-UPGRADE-LTE-VERSION</Name>
<Name>FIRMWARE-UPGRADE-LTE-IMAGE</Name>
</ParameterNames>
</Removals>
</Update>
```

Example:

```
<Update xmlns="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xsi:schemaLocation="http://www.cisco.com/ca/sse/PMGMessages-v3_0_0
pmg-messages-v3_0_0.xsd">
<TxnID>Update-TxnID-0</TxnID>
<!-- optionally can use SecondaryID -->
<EID>001B67-352639054084354</EID>
```

```
<Removals>
<ParameterNames>
<Name>FIRMWARE-UPGRADE-LTE-ENABLE</Name>
<Name>FIRMWARE-UPGRADE-LTE-VERSION</Name>
<Name>FIRMWARE-UPGRADE-LTE-IMAGE</Name>
</ParameterNames>
</Removals>
</Update>
```



Note Irrespective of the connection request status on the device, firmware upgrade is disabled on the device when the corresponding custom properties are removed from the device level on the BAC.

Disabling Firmware Upgrade on Bulk FAPs

Continuously post the xml given in Disabling Firmware Upgrade on Individual FAPs, on page 216 to disable firmware upgrades (after the upgrade is completed on a selected set of devices) on bulk of APs for a selected set of a devices at a uniform rate of two per second from the OSS for the allowed number of hours in the day.

Upgrading AP Firmware Post RMS 5.1 MR Hotfix Installation

The older LTE FAP firmware is not compatible with the RMS 5.1 MR hotfix software. Therefore, immediately after installing the hotfix, upgrade the LTE FAP firmware. This includes adding the firmware images to RMS and setting the firmware properties.

The following firmware files are required to perform the LTE AP software upgrade:

- <FAP_SoftwareVersion>_SCF.sig
- <FAP_ SoftwareVersion >_SCF.xml
- <FAP_ SoftwareVersion >_standard-kernel.bin
- <FAP_ SoftwareVersion >_rootfs.bin
- <FAP_ SoftwareVersion >_ubiqfs.bin

Uploading Firmware Files Post RMS 5.1 MR Hotfix Installation

Procedure

Step 1 Download the AP software files by following the instructions provided at this link: http://www.cisco.com/c/dam/en/us/td/docs/wireless/asr_5000/smallcell/USC_Software_Docs/R35_MR/References/USC-44-45-001_Downloading_Software_from_CloudBase.pdf.

Step 2 Save the available firmware files to your desktop or machine that is used to access the BAC UI. Save the files in the format <AP Software Version>_<filename>. For example, if AP needs to upgrade to software version DSV4.0.6T.130116, then save the five files in the format given below.

- DSV4.0.6T.130116_SCF.sig
- DSV4.0.6T.130116_SCF.xml

- DSV4.0.6T.130116_rootfs.bin
- DSV4.0.6T.130116_standard-kernel.bin
- DSV4.0.6T.130116_ubiqfs.bin

Step 3 Log in to the BAC UI using 'bacadmin' credentials.

Example:
`https://<CentralNode _eth1_IPAddress>/adminui/`

a) Select the **Configuration** tab on the BAC UI landing page.
b) Click the **Files** tab.
c) In the Files tab, click **Add** to open the Add Files page.
d) From the File Type drop-down list, select the **Firmware File**.
e) Click **Browse** to browse and select the firmware file saved locally as described in Step 2. For example, DSV4.0.6T.130116_SCF.sig.
f) Enter the Filename of the file selected in the previous step. The filename should reflect the selected firmware file name. For example, DSV4.0.6T.130116_SCF.sig.

Step 4 Repeat Step 3 for the remaining four files: DSV4.0.6T.130116_SCF.xml, DSV4.0.6T.130116_standard-kernel.bin, DSV4.0.6T.130116_rootfs.bin and DSV4.0.6T.130116_ubiqfs.bin.

Enabling Firmware Upgrade Properties

Procedure

Step 1 Log in to the BAC UI using 'bacadmin' credentials.

Example:
`https://<CentralNode _eth1_IPAddress>/adminui/`

Step 2 Remove the firmware-related properties, if any present, for specific devices:

a) Select the Devices tab on the BAC UI landing page.
b) Click on the device ID to view the list of device properties in the Modify Device page.
c) Click **Delete** against the property name that is to be deleted.
d) Click **Submit**.
e) Repeat steps 2a to 2d for all those devices that has firmware related properties at the device level. Similarly, remove the properties present at any group level.

Step 3 Update the firmware properties at the Class of Service (CoS) level.

a) Select the Configuration tab on the BAC UI landing page.
b) Click on 'activated-DSV4.0.0T.0 ' CoS to view the list of CoS properties in the Modify Class of Service page.
c) Click **Delete** against the 'FIRMWARE-UPGRADE-LTE-ENABLE' property, which has the 'false' value.
d) In the same Modify Class of Service page, add the following properties and values:

- FIRMWARE-UPGRADE-LTE-ENABLE = true

- FIRMWARE-UPGRADE-LTE-VERSION = DSV4.0.6T.130116
- FIRMWARE-UPGRADE-LTE-IMAGE = DSV4.0.6T.130116_SCF.xml

e) Click **Submit**.
f) Repeat steps 3a to 3e for the 'baseline-DSV4.0.0T.0 ' CoS.

Initiating Firmware Upgrade on Bulk LTE FAPs



Note It is not mandatory to initiate and verify firmware upgrade in the maintenance window. The AP can download firmware upgrade when it contacts RMS.

Before You Begin

Perform TR-069 connection requests (CRs) to CPEs using the massCr.sh tool.

Procedure

Step 1 Log in to the Central node as an admin or ciscorms user.

Step 2 Create a text file with the following content:

```
activated-DSV4.0.0T.0
baseline-DSV4.0.0T.0
```

Note This file must contain only the above two CoS values. For more details on triggering mass connection requests, refer to the "massCr.sh" section of the "Operational Tools" chapter in the *Cisco RAN Management System Administration Guide*.

Example:

```
[central] ~ $ cat text
activated-DSV4.0.0T.0
baseline-DSV4.0.0T.0
[central] ~ $
```

Step 3 Execute the massCr.sh tool using the following command:

```
massCr.sh -idfile <Path and name of the text file created> -type cos
```

Example:

```
[central] ~ $ massCr.sh -idfile /home/admin1/text -type cos
   Rate :: 20
   Retries :: 2
 number of devices: 1
   Output Directory :: /rms/ops/MassConnectionRequest-20160114-065543
** Please note this tool will request ConnectionRequest @ 20devices/sec
Please note this tool will process 20tasks/sec.
EID = 001B67-352639054084560, status = true, statusMsg = Success
******************   Summary Report   ****************************************
Number of successful Connection Requests :: 1
Number of failed Requests :: 0
********************************************************************************
******************   Log Report   ****************************************

Connection Request Success
```

```
Log:/rms/ops/MassConnectionRequest-20160114-065543/massCrSuccess.log

Audit FileName:/rms/ops/MassConnectionRequest-20160114-065543/logs/audit.log
Debug FileName:/rms/ops/MassConnectionRequest-20160114-065543/logs/debug.log
Error FileName:/rms/ops/MassConnectionRequest-20160114-065543/logs/error.log
**************************************************************************
Total execution time: 0 sec
[central] ~ $
```

Note Ensure that there are no errors as shown (see bold text) in the example.

Verifying Firmware Upgrade on LTE FAPs

Ensure that the firmware upgrade verification is performed only after a gap of at least one hour after the firmware upgrade initiation and firmware upgrade completion.

Before You Begin

Retrieve the device data from the RDU database using **getDeviceData.sh** tool and ensure that the firmware upgrade completed successfully on all LTE FAPs by verifying the software version.

Procedure

Step 1 Log in to the Central node console as an admin or ciscorms user.

Step 2 Prepare a configuration file with the software version parameter to retrieve only the software version of the FAPs.
In the following example, 'gddt.conf' is the configuration file created to run the **getDeviceData.sh** tool.

Example:

```
[central] ~ $ cat gddt.conf
DeviceParameter, DeviceDetailsKeys.DEVICE_ID, EID
LiveParameter, Device.DeviceInfo.SoftwareVersion, SoftwareVersion
[central] ~ $
```

Step 3 Create a text file with the following content:

```
activated-DSV4.0.0T.0
baseline-DSV4.0.0T.0
```

Note This file must contain only the above two CoS values. For more details on get device data, refer to the "getDeviceData.sh" section of the "Operational Tools" chapter in the *Cisco RAN Management System Administration Guide*.

Example:

```
[central] ~ $ cat text
activated-DSV4.0.0T.0
baseline-DSV4.0.0T.0
[central] ~ $
```

Step 4 Execute the **getDeviceData.sh** tool using the following command:

```
getDeviceData.sh -config <Path and name of the config file created> -idfile <Path and name
 of the idfile created>
```

Example:

```
[central] ~ $ getDeviceData.sh -config gddt.conf -idfile /home/admin1/text -type cos
Initializing RDU client...
ok
Execution parameters:
 -outdir /rms/ops/GetDeviceData-20160114-081804
 -config /rms/ops/GetDeviceData-20160114-081804/gddt.conf
 -rate 1000/min
 -timeout 60000
 -liveThreads 100
Retrieving device data
 * max rate of get live data requests - 1000/min
 * number of liveThreads - 100
 * timeout for get live data operations - 60000 msec
 * output to [/rms/ops/GetDeviceData-20160114-081804/device-data.csv]
 * errors to [/rms/ops/GetDeviceData-20160114-081804/logs/error.log]
 * audits to [/rms/ops/GetDeviceData-20160114-081804/logs/audit.log]
 * debug messages to [/rms/ops/GetDeviceData-20160114-081804/logs/debug.log]
Creating RDU database backup...
Calling 'sudo /rms/app/CSCObac/rdu/bin/backupDb.sh -noSubdir
/rms/ops/GetDeviceData-20160114-081804.tmp/rdu-backup'...
RDU db backup completed in 1.047 sec
Recovering RDU database ...
RDU db recover completed in 2.495 sec
Performing export of data from db backup...
To directory [/rms/ops/GetDeviceData-20160114-081804.tmp]
Calling 'sudo /rms/app/CSCObac/rdu/bin/deviceExport.sh
/rms/ops/GetDeviceData-20160114-081804.tmp/export-device-control.xml
/rms/ops/GetDeviceData-20160114-081804.tmp/rdu-backup
/rms/ops/GetDeviceData-20160114-081804.tmp'...
Export file [bac-device-details-20160114-081809.csv]
Export from RDU db completed in 0.857 sec
Processed 5 devices. Rate: 145/min. Errors: 4.  Warnings: 0.
Completed processing 5 devices.
Data retrieval completed in 6 sec
Done.
[central] ~ $
```

Note Ensure that there are no errors as shown (see bold text) in the example.

Step 5 Open the '**device-data.csv**' file from the output directory (as highlighted in the example in the previous step) and verify that the software version of all the LTE FAPs are matching and should be '**DSV4.0.6T.130116**'.

Example:

```
[central] ~ $ cat /rms/ops/GetDeviceData-20160114-081804/device-data.csv
EID,SoftwareVersion
001B67-352639054083976,
001B67-352639054089973,
001B67-357539019690128,
001B67-352639054090567,
001B67-352639054084560,DSV4.0.6T.130116
[central] ~ $
```

Note

- In the example only '001B67-352639054084560' is the only operational LTE FAP.
- If there are FAPs whose firmware is not upgraded, then refer to the "Upgrading Firmware" section in the *Cisco RAN Management System Administration Guide*.
- Proceed to the Disabling Firmware Upgrade on Bulk LTE FAPs, on page 222 procedure only if all the APs have the correct software version. This is to prevent the AP from re-attempting to download the firmware files.

Disabling Firmware Upgrade on Bulk LTE FAPs

After upgrading the FAPs successfully to the recommended software version, disable the firmware upgrade using the below procedure:

Procedure

Step 1 Log in to the BAC UI using 'bacadmin' credentials.
`https://<CentralNode _eth1_IPAddress>/adminui/`

Step 2 Select the Configuration tab on the BAC UI landing page.

Step 3 Click on 'activated-DSV4.0.0T.0 ' CoS to view the list of CoS properties in the Modify Class of Service page.

Step 4 Click **Delete** against the following properties:

- FIRMWARE-UPGRADE-LTE-ENABLE = true
- FIRMWARE-UPGRADE-LTE-VERSION = DSV4.0.6T.130116
- FIRMWARE-UPGRADE-LTE-IMAGE = DSV4.0.6T.130116_SCF.xml

Step 5 In the same Modify Class of Service page, add the following property:
`FIRMWARE-UPGRADE-LTE-ENABLE = false`

Step 6 Click **Submit**.

Step 7 Repeat steps 1 to 6 for the 'baseline-DSV4.0.0T.0 ' CoS.

What to Do Next

Proceed to the Basic Sanity Check Post RMS Upgrade, on page 229 and Post RMS 5.1 MR Hotfix Upgrade Task, on page 223 procedures.

Additional Information

- Post upgrade, the "pmguser" password is changed to the default RMS, Release 5.1 MR version password
- After upgrade, the default password provided as the "Current Password" is the default RMS, Release 5.1 MR version password for any newly created DCC UI login user. All the other user passwords, CLI passwords, BAC password, keystore passwords, and so on remain unchanged as in RMS, Release 4.1 or 5.1.
- Perform basic sanity on the system, see Basic Sanity Check Post RMS Upgrade, on page 229.
- (For HotFix only) Check the CAR license validity. To do this, navigate to the CAR Licence file located at `/rms/app/CSCOar/license` directory using the following command.

  `vi /rms/app/CSCOar/license/ CSCOar.lic`
  Example:

```
vi /rms/app/CSCOar/license/ CSCOar.lic
INCREMENT PAR-SIG-NG-TPS cisco 6.0 28-feb-2015 uncounted
VENDOR_STRING=<count>1</count>
HOSTID=ANY
NOTICE="<LicFileID>20140818221132340</LicFileID><LicLineID>1</LicLineID>
```

```
<PAK></PAK>"
SIGN=E42AA34ED7C4
```

The date shown in the example is the expiry date of the CAR license.

If the CAR License has expired, follow the steps specified in CAR/PAR Server Not Functioning , on page 238.

Currently, the license with validity till **4-apr-2016** is present in this directory: `/rms/upgrade/confFiles/license/CSCOar.lic.70`.

Post-Upgrade

Post RMS 5.1 MR Upgrade Tasks

1. The DCC UI dynamic screens, such as SDM Dashboard, Registration, Update, and Groups and IDs XMLs are auto-replaced with the respective RMS, Release 5.1 MR versions. Manually merge the customization as identified in Step 31 of the Pre-Upgrade Tasks for RMS 5.1 MR, on page 179 with the RMS 5.1 MR xml files present in `/rms/app/rms/conf` by following Mapping RMS 4.1 XML Files to RMS 5.1 or 5.1 MR XML Files, on page 223.
2. Enable a periodic backup of the configurations and databases, if it is not already enabled. For more information, see Starting Database and Configuration Backups on Central VM , on page 159.
3. If the upgrade path is from RMS 4.1 to RMS 5.1MR, run the reassign Opstool on the Central node as "ciscorms" user to associate the existing EIDs with the new groups (GlobalRegion and GlobalUMTSSecGateway):

Note The following reassignment should be performed for a set of 50,000 FAPs in each maintenance window.

```
# reassignDevices.sh -idfile eidlist.txt -type devices -donotAssignIds
```

Post RMS 5.1 MR Hotfix Upgrade Task

The DCC UI dynamic screens of Area and Region are auto-replaced with the respective RMS, Release 5.1 MR Hotfix versions. Manually merge the customization as identified in Step 5 of the Pre-Upgrade Tasks for RMS 5.1 MR Hotfix, on page 184 with the RMS 5.1 MR Hotfix xml files present in `/rms/app/rms/conf` by following Mapping RMS 5.1 MR XML Files to RMS 5.1 MR Hotfix XML Files, on page 225.

Mapping RMS 4.1 XML Files to RMS 5.1 or 5.1 MR XML Files

Post upgrade, only the new RMS configuration can be used. To use manually configured properties (specifically the DCC-UI dynamic screens), manually merge the files by copying the respective properties to the new XML of your release. Following are the XML files in RMS 4.1 that require changes and their corresponding XML files in RMS 5.1 or 5.1 MR.

Actual RMS 4.1 XML Files	Corresponding RMS 5.1 or RMS 5.1 MR XML Files
sdm-register-residential-screen-setup.xml	sdm-register-UMTS-residential-screen-setup.xml
sdm-register-enterprise-screen-setup.xml	sdm-register-UMTS-enterprise-screen-setup.xml
sdm-update-residential-screen-setup.xml	sdm-update-UMTS-residential-screen-setup.xml
sdm-update-enterprise-screen-setup.xml	sdm-update-UMTS-enterprise-screen-setup.xml
sdm-static-neighbors-filter-screen-setup.xml	sdm-static-neighbors-filter-screen-setup.xml
sdm-inter-rat-static-neighbors.xml	sdm-inter-rat-static-neighbors.xml
sdm-inter-freq-static-neighbors.xml	sdm-inter-freq-static-neighbors.xml
deviceParamsDisplayConfig.xml	deviceParamsDisplayConfig.xml
bgmt-add-group-screen-setup-Area.xml	bgmt-add-group-screen-setup-Area-MIXED.xml
bgmt-add-group-screen-setup-FemtoGateway.xml	bgmt-add-group-screen-setup-FemtoGateway.xml
bgmt-add-group-screen-setup-RFProfile.xml	bgmt-add-group-screen-setup-RFProfile.xml
bgmt-add-group-screen-setup-AlarmsProfile.xml	bgmt-add-group-screen-setup-AlarmsProfile.xml
bgmt-add-group-screen-setup-Site.xml	bgmt-add-group-screen-setup-Site.xml
bgmt-add-group-screen-setup-Enterprise.xml	bgmt-add-group-screen-setup-Enterprise.xml
bgmt-add-pool-screen-setup-CELL-POOL.xml	bgmt-add-pool-screen-setup-CELL-POOL.xml
bgmt-add-pool-screen-setup-SAI-POOL.xml	bgmt-add-pool-screen-setup-SAI-POOL.xml

Merge RMS 4.1 MR XML Files Manually

The following is a sample procedure of merging files manually.

Procedure

Step 1 If you want the following property, which was manually configured in RMS 4.1 (to block the device through update operation) to be in 5.1 MR as well, copy the below configuration to `/rms/app/rms/conf/sdm-update-residential-screen-setup.xml` from `/rmsbackupfiles/sdm-update-screen-setup.xml`:

```
<ScreenElement>
<Id>blocked</Id>
<Required>false</Required>
```

```
<Label>Block</Label>
<LabelWidth>100px</LabelWidth>
<CheckBox>
</CheckBox>
<ToolTip>Controls if the device is blocked or not.</ToolTip>
<StoredKey>Blocked</StoredKey>
<StoredSection>element</StoredSection>
<StoredType>boolean</StoredType>
</ScreenElement>
```

Step 2 Navigate to `/rms/app/rms/conf`.

Step 3 Edit `sdm-update-UMTS-residential-screen-setup.xml` using **vi editor** as follows:

a) vi **sdm-update-UMTS-residential-screen-setup.xml**

b) At the end of the file, before </ScreenElements> tag, paste the changes identified in the **sdm-update-UMTS-residential-screen-setup.xml** file.

c) Save the changes.

Mapping RMS 5.1 MR XML Files to RMS 5.1 MR Hotfix XML Files

After upgrading from RMS, Release 5.1 MR to Release 5.1 MR Hotfix, only the new RMS configuration can be used. To use manually configured properties (specifically the DCC-UI dynamic screens), manually merge the files by copying the respective properties to the new XML of your release. Following are the XML files in RMS 5.1 MR Hotfix that require changes:

- bgmt-add-group-screen-setup-Area-MIXED.xml
- bgmt-add-group-screen-setup-Region.xml
- bgmt-add-group-screen-setup-Area.xml
- bgmt-add-group-screen-setup-Area-LTE.xml

Ensure that the FC-INTRA-PCILIST-START and FC-INTRA-PCILIST-RANGE properties are not merged or copied to RMS 5.1MR Hotfix XML files because they are not supported from RMS, Release 5.1 MR Hotfix onwards.

Merging RMS 5.1 MR XML Files Manually

Procedure

Step 1 If you want the following property, which was manually configured in RMS 5.1 MR to be in 5.1 MR Hotfix, copy the below configuration to `/rms/app/rms/conf/bgmt-add-group-screen-setup-Area-MIXED.xml` from `/rmsbackupfiles/bgmt-add-group-screen-setup-Area-MIXED.xml`:

