Radia Client Automation Enterprise

For the Windows® and Linux operating systems

Software Version: 9.00

Troubleshooting Guide

Document Release Date: April 2013

Software Release Date: June 2013

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written by Daniel Stenberg (daniel@haxx.se).

This product includes OVAL language maintained by The MITRE Corporation (oval@mitre.org).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://support.persistentsys.com/

This site requires that you register for a Persistent Passport and sign in. Register online at the above address.

For more details, contact your Persistent sales representative.

Support

Persistent Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-solve knowledge base, visit the Persistent Support home page.

Note: Most of the support areas require that you register as a Persistent Support user and sign in. Many also require an active support contract. More information about support access levels can be found on the Persistent Support site.

To register for a Persistent Support ID, go to: Persistent Support Registration.

Contents

Chapter 1

Troubleshooting Radia Client Automation

HP Client Automation Enterprise (RCA) Enterprise is a real-time, policy-based, desired state management client management solution that automates the administrative tasks for the physical and virtual clients in a highly complex and ever changing environments. The desired state approach ensures that all client devices in your infrastructure are in adherence with the state information stored for the device in a central database. To achieve the desired state, RCA enforces policies and delivers the required configurations or data files to the client device without any manual intervention.

Like any other enterprise application, you can experience problem in your RCA environment. These problems occur because of the complex behavior of the application, changing hardware and software demands, and infrastructure changes.

Before attempting to troubleshoot a specific problem, there are several things that you should consider:

- *What, specifically, is the problem?*
  Sometimes, one problem might have different causes. For example, if an RCA agent resolution does not complete due to time out, the time out could be based on either a Configuration server value or an RCA agent setting.
- *At what point did the problem occur?*
  If you can determine at what point a process failed, you might be able to eliminate prior steps.
- *Are there external causes for the problem?*
  You might be able to determine if a cause related or unrelated to RCA is responsible for the problem. For example, if your directory service is not working, you will not be able to create an entitlement for the target device.

Target Audience and Prerequisites

The target audience for this guide are RCA administrators who are responsible for maintaining the client devices in their enterprise environment. The use of this guide assumes some prerequisite knowledge. Administrators must have good understanding of various features and functions of RCA.

Administrators are expected to have read the following documents included with the product:

- *Radia Client Automation Enterprise Installation and Upgrade Guide*
- *Radia Client Automation Enterprise System Administrator Guide*
- *Radia Client Automation Enterprise Release Notes*

Contact Persistent Technical Support

RCA maintains a set of log files for each component. In an event of a failure, the error messages are recorded in these log files. You can use these log files for troubleshooting purposes in case you observer any issues with RCA. A few of these log files are in use while the RCA services are running.

It recommends that you do not delete these active log files. You can archive or delete the historical log files, if required.

You can contact Persistent Support to resolve your problem. To report a problem, go to the Persistent Support web site. Before contacting Persistent Support, make sure you have the log files generated on the Core server, Satellite servers, or Agent device based on the problem you have faced.

To download all the log files from the RCA Core Console, go to **Operations** > **Infrastructure Management** > **Support** and click **Download Current Server Log Files.**

To download all the log files from the RCA Satellite Console, go to **Operations** > **Support** and click **Download Current Server Log Files.**

Abbreviations and Variables

Abbreviations Used in this Guide

Abbreviation	Definition
RCA	Radia Client Automation
Core and Satellite	RCA Enterprise environment consisting of one Core server and one or more Satellite servers.
CSDB	Configuration Server Database

Variables Used in this Guide

Variable	Description	Default Values
InstallDir	Location where the RCA server is installed	For a 32-bit OS: `C:\Program Files\Hewlett-Packard\HPCA` For a 64-bit OS: `C:\Program Files(x86)\Hewlett-Packard\HPCA`
SystemDrive	Drive label for the drive where the RCA server is installed	C:

Chapter 2

Troubleshooting RCA Core Server

This chapter covers problems and possible solutions for components that are installed on the RCA Core server. Additionally, this chapter also provides the list of log files for each component.

HPCA log files are located in the following directories under *InstallDir* on the Core server:

- \Agent\Log
- \ApacheServer\logs
- \ApacheServer\apps\console\logs
- \BootServer\logs
- \ClientConfigurationManager\logs
- \ConfigurationServer\log
- \dcs\log
- \DistributedCS\logs
- \Knowledge Base Server\logs
- \ManagementPortal\logs
- \MessagingServer\logs
- \MiniManagementServer\logs
- \MobileServer\logs
- \MulticastServer\logs
- \OOBM\logs
- \OSManagerServer\logs
- \PatchManager\logs
- \PolicyServer\logs
- \ProxyServer\logs
- \ReportingServer\log
- \tomcat\logs
- \VulnerabilityServer\logs

Troubleshooting RCA Console

This section describes the cause and solutions for the problems that you may observe while using the RCA Console.

Log Files

RCA writes several logs that you can use to track the activities and functionality taking place on RCA Console and diagnose problems.

Console: Log Files

Log File	Description
`sessionmanager.log`	Contains log entries for role-based access control. Example, what all capabilities and permissions have been given to which users. The log file is available at <*Installdir*>\tomcat\logs You must enable the debug setting in the log4j.properties file located at <*Installdir*>\tomcat\webapps\sessionmanager\WEB-INF\classes.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Console.

RCA Console: Problems and solutions

Problem	Solution
The RCA Console is not refreshed when you press the **F5** function key.	To refresh the page that you are currently viewing, use the RCA Console built-in Refresh button on that web page.
The following message appears when you click VNC or Remote Assistance remote control features on the RCA Console: `Several Java Virtual Machines running in the same process caused an error`	This is a known problem in the Java browser plug-in. For more information, see the SUN web site at http://bugs.sun.com/view_bug.do?bug_id=6516270. To resolve this problem, upgrade the Java Runtime Environment (JRE) to JRE version 6 update 16 (or later).
The following error message is displayed in the dashboard pane: `Connection to RSS feed {`*URL for RSS feed*`} has failed. Make sure that the proxy server settings for RCA Enterprise Manager have been properly configured, you have subscribed to the RSS feed, and that the RSS feed is accessible.` When hovering the mouse over the **RSS query failed** message in the lower left corner of the dashboard pane, one of the following messages is displayed in a tool tip:	To resolve this problem, check the following aspects: 1. URL for the RSS feed is correct. Also, make sure that you have registered for the RSS feed, if required. To register for the feed, click the URL displayed in the error message. 2. Proxy settings for Internet-based communications using the RCA Console are configured correctly. 3. For the HP Live Network Announcements feed: a. HP Live Network credentials are specified correctly.

Problem	Solution
• `Error processing refresh: connection timed out: connect` • `Error processing refresh: Invalid Response: Login failed` • `Error processing refresh: Error on line -1: premature end of file`	b. HP Live Network subscription is current.

The following error message appears on the RCA Console when you start a virtual machine from the RCA Console:
`Result: "Start of Machine '<machine name>' failed"`
`Details: "Received Method Fault executing task haTask-##-vim.VirtualMachine.powerOn-#####: A general system error occurred: Internal error."`
	The licensing defect in ESX version 3.5 Update 2 (build number 103908) prevents the virtual machines from being started after a certain date.
	For more information on this issue, see the VMware Release Notes at:
	http://www.vmware.com/support/vi3//doc/vi3_esx35u2_vc25u2_rel_notes.html
	To resolve this problem, install ESX version 3.5 Update 2 build 110268, or the versions listed in the *Radia Client Automation Enterprise Support Matrix* available at the URL: http://h20230.www2.hp.com/sc/support_matrices.jsp.

The Most Vulnerable Products dashboard pane under Patch Management dashboard loads slowly.	This is the expected behavior. If there are a large number of managed devices in the enterprise, the Patch Management dashboard loads slowly. This pane is disabled by default. Disable the Most Vulnerable Products dashboard pane.
The dashboard panes are in perpetual loading state.	This problem occurs if one of the following products is installed on the RCA Core server: • Oracle ODBC Driver Version 10.2.0.1.0 • Microsoft SQL Server 2005 Service Pack 2 (2005.90.3042) To verify that this problem occurs because of the Oracle ODBC Driver Version 10.2.0.1.0 and Microsoft SQL Server 2005 Service Pack 2 installation, complete the following steps: 1. From the Control Panel, open the Event Viewer under Administrative Tools. 2. In the left navigation pane, select **System.**

Problem	Solution
	3. Look for events with Application Popup in the Source column. 4. If you see an event with the following description, the problem occurs due to the two product installations: `Application popup: nvdkit.exe - Application Error: …` To resolve this problem, do not install both these products on the RCA Core server.
In non-English environments, the reporting charts display question mark (??) characters for a few strings.	This problem occurs if the JAVA JRE client installed on the client computer does not contain the non-English fonts file. To resolve this problem, replace the `font.properties` file in the JDK home directory with non-English environment file. For example, if you have a Japanese environment, replace the file `font.properties` with the file `font.properties.ja`.
No data is displayed when the user logs in to SSL Configured RCA Core Console with IE9 browser and Adobe Flash Player 10 ActiveX.	To resolve this problem, follow these steps: 1. Open IE9 browser. 2. Click **Tools** - **Internet Options**. The Internet Options window opens. 3. Click **Advanced** tab. 4. Click **Security**. 5. Clear **Do not save encrypted pages to disk** option. 6. Click **OK**. 7. Restart the IE9 browser.

The following table provides the list of problems that may occur when accessing the RCA Core server or RCA Satellite server if they are installed on IPv6-enabled servers.

Accessing IPv6 RCA Severs: Problems and Solutions

Problem	Solution
When you access the Core server or the Satellite server over HTTPS using a literal IPv6 address, you receive a certificate warning in Internet Explorer.	If your host can't do a reverse-lookup in DNS for the address, then it can't validate the man-in-the-middle defense. This is because certificates are keyed on FQDN, not on IP addresses. The same holds true for any IP address, not just IPv6 ones.

Problem	Solution
You either receive the following error message or no response, when you log on to the Core server or the Satellite server from a remote browser: `Unknown login failure`	The following list provides the possible causes and solutions to this problem: • Cause: The web browser security settings do not allow accessing the IPv6 addresses. Solution: Add *http://[<IPv6 address>]:3466/*to your trusted site list. • Cause: The Internet Explorer 7 browser cookies are not refreshed. Solution: To resolve this problem, complete the following steps: a. Open Internet Explorer 7. b. Click **Tools** > **Internet Options** > **General Tab** > **Browsing History** > **Delete** > **Delete Cookies**. c. Refresh the web page and log on again.

After you have enabled IPv6, you receive one of the following errors when you log on to the Console using a web browser:
`Bad Connection`
`Network error: Connection refused`
	Make sure that you are connecting to the Core server using a web browser that support IPv6.
	In addition, check if you can connect to the Core server using telnet to the address and port 3466 or 3464.

The web browser connection to the Core or the Satellite server using an IPv6 address is slow as compared to the IPv4 address.	This problem occurs because of a DNS issue where the server hangs for a while when trying to identify the hostname of the caller.

Troubleshooting Configuration Server

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Configuration server.

Log Files

RCA writes several logs that can be used to track Configuration server process and to diagnose problems.

You can access the Configuration server log files from the location `<InstallDir>\ConfigurationServer\log`.

RCA Configuration Server: Log Files

Log File	Description
`nvdmgr100.log`	Contains log messages related to the Configuration server activity.

Log File	Description
	The number 100 in the log file name signifies that this file is for the Core server, whereas the number 200 signifies that this log file is for the Satellite server.
`nvdms100_yyyydd_n.log` In this instance, n is a positive integer. The log file is	Contains log messages related to the Configuration server activity when log switching functionality is enabled.
`nvdur100.log`	Contains log messages related to the Configuration server activity when the user logging functionality is enabled.
`radish.log`	Records log messages when the `Radish` method is invoked.
`upmgrid.log`	Records Configuration server related log messages when you install or upgrade RCA.
`zedmams.log`	Records the return codes and summary of the tasks performed when the `ZEDMAMS` utility is run. This log file is created at the location where the `ZEDMAMS` utility is run. By default, this log file is stored in the `<InstallDir>\ConfigurationServer\bin` directory.
`raddbutil.log`	Records the return codes and summary of the tasks performed when the `RadDBUtil` utility is run.
`raddbutil.audit.log`	Contains log messages related to `RadDBUtil` calls and the corresponding return codes. This log file is created for archival reference only.

CSDB synchronization log files

The log files for CSDB Synchronization are available at the source CSDB computer and the destination CSDB computer.

You can access the log files on source CSDB computer at the location `<InstallDir>/DistributedCS/logs`.

Distributed Configuration Server (source): Log Files

Log File	Description
`HPCA-DCS-port.log` where, port is the DCS port number	Contains log messages related to the tasks that the Distributed Configuration server (DCS) performs.

Log File	Description
`httpd-port.YY.MM.DD.log`	Contains log messages related to HTTP access requests to the DCS.
`httpd-port.error.log`	Contains a consolidated list of error messages. All log messages that are prefixed ERROR are written to this log file, enabling you to view all error messages at a single location.

You can access the log files on the destination computer at the location `<InstallDir>/dcs/log`.

Distributed Configuration Server (destination): Log Files

Log File	Description
`dmabatch.log`	Contains log messaged related to the CSDB synchronization. This log file is overwritten every time a synchronization process occurs.

Setting Trace Levels

Use the MGR_TRACE section in the `edmprof.dat` file contains to set the diagnostic logging for the Configuration server. All diagnostic output produced by TRACE settings is written to the Configuration server log file `nvdmr100.log`.

To activate a TRACE keyword, specify YES for the parameter you want to trace in the MGR_ TRACE section. To de-activate a TRACE keyword, specify NO.

The TRACE keywords specified in this section are invoked during Configuration server initialization, and remain in effect until modified using one of the following methods:

- Using the MGR_TRACE setting.
- Using a REXX method that overrides the current setting.
- Using a ZCVT value that overrides the current setting. For more information, see the *ZCVT and ZTCBG* section in the Radia Client Automation *Enterprise Configuration Server Reference Guide*.

The trace settings that are enabled during the Configuration server initialization are added at the beginning of the log file.

The value for each setting is evaluated in the order it is presented in the `edmprof.dat` file. For example,

- If `ALL=YES` is set as the first setting, and all other settings are specified as `NO`, the effect is to turn OFF tracing.
- If `ALL=YES` is set as the last setting, the effect is to turn ON all tracing.
- If `ALL=NO` is set as the last setting, the effect is to turn OFF all tracing.

MGR_TRACE Settings

Setting	Description
ADMIN	Traces ADMIN transaction flow.
ADMPROM	Not used.
ALL	Turns ON all other traces.
ALLOC	Traces file allocations.
AUDIT	Traces audit file activity.
BUFF	Traces data buffers (without transformation).
CMPR	Traces data compression.
COMM	Traces data stream buffers.
COMMCBS	Traces communications control block (CCB) activity.
COMMDATA	Traces data communications.
CONFIG	Traces configuration file activities.
DATA	Traces data buffers to or from the RCA agent.
DES	This setting is no longer used.
DMA	Traces Distributed Configuration server activity.
ENQDEQ	Traces serialization activity (enqueues/dequeues).
EXPL	Traces data transformation (explode).
FILE	Traces file I/O.
IMPL	Traces data transformation (implode).
LOOKASID	Traces cache activity for classes/instances.
METHOD	Traces Configuration server method execution/return codes.
NOTIFY	Traces notify processing.
OBJCRC	Traces object CRC processing.
OBJRES	Traces object resolution (very detailed).
OBJRES1	Traces object resolution (medium detail).
OBJRESO	Traces high-level object resolution flow (light detail).
OBJXFER	Traces object transfer.
PASSWORD	Traces passwords.

Setting	Description
POOLMISS	Traces memory pool allocation.
PROFILE	Traces profile database activity.
PROMOTE	Traces file promotion.
RESOURCE	Traces resource file activity.
REXX	Traces REXX environment.
REXXOFF	Suppresses all REXX activity.
STORAGE	Traces storage in conjunction with the MGR_LOG's STORAGE_INTERVAL setting.
STATS	Traces statistics.
SUBST	Traces variable substitution.
TCP	Traces TCP/IP activity.
TEST	Reserved.
VAR	Traces the variable references.
VARSTG	Traces variable processing storage usage.
VARSUB	Traces variable substitution activity.
YEAR2000	Traces a database's Year-2000 compliance.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Configuration server.

