Release Notes for Cisco RAN Management System for Release 5.1

First Published: July 06, 2015

Introduction

The Cisco RAN Management System (RMS) provides end-to-end capabilities to support the management, monitoring, and configuration of Universal Small Cell Access Point (USC AP) devices. The RMS provides end-to-end operations to transmit high quality voice and data from the Service Provider mobility users through the Service Providers mobility core.

These release notes are for Release 5.1.0.

Abbreviations and Definitions

All abbreviations and definitions used in the document are provided here:

Table 1: Abbreviations and Definitions

Abbreviation	Description
BAC	Broadband Access Center: A Cisco TR-069 management product that includes RDU and DPE.
CIC	Chained Intra Chassis
CPE	Customer Premises Equipment
DCC UI	Device Command and Control User Interface
DPE	Distributed Provisioning Engine. A distributed server of the BAC product.
EID	Equipment Identifier
FRM	Femto RAN Manager
HNB	Home Node B
HeNB	Home eNodeB
HeNBGW	Home eNode B Gateway
HNBGW	Home Node B Gateway

Abbreviation	Description
LTE	Long Term Evolution
LUS	Log Upload Server
NWL	Network Listen
PAR	Cisco Prime Access Registrar
PNR	Cisco Prime Network Registrar
PMG	Provisioning and Management Gateway
QSS	Cisco Quantum SON Suite
RDU	Regional Distribution Unit, a part of the BAC that interfaces with the OSS north bound and DPE south bound and is the master data store.
REM	Radio Environment Measurement
RMS	RAN Management System
SMB	Small Mode Business
SON	Self Optimizing Network
SSL	Secure Socket Layer, an authentication and encryption protocol.
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).
UMTS	Universal Mobile Telecommunication System
USC AP	Universal Small Cell Access Point
Whitelist	Access control list which specifies which cell phones can register with the AP.

System Requirements

Component Versions

RMS Release 5.1 requires the following component versions:

Component	Version
Broadband Access Center (BAC)	3.10 (Build : 201506060402_199)
Cisco Prime Access Registrar (CPAR)	7.0.0 (Build : 1431469525)
Cisco Prime Network Registrar (CPNR)	8.3 (Build : 1)
BAC Tools	3.10.0.0 (Build : 27)
Baseline Configuration for BAC	5.1.0 (Build : 410)
Device Command and Control (DCC) UI	5.1.0 (Build : 478)
Operations Tools	5.1.0 (Build : 306)
OVA Installation Utilities	5.1.0 (Build : 317)
Provisioning Management Gateway (PMG)	5.1.0 (Build : 439)
Upload Server	9.3.0 (Build : 95)
Fault Manager Server	5.1.0 (Build : 164)

The PMG Database (DB) is an optional component. Contact Cisco Services to deploy the PMG DB.

Installation Image

The checksum values of the OVA files are provided in a text file together with the image download files, and as follows:

Table 2: Checksum of OVA Files

Filename	md5Sum Value
RMS-All-In-One-Solution-5.1.0-2I.tar.gz	e204ab4e17b66ef12d0bd4204a14e680
RMS-Distributed-Solution-5.1.0-2I.tar.gz	f28039d9ae802ab045cb8f28db3fb27f
RMS-Redundant-Solution-5.1.0-2I.tar.gz	772e20fa0f717b1caf89156d7edc3afb
RMS-PMGDB-5.1.0-2I.tar.gz	91a6bf96d5671c09f0adb5647a8c580b
RMS-UPGRADE-5.1.0-2I.tar.gz	224d8e7f234be5480fd5e65a066fbbda

Software Compatibility

RMS 5.1.0 is compatible with:

- USC AP versions:

Residential	BV 3.4.4.X, BV3.5.11.9 (and above), 3.5.12.X
Enterprise	BV 3.5.9.X, BV 3.5.10.X, BV3.5.11.9 (and above), 3.5.12.X
4G Enterprise USC 6732	DSV4.0.0T.X
3G Enterprise USC 6732	3.8.0T.X
LTE DM	2.2.26

- VMware vSphere, version 5.5.0
- ASR 5000 (FemtoGW, SeGW, and HeNBGW) version 17.0
- PPM version 1.6 SP1
- PC version 1.4.0.0
- RHEL 6.6

Key Notes

- The USC 6732 UMTS and LTE FAP is supported.
- By default no location verification (LV) methods are enabled on a fresh RMS 5.1 installation.
- Any LV methods enabled in RMS 4.1 are retained as part of the RMS4.1 to RMS 5.1 upgrade.
- After the RMS 4.1 to RMS 5.1 upgrade, all the LV related properties need to be removed from the various groups and should be configured from the region group level only.
- As part of the upgrade from RMS 4.1 to RMS 5.1 where INSEE is enabled, upgrade logs are displayed to the console.
- All the FAPs that are running software version 3.4.x should be rebooted as part of the upgrade from RMS 4.1 to RMS 5.1.
- The default LTE RFProfile is used for LTE FAPs.
- NTP synchronization is recommended from ESXi.
- Configuring external Syslogs post-OVA installation is not supported.
- The AP reachability alarm is not supported from RMS 5.1.
- UMT in DCC UI is not supported from RMS 5.1.