```
<ScreenElement>
        <Id>FC-NO-LV-1</Id>
        <Required>false</Required>
        <Label>NO-LV</Label>
```

```
        <LabelWidth>100px</LabelWidth>
        <BooleanFilteringSelect>
            <FieldWidth>198px</FieldWidth>
         </BooleanFilteringSelect>
        <ToolTip>Choose the value of property FC-NO-LV.</ToolTip>
        <StoredKey>FC-NO-LV</StoredKey>
        <StoredSection>parameters</StoredSection>
        <StoredType>boolean</StoredType>
        <IsDisplayedInGrid>true</IsDisplayedInGrid>
  <ColumnWidth>100px</ColumnWidth>
    </ScreenElement>
```

Step 2 Navigate to `/rms/app/rms/conf`.

Step 3 Edit **`bgmt-add-group-screen-setup-Area-MIXED.xml`** using **vi editor** as follows:

a) vi **bgmt-add-group-screen-setup-Area-MIXED.xml**

b) At the end of the file, before </ScreenElements> tag, paste the changes identified in the **bgmt-add-group-screen-setup-Area-MIXED.xml** file.

c) Save the changes.

Record BAC Configuration Template File Details

Follow this procedure to record the Class of Service (Cos) for the manually edited BAC configuration template file pre-upgrade.

Procedure

Step 1 Log in to the BAC UI.

Step 2 Go to **Configuration > Class of Service**.

Step 3 Click each CoS and record all the manual customization implemented in the configuration template.

Note Record can be a copy of additional configuration to a document on the local machine to add back in the configuration template, post upgrade.

Skip this step if the customized information is available.

Associate Manually Edited BAC Configuration Template

Follow this procedure to associate the manually edited BAC configuration template, post upgrade.

Procedure

Step 1 Log in to the BAC UI.
Step 2 Go to **Configuration > Files**.
Step 3 Export each configuration template to be customized.
Step 4 Save the file to the local machine and customize the changes in the template as per the backup file.
Step 5 Go to **Configuration > Files**.
Step 6 Click **Add** to open the Add File dialog box.
Step 7 In the File Type drop-down list, select **Configuration Template**.
Step 8 Click **Browse** and select the file from your system.
Step 9 Click **Submit**.
Step 10 Repeat the steps for all the applicable templates.

Rollback to RMS, Release 4.1

Procedure

Step 1 Power-Off the current VM.
Step 2 Right-click on the VM, and choose the option **Delete from Disk**.
Step 3 Click Yes to complete the delete operation.
Step 4 Follow the steps described in Restore from vApp Clone, on page 296.

Rollback to RMS, Release 5.1 or 5.1 MR

Procedure

Step 1 Power-Off the current VM.
Step 2 Right-click on the VM and click **Delete from Disk**.
Step 3 Click Yes to complete the delete operation.
Step 4 Follow the steps described in Restore from vApp Clone, on page 296.
Step 5 Follow the steps described in Network Unreachable on Cloning RMS VM , on page 251 to access the clone via ssh.

Remove Obsolete Data

Note Ignore the "No such file or directory" message displayed while executing the below commands.

Procedure

Step 1 Log in to the Central node as a 'root' user and delete the log files that are older than five days by executing the below commands:

a) Delete the tarred log files and tmp files in the `/rms/log/pmg` directory that are older than five days.

```
i. find /rms/log/pmg/*.log.gz -mtime +5 -exec rm {} \;

ii. find /rms/log/pmg/*.tmp -mtime +5 -exec rm {} \;
```

b) Delete log and tmp files in the `/rms/log/dcc_ui` directory that are older than five days.

```
i. find /rms/log/dcc_ui/*.log.* -mtime +5 -exec rm {} \;
ii. find /rms/log/dcc_ui/*.tmp -mtime +5 -exec rm {} \;
```

c) Delete all RMS4.1 hotfix related files (folders and tars) present in `/rms` and `/home` directory.

```
i. cd /rms
ii.rm -rf rms41hotfix05_rollback/ RMS-4.1.0-1N-HOTFIX02.tar.gz
RMS-4.1.0-1N-HOTFIX05.tar.gz rms41hotfix02/ RMS-4.1.0-1N-HOTFIX01.tar.gz
rms41hotfix05/ rms41_leap_second/ rms41hotfix/ RMS-4.1.0-1N-Leap_Second.tar.gz
RMS-4.1.0-1N-HOTFIX06.tar.gz rms41hotfix06/
```

d) Delete opstool log files in the `/rms/ops` directory that are older than five days.

```
find /rms/ops/* -daystart -mtime +5 –delete;
```

e) Delete the troubleshooting logs, agent logs, and cron backups that are older than five days using the following commands:

```
i. find /rms/data/CSCObac/rdu/logs/troubleshooting.log.* -mtime +5 -exec rm {} \;
ii. find /rms/data/CSCObac/agent/logs/*.log-[0-9]* -mtime +5 -exec rm {} \;
iii. find /rms/backups/* -mtime +5 -type f -exec rm {} \;
```

Step 2 Log in to the Serving node as a 'root' user and delete the log files that are older than five days.

a) Delete all RMS4.1 hotfix related files (folders and tars) present in `/rms` and `/home` directory.

```
i. cd /rms
ii. rm -rf rms41hotfix05_rollback/ upgrade_par/ RMS-4.1.0-1N-HOTFIX02.tar.gz
RMS-4.1.0-1N-HOTFIX05.tar.gz rms41hotfix02/ RMS-4.1.0-1N-HOTFIX01.tar.gz
rms41hotfix05/ rms41_leap_second/ rms41hotfix/ RMS-4.1.0-1N-Leap_Second.tar.gz
RMS-4.1.0-1N-HOTFIX06.tar.gz rms41hotfix06/ PAR-UPGRADE-6.1.2.3.tar.gz
```

b) Delete DPE and agent logs present in the `/rms/data/CSCObac` directory that are older than five days.

```
i. find /rms/data/CSCObac/dpe/logs/dpe.*.log -daystart -mtime +5 -delete;
ii. find /rms/data/CSCObac/agent/logs/*.log-[0-9]* -daystart -mtime +5 -delete;
```

Step 3 Log in to the Upload node as a root user and delete the log files that are older than five days by executing the following commands:

a) Delete all RMS4.1 hotfix related files (folders and tars) present in `/rms` and `/home` directory.

```
i. cd /rms
ii. rm -rf rms41hotfix05_rollback/ RMS-4.1.0-1N-HOTFIX02.tar.gz
RMS-4.1.0-1N-HOTFIX05.tar.gz rms41hotfix02/ RMS-4.1.0-1N-HOTFIX01.tar.gz
rms41hotfix05/ rms41_leap_second/ rms41hotfix/ RMS-4.1.0-1N-Leap_Second.tar.gz
RMS-4.1.0-1N-HOTFIX06.tar.gz rms41hotfix06/
```

b) Delete Upload server log files that are older than five days.

```
i. find /opt/CSCOuls/logs/*.gz -daystart -mtime +5 –delete;
ii. find /opt/CSCOuls/logs/*.tmp -daystart -mtime +5 –delete;
```

Basic Sanity Check Post RMS Upgrade

RMS installation sanity check should be performed to ensure that all processes are up and running. For more information, see RMS Installation Sanity Check, on page 101.

On DCC UI:

- Browse through all tabs on UI and check the group contents.
- Create a new user.
- Create a new role.

On Existing AP:

1. Trigger connection request.
2. Reboot.
3. Trigger on-demand log upload.
4. Perform Factory Recovery/Reset.
5. Set/Get live data.
6. Upgrade firmware.
7. Delete Device.

On New AP:

- Register and activate a small cell device.
- Perform firmware upgrade.
- Verify IPSec connection.
- Verify connection request.
- Set/Get live data.
- Reboot.
- Trigger on-demand log upload.

- Perform Factory Recovery/Reset.

Stopping Cron Jobs

Procedure

Step 1 Log in to Central node as a root user

Step 2 Disable OpsTools crons by moving the file CSCOrms-ops-tools-ga from `/etc/cron.d` to `/rms/`.

```
# mv /etc/cron.d/CSCOrms-ops-tools-ga /rms/
```

Step 3 Disable crontab for backup_central_vm cron by clearing the cron tab file.

1. Back up the cron tab entries.
   ```
   # crontab -l > /rms/crontab_backup.txt
   ```
2. Clear the crontab file.
   ```
   # crontab –r
   ```
3. Verify that the crontab is disabled.
   ```
   # crontab –l
   no crontab for root
   ```

Step 4 Terminate all the ongoing crons related to Ops tools and backup.

```
# pkill -9 -f gpsExportData;
# pkill -9 -f bulkStatusReport;
# pkill -9 -f getDeviceData;
# pkill -9 -f GetDeviceData;
# pkill -9 –f backup_central_vm;
```

Step 5 Verify that there are no cron jobs running and the output of the below command is '0'.

```
# ps -ef | grep -iE "backup_central_vm|bulkStatusReport|getDeviceData|gpsExportData" | grep
 -v grep | wc -l
0
```

Step 6 Ensure that any additional cron jobs (for any user) configured are stopped using steps 1 to 5.

Step 7 Repeat steps 1 to 6 on the cold standby Central node in case of a high availability setup.

Starting Cron Jobs

Procedure

Step 1 Log in to Central node as a root user

Step 2 Enable OpsTools crons by moving the file CSCOrms-ops-tools-ga to `/etc/cron.d` from `/rms/`.

```
# mv /rms/CSCOrms-ops-tools-ga /etc/cron.d/
```

Step 3 Enable the backup cron by repopulating the crontab file.

```
# crontab /rms/crontab_backup.txt
```

Step 4 Verify the crontab file.

```
# crontab -l
0 1 * * * /rms/ova/scripts/redundancy/backup_central_vm.cron.hourly
10 Ch@ngeme1 2>&1 | logger -p daemon.notice
```

Step 5 Enable any additional crons that were configured.

Step 6 Repeat steps 1 to 5 on the cold standby Central node in case of a high availability setup.

Disabling RMS Northbound and Southbound Traffic

Disabling RMS Northbound Traffic

To disable the Northbound traffic, stop the OSS and DCC UI operations.

Disabling RMS Southbound Traffic

Procedure

Step 1 Log in to the Central node VM and ping the eth1 IP (refer, ifconfig) of the Serving and Upload node (from the Central node) and ensure that the IP is reachable.

Step 2 Log in to the vSphere Web Client and locate the Serving and Upload node VM or vApp.

Step 3 Right-click on the Serving and Upload node VM and click **Edit Settings**.

Step 4 Identify the corresponding network adapter or VLAN of the Southbound interface (refer the descriptor file used for installing the RMS system to identify the VLAN of the Serving and Upload node Southbound interface, that is, the property value of 'net:Serving-Node Network 2' and 'net:Upload-Node Network 2').

Step 5 Uncheck the **Connected** checkbox of the network adapter or VLAN of the Serving and Upload node Southbound interface.

Step 6 Click **Ok**.

Step 7 To verify that the interface is down, ping the eth1 IP (refer, ifconfig) of the Serving and Upload node (from the Central node) and ensure that the IP is not reachable.

Step 8 Repeat the steps on the redundant Serving and Upload node in case of redundant setup.

Enabling RMS Northbound and Southbound Traffic

Enabling RMS Northbound Traffic

To enable the Northbound traffic, start the OSS and DCC UI operations.

Enabling RMS Southbound Traffic

Procedure

Step 1 Log in to the vSphere Web Client and locate the Serving and Upload node VM or vApp.

Step 2 Right-click on the Serving and Upload node VM and click **Edit Settings**.

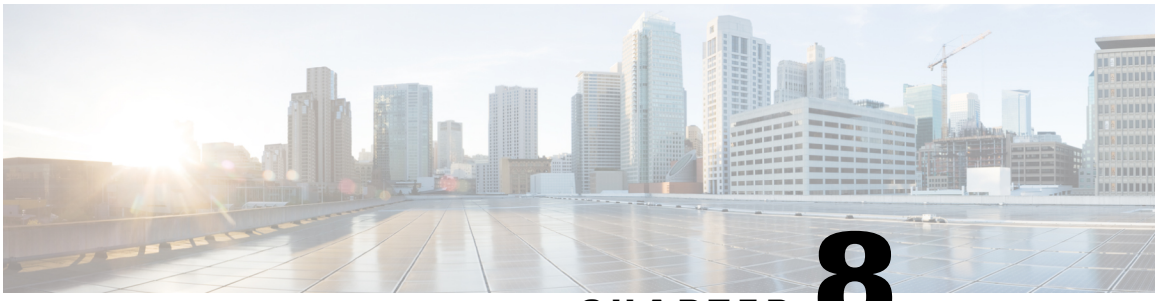
Step 3 Identify the corresponding network adapter or VLAN of the Southbound interface (refer Step 4 of "Disabling RMS Southbound Traffic" in Disabling RMS Northbound and Southbound Traffic, on page 231).

Step 4 Check the **Connected** checkbox of the network adapter or VLAN of the Serving and Upload node Southbound interface.

Step 5 Click **Ok**.

Step 6 To verify that the interface is down, ping the eth1 IP (refer, ifconfig) of the Serving and Upload node (from the Central node) and ensure that the IP is reachable.

Step 7 Repeat the steps on the redundant Serving and Upload node in case of redundant setup.



CHAPTER 8

Troubleshooting

This chapter provides procedures for troubleshooting the problems encountered during RMS Installation.

- Regeneration of Certificates, page 233
- Deployment Troubleshooting , page 238

Regeneration of Certificates

Following are the scenarios that requires regeneration of certificates:

- Certificate expiry (Certificate will have a validity of one year.)
- If importing certificates are not successful.

Follow the steps to regenerate self-signed certificates:

Certificate Regeneration for DPE

To address the problems faced during the certificate generation process in Distributed Provisioning Engine (DPE), complete the following DPE regeneration steps:

Note Manually back-up older keystores because the keystores are replaced whenever the script is executed.

Procedure

Step 1 Log in to the RMS Central node.

Step 2 Establish an ssh connection to the RMS Serving node.

Step 3 Switch to root user: **su -**

Step 4 Navigate to `/rms/ova/scripts/post_install` directory.

Step 5 Run the regeneration script: **./dpe_certificate_regenarate.sh**

The script prompts for values required for the certificate generation as shown in the sample output:

Note
- Provide appropriate values for the fields when prompted and follow the steps displayed on the console to install the regenerated certificates on RMS.
- If exceptions are seen on the console about aliases, remove the respective aliases from the cacerts using the following commands

```
keytool -delete -alias <server-ca> -keystore
/rms/app/CSCObac/jre/lib/security/cacerts -storepass changeit
```

Sample Output:

```
[root@blrrms-serving-MR post_install]# ./dpe_certificate_regenarate.sh
Enter RMS App Password
Connection closed by foreign host.
blrrms-serving-MR> enable

What is your first and last name(Common Name)? ( ex: rms-serving-blr13.cisco.com )
rms-serving-blr13.cisco.com
What is the name of your organizational unit? (Min 2 characters)
CC
What is the name of your organization? (Min 2 characters)
CISCO
What is the name of your City or Locality? (Min 2 characters)
BLR
What is the name of your State or Province? (Min 2 characters)
KA
What is the two-letter country code for this unit?
IN
Is CN=rms-serving-blr13.cisco.com OU=CC, O=CISCO, L=BLR, ST=KA, C=IN Correct (yes/no) ?
yes
Deleting server-ca , root-ca alias from cacerts
*NOTE: Ignore the error if certs are installed with different naming convention and delete
 them manually
keytool error: java.lang.Exception: Alias <server-ca> does not exist
keytool error: java.lang.Exception: Alias <root-ca> does not exist
create dpe keystore, private key and certificate request
Enter keystore password:  Re-enter new password: Enter key password for <dpe-key>
        (RETURN if same as keystore password):  Re-enter new password: Enter destination
keystore password:
Re-enter new password: Enter source keystore password:  MAC verified OK
Changing permissions
Connection closed by foreign host.
fix permissions on secure files
Dpe certificate regenerated Successfully
DPE CSR and keystore are regenerated and placed in '/rms/app/CSCObac/dpe/conf/self_signed'
 directory.

Follow the below steps to make TLS communication using the regenerated files
  1.Sign the dpe.csr using signing authority and place the '<intermediate-ca>.cer,
<root-ca>.cer and <client-ca>.cer' certificate files in
'/rms/app/CSCObac/dpe/conf/self_signed' directory
  2.Import '<intermediate-ca>.cer and <root-ca>.cer' certificates into the dpe cacerts using
 below commands:
```

```
  NOTE: Provide the 'cacerts' password when prompted
          /rms/app/CSCObac/jre/bin/keytool -import -alias server-ca -file
<intermediate-ca.cer> -keystore /rms/app/CSCObac/jre/lib/security/cacerts
    /rms/app/CSCObac/jre/bin/keytool -import -alias root-ca -file <root-ca.cer> -keystore
/rms/app/CSCObac/jre/lib/security/cacerts
  3.Import '<client-ca>.cer' certificate into dpe.keystore. using the below command:
  NOTE: Provide the 'RMS_App_Password' password when prompted
    /rms/app/CSCObac/jre/bin/keytool -import -trustcacerts -file <client-ca.cer> -keystore
 /rms/app/CSCObac/dpe/conf/self_signed/dpe.keystore -alias dpe-key
  4.Copy dpe.keystore to conf/ folder using the below command:
    cp /rms/app/CSCObac/dpe/conf/self_signed/dpe.keystore /rms/app/CSCObac/dpe/conf/
  5.Change the permission of the keystore file and restart the dpe using below command:
          chmod 640 /rms/app/CSCObac/dpe/conf/dpe.keystore
  6.Restart dpe
    /etc/init.d/bprAgent restart dpe
Verify the TLS communication between the AP and DPE
[root@SERVING-MR post_install]#
```

DPE CSR and keystore are regenerated and placed in the `/rms/app/CSCObac/dpe/conf/self_signed` directory on execution of the script.

Step 6 Install the regenerated certificates on the Serving node as described in the Self-Signed RMS Certificates, on page 112 procedure.

Note While importing certificates, if the following keytool error is displayed, "java.lang.Exception: Input not an X.509 certificate", perform the following checks:

- While trying to install the certificate, if an incorrect alias was specified.
- During import, if the certificate was improperly formatted, like having additional blank spaces in the beginning and end of the lines.
- The certificate is being imported into an incorrect keystore.

Certificate Regeneration for Upload Server

Following are the Keystore regeneration steps to be performed manually if something goes wrong with the certificate generation process in LUS:

Note Manually backup older keystores because the keystores are replaced whenever the script is executed.

Procedure

Step 1 Open the generate_keystore.sh script from /opt/CSCOuls/bin/ directory as a 'root' user using the below command.

Example:

```
vi /opt/CSCOuls/bin/generate_keystore.sh
```

Step 2 Edit the below lines as per OVA descriptor settings:

```
Cert_C="IN"
Cert_ST="KA"
Cert_L="BLR"
Cert_O="Cisco Systems, Inc."
Cert_OU="SCTG"
Upload_SB_Fqdn="femtolus17.testlab.in"
RMS_App_Password="Rmsuser@1"
```

Step 3 Run the script:

Enter:

```
./generate_keystore.sh
```

Output:

```
[root@BLR17-Upload-41N bin]# ./generate_keystore.sh
create uls keystore, private key and certificate request
Enter keystore password:  Re-enter new password: Enter key password for <uls-key>
        (RETURN if same as keystore password):  Re-enter new password: Enter destination
keystore password:  Re-enter new password: Enter source keystore password:  Adding UBI CA
certs to uls truststore
Enter keystore password:  Owner: O=Ubiquisys, CN=Co Int CA
Issuer: O=Ubiquisys, CN=Co Root CA
Serial number: 40d8ada022c1f52d
Valid from: Fri Mar 22 16:42:03 IST 2013 until: Tue Mar 16 16:42:03 IST 2038
Certificate fingerprints:
         MD5:  F0:F0:15:82:D3:22:A9:D7:4A:48:58:00:25:A9:E5:FC
         SHA1: 38:45:74:77:61:08:A9:78:53:22:C1:29:7F:B8:8C:35:52:6F:31:79
         SHA256:
DC:88:99:BE:A0:A3:BE:5F:49:11:DA:FB:85:83:05:CF:1E:A2:FA:E0:4F:4D:18:AF:0B:9B:23:3F:5F:D2:57:61

         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4B 49 74 B3 E2 EF 41 BF                            KIt...A.
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:0
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
```

```
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 4C 29 95 49 9D 27 44 86                            L).I.'D.
]
]

Trust this certificate? [no]:  Certificate was added to keystore
Enter keystore password:  Owner: O=Ubiquisys, CN=Co Root CA
Issuer: O=Ubiquisys, CN=Co Root CA
Serial number: 99af1d71b488d88e
Valid from: Fri Mar 22 16:12:43 IST 2013 until: Tue Mar 16 16:12:43 IST 2038
Certificate fingerprints:
         MD5:  FA:FA:41:EF:2E:F1:83:B8:FD:94:9F:37:A2:8E:EE:7C
         SHA1: 99:B0:FA:51:C7:B2:45:5B:44:22:C0:F6:24:CD:91:3F:0F:50:DE:AB
         SHA256:
1C:64:6E:CB:27:2D:23:5C:B3:01:09:6B:02:F9:3E:B6:B2:59:42:50:CD:8C:75:A6:3F:8A:66:DF:A5:18:B6:74

         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4B 49 74 B3 E2 EF 41 BF                            KIt...A.
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 4B 49 74 B3 E2 EF 41 BF                            KIt...A.
]
]

Trust this certificate? [no]:  Certificate was added to keystore
MAC verified OK
Changing permissions
fix permissions on secure files
```

```
[root@BLR17-Upload-41N bin]#
```

The uls.keystore and uls.csr are regenerated in this directory: /opt/CSCOuls/conf/self_signed

Step 4 Copy the certificates from the /self_signed directory to the /conf directory.