Configuration Server: Problems and solutions

Problem	Solution
The Configuration server does not start.	The following list provides the possible causes and solutions for this problem: • Cause: CSDB is not verified correctly. Solution: Reset the `VERIFY_DEPTH` setting in the Configuration Server `edmprof.dat` file. • Cause: Insufficient disk space. Solution: Free up sufficient disk space. • Cause: The `edmprof.dat` file is not processed. Solution: Make sure that the file `edmprof.dat` file and ZTOPTASK are in the same directory. • Cause: The Configuration server is installed under a non-

Problem	Solution
	administrator user account. Solution: Reinstall the Core server or Satellite server (as applicable) under a user account that is part of the Windows Administrator group.
The processor time required to load commonly used classes is high.	Add the required classes in MGR_CLASS section of the `edmprof.dat` file, such that the classes are cached during the initialization of the Configuration server.
The Configuration server methods do not run properly. The following error message is logged in the Configuration server log file: "TIMEOUT EXPIRED WAITING FOR TEMINATION OF METHOD xxx PID=xxx"	Analyze the method and increase the TIMEOUT setting in MGR_METHODS section of the `edmprof.dat` file. The default value set for TIMEOUT is 300 seconds.
Configuration server log file contains too many messages.	Set tracing to NO for unnecessary trace settings in the MGR_TRACE section.
The Configuration server log file is slow to respond.	Increase the FLUSH_SIZE in MGR_LOG section of the `edmprof.dat` file.
The Configuration server log file `nvdmgr100.log` does not provide the complete list of the Configuration server activity messages.	Change THRESHOLD setting in MGR_LOG section of the `edmprof.dat` file to a positive value.
The following error message is logged in the Configuration server log file `nvdmgr100.log`: `Initializing --- SOFT Task Limit Exceeded -- sending <retry in 5 min> response`	The number of concurrent agent connections that can happen with Configuration server is limited. Increase the value set for TSKLIMIT variable to increase the Soft Task Limit.
The following error message is logged in the Configuration server log file `nvdmgr100.log`:	The number of concurrent agent connections that can happen with Configuration server is limited. Increase the value set for TSKLIMIT variable to increase the Hard Task Limit.

Problem	Solution
`Initializing --- Hard Task Limit Exceeded -- closing connection`	
The following error message is logged in the Configuration server log file `nvdmgr100.log`: `Memory allocation failed for <xxxxxx> bytes (OBJECT ID TABLE)`	The error may occur while verifying a large database using the ZEDMAMS command with verb VERIFY_ DATABASE and DEPTH=RESOURCE, because of insufficient memory allocation. Verify that /3GB, /userva=2900, and /PAE switches are set in the `boot.ini` file. For more information on how to set these switches in `boot.ini` file, see the *Radia Client Automation Enterprise Enterprise Installation and Upgrade Guide*. Set the `OBJECTID_VERDB_INITIAL_ENTRIES` parameter in MGR_CACHE to approximately 1.2 times the total number of instances in the database.
The event log has error message: `START: Configuration Server CONTROL DISPATCHER FAILED.`	The Configuration server for Windows failed during service initialization and the start-up processing has stopped.
The event log has error message: `SET Configuration Server FAILED IN REPORT STATUS.`	An attempt was made to report the status of the Configuration server for Windows start-up process to the RCA Configuration Server service. However, the RCA Configuration Server service did not receive the status report. This could happen because the RCA Configuration Server service may actually be running, or the start-up service has stopped. The Configuration server is unable to discern what the actual condition is. Check that the RCA Configuration Server service is running.
The following error messages are logged in the `dmabatch.log` file when an administrator synchronizes the Satellite server CSDB with the Core server CSDB: `Skipping Domain [domain] because non-authoritative replica: updated (<date> <time>) since last synchronization (<date> <time>)`	This problem occurs if the Satellite server administrator manually imports the decks to the CSDB. When the decks are manually imported, the timestamp of the decks in the Satellite server differs from the decks in the Core server. To resolve this problem, review and delete the decks that are manually imported in the Satellite server. You must then re-synchronize the Satellite server CSDB with the Core server CSDB.

Problem	Solution
or `Skipping Domain [domain] because possible DB regression - destination replica (<date> <time) more recent than source (<date> <time>)`	

Troubleshooting Operating System Management

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA operating system management feature.

Log Files

RCA writes several logs on the server and the client side that you can use to track the OS Manager server process and diagnose problems.

OS Manager Server: Log Files

Log File	Description
`HPCA-OSM-`*`port`*`.log` where, *port* is the OS Manager port number.	Contains log messages related to the tasks that the OS Manager server performs, version number, and build number information for various internal OS Manager server components. RCA writes a new log file each time you start the OS Manager server. The previous log is renamed as `HPCA-OSM-port.`*`nn`*`.log`, where *nn* is a sequential number ranging from 0 through 99. The log files are purged after the higher limit for *nn* is reached. You can access this log file from the location *<InstallDir>*`\OSManagerServer\logs`.
`httpd-port.`*`yy.mm.dd`*`.log`	Contains httpd traffic-related log messages, specific to OS-manager only. The log file is created everyday, and if the log file is empty, no web server activity was performed on that day. You can access this log file from the location *<InstallDir>*`\OSManagerServer\logs`.
`machineID-all.log`	Records log messages after the OS Manager System Agent is run on the target device. A log file is created for each device managed by RCA OS Manager server. For better readability, it recommends that you open this file in WordPad. Note that if the machine instance has not been created for the target device, the log is created with the name `macAddress-all.log`.

Log File	Description
	You can access this log file from the location *<InstallDir>*\Data\OSManagerServer\upload. The log file also contains the version details for the OS Manager server boot loader. The details are logged as ROMBL_REV=<version details>.
osclone.log	Contains log messages related to the process osclone. The log file is temporarily created in the local directory from where the osclone process is run. When this process is complete, the file osclone.log is uploaded to the *<InstallDir>*\Data\OSManagerServer\upload directory on the RCA server as *imagename*.log, where *imagename* is the image name you provided during the capture.

OS Manager client logs

You can access the OS Manager agent log files from the location *<InstallDir>*\Agent\logs on the managed device.

OS Manager Client: Log Files

Log File	Description
connect.log	Contains log messages related to the RCA agent modules, RADSKMAN, RADPINIT, and RADCONCT.
Romclimth.log	Contains log messages related to the operating system service resolution.
LSB.log	Contains log messages related to LSB installation.

In addition to the agent logs, check the agent object information stored at the location *<InstallDir>*\Agent\LIB on the managed device to confirm that the following services have been installed successfully during the first agent connect:

- Operating system service
- OS Manager server agent files

Personality Backup and Restore logs

OS Manager Client: Log Files

Log File	Description
pbr.log	Contains log messages related to various processes that take place during Personality Backup and Restore operation. For example, if there is any success, failure, or error for the backup or restore process. You can access this log file from the location *<InstallDir>*\Agent\Log. If you are using the */localstore* option with pbr.exe, the log files are saved in the location *SystemDrive*\OSMGR.PRESERVE\PBR.work\log.
ScanState.log	Contains the details about user data and user settings when the backup process runs.

Log File	Description
	You can access this log file from the location `<InstallDir>\Agent\Lib\PBR\work\log` directory.
`LoadState.log`	Contains the details about user data and user settings when the restore process runs. You can access this log file from the location `<InstallDir>\Agent\Lib\PBR\work\log` directory.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA operating system management feature.

Operating system management: Problems and solutions

Problem	Solution

Either of the following error message appears during the capture or deploy process:
`Checking Machine Status Times Out`
or
`Cannot find ROMS infrastructure`
	The following list provides the possible causes and solutions for this problem:
	• Cause: The Portal is not responding. Solution: Check that the RCA Portal service is running. Additionally, verify the OS Manager server log to make sure that you are connected to the Portal.
	• Cause: The OS Manager server is not responding. Solution: Make sure that the `HPCA OS Manager` service is running.
	• Cause: Firewall is blocking the OSM ports. Solution: Make sure that the ports required for Core communications are configured. For more information on the port numbers that should be enabled, see the *HP Client Automation Enterprise Installation and Upgrade Guide*.

The following error messages are logged in the `machineID-all.log` file during image deployment:
`20120227 13:37:18 Info: rpsadr: CASSERVER:3467`
`20120227 13:37:18 Info: rpshost:`
	Check the DNS configuration to ensure that the hostnames or FQDNs are registered in the DNS. Based on the configurations set, a problem may be observed if short names are used. You must use the IP address or a fully qualified domain name.

Problem	Solution
CASSERVER 20120227 13:37:18 Info: rpsport: 3467 20120227 13:37:18 Error: GetState Error: couldn't open socket: host is unreachable 20120227 13:37:18 Error: Please check the Server configuration 20120227 13:37:18 Info: 20120227 13:37:18 Info: > sending AppEvent to http://CASSERVER:3461/proc/appeventxml 20120227 13:37:18 Info: 20120227 13:37:18 Error: Error sending AppEvent: couldn't open socket: host is unreachable 20120227 13:37:18 Error: InstallOSerr: Error(s) occurred during OS install, stopping 20120227 13:37:18 Error: This machine is in the process of having an OS installed. However, acritical aspect of the installation has failed. The machine will shut down until an administrator fixesthe problem and performs a Wake On LAN. Please contact your administrator. 20120227 13:37:18 Info: *** Start of Update Machine=======================*** Start of Update Machine ======================	
The device fails to boot into the Service OS from the ImageCapture or ImageDeploy media.	This problem is observed with a few non-HP devices. To resolve this problem, you must create a custom Service OS ISO for these devices. For more information, see “Building a Custom Windows PE Service OS” in the *Radia Client Automation Enterprise User Guide*. **Note:** When you run the script to build your custom Service OS ISO, make sure that you specify option 2 for the boot load segment setting (0x7c00).
When capturing an image, the capture process fails,	Increase the boot partition size to double

Problem	Solution

and the following error message appears on the reference machine:
`Capture Failed`
`Image preparation and capture failed:`
`1. Check the execution logs under:%Temp%/setup.`
`2. Consult the online help for further details.`
`Press OK to return to the OS capture wizard.`
The following error messages are logged in the `setup.log` file and `prepwiz.log` file at the location `%Temp%/setup`:
`There is not enough space on the boot volume so Prepwiz can inject the Local Service Boot files.`
`Required space: Z:MB, available space: 182MB.`
`Click OK to continue anyway or click cancel to stop the capture process.`
	the size of the `winpe.wim` file.

The TFTP server shuts down after starting.	Check Windows event log to see if another TFTP server is running on the same computer. Make sure that the port number used by the TFTP server (69) is not used by another application.
When publishing an OS image, the publishing process fails, and the following error message appears: `pub_file: File path <InstallDir>\Data\OSManagerServer\capture-conf\x86\substitutes specified does not exist.`	This error occurs when you try to publish an OS image that contains a corrupt or invalid `install.wim` file. Use an OS image that does not contain any corrupt files.
OS deployment to a Windows CE (thin client) device fails.	When you deploy an OS to a Windows CE device using Local Service Boot (LSB), there must be a minimum of 10 MB space available on the device to install and extract the LSB service. If the device reboots but fails to boot the Linux Service OS (SOS), the amount of storage memory that is allocated on the device is insufficient. Before you deploy the OS, complete these steps on the thin client device:

Problem	Solution
	1. Click **Start**. 2. Select **Settings** > **Control Panel**. 3. Click the **System** icon. 4. Select the **Memory** tab. 5. Use the slider on the left to increase the **Storage Memory** to 10 MB or more. **Note:**RCA does not support the operating system deployment through LSB on Windows CE-based HP thin client models t5550 and above.
You cannot reinstall an operating system on the target device if it contains an encrypted drive.	The following list provides the possible causes and solutions for this problem: • Cause: The target device does not contain any recognizable partition and the Encryption Support Mode parameter, ENCMODE, is set to the default value, AUTO, which means that supported encryption products are detected. Solution: Use the OS Deployment Wizard from the RCA Core Console to reinstall the operating system. • Cause: The target device does not contain any recognizable partition and the Encryption Support Mode parameter, ENCMODE, is set to ENC. Solution: Use the OS Deployment Wizard from the RCA Core Console to reinstall the operating system. • Cause: The target device contains a corrupted partition table and the Encryption Support Mode parameter, ENCMODE, is set to NONE. Solution: Set the disaster recovery behavior setting `PMDISRCV=_AUTO_` for the ZSERVICE using the CSDB Editor, and then start the operating system deployment.

When you are migrating the operating system for an agent device to another version, you might consider using the Personality Backup and Restore (PBR) feature with RCA to migrate the user files and settings. This section lists the causes and solutions for the problems related to this feature.

You can access the PBR log files, `pbr.log` on the agent computer from the location `<InstallDir>\Agent\Log`

Personality Backup and Restore: Problems and solutions

Problem	Solution
The user forgot the password and therefore, cannot restore the data.	To perform a restore using the Personality Backup and Restore Utility, the computer name and password that supplied during the backup are required. The user cannot recover a lost password, but as an administrator, you can create a new password to enable the user to perform a restore operation. Complete the following steps to create a new password: 1. Locate the backup directory on the RCA Core server that contains the user files and settings. You can find these files at the location `<InstallDir>\Data\PersonalityBackupAndRestore\backups`. The naming convention for the subdirectories is as follows: `ComputerNameEncodedComputerNameAndPassword` 2. Run the Personality Backup and Restore Utility on a computer other than computer for which the user has forgotten the password. To ensure a faster backup process, run this utility on a computer with less amount data. While creating the backup, enter the same computer name that was used for the original backup, and is part of the backup folder name. 3. Enter a password that will be given to the user to perform the restore. The new directory is created at the location at the location `<InstallDir>\Data\PersonalityBackupAndRestore\backups`. 4. Deletes the contents of the new subdirectory and copy the contents from the original user backup directory, as listed in step 1. 5. Provide the user with the new password, and instruct the user to use the old computer name with the new password to restore the files and settings. **Note:** If the end user forgets the password but data restore is not required, instruct the user to enter a new password the next time the backup is run, and use that password to perform a restore.

Information required by Persistent Support

Before contacting Persistent Support to resolve your problem, gather the following information about your current environment:

- Hardware information, including manufacturer, model number, BIOS or the firmware version for the NIC card, hard drive controller card, and hard drive.
- Provide the log files based on the OS provisioning phase that you are experiencing problems with:
  - Capture-related log files
    - `setup.log` and `prepwiz.log`, stored in the reference machine at the location `%TEMP%\setup`. These log files contains log messages related to the Image Preparation wizard.
    - `machineID-all.log` and `machineID_rnl.log`, stored in the OS Manager Server `upload` directory at the location *<InstallDir>*`\OSManagerServer\upload`.
  - Publish-related log files
    - `pubport.log`, stored in the Core server at the location *<InstallDir>*`\Agent\log`.
  - Deploy-related log files
    - `machineID-all.log` and `machineID_rnl.log`, stored in the OS Manager Server `upload` directory.
    - OS Manager Server logs *<InstallDir>*`\OSManagerServer\logs`
    - If you are using the LSB deploy method, , from the agent machine *<InstallDir>*`\log\lsb.log`, *<AGENT-INSTALL-DIR>*`\log\romclimth.log`, *<InstallDir>*`\log\pbr.log` (PBR log exists only if Personality Backup and Restore is used)
    - Portal logs stored at the location *<InstallDir>*`\ManagementPortal\Logs`
    - Configuration server logs, `radish.log` and `nvdmrnn.log`, stored at the location *<InstallDir>*`\ConfigurationServer\logs`.
    - If you observe that the deployment of an image has stopped and the bash prompt opens, collect the file `OSSELECT.log`.
      Run the following command from the target machine `/Work` directory to copy the file `OSSELECT.log` to the Integration Server `upload` folder:
      `curl -T osselect.log http://$ISVR:$ISVRPORT/upload/`

Troubleshooting Out-of-Band Management

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Out-of-Band Management feature.

Log Files

RCA creates the `stdout.log` file that you can use to track OOBM processes and diagnose OOBM problems. The `stdout.log` file is located at *<InstallDir>*`\tomcat\logs` and it contains all errors related to OOBM.

In addition, for agent-related problems such as problems in remote provisioning, you can view the details in Event Viewer on the vPro client devices.

To open the Event Viewer on a 32-bit system,

Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**.

To open the Event Viewer on a 64-bit system,

Click **Start > Control Panel > System and Security > Administrative Tools > Event Viewer**.