- By default it is recommended to set powerOn==False in all the descriptor files during a fresh RMS installation. Once the installation is complete, start the serving node once the central node is completely up.
- The INSEE SAC configuration script name changed from configure_func2.sh to configure_Insee_RF_AlarmsProfile.sh.
- RMS alarm integration has been qualified with Cisco Prime Central.

New and Changed Information

RMS 5.1.0 adds new features and enhancements to earlier RMS system releases. Following is a list of the new features of the RMS:

Table 3: RMS 5.1.0 New and Changed Information

Feature	Description
All-In-One Redundancy	Redundancy support for all-in-one RMS deployments.
Automatic DNL update	A detected neighbor location (DNL) file can be created and maintained in the RMS file system, and it can also be updated when required. This file is automatically imported as a generic configuration file to the RDU when any change needs to be implemented in the RMS within one hour after the change.
Bulk FAP registration	The bulkRegistrationTool.sh script within the Ops Tools is used to perform bulk registrations by sending register messages to the PMG. It supports concurrency, which enables several registered messages to be sent at once.
Multiple Cisco ASR 5000 configuration	New scripts configure_PAR_hnbgw.sh and configure_PNR_hnbgw.sh configure PAR and PNR in the Serving nodes. These scripts can be used to create multiple instances of scope/lease and Radius clients.
IP-based Location Verification (LV)	IP address of the AP (the public IP address which it uses to communicate with RMS) is used to verify that the location of the AP is within the expected distance.
Security Gateway (SecGW) Geographic Redundancy	A second redundant security gateway (Cisco ASR 5000 server) IP address can be configured for the connected HNBs using the RMS DCC-UI.
Overwrite Cell ID by RMS	Allows operator to specify the C-ID portion of the Cell ID assigned to a small cell.
Provisioning the USC 6732	Provisioning of both UMTS and LTE on the USC 6732 are supported.
Third Party Security Gateway	A third party SecGW can use a third party DHCP server or an internal DHCP server and does not use the PNR, which is the DHCP server provided by the RMS.

ISM Location Verification (LV) Optimization	Avoids the process of loading and parsing the ISM file each time the AP boots up, as well as the check by the ISM LV flow that the AP IP address falls under the subnet configured in the ISM file and then updating the RDU records accordingly. The cache mechanism provides the ISM LV optimization by parsing and caching (listing) the network IDs (types of Informs which trigger ISM LV), and caching the EID to IP address and subnet mapping.
BAC provisioning flow optimization	The main objective of the provisioning flow optimization is: • Avoid unwanted configuration synchronization • Avoid subsequent "gets" by the PMG This is achieved by: • Implementation of assignedDataNotification Event and GroupUpdated Event which can be enabled and disabled as required. • Addition of new attributes Cell ID, OTA Cell ID, Detected DNM List in all the events to avoid subsequent "gets" by the PMG
Security enhancements	RMS components have been implemented with security hardening according to the Cisco Security Development Lifecycle (CSDL) guidelines

Deployment

The only supported deployments for RMS release 5.1 are:

- All-in-one
- Distributed Redundant

Installation

The RMS provides an integrated installation process, which installs a pre-packaged set of software, such that you do not have to install each separate component.

Upgrade Paths

Upgrade support is provided for these paths only:

- RMS release 4.1.0-1N with Hotfix05 and above to RMS release 5.1.0 FCS
- RMS release 5.1.0 EFT to RMS release 5.1.0 FCS

Supported Hardware

- UCS 240

Workarounds for Known Problems – Post Installation

This section contains workarounds for known issues that might occur post installation.

CSCuu96911: Upgrade Error: Password lifetime is set for roles associated to system users

Workround:

1 Login to the Central Node and run the following command:

```
$psql -U dcc_app -p 5439 dcc
Password for user dcc_app:
psql (8.4.20)
Type ""help"" for help.
dcc=#
```

When prompted, input the dcc_app password.

2
```
dcc=# UPDATE role_names SET password_lifetime=0,
    password_warning_period=0, password_grace_period=0 WHERE rolename='superuser'
    OR rolename='pmgadmin' OR rolename='pmgreadonly';
```

3
```
dcc-# \q"
```

CSCuu96850: RMS51:AlarmHandler is not up after EFT to FCS upgrade

Workaround: Restart the AlarmHandler manually, using this command:

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

CSCuu93243: Updated ISM file content not used

Workaround: Restart the DPE or load the file again once the RDU-DPE link is restored. Use this command:

```
/etc/init.d/bprAgent restart dpe
```

CSCuu91794: configure_fm_server script needs to enable Snmptrap_Enable == True

Workaround: In the Central Node, execute the following command on the console

```
ovfenv -f /rms/ovf-env.xml -k Snmptrap_Enable -v True
```

CSCuu83273: Update User fails after the upgrade with XML validation error

Workaround: Retry the update.