```
cp /opt/CSCOuls/conf/self_signed/openssl.cnf /opt/CSCOuls/conf/openssl.cnf
cp /opt/CSCOuls/conf/self_signed/uls.trustore /opt/CSCOuls/conf/uls.trustore
```

Step 5 After getting the uls.csr file, get it signed by the signing authority to get client, server, and root certificates.

Step 6 Reinstall the certificates. For more information, see the "Installing RMS Certificates" section.

Step 7 Reload the server process. Follow the step 7 in "Installing RMS Certificates" section.

Deployment Troubleshooting

To address the problems faced during RMS deployment, complete the following steps.

For more details to check the status of CN, ULS and SN see RMS Installation Sanity Check, on page 101.

CAR/PAR Server Not Functioning

Issue	CAR/PAR server is not functioning. During login to **aregcmd** with user name 'admin' and proper password, this message is seen: "Communication with the 'radius' server failed. Unable to obtain license from server."
Cause	**1** The property, "prop:Car_License_Base " is set incorrectly in the descriptor file. or **2** CAR license has expired.

Solution	**1** Log in to Serving node as a root user.
	2 Navigate to the /rms/app/CSCOar/license directory (`cd /rms/app/CSCOar/license`).
	3 Edit CSCOar.lic file to vi CSCOar.lic. Either overwrite the new license in the file or comment the existing one and add the fresh license in a new line:
	Overwrite:
	`[root@rms-aio-serving license]# vi CSCOar.lic`
	`INCREMENT PAR-SIG-NG-TPS cisco 6.0 28-feb-2015 uncounted`
	`VENDOR_STRING=<count>1</count>`
	`HOSTID=ANY`
	`NOTICE="<LicFileID>20140818221132340</LicFileID><LicLineID>1</LicLineID> <PAK></PAK>"`
	`SIGN=E42AA34ED7C4`
	Comment the existing license and add the fresh license in the new line:
	`[root@rms-aio-serving license]# vi CSCOar.lic`
	`#INCREMENT PAR-SIG-NG-TPS cisco 6.0 06-sept-2014 uncounted`
	`VENDOR_STRING=<count>1</count> HOSTID=ANY NOTICE="`
	`<LicFileID>20140818221132340</LicFileID><LicLineID>1</LicLineID>`
	`<PAK></PAK>"`
	`SIGN=E42AA34ED7C4`
	`INCREMENT PAR-SIG-NG-TPS cisco 6.0 28-feb-2015 uncounted`
	`VENDOR_STRING=<count>1</count>`
	`HOSTID=ANY NOTICE="<LicFileID>20140818221132340</LicFileID>`
	`<LicLineID>1</LicLineID> <PAK></PAK>" SIGN=E42AA34ED7C4`
	4 Navigate to the /home directory (`cd /home`) and repeat the previous step on the CSCOar.lic file in this directory.
	5 Go to the Serving node console and restart PAR server using the following command:
	`/etc/init.d/arserver stop`
	`/etc/init.d/arserver start`
	After restarting the PAR server, check the status using the following command:
	`/rms/app/CSCOar/usrbin/arstatus`
	Output:
	`Cisco Prime AR RADIUS server running (pid: 1668)`
	`Cisco Prime AR Server Agent running (pid: 1655)`
	`Cisco Prime AR MCD lock manager running (pid: 1659)`
	`Cisco Prime AR MCD server running (pid: 1666)`
	`Cisco Prime AR GUI running (pid: 1669)`

Unable to Access BAC and DCC UI

Issue	Not able to access BAC UI and DCC UI due to expiry of certificates in browser.
Cause	Certificate added to the browser just has three months validity.

Solution	**1** Delete the existing certificates from the browser. Go to **Tools > Options**. In the Options dialog, click **Advanced > Certificates > View Certificates**. **2** Select RMS setup certificate and delete. **3** Clear the browser history. **4** Access DCC UI/BAC UI again. The message "This Connection is Untrusted" appears. Click Add Exception and click Confirm Security Exception from Add Security Exception dialog.

DCC UI Shows Blank Page After Login

Issue	Unsupported plugins installed in the Browser
Cause	Unsupported plugins cause conflicts with the DCC UI Operation
Solution	**1** Remove or uninstall all unsupported/incompatible third party plugins on the browser. Or, **2** Reinstall the Browser

DHCP Server Not Functioning

Issue	DHCP server is not functioning. During login to **nrcmd** with user name 'cnradmin' and proper password, it shows groups and roles as 'superuser'; but if any command related to DHCP is entered, the following message is displayed. "You do not have permission to perform this action."
Cause	The property, "prop:Cnr_License_IPNode" is set incorrectly in the descriptor file.

Solution

1. Edit the following *product.license* file with proper license key for PNR by logging into central node.

```
/rms/app/nwreg2/local/conf/product.licenses
Sample license file for reference:
INCREMENT count-dhcp cisco 8.1 permanent uncounted
VENDOR_STRING=<Count>10000</Count>
   HOSTID=ANY
NOTICE="<LicFileID>20130715144658047</LicFileID><LicLineID>1</LicLineID>

   <PAK></PAK><CompanyName></CompanyName>" SIGN=176CCF90B694
INCREMENT base-dhcp cisco 8.1 permanent uncounted
VENDOR_STRING=<Count>1000</Count>
   HOSTID=ANY
NOTICE="<LicFileID>20130715144658047</LicFileID><LicLineID>2</LicLineID>

   <PAK></PAK><CompanyName></CompanyName>" SIGN=0F10E6FC871E
INCREMENT base-system cisco 8.1 permanent uncounted
VENDOR_STRING=<Count>1</Count>
   HOSTID=ANY
NOTICE="<LicFileID>20130715144658047</LicFileID><LicLineID>3</LicLineID>

   <PAK></PAK><CompanyName></CompanyName>" SIGN=9242CBD0FED0
```

2. Log in to PNR GUI.
   http://<central nb ip>:8090

   User Name: cnradmin

   Password: <prop:Cnradmin_Password> (Property value from the descriptor file)

3. Click **Administration > Licenses** from Home page.
   The following three types of license keys should be present. If not present, add them using browser.
   1. Base-dhcp
   2. Count-dhcp
   3. Base-system
4. Click **Administration > Clusters**.
5. Click **Resynchronize**.
   Go to Serving Node Console and restart PNR server using the following command:

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

   After restarting the PNR server, check the status using the following command:

```
/rms/app/nwreg2/local/usrbin/cnr_status
```

   Output:

```
DHCP Server running             (pid: 8056)
Server Agent running            (pid: 8050)
CCM Server running              (pid: 8055)
WEB Server running              (pid: 8057)
CNRSNMP Server running          (pid: 8060)
RIC Server Running              (pid: 8058)
TFTP Server is not running
DNS Server is not running
DNS Caching Server is not running
```

DPE Processes are Not Running

Scenario 1:

DPE Installation Fails with error log:

Issue	This DPE is not licensed. Your request cannot be serviced"
Cause	Configure the property `prop:Dpe_Cnrquery_Client_Socket_Address=NB IP address of serving node` in the descriptor file. If other than NB IP address of serving node is given then "DPE is not licensed error" will appear in OVA first boot log.

Solution	1 Log in to DPE CLI using the command **[admin1@blr-rms11-serving ~]$**
	2 Execute the command **telnet localhost 2323**.
	`Trying 127.0.0.1...`
	`Connected to localhost.`
	`Escape character is '^]'.`
	`blr-rms11-serving BAC Device Provisioning Engine`
	`User Access Verification`
	`Password:`
	`blr-rms11-serving> en`
	`Password:`
	`blr-rms11-serving# dpe cnrquery giaddr x.x.x.x`
	`blr-rms11-serving# dpe cnrquery server-port 61610`
	`blr-rms11-serving# dhcp reload`

Scenario 2:

Issue	DPE process might not run when the password of keystore and key mismatches from the descriptor file.
Cause	The Keystore was tampered with, or password entered is incorrect resulting in a password verification failure. This occurs when the password used to generate the Keystore file is different than the one given for the property "prop:RMS_App_Password" in descriptor file.

Solution	**1** Navigate to /rms/app/CSCObac/dpe/conf and execute the below command to change the password of the Keystore file.
	Input:
	`"[root@rtpfga-s1-upload1 conf]# keytool -storepasswd –keystore dpe.keystore"`
	Output:
	`Enter keystore password:OLD PASSWORD`
	`New keystore password: NEW PASSWORD`
	`Re-enter new keystore password: NEW PASSWORD`
	Input:
	`[root@rtpfga-s1-upload1 conf]# keytool -keypasswd -keystore dpe.keystore -alias dpe –key`
	Output:
	`Enter keystore password: NEW AS PER LAST COMMAND`
	`Enter key password for <dpe-key> : OLD PASSWORD`
	`New key password for <dpe-key>: NEW PASSWORD`
	`Re-enter new key password for <dpe-key>: NEW PASSWORD`
	Note The new keystore password should be same as given in the descriptor file.
	2 Restart the server process.
	`[root@rtpfga-s1-upload1 conf]# /etc/init.d/bprAgent restart dpe`
	`[root@rtpfga-s1-upload1 conf]# /etc/init.d/bprAgent status dpe`
	`BAC Process Watchdog is running.`
	`Process [dpe] is running.`
	`Broadband Access Center [BAC 3.8.1.2 (LNX_BAC3_8_1_2_20140918_1230_12)].`
	`Connected to RDU [10.5.1.200].`
	`Caching [3] device configs and [52] files.`
	`188 sessions succeeded and 1 sessions failed.`
	`6 file requests succeeded and 0 file requests failed.`
	`68 immediate device operations succeeded, and 2 failed.`
	`0 home PG redirections succeeded, and 0 failed.`
	`Using signature key name [] with a validity of [3600].`
	`Abbreviated ParamList is enabled.`
	`Running for [4] hours [23] mins [17] secs.`

Connection to Remote Object Unsuccessful

Issue	A connection to the remote object could not be made. OVF Tool does not support this server. Completed with errors
Cause	The errors are triggered by ovftool command during ova deployment. the errors can be found in both Console and vCenter logs.
Solution	User must have Administrator privileges to VMware vCenter and ESXi.

VLAN Not Found

Issue	VLAN not found.
Cause	The errors are triggered by ovftool command during ova deployment. the errors can be found in both Console and vCenter logs.
Solution	Check for the appropriate "portgroup" name on virtual switch of Elastic Sky X Integrated (ESXi) host or Distributed Virtual Switch (DVS) on VMware vCenter.

Unable to Get Live Data in DCC UI

Issue	Live Data of an AP is not coming and Connection request fails.
Cause	**1** Device is offline. **2** Device is not having its radio activated/ device is registered but not activated.
Solution	**1** In the Serving Node, add one more route with Destination IP as HNB-GW SCTP IP and Gateway as Serving Node North Bound IP as in the following example: Serving NB Gateway IP-10.5.1.1 HNBGW SCTP IP- 10.5.1.83 Add the following route in Serving node: `route add -net 10.5.1.83 netmask 255.255.255.0 gw 10.5.1.1` **2** Activate the device from DCC UI post registration. **3** Verify trouble shooting logs in bac. **4** Verify DPE logs and ZGTT logs from ACS simulator.

Installation Warnings about Removed Parameters

These properties have been completely removed from the 4.0 OVA installation. A warning is given by the installer, if these properties are found in the OVA descriptor file. However, installation still continues.

```
prop:vami.gateway.Upload-Node
prop:vami.DNS.Upload-Node
prop:vami.ip0.Upload-Node
prop:vami.netmask0.Upload-Node
prop:vami.ip1.Upload-Node
prop:vami.netmask1.Upload-Node
prop:vami.gateway.Central-Node
prop:vami.DNS.Central-Node
prop:vami.ip0.Central-Node
prop:vami.netmask0.Central-Node
```