General Problems

Problem	Solution
RCA Console hangs when selecting vPro device type. This happens because the SCS Service failed to communicate with the Out of Band Management Service due to excessive CPU utilization (Tomcat is utilizing 100% of the CPU).	If the problem persists, reboot the RCA Tomcat server.
Error page shown in place of single device console, is not cleared. This is because the Internet Explorer browser cache is not cleared. Sometimes the error page that is shown in place of the single device console is not cleared till the Internet Explorer reopens.	Manually clear the cache of Internet Explorer.
Keyboard and power buttons are locked although they are not set to locked in the RCA Console. This locking depends on the version of the BIOS running on the vPro device. Some versions, by default, lock the power button and keyboard.	On some devices, the BIOS settings are user configurable. See the device documentation for BIOS versions that are configurable.
You cannot connect to vPro device using the wired NIC due to following possible causes: 1. The vPro device has been removed from the network. 2. The web services for the vPro device are busy.	In these cases, select the devices of interest and refresh the RCA Console screen by using the Refresh from Repository icon after a time lag of several seconds so that the RCA Console web service requests can be fetched again from the vPro device.
There is wrong alert subscription status on OOBM device management screen. This issue is due to third-party dependencies of OOBM. When RCA is installed on Windows Server 2008, the alert subscription operation, though successful, is incorrectly reported in the status column. This will cause a problem when the user is performing the alert subscription operation on vPro device by selecting **Operations** > **Out Of Band Management** > **Device Management** > **Alert Subscription**.	There is no workaround for this problem.
Accessing OOBM Device Details window after long idle period on RCA Console causes you to exit to login screen. This is due to database access related issue.	Close the browser and re-login to RCA Console in a new browser session.
You are not able to save SCS properties when managing vPro	You must provide the

Problem	Solution
devices in device type selection window. For SCS login, the User Name was not specified in the domainName\userName format. This format is now required and authenticated. In earlier releases of OOBM, the domainName part of the login name was ignored. As a result, even if you provided the wrong domainName, it appeared to be accepted. Also, in earlier OOBM releases, the example given for the User Name login (provisionserver.yourenterprise.com\Administrator) was incorrect but worked because the domain name was ignored by OOBM.	User Name login in the correct domainName\userName format in order to save SCS properties.
You are not able to access DASH device after changing DASH credentials because the previous credentials are cached causing the erroneous behavior.	If you have changed the DASH device credentials, you must restart the Tomcat service to make them effective.
Synchronizing vPro devices with SCS repository is taking long time because several web services calls are made to determine the list of available vPro devices. This may take several minutes depending on how many systems are not available or on current network routing issues.	You can improve performance by reducing the web service timeout value. However, reducing the timeout value may cause some available machines to be missed or other operations (such as power or deployment) to be not completed.
You are not able to access the correct vPro device because of IP address conflict problem, that is more than one vPro device may have the same IP address.	IP addresses must be distinct. Contact the Network Administrator to resolve this problem.
Text is not displayed correctly by HyperTerminal during SOL operations because wrap lines that exceed terminal width option may be enabled in HyperTerminal.	Open **HyperTerminal**. Go to **File Properties**. Select the **Settings** Tab. Click **ASCII Setup**. In the ASCII Setup window, uncheck the Wrap lines that exceed terminal width option.
Deployment of software list to OOB devices throws network error 26 in TLS mode because the client certificate is not properly configured on Radia Client Automation install machine. Deployment of the software list to OOB devices causes the network error of 26 to be thrown in TLS mode. This will cause a problem when the user is	Install the client certificate on Radia Client Automation installed machine and specify the certificate's

Problem	Solution
performing the software list deployment operation by selecting **Operations** > **Out Of Band Management** > **Device Management** > **Software List Deployment**.	subject name as the value for the "ca_ server_commonname" property in the `config.properties` file.
You cannot read or write to the managed vPro device because the flash limit has been exceeded for vPro storage. Flash wear-out protection mechanism can cause a flash limit exception to occur if you have made several read/write accesses to the same vPro device. When the counter reaches 200, the vPro device does not allow anymore write operations.	Use the **Reset Flash Limit** option from the pull-down menu on the common utilities icon.
I18N issues with OOBM and SCS because of dependencies on underlying components and technologies like the hardware BIOS or the Intel SCS. Although RCA Console can be installed on non-English operating systems, there are some restrictions due to dependencies on underlying components and technologies like the hardware BIOS or the Intel SCS. As a result, you cannot enter non-English names for several user-defined items, including filters, watchdogs, and policies by selecting **Configuration** > **Out Of Band Management** > **vPro System Defense Settings**. The SOL console for the BIOS setup works only for supported character sets. Similarly, other features may not work as expected in non English locales. Numbers, dates, and time are not being displayed in the format of the non-English operating system's locale.	There is no workaround for this problem.
English path separator is displayed on Japanese locale for OOBM features. This is because of limitation in the underlying Intel SCS component. The RCA Console shows the English path separator on a Japanese locale. This problem will occur only for the OOBM functionality.	There is no workaround for this problem.
You cannot read or write to the managed vPro device because the flash limit has been exceeded for vPro storage. Flash wear-out protection mechanism can cause a flash limit exception to occur if you have made several read/write accesses to the same vPro device. When the counter reaches 200, the vPro device does not allow anymore write operations.	Use the **Reset Flash Limit** option from the pull-down menu on the **common utilities** icon.
Error such as unauthorized user or access denied occurs on performing vPro operations.	Enable appropriate realm on SCS profile.
Error such as unauthorized user or access denied occurs on performing DASH operations.	User should have permissions to perform the operation.

Provisioning Problems

Problem	Solution
Status of provisioned vPro device does not appear as provisioned in the Device List table on the vPro Provisioning tab because the table is not refreshed with updated information.	Re-discover the device using Active Directory discovery. The status of the device will be updated after this operation.
You are unable to set ACLs when provisioning vPro devices whose version of AMT firmware is less than 4.0 on SCS 5.0 because all realms have been selected when creating the profile for vPro devices with 4.0 AMT firmware or earlier.	Create a separate profile for devices with the earlier version of AMT firmware. In this profile, select only the Redirection, PT Administration, Hardware Asset, Remote Control, Storage, Event Manager, Storage, Administration, Agent Presence Local, Agent Presence Remote, Circuit Breaker, Network Time, General Info, and Firmware Update realms.
Console gives SCS error when provisioning vPro devices because of internal error returned from Intel SCS. In some cases when you are trying to provision vPro devices through the RCA Console, the console throws up an SCS error or an error message without any other information.	This is harmless and can be ignored. The provisioning operation has been initiated successfully on the vPro device and this can be confirmed by verifying the results of the operation after a period of time.
Provisioning vPro device multiple times causes console to exit to login screen due to database access related issue.	In some cases when you attempt to provision a vPro device multiple times through the RCA Console, the console may exit to the login screen. In such cases, close the browser completely and re-login to the RCA Console.
In remote provisioning, the watchdog is not getting registered.	Ensure that you have provided correct IP address of SCS and the SCS user has enterprise administrator role. This issue can also arise because the HECI driver is not installed or the version is not correct or the BIOS is not updated. It is required that the driver and BIOS be compatible with each other.

Discovery Problems

Problem	Solution
Failure to discover vPro devices although OOBM agent is installed because the Port 9998 might be blocked by the firewall.	Ensure that port 9998 is not blocked on the vPro device.
No hardware assets are discovered for a managed vPro	Shut down the device, remove the

Problem	Solution
device because internal error has occurred in the vPro device during this operation.	power cord, wait 10 to 15 seconds, and restart the device.
No hardware assets are discovered for a managed vPro device because of incorrect provisioning of the vPro device. The device displays in the list while its state is disabled. Also, the "connect time out" error is displayed on single device console.	If the vPro device is pingable, the problem is with the web service of the vPro device. Restart the target vPro device.
No hardware assets are discovered for a managed vPro device because container space limitation prevents capture of additional asset data. This can occur if there are a large number of devices on a system.	Disconnect some of the devices.
No hardware assets are discovered for a managed vPro device. This problem can arise because of network error, while querying for hardware assets, due to heavy network traffic.	Re-issue the command after a time lag.
The "`maximum space reached`" error appears. This error occurs ff the Core Server is changed while deploying the software list.	Do a full reprovision of the vPro device.
No software assets are discovered for a managed vPro device. This problem can arise because of network error, while querying for software list, due to heavy network traffic.	Re-issue the command after a time lag.
Some properties are displayed as blank for discovered hardware and software assets because no information is available for the property on the device.	This is normal behavior if no information for a particular property is stored on the device.
OOBM groups will fail to reload when the OOBM device database does not have the latest devices because it is not updated with the latest devices. OOBM groups will fail to reload and the error "No devices with Given Name" is displayed. As a result, groups will not be updated. This will cause a problem when the user is performing the groups reload operation by selecting **Operations** > **Out Of Band Management** > **Group Management** > **Reload**.	Perform the OOBM device discovery operation again to update to the latest devices. This will solve the groups reload error.
Discovery of valid DASH device fails. This can occur because the device fails to respond in time because of network traffic.	Increasing the configuration values of HTTP_READ_TIMEOUT and HTTP_CONNECT_TIMEOUT may resolve this problem.
DASH device is discovered and displayed with IP address instead of hostname. This can happen because the device has been discovered by specifying the IP address and the DNS server is not configured for	Specify the hostname when attempting to discover DASH devices. If the DNS server is not configured for

Problem	Solution
"reverse DNS lookup."	"reverse DNS lookup," it is not possible to get the translation from IP address to hostname for the device. All operations should work as expected irrespective of whether the IP address or hostname is displayed.
Provisioned vPro device is not discovered or shown as unavailable because the vPro device, although provisioned earlier, may no longer be provisioned.	Reprovision the vPro device.
Provisioned vPro device is not discovered or shown as unavailable because the vPro device may have been removed from the Domain Controller although it still exists in the SCS database.	Ensure that the vPro device exists in the Domain Controller with the correct FQDN.
Provisioned vPro device is not discovered or shown as unavailable because the vPro device has multiple entries in the DNS server.	Ensure that the vPro device has only one entry in the DNS server.
Provisioned vPro device not discovered or shown as unavailable because the vPro device has a different IP address in the DHCP server from the one displayed in the device list in the RCA Console.	Ensure that the vPro device has the same IP address in the RCA Console device window as that in the DHCP server.
Provisioned vPro devices in Client Automation groups are not shown on Devices tab in Group Details window because the vPro device in the Client Automation group may not be listed with a FQDN.	Import the device in to the Client Automation group by using the FQDN and add this device to the group. Then reload the Client Automation group into the RCA Console.

Remote Operations Problems

Problem	Solution
The PuTTY console fails to open when performing remote operations on DASH devices. This may be caused by another PuTTY console running on the system. While performing DASH remote operation with the display to console option enabled, the PuTTY console will fail to open if another PuTTY console is running on the system.	Ensure that no other PuTTY console is running before performing DASH remote operation.
Telnet console does not open when performing remote operations. This is caused by specific Internet settings not set correctly, preventing the display of the telnet console	In your Internet Explorer, go to **Tools** > **Internet Options** > **Advanced**. Ensure that both the **Disable script debugging (Internet Explorer)** and **Disable script debugging (other)** options are selected.

Problem	Solution
Telnet console does not open when performing remote operations. The default security settings for ActiveX controls are preventing the display of the telnet console	In your Internet Explorer, go to **Tools** > **Internet Options** > **Security**. Click **Custom Level**. Select **Enable** for **Download unsigned ActiveX controls** and **Initialize and script ActiveX controls not marked as safe**.
Telnet session does not open on the client console on Windows Server 2003 64-bit platforms because OOBM is not able to open the telnet connection on this platform.	Use HyperTerminal to view the vPro device text console. Configure the PuTTY client to view the DASH device text console.
PuTTY is not able to establish the connection with the client DASH device on Windows 64-bit systems.	Copy the executable for Putty on a Windows 64-bit system. Append the path of the Putty executable to the PATH system variable on the Windows 64-bit system.
OOBM remote operations fail on vPro device after changing the provisioned state of the device because of inconsistency between the information in the OOBM database and the SCS database. When changing the provisioned state of a vPro device (including changing TLS mode and re-provisioning the device with a different SCS profile), remote operations on individual or multiple vPro devices fail.	Select the device for which the provisioned state has changed and click the **Reload Device Information** button from **Operations** > **Out of Band Management** > **Device Management**. Alternatively, click the **Reload Device Information** button (without selecting a device). The latter takes longer but will refresh all device information so that latest information is loaded into OOBM database and is consistent with the information in SCS database.
Nothing appears to be happening when performing OOBM remote operations on vPro device because of following causes: • Inconsistency between the information in the OOBM database and the SCS database • Unavailability of the device on the network	Close the Device Detail window and open a new one. This should allow you to see the error messages. If the problem is caused by an inconsistency between the OOBM and SCS databases, click the **Reload Device Information** button under **Operations** > **Out Of Band Management** > **Device Management** > **Refresh All**.
OOB DASH device boots from hard drive regardless of boot order because of issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. If the user has included USB in the boot order and if the USB boot source is not bootable, the system will boot from the hard-drive regardless of the other boot sources in the boot order. This will cause a problem when the user is performing boot operations on a DASH device when selecting **Operations** > **Out Of**	There is no workaround.

Problem	Solution
Band Management > **Device Management** > <*DASH Device*> > **Remote Operations**.	
OOB DASH device tries all boot sources including ones that are not specified in the boot order because of issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. If the user selects the persistent boot option, the device will try all the boot sources, including those that are not specified in boot order. This will cause a problem when the user is performing boot operations on a DASH device when selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Remote Operations**.	There is no workaround.
Incorrect network controller set as first boot source for OOB DASH devices. This is because of issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. For Dash-enabled devices, if you change the boot order to make Network the first boot device, it will set the embedded network controller as the first boot source instead of the Broadcom DASH NIC. As a result, the PXE boot from the Broadcom NIC will fail.	Go into the F10 Setup Advanced menu. The embedded NIC PXE option ROM can be prevented from loading by disabling the **NIC PXE Option ROM Download** option in the Device Options list. Retry booting from the Broadcom PXE after you have disabled this option.
During reboot or power on operation, you are unable to go to the next page from the Remote Operations Wizard Task page because of incorrect version of the JRE installed.	Install JRE version 1.5 or later and select the option in the Internet Explorer to install the JRE plug-in. To select this option, in your Internet Explorer, go to **Tools** > **Internet Options** > **Advanced** and select the **Use JRE 1.5.XX for**<*applet*>**(requires restart)** option. Restart the Internet Explorer once the JRE is installed and enabled.
Telnet session fails to open for SOL/IDE-R operations on vPro devices because the telnet client may not be installed. By default, the telnet client is not installed on Windows Server 2008. When RCA is installed on Windows Server 2008 x64 (AMD64T), the telnet session does not open for SOL/IDER operations. The boot operation however is successful and the machine boots from the correct media. The Heal use case is not fully supported due to this issue. For example, the BIOS updates cannot be performed.	Install the telnet client by using the server manager option in Windows Server 2008.
Remote Operations wizard for DASH device	The progress bar spins for a few seconds

Problem	Solution
keeps on showing progress bar without showing operation completion. This could be possibly because the device hardware is not sending an acknowledgement for the remote operation to the Remote Operation wizard causing the wizard to continuously wait. However, the remote operation is successful.	before the job is completed. Hence, wait for a minute and check the status. If the status is not updated, close the current IE session and log in again in a new IE session.
Boot configuration setting for DASH devices remains enabled for a while. This reflects the fact that the operation is still in progress and then eventually completes.	This is the expected behavior.
Remote operations like Hibernate (Soft) and Suspend do not work on target DASH device. This is because the Broadcom management agent may not be running on the target DASH device or the DASH device may not be in the Windows OS running state. If either of these conditions exist, Hibernate and Suspend operations will not function on the DASH device even though the operation is shown as successful in the RCA console.	Make sure that the latest Broadcom Management Plus agent(Example, NetXtreme) and the latest Graphics driver have been installed on the target DASH device.
vPro device IDE-R operations information does not align properly in HyperTerminal console. This could be either due to timing issues or issue with the firmware from hardware vendor.	There is no workaround for this problem.
Multiple users performing operation on same OOBM device causes erratic behavior because of architectural limitation.	At any given time, only a single user should be performing remote operations on a device.
vPro device does not power down after IDE-R reboot because the web services are busy performing current operation.	The vPro device may not successfully perform a Power Down command after an IDE-R reboot. Waiting ten seconds before issuing the Power Down command should work around the problem.
vPro device floppy IDE-R reboot produces unintelligible output to SOL display. This can be caused by creating the bootable floppy from an MS Windows version of MS-DOS (for example, using Format in Windows to create an MS-DOS Startup Disk).	Use another means of creating a bootable floppy drive.
vPro devices appear grayed out after power down command because the ME power setting options may not be set properly. In the SCS profile, the power policy may not be set properly. Also, there	Make sure your ME power setting options are set to always on ME or wake on ME in all possible power states. Also, check in the SCS profile that the power policy is set to

Problem	Solution
may be multiple entries for the vPro device in the DNS server.	always ON. And finally, check if there are multiple entries for the vPro device in the DNS server. If there are multiple entries, delete the wrong entries, restart the DNS server, flush the DNS in the RCA Console server, and re-start the RCA Console server. Alternatively, you can increase the web service timeout value on the RCA server.
OOB devices transitioning to S1/S2 or Sleep-Light power states show erratic behavior. This is because some hardware vendors do not support the S1/S2 or Sleep-Light power states.	For more information, see the documentation from the hardware vendor.
OOB device stays in suspended state after power down. Because on certain hardware, if the system is in a suspended state and a user invokes power off, the RCA Console reports success, but the machine stays in the suspended state. This is due to the fact that the hardware in these cases does not support the power off operation from the suspended state.	For more information, see the documentation from the hardware vendor if you are seeing such behavior.
Graceful power operations on DASH devices are displayed as supported options but are not working because the broadcom management agent is not installed.	Install latest Broadcom management agent on DASH device.
Error such as unauthorized user or access denied occurs on performing KVM operations.	Enable PT Administration realm on SCS profile and re-provision the vPro device.