CSCuu78502: After upgrade of RHEL 6.6 the console for all nodes is stuck

Workaround:

1 Login to the Vcenter.

2 Open the VM console.

3 Reboot the VM from “VM” == > “guest “ == > “Send ctrl+alt+del “

4 Wait for the Booting Red Hat Enterprise Linux Server in X seconds countdown to begin and then press any key.

5 Once the kernel list is displayed, select the first one and press “e” on your keyboard once.

6 Using the arrow key, select the second line starting with “kernel” and press “e” again.

7 Press the spacebar once and add number “1” and press Enter. It will return to the previous screen where the “kernel “ line was selected.

8 Press “b” on your keyboard on once.

9 System will boot in run level 1 and come to # prompt.

CSCuu71858: configursnmpserving node script overwrites CPAR SNMP configuration

Workaround: Edit the snmpd.conf file at /cisco-ar/ucd-snmp/share/snmp/snmpd.conf. Then restart CAR server.

```
service arserver stop
service arserver start
```

CSCut05537: Configure NTP post install script requires changes

Workaround: Modify the server details manually in /etc/ntp.conf and restart ntpd.

CSCuu98189: Upgrade Logs printing in console for INSEE enabled configurations

Workaround: No workaround. Logs will be printed to console during INSEE enabled configuration upgrade.

CSCuu83243: First time login to DCC UI after upgrade giving error

Workaround: Try logging in to the DCC UI again.

Caveats

This section only includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a particular bug you must use the Bug Search Tool.

Use the following link to access the tool: https://tools.cisco.com/bugsearch/search. You are prompted to log into www.cisco.com. After successful login, the Bug Search Tool page opens. Use the Help link in the Bug Search Tool to obtain detailed help.

Table 4: Open Caveats

Bug ID	Description
CSCut90396	SSL Version 2 and 3 Protocol Detection on Upload node
CSCut77579	APRIL 2015 NTPd Vulnerabilities
CSCuu82218	RHEL-6.6 Redhat Linux Patch level-Vulnerabilities

Bug ID	Description
CSCuu48368	Group-Usage Report and Maximum Number of Devices shows incorrect data
CSCuu28638	configure_fm_server script should support PC-DR integration
CSCuu91794	configure_fm_server script needs to enable Snmptrap_Enable == True
CSCuu74007	RMS Systemtime changes and NTP sync events are not logged by auditd
CSCuu98189	RMS5.1 Upgrade Logs printing in console for INSEE enabled configurations
CSCuu94167	[Upgrade] AP reboots post upgrade due to configuration template value change
CSCuv06728	PMG allows provisioning even after out of sync with RDU
CSCut59749	OVAdeployer_redundancy.sh script doesn't allow only hotstandbyDeployment
CSCup08895	RMS4.1 : Script for regenerating certificate for DPE
CSCuu54870	Audit Log Manipulation - Central Node
CSCuv03381	Post upgrade from RMS41-RMS51FCS GDDT has exception visible on console
CSCus10435	FM: PMG server terminated alarm's last occurrence time value NOT correct
CSCuv04372	RMS5.1_PeT_ReSync OpsTool result failure

Table 5: Closed Caveats

Bug ID	Description
CSCup68131	CSRF Token mismatch error on Cancel Export Group Task on DCC-UI
CSCur29179	RMS5.0_DCCUI Dashboard doesn't display livedata information
CSCur39710	RMS50 : searchAndExport.sh is not listing EIDs with selected CoS as arg
CSCur63528	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability
CSCus25941	Fap firmware file upload failed if file size is more than 35MB
CSCus28084	RMS50: PMG logs are not gzipped few times only moved as .tmp file
CSCus72781	RMS50: PMG is not responding for NB request(having deadlock in threadump)
CSCut79759	Subscriber ID with space can not be searched
CSCuu64883	RMS Sending Grid ID = O for APs registered as residential in RMS

Bug ID	Description
CSCus77514	RMS - INSEE code define and update for enterprise APs
CSCus72966	Multi-instance Live data not visible after parent parameter refresh

Related Documentation

- *Cisco RAN Management System Installation Guide*
- *Cisco RAN Management System Administration Guide*
- *Cisco RAN Management System SNMP/MIB Guide*
- *High Availability for Cisco RAN Management Systems*
- *Cisco RAN Management System API Guide*
- *RMS Configurable Parameters*
- *BAC Custom Properties*

Services and Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.