```
prop:vami.ip1.Central-Node
prop:vami.netmask1.Central-Node
prop:vami.gateway.Serving-Node
prop:vami.DNS.Serving-Node
prop:vami.ip0.Serving-Node
prop:vami.netmask0.Serving-Node
prop:vami.ip1.Serving-Node
prop:vami.netmask1.Serving-Node
prop:Debug_Mode
prop:Server_Crl_Urls
prop:Bacadmin_Password
prop:Dccapp_Password
prop:Opstools_Password
prop:Dccadmin_Password
prop:Postgresql_Password
prop:Central_Keystore_Password
prop:Upload_Stat_Password
prop:Upload_Calldrop_Password
prop:Upload_Demand_Password
prop:Upload_Lostipsec_Password
prop:Upload_Lostgwconnection_Password
prop:Upload_Nwlscan_Password
prop:Upload_Periodic_Password
prop:Upload_Restart_Password
prop:Upload_Crash_Password
prop:Upload_Lowmem_Password
prop:Upload_Unknown_Password
prop:Serving_Keystore_Password
prop:Cnradmin_Password
prop:Caradmin_Password
prop:Dpe_Cli_Password
prop:Dpe_Enable_Password
prop:Fc_Realm
prop:Fc_Log_Periodic_Upload_Enable
prop:Fc_Log_Periodic_Upload_Interval
prop:Fc_On_Nwl_Scan_Enable
prop:Fc_On_Lost_Ipsec_Enable
prop:Fc_On_Crash_Upload_Enable
prop:Fc_On_Call_Drop_Enable
prop:Fc_On_Lost_Gw_Connection_Enable
prop:Upload_Keystore_Password
prop:Dpe_Keystore_Password
prop:Bac_Secret
prop:Admin2_Username
prop:Admin2_Password
prop:Admin2_Firstname
prop:Admin2_Lastname
prop:Admin3_Username
prop:Admin3_Password
prop:Admin3_Firstname
prop:Admin3_Lastname
prop:Upgrade_Mode
prop:Asr5k_Hnbgw_Address
```

Upload Server is Not Up

The upload server fails with java.lang.ExceptionInInitializerError in the following scenarios.

The errors can be seen in `opt/CSCOuls/logs/uploadServer.console.log` file.

Scenario 1:

Issue	Upload Server failed with java.lang.ExceptionInInitializerError java.lang.ExceptionInInitializerError at com.cisco.ca.rms.upload.server.UlsSouthBoundServer.getInstance (UlsSouthBoundServer.java:58) at com.cisco.ca.rms.upload.server.UlsServer.<init>(UlsServer.java:123) at com.cisco.ca.rms.upload.server.UlsServer.<init>(UlsServer.java:25) at com.cisco.ca.rms.upload.server.UlsServer$SingleInstanceHolder.<clinit> (UlsServer.java:70) at com.cisco.ca.rms.upload.server.UlsServer.getInstance(UlsServer.java:82) at com.cisco.ca.rms.upload.server.UlsServer.main(UlsServer.java:55) Caused by: org.jboss.netty.channel.ChannelException: Failed to bind to: /10.6.22.12:8080 at org.jboss.netty.bootstrap.ServerBootstrap.bind(ServerBootstrap.java:298) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer.<init> (UlsSouthBoundServer.java:109) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer.<init> (UlsSouthBoundServer.java:22) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer$SingleInstanceHolder.<clinit> (UlsSouthBoundServer.java:46) ... 6 more Caused by: java.net.BindException: Cannot assign requested address at sun.nio.ch.Net.bind0(Native Method) at sun.nio.ch.Net.bind(Unknown Source) at sun.nio.ch.Net.bind(Unknown Source) at sun.nio.ch.ServerSocketChannelImpl.bind(Unknown Source) at sun.nio.ch.ServerSocketAdaptor.bind(Unknown Source) at org.jboss.netty.channel.socket.nio.NioServerSocketPipelineSink.bind (NioServerSocketPipelineSink.java:140) at org.jboss.netty.channel.socket.nio.NioServerSocketPipelineSink.handleServerSocket (NioServerSocketPipelineSink.java:90) at org.jboss.netty.channel.socket.nio.NioServerSocketPipelineSink.eventSunk (NioServerSocketPipelineSink.java:64) at org.jboss.netty.channel.Channels.bind(Channels.java:569) at org.jboss.netty.channel.AbstractChannel.bind(AbstractChannel.java:189) at org.jboss.netty.bootstrap.ServerBootstrap$Binder.channelOpen(ServerBootstrap.java:343) at org.jboss.netty.channel.Channels.fireChannelOpen(Channels.java:170) at org.jboss.netty.channel.socket.nio.NioServerSocketChannel.<init> (NioServerSocketChannel.java:80) at org.jboss.netty.channel.socket.nio.NioServerSocketChannelFactory.newChannel (NioServerSocketChannelFactory.java:158) at org.jboss.netty.channel.socket.nio.NioServerSocketChannelFactory.newChannel (NioServerSocketChannelFactory.java:86) at org.jboss.netty.bootstrap.ServerBootstrap.bind(ServerBootstrap.java:277) ... 9 more
Cause	The server failed to bind to the IP /10.6.22.12:8080 because the requested address was unavailable.
Solution	Navigate to /opt/CSCOuls/conf and modify the UploadServer.properties file with proper SB and NB IP address.

Scenario 2:

Issue	Upload Server failed with java.lang.ExceptionInInitializerError java.lang.ExceptionInInitializerError at com.cisco.ca.rms.upload.server.security.UlsSbSslContextMgr.getInstance (UlsSbSslContextMgr.java:65) at com.cisco.ca.rms.upload.server.UlsSouthBoundPipelineFactory.<init> (UlsSouthBoundPipelineFactory.java:86) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer.<init> (UlsSouthBoundServer.java:102) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer.<init> (UlsSouthBoundServer.java:22) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer$SingleInstanceHolder.<clinit> (UlsSouthBoundServer.java:46) at com.cisco.ca.rms.upload.server.UlsSouthBoundServer.getInstance (UlsSouthBoundServer.java:58) at com.cisco.ca.rms.upload.server.UlsServer.<init>(UlsServer.java:123) at com.cisco.ca.rms.upload.server.UlsServer.<init>(UlsServer.java:25) at com.cisco.ca.rms.upload.server.UlsServer$SingleInstanceHolder.<clinit> (UlsServer.java:70) at com.cisco.ca.rms.upload.server.UlsServer.getInstance(UlsServer.java:82) at com.cisco.ca.rms.upload.server.UlsServer.main(UlsServer.java:55) Caused by: java.lang.IllegalStateException: java.io.IOException: Keystore was tampered with, or password was incorrect at com.cisco.ca.rms.commons.security.SslContextManager.<init> (SslContextManager.java:79) at com.cisco.ca.rms.upload.server.security.UlsSbSslContextMgr.<init> (UlsSbSslContextMgr.java:72) at com.cisco.ca.rms.upload.server.security.UlsSbSslContextMgr.<init> (UlsSbSslContextMgr.java:28) at com.cisco.ca.rms.upload.server.security.UlsSbSslContextMgr$SingleInstanceHolder.<clinit> (UlsSbSslContextMgr.java:53) ... 11 more Caused by: java.io.IOException: Keystore was tampered with, or password was incorrect at sun.security.provider.JavaKeyStore.engineLoad(Unknown Source) at sun.security.provider.JavaKeyStore$JKS.engineLoad(Unknown Source) at java.security.KeyStore.load(Unknown Source) at com.cisco.ca.rms.upload.server.security.UlsSbSslContextMgr.loadKeyManagers (UlsSbSslContextMgr.java:91) at com.cisco.ca.rms.commons.security.SslContextManager.<init>(SslContextManager.java:48) ... 14 more Caused by: java.security.UnrecoverableKeyException: Password verification failed ... 19 more
Cause	The Keystore was tampered with, or password entered is incorrect resulting in a password verification failure. This occurs when the password used to generate the Keystore file is different than the one given for the property “Upload_Keystore_Password” in descriptor file.

Solution	**1** Navigate to /opt/CSCOuls/conf and execute the below command to change the password of the Keystore file.
	`"[root@rtpfga-s1-upload1 conf]# keytool -storepasswd -keystore uls.keystore"`
	Output:
	`keytool -storepasswd -keystore dpe.keystore`
	`Enter keystore password:OLD PASSWORD`
	`New keystore password: NEW PASSWORD`
	`Re-enter new keystore password: NEW PASSWORD`
	Note The new Keystore password should be same as given in the descriptor file.
	2 Run another command before restarting the server to change the key password.
	`keytool -keypasswd -keystore dpe.keystore -alias dpe -key`
	`Enter keystore password: NEW AS PER LAST COMMAND`
	`Enter key password for <dpe-key> : OLD PASSWORD`
	`New key password for <dpe-key>: NEW PASSWORD`
	`Re-enter new key password for <dpe-key>: NEW PASSWORD`
	3 Restart the server process.
	`[root@rtpfga-s1-upload1 conf]# service god restart`
	`[root@rtpfga-s1-upload1 conf]# service god status`
	`UploadServer: up`

Scenario 3:

Issue	Upload Server failed with java.lang.ExceptionInInitializerError java.lang.ExceptionInInitializerError at com.cisco.ca.rms.dcc.lus.server.LusNorthBoundServer.getInstance (LusNorthBoundServer.java:65) at com.cisco.ca.rms.dcc.lus.server.LusServer.<init>(LusServer.java:98) at com.cisco.ca.rms.dcc.lus.server.LusServer.<init>(LusServer.java:17) at com.cisco.ca.rms.dcc.lus.server.LusServer$SingleInstanceHolder.<clinit> (LusServer.java:45) at com.cisco.ca.rms.dcc.lus.server.LusServer.getInstance(LusServer.java:57) at com.cisco.ca.rms.dcc.lus.server.LusServer.main(LusServer.java:30) Caused by: org.jboss.netty.channel.ChannelException: Failed to bind to: /0.0.0.0:8082 at org.jboss.netty.bootstrap.ServerBootstrap.bind(ServerBootstrap.java:298) at com.cisco.ca.rms.dcc.lus.server.LusNorthBoundServer.<init> (LusNorthBoundServer.java:120) at com.cisco.ca.rms.dcc.lus.server.LusNorthBoundServer.<init> (LusNorthBoundServer.java:30) at com.cisco.ca.rms.dcc.lus.server.LusNorthBoundServer$SingleInstanceHolder.<clinit> (LusNorthBoundServer.java:53) ... 6 more Caused by: java.net.BindException: Address already in use at sun.nio.ch.Net.bind(Native Method) at sun.nio.ch.ServerSocketChannelImpl.bind(ServerSocketChannelImpl.java:137) at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:77) at org.jboss.netty.channel.socket.nio.NioServerSocketPipelineSink.bind (NioServerSocketPipelineSink.java:140) at org.jboss.netty.channel.socket.nio.NioServerSocketPipelineSink.handleServerSocket (NioServerSocketPipelineSink.java:92) at org.jboss.netty.channel.socket.nio.NioServerSocketPipelineSink.eventSunk (NioServerSocketPipelineSink.java:66) at org.jboss.netty.channel.Channels.bind(Channels.java:462) at org.jboss.netty.channel.AbstractChannel.bind(AbstractChannel.java:186) at org.jboss.netty.bootstrap.ServerBootstrap$Binder.channelOpen (ServerBootstrap.java:343) at org.jboss.netty.channel.Channels.fireChannelOpen(Channels.java:170) at org.jboss.netty.channel.socket.nio.NioServerSocketChannel.<init> (NioServerSocketChannel.java:77) at org.jboss.netty.channel.socket.nio.NioServerSocketChannelFactory.newChannel (NioServerSocketChannelFactory.java:137) at org.jboss.netty.channel.socket.nio.NioServerSocketChannelFactory.newChannel (NioServerSocketChannelFactory.java:85) at org.jboss.netty.bootstrap.ServerBootstrap.bind(ServerBootstrap.java:277) ... 9 more
Cause	The server failed to bind to the IP /0.0.0.0:8082 because the requested address is already in use.

Solution	Execute the command:
	`netstat –anp |grep <port number>`
	For example:
	`[root@rtpfga-s1-upload1 conf]# netstat -anp |grep 8082`
	`tcp 0 0 10.6.23.16:8082 0.0.0.0:* LISTEN 26842/java`
	
	Kill the particular process.
	`[root@rtpfga-s1-upload1 conf]# kill -9 26842`
	Start the server.
	“`[root@rtpfga-s1-upload1 conf]# service god start`
	
	`[root@rtpfga-s1-upload1 conf]# service god status`
	`UploadServer: up`”

OVA Installation failures

Issue	If the OVA installer displays an error on the installation Console.
Cause	OVA Installation failures
Solution	If there are any issues during OVA installation, the **ova-first-boot.log** should be referred that is present in the Central node and Serving node. Validate the appropriate errors in the boot log files.

Update failures in group type, Site - DCC UI throws an error

Issue	SITE Creation Fails While Importing All Mandatory and Optional Parameters.
Cause	Invalid parameter value- FC-CSON-STATUS-HSCO-INNER with **Optimi*sed***.
Solution	For FC-CSON-STATUS-HSCO-INNER parameter, allowed value is **Optimi*zed*** not **Optimi*sed***. The spelling for Optimized should be corrected.

Kernel Panic While Upgrading to RMS, Release 5.1

To recover the system from kernel panic while upgrading, follow these steps

Note Follow this procedure only when the following error is seen:

```
Kernel panic-not syncing: VFS: unable to mount root fs on
unknown block(0,0)
```

Procedure

Step 1 Open the VM console when you encounter the kernel panic error.

Step 2 In the VM console, click on the **VM** option, then select **guest > Send ctrl+alt+del**.

Step 3 Wait for the "Booting Red Hat Enterprise Linux Server in X seconds..." countdown to begin and press any key to enter the menu.

Step 4 Select the kernel in the second line (older kernel) when the kernel list is displayed and press **Enter**. The selected older kernel will boot.

Step 5 In the login screen, provide the admin username/password. Then switch to root user using the root credentials.

Step 6 Navigate to the `/tmp` directory and copy the upgraded kernel rpm file in the system (that is, if upgrading to RHEL 6.6, the rpm file name will be **kernel-2.6.32-504.el6.x86_64.rpm**).

Step 7 Navigate to `/boot` directory and rename the latest **initrd-2.6.32-504.el6.x86_64.img** (assuming upgrading to RHEL 6.6) files to **2.6.32-504.el6.x86_64.img.old**.

Step 8 Verify the kernel rpm already installed on the system.

```
rpm –qa|grep kernel
```

The output of the above command will list the available kernel rpms in this system. Check that the latest kernel rpm is seen in this list (example, kernel-2.6.32-504.el6.x86_64).

Step 9 Remove the package (upgraded kernel) if the **kernel-2.6.32-504.el6.x86_64.rpm** is already installed (in case of RHEL 6.6) by using the following command.

```
rpm -e kernel-2.6.32-504.e16.x86_64
```

Step 10 Verify that the upgraded kernel is removed if it was already installed using the following command:

```
rpm -qa|grep kernel
```

Step 11 Navigate to the `/tmp` location and reinstall the latest rpm copied in Step 6 using the following command:

```
rpm -ivh -force kernel-2.6.32-504.e16.x86_64.rpm
```

Step 12 Navigate to the `/boot` location after reinstallation and verify if the **initrd-2.6.32-504.el6.x86_64.img** is copied.

Step 13 Verify if the `/boot/grub/grub.conf` points to the latest kernel ("default" should be zero if latest kernel is placed in the first place in the `grub.conf` file).

Step 14 Reboot the system. The system will now boot accurately.

Network Unreachable on Cloning RMS VM

When the network is unreachable on cloning RMS VM due to MAC address change, perform the following steps to resolve it.

Procedure

Step 1 Log in to vCenter.

Step 2 Open console of the affected VM.

Step 3 Reboot VM from "VM" > "guest " > "Send ctrl+alt+del ".

Step 4 Wait for the "Booting Red Hat Enterprise Linux Server in X seconds..." countdown to begin and press any key to enter the menu.

Step 5 Select the first kernel, that is, Red Hat Enterprise Linux Server (2.6. 32-504.e16 x86_64), when the kernel list is displayed and press the *e* key, once to edit the command before booting.

Step 6 Use the arrow key to select the second line starting with "kernel" in the next screen, and press the *e* key to edit the selected command in the boot sequence.

Step 7 Next, press the spacebar once and add number "1" and press **Enter**.
It will return to previous screen again where "kernel " line was selected.

Step 8 Press the *b* key, once to boot.
The system will boot in run level 1 and come to # prompt.

Step 9 Go to vCenter UI and click **VM > Edit Settings** to open the Virtual Machine Properties window.

Step 10 Note down both the network interface listed in the Hardware column and the "MAC address". The network adaptor1 is treated as eth0 by RHEL.

Step 11 Exit the Virtual Machine Properties window.

Step 12 Return to the VM console and edit the `/etc/udev/rules.d/70-persistent-net.rules` file.

Step 13 Comment the lines that are not matching with above-noted MAC address.

Step 14 Change the interface ID in the order noted in the VM > Edit Settings window (see, Step 10).

Step 15 Save the file and reboot the system.
After rebooting, the system will be available.

Unable to Stop UMT Jobs

The following two issues are seen that may prevent stopping of UMT jobs.

Issue 1:

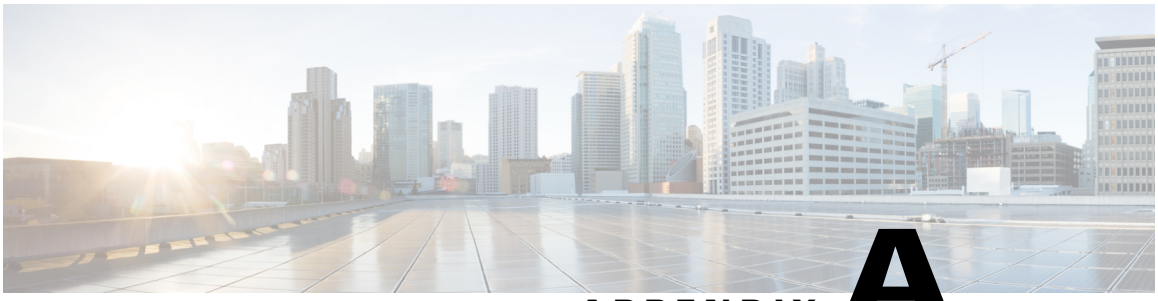
Issue	In DCC UI, stop monitoring of all running jobs. If the monitoring jobs do not stop due to some issue, log in to the postgress DB and follow the commands provided in the "Solution" row of this table.
Cause	The transaction ID has crossed the limit and the vacuum operation to clear the database fails. Any SQL operations on RMS (postgres) database fails and causes DCC UI log in to fail.

Solution	**1** Log in to the Central node as a root user.
	2 Log in to the postgres DB using the following command:
	`psql -U dcc_app -p <postgres port no> dcc`
	<postgres port no> is 5435 for 4.1 setup and 5439 for 5.1 setup.
	Note The password for DCC UI is the RMS_App_Password provided during installation.
	3 Check status of jobs in the umt_ga.job table using the following command
	`select * from umt_ga.job;`
	4 If any job state is other than 6 or 7, change the job state to 6 using the following SQL command:
	`update umt_ga.job set state=6,completetime=(extract('epoch' from CURRENT_TIMESTAMP)*1000::bigint),statetime=(extract('epoch' from CURRENT_TIMESTAMP)*1000::bigint) where state not in(6,7);`
	5 Check the umt_ga.job table to confirm that all jobs have moved to state 6 or 7 by using the following SQL command:
	`select * from umt_ga.job;`

Issue 2:

Issue	When checking logs (at `/rms/data/dcc_ui/postgres/dbbase/pg_log`), messages similar to "WARNING: skipping "user_role" --- only table or database owner can vacuum it" are seen.
Cause	The transaction ID has crossed the limit and the vacuum operation to clear the database fails. Any SQL operations on RMS (postgres) database fails and causes DCC UI login to fail.

Solution	**1** Log in to the Central node as a root user and run the following SQL command. When prompted for a password, enter the RMS_App_Password using the following SQL command:
	`SELECT age(datfrozenxid) FROM pg_database WHERE datname='dcc'" -d dcc -p <postgres port no> -U dcc_app`
	<postgres port no> is 5435 for 4.1 setup and 5439 for 5.1 setup.
	Note The password for DCC UI is the RMS_App_Password provided during installation.
	Sample Output:
	`[blrrms-central-01] /home/admin1 # psql -t -c "SELECT age(datfrozenxid) FROM pg_database WHERE datname='dcc'" -d dcc -p 5435 -U dcc_app`
	`Password for user dcc_app:`
	`199`
	If the resultant value is >=50 million or more, then vacuum the postgres DB as suggested in Step 2.
	2 Manually vacuum the postgres DB using the following command:
	`/usr/bin/vacuumdb -p <postgres port no>-U dcc_app -d dcc`
	<postgres port no> is 5435 for 4.1 setup and 5439 for 5.1 setup.
	Note The password for DCC UI is the RMS_App_Password provided during installation.



APPENDIX A

OVA Descriptor File Properties

All required and optional properties for the OVA descriptor file are described here.

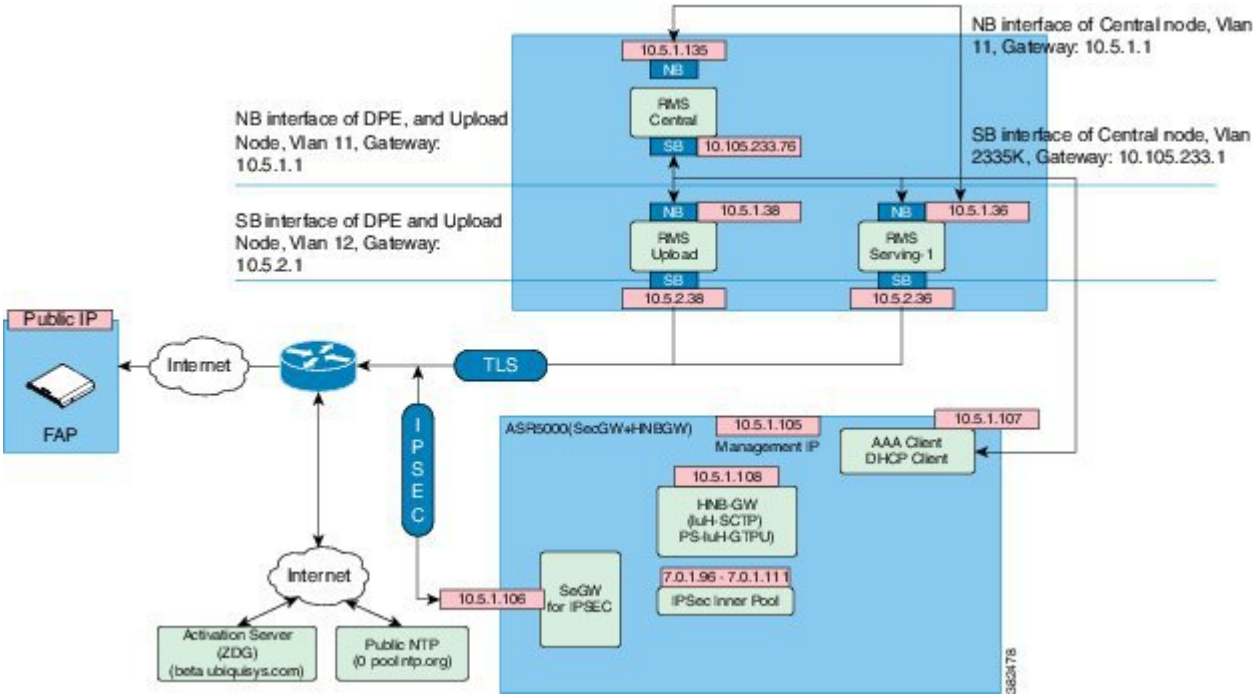
- RMS Network Architecture, page 255
- Virtual Host Network Parameters, page 256
- Virtual Host IP Address Parameters, page 258
- Virtual Machine Parameters, page 262
- HNB Gateway Parameters, page 263
- Auto-Configuration Server Parameters, page 265
- OSS Parameters, page 265
- Administrative User Parameters, page 268
- BAC Parameters, page 269
- Certificate Parameters, page 270
- Deployment Mode Parameters, page 271
- License Parameters, page 271
- Password Parameters, page 272
- Serving Node GUI Parameters, page 273
- DPE CLI Parameters, page 274
- Time Zone Parameter, page 274

RMS Network Architecture

The descriptor files are used to describe to the RMS system the network architecture being used so that all network entities can be accessed by the RMS. Before you create your descriptor files you must have on hand the IP addresses of the various nodes in the system, the VLAN numbers and all other information being configured in the descriptor files. Use this network architecture diagram as an example of a typical RMS installation. The examples in this document use the IP addresses defined in this architecture diagram. It might

be helpful to map out your RMS architecture in a similar manner and thereby easily replace the values in the descriptor example files provided here to be applicable to your installation.

Figure 13: Example RMS Architecture



Virtual Host Network Parameters

This section of the OVA descriptor file specifies the virtual host network architecture. Information must be provided regarding the VLANs for the ports on the central node, the serving node and the upload node. The virtual host network property contains the parameters described in this table.

Note VLAN numbers correspond to the network diagram in RMS Network Architecture, on page 255.

Name: Description	Values	Required	Example
Central-node Network 1 VLAN for the connection between the central node (southbound) and the upload node	VLAN #	In all-in-one deployment descriptor file In distributed central node descriptor file	`net:Central-Node Network 1=VLAN 11`

Name: Description	Values	Required	Example
Central-node Network 2 VLAN for the connection between the central node (northbound) and the serving node	VLAN #	In all-in-one deployment descriptor file In distributed central node descriptor file	`net:Central-Node Network 2=VLAN 2335K`
Serving-node Network 1 VLAN for the connection between the serving node (northbound) and the central node	VLAN #	In all-in-one deployment descriptor file In serving node descriptor file for distributed deployment	`net:Serving-Node Network 1=VLAN 11`
Serving-node Network 2 VLAN for the connection between the serving node (southbound) and the CPE network (FAPs)	VLAN #	In all-in-one deployment descriptor file In distributed serving node descriptor file	`net:Serving-Node Network 2=VLAN 12`
Upload-node Network 1 VLAN for the connection between the upload node (northbound) and the central node	VLAN #	In all-in-one deployment descriptor file In distributed upload node descriptor file	`net:Upload-Node Network 1=VLAN 11`
Upload-node Network 2 VLAN for the connection between the upload node (southbound) and the CPE network (FAPs)	VLAN #	In all-in-one deployment descriptor file In distributed upload node descriptor file	`net:Upload-Node Network 2=VLAN 12`

Virtual Host Network Example Configuration

Example of virtual host network section for all-in-one deployment:

```
net:Upload-Node Network 1=VLAN 11
net:Upload-Node Network 2=VLAN 12
net:Central-Node Network 1=VLAN 11
net:Central-Node Network 2=VLAN 2335K
net:Serving-Node Network 1=VLAN 11
net:Serving-Node Network 2=VLAN 12
```

Example of virtual host network section for distributed central node:

```
net:Central-Node Network 1=VLAN 11
net:Central-Node Network 2=VLAN 2335K
```

Example of virtual host network section for distributed upload node:

```
net:Upload-Node Network 1=VLAN 11
net:Upload-Node Network 2=VLAN 12
```

Example of virtual host network section for distributed serving node:

```
net:Serving-Node Network 1=VLAN 11
net:Serving-Node Network 2=VLAN 12
```

Virtual Host IP Address Parameters

This section of the OVA descriptor file specifies information regarding the virtual host. The Virtual Host IP Address property includes these parameters:



Note

- The **Required** column in the tables, **Yes** indicates Mandatory field, and **No** indicates Non-mandatory field.
- Underscore (_) cannot be used for the hostname for hostname parameters.

Hostname Parameters

Parameter Name: Description	Valid Values / Default	Required	Example
Central_Hostname Configured hostname of the server	Character string; no periods (.) allowed Default: rms-aio-central for all-in-one descriptor file, rms-distr-central for central node descriptor file	Yes	`prop:Central_Hostname=hostname-central`
Serving_Hostname Configured hostname of the serving node	Character string; no periods (.) allowed Default: rms-aio-serving for distributed all-in-one descriptor file, rms-distr-serving for distributed descriptor file	Required	`prop:Serving_Hostname=hostname-serving`
Upload_Hostname Configured hostname of the upload node	Character string; no periods (.) allowed Default: rms-aio-upload for all-in-one, rms-distr-upload for distributed	Required	`prop:Upload_Hostname=hostname-upload`

Central Node Parameters

Name: Description	Valid Values / Default	Required	Example
Central_Node_Eth0_Address IP address of the southbound VM interface	IP address	In all descriptor files	`prop:Central_Node_Eth0_Address=10.5.1.35`
Central_Node_Eth0_Subnet Network mask for the IP subnet of the southbound VM interface	Network mask	In all descriptor files	`prop:Central_Node_Eth0_Subnet=255.255.255.0`
Central_Node_Eth1_Address IP address of the northbound VM interface	IP address	In all descriptor files	`prop:Central_Node_Eth1_Address=10.105.233.76`
Central_Node_Eth1_Subnet Network mask for the IP subnet of the northbound VM interface	Network mask	In all descriptor files	`prop:Central_Node_Eth1_Subnet=255.255.255.0`
Central_Node_Gateway IP address of the gateway to the management network for the northbound interface of the central node	IP address	In all descriptor files	`prop:Central_Node_Gateway=10.105.233.1`
Central_Node_Dns1_Address IP address of primary DNS server provided by network administrator	IP address	In all descriptor files	`prop:Central_Node_Dns1_Address=72.163.128.140`
Central_Node_Dns2_Address IP address of secondary DNS server provided by network administrator	IP address	In all descriptor files	`prop:Central_Node_Dns2_Address=171.68.226.120`

Serving Node

Name: Description	Valid Values / Default	Required	Example
Serving_Node_Eth0_Address IP address of the northbound VM interface	IP address	In all descriptor files	`prop:Serving_Node_Eth0_Address=10.5.1.36`

Name: Description	Valid Values / Default	Required	Example
Serving_Node_Eth0_Subnet Network mask for the IP subnet of the northbound VM interface	Network mask	In all descriptor files	`prop:Serving_Node_Eth0_Subnet=255.255.255.0`
Serving_Node_Eth1_Address IP address of the southbound VM interface	IP address	In all descriptor files	`prop:Serving_Node_Eth1_Address=10.5.2.36`
Serving_Node_Eth1_Subnet Network mask for the IP subnet of the southbound VM interface	Network mask	In all descriptor files	`prop:Serving_Node_Eth1_Subnet=255.255.255.0`
Serving_Node_Gateway IP address of the gateway to the management network for the southbound interface of the serving node	IP address, can be specified in comma separated format in the form <NB GW>,<SB	In all descriptor files	`prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1`
Serving_Node_Dns1_Address IP address of primary DNS server provided by network administrator	IP address	In all descriptor files	`prop:Serving_Node_Dns1_Address=10.105.233.60`
Serving_Node_Dns2_Address IP address of secondary DNS server provided by network administrator	IP address	In all descriptor files	`prop:Serving_Node_Dns2_Address=72.163.128.140`

Upload Node

Name: Description	Valid Values / Default	Required	Example
Upload_Node_Eth0_Address IP address of the northbound VM interface	IP address	In all descriptor files	`prop:Upload_Node_Eth0_Address=10.5.1.38`
Upload_Node_Eth0_Subnet Network mask for the IP subnet of the northbound VM interface	Network mask	In all descriptor files	`prop:Upload_Node_Eth0_Subnet=255.255.255.0`

Name: Description	Valid Values / Default	Required	Example
Upload_Node_Eth1_Address IP address of the southbound VM interface	IP address	In all descriptor files	`prop:Upload_Node_Eth1_Address=10.5.2.38`
Upload_Node_Eth1_Subnet Network mask for the IP subnet of the southbound VM interface	Network mask	In all descriptor files	`prop:Upload_Node_Eth1_Subnet=255.255.255.0`
Upload_Node_Gateway IP address of the gateway to the management network for the southbound interface of the upload node	IP address, can be specified in comma separated format in the form <NB GW>,<SB GW>	In all descriptor files	`prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1`
Upload_Node_Dns1_Address IP address of primary DNS server provided by network administrator	IP address	In all descriptor files	`prop:Upload_Node_Dns1_Address=10.105.233.60`
Upload_Node_Dns2_Address IP address of secondary DNS server provided by network administrator	IP address	In all descriptor files	`prop:Upload_Node_Dns2_Address=72.163.128.140`

Virtual Host IP Address Examples

All-in-one Descriptor File Example:

```
prop:Central_Node_Eth0_Address=10.5.1.35
prop:Central_Node_Eth0_Subnet=255.255.255.0
prop:Central_Node_Eth1_Address=10.105.233.76
prop:Central_Node_Eth1_Subnet=255.255.255.128
prop:Central_Node_Dns1_Address=72.163.128.140
prop:Central_Node_Dns2_Address=171.68.226.120
prop:Central_Node_Gateway=10.105.233.1

prop:Serving_Node_Eth0_Address=10.5.1.36
prop:Serving_Node_Eth0_Subnet=255.255.255.0
prop:Serving_Node_Eth1_Address=10.5.2.36
prop:Serving_Node_Eth1_Subnet=255.255.255.0
prop:Serving_Node_Dns1_Address=10.105.233.60
prop:Serving_Node_Dns2_Address=72.163.128.140
prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1

prop:Upload_Node_Eth0_Address=10.5.1.38
prop:Upload_Node_Eth0_Subnet=255.255.255.0
prop:Upload_Node_Eth1_Address=10.5.2.38
prop:Upload_Node_Eth1_Subnet=255.255.255.0
```

```
prop:Upload_Node_Dns1_Address=10.105.233.60
prop:Upload_Node_Dns2_Address=72.163.128.140
prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1
```

Distributed Serving Node Descriptor File Example:

```
prop:Serving_Node_Eth0_Address=10.5.1.36
prop:Serving_Node_Eth0_Subnet=255.255.255.0
prop:Serving_Node_Eth1_Address=10.5.2.36
prop:Serving_Node_Eth1_Subnet=255.255.255.0
prop:Serving_Node_Dns1_Address=10.105.233.60
prop:Serving_Node_Dns2_Address=72.163.128.140
prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1
```

Distributed Upload Node Descriptor File Example:

```
prop:Upload_Node_Eth0_Address=10.5.1.38
prop:Upload_Node_Eth0_Subnet=255.255.255.0
prop:Upload_Node_Eth1_Address=10.5.2.38
prop:Upload_Node_Eth1_Subnet=255.255.255.0
prop:Upload_Node_Dns1_Address=10.105.233.60
prop:Upload_Node_Dns2_Address=72.163.128.140
prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1
```

Distributed Central Node Descriptor File Example:

```
prop:Central_Node_Eth0_Address=10.5.1.35
prop:Central_Node_Eth0_Subnet=255.255.255.0
prop:Central_Node_Eth1_Address=10.105.233.76
prop:Central_Node_Eth1_Subnet=255.255.255.128
prop:Central_Node_Dns1_Address=72.163.128.140
prop:Central_Node_Dns2_Address=171.68.226.120
prop:Central_Node_Gateway=10.105.233.1
```

Virtual Machine Parameters

The following virtual machine (VM) parameters can be configured.

Note Make sure that the value of the parameter powerOn is set to false as the VMware hardware version needs to be upgraded before starting the VMs.

Parameter Name: Description	Values	Required	Example
acceptAllEulas Specifies to accept license agreements	True/False Default: False	No	`acceptAllEulas=False`
skipManifestCheck Specifies to skip validation of the OVF package manifest	True/False Default: False	No	`skipManifestCheck=True`
powerOn Specifies to set the VM state for the first time once deployed	True/False Default: False	No	`powerOn=False`

Parameter Name: Description	Values	Required	Example
diskMode Logical disk type of the VM	thick/thin Default: thin Recommended: thin	Yes	`diskMode=thin`
vmFolder Grouping virtual machine to add additional security	folder name	Yes	`vmFolder=FEM-GA-PEST`
datastore Name of the physical storage to keep VM files	text	Yes	`datastore=ds-rtprms-c220-02`
name Name of the vApp that will be deployed on the host	text Default: VSC ovfid	Yes	`name=RMS-Provisioning-Solution`

VM Parameter Configurations Example

```
acceptAllEulas=True
skipManifestCheck=True
powerOn=False
diskMode=thin
vmFolder=FEM-GA-PEST
datastore=ds-rtprms-c220-02
name=RMS-Provisioning-Solution
```

HNB Gateway Parameters

These parameters can be configured for the Cisco ASR 5000 hardware that is running the central and serving nodes in all descriptor files. A post-installation script is provided to configure correct values for these parameters. For more information, refer to Configuring the HNB Gateway for Redundancy, on page 89.

- IPSec address
- HNB-GW address
- DHCP pool information
- SCTP address

Parameter Name: Description	Values	Required	Example
Asr5k_Dhcp_Address DHCP IP address of the ASR 5000	IP address	Yes, but can be configured with post-installation script	`prop:Asr5k_Dhcp_Address= 172.23.27.152`

Parameter Name: Description	Values	Required	Example
Asr5k_Radius_Address Radius IP address of the ASR 5000	IP address	Yes, but can be configured with post-installation script	`prop:Asr5k_Radius_Address= 172.23.27.152`
Asr5k_Radius_Secret Radius secret password as configured on the ASR 5000	text Default: secret	No	`prop:Asr5k_Radius_Secret= ***`
Dhcp_Pool_Network DHCP Pool network address of the ASR 5000	IP address	Yes, but can be configured with post-installation script	`prop:Dhcp_Pool_Network= 6.0.0.0`
Dhcp_Pool_Subnet Subnet mask of the DHCP Pool network of the ASR 5000	Network mask	Yes, but can be configured with post-installation script	`prop:Dhcp_Pool_Subnet= 255.255.255.0`
Dhcp_Pool_FirstAddress First IP address of the DHCP pool network of the ASR 5000	IP address	Yes, but can be configured with post-installation script	`prop:Dhcp_Pool_FirstAddress= 6.32.0.2`
Dhcp_Pool_LastAddress Last IP address of the DHCP pool network of the ASR 5000	IP address	Yes, but can be configured with post-installation script	`prop:Dhcp_Pool_LastAddress= 6.32.0.2`
Asr5k_Radius_CoA_Port Port for RADIUS Change-of-Authorization (with white list updates) and Disconnect flows from the PMG to the ASR 5000.	Port number Default: 3799	No	`prop:Asr5k_Radius_CoA_Port=3799`
Upload_SB_Fqdn Southbound fully qualified domain name or IP address for the upload node. For NAT based deployment, this can be set to public IP/FQDN of the NAT.	IP address Default: Upload eth1 address	Yes	`prop:Upload_SB_Fqdn= <Upload_Server_Hostname>`

HNB Gateway Configuration Example

```
prop:Asr5k_Dhcp_Address=10.5.4.152
```

```
prop:Asr5k_Radius_Address=10.5.4.152
prop:Asr5k_Radius_Secret=secret
prop:Dhcp_Pool_Network=7.0.2.192
prop:Dhcp_Pool_Subnet=255.255.255.240
prop:Dhcp_Pool_FirstAddress=7.0.2.193
prop:Dhcp_Pool_LastAddress=7.0.2.206
prop:Asr5k_Radius_CoA_Port=3799
```

Auto-Configuration Server Parameters

Configure the virtual Fully Qualified Domain Name (FQDN) on the Central node, Serving node, and the Upload node descriptors. The virtual FQDN is used as the Auto-Configuration Server (ACS) for TR-069 informs, download of firmware files, and upload of diagnostic files. The virtual FQDN should point to the Serving node Southbound address or Southbound FQDN.

The following parameters are used to configure the auto-configuration server information:

Parameter Name: Description	Values	Required	Example
Acs_Virtual_Fqdn ACS virtual fully qualified domain name (FQDN). Southbound FQDN or IP address of the serving node. For NAT based deployment, this can be set to public IP/FQDN of the NAT.	Domain name or IP address	In all descriptor files	`prop:Acs_Virtual_Fqdn= femtosetup11.testlab.com`

ACS Configuration Example

```
prop:Acs_Virtual_Fqdn=femtosetup11.testlab.com
```

OSS Parameters

Use these parameters to configure the integration points that are defined in the operation support systems (OSS). Only a few integration points must be configured, while others are optional. The optional integration points can be enabled or disabled using a Boolean flag.

NTP Servers

Use these parameters to configure the NTP server address defined for virtual hosts:

Note NTP servers can be configured after deploying the OVA files. Refer to NTP Servers Configuration , on page 163.

Parameter Name: Description	Values	Required	Example
Ntp1_Address Primary NTP server	IP address	No	`prop:Ntp1_Address= <ip address>`

Parameter Name: Description	Values	Required	Example
Ntp2_Address Secondary NTP server	IP address Default: 10.10.10.2	No	`prop:Ntp2_Address= <ip address>`
Ntp3_Address Alternative NTP server	IP address Default: 10.10.10.3	No	`prop:Ntp3_Address= <ip address>`
Ntp4_Address Alternative NTP server	IP address Default: 10.10.10.4	No	`prop:Ntp4_Address= <ip address>`

NTP Configuration Example

```
prop:Ntp1_Address=<ip address>
prop:Ntp2_Address=ntp-rtp2.cisco.com
prop:Ntp3_Address=ntp-rtp3.cisco.com
prop:Ntp4_Address=10.10.10.5
```

DNS Domain

Use these parameters to configure the DNS domain for virtual hosts:

Parameter Name: Description	Valid Values / Default	Required	Example
Dns_Domain Configures the domain address for virtual hosts	Domain address Default: cisco.com	No	`prop:Dns_Domain=cisco.com`

DNS Configuration Example

```
prop:Dns_Domain=cisco.com
```

Syslog Servers

Use these parameters to configure the two syslog servers defined for remote logging support:

Parameter Name: Description	Valid Values / Default	Required	Example
Syslog_Enable Enables or disables syslog	True/False Default: False	No	`prop:Syslog_Enable=True`

Parameter Name: Description	Valid Values / Default	Required	Example
Syslog1_Address Primary syslog server IP address	IP address of syslog server Default: 10.10.10.10	No	`prop:Syslog1_Address=10.0.0.1`
Syslog2_Address Secondary syslog server IP address	IP address of syslog server Default: 10.10.10.10	No	`prop:Syslog2_Address=10.0.0.2`



Note The syslog server configuration can be performed after the OVA file deployment. For more information, see the "Syslog Servers" sub-section in OSS Parameters, on page 265.

Syslog Configuration Example