Power State Problems

Problem	Solution
You are unable to view or change the power state of a managed vPro device. This problem can arise because of network error, while querying the system, due to heavy network traffic.	Re-issue the command after a time lag.
You are unable to view or change the power state of a managed vPro device. This failure to power down occurs because of an active IDE-R/SOL session.	Power down command is not supported when there is an active IDE-R/SOL session. The console throws the "Parameters are valid but not supported by platform" exception. Check if there is an active session. If so, close the session and try to power down after a time lag.
Power state of a device is grayed	Reconfigure the timeout period.

Problem	Solution
out after a power down operation because the timeout period exceeded	
Device does not respond to power commands from the RCA server possibly due to a problem in the configuration of network devices such as routers and switches.	Test the network path from the RCA server to the managed device for Wake-on-LAN support. A number of third party tools exist for sending a remote power on command to a network device. Searching the internet for "Wake-on-LAN tools" will return many free tools for testing this capability.

Reboot Problems

To troubleshoot reboot problems, you must examine the global configuration settings for IDE-R and SOL and the remote control options. The following table lists some common problems and their possible solutions.

Problem	Solution
You must perform boot order operation before reboot of OOB DASH devices for one time boot setting. This is because of issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware. If the user selects the boot configuration setting of one time boot for a reboot operation on Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware, the user is required to perform the boot order operation before reboot. Otherwise, the remote operation will display erratic behavior. Also note that although the user has performed an explicit boot order operation, after reboot, the boot order will get reset to default boot order. This will cause a problem when the user is performing boot operations on a DASH device by selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Boot Configuration**.	There is no workaround.
On DASH device, one time boot configuration does not reset because of issue with system BIOS. One time boot configuration on the DASH device is not resetting even after the device reboots. When the one time boot configuration is selected or enabled for any remote operation, it is not unselected or disabled once the remote operation has been successfully completed. Once this problem occurs, all the future remote operations will always use the one time boot configuration. This will cause a problem when the user is setting the one time boot configuration on a DASH device by selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Boot Configuration**.	Change the boot order of the one time one-boot configuration before performing any reboot operation by selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Remote Operations.
You are unable to change boot configuration setting for DASH device to default and permanent boot. Because the settings are hard coded to the permanent boot configuration setting for the first	There is no workaround for this problem.

Problem	Solution
boot configuration setting listed. It is not possible to change the boot configuration settings to default and permanent boot. The user cannot change this to one time boot. However, the user can change the settings for second boot configuration setting listed to one time boot. This will cause a problem when the user is performing boot configuration settings on a DASH device when selecting **Operations** > **Out Of Band Management** > **Device Management** > <*DASH Device*> > **Boot Configuration**.	
You are unable to see the reboot process on the RCA Console using SOL because the port 9999 is being used by another device.	Free up port 9999 for SOL transmission.
You are unable to see the reboot process on the RCA Console using SOL because the SOL redirection was not enabled during provisioning.	Enable SOL redirection using Intel SCS.
You are unable to see the reboot process on the RCA Console using SOL because the bootable floppy was created with Windows Explorer.	Using Format in Windows to create an MS-DOS Startup Disk produces a bootable drive but the output to SOL is unintelligible. Use another means of creating a bootable floppy drive.
You are unable to remotely reboot a managed vPro device because of incorrect reboot parameters.	View logs to check reboot parameters. If they are incorrect, try rebooting with the correct parameters.
You are unable to remotely reboot a managed vPro device because of known limitations in firmware for certain options.	Check the Intel vPro SCS server Release Notes located in the `Media\oobm\win32\AMT Config Server` directory on the RCA Core distribution media.
There are problems rebooting with IDE-R because the physical bootable device (drive/image) is not present in the management console.	Boot to an existing drive in the management console. If the physical device is not present, use the ISO image instead.
There are problems rebooting with IDE-R because the image in the media is not bootable.	Check if image is bootable. If not, replace it with bootable image.
There are problems rebooting with IDE-R because while trying to reboot to CD/DVD, the CD drive on the RCA Console server does	Reconfigure the default drive setting to match the

Problem	Solution
not match the default D: drive setting.	CD/DVD drive on RCA Console server.
You are unable to remotely reboot a managed vPro device to BIOS settings because the BIOS does not support booting to BIOS settings.	Upgrade BIOS on the target device to a version of the BIOS where this feature is supported.
You are unable to reset the boot order of a managed vPro device. The cause for this is difficult to determine.	Perform a local HDD boot command and reboot the target device.

System Defense and Agent Presence Problems

Problem	Solution
You are unable to deploy System Defense policies to the managed vPro device because the filter limit of 31 inbound and 30 outbound filters has been exceeded for vPro device.	Delete some of the existing filters on the vPro device.
System Defense policies do not always function properly on vPro devices with wireless network driver. This is because wireless network driver version on vPro device is not consistent with the installed version of the Intel AMT.	To ensure proper functionality of System Defense policies, the wireless network driver version on the vPro device must be consistent with the installed version of Intel Active Management Technology. More details regarding version compatibility can be obtained from the hardware vendor.
You are unable to deploy watchdog on the managed vPro device. Only one OOBM agent watchdog can be deployed to a vPro device. Multiple third party agent watchdogs can be deployed, one per third party agent installed on the vPro device. The total number of watchdogs that can be deployed to a single device is 16.	Remove or undeploy watchdogs from the vPro device.
You are unable to deploy watchdog on the managed vPro device because invalid, contradictory actions are defined for the watchdog.	Review actions specified for the watchdog and modify contradictions.
OOBM agent installation fails with error code 1920 because of issues with a previous install or uninstall of the OOBM agent.	Remove the HPCA-OOBM agent service from the vPro device. To do this, right click the My Computer icon and navigate to **Manage** > **Services and Applications** > **Services**. Check for the HPCA-OOBM agent service. If this service

Problem	Solution
	exists, do the following: • Open a command prompt window • Type `sc delete HPCA-OOBM` • Restart the system
OOBM agent installation fails with error code 1920 because you did not provide a user name and password when installing the OOBM agent.	Provide a "dummy" user name and password even if you do not intend to provision devices using delayed configuration. If you do not provide a user name and password, the installation will fail with error code 1920.
OOBM agent shuts down because no applications have been defined for it to monitor.	Create and deploy a software list of applications for the OOBM agent to monitor. For more information, see *Managing Watchdog* section in the *Radia Client Automation Enterprise Out of Band Management User Guide*.
Deployment of OOBM agent software list on vPro device throws SOAP error. This happens because vPro Web Services returns the error. Deployment of the OOBM agent software list may throw one of several errors including "Network Error – SOAP error code: 22," "Integrity check error," "Not initialized," and "Invalid parameter."	Retry the same operation after a time lag. If the error still occurs, logout and re-login to the RCA Console.
OOBM agent does not appear in software list on vPro device. This is because of architectural limitation occurring when the OOBM agent is installed by one user account and viewed by a user who has logged in with another account.	There is no workaround for this problem.
Deploying Agent Presence policy to one NIC on an vPro device with multiple NICs returns error. This is an internal error.	Deploy the Agent Presence policy to all NICs and then undeploy the Agent Presence policy from the unwanted NIC.
Anti spoofing filter causes all outgoing traffic on vPro device to be dropped. If a vPro device is provisioned with a profile in SCS with environment detection enabled and the device is connected to a domain, which has not been specified in the environment detection domain(s), all outgoing traffic will be dropped if the System Defense policy on the vPro device has the anti spoofing filter enabled.	Connect the device to a domain specified in the environment detection domain(s).

Problem	Solution
OOBM agent cannot register with watchdog on vPro device. If the OOBM agent is not able to register with the watchdog, the issue may be with Digest username (Intel AMT username). In the Intel AMT firmware, the Digest username is case sensitive. You must specify the Digest username with the exact case when installing the OOBM agent. Otherwise, the OOBM agent will not be able to register successfully with the watchdog.	Be sure to specify the Digest username correctly with the exact case.
Repeated messages are displayed when OOBM agent is stopped on vPro device. This is because of internal error in HPCA-OOBM Agent.	If this occurs, restart the HPCA-OOBM agent service (HPCA-OOBM) on the client vPro device.
You are unable to access vPro device after changing Digest credentials. Agent gets the password only during install time and not dynamically when it is changed. You will not be able to access a vPro device if you have changed the Digest username/password for this device through the SCS console.	To be able to access and manage this device after changing the Digest credentials, you must stop the OOBM agent (HPCA-OOBM) service on the vPro device. If you are using the Agent Presence functionality, you must reinstall the OOBM agent on the vPro device with the new password.
OOBM agent does not work properly on vPro device after changing from TLS profile to non-TLS profile. If the OOBM agent is installed using a TLS profile, and at some point, the vPro device is re-provisioned with a non-TLS profile, the OOBM agent will not work properly. Similarly, if the OOBM agent is installed using a non TLS profile, and at some point, the vPro device is re-provisioned with a TLS profile, the OOBM agent will not work properly.	If this occurs, you must re-install the OOBM agent using appropriate profile.
OOBM agent admin pop-up message displays briefly and disappears. This is the default behavior of the admin pop-up message when the Agent Presence policy is activated.	Open the Windows Event Viewer on the vPro device to see all agent-related log messages.
You are unable to deploy OOBM agent software list and system message to the managed vPro device. The possible causes are: • Multiple actions occurring at the same time to the 3PDS • Multiple accesses to 3PDS during one session • Data transfer problem over the network	Retry deployment after a time lag.
You are unable to deploy the OOBM agent software list or view the software information in TLS mode. The Tomcat service may not be running on the Domain administrator	Ensure that the RCA Tomcat Server service is running on the Domain administrator account. If not,

Problem	Solution
account.	reconfigure and restart Tomcat.
You are unable to deploy the OOBM agent software list or view the software information in TLS mode. This is because the common name on the Certification Authority (CA) may not be specified correctly.	Ensure that the common name on the CA is specified correctly. The setting can be found in the `local_settings.ini` file in the installation directory.
There is no change in the watchdog state on the RCA Console after the OOBM agent is successfully installed because the watchdog registration failed.	Open the Windows Event Viewer on the vPro device and check for watchdog registration log messages. If unsuccessful, install the Host Embedded Controller Interface (HECI) driver and the Local Manageability Service (LMS) service on the vPro device and re-check the watchdog status.
Deployed Agent Presence Policy is not activated when defined actions occur. This is because the defined actions may not have occurred in the anticipated order. The OOBM agent may have expired before the OOBM agent transitioned to the specified state.	It is safest to specify “Do not Care About State” as the transition to state when specifying watchdog actions.
Agent Presence Policy is activated immediately after deployment. Because the transition state activating the Agent Presence policy may have already occurred triggering the immediate activation of the Agent Presence Policy by the watchdog.	Delete the existing watchdog and redeploy.
You are unable to deploy System Defense policies with special characters in name. This problem arises because it is possible to create filters and policies with non ASCII characters in their names, but it is not possible to deploy them. Also, filters and policies with special characters like ‘:’, ‘,’, '>', '<', '&', and ‘”’ in their names cannot be deployed. This limitation is indicated in the Intel AMT specification.	Create filters and policies with names that adhere to the specification.

Wireless Problems

Problem	Solution
You are unable to connect to a wireless device through the RCA Console. Because the web service timeout occurred since the time it takes to communicate with a wireless device is greater. When the RCA Console cannot connect, the devices appear unavailable in the console.	Reconfigure the timeout period.

Problem	Solution
You are unable to connect to vPro device using the wireless NIC. This is expected behavior for the 2.5 version of vPro devices when only the wireless NIC is configured and the device is not plugged in and powered on.	Connect the vPro devices to a power source and power them on.
Failure to establish SOL/IDE-R session on wireless network for vPro devices. This problem is caused by time-out because vPro devices with wireless NICs require a greater amount of time to communicate with the OOBM Server.	Configure the IDER* and SOL* parameters as described in the "Configuring the IDE-R and SOL Time-out Values" section in the Radia Client Automation Out of Band Management User Guide.
Policy settings for wireless NIC fail because the vPro device does not have a wireless NIC although the policy appears to have been deployed successfully.	Undeploy the policy or install a wireless NIC on the vPro device and redeploy the policy.

Migration Problems

Problem	Solution
OOBM agent software list and system message cannot be displayed after migration to the current release of Out of Band Management Software. This is the normal behavior. If the software list and system message for the OOBM agent are created and deployed in an earlier release of Out of Band Management Software, they are not available if you migrate to a later version.	Create and redeploy the OOBM agent and system message in the current release.

Checklist Questions

If you are still having problems with the Out of Band Management features in the RCA Console, call Persistent support. Before calling, be sure you know the answers to the following questions. This information will expedite the support team's ability to solve any problem you may be experiencing.

- What is the operating system and service pack installed on your RCA Console server?
- What is the IIS version on the SCS Server?
- Are SCS and the RCA Console installed on the same machine?
- Are SCS and the SQL server installed on the same machine?
- Is Active Directory installed on your network?
- Do you have a DNS and DHCP-enabled network?
- Are you using the NTLM v2 protocol for authentication between the SCS server and the Out of Band Management Service on the RCA Console (you can check in local policies to confirm)?
- What user ID did you use when installing SCS regardless if it was a local or domain user?
- Does that local or domain user have local administrator rights?

- What authentication mode are you using to communicate with SQL (Windows authentication is recommended)?
- Are you able to login to the RCA Console?
- Are any devices listed on the Devices tab in the RCA Console?
- Are the devices displayed but are disabled, that is, they appear grayed out and are not accessible?
- Are any devices provisioned using SCS?
- Are the provisioned devices listed in the SCS table?
- For SCS login, are you using http://IP/AMTSCS or https://IP/AMTSCS as the URL?

Troubleshooting Portal

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Portal.

Log Files

The Portal writes several logs, which can be used to track progress and diagnose problems. The log files are stored by default in `<InstallDir>\ManagementPortal\logs` for the Portal for Windows.

Portal: Log Files

Log File	Description
`HPCA-RMP-port.log` where, port is the Portal port number.	Contains log messages related to the tasks that the Portal Manager performs, the operational statistics, the build number, and the version number details of the Portal modules Each time you start the web server a new log is written, and the old log is saved as `HPCA-RMP-port.nn.log`.
`httpd-port.YY.MM.DD.log`	This log contains the web server activity for each day. If the log file is empty, no web server activity was performed on that day. The following types of messages are logged in this file: • Error: Indicates a critical problem. • Warning: Indicates a non-critical problem. • Info: Provides general information. • Audit/success: Indicates a successful change to an object in the Portal directory. • Audit/failure: Indicates an unsuccessful change to an object in the Portal directory.
`httpd-`	Contains a consolidated list of error messages. All log messages that are

Log File	Description
port `.error.txt`	prefixed ERROR are written to this log file, enabling you to view all error messages at a single location.

`rms.log`
`rms.`*n*`.log`
where, n is a positive integer.
	Contains a list of messages processed by the Messaging server that are stored on the Portal. The value of *n* is incremented when the log file size reaches its maximum limit. The log file size can be configured by updating the `-loglines` parameter in the `rsm.cfg` file under *<InstallDir>\ManagementPortal\etc*.

`RMP-Signals.log`
`RMP-Signals.`*n*`.log`
where, n is a positive integer.
	This log file contains messages related to the management agent signal processing. The value of *n* is incremented when the log file size reaches its maximum limit. The log file size can be configured by updating the `-loglines` parameter in the `HTTPD-RMP.rc` file under *<InstallDir>\ManagementPortal\etc*.

Setting Trace Levels

By default the trace level is set to 3, which is the informational tracing level, and enables the logging of INFO, WARNING, and ERROR messages.

To change the trace level for the logs:

1. Open the file `HPCA-RMP.rc` from the location *<InstallDir>*`\ManagementPortal\etc\`.
2. Type `LOG_LEVEL` and the appropriate trace level, space delimited, within the `Overrides Config` section starting and ending brackets { }. Set the trace level using the options listed in the following table:

   Trace Levels

Trace Level	Description
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. Recommended trace level setting for customers.
4	Logs all debug information. *Recommended for experienced customers only*.
5 - 9	Full trace *Not recommended for customer use*.

3. Save the file, and then restart the RCA Portal service.

Setting Trace Levels for Portal Directory

The following two options can be configured if you are having difficulties with the Portal Directory's Slapd service.