```
prop:Syslog_Enable=True
prop:Syslog1_Address=10.0.0.1
prop:Syslog2_Address=10.0.0.2
```

TACACS

Use these parameters to configure the two TACACS servers defined for the centralized authentication support. Each of the applications that support TACACS is configured with these hosts and the TACACS secret.

Parameter Name: Description	Valid Values / Default	Required	Example
Tacacs_Enable Enables or disables use of TACACS(Terminal Access Controller Access-Control System) servers defined for the centralized authentication support	True/False; values other than True are treated as False Default: False	No	`prop:Tacacs_Enable=False`
Tacacs_Secret Tacacs secret password	text Default: tacacs-secret	No	`prop:Tacacs_Secret=***`
Tacacs1_Address IP address of primary Tacacs server	IP address Default: 10.10.10.10	No	`prop:Tacacs1_Address=10.0.0.1`

Parameter Name: Description	Valid Values / Default	Required	Example
Tacacs2_Address IP address of secondary Tacacs server	IP address Default: 10.10.10.10	No	`prop:Tacacs2_Address=10.0.0.2`

LDAP

Use these parameters to configure the two Lightweight Directory Access Protocol (LDAP) servers defined for the centralized authentication support. The system Operating System is configured with these LDAP servers and the Root domain name if the LDAP option is enabled.

Parameter Name: Description	Valid Values / Default	Required	Example
Ldap_Enable Enables or disables use of LDAP servers defined for the centralized authentication support.	True/False; values other than True are treated as False Default: False	No	`prop:Ldap_Enable=True`
Ldap_Root_DN LDAP root domain name	Domain name Default: root-dn	No	`prop:Ldap_Root_DN=root-dn`
Ldap1_Address IP address of primary LDAP server	IP address Default: 10.10.10.10	No	`prop:Ldap1_Address=10.0.0.1`
Ldap2_Address IP address of secondary LDAP server	IP address Default: 10.10.10.10	No	`prop:Ldap2_Address=10.0.0.2`

Administrative User Parameters

Use these parameters to define the RMS administrative user. Configuring the administrative user ensures that accounts are created for all the software components such as Broadband Access Center Database (BAC DB), Cisco Prime Network Registrar (PNR), Cisco Prime Access Registrar (PAR), and Secure Shell (SSH) system accounts. The user administration is an important security feature and ensures that management of the system is performed using non-root access.

One admin user is defined by default during installation. You can change the default with these parameters. Other users can be defined after installation using the DCC UI.

Note LINUX users can be added using the appropriate post-configuration script. Refer to Configuring Linux Administrative Users, on page 161.

Parameter Name: Description	Values	Required	Example
Admin1_Username System Admin user 1 login id	text Default: admin1	No	`prop:Admin1_Username=Admin1`
Admin1_Password System Admin user 1 password	Passwords must be mixed case, alphanumeric, 8-127 characters long and contain one of the special characters (*,@,#), at least one numeral and no spaces. Default: Ch@ngeme1	No	`prop:Admin1_Password=***`
Admin1_Firstname System Admin user 1 first name	text Default: admin1	No	`prop:Admin1_Firstname= Admin1_Firstname`
Admin1_Lastname System Admin user 1 last name	text Default: admin1	No	`prop:Admin1_Lastname= Admin1_Lastname`

BAC Parameters

These BAC parameters can be optionally configured in the descriptor file:

Parameter Name: Description	Values	Required	Example
Bac_Provisioning_Group Name of default provisioning group which gets created in the BAC **Note** The value of the Bac_Provisioning_Group name is shown only in lower case.	text Default: pg01	No	`prop:Bac_Provisioning_Group= default`
Ip_Timing_Server_Ip IP-TIMING-SERVER-IP property of the provisioning group specified in this descriptor. If there is no IP timing configured then provide a dummy IP address for this parameter, something like 10.10.10.5	IP address Default: 10.10.10.10	No	`prop:Ip_Timing_Server_Ip= 10.10.10.5`

Certificate Parameters

The CPE-based security for the RMS solution is a private key, certificate-based authentication system. Each Small Cell and server interface requires a unique signed certificate with the public DNS name and the defined IP address.

Parameter Name: Description	Values	Required	Example
System_Location System Location used in SNMP configuration	text Default: Production	No	`prop:System_Location= Production`
System_Contact System contact used in SNMP configuration	email address Default: Contact@Customer.com	No	`prop:System_Contact= Contact@Customer.com`
Cert_C Certificate parameters to generate a Certificate Signing Request (CSR): Country name	text Default: US	No	`prop:Cert_C=US`
Cert_ST Certificate parameters to generate csr: State or Province name	text Default: NC	No	`prop:Cert_ST= North Carolina`
Cert_L Certificate parameters to generate csr: Locality name	text Default: RTP	No	`prop:Cert_L=RTP`

Parameter Name: Description	Values	Required	Example
Cert_O Certificate parameters to generate csr: Organization name	text Default: Cisco Systems, Inc.	No	`prop:Cert_O= Cisco Systems, Inc.`
Cert_OU Certificate parameters to generate csr: Organization Unit name	text Default: MITG	No	`prop:Cert_OU= SCTG`

Deployment Mode Parameters

Use these parameters to specify deployment modes. Secure mode is set to True by default, and is a required setting for any production environment.

Parameter Name: Description	Values	Required	Example
Secure_Mode Ensures that all the security options are configured. The security options include IP Tables and secured "sshd" settings.	True/False Default: True	No	`prop:Secure_Mode=True`

License Parameters

Use these parameters to configure the license information for the Cisco BAC, Cisco Prime Access Registrar and Cisco Prime Network Registrar. Default or mock licenses are installed unless you specify these parameters with actual license values.

Parameter Name: Description	Valid Values / Default	Required	Example
Bac_License_Dpe: License for BAC DPE	text A default dummy license is provided	No	`prop:Bac_License_Dpe=AAfA...`
Bac_License_Cwmp: License for BAC CWMP	text A default dummy license is provided	No	`prop:Bac_License_Cwmp=AAfa...`

Parameter Name: Description	Valid Values / Default	Required	Example
Bac_License_Ext: License for BAC DPE extensions	text A default dummy license is provided	No	`prop:Bac_License_Ext=AAfa...`
Bac_License_FemtoExt: License for BAC DPE extensions **Note** License should be of PAR type and not SUB type	text A default dummy license is provided	No	`prop:Bac_License_FemtoExt=AAfa...`
Car_License_Base: License for Cisco PAR	text A default dummy license is provided	No	`prop:Bac_License_Cwmp=AAfa...`
Cnr_License_IPNode: License for Cisco PNR	text A default dummy license is provided	No	`prop:Bac_License_Cwmp=AAfa...`

Note For the PAR and PNR licenses, the descriptor properties Car_License_Base and Cnr_License_IPNode need to be updated in case of multi-line license file . (Put '/n' at the start of new line of the license file)

For example: `prop:Cnr_License_IPNode=INCREMENT count-dhcp cisco 8.1 uncounted VENDOR_STRING=<Count>10000</Count> HOSTID=ANY NOTICE="<LicFileID>20130715144658047</LicFileID><LicLineID>1</LicLineID> <PAK></PAK><CompanyName></CompanyName>" SIGN=176CCF90B694 \nINCREMENT base-dhcp cisco 8.1 uncounted VENDOR_STRING=<Count>1000</Count> HOSTID=ANY NOTICE="<LicFileID>20130715144658047</LicFileID><LicLineID>2</LicLineID> <PAK></PAK><CompanyName></CompanyName>" SIGN=0F10E6FC871E`

Password Parameters

The password for the root user to all virtual machines (VM) can be configured through the deployment descriptor. If this property is not set, the default root password is *Ch@ngeme1* . However, it is strongly recommended to set the Root_Password through the deployment descriptor file.

The RMS_App_Password configures access to all of the following applications with one password:

- BAC admin password
- DCC application

- Operations tools
- ciscorms user password
- DCC administration
- Postgres database
- Central keystore
- Upload statistics files
- Upload demand files
- Upload periodic files
- Upload unknown files

Parameter Name: Description	Values	Required	Example
Root_Password Password of the root user for all RMS VMs	text Default: Ch@ngeme1	No	`prop:Root_Password=***`
RMS_App_Password Password of the root user for all RMS VMs	Passwords must be mixed case, alphanumeric, 8-127 characters long and contain one of the special characters (*,@,#), at least one numeral and no spaces. Default: Rmsuser@1	No	`prop:RMS_App_Password=***`

Password Configuration Example

```
prop:Root_Password=cisco123
prop:RMS_App_Password=Newpswd#123
```

Serving Node GUI Parameters

The serving node GUI for Cisco PAR and Cisco PNR is disabled by default. You can enable it with this parameters.

Parameter Name: Description	Valid Values / Default	Required	Example
Serving_Gui_Enable: Option to enable/disable GUI of PAR and PNR	True/False; values other than "True" treated as "False." Default: False	No	`prop:Serving_Gui_Enable=False`

DPE CLI Parameters

The properties of the DPE command line interface (CLI) on the serving node can be configured through the deployment descriptor file with this parameter.

Parameter Name: Description	Values	Required	Example
Dpe_Cnrquery_Client_ Socket_Address Address and port of the CNR query client configured in the DPE	IP address followed by the port Default: serving eth0 addr:61611	No	`prop: Dpe_Cnrquery_Client_Socket_Address= 127.0.0.1:61611`

DPE CLI Configuration Example

```
prop:Dpe_Cnrquery_Client_Socket_Address=10.5.1.48:61611
```

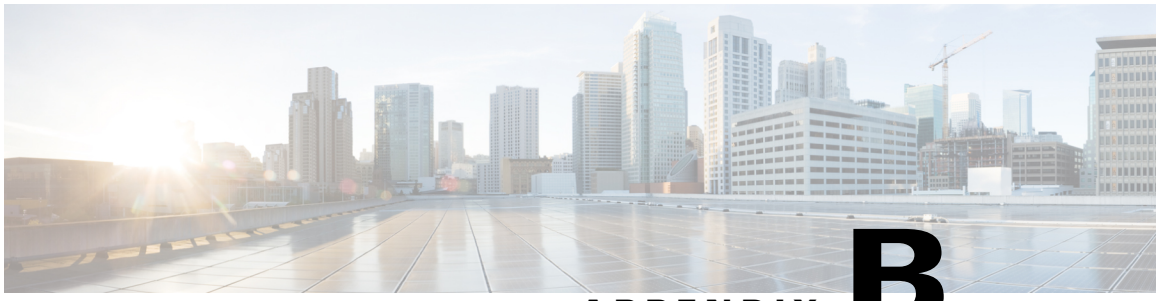
Time Zone Parameter

You can configure the time zone of the RMS installation with this parameter.

Parameter Name: Description	Values	Required	Example
prop:vamitimezone Default time zone	Default: Etc/UTC Supported values: • Pacific/Samoa • US/Hawaii • US/Alaska • US/Pacific • US/Mountain • US/Central • US/Eastern • America/Caracas • America/Argentina/Buenos_Aires • America/Recife • Etc/GMT-1 • Etc/UTC • Europe/London • Europe/Pari • Africa/Cairo • Europe/Moscow • Asia/Baku • Asia/Karachi • Asia/Calcutta • Asia/Dacca • Asia/Bangko • Asia/Hong_Kong • Asia/Tokyo • Australia/Sydney • Pacific/Noumea • Pacific/Fiji	No	`prop:vamitimezone=Etc/UTC`

Time Zone Configuration Example

```
prop:vamitimezone=Etc/UTC
```



APPENDIX B

Examples of OVA Descriptor Files

This appendix provides examples of descriptor files that you can copy and edit for your use. Use the "*.ovftool*" suffix for the file names and deploy them as described in Preparing the OVA Descriptor Files, on page 56.

- Example of Descriptor File for All-in-One Deployment, page 277
- Example Descriptor File for Distributed Central Node, page 279
- Example Descriptor File for Distributed Serving Node, page 280
- Example Descriptor File for Distributed Upload Node, page 282
- Example Descriptor File for Redundant Serving/Upload Node, page 283

Example of Descriptor File for All-in-One Deployment

```
#Logical disk type of the VM. Recommended to use thin instead of thick to conserve VM disk
 utilization
diskMode=thin

#Name of the physical storage to keep VM files
datastore=ds-blrrms-240b-02

#Name of the vApp that will be deployed on the host
name=BLR-RMS40-AIO

#VLAN for communication between central and serving/upload node
net:Central-Node Network 1=VLAN 11

#VLAN for communication between central-node and management network
net:Central-Node Network 2=VLAN 233

#IP address of the northbound VM interface
prop:Central_Node_Eth0_Address=10.5.1.55

#Network mask for the IP subnet of the northbound VM interface
prop:Central_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Central_Node_Eth1_Address=10.105.233.81

#Network mask for the IP subnet of the southbound VM interface
prop:Central_Node_Eth1_Subnet=255.255.255.128

#IP address of primary DNS server provided by network administrator
prop:Central_Node_Dns1_Address=64.102.6.247
```

```
#IP address of secondary DNS server provided by network administrator
prop:Central_Node_Dns2_Address=10.105.233.60

#IP address of the gateway to the management network
prop:Central_Node_Gateway=10.105.233.1

#VLAN for the connection between the serving node (northbound) and the central node
net:Serving-Node Network 1=VLAN 11

#VLAN for the connection between the serving node (southbound) and the CPE network (FAPs)
net:Serving-Node Network 2=VLAN 12

#IP address of the northbound VM interface
prop:Serving_Node_Eth0_Address=10.5.1.56

#Network mask for the IP subnet of the northbound VM interface
prop:Serving_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Serving_Node_Eth1_Address=10.5.2.56

#Network mask for the IP subnet of the southbound VM interface
prop:Serving_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Serving_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Serving_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of serving node
prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1

#VLAN for the connection between the upload node (northbound) and the central node
net:Upload-Node Network 1=VLAN 11

#VLAN for the connection between the upload node (southbound) and the CPE network (FAPs)
net:Upload-Node Network 2=VLAN 12

#IP address of the northbound VM interface
prop:Upload_Node_Eth0_Address=10.5.1.58

#Network mask for the IP subnet of the northbound VM interface
prop:Upload_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Upload_Node_Eth1_Address=10.5.2.58

#Network mask for the IP subnet of the southbound VM interface
prop:Upload_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Upload_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Upload_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of upload node
prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1

#Southbound fully qualified domain name or IP address for the upload node for setting
logupload URL on CPE
prop:Upload_SB_Fqdn=femtosetup11.testlab.com

#Primary RMS NTP server
prop:Ntp1_Address=10.105.233.60


#ACS virtual fully qualified domain name (FQDN). Southbound FQDN or IP address of the serving
 node.
prop:Acs_Virtual_Fqdn=femtosetup11.testlab.com
```

```
#Central VM hostname
prop:Central_Hostname=blrrms-central-22

#Serving VM hostname
prop:Serving_Hostname=blrrms-serving-22

#Upload VM hostname
prop:Upload_Hostname=blr-blrrms-lus-22
```

Example Descriptor File for Distributed Central Node

```
#Logical disk type of the VM. Recommended to use thin instead of thick to conserve VM disk
 utilization
diskMode=thin

#Name of the physical storage to keep VM files
datastore=ds-blrrms-240b-02

#Name of the vApp that will be deployed on the host
name=BLR-RMS40-CENTRAL

#VLAN for communication between central and serving/upload node
net:Central-Node Network 1=VLAN 11

#VLAN for communication between central-node and management network
net:Central-Node Network 2=VLAN 233

#IP address of the northbound VM interface
prop:Central_Node_Eth0_Address=10.5.1.55

#Network mask for the IP subnet of the northbound VM interface
prop:Central_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Central_Node_Eth1_Address=10.105.233.81

#Network mask for the IP subnet of the southbound VM interface
prop:Central_Node_Eth1_Subnet=255.255.255.128

#IP address of primary DNS server provided by network administrator
prop:Central_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Central_Node_Dns2_Address=10.105.233.60

#IP address of the gateway to the management network
prop:Central_Node_Gateway=10.105.233.1

#IP address of the northbound VM interface
prop:Serving_Node_Eth0_Address=10.5.1.56

#Network mask for the IP subnet of the northbound VM interface
prop:Serving_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Serving_Node_Eth1_Address=10.5.2.56

#Network mask for the IP subnet of the southbound VM interface
prop:Serving_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Serving_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Serving_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of serving node
```

```
prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1

#IP address of the northbound VM interface
prop:Upload_Node_Eth0_Address=10.5.1.58

#Network mask for the IP subnet of the northbound VM interface
prop:Upload_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Upload_Node_Eth1_Address=10.5.2.58

#Network mask for the IP subnet of the southbound VM interface
prop:Upload_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Upload_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Upload_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of upload node
prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1

#Southbound fully qualified domain name or IP address for the upload node for setting
logupload URL on CPE
prop:Upload_SB_Fqdn=femtosetup11.testlab.com

#Primary RMS NTP server
prop:Ntp1_Address=10.105.233.60


#ACS virtual fully qualified domain name (FQDN). Southbound FQDN or IP address of the serving
 node.
prop:Acs_Virtual_Fqdn=femtosetup11.testlab.com

#Central VM hostname
prop:Central_Hostname=blrrms-central-22

#Serving VM hostname
prop:Serving_Hostname=blrrms-serving-22

#Upload VM hostname
prop:Upload_Hostname=blr-blrrms-lus-22
```

Example Descriptor File for Distributed Serving Node

```
#Logical disk type of the VM. Recommended to use thin instead of thick to conserve VM disk
 utilization
diskMode=thin

#Name of the physical storage to keep VM files
datastore=ds-blrrms-240b-02

#Name of the vApp that will be deployed on the host
name=BLR-RMS40-SERVING

#IP address of the northbound VM interface
prop:Central_Node_Eth0_Address=10.5.1.55

#Network mask for the IP subnet of the northbound VM interface
prop:Central_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Central_Node_Eth1_Address=10.105.233.81

#Network mask for the IP subnet of the southbound VM interface
prop:Central_Node_Eth1_Subnet=255.255.255.128
```

```
#IP address of primary DNS server provided by network administrator
prop:Central_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Central_Node_Dns2_Address=10.105.233.60

#IP address of the gateway to the management network
prop:Central_Node_Gateway=10.105.233.1

#VLAN for the connection between the serving node (northbound) and the central node
net:Serving-Node Network 1=VLAN 11

#VLAN for the connection between the serving node (southbound) and the CPE network (FAPs)
net:Serving-Node Network 2=VLAN 12

#IP address of the northbound VM interface
prop:Serving_Node_Eth0_Address=10.5.1.56

#Network mask for the IP subnet of the northbound VM interface
prop:Serving_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Serving_Node_Eth1_Address=10.5.2.56

#Network mask for the IP subnet of the southbound VM interface
prop:Serving_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Serving_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Serving_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of serving node
prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1

#IP address of the northbound VM interface
prop:Upload_Node_Eth0_Address=10.5.1.58

#Network mask for the IP subnet of the northbound VM interface
prop:Upload_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Upload_Node_Eth1_Address=10.5.2.58

#Network mask for the IP subnet of the southbound VM interface
prop:Upload_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Upload_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Upload_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of upload node
prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1

#Southbound fully qualified domain name or IP address for the upload node for setting
logupload URL on CPE
prop:Upload_SB_Fqdn=femtosetup11.testlab.com

#Primary RMS NTP server
prop:Ntp1_Address=10.105.233.60



#ACS virtual fully qualified domain name (FQDN). Southbound FQDN or IP address of the serving
 node.
prop:Acs_Virtual_Fqdn=femtosetup11.testlab.com

#Central VM hostname
prop:Central_Hostname=blrrms-central-22
```

```
#Serving VM hostname
prop:Serving_Hostname=blrrms-serving-22

#Upload VM hostname
prop:Upload_Hostname=blr-blrrms-lus-22
```

Example Descriptor File for Distributed Upload Node

```
#Logical disk type of the VM. Recommended to use thin instead of thick to conserve VM disk
 utilization
diskMode=thin

#Name of the physical storage to keep VM files
datastore=ds-blrrms-240b-02

#Name of the vApp that will be deployed on the host
name=BLR-RMS40-UPLOAD

#IP address of the northbound VM interface
prop:Central_Node_Eth0_Address=10.5.1.55

#Network mask for the IP subnet of the northbound VM interface
prop:Central_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Central_Node_Eth1_Address=10.105.233.81

#Network mask for the IP subnet of the southbound VM interface
prop:Central_Node_Eth1_Subnet=255.255.255.128

#IP address of primary DNS server provided by network administrator
prop:Central_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Central_Node_Dns2_Address=10.105.233.60

#IP address of the gateway to the management network
prop:Central_Node_Gateway=10.105.233.1

#IP address of the northbound VM interface
prop:Serving_Node_Eth0_Address=10.5.1.56

#Network mask for the IP subnet of the northbound VM interface
prop:Serving_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Serving_Node_Eth1_Address=10.5.2.56

#Network mask for the IP subnet of the southbound VM interface
prop:Serving_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Serving_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Serving_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of serving node
prop:Serving_Node_Gateway=10.5.1.1,10.5.2.1

#VLAN for the connection between the upload node (northbound) and the central node
net:Upload-Node Network 1=VLAN 11

#VLAN for the connection between the upload node (southbound) and the CPE network (FAPs)
net:Upload-Node Network 2=VLAN 12

#IP address of the northbound VM interface
prop:Upload_Node_Eth0_Address=10.5.1.58
```

```
#Network mask for the IP subnet of the northbound VM interface
prop:Upload_Node_Eth0_Subnet=255.255.255.0

#IP address of the southbound VM interface
prop:Upload_Node_Eth1_Address=10.5.2.58

#Network mask for the IP subnet of the southbound VM interface
prop:Upload_Node_Eth1_Subnet=255.255.255.0

#IP address of primary DNS server provided by network administrator
prop:Upload_Node_Dns1_Address=64.102.6.247

#IP address of secondary DNS server provided by network administrator
prop:Upload_Node_Dns2_Address=10.105.233.60

#Comma separated northbound and southbound gateway of upload node
prop:Upload_Node_Gateway=10.5.1.1,10.5.2.1

#Southbound fully qualified domain name or IP address for the upload node for setting
logupload URL on CPE
prop:Upload_SB_Fqdn=femtosetup11.testlab.com

#Primary RMS NTP server
prop:Ntp1_Address=10.105.233.60


#ACS virtual fully qualified domain name (FQDN). Southbound FQDN or IP address of the serving
 node.
prop:Acs_Virtual_Fqdn=femtosetup11.testlab.com