To enable logging of the HP Client Automation Directory Service:

If the Portal directory service requires troubleshooting, Persistent Software customer support may ask you to turn on logging for the slapd service.

To create a `slapd.log` in the HPCA Directory Service Directory, set the following Registry entry:

`HKEY_LOCAL_MACHINE\SOFTWARE\hpca-ds\DebugLevel` *256* `(decimal)`

Where: *256* represents a sample debug level. Replace 256 with the desired debug level from the following table. If no value is entered, the default is 0, which turns logging off.

Debug levels for slapd, backupslapd, and slurpd logs

Debug level	Description
-1	Enable all debugging **Warning**: Logs ferocious amounts of data. Not recommended.
0 (default)	Turn off logging
1	Trace function calls
2	Debug packet handling
4	Heavy trace debugging
8	Connection management
16	Print out packets sent and received
32	Search filter processing
64	Configuration file processing
128	Access control list processing
256	Stats log connections/operations/results
512	Stats log entries sent
1024	Print communication with shell backends
2048	Print entry parsing debugging

Restart the HP Client Automation Directory Service service to begin logging the `slapd.exe` process.

To turn off logging for the HPCA Directory Service:

1. Reset the `HKEY_LOCAL_MACHINE\SOFTWARE\hpca-ds\DebugLevel` registry entry to 0.
2. Restart the HPCA Directory Service.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Portal.

Problem	Solution
Current jobs (scheduled and running) do not show the correct status.	One of the cause for this problem could be the jobs checkpoint file, jobs.ckpt, has got corrupted. Perform the following steps to get a fresh jobs checkpoint. 1. Stop the HPCA Portal service. 2. Delete the existing `jobs.ckpt` file from the `<InstallDir>\ManagementPortal\etc` directory. 3. Create a copy of the `jobs.ckpt.tmp` file with the name `jobs.ckpt`. 4. Start the HPCA Portal service. Check if the jobs show the correct status. If this does not solve the problem: 1. Delete all three job checkpoint files - `jobs.ckpt, jobs.ckpt.tmp, and jobs.ckpt.old`. 2. Restart the HPCA Portal service to create the jobs files again. If the job files have been backed up, you can see the jobs status. Else, you need to recreate the jobs.
Unable to log on to the RCA Console. The following error is displayed on the RCA Core Console: `Unable to communicate with the authentication portal`	Make sure that the HPCA Portal service is running. If the HPCA Portal service is running, the Directory Source drop-down box on the RCA Core Console shows HP Zone.

Information required by Persistent Support

Before contacting Persistent Support to resolve your problem, gather the following information about your current environment:

- The log files, stored by default at the location `<InstallDir>\ManagementPortal\logs`.
- Version information for `nvdkit.exe`. To know the nvdkit.exe version:
  a. Open the command prompt.
  b. Navigate to the <InstallDir>\ManagementPortal directory.
  c. Run the following command, `nvdkit-hpca-rmp.exe version`
- The `etc` directory files, stored by default at the location `<InstallDir>\HPCA\ManagementPortal\etc`.

Troubleshooting Messaging Server

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Messaging server.

Log Files

RCA writes several logs that you can use to track the Messaging server process and diagnose problems. You can access the log files from the location `<InstallDir>\MessagingServer\logs`.

The following table lists the log files available for troubleshooting the Messaging server component.

Messaging Server: Log Files

Log File	Description
`rms.log`	Contains log entries for incoming and outgoing messages, and the data that is sent to the RDBMS.
`rms-core-qx-0n.log` where, x is the worker. n is the queue number.	Contains log messages related to the core data queue.
`rms-default-n.log` where, n is the queue number.	Contains log messages related to the default data queue.
`rms-httpd-3461.yy.mm.dd.log`	Contains httpd traffic-related log messages, specific to Messaging server only. The log file is created everyday, and if the log file is empty, no web server activity was performed on that day.
`rms-patch.queue-n.log` where, n is the queue number.	Contains log messages related to the patch data objects that are imported to the RDBMS

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Messaging server.

Messaging server: Problems and solutions

Problem	Solution
You receive either of the following	This error occurs if one or more `sql` files located in the

Problem	Solution

error messages for all attempted posts to the Messaging server:
`404 Not found`
`500 Internal Server Error`
	`<InstallDir>\MessagingServer\etc\` folder and its subfolders contain the following commented section:
	`#sql::url ...`
	To resolve this problem, remove the # (pound sign) to un-comment this line.
	• Note that if you do not have any customized SQL files, you can move all sql files out of `<InstallDir>\MessagingServer\etc\` directory (place them in an outside location), and then restart the Messaging server. This unpacks the new `.sql` files, which should fix the error.
	• If you have more than one customization, use the following steps to correct the problem and still keep your customizations:
	a. Locate any `*.sql` files that you have customized in the following directories:
	◦ <InstallDir>\MessagingServer\etc\core
	◦ <InstallDir>\MessagingServer\etc\inventory
	◦ <InstallDir>\MessagingServer\etc\vm
	◦ <InstallDir>\MessagingServer\etc\wbem
	b. Delete the remaining `*.sql` files from the following folders.
	◦ <InstallDir>\MessagingServer\etc\core\hp
	◦ <Install-Dir>\MessagingServer\etc\inventory\hp
	◦ <InstallDir>\MessagingServer\etc\vm\hp
	◦ <InstallDir>\MessagingServer\etc\wbem\hp
	c. Restart the Messaging server to unpack a new set of `*.sql` files into the default following locations.
	◦ <InstallDir>\MessagingServer\etc\core\hp
	◦ <Install-Dir>\MessagingServer\etc\inventory\hp
	◦ <InstallDir>\MessagingServer\etc\vm\hp
	◦ <InstallDir>\MessagingServer\etc\wbem\hp
	d. Go to where you placed the customized `*.sql` files, and un-comment the sql::url line at the bottom of each file.

Problem	Solution
	e. Restart the RCA Messaging Server service.

The following deadlock errors are logged in the `rms-core-n.log` file:
`Transaction (Process ID n) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction`
	The deadlock situation occurs when multiple worker threads process the messages from a single computer.
	Replace the contents of the file `core.dda.cfg` with the following code, and the restart the Messaging Server service:
	`msg::register core {`
	`TYPE SQLBALANCER`
	`WORKERS 4`
	`QUEUE_DIR {<InstallDir>/Data/MessagingServer/core}`
	`QUEUE_POLL 1`
	`QUEUE_COUNT 5000`
	`QUEUE_DELAY 120`
	`QUEUE_ATTEMPTS 5`
	`SQL_REJECTS rejects`
	`SQL_DSN " <dsn> "`
	`SQL_SERVER ""`
	`SQL_USER " <username> "`
	`SQL_PASS " <password> "`
	`SQL_USE ""`
	`SQL_AUTOCOMMIT off`
	`SQL_DSN_DELAY 30`
	`SQL_DSN_PING 86400`
	`SQL_ENABLE-CORE true`
	`SQL_ENABLE-WBEM true`
	`SQL_ENABLE-INVENTORY true`
	`SQL_ENABLE-VM true`
	`SQL_AUTOCREATE true`
	`SQL_AUTOLOAD true`
	`SQL_STARTUPLOAD true`
	`}`

Problem	Solution
	where, • *dsn* is the Data Source Name (DSN) for the Core ODBC database. • *username* is the user ID for the DSN • *password* is the password for the DSN. The new core handler creates q*n* folders in the `<InstallDir>\DATA\MessagingServer\core` folder, where the value for n depends on the WORKER parameter. The messages from one computer are routed to the same q* folder and the same worker thread processing the message.
The number of rejected messages in the `<InstallDir>\DATA\MessagingServer\reject` is high.	Decrease the number of attempts to retry a failed message delivery before discarding the message. Set the ATTEMPTS parameter in the `core.dda.cfg` file to a value less than 5, and then restart the Messaging Server service.

Information required by Persistent Support

Before contacting Persistent Support to resolve your problem, gather the following information about your current environment:

- Collect sample agent messages on the RCA Core server.
  a. Open the file `rms.cfg` from the location `<InstallDir>\MessagingServer\etc`.
  b. Set the `DIAG` parameter in the `Overrides Config` block as `core`. This enables the message copies to be stored in the DIAG queue of the Messaging server.
  ```
  DIAG core
  ```
  c. Restart the RCA Messaging Server service.
- Increase the log level.
  a. Create a backup of the existing log files.
  b. Open the file `rms.cfg` from the location `<InstallDir>\MessagingServer\etc`.
  c. Set the loglevel parameter in the `log::init` block as 9.
  ```
  -loglevel 9
  ```
  d. Restart the RCA Messaging Server service.
- Reproduce the problem that you observed and collect the following files:
  - Server-related files:
    - Diags: `<InstallDir>\DATA\MessagingServer\diag`
    - Rejects: `<InstallDir>\DATA\MessagingServer\rejects`
    - Messaging server Logs:`<InstallDir>\MessagingServer\logs`

  - Management Portal Logs: `<InstallDir>\ManagementPortal\logs`, with WS_DEBUG turned ON in the `rmp.cfg` file located at `<InstallDir>\ManagementPortal\etc` only when the problem is related to data that is populated to the OpenLDAP.
  - ZTASKEND Rexx file: `<InstallDir>\ConfigurationServer\rexx\NOVADIGM\ZTASKEND`

- Agent-related files:
  - The `lib` and the `log` folders from the agent computer, for which the messages are getting rejected.

Make sure that you collect this information at the same time interval.

Troubleshooting Multicast Server

This section describes the log files, and the cause and solutions for the problems that you may observe during the multicast transmission.

Log Files

The following log files are created on the RCA Server where you have configured the multicast services under `<InstallDir>\MulticastServer\logs` directory.

Multicast server: Log files

Log File	Description
`HPCA-MCAST-port.log` *port* is the Multicast server port number.	Contains log messages related to the tasks that the Multicast server performs, the build number, and the version number details of the Multicast server internal components.
`httpd-port.YY.MM.DD.log`	Contains httpd traffic-related log messages, specific to Multicast server only. The log file is created everyday, and if the log file is empty, no web server activity was performed on that day.
`httpd-port.error.log`	Contains a consolidated list of error messages. All log messages that are prefixed ERROR are written to this log file, enabling you to view all error messages at a single location.
`gdmcsend.log`	Contains details about the OSM files sent to each client during the multicast session. For example, file name, number of packets, delay between packets, packet data size, and so on.

This section provides information on what to look for in the RCA agent logs (located in `IDMSYS\log`) when running a multicast session.

Multicast client: Log files

Log File	Description
`connect.log`	Contains log messages related to the RCA agent modules, `RADSKMAN`, `RADPINIT`, and `RADCONCT`.
`RADCRECV.log`	Contains information about the files received by an RCA agent through multicast transmission. For example, number and names of files transmitted, any error related to time out or file size.
`RADREQST.log`	Contains information about each file that RCA agent requests from the RCA Server during the multicast session.
`RADCLECT.log`	Contains details of processing done on RCA agent to create the list of files (MMCLIST) to be requested from the RCA Server during the multicast session.
`gdmcrecv.log`	Contains details about the OSM files received by the client during the multicast session. For example, Multicast IP address, mode, total packets, resend packets, and total time, and so on. You can access this log file from the location `C:\osmgr.hlp`.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA multicast feature.

Multicast: Problems and solutions

Problem	Solution
The following error message is logged in the `RADCRECV.log` file. `Multicast Packet Inactivity Timeout [5] (minutes)`	Reset the `MWINDOW` attribute of the Multicast class to zero.
The following error message is logged in the `RADCRECV.log` file. `Packets received: 39216 dropped(est): 0 (The number of unique packets received, not counting resends. The number dropped is an estimate, based on the gaps in the packet number sequence.)`	Increase the value set for DELAYBP or RESENDS attributes of the Multicast class.

Troubleshooting Patch Management

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Patch management feature.

Log Files

RCA writes several logs on the Core server and the client side that you can use to track the Patch Manager server process and diagnose problems.

You can access the Patch Manager server logs from the location `<InstallDir>\PatchManager\logs`.

Patch Manager Server: Log Files

Log File	Description
`HPCA-PATCH-port.log` where, *port* is the Patch Manager port number.	Contains log messages related to the tasks that the Patch Manager performs, the build number, and the version number details of the Patch Manager server internal components. The log file also provides log messages related to the patch gateway transactions.
`httpd-port.error.log`	Contains a consolidated list of error messages. All log messages that are prefixed ERROR are written to this log file, enabling you to view all error messages at a single location.
`patch-acquire.log`	Contains log messages related to the patch acquisition job. This log file is created only after a patch acquisition job is complete.
`patch-sync.log`	Contains log messages related to CSDB to RDBMS patch data synchronization.

The following table provides the list of patch manager client log files.

Patch manager client: Log files

Log File	Description
`connect.log`	Contains log messages related to the three RCA agent modules, `RADSKMAN`, `RADPINIT`, and `RADCONCT`. Note that by default the patch connect log information is stored in the file `connect.log`, however, if you specify a custom log file name while scheduling a patch job, the patch connect related log messages are logged in the custom log file only. `<InstallDir>\Agent\logs`
`Windowsupdate.log`	Contains log messages related to installation of Windows update agent. This log file also provides the scan details for the Windows update agent. You can access this log file from the location `<SystemDrive>\WINDOWS`.
`wuascan.txt`	Contains log messages related to the scan performed by the Windows update agent. You can access this log file from the location `<InstallDir>\Agent\lib\wua\`

Problems and Solutions

This table lists the problems that may occur when you are using the RCA patch management feature.

Patch management: Problems and solutions

Problem	Solution
After performing a patch acquisition, you are unable to deliver these patches to the agents.	This problem appears if you are using the Metadata model-based patch acquisition, but have not enabled the Patch Manager Gateway. To resolve this problem, complete the following steps to enable Patch Manager Gateway in the Core Console: 1. Log on to the Core Console and click **Configuration** tab. 2. Expand Patch Management in the left navigation pane, and then click **Distribution Settings**. 3. Under Patch Gateway Operations, click **Enable Gateway** check box, and then click **Save**.
After you have scheduled a patch connect, patches are not installed during the first connect. Subsequent patch connects are required to install the patches.	This is the expected agent behavior if agent preload option is enabled. To verify if the agent preload option is enabled, check if the discover method is set as `-pl Y` in the patch agent connect log file (`connect.log`). If the agent preload option is enabled, the first connect is used to discover the vulnerabilities and queue the patches to be downloaded to the Download Manager. After the patch binaries are downloaded by the Download Manager in subsequent agent connects, the patch is installed on the target device. Additionally, you can also configure the Download Manager options for the Patch agent, such that the Download Manager triggers the subsequent connect after the download completes. Set the **Apply patches after download completion** option [callback (`-cb`)] to `Yes` to trigger a Patch Agent Connect to apply the patches. For more information on how to set this option, see the section Agent Options in the *Radia Client Automation Enterprise User Guide*.
In addition to the patch connect, the Reporting Differencer module (`RepObjDiff.exe`) is incorrectly run during software connect also, even when this module is disabled for software connect.	This is the expected behavior. If the Reporting Differencer module is enabled, the RCA agent invokes this utility only if a patch connect object, such as `DESTATUS.edm`, `BUSTATUS.edm`, or `PASTATUS.edm` is available in the OUTBOX folder at the location `<InstallDir>lib\system\radia` on the agent computer. For more information on how to enable the Reporting Differencer module, see the section *Configuring Messaging Server to Report Differenced Objects* in the

Problem	Solution
	Radia Client Automation Enterprise Messaging Server Reference Guide. If any of these objects are still present in the OUTBOX folder during software connect, the Reporting Differencer module is invoked.
While acquiring Microsoft patches, you cannot exclude the patches for 64-bit operating systems.	In WSUS feed (`wsusscn2.cab`), the architecture is not separated for 64-bit operating systems. For more information, see the Microsoft web site at http://technet.microsoft.com/en-us/library/cc708464.aspx To exclude the 64-bit operating system, complete the following steps: 1. Log on to the Core Console and click **Configuration** tab. 2. Expand Patch Management in the left navigation pane, and then click **Vendor Settings**. 3. Under Microsoft Feed area in the Vendor Settings details pane, clear the **x64 (AMD64/Intel EM64T)** check box to exclude the 64-bit operating systems.
The following error message is logged in the file `patch-acquire.log` when you run an acquisition: `Error: HTTP file size mismatch; on disk: 12419072, Content-Length: 12568554`	Rename or delete the file `wsusscn2.cab` file stored at the location `<InstallDir>\data\patch\microsoft`. Run the acquisition process again.
The following error message, related to the web Proxy server configuration is logged in the file `patch-acquire.log`: `Error: HTTP error code 407 while downloading`	This problem occurs when the HTTP Proxy server for Internet-based communications is not configured properly. To reconfigure the HTTP Proxy server settings, complete the following steps: 1. Log on to the Core Console and click **Configuration** tab. 2. Expand Infrastructure Management in the left navigation pane, and then click **Proxy Settings**. 3. Enter the credentials for the HTTP Proxy in the Proxy Settings details pane, and click **Save**.
When a bulletin is reacquired with Force and Replace option enabled, the compliance information for the agent is not available in the following	This is the expected behavior. When a bulletin is reacquired with the Force and Replace option enabled, the internal bulletin and patch IDs are updated. As a result, the ID for which an agent had earlier reported a

Problem	Solution
reports: • Bulletin Status • Patch Status • Release Status • Product Status	compliance for, is no longer available. The compliance information can be viewed in the reports after the Patch connect process is run on the agent computer.

After you have successfully acquired the patches and performed a patch connect, the patch reports are not available for the target device.	This issue can occur when the Configuration server that the agent is connecting to has not been synchronized with the Configuration server where the bulletins were published. Since the object IDs are different in the two Configuration servers, the reports are not available.
	To resolve this problem, synchronize the Configuration server to which the agent is connecting to with the Configuration server where the bulletins are published. You can verify the Configuration server to which the agent is connecting to from the patch connect log file. Check for the following entry:
	`Attempting to connect to RCS: radia://aa.bb.cc.dd:xx`
	`Successfully connected to RCS: radia://aa.bb.cc.dd:xx`

The following error message is logged in the patch agent connect log file (`connect.log`) when deploying patches to target devices: `WUA Install Result Code 3 HRESULT $hresult`	Make sure that the correct Windows Installer version is installed on the target devices that are receiving patch updates.
Certain patches in the KB articles could not be managed using MUC (Microsoft Update Catalog). Because the Patch Manager MUC acquisition is highly dependent on Microsoft Update catalog. So, as long as you have Microsoft support, the Patch Manager is able to work.	If the KB article is not supported by MUC, then Patch Manager is not able to support it.
The patch installation fails with the error code `0x80070641` when you entitle a Service Pack along with the patch.	This problem occurs when the Service Pack is installed prior to the patch, and the computer is not set to reboot after the Service Pack installation. The Windows Installer Service fails to start until the computer reboots, and as a result the patches

Problem	Solution
	are not installed. Reboot your computer after the Service Pack installation. It recommends that you do not install the operating system patches along with Service Packs because some of the operating system patches may not be applicable after the Service Pack installation. However, if it is required to install the patches with Service Packs, change the priority to enable the Service Pack to install after the patches.
Microsoft Baseline Security Analyzer (MBSA) detects that a patch is required on the target device, but the Patch Manager does not install the required patch.	This problem occurs because of the `Update Id` parameter in WSUS. Each time Microsoft releases the `wsusscn2.cab` file, the value for the `Update ID` parameter is modified for the bulletin. When an acquisition is run for a particular bulletin for the first time, the `Update Id` is imported into the CSDB as part of the data feed. Thereafter, if Microsoft releases a new version of the `wsusscn2.cab` file, the `Update ID` parameter is updated. When you run the acquisition again for the same or any other bulletin, then only the `wsusscn2.cab` file changes in CSDB. The `Update Id` for that bulletin does not change until you use Force and Replace option. The SUSNAME for the patch instance is the `Update ID` that is retrieved from the `wsusscn2.cab` file for a particular patch. The entry for SUSNAME in the XML is still `MSSUSName`, but the `Update Id` in `wsusscn2.cab` file is changed. To identify if the patch is not being installed due to a mismatch in the Update ID parameter, complete the followings steps: 1. Run the MBSA scan to detect the required patch. 2. Check the MBSA scan logs to verify if the Patch is Not Applicable. 3. If the log contains the 'Patch is Not Applicable' entry, open the `patch_objects` folder at the location *<InstallDir>*`\lib` on the agent computer, and search for that particular bulletin. Remove the SUSNAME variable from the object. 4. Search the SUSNAME in `wuascan.txt`. If this entry does not exist in `wuascan.txt`, the patch is not installed. To resolve this issue, run the acquisition again with the Force and Replace Options set.
You have entitled a target device with `FINALIZE_`	This problem occurs when the `FINALIZE_PATCH` service is run before any other patch ZSERVICE, and as a result the

Problem	Solution
PATCH service, but the patches are not getting installed.	patches are queued up. By default, the ZSVCPRI parameter for the FINALIZE_PATCH is set as 20. The ZSVCPRI parameter determines the priority, that is when this service should run. By default, the bulletin ZSERVICE has the ZSVCPRI either set as blank, or a priority less than the FINALIZE_PATCH. To resolve this problem, set the ZSVCPRI parameter in the BASE_INSTANCE of the PATCHMGR.ZSERVICE to blank or of lesser priority than FINALIZE_PATCH in the Configuration server, and then run the patch connect. Alternatively, you can also set the priority for FINALIZE_PATCH (PATCHMGR.ZSERVICE.FINALIZE_PATCH) lower than the bulleting using the CSDB Editor.
When you run a patch connect and the Automatic Update (AU) service is initiated, the AU service does not stop after the patch connect has been completed.	Enable the Windows group policy to control the status of AU service.
The agent computer hangs during the patch connect process.	This problem occurs when corrupt objects are created on the agent computer. Corrupt objects are the objects with NULL values. To resolve this problem, delete the IDMLIB directory after the patch connect process completes. IDMLIB directory is a dynamic directory that the agent creates for each machine or user policy.
The software distribution [DataStore.edb] file size is very large during the patch connect process.	To resolve this problem, delete the Software Distribution directory. To delete this directory, complete the following steps: 1. Logon to the RCA Core Console and click **Configuration** tab. 2. In the left navigation pane, expand Patch Management, and then click **Agent Options**. The Agent Options view opens. 3. From the Delete Software Distribution list, select **Yes**, and click **Save**. For more information on Patch Agent Options, see the *Radia Client Automation Enterprise User Guide*.
The following error message is	Deploy the XML Parser Service Packs from Microsoft.

Problem	Solution
logged in the patch connect log file: `Error: No such interface supported while executing com::Invoke $updateSearcher Search [list VT_BSTR Type='Software'] Error: Error in WUA scan: No such interface supported`	
The patch connect time does not improve when the Manage Installed Bulletin (`mib`) option is set as `n`.	Set `-mib none` to improve the patch connect time.

Troubleshooting Security and Compliance Management

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA security and compliance management feature.

Log Files

RCA writes several logs on the Core server and the client side that you can use to track the Vulnerability Management Server process and diagnose problems.

Vulnerability Management server: Server log files

Log File	Description
`vms.log`	Contains log messages related to the Live Network update and messages related to the publishing. You can access this log file from the location `<InstallDir>\VulnerabilityServer\logs\vms.log`.
`connector-exec-cmd.log`	Contains log messages related to the processes that are run when a secure connection from RCA to HP Live Network is created using the Live Network Connector (LNc). You can access this log file from the location `<InstallDir>\VulnerabilityServer\logs`.
`live-network-connector.log`	Contains log messages related to installation and configuration tasks for the LNc tool.

Log File	Description
	You can access this log file from the location *<InstallDir>*\LiveNetwork\lnc\log.
lncm.log	Contains log messages related to the LNc update. You can access this log file from the location *<InstallDir>*LiveNetwork\lncm\log.
csdb-promote-PRIMARY.SECURITY*.log	Contains log messages related to the packages that are published to the CSDB. For each package that you publish to CSDB, a new log file is created. You can access these log files from the location *<InstallDir>*\VulnerabilityServer\logs\publish.

Vulnerability Management server: Client log files

Log File	Description
connect.log	Contains log messages related to the three RCA agent modules, RADSKMAN, RADPINIT, and RADCONCT. Note that by default the security connect log information is stored in the connect.log file, however, if you specify a custom log file name while scheduling a security job, the patch connect related log messages are logged in the custom log file only. You can access this log file from the location *<InstallDir>*\Agent\logs.
vulnerability-director.log	Contains log messages related to agent profiling and vulnerability security connect. You can access this log file from the location *<InstallDir>*\security.
scap-director.log	Contains log messages related to agent profiling and compliance security connect. You can access this log file from the location *<InstallDir>*\security.
sectools-remediation-director.log	Contains log messages related to security tools scan and the results of the scan process. You can access this log file from the location *<InstallDir>*\security\sectools.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA security and compliance management feature.

Security and compliance: Problems and solutions

Problem	Solution
The following error appears when connecting to HP Live Network. `Failed to connect. Exception [<urlopen error Proxy connection failed. Please verify the Proxy settings.]`	This problem occurs when the HTTP Proxy server for Internet-based communications is not configured correctly. The RCA Core server does not perform any validation on the proxy settings. It does not validate the format or make any attempt to determine whether the proxy server that you have specified is a valid proxy host. To reconfigure the HTTP Proxy server settings, complete the following steps: 1. Log on to the RCA Core Console and click **Configuration** tab. 2. Expand Infrastructure Management in the left navigation pane, and then click **Proxy Settings**. 3. Enter the credentials for the HTTP Proxy in the Proxy Settings details pane, and click **Save**.

Troubleshooting Application Usage Manager

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA application usage management feature.

Log Files

RCA writes several logs on the Core server and the client side that you can use to track the Knowledge Base server process and to diagnose problems.

Server logs

You can access the Knowledge Base server logs from the location `<InstallDir>\Knowledge Base Server\logs`.

Knowledge Base server: Log files

Log File	Description
mmyyyy `RADKBMGR.0.0.log`	Contains log messages related to the data that is imported from the `USDBase` file to the RDMBS.

Client logs

You can access the Application Usage Manager agent log files from the location `<InstallDir>\AUM Agent\Usage Manager\log` on the RCA agent device.

Application Usage Manager agent: Client log files

Log File	Description
`connect.log`	Contains log messages related to the three RCA agent modules, `RADSKMAN`, `RADPINIT`, and `RADCONCT`.
`Usage_Log_For_<Date>.csv`	Records the log messages when the `USDBase` file is sent to the Core

Log File	Description
where *Date* is the current date when log is created.	server or to the collection point. To enable debug mode logging for this log file, create a new registry string value with the (name, value) pair as `(debug,1)` in one of the following registry paths, based on your operating system: For a 32-bit operating system: `HKEY_LOCAL_MACHINE\SOFTWARE\Novadigm\Application Extensions\Usage Manager\` For a 64-bit operating system: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novadigm\Application Extensions\Usage Manager\` After creating the registry setting, restart the Application Usage Manager Service (`AUMService`).

Problems and Solutions

This table lists the problems that may occur when you are using the RCA usage management feature.

Usage management: Problems and solutions

Problem	Solution
The Usage Management reports appear blank after deploying the Application Usage Manager agent on the target device. Additionally, the `USDBase` file size is 1 KB.	This problem occurs if the usage management filters are disabled. By default, none of the usage management filters are enabled. After installing RCA Core server, use the following steps to enable the usage filters: 1. Log on to the RCA Core Console and click **Operations** tab. 2. Expand **Usage Management**, and then click **Collection Filters**. 3. Select the collection filters you want to enable, and then click **Enable Selected Items**. 4. Click **OK**.
After you update the database settings, the Knowledge Base server stops importing the `USDBase` files.	After modifying the database settings, restart the `HpKbmanager.exe` service.
In the Reporting home page, the Monthly Usage by Product report shows `[undefined]` value in the Product Name column.	The usage manager extracts the application information from the application header. If the application header does not contain the Product Name or Vendor information, the value of Product Name or the Vendor Name field is set as `[undefined]`.

Problem	Solution
	Additionally, the Application Usage Manager agent is not localized, therefore, for localized applications, this field is set as `[undefined]`.

Troubleshooting Reporting Server

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Reporting server.

Log Files

RCA writes several logs on the server side that you can use to track the Reporting server process and diagnose problems.

You can access the Reporting server log files from the location `<InstallDir>\ReportingServer\log`.

Reporting server: Log files

Log File	Description
`results.log`	Contains log messages related to the query results.
`export.log`	Contains log messages related to the communication between the Reporting server and other RCA components.
`navigate.log`	Contains log messages related to the tasks performed on the left pane in Reporting server home page, that you access using the RCA Core Console.
`startup.log`	Contains log messages related to the Reporting server startup page.
`content.log`	Contains log messages related to the Reporting server initialization activities.

Problems and Solutions

Problem	Solution
When accessing the Reporting tab from the Core Console, the Reporting page hangs while displaying the navigation bar (`navigate.tcl`) or the reports (`results.tcl`).	Change the file permissions of `C:\WINNT\Temp`, including subfolders, to allow everyone full control.
On the Reporting home page, the managed and scanned device count is zero for Compliance Management, Vulnerability Management, and Security Tools Management dashboard.	This problem occurs if the Reporting server database and the CSDB are not in synch for the content that has been downloaded from the HP Live Network. To manually run this synch operation, complete the following tasks: 1. Logon to the RCA Core Console and click the

Problem	Solution
	Operations tab. 2. Expand Infrastructure Management and click **Live Network**. The Live Network view opens in the details pane. 3. In the HP Live Network Updates section, click **From the Configuration Server Database**, and click **Save**. For more information on HP Live Network updates, see the Operations chapter in the *Radia Client Automation Enterprise User Guide*.

Troubleshooting Virtual Application Management

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA virtual application management feature.

Log Files

RCA writes a few logs, which can be used to track progress and diagnose problems related to ThinApp and Microsoft App-V applications management.

Virtual Application Management: Server side Log Files

Log File	Description
`discover-thinapps.log`	Contains log messages related to ThinApp packages discovered in the database, status of the download of ThinApp packages, and status of publishing of ThinApp packages. This file is located at *<InstallDir>\ThinApp\logs*.
`vms_server.log`	Contains log messages related to the App-V packages that you publish to the CSDB. This file is located at *<InstallDir>\VulnerabilityServer\logs*.

Virtual Application Management: Client side Log Files

Log File	Description
`Appsync.log`	Contains log messages related to success, failure, or warning status for the AppSync.exe utility. This file is located at *<InstallDir>\Agent\logs*.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA virtual application management feature.

Virtual application management: Problems and solutions

Problem	Solution

The following error message is logged in the `Appsync.log` file on the agent computer:
`Error: AppSync.exe not found at C:\PROG~1\ HEWLET~1\ HPCA\ Agent. Exiting…`
`AppSync.exe does not exist on agent system.`
	The ThinApp Updater script (`updatethinapp.tcl`) that runs on an agent computer requires that the VMware AppSync executable (`AppSync.exe`) exists in the `IDMSYS` (Agent) directory on the agent.
	Because of licensing restrictions, this executable is not included with the ThinApp Updater (`HPCA_THINAPP`) service. You must obtain this from VMware as part of the VMware ThinApp and distribute this to the agent computers using an appropriate method, subject to VMware licensing restrictions.

After publishing a ThinApp application, you cannot locate the ThinApp MSI file in the *<InstallDir>*`\Media\virtual\thinapp\`*<Product>* directory on the Core server.	This problem occurs if the `discover-thinapps.tcl` is not run after publishing a ThinApp MSI. To resolve this problem, run the `discover-thinapps.tcl` script in the *<InstallDir>*`\ThinApp` directory, after publishing the ThinApp MSI packages to the CSDB. This script extracts the ThinApp MSI from the CSDB for each product, and place the executable in the *<InstallDir>*`\Media\virtual\thinapp\`*<Product>* directory.
After the VMware ThinApp Sync job completes successfully on an agent computer, the ThinApp application does not work.	This problem occurs if the ThinApp application that you have deployed contains more than one executable file. There is no solution to this problem. This is a limitation in the current version of the AppSync utility.
The VMware ThinApp Sync job does not update the ThinApp application on the agent system, though the correct version of the ThinApp exists in the *<InstallDir>*`\Media\virtual\thinapp\` *<Product>* directory on the Core server. The following	This problem occurs if the ThinApp application deployment settings are not consistent in `package.ini` file and the settings that you provide while publishing the ThinApp application. If you uncomment the line `AppSyncURL` in `package.ini` while packaging the ThinApp,

Problem	Solution
message is logged in the `appsync.log` log file on the agent computer: `No updates available`	click **Yes** for the `Enable AppSync?` prompt that you receive while publishing the ThinApp application. If you comment out the `AppSyncURL` settings in the `package.ini`, click **No** to the `Enable AppSync?` prompt while publishing the ThinApp application.
The updated ThinApp application does not show the correct `Product Name`.	This problem occurs if there is an inconsistency in the value of the Inventory Name parameter in the ThinApp `package.ini` file. The value of this parameter must be same for each version of the application. Although the new version is placed in the `InstallDir/media/virtual/thinapp/<product_name>` directory, the update utility cannot search for this newer version because it uses the old name to check for the updates. This value is set during the VMware ThinApp Setup Capture by specifying the Inventory Name or explicitly modifying the `package.ini` file. If the value is not same, the agent computer shows the old version of the application, even if you have entitled the agent computer to receive the updated version.
The version number is not updated after the updated ThinApp application has been installed.	This problem occurs if the `Product Version` property is not set appropriately when packaging the updated ThinApp application. To resolve this problem, increase the value of the `MSIProductVersion` parameter in the `package.ini` for each new version.
The ThinApp application does not appear on the agent computer.	Entitle the agent computer to the *base* version of the ThinApp service.
You are unable to discover the ThinApp services on an agent computer.	The following list provides the possible causes and solutions for this problem: • **Cause**: The `APPTYPE` attribute for `ThinAppStrm` is not set for the packaged ThinApp service (`ZSERVICE`). The `discover-thinapps.tcl` script uses the `APPTYPE` attribute to determine which `ZSERVICE` contains AppSync enabled ThinApp applications. This value is set

Problem	Solution
	using the RCA Administrator Publisher. **Solution**: Enable auto-update via AppSync when you publish the ThinApp application. • **Cause**: The `APPTYPE` attribute is not set for the `ZSERVICE` in the custom domain. **Solution**: Check if the `THINSYNC` instance exists in the Custom domain and `HPCA_THINAPP` appears in the Service list of the Custom domain. Also, make sure that the `AppSync.exe` is available in the `<InstallDir>\Agent` folder on the agent computer.