#Central VM hostname
prop:Central_Hostname=blrrms-central-22

#Serving VM hostname
prop:Serving_Hostname=blrrms-serving-22

#Upload VM hostname
prop:Upload_Hostname=blr-blrrms-lus-22
```

Example Descriptor File for Redundant Serving/Upload Node

```
datastore=ds-blrrms-5108-01
name=blrrms-central06-harsh

net:Upload-Node Network 1=VLAN 11
net:Upload-Node Network 2=VLAN 12
net:Central-Node Network 1=VLAN 11
net:Central-Node Network 2=VLAN 2335K
net:Serving-Node Network 1=VLAN 11
net:Serving-Node Network 2=VLAN 12

prop:Central_Node_Eth0_Address=10.5.1.35
prop:Central_Node_Eth0_Subnet=255.255.255.0
prop:Central_Node_Eth1_Address=10.105.233.76
prop:Central_Node_Eth1_Subnet=255.255.255.128
prop:Central_Node_Dns1_Address=72.163.128.140
prop:Central_Node_Dns2_Address=171.68.226.120
prop:Central_Node_Gateway=10.105.233.1
prop:Serving_Node_Eth0_Address=10.5.1.36
prop:Serving_Node_Eth0_Subnet=255.255.255.0
prop:Serving_Node_Eth1_Address=10.5.2.36
prop:Serving_Node_Eth1_Subnet=255.255.255.0
prop:Serving_Node_Dns1_Address=10.105.233.60
prop:Serving_Node_Dns2_Address=72.163.128.140
prop:Serving_Node_Gateway=10.5.1.1
prop:Upload_Node_Eth0_Address=10.5.1.38
```

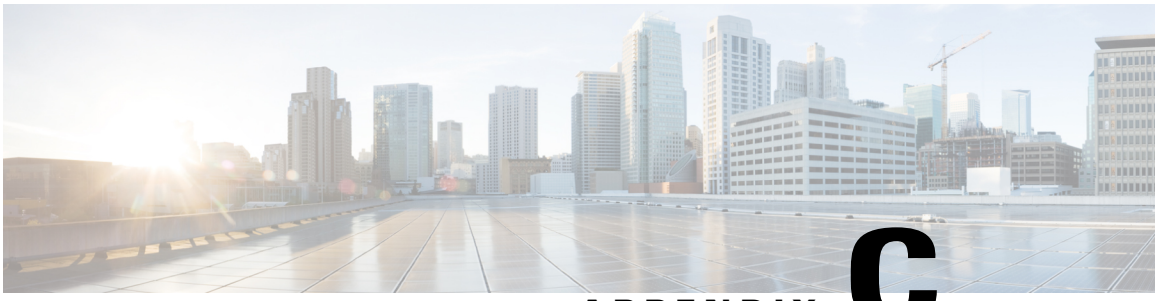
```
prop:Upload_Node_Eth0_Subnet=255.255.255.0
prop:Upload_Node_Eth1_Address=10.5.2.38
prop:Upload_Node_Eth1_Subnet=255.255.255.0
prop:Upload_Node_Dns1_Address=10.105.233.60
prop:Upload_Node_Dns2_Address=72.163.128.140
prop:Upload_Node_Gateway=10.5.1.1

prop:Central_Hostname=rms-distr-central
prop:Serving_Hostname=rms-distr-serving2
prop:Upload_Hostname=rms-distr-upload2

prop:Ntp1_Address=10.105.233.60


prop:Acs_Virtual_Fqdn=femtoacs.testlab.com

prop:Asr5k_Dhcp_Address=10.5.1.107
prop:Asr5k_Radius_Address=10.5.1.107
prop:Asr5k_Hnbgw_Address=10.5.1.107
prop:Dhcp_Pool_Network=7.0.1.96
prop:Dhcp_Pool_Subnet=255.255.255.240
prop:Dhcp_Pool_FirstAddress=7.0.1.96
prop:Dhcp_Pool_LastAddress=7.0.1.111
prop:Upload_SB_Fqdn=femtouls.testlab.com
```



APPENDIX C

Backing Up RMS

This chapter describes the backup procedure for the RMS system. There are two types of backups supported for RMS.

A full system backup of the VM is recommended before installing a new version of Cisco RMS so that if there is a failure while deploying the new version of Cisco RMS, the older version can be recovered.

Full System Backup: This type of backup can be performed using the VMware snapshot features. Sufficient storage space must exist in the local data store for each server to perform a full system backup. For more information on storage space, Virtualization Requirements, on page 14.

Full system backups should be deleted or transported to external storage for long-duration retention.

Application Data Backup: This type of backup can be performed using a set of "tar" and "gzip" commands. This document identifies important data directories and database backup commands. Sufficient storage space must exist within each virtual machine to perform an application data backup. For more information on storage space, see Virtualization Requirements, on page 14.

Performing an application data backup directly to external storage requires an external volume to be mounted within each local VM; this configuration is beyond the scope of this section.

Both types of backups can support Online mode and Offline mode operations:

- **Online mode** backups are taken without affecting application services and are recommended for hot system backups.
- **Offline mode** backups are recommended when performing major system updates. Application services or network interfaces must be disabled before performing Offline mode backups. Full system restore must always be performed in Offline mode.

The following sections describe the full system and application data backups.

- Full System Backup, page 285
- Application Data Backup, page 288

Full System Backup

Full system backups can be performed using the VMware vSphere client and managed by the VMware vCenter server.

With VMware, there are two options to have full system backup:

- VM Snapshot
  - VM snapshot preserves the state and data of a virtual machine at a specific point in time. It is not a full backup of VMs. It creates a disk file and keeps the current state data. If the full system is corrupted, it is not possible to restore.
  - Snapshots can be taken while VM is running.
  - Requires lesser disk space for storage than VM cloning.
- vApp/VM Cloning
  - It copies the whole vApp/VM.
  - While cloning, vApp needs to be powered off

    Note It is recommended to clone vApp instead of individual VMs

    .
  - Requires more disk space for storage than VM snapshots.

Back Up System Using VM Snapshot

Note If offline mode backup is required, disable network interfaces for each virtual machine. Create Snapshot using the VMware vSphere client.

Following are the steps to disable the network interfaces:

Procedure

Step 1 Login as 'root' user to the RMS node through the Vsphere Client console.

Step 2 Run the command: **#service network stop**.

Using VM Snapshot

Procedure

Step 1 Log in to vCenter using vSphere client.

Step 2 Right-click on the VM and click **Take Snapshot** from the Snapshot menu.

Step 3 Specify the name and description of the snapshot and click **OK**.

Step 4 Verify that the snapshot taken is displayed in the Snapshot Manager. To do this, right-click on the VM and select Snapshot Manager from Snapshot menu.

Back Up System Using vApp Cloning

Procedure

Step 1 Log in to the VM to be cloned and execute the following command as a root user:
```
mv /etc/udev/rules.d/70-persistent-net.rules /root
```

Step 2 Select the vApp of the VM to be cloned, right-click and in the Getting Started tab, click **Power off vApp**.

Note Steps 3 to 6 should be performed only on the Upload node if it has additional hard disks configured as mentioned in Upload VM, on page 17. If there are not additional hard disks configured on the Upload node, steps 3 to 6 can be skipped.

Step 3 After the power-off, right-click on the VM and click **Edit Settings**.

Step 4 Click on the additionally-configured hard disk (other than the default hard disk – Hard Disk 1) from the drop-down list. For example, Hard Disk 2. Repeat the steps for all the additionally configured hard disks. Exmaple, Hard Disk 3, Hard Disk 4, and so on.

Step 5 Make a note of the Disk File from the drop-down list.

Step 6 Close the drop-down and remove (click on the "X" symbol against each additionally added hard disk) the additional hard disks. Example, Hard Disk 2. Repeat the steps 5 and 6 on all the additionally-configured hard disks. For example, Hard Disk 3, Hard Disk 4 and so on. Click **Ok**. Note:

Note Do not check the checkbox because that would delete the files from the datastore, which cannot be recovered.

Step 7 Right-click on the vApp and select **All vCenter Actions** and click **Clone**. The New vApp Wizard is displayed.

Step 8 In the Select a creation type screen, select **Clone an existing vApp** and click **Next**.

Step 9 In Select a destination screen, select a host which has to be cloned and click **Next**.

Step 10 In Select a name and location screen, provide a name and target folder/datacenter for the clone and click **Next**.

Step 11 In Select storage screen, select the virtual disk format from the drop-down, which has the same format as the source and the destination datastore and click **Next**.

Step 12 Click **Next** in Map Networks, vApp properties, and Resource allocation screens.

Step 13 In the Ready to complete screen, click **Finish**.
The status of the clone is shown in the Recent Tasks section of the window.

Step 14 After the task is completed, to remount the additional hard disks in step r above, right-click on the cloned VM and select **Edit Settings**.

Step 15 Select the new device as **Existing Hard Disk** and click **Add**.

Step 16 In the Select File screen, select the disk file as noted before the clone in Step 5 and click **Ok**. Repeat this step for each additional hard disk seen in Step 4.

Step 17 Repeat the Steps 14 to 16 on the original VM.

Step 18 Select the vApp (either cloned or original) to be used and in the Getting Started tab, click **Power on vApp**.

Note Make sure Serving node and Upload node is powered on only after the Central node is completely up and running.

Application Data Backup

Application data backups are performed from the guest OS themselves. These backups will create compressed tar files containing required configuration files, database backups and other required files. The backups and restores are performed using **root** user.

Excluding Upload AP diagnostic files, a typical total size of all application configuration files would be 2-3 MB.

Upload AP diagnostic files backup size would vary depending on the size of AP diagnostic files.

The rdu/postgres db backup files would depend on the data and devices. A snapshot of backup files with 20 devices running has a total size of around 100 MB.

Perform the following procedure for each node to create an application data backup.



Note Copy all the backups created to the local PC or some other repository to store them.

Backup on the Central Node

Follow the below procedure to take backup of the RDU DB, postgres DB, and configuration files are on the Central node.

1 Log in to the Central node and switch to 'root' user.

2 Execute the backup script to create the backup file. This script prompts for following inputs:

- **new backup directory:** Provide a directory name with date included in the name to ensure that it is easy to identify the backup later when needed to restore. For example, CentralNodeBackup_March20.
- **PostgresDB password:** Provide the password as defined in the descriptor file for RMS_App_Password property during RMS installation. If RMS_App_Password property is not defined in the descriptor file, use the default password Rmsuser@1.

Enter:	`cd /rms/ova/scripts/redundancy;` `./backup_central_vm.sh`
Output:	

```
 [blrrms-central50-ucs240-ha] /rms/ova/scripts/redundancy #
./backup_central_vm.sh

Existing backup directories:

Enter name of new backup directory: CentralNodeBackup_March20

Enter password for postgresdb: Rmsuser@1

Doing backup of Central VM configuration files.
tar: Removing leading `/' from member names
-rw-------. 1 root root 181089 Mar 20 05:13
/rms/backups/CentralNodeBackup_March20//central-config.tar.gz
Completed backup of Central VM configuration files.
Doing backup of Central VM Postgress DB.
-rw-------. 1 root root 4305935 Mar 20 05:13
/rms/backups/CentralNodeBackup_March20//postgres_db_bkup
Completed backup of Central VM Postgress DB.
Doing backup of Central VM RDU Berklay DB.

Database backup started
Back up to:
/rms/backups/CentralNodeBackup_March20/rdu-db/rdu-backup-20150320-051308

Copying DB_VERSION.
DB_VERSION: 100% completed.
Copied DB_VERSION. Size: 394 bytes.

Copying rdu.db.
rdu.db: 1% completed.
rdu.db: 2% completed.
.
.
.
rdu.db: 100% completed.
Copied rdu.db. Size: 5364383744 bytes.

Copying log.0000321861.
log.0000321861: 100% completed.
Copied log.0000321861. Size: 10485760 bytes.

Copying history.log.
history.log: 100% completed.
Copied history.log. Size: 23590559 bytes.

Database backup completed



Database recovery started
Recovering in:
/rms/backups/CentralNodeBackup_March20/rdu-db/rdu-backup-20150320-051308
This process may take a few minutes.
Database recovery completed
rdu-db/
rdu-db/rdu-backup-20150320-051308/
rdu-db/rdu-backup-20150320-051308/DB_VERSION
rdu-db/rdu-backup-20150320-051308/log.0000321861
rdu-db/rdu-backup-20150320-051308/history.log
rdu-db/rdu-backup-20150320-051308/rdu.db
-rw-------. 1 root root 664582721 Mar 20 05:14
/rms/backups/CentralNodeBackup_March20//rdu-db.tar.gz
Completed backup of Central VM RDU Berklay DB.
CentralNodeBackup_March20/
CentralNodeBackup_March20/rdu-db.tar.gz
CentralNodeBackup_March20/postgres_db_bkup
CentralNodeBackup_March20/.rdufiles_backup
CentralNodeBackup_March20/central-config.tar.gz
-rwxrwxrwx. 1 root root 649192608 Mar 20 05:16
/rms/backups/CentralNodeBackup_March20.tar.gz
backup done.
[blrrms-central50-ucs240-ha] /rms/ova/scripts/redundancy #
```

3 Check for the backup file created in `/rms/backups/ directory`.

Enter:	**`ls -l /rms/backups`**

Output:	`[blrrms-central50-ucs240-ha] /rms/ova/scripts/redundancy # ls -l /rms/backups`
	`total 634604`
	`-rwxrwxrwx. 1 root root 649192608 Mar 20 05:16 CentralNodeBackup_March20.tar.gz`
	`[blrrms-central50-ucs240-ha] /rms/ova/scripts/redundancy #`

Backup on the Serving Node

Perform the following commands to create a backup of RMS component data on the Serving node.

1 **Back up Femtocell Firmware Files:**

Enter:	`cd /root`
	`mkdir -p /rms/backup`
	`tar cf /rms/backup/serving-firmware.tar /rms/data/CSCObac/dpe/files`
	`gzip /rms/backup/serving-firmware.tar`
	`ls /rms/backup/serving-firmware.tar.gz`

Output:	`[root@rtpfga-ova-serving06 ~]# cd /root` `[root@rtpfga-ova-serving06 ~]# mkdir -p /rms/backup` `[root@rtpfga-ova-serving06 ~]# tar cf /rms/backup/serving-firmware.tar` `    /rms/data/CSCObac/dpe/files` `tar: Removing leading `/' from member names` `[root@rtpfga-ova-serving06 ~]# gzip /rms/backup/serving-firmware.tar` `[root@rtpfga-ova-serving06 ~]# ls /rms/backup/serving-firmware.tar.gz`  `/rms/backup/serving-firmware.tar.gz` `[root@rtpfga-ova-serving06 ~]#`

2 **Back up Configuration Files:**

Enter:	cd /root mkdir -p /rms/backup tar cf /rms/backup/serving-config.tar /rms/app/CSCOar/conf /rms/app/nwreg2/local/conf /rms/app/CSCObac/dpe/conf /rms/app/CSCObac/car_ep/conf /rms/app/CSCObac/cnr_ep/conf /rms/app/CSCObac/snmp/conf/ /rms/app/CSCObac/agent/conf /rms/app/CSCObac/jre/lib/security/cacerts gzip /rms/backup/serving-config.tar ls /rms/backup/serving-config.tar.gz
Output:	[root@rtpfga-ova-serving06 ~]# cd /root [root@rtpfga-ova-serving06 ~]# mkdir -p /rms/backup [root@rtpfga-ova-serving06 ~]# tar cf /rms/backup/serving-config.tar /rms/app/CSCOar/conf /rms/app/nwreg2/local/conf /rms/app/CSCObac/dpe/conf /rms/app/CSCObac/car_ep/conf /rms/app/CSCObac/cnr_ep/conf /rms/app/CSCObac/snmp/conf/ /rms/app/CSCObac/agent/conf /rms/app/CSCObac/jre/lib/security/cacerts tar: Removing leading `/' from member names [root@rtpfga-ova-serving06 ~]# gzip /rms/backup/serving-config.tar [root@rtpfga-ova-serving06 ~]# ls /rms/backup/serving-config.tar.gz /rms/backup/serving-config.tar.gz [root@rtpfga-ova-serving06 ~]#

Backup on the Upload Node

Perform the following commands to create a backup of RMS component data on the Upload node.

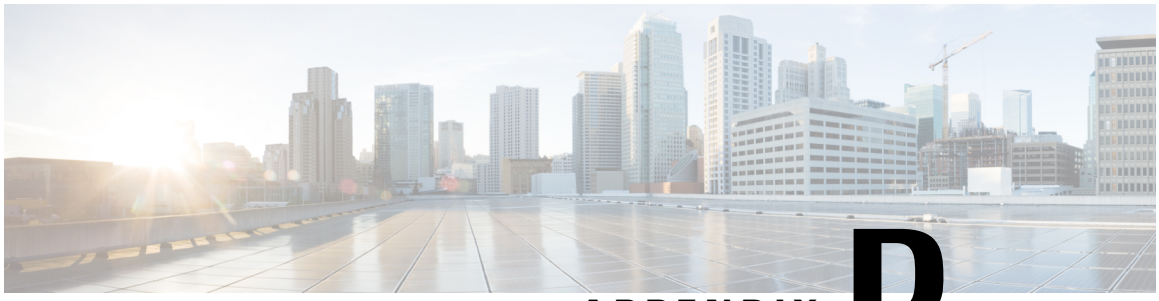
1 Back up Configuration Files:

Enter:	cd /root mkdir -p /rms/backup tar cf /rms/backup/upload-config.tar /opt/CSCOuls/conf gzip /rms/backup/upload-config.tar ls /rms/backup/upload-config.tar.gz
Output:	[root@rtpfga-ova-upload06 ~]# cd /root [root@rtpfga-ova-upload06 ~]# mkdir -p /rms/backup [root@rtpfga-ova-upload06 ~]# tar cf /rms/backup/upload-config.tar /opt/CSCOuls/conf tar: Removing leading `/' from member names [root@rtpfga-ova-upload06 ~]# gzip /rms/backup/upload-config.tar [root@rtpfga-ova-upload06 ~]# ls /rms/backup/upload-config.tar.gz /rms/backup/upload-config.tar.gz

2 Back up AP Files:

Enter:	`cd /root`
	`mkdir -p /rms/backup`
	`tar cf /rms/backup/upload-node-apfiles.tar /opt/CSCOuls/files`
	`gzip /rms/backup/upload-node-apfiles.tar`
	`ls /rms/backup/upload-node-apfiles.tar.gz`

Output:	`[root@rtpfga-ova-upload06 ~]# cd /root` `[root@rtpfga-ova-upload06 ~]# mkdir -p /rms/backup` `[root@rtpfga-ova-upload06 ~]# tar cf /rms/backup/upload-node-apfiles.tar /opt/CSCOuls/files` `tar: Removing leading `/' from member names` `[root@rtpfga-ova-upload06 ~]# gzip /rms/backup/upload-node-apfiles.tar` `[root@rtpfga-ova-upload06 ~]# ls /rms/backup/upload-node-apfiles.tar.gz` `/rms/backup/upload-node-apfiles.tar.gz`



APPENDIX D

RMS System Rollback

This section describes the Restore procedure for the RMS provisioning solution.

- Full System Restore, page 295
- Application Data Restore, page 296
- End-to-End Testing, page 304

Full System Restore

Restore from VM Snapshot

To perform a full system restore from VM snapshot, follow the steps:

1. Restore the Snapshot from the VMware data store.
2. Restart the virtual appliance.
3. Perform end-to-end testing.

To restore VM snapshot, follow the steps:

Procedure

Step 1 Right-click on the VM and select **Snapshot > Snapshot Manager**.

Step 2 Select the snapshot to restore and click **Go to**.

Step 3 Click **Yes** to confirm the restore.

Step 4 Verify that the Snapshot Manager shows the restored state of the VM.

Step 5 Perform end-to-end testing.

Restore from vApp Clone

To perform a full system restore from vApp clone, follow the steps:

Procedure

Step 1 Select the running vApp, right-click and click **Power Off**.

Step 2 Clone the backup vApp to restore, if required, by following steps mentioned in the Back Up System Using vApp Cloning, on page 287.

Step 3 Right-click on the vApp that is restored and click **Power on vApp** to perform end-to-end testing.

Application Data Restore

Place the backup of all the nodes at `/rms/backup` directory. Execute the restore steps for all the nodes as a root user.

Restore from Central Node

Execute the following procedure to restore a backup of the RMS component data on the Central Node. Take care to ensure the application data backup is being restored onto a system running the same version as it was created on.

Procedure

	Command or Action	Purpose
Step 1	Log in to the Central node and switch to 'root' user.	

Step 2	Create a restore directory in `/rms/backups` if it does not exist and copy the required backup file to the restore directory.
	
	Example:
	`mkdir –p /rms/backups/restore`
	`cp /rms/backups/CentralNodeBackup_March20.tar.gz /rms/backups/restore`	

Step 3	Run the script to restore the RDU database, postgres database, and configuration on the primary Central VM using the backup file. This script lists all the available backups in the restore directory and prompts for the following:	• **backup file to restore:** Provide one of the backup file • **PostgresDB password**: Provide the password as defi RMS_App_Password property during RMS installatio defined in the descriptor file, use the default password

	Command or Action	Purpose
		Enter: **cd /rms/ova/scripts/redundancy/;** **./restore_central_vm_from_bkup.sh** **Output:** [blrrms-central50-ucs240-ha] /rms/ova/scripts/ ./restore_central_vm_from_bkup.sh Existing backup files: CentralNodeBackup_March20.tar.gz CentralNodeBackup_March20_1.tar.gz Enter name of backup file to restore from: Cen Enter password for postgresdb: Rmsuser@1 CentralNodeBackup_March20/ CentralNodeBackup_March20/rdu-db.tar.gz CentralNodeBackup_March20/postgres_db_bkup CentralNodeBackup_March20/.rdufiles_backup CentralNodeBackup_March20/central-config.tar.g Stopping RDU service Encountered an error when stopping process [rd Encountered an error when stopping process [to ERROR: BAC Process Watchdog failed to exit aft BAC Process Watchdog has stopped. RDU service stopped Doing restore of Central VM RDU Berklay DB. / ~ rdu-db/ rdu-db/rdu-backup-20150320-051308/ rdu-db/rdu-backup-20150320-051308/DB_VERSION rdu-db/rdu-backup-20150320-051308/log.00003218 rdu-db/rdu-backup-20150320-051308/history.log rdu-db/rdu-backup-20150320-051308/rdu.db Restoring RDU database... Restoring from: /rms/backups/restore/temp/CentralNodeBackup_Ma Copying rdu.db. rdu.db: 1% completed. rdu.db: 2% completed. . . . Copied DB_VERSION. Size: 394 bytes. Database was successfully restored You can now start RDU server.

	Command or Action	Purpose
		~ Completed restore of Central VM RDU Berklay DB. Doing restore of Central VM Postgress DB. / ~ TRUNCATE TABLE SET SET . . . Completed restore of Central VM Postgress DB. Doing restore of Central VM configuration files. / ~ rms/app/CSCObac/rdu/conf/ rms/app/CSCObac/rdu/conf/cmhs_nba_client_logback. . . . rms/app/rms/conf/dcc.properties xuSrz6FQB9QSaiyB2GreKw== xuSrz6FQB9QSaiyB2GreKw== Taking care of special characters in passwords xuSrz6FQB9QSaiyB2GreKw== xuSrz6FQB9QSaiyB2GreKw== ~ Completed restore of Central VM configuration fil BAC Process Watchdog has started. Restore done. [blrrms-central50-ucs240-ha] /rms/ova/scripts/red
Step 4	Check the status of the RDU and tomcat process with the following command.	**Enter:** **/etc/init.d/bprAgent status** **Output:** [blrrms-central50-ucs240-ha] /rms/ova/scripts/redu BAC Process Watchdog is running. Process [snmpAgent] is running. Process [rdu] is running. Process [tomcat] is running. [blrrms-central50-ucs240-ha] /rms/ova/scripts/red
Step 5	Restart god service to restart PMGServer, AlarmHandler, and FMServer components with the following command.	**Enter:** **service god restart** **Output:** [blrrms-central50-ucs240-ha] /rms/ova/scripts/red Sending 'stop' command . The following watches were affected: PMGServer Sending 'stop' command The following watches were affected:

	Command or Action	Purpose
		AlarmHandler .. Stopped all watches Stopped god Sending 'load' command The following tasks were affected: PMGServer Sending 'load' command The following tasks were affected: AlarmHandler [blrrms-central50-ucs240-ha] /rms/ova/scripts/
Step 6	Check that PMGServer, AlarmHandler, and FMServer components are up with the below command.	**Enter:** **service god status** **Output:** [blrrms-central50-ucs240-ha] /rms/ova/scripts/ AlarmHandler: up FMServer: up PMGServer: up [blrrms-central50-ucs240-ha] /rms/ova/scripts/ **Note** It takes 10 to 15 minutes (based on the number bring-up its service completely.
Step 7	Check that 8083 port is listening and run the following command to confirm that the PMG service is up.	**Enter:** **netstat -an|grep 8083|grep LIST** **Output:** [blrrms-central50-ucs240-ha] /rms/ova/scripts/ LIST tcp 0 0 0.0.0.0:8083 [blrrms-central50-ucs240-ha] /rms/ova/scripts/

Restore from Serving Node

Procedure

Step 1 Stop Application Services:
Enter:

```
cd /root
service bprAgent stop
service nwreglocal stop
service arserver stop
```

Output:

```
[root@rtpfga-ova-serving06 ~]# service bprAgent stop
Encountered an error when stopping process [dpe].
Encountered an error when stopping process [cli].
ERROR: BAC Process Watchdog failed to exit after 90 seconds, killing processes.
BAC Process Watchdog has stopped.

[root@rtpfga-ova-serving06 ~]# service nwreglocal stop
# Stopping Network Registrar Local Server Agent
INFO: waiting for Network Registrar Local Server Agent to exit ...
[root@rtpfga-ova-serving06 ~]# service arserver stop
Waiting for these processes to die (this may take some time):
AR RADIUS server running       (pid: 4568)
AR Server Agent running        (pid: 4502)
AR MCD lock manager running    (pid: 4510)
AR MCD server running          (pid: 4507)
AR GUI running                 (pid: 4517)
4 processes left.3 processes left.1 process left.0 processes left
Access Registrar Server Agent shutdown complete.
```

Step 2 Restore Femtocell Firmware Files:

Enter:

```
cd /root
pushd /
tar xfvz /rms/backup/serving-firmware.tar.gz
popd
```

Output:

```
[root@rtpfga-ova-serving06 ~]# pushd /
/ ~
[root@rtpfga-ova-serving06 /]# tar xfvz /rms/backup/serving-firmware.tar.gz
rms/data/CSCObac/dpe/files/
[root@rtpfga-ova-serving06 /]# popd
~
```

Step 3 Restore Configuration Files:

Enter:

```
cd /root
pushd /
tar xfvz /rms/backup/serving-config.tar.gz
popd
```

Output:

```
[root@rtpfga-ova-serving06 ~]# pushd /
/ ~
[root@rtpfga-ova-serving06 /]# tar xfvz /rms/backup/serving-config.tar.gz
rms/app/CSCOar/conf/
rms/app/CSCOar/conf/tomcat.csr
rms/app/CSCOar/conf/diaconfig.server.xml
rms/app/CSCOar/conf/tomcat.keystore
rms/app/CSCOar/conf/diaconfiguration.dtd
rms/app/CSCOar/conf/arserver.orig
rms/app/CSCOar/conf/car.conf
rms/app/CSCOar/conf/diadictionary.xml
rms/app/CSCOar/conf/car.orig
rms/app/CSCOar/conf/mcdConfig.txt
rms/app/CSCOar/conf/mcdConfig.examples
rms/app/CSCOar/conf/mcdConfigSM.examples
```

```
rms/app/CSCOar/conf/openssl.cnf
rms/app/CSCOar/conf/diadictionary.dtd
rms/app/CSCOar/conf/release.batch.ver
rms/app/CSCOar/conf/add-on/
rms/app/nwreg2/local/conf/
rms/app/nwreg2/local/conf/cnrremove.tcl
rms/app/nwreg2/local/conf/webui.properties
rms/app/nwreg2/local/conf/tomcat.csr
rms/app/nwreg2/local/conf/localBasicPages.properties
rms/app/nwreg2/local/conf/tomcat.keystore
rms/app/nwreg2/local/conf/nwreglocal
rms/app/nwreg2/local/conf/userStrings.properties
rms/app/nwreg2/local/conf/nrcmd-listbrief-defaults.conf
rms/app/nwreg2/local/conf/tramp-cmtssrv-unix.txt
rms/app/nwreg2/local/conf/localCorePages.properties
rms/app/nwreg2/local/conf/regionalCorePages.properties
rms/app/nwreg2/local/conf/cnr_cert_config
rms/app/nwreg2/local/conf/product.licenses
rms/app/nwreg2/local/conf/dashboardhelp.properties
rms/app/nwreg2/local/conf/cmtssrv.properties
rms/app/nwreg2/local/conf/tramp-tomcat-unix.txt
rms/app/nwreg2/local/conf/cert/
rms/app/nwreg2/local/conf/cert/pubkey.pem
rms/app/nwreg2/local/conf/cert/cert.pem
rms/app/nwreg2/local/conf/cnr_status.orig
rms/app/nwreg2/local/conf/localSitePages.properties
rms/app/nwreg2/local/conf/regionalBasicPages.properties
rms/app/nwreg2/local/conf/manifest
rms/app/nwreg2/local/conf/cnr.conf
rms/app/nwreg2/local/conf/basicPages.conf
rms/app/nwreg2/local/conf/openssl.cnf
rms/app/nwreg2/local/conf/regionalSitePages.properties
rms/app/nwreg2/local/conf/priv/
rms/app/nwreg2/local/conf/priv/key.pem
rms/app/nwreg2/local/conf/genericPages.conf
rms/app/nwreg2/local/conf/aicservagt.orig
rms/app/CSCObac/dpe/conf/
rms/app/CSCObac/dpe/conf/self_signed/
rms/app/CSCObac/dpe/conf/self_signed/dpe.keystore
rms/app/CSCObac/dpe/conf/self_signed/dpe.csr
rms/app/CSCObac/dpe/conf/dpeextauth.jar
rms/app/CSCObac/dpe/conf/dpe.properties.29052014
rms/app/CSCObac/dpe/conf/AuthResponse.xsd
rms/app/CSCObac/dpe/conf/dpe.properties_May31_before_increasing_alarmQuesize_n_session_timeout
rms/app/CSCObac/dpe/conf/bak_dpe.properties
rms/app/CSCObac/dpe/conf/dpe-genericfemto.properties
rms/app/CSCObac/dpe/conf/dpe.keystore_changeme1
rms/app/CSCObac/dpe/conf/bak_orig_dpe.keystore
rms/app/CSCObac/dpe/conf/AuthRequest.xsd
rms/app/CSCObac/dpe/conf/dpe-femto.properties
rms/app/CSCObac/dpe/conf/dpe-TR196v1.parameters
rms/app/CSCObac/dpe/conf/dpe.properties
rms/app/CSCObac/dpe/conf/dpe.keystore
rms/app/CSCObac/dpe/conf/dpe.properties.bak.1405
rms/app/CSCObac/dpe/conf/bak_no_debug_dpe.properties
```

```
rms/app/CSCObac/dpe/conf/dpe.csr
rms/app/CSCObac/dpe/conf/dpe.properties.org
rms/app/CSCObac/dpe/conf/dpe-TR196v2.parameters
rms/app/CSCObac/dpe/conf/server-certs
rms/app/CSCObac/dpe/conf/Apr4_certs_check.pcap
rms/app/CSCObac/car_ep/conf/
rms/app/CSCObac/car_ep/conf/AuthResponse.xsd
rms/app/CSCObac/car_ep/conf/AuthRequest.xsd
rms/app/CSCObac/car_ep/conf/car_ep.properties
rms/app/CSCObac/car_ep/conf/server-certs
rms/app/CSCObac/cnr_ep/conf/
rms/app/CSCObac/cnr_ep/conf/cnr_ep.properties
rms/app/CSCObac/snmp/conf/
rms/app/CSCObac/snmp/conf/sys_group_table.properties
rms/app/CSCObac/snmp/conf/trap_forwarding_table.xml
rms/app/CSCObac/snmp/conf/proxy_table.xml
rms/app/CSCObac/snmp/conf/access_control_table.xml
rms/app/CSCObac/snmp/conf/sys_or_table.xml
rms/app/CSCObac/snmp/conf/agent_startup_conf.xml
rms/app/CSCObac/agent/conf/
rms/app/CSCObac/agent/conf/agent.ini
rms/app/CSCObac/agent/conf/agent.conf
rms/app/CSCObac/jre/lib/security/cacerts

[root@rtpfga-ova-serving06 /]# popd
~
[root@rtpfga-ova-serving06 ~]#
```

Step 4 Start Application Services:
Enter:

```
cd /root
service arserver start
service nwreglocal start
service bprAgent start
```

Output:

```
[root@rtpfga-ova-serving06 ~]# service arserver start
Starting Access Registrar Server Agent...completed.
[root@rtpfga-ova-serving06 ~]# service nwreglocal start
# Starting Network Registrar Local Server Agent
[root@rtpfga-ova-serving06 ~]# service bprAgent start
BAC Process Watchdog has started.
```

Restore from Upload Node

Perform the following commands to restore a backup of the RMS component data on the Upload node.

Procedure

Step 1 Stop Application Services:

Enter:

```
cd /root
service god stop
```

Output:

```
[[root@rtpfga-ova-upload06 ~]# service god stop
..
Stopped all watches
Stopped god
```

Step 2 Restore Configuration Files:

Enter:

```
cd /root
pushd /
tar xfvz /rms/backup/upload-config.tar.gz
popd
```

Output:

```
[root@rtpfga-ova-upload06 ~]# pushd /
/ ~
[root@rtpfga-ova-upload06 /]# tar xfvz /rms/backup/upload-config.tar.gz
opt/CSCOuls/conf/
opt/CSCOuls/conf/CISCO-SMI.my
opt/CSCOuls/conf/proofOfLife.txt
opt/CSCOuls/conf/post_config_logback.xml
opt/CSCOuls/conf/god.dist
opt/CSCOuls/conf/UploadServer.properties
opt/CSCOuls/conf/server_logback.xml
opt/CSCOuls/conf/CISCO-MHS-MIB.my
[root@rtpfga-ova-upload06 /]# popd
~
```

Step 3 Restore AP Files:

Enter:

```
cd /root
pushd /
tar xfvz /rms/backup/upload-node-apfiles.tar.gz
popd
```

Output:

```
[root@rtpfga-ova-upload06 ~]# pushd /
/ ~
[root@rtpfga-ova-upload06 /]# tar xfvz /rms/backup/upload-node-apfiles.tar.gz
opt/CSCOuls/files/
opt/CSCOuls/files/uploads/
opt/CSCOuls/files/uploads/lost-ipsec/
opt/CSCOuls/files/uploads/lost-gw-connection/
opt/CSCOuls/files/uploads/stat/
opt/CSCOuls/files/uploads/unexpected-restart/
opt/CSCOuls/files/uploads/unknown/
opt/CSCOuls/files/uploads/nwl-scan-complete/
opt/CSCOuls/files/uploads/on-call-drop/
opt/CSCOuls/files/uploads/on-periodic/
opt/CSCOuls/files/uploads/on-demand/
opt/CSCOuls/files/conf/
opt/CSCOuls/files/conf/index.html
opt/CSCOuls/files/archives/
opt/CSCOuls/files/archives/lost-ipsec/
opt/CSCOuls/files/archives/lost-gw-connection/
```

```
opt/CSCOuls/files/archives/stat/
opt/CSCOuls/files/archives/unexpected-restart/
opt/CSCOuls/files/archives/unknown/
opt/CSCOuls/files/archives/nwl-scan-complete/
opt/CSCOuls/files/archives/on-call-drop/
opt/CSCOuls/files/archives/on-periodic/
opt/CSCOuls/files/archives/on-demand/
[root@rtpfga-ova-upload06 /]# popd
~
[root@rtpfga-ova-upload06 ~]#
```

Step 4 Start Application Services:
Enter:

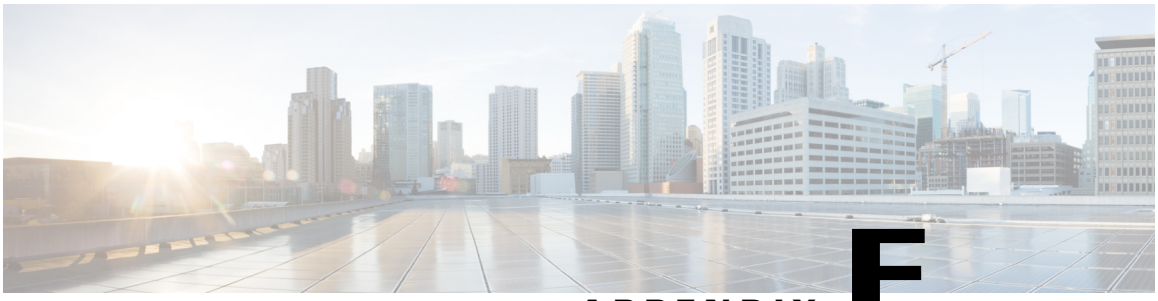
```
cd /root
service god start
sleep 30
service god status
```

Output:

```
[root@rtpfga-ova-upload06 ~]# cd /root
[root@rtpfga-ova-upload06 ~]# service god start
[root@rtpfga-ova-upload06 ~]# sleep 30
[root@rtpfga-ova-upload06 ~]# service god status
UploadServer: up
[root@rtpfga-ova-upload06 ~]#
```

End-to-End Testing

To perform end-to-end testing of the Small Cell device, see End-to-End Testing, on page 175:



APPENDIX E

Glossary

Term	Description
3G	Refers to the 3G or 4G cellular radio connection.
ACE	Application Control Engine.
ACS	Auto Configuration Server. Also refers to the BAC server.
ASR5K	Cisco Aggregation Service Router 5000 series.
BAC	Broadband Access Center. Serves as the Auto Configuration Server (ACS) in the Small Cell solution.
CPE	Customer Premises Equipment.
CR	Connection Request. Used by the ACS to establish a TR-069 session.
DVS	Distributed Virtual Switch.
DMZ	Demilitarized Zone.
DPE	Distributed Provisioning Engine.
DNS	Domain Name System.
DNM	Detected Neighbor MCC/MNC.
DNB	Detected Neighbor Benchmark.
ESXi	Elastic Sky X Integrated.
FQDN	Fully Qualified Domain Name.
HNB-GW	Home Node Base station Gateway also known as Femto Gateway.

INSEE	Institute for Statistics and Economic Studies.
LV	Location Verification.
LDAP	Lightweight Directory Access Protocol.
LAC	Location Area Code.
LUS	Log Upload Server.
NB	North Bound.
NTP	Network Time Protocol.
OSS	Operations Support Systems.
OVA	Open Virtual Application.
PAR	Cisco Prime Access Registrar (PAR).
PNR	Cisco Prime Network Registrar (PNR).
PMG	Provisioning and Management Gateway.
PMGDB	Provisioning and Management Gateway Data Base.
RMS	Cisco RAN Management System.
RDU	Regional Distribution Unit.
SAC	Service Area Code.
RNC	Radio Network Controller.
SIB	System Information Block.
TACACS	Terminal Access Controller Access-Control System.
SNMP	Simple Network Management Protocol.
USC	Ubiquisys Small Cell.
TLS	Transport Layer Security.
TR-069	Technical Report 069 is a Broadband Forum (standard organization formerly known as the DSL forum) technical specification entitled CPE WAN Management Protocol (CWMP).
UBI	Ubiquisys.
UCS	Unified Computing System.

VM	Virtual Machine.
XMPP	Extensible Messaging and Presence Protocol.