Troubleshooting SSL

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA SSL feature.

Log Files

RCA writes several logs that you can use to track secure communication and diagnose problems. You can access the log files from the location *<InstallDir>*`\ApacheServer\logs`on RCA Core or RCA Satellite servers.

The following table lists the log files that help troubleshooting SSL in RCA environment.

SSL: Log Files

Log File	Description
`ssl_access.log`	Contains log messages that provide details of all SSL requests including corresponding resource being requested, HTTP response code, resource size and so on.
`ssl_error.log`	Contains log messages that provide details of all warnings and errors encountered during SSL enablement in RCA environment.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA SSL feature.

SSL: Problems and solutions

Problem	Solution
The following error appears while installing a Certificate Generation Utility program on RCA server:	This problem occurs if the RCA server already contains a different version of the Certificate Generation Utility.

Problem	Solution
`A certificate or private key already exists for the specified server name. Choose another server name.`	To resolve this problem, perform one of the following steps: • In the Review and Password window, change the name in the text box Server to Generate For and try again. (This generates a new server certificate request for the server that is identified in this text box.) • Cancel the installation (since a server certificate request and private key already exist for this server).

The secure communication between one of the following fails:
• RCA Core server and RCA Satellite server
• RCA Satellite server and RCA Satellite server
• RCA Agent server and RCA Core server
• RCA Agent server and RCA Satellite server
	There could be various reasons for secure communication failure in your environment.
	• Expired certificates
	• SSL port not enabled
	• Signed certificate is not set
	• Host name mismatch
	Solution:
	• If you discover that the certificate is expired, on the RCACore or Satellite servers, use the current version of the Certificate Generation Utility to create new certificates, new keystore and truststore files.
	• Verify that the correct port is enabled.
	• Make sure that signed certificate is set.
	• The form of the host name, simple or fully qualified, must also match.
	For example, if you use the Certificate Generation Utility to create certificates using this command:
	`cert_mgr create signed –hostname cmserver1.mycorp.com`
	You must use the following URL to create the SSL connection:
	`https://cmserver1.mycorp.com:SSLport/Console`
	where:
	SSLport is the SSL port configured on cmserver1.mycorp.com

Problem	Solution
The following message is logged in the `RCA-PS-3481.log` on RCA Core or Satellite servers. Similar error is logged in the `ssl_error.log` file on RCA Core. `20050621 21:49:11 Warning: TLS startup failed: Certificate "D:\Program Files\Hewlett-Packard\HPCA\IntegrationServer\etc\Certificates\server.HP.comcert.pem" not found.`	Make sure that the signed certificate is set.
The following message is logged in the HPCA-PS-3481.log on RCA Satellite server. Similar error is logged in the `ssl_error.log` file on RCA Core server. `20050621 22:10:08 Warning: TLS startup failed: LAVENEL1:443 couldn't open socket: address already in use`	Make sure that the SSL port is not in use by another application.

Troubleshooting OpenLDAP Directory Service

This section describes the log files, and the cause and solutions for the problems that you may observe while using the OpenLDAP directory service. You can access the directory services log file from the location `<InstallDir>\PolicyServer\logs`.

OpenLDAP Directory Service: Log Files

Log File	Description
`ldap-n` where `n` is a positive integer.	Contains log messages that Policy server creates to handle simultaneous LDAP connections. The LDAP connections are named as ldap-1, ldap-2, and ldap-n. In this instance, n is a positive integer.
`ldap-hpca-internal.log`	Contains log messages that provide debug information of the LDAP connections connecting to the RCA OpenLDAP.

Setting Debug Level

If you observer OpenLDAP specific errors, it recommends that you turn ON additional logging.

To set the debug level:

1. Stop the RCA Directory Service service.
2. Update the following registry entry:
   - 32-bit computer: Update the `HKEY_LOCAL_MACHINE\Software\HPCA-DS\` registry entry `DebugLevel` (a REG_DWORD).
   - 64-bit computer: Update the `HKEY_LOCAL_MACHINE\Software\Wow6432Node\HPCA-DS\` registry entry `DebugLevel` (a REG_DWORD).
3. Restart the RCA Directory Service service.

Debug Levels

Keyword	Description
-1 (any)	Enables all debugging
0	No debugging
1 (0x1 trace)	Trace function calls
2 (0x2 packets)	Debug packet handling
4 (0x4 args)	Heavy trace debugging
8 (0x8 conns)	Connection management
16 (0x10 BER)	Print out packets sent and received
32 (0x20 filter)	Search filter processing
64 (0x40 config)	Configuration processing
128 (0x80 ACL)	Access control list processing
256 (0x100 stats)	Stats log connections/operations/results
512 (0x200 stats2)	Stats log entries sent
1024 (0x400 shell)	Print communication with shell backends
2048 (0x800 parse)	Print entry parsing debugging
16384 (0x4000 sync)	Syncrepl consumer processing
32768 (0x8000 none)	Only messages that get logged whatever log level is set

Note: The debugging levels can be logically added, so if you want both stats log `connections/ops/results` as well as replication information (syncrepl consumer processing), add 256 + 16384 and use that value (i.e. 0x4100).

In general, 256 (0x100) generates useful debugging information. Also, note that OpenLDAP generates a log of logging, so only enable this temporarily until the error is shown in the logs, then disable it.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA OpenLDAP directory service.

Directory Services: Problems and solutions

Problem	Solution
You are unable to log on to the Console. or Policy resolution is not happening.	These problem can occur when the RCA directory service stops working. To resolve these problems, complete the following steps in the mentioned order to make sure that your directory service is working: 1. Stop the HPCA Directory Service service. 2. Open command prompt and navigate to the following directory: `<InstallDir>\Directory Service`. 3. Run the following command: `slapd.exe -h ldap://localhost:3474/ -f slapd.conf -d 256` 4. Save the output to a temporary text file. ▪ If there server did not start properly, one of the following errors are listed in the output. Check the respective log file to know the issue and how to resolve it. ◦ Database not properly shutdown ◦ PANIC ◦ Fatal Region ◦ Internal error ▪ If the server starts properly, the following entry is listed in the output: `slapd starting` Stop the `slapd.exe` command line by pressing `CTRL+C` and start the RCA Directory Service.
How to recover the OpenLDAP database.	Recover the OpenLDAP database by completing the following steps: 1. Stop the RCA Directory Service service. 2. Open the command prompt and navigate to the directory `<InstallDir>\Directory Service`. 3. Run the following command twice, and save the output each time you run this command: `db_recover -e -h Database/rmp` If there are no errors during the second run, the database recovery is complete. Start the RCA Portal service and other RCA services. However, if you observe error messages in the output, contact Persistent Support.
Restoring	If you have a backup copy of the OpenLDAP Database (the files in

Problem	Solution
backup copy of the OpenLDAP database	`<InstallDir>\Data\DirectoryService`), and perform the following steps to restore the database. 1. Stop the HPCA Directory Service. 2. Save a copy of current `<InstallDir>\Data\DirectoryService\rmp\` directory. 3. Copy the backed up files in the `<InstallDir>\Data\DirectoryService` directory. 4. Restart the HPCA Directory Service.

Troubleshooting Policy Server

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Policy server service.

Log Files

RCA writes several logs that you can use to track the Policy server process and diagnose problems. You can access the log files from the location *<InstallDir>*`\PolicyServer\logs`.

The following table lists the log files available for troubleshooting the Policy server component.

Policy Server: Log Files

Log File	Description
`HPCA-PM-3468.log`	Contains log messages that provide details of policy store, policy resolution status, and services resolved.
`httpd-3468.yy.mm.dd.log`	Contains log messages for Integration server and show the status of the access requests. The log messages are maintained in date and time format.
`httpd-3468.error.log`	Contains log messages that contain error messages occurring in integration server. The log file also provides log messages that occur during shutdown.
`ldap-n.log` In this instance, n is a positive integer.	Contains log messages that Policy server creates to handle simultaneous LDAP connections. The LDAP connections are named as ldap-1, ldap-2, and ldap-n. In this instance, n is a positive integer.
`ldap-hpca-internal.log`	Contains log messages that provide debug information of the LDAP connections connecting to the RCA OpenLDAP.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Policy Server service.

Policy server: Problems and solutions

Problem	Solution
Policy Flush Errors in the Policy Server Log with Agents receiving a 650 error	This problem occurs when a number of agents try to connect to the Core server at the same time. To resolve this problem, complete the following steps to tune the `TASKLIM` and `HTTP_TIMEOUT` parameters as follows: 1. Stop the RCA Configuration Server service. 2. Navigate to the `<InstallDir>\ConfigurationServer\bin` directory. 3. Use a text editor to open the `edmprof.dat` file. 4. In the `[MGR_TASK_LIMIT]` section, modify the value of `TASKLIM` based on the number of agents that you expect to connect simultaneously. 5. In the `[MGR_POLICY]` section, add `HTTP_TIMEOUT` and set it to a value based on the number of agents that you expect to connect simultaneously. Add `HTTP_TIMEOUT` at the end of the section. `HTTP_TIMEOUT` is the time for which the HTTP connection waits to receive the request before closing the connection. 6. Save and close the `edmprof.dat` file. 7. Start the RCA Configuration Server service.

Troubleshooting Mobile Server

This section describes the log files, and the cause and solutions for the problems that you may observe while using the RCA Mobile Server.

To troubleshoot RCA agent issues on iOS operating system-based devices, you can install the iPhone Configuration Utility from the Apple website at http://support.apple.com/kb/DL1466. This utility enables you to view the device console and track the device activity.

Log Files

The Mobile Server writes several logs, which can be used to track progress and diagnose problems. The log files are stored by default in *<InstallDir>*\MobileServer\logs .

Mobile Server: Server Log Files

Log File	Description
`HPCA-MDM-`*`port`*`.log` where, port is the Mobile Server port	Contains log messages related to the tasks that the Mobile Server performs. For example, details about communication between Configuration server and all mobile agents. Each time you start the web server a new log is written, and the old log is saved as `HPCA-MDM-`*`port.nn`*`.log`.

Log File	Description
number.	
`httpd-`*`port.YY.MM.DD`*`.log`	This log contains the web server activity for each day. If the log file is empty, no web server activity was performed on that day.
`httpd-`*`port`*`.error.txt`	Contains a consolidated list of error messages. All log messages that are prefixed ERROR are written to this log file, enabling you to view all error messages at a single location.

Setting Trace Levels

By default the trace level is set to 3, which is the informational tracing level, and enables the logging of INFO, WARNING, and ERROR messages.

To change the trace level for the logs:

1. Open the file `HPCA-MDM.rc` from the location <*`InstallDir`*>`\MobileServer\etc\`.
2. Type `LOG_LEVEL` and the appropriate trace level, space delimited, within the `Overrides Config` section starting and ending brackets { }. Set the trace level using the options listed in the following table:

   Trace Levels

Trace Level	Description
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. Recommended trace level setting for customers.
4	Logs all debug information. *Recommended for experienced customers only*.
5 - 9	Full trace *Not recommended for customer use*.

3. Save the file, and then restart the HPCA Mobile Server Service.

Problems and Solutions

This section lists the problems that may occur when you are using the RCA agent for mobile devices.

RCA Agent: Problems and Solutions

Problems	Solutions
You receive the following error message during agent installation on an iOS operating system based device: `Cannot install profile`	This problem can occur due to one of the following reasons: • SSL certificate settings on the Core server are not configured correctly • Synchronization between the Core and Satellite server is not complete • Agent cannot connect to the RCA servers because of network connection error. You can view the complete error details in the Mobile server and Mobile Device Management (MDM) server log files available at the following locations: • Core server and Satellite server: `<InstallDir>\MobileServer\logs\HPCA-MDM-3482.log` • Satellite server only: `<InstallDir>\tomcat\logs\mdm.log`

Chapter 3

Troubleshooting RCA Satellite Server

This chapter covers problems and possible solutions for components that are installed on the RCA Satellite server. Additionally, this chapter also provides the list of log files for each component.

Log Files

The different components installed with the RCA Satellite server write the log files listed in the following tables:

Configuration Server Log Files

The Configuration server log files on the Satellite server are similar to the log files created by the Configuration server on the RCA Core server.

For the list of Configuration server log files created on the RCA Core server, see "Log Files" on page 14. You can access these log files from the location `<InstallDir>\ConfigurationServer\logs`.

Proxy Server Log Files

RCA writes several logs that can be used to track Proxy server process and to diagnose problems. You can access these log files from the location `<InstallDir>\ProxyServer\logs`.

Proxy server: Log files

Log File	Description
`httpd-port.log` where, *port* number is the Proxy server port number.	Contains log messages related to Proxy server activities of the TCL web server that it runs on.
`httpd-port.YY.MM.DD.log`	Contains log messages related to the web server activity for each day. If the log is empty, it means that there was no activity for that day.
`httpd-port.error.log`	Contains a consolidated list of error messages. All log messages that are prefixed ERROR are written to this log file, enabling you all error at a single location.
`hpca-ps-<port>.log`	Contains log messages related to Proxy server activities, such as starting proxy server, stopping proxy server, and synchronization status.
`CONNECT.LOG`	Contains log messages related to the preload data and the agent modules that are invoked when the Proxy server connects to the Configuration server

Log File	Description
	to preload the static cache. Each time you start the web server a new log is written. The old log is saved as `httpdport.nn.log`. You can access this log file from the location `<InstallDir>\ProxyServer\logs\rps`.

Application Usage Manager Log Files

RCA writes several logs that can be used to track Knowledge Base server process and to diagnose problems.

You can access the log files from the location `<InstallDir>\MessagingServer\logs`.

Application Usage Manager: Log Files

Log File	Description
`rms-usage.aggregate-x.log`	Contains log messages related to aggregation package data on a Satellite server.
`USDBAggr_Log_For_yyyymmdd.log`	Contains log messages related to the aggregation process, and how the aggregation data was processed. The information in this log file is populated only when aggregation is enabled on the Satellite server.

Patch Manager Server Log Files

RCA writes the `patchgw.log` file on the Satellite server, if the Patch Management Gateway is enabled. You can use this file to track the Patch Manager Gateway process and diagnose problems.

You can access this log file from the location `<InstallDir>\ApacheServer\apps\patchgw\logs`

Patch Manager Server: Log files

Log File	Description
`patchgw.log`	Contains log messages related to the Patch Management Gateway transactions on the Satellite server.

Mobile Device Management Server Log Files

RCA writes the `mdm.log` file on the full-service Satellite server that is enabled for managing iOS operating system-based mobile devices. You can access this log file from the location `<InstallDir>\tomcat\logs`.

Mobile Device Management Server: Log files

Log File	Description
`mdm.log`	Contains log messages related to the MDM server activity.

Setting Trace Levels

By default the trace level is set to 3, which is the informational tracing level, and enables the logging of INFO, WARNING, and ERROR messages.

To change the log level, perform one of the following options:

- Using command prompt:
  a. Open command prompt and navigate to the <InstallDir>\ProxyServer directory.
  b. Run the following command:
  `nvdkit-hpca-ps.exe httpd.tkd -log_level 4`
- Using HPCA-PS.rc configuration file:
  a. Stop the RCA Proxy Server service.
  b. Open the HPCA-PS.rc file from the location <InstallDir>\ProxyServer\etc.
  c. Type LOG_LEVEL and the appropriate trace level, space delimited, within the Overrides Config section starting and ending brackets { }. Set the trace level using the options listed in the following table:

Trace Levels

Trace Level	Description
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. *Recommended trace level setting for customers*.
4	Logs all debug information. *Recommended for experienced customers only*.
5-9	Full trace *Not recommended for customer use*.

  d. Save the file, and the restart the RCA Proxy Server service.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Satellite server.

RCA Satellite server: Problems and solutions

Problem	Solution
You are experiencing performance issues for HPCA httpd.tkd-based modules in a Windows environment.	This problem occurs if the value for registry IRPStackSize is set to a non-recommended value. Typically, anti-virus software programs reset the value for this entry, causing performance issues for HPCA httpd.tkd-based modules.

Problem	Solution
	Verify the value for IRPStackSize from the following registry location: `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]` Use your operating system's registry editor to check this value. If the value is less than the recommended value, create a backup of the Windows Registry, and then increase the IRPStackSize value to be within the recommended range. To obtain the recommended values for IRPStackSize as well as detailed instructions of how to change the IRPStackSize value, see the following Symantec and Microsoft web sites: • How to Change the IRPStackSize for Computers registry value • IRPStackSize Parameter Windows 2003 • Antivirus Software May Cause Event ID 2011 **Note:** For Windows Server 2003, the IRPStackSize value is not created during installation. If the value is not set, the default value is used, which does not create any performance problems. If IRPStackSize is set, make sure that the value is as per the recommended standards.

Any of the following error message is logged in the `connect.log` file during preload process:
`13:43:36 Warning: RPS/Static: sync: Radskman rc:[109] [Presently there are no applications available in the software catalog. Please contact your system administrator for assistance.] (CHILDSTATUS -1 109)`
or
`[17:10:21 [RADCONCT / 000005a4] SYSTEM --- RADCONCT exit status [650]`
	• Verify that the user specified in the `_static_user` parameter in the `rps.cfg` file matches with the user defined in the Policy domain on the Core server. The `rps.cfg` file is available at InstallDir`\ProxyServer\etc`.
	• You have not entitled any services or applications to the user specified in `rps.cfg` file. Entitle services and applications to the user.

Problem	Solution

`[17:10:21 [RADCONCT / 000005a4] SYSTEM --- RADCONCT [Server stopped application configuration.]`
 	
`NVD000010A [radconnect_ term] 17:10:21 [RADCONCT / 000005a4] SYSTEM --- RADCONCT Return Code [650]`
 	
`NVD000005E [radconct_ cleanu] 17:10:21 [RADCONCT / 000005a4] SYSTEM --! RADCONCT Exit code [650]`	

The following error message is logged in the `HPCA-PS-<port>.log` when you start the Satellite server synchronization process from the RCA Core Console: `Sync Failed`	Add the IP address and hostname of the Satellite server in the host file located in the `SystemDrive\Windows\System32\drivers\etc` folder, and then synchronize the Satellite server.
The Satellite server data cache usage does not appear in the RCA Satellite Console, however, the log file `HPCA-PS-<port>.log` shows `RC=0` or `[RC:0]`, which indicates that the synchronization was successful.	Complete the following steps to make sure that the data is preloaded to the Satellite server: 1. Verify the Satellite server preload options: a. Log on to the RCA Core Console and click **Configuration** tab. b. Expand **Infrastructure Management,** and then click **Satellite Management**. c. Click the Satellite server from the Hostname column to open the Server Details window. d. Click **Cache** tab and make sure that the preload option is enabled for Software, Patch, and OS, as per your requirement. 2. Verify that the upstream server details are correct. Also, make sure that you are able to ping the upstream server successfully.
The file size of memory dump files in the Apache log directory is greater than 1 GB.	To resolve this problem, complete the following steps: 1. Open the configuration file `httpd.conf` from the location *InstallDir*`\apacheserver\conf`. 2. Add the parameter `TclDumpEnable off` in the configuration file to turn ON the creation of memory dump files. 3. Restart the RCA Apache Server service.

Chapter 4

Troubleshooting RCA Administrator Tools

This chapter covers problems and possible solutions for RCA Administrator tools.

Log Files

RCA writes several logs on the computer where you run the RCA Administrator tools. You can use these log files to track the Administrator Tools process and diagnose problems.

You can access the Administrator Tools log files from the location `<InstallDir>\Agent\Log` on the computer where the RCA Administrator tools are installed.

RCA Administrator tools: Log files

Log File	Description
`pubport.log`	Contains log messages related to the RCA Administrator Publisher.
Radxplor.log	Contains log messages related to the RCA Administrator CSDB Editor
publishr.log	Contains log messages related to the RCA Administrator Packager
NvdObjed.log	Contains log messages related to the RCA Administrator Agent Explorer
ampedit.log	Contains log messages related to the AMP Editor.

Problems and Solutions

This table lists the problems that may occur when you are using the RCA Administrator tools.

Administrator tools: Problems and solutions

Problem	Solution
Published packages that only contain registry keys have connection to the FILE and PATH instances that do not	The RCA Administrator Publisher populates the FILE and PATH instances even though there are no connections specified for the FILE and PATH instances. This issue does not affect the deployment of the packages. You can safely ignore this issue.

Problem	Solution
exist.	
Publishing Windows Installer file using RCA Admin-istrator Publisher takes long time to respond.	This problem occurs if large number of files are present in the same directory location as the Windows Installer file that you want to publish. Place the Windows Installer file in a separate location along with the additional files that you want to package.
You cannot publish native Linux software packages.	Contact Persistent Support. Perform the following steps before you contact Persistent Support: • Enable full diagnostic tracing by appending the text `-debug all` to your command line and rerun the publishing session. • Generate the RCA Native Packager publishing log file (`publish.log`) readily accessible to provide to support. By default, this log file is stored in the directory where you installed the RCA Batch Publisher. **Note:** You should only use the command-line option `-debug all` to diagnose publishing problems.
Publisher UI does not display applications to be published on a 64-bit Windows system.	Place the files that you want to publish under `C:\Windows\SysWOW64\`. On a 64-bit system, Publisher is redirected from `C:\Windows\System32` to `C:\Windows\SysWOW64\`.
Application Self-Service Manager UI does not show the updated list of services entitled to a user.	This problem occurs if you have published an application for a user on 32-bit computer using RCA Administrator Publisher installed on a 64-bit computer. Republish the applications that should be deployed on a 32-bit computer using the RCA Administrator Publisher installed on a 32-bit computer.
You are unable to log on to the	Make sure that the user account does exist in Active Directory and the RCA Policy Server service is running.

Problem	Solution
CSDB Editor or Publisher.	
You are unable to connect to the CSDB Editor after providing valid login credentials.	Make sure that the RCA Configuration Server service is running. Additionally, check that the following registry entry is set: For a 32-bit computer: `HKEY_LOCAL_MACHINE\SOFTWARE\Novadigm\Radia\Settings\INIPath` For a 64-bit computer: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novadigm\Radia\Settings\INIPath`
Accessing RCA CSDB using RCA Administrator CSDB Editor gives an INVALID USER ID error	This problem occurs because of either of the two reasons: • The external user account specified in the Directory Service is not configured to access the RCA CSDB. Solution: Configure the user account to access the RCA CSDB using Directory Services. For information on how to configure Directory Service external user accounts, see *Accessing RCA Administrator Tools using Directory Services* appendix in *Radia Client Automation Enterprise Administrator User Guide*. • The Directory Service is not configured in the RCA Core Console. Solution: Configure the Directory Service using the RCA Core Console. For more information on how to configure the external Directory Service using the RCA Core Console, see the *Directory Services* explained in the section *Infrastructure Management* in the *Radia Client Automation Enterprise User Guide*.
Accessing RCA CSDB using RCA Administrator CSDB Editor gives an NO ACCESS error	The external user account specified in Directory Service is not configured properly. Perform the required steps to configure the external user accounts in RCA Administrator CSDB Editor. For information on the configuration steps, see *Accessing RCA Administrator Tools using Directory Services* appendix in *Radia Client Automation Enterprise Administrator User Guide*.

Chapter 5

Troubleshooting RCA Agent

This chapter covers problems and possible solutions for RCA agent.

Log Files

The log files available on an RCA agent device may vary based on the functionality implemented in your RCA environment. Note that the log files listed in the section are the generic log files. For details on the agent log files pertaining to a specific feature, for example patch management, see the respective log files section in the chapter "Troubleshooting RCA Core Server" on page 10

You can access the agent log files from the location `<InstallDir>\Agent\log` on an RCA agent device.

Agent: Log Files

Log File	Description
`connect.log`	Contains log messages related to the activity-reporting of three RCA agent modules `RADSKMAN`, `RADPINIT`, and `RADCONCT`. is shared in this one log file. When `connect.log` file reaches 1 MB in size, a backup log `connect.bak` is created. You have an option to create different log files for different commands such as `RADSKMAN`, `RADPINIT`, and `RADCONCT`. For more information on how to create these log files, see *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.
`radalert.log`	Contains log messages related to hardware failures, such as disk failure and fan failure.
`radexecd.log`	Contains log messages related to the `Notify` daemon. This log provides information on the remote and local notify requests to the agent computer.
`radiafd.log`	Contains log messages that provide communication details for each file requested by the MSI that is to be deployed on the agent computer. This log is updated only when the MSI is published in advanced publishing mode.
`radstgms.log`	Contains log messages related to the `MSI Redirector` daemon. The MSI redirector is used during deployment of MSI applications that are published in advanced mode.
`radsched.log`	Contains log messages related to the `Scheduler` daemon. This log contains information on timer based communications on the agent computer. For each communication, the log contains information on the module that was run, and whether it was successful or not.
`radshist.log`	Contains log messages that provide history of all commands run by the

Log File	Description
	timer.
`radstate.log`	Contains log messages related to the current state and version details (for example, DLL version, patch level, last modified date) for all agent modules. This log also provides summary of all services deployed on the agent computer, per domain.
`radtray.log`	Contains log messages related to the communications between the different agent modules and the RadTray.
`upgrdmaint.log`	Records log messages when you perform agent maintenance tasks, such as apply a hotfix, a patch, or when you upgrade the agent. This is a detailed log and provides information on which modules are called or replaced during the maintenance tasks. The log also provides details on the MSI drivers that are installed during the maintenance.
`upgrdmaint_setup.log`	Records log messages when you perform an agent upgrade or apply a patch. Compared to the `upgradmaint.log` file, this log provides minimum details.

Message Logs

An RCA agent generates various types of messages during the connect process. All these messages are numbered and logged in the message log files. The messages that RCA can produce during the connect process are organized into the following categories:

- API Errors
- Catalog Processing
- Client Processing
- External Data Download Codes
- Client Automation Internal Errors
- Invalid Data Errors
- Method Execution Errors
- SAP Errors
- Server Errors
- SSL Errors
- Transmission Errors
- User Exceptions
- User Interface Errors
- Verification Errors

These categories are high-level indicators of which part of the connect process is active when the message is produced. There are two types of messages:

- **Note messages**: Provide information about a condition that allows the connect process to continue.
- **Error messages**: Describe a condition that prevents the connect process from proceeding to a successful completion.

Note: For details on each Note or Error message that an RCA Agent can generate, see *Radia Client Automation Reference Guide*.

When a message is issued, its number and text are recorded in the appropriate log on the user's computer. The log files are located in the `log` subdirectory of the directory in which the RCA agent was installed. The default directories for log files are listed below.

- For Windows: `C:\Program Files\Hewlett-Packard\HPCA\Agent\log`
- For Linux and Macintosh: `opt/HP/HPCA/Agent/log`

The messages are written in the following three files:

- `RADPINIT.LOG`
- `RADCONCT.LOG`
- `RADAPI.LOG`

If the cause of an error is not immediately apparent by reading the log, note the steps that were performed immediately before the message appeared.

Caution: Do not modify RCA until the log files are copied to a backup location. This will preserve information that might prove valuable in resolving the issue.

Setting Trace Levels

Use the Diagnostics (DIAGS) class to override default trace settings on the RCA agent computer. Instances of the DIAGS class enable you to set tracing levels as well as RADSTATE parameters for a user, a machine, or a group of users.

To set the tracing level, complete the following steps:

1. Set the _ALWAYS_ Diagnostics Class connection in LOCATION._BASE_INSTANCE_ to `DIAGS.&(ZCONFIG.ZHDWCOMP.`
2. Create an instance in the DIAGS Class with the computer name of the RCA agent computer for which you want to set the tracing. If the machine name does not exist in the DIAGS Class, the DEFAULT_DIAGS instance settings will be used.

The following table describes the attributes of the DIAGS class:

Attributes of the DIAGS Class

Attribute	Description
NAME	The friendly name of the instance.
RADSTATE	Specify the parameters for RADSTATE to run. RADSTATE is a diagnostic

Attribute	Description
	module that is designed to give an overview of the current state of the RCA agent. If no parameters are specified, RADSTATE will not run. Note that RADSTATE must exist in the `IDMSYS` directory. The _BASE_ INSTANCE_ of the DIAGS Class is set to **VO**, which will run RADSTATE in verbose mode, building the ZRSTATE and ZRSTATES objects. Make sure that you specify the value for the radstate parameter as `MODE=VO`, and not as `radstate MODE=VO`. The information in the RADSTATE output is based on data that has been retrieved from numerous RCA agent objects. For additional information on RADSTATE, see the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.
ZTRACE	Specify whether communications tracing should be recorded to the RCA agent log file. • `N` (the default) turns off communication buffer tracing. • `S` provides summary communication buffer information to the RCA agent log. This includes the number of records read and written, and the type of records processed. • `Y` provides full communication buffer information to the RCA agent log. All data that has been transmitted and received will be echoed to the RCA agent log file. **Caution:** `ZTRACE=Y` could result in a large amount of data being written to the RCA agent log and could severely impact RCA agent performance. *Do not specify this setting unless instructed to do so by Persistent Technical Support*.
ZTRACEL	Specify the level of tracing (as `000`, `040`, or `999`) that will be recorded to the RCA agent log file. The tracing levels vary form 000 to 999. The default tracing level is set to 040. If no value is specified, the last value that was set at the agent is used. Setting ZTRACEL to a high number could result in a large amount of data being written to the RCA agent log and could severely impact RCA agent performance. *Do not specify this setting unless instructed to do so by Persistent Technical Support*.

Problems and Solutions

This table lists the problems that may occur with the RCA agent.

RCA Agent: Problems and solutions

-Problem	Solution
The Agent connect process fails.	There could be various reasons for the connect process failure. • Make sure that the Configuration server that Agent is connecting to is running. For more details, see Configuration Server section.

-Problem	Solution
	• Make sure that the CSDB is configured for the user and for managing the user's software applications. • Make sure that user's computer has sufficient available resources for the programs that are associated with the connect process, and for the management of the subscriber's software applications. • Make sure that the hardware and communication links are properly operating. For secure communication related problems, see SSL Troubleshooting section. Even with these conditions met during the connect process, other conditions can exist or events (such as the inadvertent deletion of needed files) can arise that prevent a successful completion. When this happens, RCA produces informational messages in the respective log files with the cause and suggested action, if any.
The RCA Agent maintenance fails from RCA Application Self-Service Manager on Windows Vista operating system.	Run the RCA Agent Maintenance through the RCA Application Manager by using the Notify scheduled connect or a logon script.
A message box indicating a `.tmp` file is in use is displayed while the RCA Application Self-Service Manager is used to upgrade the RCA Agent on Windows Vista operating system.	During the RCA Agent upgrade, close the message box by clicking **Ignore** or **OK**.
Application Self-Service Manager UI displays the status of an application installed when the installation process has failed.	Application Self-Service Manager depends on a return code to detect whether or not an application is installed successfully. This may happen if the installation program returned a zero upon failure. The installation program must return a non-zero code for the Application Self-Service Manager to detect the failure of the program. To obtain the status of the installation, create a custom script that launches the application and sends a return code signifying whether the script is able to launch the application or not. This return code is then passed to the Application Self-Service Manager. You must wrap this custom script with the installation to obtain the application installation status .
RADTRAY option is not available in the System Tray.	Probably machine connect is run on the system. Run user connect.

-Problem	Solution
Thin client device reboots indefinitely after installing RCA agent.	Make sure that RADALERT is disabled before you install RCA agent on thin client device. After the RCA agent is installed you can enable RADALERT using CSDB editor. To disable RADALERT on the thin client devices, follow these steps: 1. Log on to the CSDB editor on the Core server. 2. Expand the **PRIMARY.CLIENT.SETTINGS** class. 3. Double-click **Core Settings**. 4. Set the parameter `RALERTEN` to **N**.

On 64-bit Windows systems - Audit scan fails	Make sure that `msvcr71.dll` and `msvcp71.dll` are available on your Windows system in the following folder:
	
	For 32-bit
	
	`c:\Windows\system`
	
	For 64-bit
	
	`c:\Windows\SysWOW64`
	
	For Windows 7, make sure that you install SP1 or SP2 before running the audit scan.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to radiadocfeedback@persistent.co.in.

Product name and version: Radia Client Automation Enterprise, 9.00

Document title: Troubleshooting Guide

Feedback: