Universal CMDB

Software Version: 10.33

CMS Troubleshooting Guide

Document Release Date: August 2017
Software Release Date: July 2017

Legal Notices

Disclaimer

Certain versions of software and/or documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

MICRO FOCUS and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus (IP) Limited or its subsidiaries in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.softwaregrp.com.

This site requires that you register for a Software Passport and to sign in. To register for a Software Passport ID, click **Register for Software Passport** on the Micro Focus Support website at https://softwaresupport.softwaregrp.com.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Micro Focus sales representative for details.

Support

Visit the Micro Focus Support site at: https://softwaresupport.softwaregrp.com.

This website provides contact information and details about the products, services, and support that Micro Focus offers.

Micro Focus online 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 using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up Micro Focus support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as a Software Passport user and to sign in. Many also require a support contract. To register for a Software Passport ID, click **Register for Software Passport** on the Micro Focus Support website at https://softwaresupport.softwaregrp.com.

To find more information about access levels, go to: https://softwaresupport.softwaregrp.com/web/softwaresupport/access-levels.

Integration Catalog accesses the Micro Focus Integration Catalog website. This site enables you to explore Micro Focus Product Solutions to meet your business needs, includes a full list of Integrations between Micro Focus Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.softwaregrp.com/km/KM01702731.

Contents

About This Guide

This guide describes how to troubleshoot problems you may encounter when using HPE Configuration Management System components. It contains problems and proposed solutions to resolve them.

This chapter includes:

Intended Audience

This guide is intended for administrators and support engineers responsible for administering and maintaining CMS systems.

General Information

General information about HPE Configuration Management System can be found at https://saas.hpe.com/en-us/software/configuration-management-system-database.

HPE Websites

For additional information, see the following HHPE websites:

- http://www.hpe.com
- https://www.hpe.com/us/en/software.html
- https://softwaresupport.hpe.com/group/softwaresupport
- HPE Softwar Support Matrices site:
  https://softwaresupport.hpe.com/group/softwaresupport/support-matrices

Chapter 1: About Troubleshooting HPE Configuration Management System

This chapter includes:

How to Troubleshoot

To solve problems quickly and efficiently:

1. Make yourself familiar with the general troubleshooting information
2. Check if your problem is described in the **Universal CMDB Help Center**, the Release Notes or the troubleshooting sections of applicable guides:
   a. To troubleshoot Installation and Upgrade, see the *HPE Universal CMDB Deployment Guide*.
   b. To troubleshoot Integrations, see the *HPE UCMDB Discovery and Integrations Content Guide - HPE Integrations* or *HPE UCMDB Discovery and Integrations Content Guide - Third Party Integrations*.
   c. To troubleshoot Discovery, see the HPE Universal CMDB Discovery and Integrations Content Guide Help or the following:
      - *HPE UCMDB Discovery and Integrations Content Guide - Discovery Activities*
      - *HPE UCMDB Discovery and Integrations Content Guide - Discovery Modules*

- *HPE UCMDB Discovery and Integrations Content Guide - Supported Content*

d. To troubleshoot general administration or configuration tasks, see the *HPE Universal CMDB Administration Guide*.

3. If you cannot find a solution to your problem, report the problem to the HPE Customer Support Service. On how to prepare the required data for the support organization, see "Prepare the Generated Data to Be Sent to HPE Customer Support Service" on page 11.

General Checks

Before proceeding, ensure that:

- You are not running into known limitations that cannot currently be overcome. For specific information on Universal CMDB limitations and recommendations, as well as known Universal CMDB and non-Universal CMDB problems, see the *HPE Universal CMDB Support Matrix*, HPE Universal CMDB Release Notes or known issues in general across UCMDB. You can also check the Knowledge Base: https://softwaresupport.hpe.com/group/softwaresupport.
- Your problem is not related to third-party hardware or software. In this case, contact the vendor support.
- You have the latest Universal CMDB patches or hotfixes installed. Patches and hotfixes can be obtained from:
  - To check which UCMDB patches are installed on your system, go to the UCMDB Server JMX console and invoke the **UCMDB:service=Server Services > viewSystemInformation** JMX method.
- Check the if your problems is not a known issue or has a solution mentioned in the latest release notes:

  UCMDB Content Pack, UCMDB CUP, UCMDB Browser, or Discovery Knowledge Pack
- You have appropriate operating system patches installed
- The system is not running low on memory – there is sufficient resource allocation on the server
- Check the respective UCMDB logs for each type:
  - Client (UI) logs: **%temp%\UcmdbLog\log\applet-errors.log** (Windows)
  - Browser Embedded logs: **<UCMDBServer>\runtime\log\ucmdb_browser.log** or **warn_log**
  - Browser Standalone logs : **<WebAppServer>\<webappcontext>\<log_folder>**

- Server logs: **<UCMDBServer>\runtime\log\error.log**
- Probe logs: **<DataFlowProbe>\runtime\log\probe-error.log**

- Check if your problem is not described in the troubleshooting sections of applicable user guides.

Before Calling Support

This chapter includes:

Before Calling Your Support Representative

If you cannot solve your problem, report it. Before contacting the HPE Customer Support Service, ensure that:

- You have performed the general checks

  See "About Troubleshooting HPE Configuration Management System" on page 8.

- You have collected the relevant data about the problem you will send to the HPE Customer Support Service:

  a. A description of the problem, including timestamps if applicable.

  b. A description of your environment:

     i. Is this productions or test environment

     ii. Is it a new implementation – install or upgrade

     iii. Any environment changes prior to the encountered issue

     iv. Has the observed behavior ever functioned correctly previously

  c. Collect the output of the **viewSystemInformation** JMX method from the UCMDB server **JMX console > UCMDB:service=Server Services > viewSystemInformation**.

  d. Collect the relevant error logs from the General Check section

  e. Collect the output of Run Support Handlers from the UCMDB server **JMX console > UCMDB:service=Supportability Services > runSupportHandlersForSpecificCategories**, use empty categories.

The HPE Customer Support Service will then provide you with the further instructions. You might be asked to:

1. Enable UCMDB Debugging
2. Prepare the generated data for sending to the HPE Customer Support Service

Prepare the Generated Data to Be Sent to HPE Customer Support Service

The HPE Customer Support Service might ask you to gather and send the data they need to resolve a technical issue. Since UCMDB operates in large network environments, the data sometimes may be difficult to gather. The UCMDB LogGrabber is a tool for collecting and packaging log data. The methods to use the LogGrabber tool are described below.

Retrieve Server Logs by Executing LogGrabber

This task describes how to retrieve UCMDB Server log files.

- **If the UCMDB Server is operational**
  a. Launch the Web browser and enter the following address: **https://localhost:8443/jmx-console**

     You may have to log in with a user name and password. (Default user name is **sysadmin**)

  b. Search and click **UCMDB:service=Server Services** to open the JMX MBEAN View page.
  c. Click **executeLogGrabber**.
  d. Click **Invoke**.
  e. Provide the downloaded zip package to HPE Customer Support Service.
- **If the UCMDB server is not operational**
  a. Execute the LogGrabber script: **<UCMDB_Server_Home>/tools/logGrabber/logGrabber.bat**
  b. Clear the content of the following folder: **<UCMDB_Server_Home>/runtime/log**

     Make sure NOT to remove the **log** folder itself.

  c. Restart the UCMDB Server.

d. Allow some time for the problem to reproduce.

e. Execute the LogGrabber script again: **<UCMDB_Server_Home>/tools/logGrabber/logGrabber.bat**

f. Collect the most recent LogGrabber archive first from **<UCMDB_Server_Home>/runtime/logGrabber_xxx.zip** and upload it to the Support incident.

g. Once the upload completes in step f, inform Support and upload the LogGrabber output of Step a.

Retrieve Probe Logs

- If the Probe is operational

  a. Launch the Web browser and enter the following address: **https://localhost:8453/**

     You may have to log in with a user name and password. (Default user name is **sysadmin**)

  b. Go to **GeneralUtils**.

  c. Click **executeLogGrabber**.

  d. Click **Invoke**.

  e. Provide the downloaded zip package to HPE Customer Support Service.

- If the Probe is not operational

  a. Zip the content of the following folder: **<DataFlowProbe>/runtime/log**

  b. Clear the content of the following folder: **<DataFlowProbe>/runtime/log**

     Make sure NOT to remove the **log** folder itself.

  c. Restart the Data Flow Probe.

  d. Allow some time for the problem to reproduce.

  e. Zip again the content of the folder: **<DataFlowProbe>/runtime/log**

  f. Collect the most recent log archive first and upload it to the Support incident.

  g. Once the upload completes in step f, inform Support and upload the log zip of Step a.

Available Troubleshooting Resources for UCMDB

- **Installation troubleshooting.** Use to troubleshoot common problems that you may encounter when installing HPE Universal CMDB, and the solutions to those problems. See "Troubleshooting Deployment" on page 42.
- **Login troubleshooting.** Use to troubleshoot possible causes of failure to log in to HPE Universal CMDB. See "Troubleshooting – Logging In to UCMDB" on page 59.
- **HPE Software Self-solve knowledge base.** Use to search for specific troubleshooting information on a wide variety of topics. Located on the HPE Software Support site, the HPE Software Self-solve knowledge base can be accessed by selecting Troubleshooting & Knowledge Base from the HPE Universal CMDB Help menu.

  Note that only registered customers can access the resources on the HPE Software Support site. Customers who have not yet registered can do so from this site.
- **HPE Universal CMDB Log files.** Use to troubleshoot CMDB runtime problems. For details, see .
- **Data Flow Management log files.** Use to troubleshoot DFM problems. For details, see "Data Flow Probe Log Files" on page 33 .
- **Query log files.** Use to view definitions for query parameter log files. For details, see "UCMDB Log Files" on the next page.

About Log Files

This section includes:

UCMDB Log Files

This section includes:

UCMDB Log Files

CMDB log files enable you to perform basic troubleshooting of CMDB runtime problems. Additionally, by tracking the CMDB behavior in the log files, you can examine the effects of changes made in the system. The CMDB is composed of subsystems and each subsystem records to several log files. CMDB Server logs have consistent format. The order is data and time: **(format "yyyy-MM-dd hh:mm:ss:SSS") logLevel [Thread Name]**. The wrapper log is an exception to this standard. These settings can be changed from log properties files located in the **UCMDBServer\conf\log** folder.

Log files are located in:

- **Windows: C:\hp\UCMDB\UCMDBServer\runtime\log**
- **Linux: /opt/hp/UCMDB/UCMDBServer/runtime/log**

> **Note:** UCMDB log levels should be set to the OOTB values. They may be increased when investigating issues. However, after obtaining the required information the log levels should be reverted. Increased log levels for a longer period of time may have an impact over performance.
>
> If you want to delete the logs, you should delete the content in the **log** folder only, and never delete the folder itself. Make sure that the **log** folder always exists. If the **log** folder is deleted accidentally, create the **log** folder manually before starting up the UCMDB Server.

This section includes the following topics:

- "General Log Files" on the next page
- "Class Model Log Files" on page 17
- "TQL Log Files" on page 18
- "Data-In Log Files" on page 19
- "History Log Files" on page 20
- "Enrichment Log Files" on page 22

General Log Files

Quota Log Parameters

The log name is **cmdb.quota.log**.

Log File	Description
Purpose	Quota names, quota values, and current quota levels.
Information Level	Quota names and values set in the server and customer levels during a customer load.
Error Level	CMDB operations that fail because they exceed quota limits.
Debug Level	A count collector runs every **n** minutes and gathers current counts for all quotas. Collected counts are logged.
Basic Troubleshooting	If operations fail because of quota limits, check the count growth and quota values.

CMDB Operation Statistics Log

The log name is **cmdb.operation.statistics.log**.

The log does not appear in the log folder by default. Only when you perform some specific action, the log becomes available. For example, when you invoke the **resetOperationStatistics** JMX method from the **Framework Services** category, it resets CMDB Server Operation Statistics and writes dump to this log.

Log File	Description
Purpose	Statistics for all operations performed in the past 15 minutes including worst operation instances.
Information Level	Statistics per operation including operation class name, caller application, and

Log File	Description
	customer ID. Default of 10 worst operation instances.
Error Level	Disables the statistics feature.
Debug Level	Not available.
Basic Troubleshooting	Check when there is a performance slowdown.

Configuration Log

The log name is **configuration.log**.

Log File	Description
Purpose	Contains basic environment details, including: • Server version and CUP version • Database vendor and version • Content pack version • High Availability configuration • Data Flow Probe version • Changes to settings (each setting is audited in the log)
Information Level	Information is written to the log when the system starts up or when a setting is changed.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	Used by Customer Support to help reproduce customer problems.

Keystore and Truststore Password Save Log

The log name is **save_store_pass.log**.

Log File	Description
Purpose	Information about installation log: keystore password and truststore password save time and encryption type.

Log File	Description
Information Level	Operation details.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	This is especially useful when installing and starting the UCMDB server. You can use this log information together with the information in Troubleshooting Keystore and Truststore.

Keystore and Truststore Password Verify Log

The log name is **verify_store_pass.log**.

Log File	Description
Purpose	Information about the installation log: whether keystore password and truststore password are saved correctly or not. If **server-storepass.conf** exists, then the UCMDB server installer will change keystore and truststore passwords with keytool.
Information Level	Operation details.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	This is especially useful when installing and starting the UCMDB server. You can use this log information together with the information in Troubleshooting Keystore and Truststore.

Class Model Log Files

CI Type Model Log

The log name is **cmdb.classmodel.log**.

This log should appear when you perform operations on the UCMDB class model, like creating a new CI Type, or adding an attribute on an existing CI Type.

Log File	Description
Purpose	CI Type Model errors and debug messages.
Information Level	When a CI Type Model is loaded, incorrect definitions are logged as informational messages. An example of an incorrect definition is `duplicate attributes`.
Error Level	Not available.
Debug Level	Every CI Type update includes the following: • Original CIT in XML format • New CIT in XML format • Differences between the CITs If the CI Type Model update is rejected, the reason is logged.
Basic Troubleshooting	Compares the differences that the server finds between the original CIT and the new CIT. This is useful to understand the following scenarios: • A CIT in a package failed • An action in the CIT browser applet failed • An action in the CIT browser applet succeeded when it should have failed

TQL Log Files

CMDB Notification Log

The log name is **cmdb.notification.log**.

Log File	Description
Purpose	Notification messages from the time of the component's creation in the CMDB until the client's listener receives a message. Most components receive configuration changes from the CMDB in push mode, by the notification mechanism, rather than in pull mode.
Information Level	• Startup and shutdown of publishers • Register and unregister remote and internal listeners
Error Level	• Errors when messages are published • Errors when messages are received

Log File	Description
Debug Level	• Unique message ID • Number of changes that a message includes as well as more details according to the type of the message (for example, the TQL result version) • JMS header properties
Basic Troubleshooting	If an application does not receive a notification, check the following: • a listener is registered with the appropriate notification filter • a message is published with data that matches this filter • a message is received by the listener (use the unique message ID to verify)

Data-In Log Files

CMDB Model Audit Short Log

The log name is **cmdb.model.audit.short.log**.

Log File	Description
Purpose	Information about a CI Type operation: type of operation, data received as input, and what happened to the data in each CIT. Also contains information about the caller application, execution time, and persistency time.
Information Level	Operation details.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	If there are no changes when there should be, check the following: • Whether the operation exists. • Whether the input is correct. • What happened to the data. There may have been a false update. This is especially useful when running DFM to trace the input.

History Log Files

History Log

The log name is **history.log**.

Log File	Description
Purpose	Records general history events
Information Level	• Auto completion events • Auto complete table lock/unlock messages • Tenants bitmask column size handling • Delete customer fuse notice
Debug Level	• Auto completion details • History Root table handling messages

History Audit Update Log

The log name is **history.update.audit.log**.

Log File	Description
Purpose	Tracks events saved in the History tables
Information Level	• Details all events stored in the history tables • Event statistics
Debug Level	Database statistics

History Partition Log

The log name is **history.partition.log**.

Log File	Description
Purpose	• Records history partition data. • Records the Baseline process events.
Information Level	• Add/Remove partition history tables

Log File	Description
	• Baseline events • Baseline statistics
Error Level	• Table partition failures • Baseline process failures

Query History Log

The log name is **history.queries.log**.

Log File	Description
Purpose	Records all the queries performed on the history tables.
Information Level	• Query condition • Query results summary
Error Level	Fuse exceeded
Debug Level	• Query condition details • Query result details

History Class Model Changes Log

The log name is **history.classmodel.changes.log**.

Log File	Description
Purpose	Tracks all the class model changes that affect the history tables.
Information Level	Class aligning messages
Error Level	Errors that occurred during class aligning

History Purging Log

The log name is **history.purge.log**.

Log File	Description
Purpose	Records the History purging process events

Log File	Description
Information Level	Purging process information
Error Level	Errors that occurred during the purging process
Debug Level	Details about purged data

Enrichment Log Files

CMDB Enrichment Log

The log name is **cmdb.enrichment.log**.

Log File	Description
Purpose	• Enrichment definitions: adding, updating, removing, and calculating. • Calculation results such as how many CIs were added, how many relationships were removed, and so forth. • Supplies the reason for a calculation failure. Failure in a model update, however, is not included since it is an asynchronous execution.
Information Level	• Add, update, and remove enrichment definitions. • Add, update, and remove CIs or relationships to or from a model.
Error Level	Calculation failure.
Debug Level	Traces the enrichment calculation process.
Basic Troubleshooting	• If no calculation was carried out, check the definition of **add enrichment**. • If there are no results, check the **finish calculate** entry.

Dal Log Files

CMDB Dal Log

The log name is **cmdb.dal.log**.

Log File	Description
Purpose	Information about activity that occurred in the data access layer, the layer that works with the CMDB.
Information Level	Not available.
Error Level	• Connection pool errors • Database errors • Command execution errors
Debug Level	• All DAL commands executed • All SQL commands executed
Basic Troubleshooting	If you suspect that CMDB actions are taking too long, check the time spent on queries and updates in the DAL logs and operation logs. Exception details and ID are entered into the log. The exception ID appears in the exception itself.

Authorization Log Files

CMDB Authorization Management Log

The log name is **security.authorization.management.log**.

Log File	Description
Purpose	Audit all modifications related to the authorization model.
Information Level	• Creation and deletion of users, user groups, tenants, roles, and resource groups. • Addition and removal of users from user groups, changes to user passwords,

Log File	Description
	and changes in users' default tenants. • Addition and removal of permissions from roles and changes in read-only status of roles. • Addition and removal of resources from resource groups. • Changes in user role assignments. • Changes in resource tenant associations.
Error Level	Failure to create or modify authorization resources, such as trying to create a user with an existing name.
Debug Level	Web services login requests.
Basic Troubleshooting	May be used to track why a user no longer has a specific permission.

CMDB Authorization Permissions Log

The log name is **security.authorization.permissions.log**.

This log contains detailed information for authorization and out-of-the-box information. To enable the print of information, you may need to set the log level to **DEBUG**.

Log File	Description
Purpose	Debug authorization permissions queries.
Debug Level	Print all existing permissions for the user currently logged in, whenever they are queried in the server.
Basic Troubleshooting	To check a specific permission issue,turn on the debug level, perform the action in the UI, turn the debug level off, and check the log for the existing permissions of the user. It is not recommended to keep this log at debug level, because it generates a large amount of printed output.

UCMDB UI Log Files

Client-side Applet Logs

The following client side applet logs are also available:

- **applet-operations.log.** Tracks the operations that are executed from the CMDB UI to the UCMDB server.
- **applet-general.log.** General log for the UI.
- **applet-cacheStatistics.log.** Tracks statistics of the UI cache.
- **applet-missing_resources.log.** Missing resources log.
- **applet-applet-tasks.log.** Logs task executions.
- **applet-timeMeasure.log.** Log for measuring performance.
- **applet-memoryTracker.log.** Tracks the memory usage of the UI.
- **applet-errors.log.** Logs the errors that occurred in the UI

> **Note:** UCMDB UI log files are present in the **%Temp%/UcmdbLog/log** folder on the machine from which you access the UCMDB UI.

Data Flow Management Log Files

Data Flow Management log files store information about data flow activity (discovery and integrations), as well as related errors, that occur on the Server side.

mam.AutoDiscovery.log

Contains information about tasks running on the server. The server provides services to the user interface or the Probe Gateway, such as: activating jobs, processing results from the Probe, or creating tasks for the Probe.

Level	Description
Error	All DFM process errors on the server side.
Information	Information about requests being processed.
Debug	Logs mainly for debugging purposes.

Basic Troubleshooting. Check this log when you have invalid user interface responses or errors you need to explore. This log provides information to enable you to analyze the problems.

mam.autodiscovery.results.stat.log

Contains the statistics of the results received from the Probe.

mam.autodiscovery.accuratedependency.log

(Deprecated) Contains information about accurate dependency for the Automatic Service Modeling feature. This log is related to the old ASM version (before Content Pack 18), and is no longer in use.

mam.dispatch.log

Contains all the dispatch related information.

To enable this log,

1. Locate and open the **<*UCMDB_Server_Home*>/conf/log/mam.properties** file.
2. Manually add the following settings into the **mam.properties** file:

```
log4j.category.mam.dispatch=${loglevel}, mam.dispatch.appender

#######################################

##   mam.packaging                   ##

#######################################

log4j.appender.mam.dispatch.appender=com.mercury.topaz.cmdb.shared.base.log.
BetterRollingFileAppender

log4j.appender.mam.dispatch.appender.File=${logs.dir}/mam.dispatch.log

log4j.appender.mam.dispatch.appender.MaxFileSize=${def.file.max.size}

log4j.appender.mam.dispatch.appender.MaxBackupIndex=${def.files.backup.coun
t}

log4j.appender.mam.dispatch.appender.layout=org.apache.log4j.PatternLayout

log4j.appender.mam.dispatch.appender.layout.ConversionPattern=${msg.layout}
```

3. Save the file.

Autodiscovery Dal Log

The log name is **mam.autodiscovery.dal.log**.

Log File	Description
Purpose	Holds information on queries and other actions taken on the server's database tables as part of the discovery process.
Information Level	A summary of actions taken and their results on the database (such as retrieving information, deleting records, and so on).
Error Level	All critical errors that occurred during the attempt to access the database.
Debug Level	Detailed information on query parameters and/or the results that are retrieved from them
Basic Troubleshooting	If there are any database errors or failures (such as connection failed, technical error in the query, and so on), the error log is included in this log file also.

workflow_sizing.log

Enabling this log file helps you to collect running statistics (for example, time spent on normalization and auto delete) of each modules on a probe.

How to Enable this log?

To enable this log,

1. On the probe, locate and open the **/conf/log/probeGWLog4j.properties** and **/conf/log/probeMgrLog4j.properties** files.
2. Manually add the following settings into each of the above files:

```
#######################################
### cmdb.workflow.sizing             ##
#######################################
log4j.category.cmdb.workflow.sizing=INFO, cmdb_workflow_sizing
log4j.appender.cmdb_workflow_
sizing=com.mercury.topaz.cmdb.shared.base.log.BetterRollingFileAppender
log4j.appender.cmdb_workflow_sizing.File=${logs.dir}/workflow_sizing.log
log4j.appender.cmdb_workflow_sizing.Append=true
log4j.appender.cmdb_workflow_sizing.MaxFileSize=512MB
log4j.appender.cmdb_workflow_sizing.Threshold=INFO
log4j.appender.cmdb_workflow_sizing.MaxBackupIndex=10
```

```
log4j.appender.cmdb_workflow_sizing.layout=org.apache.log4j.PatternLayout

log4j.appender.cmdb_workflow_sizing.layout.ConversionPattern=<%d> [%-5p]
[%t] (%F:%L) - %m%n

log4j.appender.cmdb_workflow_sizing.encoding=UTF-8
```

3. Save the files.
4. Restart the probe.

Sample log

```
<2015-11-11 13:56:51,459> [INFO ] [ProbeGW Task Results Sender]
(TaskResultsSenderThread.java:458) -
[TaskResultsSenderThread.handleSuccessTriggers.start][desc=update ID
mapping,size=1]

<2015-11-11 13:56:51,460> [INFO ] [ProbeGW Task Results Sender]
(TaskResultsSenderThread.java:481) -
[TaskResultsSenderThread.handleSuccessTriggers.stop][desc=update ID
mapping,size=1]
```

Probe Auto Upgrade Log

The log name is **probe_auto_upgrade.log**.

It shows in the **C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\<source_version>to<target_version>** folder. For example: **C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\10.32to10.33**.

This log file is also sent to the UCMDB server and shows as **<domain_name>_probename_auto_upgrade.log** in the **C:\hp\UCMDB\UCMDBServer\runtime\log\probeUpgradeLogs\<source_version>to<target_version>\failed|success** folder.

Log File	Description
Purpose	Shows the related information when the probe auto upgrade agent upgrades a probe.
Information Level	Shows the console output of normal information.
Error Level	Any error that occurs when the probe auto upgrade agent upgrades a probe.
Debug Level	N/A
Basic Troubleshooting	Check this log file when the probe upgrade fails.

Log Severity Levels

Each log is set so that the information it records corresponds to a certain severity threshold. Because the various logs are used to keep track of different information, each is pre-set to an appropriate default level. For details on changing the log level, see "Changing Log Levels" below.

Typical log levels are listed below from narrowest to widest scope:

- **FATAL.** The log records only events that prevent the system from functioning.
- **ERROR.** In addition to Fatal events, the log records events that adversely affect the immediate functioning of the CMDB. When a malfunction occurs, you can check if Error messages were logged and inspect their content to trace the source of the failure.
- **WARN.** The log's scope includes, in addition to Fatal and Error-level events, problems for which the CMDB is currently able to compensate and incidents that should be noted to prevent possible future malfunctions.
- **INFO.** The log records all activity. Most of the information is normally routine and of little use and the log file quickly fills up.
- **DEBUG.** This level is used by HPE Software Support when troubleshooting problems.

> **Note:** The names of the different log levels may vary slightly on different servers and for different procedures. For example, **INFO** may be referred to as **Always logged** or **Flow**.

Changing Log Levels

If requested by HPE Software Support, you may have to change the severity threshold level in a log, for example, to a debug level. For details on changing the log level, see "Log Configuration Dialog Box" on page 32.

How to Download a Zip File of Log Files and Thread Dumps

You can produce a zip file that includes all logs and thread dumps. You create the file either through a JMX operation on the client machine, or by running a batch file on the UCMDB Server.

Thread dumps are created periodically: Once a minute, a thread dump snapshot is taken and is saved to a new file in the **C:\hp\UCMDB\UCMDBServer\runtime\log\threadDumps** folder. Thread dump files from the last hour are kept. This folder also holds the ad hoc Server snapshots that are generated during the **logGrabber** execution.

To generate the zip file from the client machine:

1. Launch the Web browser and enter the server address, as follows: **https://<UCMDB Server Host Name or IP>:8443/jmx-console**.

   You may have to log in with a user name and password.

2. Under **UCMDB**, click **UCMDB:service=Server services** to open the JMX MBEAN View page.
3. Locate the **executeLogGrabber** operation.
4. Click **Invoke**.

   A Server snapshot file with the name **LogGrabber_serverSnapshot_ <current date and time>.txt** is created in the following location: **C:\hp\UCMDB\UCMDBServer\runtime\log\threadDumps**. This is a thread dump that includes the threads of the Server framework only.

5. In the File Download dialog box, you can open the **logGrabber_<current time>.zip** file, or download it to the client machine.

To generate the zip file from the UCMDB Server:

1. Access the following folder on the UCMDB Server: **C:\hp\UCMDB\UCMDBServer\tools\logGrabber**.
2. Run the **logGrabber.bat** file.

   The **LogGrabber_<current time>.zip** file is created in the following location: **C:\hp\UCMDB\UCMDBServer\runtime**. This is a thread dump that includes the threads of the Server framework only.

How to Retrieve UCMDB Server Logs for a Specific Time Frame

You can produce a zip file containing all UCMDB server logs for a given time frame. This is intended for support engineers or other users who need to obtain logs for a specific time frame.

To generate the zip file from the client machine:

1. Launch the Web browser and enter the server address, as follows: **https://<UCMDB Server Host Name or IP>:8443/jmx-console**.

   You may have to log in with a user name and password.

2. Under **UCMDB**, click **UCMDB:service=Server Services** to open the JMX MBEAN View page.
3. Locate the **executeServerLogParser** operation.
4. Enter the start time in the required format.
5. (Optional) Enter an end time. If you do not provide an end time, the current time that the JMX method is invoked is used.
6. Click **Invoke**.

   When the process has finished, the file can be downloaded from the browser.

Limitations

- The zip file is also located on the UCMDB server machine as the **c:\hp\UCMDB\UCMDBServer\runtime\ParsedLogGrabber_<time>.zip** file. For maintenance purposes, this file must be manually deleted.
- The folder **c:\hp\UCMDB\UCMDBServer\runtime\log\ParsedLogs_<date>** is also created and contains the unzipped contents. For maintenance purposes, this file must be manually deleted.
- In high availability UCMDB deployments, this JMX method is running against one server only.
- Only logs from the same date can be parsed.

How to Use the User Activity Log

When troubleshooting a problem in your system, another useful tool is the User Activity log. When activated, this log records all the actions performed on your system, enabling HPE Software Support to reproduce the problem and troubleshoot it.

To activate the User Activity log, first verify that it is enabled:

1. On the UCMDB server, launch the Web browser and enter the following address: **https://localhost:8443/jmx-console**

   You may have to log in with a user name and password.

2. Click **UCMDB:service=Settings Services** to open the JMX MBEAN View page.
3. Locate the **showSettingsByCategory** method.
4. Enter General Settings as the category name and click **Invoke**.
5. Locate the **mam.web.user.activity.log.enabled** setting and verify that it is set to **true**.
6. If it is set to false, go back to the **Settings Services** page, and select the **setSettingValue** method.
7. Enter **mam.web.user.activity.log.enabled** as the setting and **true** as the value and click **Invoke**.

Next, change the log level to INFO:

1. In the JMX Console, click **UCMDB:service=Server Services**
2. Locate the **loggersLevels** method and click **Invoke**.
3. Locate the **com.hp.ucmdb.uiserver.aspects** logger and select **INFO** from the drop-down list.
4. Click **Update loggers**.

The log is now activated. Perform the actions that led to the problem. The User Activity log automatically records them.

When you are finished, disable the log using the **loggersLevels** method and selecting **ERROR** as the level for the **com.hp.ucmdb.uiserver.aspects** logger.

Log Configuration Dialog Box

This dialog box enables you to view Universal CMDB logs and change the log level.

To access	On the Status bar, click **Log Level Configuration** or select **Tools > Log Configuration...** from the Modeling main menu.
See also	"Log Severity Levels" on page 29

User interface elements are described below:

UI Element	Description
Apply	**Apply.** Click to apply the selected log level to the log.

UI Element	Description
Appender	The name of the appender.
Appender pane	Displays details for the appender you selected in the Loggers pane.
File	Click the link to open the log file in an editor.
Max file size	Maximum appender file size.
Max backup index	Maximum number of backup indexes. Default: **5**
Loggers pane	An expandable list of Universal CMDB logs. Select the required log from the list: the details of the log appear in the lower pane.
Logger pane	Displays details for the logger you selected in the Loggers pane.
Loggers table	Displays a list of loggers (with Logger Name and Log level) for the selected log.
Log level	Select a log level from the drop-down list.
Logger's appender	A string defining the log category. For internal use only.
Appender file	The name of the logger's appender file.

Data Flow Probe Log Files

Data Flow Probe logs store information about job activation that occurs on the Probe Gateway and Probe Manager. The log files can be accessed from the following location:

C:\hp\UCMDB\DataFlowProbe\runtime\log

> **Note:** Alternatively, to access the Data Flow Probe's log files, log in to the JMX console (**https://localhost:8453**) and, from the main page, select the **GeneralUtils** mbean. Activating the **executeLogGrabber** function zips all the Data Flow Probe's log files. Save the .zip file locally on your client machine.

General Logs

WrapperProbeGw.l	Records all the Probe's console output in a single log file.

og	• **Levels:** ◦ **Error.** Any error that occurs within the Probe Gateway. ◦ **Information.** Important information messages, such as the arrival or removal of a new task. ◦ **Debug.** N/A • **Basic Troubleshooting:** Use this file for any Probe Gateway problems to verify what occurred with the Probe Gateway at any time as well as any important problems it encountered.
probe-error.log	Summary of the errors from the Probe. • **Levels:** ◦ **Error.** All errors in the Probe components. ◦ **Information.** N/A ◦ **Debug.** N/A • **Basic Troubleshooting:** Messages from the Probe's infrastructure only.
wrapperLocal.log	When running the Probe in separate mode (that is, the Probe Manager and Probe Gateway are installed on separate machines), a log file is also saved to the Probe Manager. • **Levels:** ◦ **Error.** Any error that occurs within the Probe Manager. ◦ **Information.** Important information messages such as received tasks, task activation, and the transferring of results. ◦ **Debug.** N/A • **Basic Troubleshooting:** Use this file for any Probe Manager problems to verify what occurred with the Probe Manager at any time as well as any important problems it encountered.
postgresql.log	Displays database related error during the installation. **Note:** If this log is empty check in the Event Viewer logs.
pg_upgrade.log	Shows the running details of the **pg_upgrade.bat** script, including the details about PostgreSQL upgrade and table splitting. The log does not appear in the **log** folder by default. It appears only when you manually run the **pg_upgrade.bat** script or may appear when you select the upgrade option during probe installation. • **Levels:** ◦ **Error.** Any error that occurs when PostgreSQL upgrade or table

	splitting fails. ○ **Information.** Shows the console output and suggestions when it fails. ○ **Debug.** N/A • **Basic Troubleshooting:** Check this log file when PostgreSQL upgrade or table splitting fails.
probe_upgrade_conf_merge.log	Shows the related information when probe installer merger configuration files. • **Levels:** ○ **Error.** Any error that occurs when merging configuration files. ○ **Information.** Shows the console output of normal information. ○ **Debug.** N/A • **Basic Troubleshooting:** Check this log file when the probe installer has problems.
probe_auto_upgrade.log	Shows the related information when the probe auto upgrade agent upgrades a probe. It shows in the **C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\<source_version>to<target_version>** folder. For example: **C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\10.32to10.33**. This log file is also sent to the UCMDB server and shows as **<domain_name>_probename_auto_upgrade.log** in the **C:\hp\UCMDB\UCMDBServer\runtime\log\probeUpgradeLogs\<source_version>to<target_version>\failed|success** folder. • **Levels:** ○ **Error.** Any error that occurs when the probe auto upgrade agent upgrades a probe. ○ **Information.** Shows the console output of normal information. ○ **Debug.** N/A • **Basic Troubleshooting:** Check this log file when the probe upgrade fails.

Probe Gateway Logs

probeGW-	Records all the task results sent from the Probe Gateway to the server.

taskResults.log	• **Levels:** ◦ **Error.** N/A ◦ **Information.** Result details: task ID, job ID, number of CIs to delete or update. ◦ **Debug.** The **ObjectStateHolderVector** results that are sent to the server (in an XML string). • **Basic Troubleshooting:** ◦ If there is a problem with the results that reach the server, check this log to see which results were sent to the server by the Probe Gateway. ◦ The results in this log are written only after they are sent to the server. Before that, the results can be viewed through the Probe JMX console (use the **ProbeGW Results Sender** MBean). You may have to log in to the JMX console with a user name and password.
probeGW-tasks.log	Records all the tasks received by the Probe Gateway. • **Levels:** ◦ **Error.** N/A ◦ **Information.** N/A ◦ **Debug.** The task's XML. • **Basic Troubleshooting:** ◦ If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received. ◦ You can view the current task's state through the JMX console (use the **Discovery Scheduler** MBean).

Probe Manager Logs

probeMgr-performance.log	Performance statistics dump, collected every predefined period of time, which includes memory information and thread pool statuses. • **Levels:** ◦ **Error.** N/A ◦ **Information.** N/A ◦ **Debug.** N/A • **Basic Troubleshooting:**

	◦ Check this log to investigate memory issues over time. ◦ The statistics are logged every 1 minute, by default.
probeMgr-adaptersDebug.log	Contains messages that are created following a job execution.

Discovery Rules Engine Log Files

normalization.audit.log	Logs information about the processing of the Discovery Rules Engine. • **Levels:** ◦ **Error.** N/A ◦ **Information.** Audits the number of element processed and the number of CIs that were changed. **Example:** `Normalization (OSHV: 8 elements) (Time: 125 ms) (Modified CIs: 1)` ◦ **Debug.** N/A
normalization.log	Logs detailed information about the processing of the Discovery Rules Engine, enabling you to trace detailed information of the Discovery Rule Engine process. • **Levels:** ◦ **Error.** All discovery rule processing errors. ◦ **Information.** Logs all levels of information about the processing of the Discovery Rules Engine. ◦ **Debug.** Logs mainly for debugging purposes. • **Basic Troubleshooting.** Check this log when you need to analyze why a CI was not enriched by the Discovery Rules Engine.

TQL Parameter Logs

This section contains definitions for TQL parameter log files.

This section includes the following topics:

- "Pattern Statistics Log" below
- "Audit Short/Detailed Log (TQL Perspective)" below
- "Incremental Statistics Log" on the next page
- "Incremental Splitter Log" on page 40
- "Incremental Detailed Log" on page 40

Pattern Statistics Log

The log name is **cmdb.pattern.statistics.log**.

Log File	Description
Purpose	General calculation data for each TQL query, updated at predefined intervals.
Information Level	The following information is given for each TQL query: • name • average, minimum, and maximum calculation times • number of calculations • last calculation time • result size
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	• Verify that a specific TQL query was updated. • Evaluate a TQL query's calculation time. • Evaluate a TQL query's result size.

Audit Short/Detailed Log (TQL Perspective)

The log name is **cmdb.audit.short.log**.

Log File	Description
Purpose	CMDB state changes, CI Type changes, and TQL query results. You can use this log to follow the results of TQL queries.

Log File	Description
Information Level	Not available.
Error Level	Not available.
Debug Level	• Final calculation for TQL queries is logged. • If the final TQL query calculation is unchanged from the previous calculation, this is noted. • If the final TQL query calculation is changed from the previous calculation, results of the CIs and relationships are recorded in the detailed log. The number of CIs and relationships are recorded in the short log.
Basic Troubleshooting	• Use this log to verify which notifications are published by the TQL query subsystem. • Check the section at the end of each result. This section includes added, removed, and updated CIs and relationships. • Track the CIT changes and see if the query results also change. You can thus correlate the CIT changes to the results of the query calculations.

Incremental Statistics Log

The log name is **cmdb.incremental.statistics.log**.

Log File	Description
Purpose	Traces the calculation procedure, full or incremental, of every query.
Information Level	Not available.
Error Level	Not available.
Debug Level	• Gives the date, time, query name, and whether an incremental statistic calculation was performed (yes/no). • If an incremental statistic calculation was not performed, states the reason, the number of subcalculations (relevant for incremental calculations only), and the complete calculation time.
Basic Troubleshooting	Monitors the calculation process. If a specific query calculation takes a long time, check if it is a full or incremental calculation:

Log File	Description
	• If full, check whether a full calculation is necessary. • If incremental, check how many subcalculations have been performed.

Incremental Splitter Log

The log name is **cmdb.incremental.splitter.log**.

Log File	Description
Purpose	Monitors the incremental splitter result made during an incremental calculation.
Information Level	Not available.
Error Level	Not available.
Debug Level	Gives the set of query node numbers of each query graph created by the incremental splitter.
Basic Troubleshooting	If the TQL result calculated by the incremental calculator is wrong, verify that the splitter result is correct.

Incremental Detailed Log

The log name is **cmdb.incremental.detailed.log**.

Log File	Description
Purpose	Monitors the incremental calculation process.
Information Level	Not available.
Error Level	Not available.
Debug Level	Each incremental subcalculation entry includes the following: • the trigger query node • the number of elements classified to the trigger query node • whether the subcalculation step is driven by new elements added to the model or by existing elements • the calculated query graph
Basic Troubleshooting	Follows the basic steps of an incremental calculation.

How to Troubleshoot and Debug Using Generic Adapter Log Files

For troubleshooting and debugging, use the following:

- Adjust logging levels in these files (set the *loglevel* variable to TRACE for the most detailed results):
  - **<UCMDB_DataFlowProbe>\conf\log\fcmdb.push.properties**

    <UCMDB_DataFlowProbe> is the UCMDB Data Flow Probe installation directory.
  - **<UCMDB_Server>\conf\log\reconciliation.properties**

    <UCMDB_Server> is the UCMDB Server installation directory.
- Analyze the following Generic Adapter log files:
  - **<UCMDB_DataFlowProbe>\runtime\log\fcmdb.push.all.log**
  - **<UCMDB_DataFlowProbe>\runtime\log\fcmdb.push.configuration.log**
  - **<UCMDB_DataFlowProbe>\runtime\log\fcmdb.push.connector.all.log**
  - **<UCMDB_DataFlowProbe>\runtime\log\fcmdb.push.connector.configuration.log**
  - **<UCMDB_DataFlowProbe>\runtime\log\fcmdb.push.mapping.log**
  - **<UCMDB_DataFlowProbe>\runtime\log\fcmdb.push.all.log**
- Analyze the following generic log files:
  - **<UCMDB_DataFlowProbe>\runtime\log\probe-error.log**
  - **<UCMDB_DataFlowProbe>\runtime\log\WrapperProbeGw.log**
  - **<UCMDB_Server>\runtime\log\error.log**
  - **<UCMDB_Server>\runtime\log\cmdb.reconciliation.log**

Chapter 2: Troubleshooting Deployment

This chapter includes:

Troubleshooting Deployment - UCMDB Server

Problem: The UCMDB Server does not start automatically upon system restart.

Solution:

1. Open the Windows Services dialog box and select the **UCMDB_Server** service.
2. Open the UCMDB_Server Properties (Local Computer) dialog box.
3. In the **General** tab, ensure that:
   - **The Path to executable** field points to the correct executable location.
   - The service is configured to automatically start (Startup type is **Automatic**).
4. In the **Log On** tab, ensure that the service uses the correct user for logon. For details on changing the service user, see the HPE Universal CMDB Hardening Guide.
5. In the **Dependencies** tab, ensure that the service is configured to have no dependencies (**<No Dependencies>**).

Troubleshooting Deployment - Keystore and Truststore

Troubleshooting Keystore and Truststore - Non-FIPS mode

Problem: UCMDB server startup failed, and the **startup.log** shows message similar to the following:

```
2017-05-04 08:32:17,074  ERROR  [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
       at org.eclipse.jetty.server.Server.doStart(Server.java:329)
       at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
       at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
       at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
       at com.hp.ucmdb.server.Main.main(Main.java:23)
       at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
       at sun.reflect.NativeMethodAccessorImpl.invoke
```

```
(NativeMethodAccessorImpl.java:62)
       at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
       at java.lang.reflect.Method.invoke(Method.java:498)
       at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
       at java.lang.Thread.run(Thread.java:745)
```

Solution A:

Check the **verify_store_pass.log** (in the **C:\hp\UCMDB\UCMDBServer\runtime\log** folder), if you see the following message:

```
INFO: server-storepass.conf file exists and it contains keystore and truststore.
```

Do the following:

1. Stop the UCMDB Server.
2. Run commands.
   a. Check keystore password.

      Windows:

      From **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, run the following commands.

      ```
      keytool -list -keystore
      C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
      ```

      Linux:

      From **/opt/hp/UCMDB/UCMDBServer/bin/jre/bin**, run the following commands:

      ```
      ./keytool -list -keystore
      /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore
      ```

      Enter the password that you set up during the installation of UCMDB server. If you see the following message:

      ```
      keytool error: java.io.IOException:Keystore was tampered with, or password
      was incorrect.
      ```

      Then the password was not properly set, and you need to change keystore and truststore passwords using keytool.

   b. Change the store password:

      Windows:

```
keytool -storepasswd -new <new_keystore_pass> -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
<current_keystore_pass>
```

Linux:

```
./keytool -storepasswd -new <new_keystore_pass> -keystore
/opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore -storepass
<current_keystore_pass>
```

c. Change the key password (if the store is not empty):

Windows:

```
keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass>
-keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

Linux:

```
./keytool -keypasswd -alias <alias> -keypass <currentPass> -new
<newPass> -keystore
/opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore
```

d. Change the trust store password:

Windows:

```
keytool -storepasswd -new <new_truststore_pass> -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore -storepass
<current_truststore_pass>
```

Linux:

```
./keytool -storepasswd -new <new_truststore_pass> -keystore
/opt/hp/UCMDB/UCMDBServer/conf/security/server.truststore -storepass
<current_truststore_pass>
```

3. Start the UCMDB Server service.

Solution B:

Check the **verify_store_pass.log**, if you see the following message:

```
INFO:  keystore password and truststore password don't exist.
```

Or the following:

```
INFO:  server-storepass.conf file doesn't exist.
```

Do the following:

1. Generate the **server-storepass.conf** file.

   Windows:

   From the **C:\hp\UCMDB\UCMDBServer\bin** folder, run the following command:

   ```
   key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   Linux:

   From the **/opt/hp/UCMDB/UCMDBServer/bin** folder, run the following command:

   ```
   ./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   where `<fips_mode>` can be only set to **true** or **false**. For non-FIPS mode UCMDB server, **false** for `<fips_mode>`.

2. Stop the UCMDB Server.
3. Change keystore password and truststore password with keytool.

   From the **C:\hp\UCMDB\UCMBServer\bin\jre\bin** (Windows) or **/opt/hp/UCMDB/UCMBServer/bin/jre/bin** (Linux) folder, run the following commands:

   a. Change the store password:

   Windows:

   ```
   keytool -storepasswd -new <new_keystore_pass> -keystore
   C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
   <current_keystore_pass>
   ```

   Linux:

   ```
   ./keytool -storepasswd -new <new_keystore_pass> -keystore
   /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore -storepass
   <current_keystore_pass>
   ```

   b. Change the key password (if the store is not empty):

   Windows:

   ```
   keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass>
   -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
   ```

   Linux:

   ```
   ./keytool -keypasswd -alias <alias> -keypass <currentPass> -new
   <newPass> -keystore
   /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore
   ```

c. Change the trust store password:

Windows:

```
keytool -storepasswd -new <new_truststore_pass> -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore -storepass
<current_truststore_pass>
```

Linux:

```
./keytool -storepasswd -new <new_truststore_pass> -keystore
/opt/hp/UCMDB/UCMDBServer/conf/security/server.truststore -storepass
<current_truststore_pass>
```

4. Start the UCMDB Server service.

Solution C:

If you only changed keystore password or truststore password during UCMDB server installation, and then server startup failed and the **startup.log** shows similar error messages as shown above. You can follow the instructions provided in Solution A or Solution B, but you need to change the keystore password or truststore password that you set during installation.

For example, if you only changed truststore password during installation and you need to generate **server-storepass.conf**, run the following command:

Windows: `key-truststore.bat <fips_mode> null <new_truststore_pass>`

Linux: `./key-truststore.sh <fips_mode> null <new_truststore_pass>`

Problem: You have changed schema in UCMDB Server. The server startup failed and the **startup.log** shows the following message:

```
2017-05-04 08:32:17,074  ERROR  [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
        at org.eclipse.jetty.server.Server.doStart(Server.java:329)
        at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
        at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
        at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
        at com.mercury.topaz.cmdb.server.manage.Framework.access$100
```

```
(Framework.java:102)
        at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
        at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
        at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
        at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
        at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
        at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
        at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
        at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
        at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
        at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
        at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
        at com.hp.ucmdb.server.Main.main(Main.java:23)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:498)
        at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
        at java.lang.Thread.run(Thread.java:745)
```

Solution: You need to re-generate **server-storepass.conf**, because the new schema does not store any keystore and truststore passwords.

- If you remember what passwords were specified previously, you can generate the **server-storepass.conf** file with the following command:

  Windows: `key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>`

  Linux: `./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>`

  where `<fips_mode>` can be only set to **true** or **false**. For non-FIPS mode UCMDB server, **false** for `<fips_mode>`.

- If you don't remember the passwords, follow the instructions in Solution B to regenerate the passwords.

Troubleshooting Keystore and Truststore - FIPS mode

Problem: If starting the UCMDB server failed, and the **startup.log** shows message similar to the following:

```
2017-05-04 08:32:17,074  ERROR  [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
       at org.eclipse.jetty.server.Server.doStart(Server.java:329)
       at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
       at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
       at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
       at com.hp.ucmdb.server.Main.main(Main.java:23)
       at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
       at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
```

```
        at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:498)
        at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
        at java.lang.Thread.run(Thread.java:745)
```

Solution A:

Check the **verify_store_pass.log**, if you see the following message:

```
INFO: server-storepass.conf file exists and it contains keystore and truststore.
```

Do the following:

1. Change the keystore and truststore passwords using keytool.

   For detailed instructions, see the "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" section in the *HPE Universal CMDB FIPS Deployment Guide*.

2. Start the UCMDB Server service.

Solution B:

Check the **verify_store_pass.log**, if you see the following message:

```
INFO:  keystore password and truststore password don't exist.
```

Or the following:

```
INFO:  server-storepass.conf file doesn't exist.
```

Do the following:

1. Make sure you have stopped the UCMDB Server.
2. Generate the **server-storepass.conf** file.

   Windows:

   From **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, run the following command:

   ```
   key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   Linux:

   From **opt/UCMDB/UCMBServer/bin/jre/bin**, run the following command:

   ```
   ./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

where `<fips_mode>` can be only set to **true** or **false**. For FIPS mode UCMDB server, **true** for `<fips_mode>`.

3. Change the keystore and truststore passwords using keytool.

   For detailed instructions, see the "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" section in the *HPE Universal CMDB FIPS Deployment Guide*.

4. Start the UCMDB Server service.

Solution C:

If you only changed keystore password or truststore password during UCMDB server installation, and then server startup failed and the **startup.log** shows similar error messages as shown above. You can follow the instructions provided in Solution A or Solution B, but you need to change the keystore password or truststore password that you set during installation.

For example, if you only changed truststore password during installation and you need to generate **server-storepass.conf**, run the following command:

Windows: `key-truststore.bat <fips_mode> null <new_truststore_pass>`

Linux: `./key-truststore.sh <fips_mode> null <new_truststore_pass>`

Troubleshooting Deployment - Configuration Manager

Configuration Manager General Limitations and Troubleshooting

Limitations

- The time settings on the UCMDB and Configuration Manager servers must be synchronized, down to the seconds.
- The time zone and time format on the UCMDB and Service Manager servers must be synchronized.

- You will not see a new CI type that you created in UCMDB until you log out of Configuration Manager and then log on again.
- Whenever the time is changed on the Configuration Manager Tomcat server, the server must be restarted to update the time on the server.

Troubleshooting

Problem. When you start the Configuration Manager service, you receive the following error message:

```
Windows could not start the HPE Universal CMDB Configuration Manager on
Local Computer. For more information, review the System Manager Event
log. If this is a non-Microsoft service, contact the service vendor, and
refer to service-specific error code 0.
```

Solution. Do the following:

1. Go to the **<*Configuration_Manager_installation_directory*>\cnc\bin** folder and execute the following command:

   ```
   edit-server-0.bat
   ```

2. Select the Startup tab. In the Mode drop-down list (at the bottom), select **jvm** instead of **exe**.
3. Click **OK**.
4. Run your service.

Configuration Manager Upgrade

Problem. The upgrade to version 10.23 fails.

Solution: To restore to the previous version, perform the following steps:

- Uninstall Configuration Manager version 10.23.
- Restore the installation folder for the previous version of Configuration Manager (that you backed up before upgrading) to its original location.
- Restore the database (that you backed up before upgrading).
- Import the Windows registry entry (that you backed up before upgrading).

Logging In to Configuration Manager

Problem. You have been assigned the appropriate permissions for Configuration Manager but you are not able to log in.

Solution. Verify that the following parameters are configured correctly in UCMDB:

- LW-SSO init string: This string must not be empty.
- LW-SSO domain: Must be set to the same domain as UCMDB.
- LW-SSO trusted DNS domains: The Configuration Manager domain must be listed here, even if it is the same as the UCMDB domain.

Problem. There is an error in the UCMDB connection.

Solution. One of the following may be the cause:

- The UCMDB server is down. Restart Configuration Manager after UCMDB is fully up (verify that the UCMDB server status is **Up**).
- The UCMDB server is up but the Configuration Manager connection credentials or URL is wrong.

Problem. After changing UCMDB connection settings (such as changes to: host/port/protocol/SRP), the Configuration Manager server fails to start.

Solution. Reconfigure Configuration Manager and specify the UCMDB connection settings that reflect your latest changes. The reconfiguration wizard (**HPCM_10.01.exe**) is located in the ***<Configuration_Manager_installation_directory>*_installation** folder.

Problem. Changes to the UCMDB class model are not detected in Configuration Manager.

Solution. Restart the Configuration Manager server.

Problem. The Configuration Manager log contains a **UCMDBExecution timeout expired** error.

Solution. This occurs when the UCMDB database is overloaded. To correct this, increase the connection timeout as follows:

1. Create a **jdbc.properties** file in the **UCMDBServer\conf** folder.
2. Enter the following text: `QueryTimeout=<number in seconds>`.
3. Restart the UCMDB server.

Problem. Configuration Manager does not allow you to add a view to be managed.

Solution. When a view is added to be managed, a new TQL is created in UCMDB. If the maximum limit of active TQLs is reached, the view cannot be added. Increase the limit of active TQLs in UCMDB by changing the following settings in the Infrastructure Settings Manager:

- Max Number Of Active TQLs In Server
- Max Number Of Customer Active TQLs

Problem. The HTTPS Server certificate is not valid.

Solution. One of the following may be the cause:

- The validation date of the certificate has passed. You need to get a new certificate.
- The certification authority on the certificate is not a trusted authority. Add the certification authority to your Trusted Root Certification Authority list.

Problem. When logging in from the Configuration Manager login page, you get a login error or access denied page.

Solution. Check that the LW-SSO settings are correct. For details, see the general LW-SSO reference in the *HPE Universal CMDB Hardening Guide*.

Problem. The Configuration Manager server does not start due to entering incorrect database credentials.

Solution. If you made a change to the database credentials and the server fails to start, the credentials may be wrong. You need to re-encrypt the database password and enter new credentials in the configuration file. Proceed as follows:

1. From a command line, run the following command to encrypt the updated database password:

   ```
   <Configuration_Manager_installation_directory>\bin\encrypt-password.bat -p
   <password>
   ```

   which returns an encrypted password.

2. Copy the encrypted password (including the `{ENCRYPTED}` prefix), into the **db.password** parameter in the ***<Configuration_Manager_installation_directory>*\conf\database.properties** file.

Problem. The Configuration Manager Tomcat server does not start due to a bind port issue.

Solution. Try one of the following:

- Run the Post install wizard and replace the Configuration Manager server ports.
- Abort the other process that occupies the Configuration Manager ports.
- Manually change the ports in Configuration Manager configuration files by editing the following file: **<Configuration Manager installation directory>\servers\server-0\conf\server.xml** and updating the relevant ports:
  - HTTP (8180): line 69
  - HTTPS (8143): lines 71, 90

Problem. You receive an "out of memory" message.

Solution. Do the following to change the server startup parameters:

1. Run the following batch file:

   <Configuration Manager installation directory>/bin/edit-server-0.bat

2. Change the following settings:

   -Dapplication.ms=<inital memory pool size>
   -Dapplication.mx=<maximum memory pool size>

Problem. Changes in CIs in UCMDB are not reflected in Configuration Manager.

Solution. Configuration Manager runs an offline asynchronous analysis process. The process may not yet have processed the latest changes in UCMDB. To resolve this, try one of the following:

- Wait a few minutes. The default interval between analysis process executions is 10 minutes. It is configurable in **Administration > Settings**.
- Execute a JMX call to run the offline analysis calculation on the relevant view.
- In **Policies**, click the **Recalculate Policy Analysis** button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

Configuration Manager Authentications

Problem. During authentication of Configuration Manager after redirection to the UCMDB login page, you are not redirected back to Configuration Manager but UCMDB opens instead.

Solution. The Configuration Manager authentication session cookie is blocked or denied when using Internet Explorer version 6.0, 7.0 or 8.0 browsers. Add the Configuration Manager server to the Intranet/Trusted zone in the Internet Explorer security zones on your computer (**Tools > Internet Options > Security > Local Intranet > Sites > Advanced**). This allows all cookies to be accepted.

Solution. Make sure that the LW-SSO configuration in UCMDB settings is correct. For details, see the section about LW-SSO in the *HPE Universal CMDB Hardening Guide*.

Possible solution. Make sure that you access the application with the Fully Qualified Domain Name (FQDN) in the login URL (for example: **http://myserver.companydomain.com/WebApp**).

Troubleshooting Deployment - Data Flow Probe

Probe Downgrade or Rollback

Automatic downgrade or rollback of the probe version is not supported. To perform downgrade or to rollback a version upgrade, uninstall the probe and then install the required version.

Probe Restart

There are several situations where the Probe automatically restarts itself. For example, when deploying a new Content Pack or applying a CUP. In these cases, the Probe waits for 15 minutes to allow the running jobs to finish, and only then shuts down. Jobs that did not finish in that time (for example, long integrations) start running again when the Probe restarts.

How to Change the PostgreSQL Database Default Port

To change the port for the PostgreSQL database, that is defined by default in the Data Flow Probe installation:

1. Stop the Probe (if already started).
2. Stop the UCMDB Probe DB Service.
3. Modify the port in the following file:
   - Windows: **C:\hp\UCMDB\DataFlowProbe\pgsql\data\postgresql.conf**
   - Linux: **/opt/hp/UCMDB/DataFlowProbe/pgsql/data/postgresql.conf**

   The following shows how to change the port from **5432** to **5433**:

> **Note:** If two probes coexist on the same machine, plan the port usage carefully so that the ports used by the two probes do not conflict.

```
#port = 5432 # (change requires restart) < Old line

port = 5433 # (change requires restart) < New line
```

4. Make the following changes in the **DataFlowProbe.properties** file (in **C:\hp\UCMDB\DataFlowProbe\conf** on Windows, and **/opt/hp/UCMDB/DataFlowProbe/conf** on Linux):
   - Change:

     ```
     jdbc:postgresql://localhost/dataflowprobe
     ```

     to

     ```
     jdbc:postgresql://localhost:5433/dataflowprobe
     ```

   - Change:

     ```
     appilog.agent.local.jdbc.uri = jdbc:postgresql://localhost/dataflowprobe
     ```

     to

     ```
     appilog.agent.local.jdbc.uri =
     jdbc:postgresql://localhost:5433/dataflowprobe
     ```

   - Change:

     ```
     appilog.agent.normalization.jdbc.uri =
     jdbc:postgresql://localhost/dataflowprobe
     ```

     to

     ```
     appilog.agent.normalization.jdbc.uri =
     jdbc:postgresql://localhost:5433/dataflowprobe
     ```

   - Change:

     ```
     appilog.agent.netflow.jdbc.uri =
     jdbc:postgresql://localhost/dataflowprobe
     ```

     to

```
appilog.agent.netflow.jdbc.uri =
jdbc:postgresql://localhost:5433/dataflowprobe
```

Chapter 3: Troubleshooting Administration

This chapter includes:

Troubleshooting – Logging In to UCMDB

Use the following information to troubleshoot possible causes of failure to log in to UCMDB.

This section includes the following:

- "Possible Causes for Failure to Log In to UCMDB" below
- "Java Not Installed on Client Machine" on page 61

Possible Causes for Failure to Log In to UCMDB

Use the following information to troubleshoot possible causes of failure to log into Universal CMDB.

Problem/Possible Causes	Solutions
Universal CMDB is not started successfully. **Indication:** The **startup.log** file does not include the	**Solution 1:** Verify that the Universal CMDB Server is up and running by accessing the Web console **https://<Server name>:8443/web-console** where **<server name>** is the name of the Universal CMDB Server to which you are connecting.

Problem/Possible Causes	Solutions
following line: **** All components started ****	**Solution 2:** Check the database connection: To check that the database server is up and running: 1. Launch the Web browser and navigate to: **https://localhost:8443/jmx-console**. 2. Under **UCMDB**, click **UCMDB:service=Dal Services** to open the JMX MBean View. 3. Invoke the function **getDbContext** with a **customerID** parameter value of **1**. 4. Check that the operation result shows no problems. **Solution 3:** Check that the database connection parameters are correct. Ensure that you can log into the database server using the credentials you provided during the configuration procedure. **Solution 4:** Use the **cmdb.dal.log** file to verify the database connections. The **cmdb.dal.log** file can be found in the following directory: • Windows: **C:\hp\UCMDB\UCMDBServer\runtime\log** • Linux: **/opt/hp/UCMDB/UCMDBServer/runtime/log** **Solution 5:** To verify that the database connection is valid, in the Windows command interpreter (**cmd.exe**), type `sqlplus cmdb/cmdb@skazal`.
The CMDB is corrupted (for example, a user record may have been deleted accidentally from the CMDB).	Import a previously backed up database file. For details, see the *HPE Universal CMDB Database Guide*. **Important:** The Universal CMDB server must be down while importing the database. > **Note:** When you import a previously backed up database file, you lose all data previously existing in the system.
The Universal CMDB login fails. This may be due to an incorrect login name/password combination.	**Solution 1:** Ensure that you enter a correct login user name/password combination. **Solution 2:** Restore the default
Universal CMDB login fails due to unexpected errors.	**Solution 1**: Select **Start > All Programs > UCMDB > Universal CMDB Server Status** and ensure that the service is running. **Solution 2**: Look for errors in the following log files: • **C:\hp\UCMDB\UCMDBServer\runtime\log\error.log**

Problem/Possible Causes	Solutions
	• **C:\hp\UCMDB\UCMDBServer\runtime\log\ui-server.log** If you find errors that are unfamiliar to you, contact HPE Software Support.
Universal CMDB fails to start, even though the password was successfully changed.	Restore the default passwords: 1. Overwrite the existing file by copying the **Basic_ Authorization.zip** file from the following folder: ◦ Windows: **C:\hp\UCMDB\UCMDBServer\content\backup** ◦ Linux: **/opt/hp/UCMDB/UCMDBServer/content/backup** to the following folder: ◦ Windows: **C:\hp\UCMDB\UCMDBServer\content/basic_ packages** ◦ Linux: **/opt/hp/UCMDB/UCMDBServer/content/basic_ packages** 2. Log into the the JMX Console and locate the **UCMDB-UI:name=UCMDB Integration** service. 3. Run **setCMDBSuperIntegrationUser** by using the credentials of UISysadmin. 4. Stop the UCMDB Server. 5. Create a new schema. 6. Restart the UCMDB Server.

Java Not Installed on Client Machine

If Java is not installed on your machine or you have a version older than Java 8, during login a message is displayed asking you to install the correct Java Runtime Environment version. JRE is needed to view Universal CMDB applets.

Click the relevant button to allow Universal CMDB to install Java from either oracle.com or the Universal CMDB Server.

Troubleshooting and Limitations – UCMDB Server Administration

This section describes troubleshooting and limitations for UCMDB.

- If the **wrapper.java.additional.10=-XX:+HeapDumpOnOutOfMemoryError** parameter is set (it is enabled by default) in the **wrapper.conf** file, then every time the server fails with an Out of Memory error, it dumps the full memory to the disk. Since the memory contents could be very large, you should delete these files to avoid disk space problems.
- **Problem:** When working in a Firefox browser using Linux, you get an **OutOfMemoryError: PermGen space** error.

  Solution: Follow these steps:

  a. Go to the **bin** directory of the Java installation directory and open the Control Panel.

  b. In the **Java** tab, select **View**.

  c. In the Java runtime environment settings, under Runtime parameters, increase the **-XX:MaxPermSize**.
- **Limitation: Unsupported characters in password when UCMDB is used in integrations**

  When UCMDB is used in integrations, the following characters should not be used in the password:

  - All non-ASCII characters (valid ISO 8859/1 characters that are not also ASCII characters)
  - The following special characters: the tab character, the space character, and [\ ] ^ ` { | } ~ " # % & + , / : < = > ? @
- **Problem:** The **"User {0} has exceeded the maximum number of login sessions"** message is displayed.

  Solution: Ensure that you are properly logged out from other sessions on other computers. For example, closing a tab or closing the browser does not immediately close a user session on the server.

Troubleshooting Keystore and Truststore

Troubleshooting Keystore and Truststore - Non-FIPS mode

Problem: UCMDB server startup failed, and the **startup.log** shows message similar to the following:

```
2017-05-04 08:32:17,074  ERROR  [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
```

```
incorrect]
       at org.eclipse.jetty.server.Server.doStart(Server.java:329)
       at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
       at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
       at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
       at com.hp.ucmdb.server.Main.main(Main.java:23)
       at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
       at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
       at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
       at java.lang.reflect.Method.invoke(Method.java:498)
       at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
       at java.lang.Thread.run(Thread.java:745)
```

Solution A:

Check the **verify_store_pass.log** (in the **C:\hp\UCMDB\UCMDBServer\runtime\log** folder), if you see the following message:

```
INFO: server-storepass.conf file exists and it contains keystore and truststore.
```

Do the following:

1. Stop the UCMDB Server.
2. Run commands.
   a. Check keystore password.

      Windows:

      From **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, run the following commands.

      ```
      keytool -list -keystore
      C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
      ```

      Linux:

      From **/opt/hp/UCMDB/UCMDBServer/bin/jre/bin**, run the following commands:

      ```
      ./keytool -list -keystore
      /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore
      ```

      Enter the password that you set up during the installation of UCMDB server. If you see the following message:

      ```
      keytool error: java.io.IOException:Keystore was tampered with, or password
      was incorrect.
      ```

      Then the password was not properly set, and you need to change keystore and truststore passwords using keytool.

   b. Change the store password:

      Windows:

      ```
      keytool -storepasswd -new <new_keystore_pass> -keystore
      C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
      <current_keystore_pass>
      ```

      Linux:

      ```
      ./keytool -storepasswd -new <new_keystore_pass> -keystore
      /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore -storepass
      <current_keystore_pass>
      ```

   c. Change the key password (if the store is not empty):

      Windows:

      ```
      keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass>
      -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
      ```

Linux:

```
./keytool -keypasswd -alias <alias> -keypass <currentPass> -new
<newPass> -keystore
/opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore
```

d. Change the trust store password:

Windows:

```
keytool -storepasswd -new <new_truststore_pass> -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore -storepass
<current_truststore_pass>
```

Linux:

```
./keytool -storepasswd -new <new_truststore_pass> -keystore
/opt/hp/UCMDB/UCMDBServer/conf/security/server.truststore -storepass
<current_truststore_pass>
```

3. Start the UCMDB Server service.

Solution B:

Check the **verify_store_pass.log**, if you see the following message:

```
INFO:  keystore password and truststore password don't exist.
```

Or the following:

```
INFO:  server-storepass.conf file doesn't exist.
```

Do the following:

1. Generate the **server-storepass.conf** file.

   Windows:

   From the **C:\hp\UCMDB\UCMDBServer\bin** folder, run the following command:

   ```
   key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   Linux:

   From the **/opt/hp/UCMDB/UCMDBServer/bin** folder, run the following command:

   ```
   ./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   where `<fips_mode>` can be only set to **true** or **false**. For non-FIPS mode UCMDB server, **false** for `<fips_mode>`.

2. Stop the UCMDB Server.
3. Change keystore password and truststore password with keytool.

   From the **C:\hp\UCMDB\UCMBServer\bin\jre\bin** (Windows) or **/opt/hp/UCMDB/UCMBServer/bin/jre/bin** (Linux) folder, run the following commands:

   a. Change the store password:

   Windows:

   ```
   keytool -storepasswd -new <new_keystore_pass> -keystore
   C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
   <current_keystore_pass>
   ```

   Linux:

   ```
   ./keytool -storepasswd -new <new_keystore_pass> -keystore
   /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore -storepass
   <current_keystore_pass>
   ```

   b. Change the key password (if the store is not empty):

   Windows:

   ```
   keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass>
   -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
   ```

   Linux:

   ```
   ./keytool -keypasswd -alias <alias> -keypass <currentPass> -new
   <newPass> -keystore
   /opt/hp/UCMDB/UCMDBServer/conf/security/server.keystore
   ```

   c. Change the trust store password:

   Windows:

   ```
   keytool -storepasswd -new <new_truststore_pass> -keystore
   C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore -storepass
   <current_truststore_pass>
   ```

   Linux:

   ```
   ./keytool -storepasswd -new <new_truststore_pass> -keystore
   /opt/hp/UCMDB/UCMDBServer/conf/security/server.truststore -storepass
   <current_truststore_pass>
   ```

4. Start the UCMDB Server service.

Solution C:

If you only changed keystore password or truststore password during UCMDB server installation, and then server startup failed and the **startup.log** shows similar error messages as shown above. You can follow the instructions provided in Solution A or Solution B, but you need to change the keystore password or truststore password that you set during installation.

For example, if you only changed truststore password during installation and you need to generate **server-storepass.conf**, run the following command:

Windows: `key-truststore.bat <fips_mode> null <new_truststore_pass>`

Linux: `./key-truststore.sh <fips_mode> null <new_truststore_pass>`

Problem: You have changed schema in UCMDB Server. The server startup failed and the **startup.log** shows the following message:

```
2017-05-04 08:32:17,074  ERROR  [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
        at org.eclipse.jetty.server.Server.doStart(Server.java:329)
        at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
        at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
        at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
        at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
        at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
        at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
        at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
        at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
        at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
        at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
        at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
        at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
        at
```

```
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
        at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
        at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
        at com.hp.ucmdb.server.Main.main(Main.java:23)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:498)
        at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
        at java.lang.Thread.run(Thread.java:745)
```

Solution: You need to re-generate **server-storepass.conf**, because the new schema does not store any keystore and truststore passwords.

- If you remember what passwords were specified previously, you can generate the **server-storepass.conf** file with the following command:

  Windows: `key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>`

  Linux: `./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>`

  where `<fips_mode>` can be only set to **true** or **false**. For non-FIPS mode UCMDB server, **false** for `<fips_mode>`.

- If you don't remember the passwords, follow the instructions in Solution B to regenerate the passwords.

Troubleshooting Keystore and Truststore - FIPS mode

Problem: If starting the UCMDB server failed, and the **startup.log** shows message similar to the following:

```
2017-05-04 08:32:17,074  ERROR  [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
       at org.eclipse.jetty.server.Server.doStart(Server.java:329)
       at org.eclipse.jetty.util.component.AbstractLifeCycle.start
```

```
(AbstractLifeCycle.java:68)
       at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
       at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
       at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
       at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
       at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
       at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
       at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
       at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
       at com.hp.ucmdb.server.Main.main(Main.java:23)
       at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
       at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
       at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
       at java.lang.reflect.Method.invoke(Method.java:498)
       at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
       at java.lang.Thread.run(Thread.java:745)
```

Solution A:

Check the **verify_store_pass.log**, if you see the following message:

```
INFO: server-storepass.conf file exists and it contains keystore and truststore.
```

Do the following:

1. Change the keystore and truststore passwords using keytool.

   For detailed instructions, see the "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" section in the *HPE Universal CMDB FIPS*

Deployment Guide.

2. Start the UCMDB Server service.

Solution B:

Check the **verify_store_pass.log**, if you see the following message:

```
INFO:  keystore password and truststore password don't exist.
```

Or the following:

```
INFO:  server-storepass.conf file doesn't exist.
```

Do the following:

1. Make sure you have stopped the UCMDB Server.
2. Generate the **server-storepass.conf** file.

   Windows:

   From **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, run the following command:

   ```
   key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   Linux:

   From **opt/UCMDB/UCMBServer/bin/jre/bin**, run the following command:

   ```
   ./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>
   ```

   where `<fips_mode>` can be only set to **true** or **false**. For FIPS mode UCMDB server, **true** for `<fips_mode>`.

3. Change the keystore and truststore passwords using keytool.

   For detailed instructions, see the "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" section in the *HPE Universal CMDB FIPS Deployment Guide*.

4. Start the UCMDB Server service.

Solution C:

If you only changed keystore password or truststore password during UCMDB server installation, and then server startup failed and the **startup.log** shows similar error messages as shown above. You can follow the instructions provided in Solution A or Solution B, but you need to change the keystore password or truststore password that you set during installation.

For example, if you only changed truststore password during installation and you need to generate **server-storepass.conf**, run the following command:

Windows: `key-truststore.bat <fips_mode> null <new_truststore_pass>`

Linux: `./key-truststore.sh <fips_mode> null <new_truststore_pass>`

Troubleshooting and Limitations – Package Manager

This section describes some of the troubleshooting issues that might arise when deploying and undeploying packages.

This section includes the following topics:

Gold Master Reports Cannot be Deployed by Package Manager

If you export a package's resources from Package Manager that includes a Gold Master report definition, and then export those resources again to another system, the Gold Master report definition is not deployed.

Datamodel Resources Cannot Be Undeployed

For a list of the package resources, see Package Resources.

Additional Information on Package Deployment Failure

If package deployment fails, you can check the Package Manager log files for additional information on why the deployment failure occurred.

Log files are located in the **C:\hp\UCMDB\UCMDBServer\runtime\log** folder.

Package Creation and Deployment in a Non-English Locale

This section describes the limitations when working in a non-English locale.

- You cannot deploy a package if the server locale is different than the client locale and the package name contains non-English characters.
- You cannot create a package that contains resources (for example, views and TQL queries) having non-English characters in their names, if the server locale is different from the client locale.

UCMDB Browser - Known Issues

Problem: Performance for the UCMDB Browser is slow.

- **Possible Solution**: Add the variable **CATALINA_OPTS** to the Operating Systems environment variables with values:

  -Xms512M -Xmx4096M

Problem: The Tomcat log that contains requests to the UCMDB Browser and their HTTPS codes becomes too large and is unreadable.

- Solution: Comment out the following lines in the **server.xml** file, located in ***<UCMDB_Browser_installation_directory>*\webapps\release\conf**:

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%h %l %u %t &quot;%r&quot; %s %b" />
```

Problem: Icons are not displayed when the Turn Off Data URI support setting is not disabled.

- Solution: Disable the **Turn Off Data URI support** setting on Windows as follows:

a. Click **Start**, type **gpedit.msc** in the **Start Search** box, and then press **ENTER**.

b. In the navigation pane of the Local Group Policy Editor window, expand **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features.**

c. In the right pane, double-click **Turn Off Data URI support**.

d. Select **Enabled**, click **Apply**, and then click **OK**.

e. Go back to the navigation pane of the Local Group Policy Editor window, expand **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features.**

f. Repeat step 3 and step 4.

Troubleshooting - Configure the Enhanced Search Engine

UCMDB doesn't start because of the search subsystem manager. What do I do?

Stop UCMDB, delete the folder **<UCMDB installation folder>/search**, then restart UCMDB.

If the search still does not start, disable it, as explained in "Troubleshooting - Configure the Enhanced Search Engine" above and revert to the legacy search engine.

The search doesn't return any results.

In the Topology Search JMX, invoke the following methods:

- **restoreFactoryDefaults:** This restores factory configuration for the search.
- **reindex:** This recreates a search index for CIs in the UCMDB model. Note, this can take up to several hours for large databases (approx 1M CIs/hour).

  You can also invoke the **reindexCiType** method to re-index all the CIs of a given CI type from the CMDB model database.

The search doesn't find CI types that I want.

There are several different possible causes for this. Check the following:

- Check that the attribute and CI type are indexable according to the indexing configuration. If they are not, add the class attributes configuration item as explained "Troubleshooting - Configure the Enhanced Search Engine" on the previous page.
- Check that you have correct synonyms defined for the class in Class synonyms.
- Check that **rating** and **pageItemCount** for this CI are non-zero. Check for **rating** in the Attribute ranking and for **pageItemCount** in Presentable CI types.

Cardinality conditions don't work or return incorrect results.

In addition to checking attribute synonyms, check that the attribute type is defined as numeric in Indexing Configuration and that units configuration matches attribute units in **Search_Parser_Configuration_XML**.

The search presents too many unwanted results.

- Check if you are you using queries with natural language. This can limit results of the "best guess" of what the user intended.
- If you need to be 100% certain that your query returns results only of one specific CI type, use type: **ci-type** filter in the query.
- If the two suggestions above don't help, contact the R&D team with your use case and status report from JMX.

Problem with configuration - restore factory defaults

To restore the default configuration XML files from the factory content, go to **JMX Console > UCMDB:service=Topology Search Services** and invoke the **restoreFactoryDefaults()** method.

> **Caution:** This method overwrites the current configuration. You should back up the configuration files before invoking it.

Logs and debugging info

Logs

search.log logs everything related to searches. Default log level is INFO, only statistics are printed. The log level and number of logs are configured with the **search.loglevel** variable in **conf/log/cmdb.properties**.

Status Report

The topology search JMX status report displays all current configuration tables and statistics for the search engine component. It is useful to include it when reporting issues to R&D.

Content of Solr Database

By default, the Solr search engine is embedded inside UCMDB server. To query it directly, go to **JMX Console > UCMDB:service=Topology Search Services** and invoke the **debugSolrQuery()** method.

Example queries:

- empty query returns all CIs
- "id:a6693cd46cfd1b4fab0c3551bac9289e" returns a CI with cmdbId a6693cd46cfd1b4fab0c3551bac9289e. This uses Solr/Lucene syntax.

Troubleshooting - FIPS Deployment

Troubleshooting the Data Flow Probes

- When probes finish upgrading, the new keystore/truststore is in place. If the UCMDB Server does not perform the last step of turning on FIPS, and HTTPs communication is enabled, in the UCDMB UI, you will see probe disconnected until the UCMDB Server replaces the new FIPS keystore/truststore in JMX.
- If you want to find out whether an agent has been switched to the FIPS mode, follow the steps below:

  a. Run the **UDA Status Collector** job.

     In UCMDB UI, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab **> Discovery Modules** tree **> Tools and Samples > UD Agent Management**, right-click **UDA Status Collector**, and select **Activate**.

  b. Access the Data Flow Probe JMX console: On the probe machine, launch a Web browser and enter the following address: **https://localhost:8453**.

     You may have to log in with a user name and password.

c. Locate the **exportUdaStatus** method, provide the path, for example, **C:**, and then click **Invoke**.

d. Go to the probe node and find the **uda_status.csv** file under the path you specified and open it.

e. Check the **agentVersion** column in the file. If the **agentVersion** value is in the **<agent version>-fips** format, for example, **v10.33.000 build:185-fips**, then it means the agent has been migrated to FIPS mode successfully. Otherwise, it is still a non-FIPS agent.

f. Count the rows where **agentVersion** value is in the **<agent version>-fips** format.

- **Problem:** If HTTPS communication is enabled on the UCMDB Server side, after the UCMDB server is switched to FIPS mode, data flow probes cannot connect to the UCMDB server.

  Solution: Update keystore and truststore values in the **ssl.properties** file (located in the **<*DataFlowProbe_Home*>\conf\security** directory) manually.

  To do so,

  a. Open the **ssl.properties** file in a text editor.

  b. Locate the following two lines:

  ```
  javax.net.ssl.keyStore=HPProbeKeyStore.jks
  javax.net.ssl.trustStore=HPProbeTrustStore.jks
  ```

  c. Update the values for the two settings manually to the following:

  ```
  javax.net.ssl.keyStore=FIPS_HPProbeKeyStore.jks
  javax.net.ssl.trustStore=FIPS_HPProbeTrustStore.jks
  ```

  d. Save the file.

  e. Restart the Probe.

- **PROBLEM:** After adding a new probe to the UCMDB server that was already switched to the FIPS mode, the automatic FIPS switch process for the new probe might fail. This is because once the newly installed probe is started, it downloads all the resources from the UCMDB server, and when the probe gets the probe upgrade package, it would schedule a restart, which blocks the automatic FIPS Switch process. (QCCR1H106144)

  Workaround: Once you find that the automatic FIPS Switch process for a new probe failed,

  a. Copy the jar files of Zulu JCE Unlimited Strength Policy Files 8 into the **%\DataFlowProbe_HOME%\bin\jre\lib\security** directory on the Data Flow Probe machine.

  b. Add the following line into the **DataFlowProbe.properties** file on the Data Flow Probe

machine, and then save the file.

```
probe.fips.status=1
```

c. Restart the Data Flow Probe.

> **Note:** If the Data Flow Probe is in separate mode, you need to perform the above steps for both the Probe Manager and Probe Gateway.

- **PROBLEM:** After switching to the FIPS mode, you cannot log in to the Data Flow Probe JMX Console using some of the latest versions of Internet Explorer 11, Microsoft Edge, or Firefox. And when using these browsers you may get “Unsupported Cipher” error message.

  Workaround: To resolve the issue, do either of the following:

  - **Configure your web browser**
    - For Internet Explorer 11 or Microsoft Edge
      A. On Windows, click **Start**, in the Search box, enter **Edit Group Policy**, then click **Edit group policy** that shows under Control Panel. The Local Group Policy Editor window opens.
      B. In the navigation pane, go to **Computer Configuration > Administrative Templates > Network > SSL Configuration Settings**.
      C. In the right pane, double-click **SSL Cipher Suite Order**.
      D. In the SSL Cipher Suite Order, select the **Enabled** radio button.
      E. In the Options pane, edit the order of SSL Cipher Suites by placing a cipher that doesn't contain ECDHE in the first place.
      F. Click **Apply** and **OK**.
      G. Restart your computer.
    - For Firefox
      A. In the Address bar of the web browser, type **about:config** and press **Enter**.
      B. Click **I accept the risk!** when prompted.
      C. In the Search bar that appears below the Address bar, type **ssl3**.

         All preferences that contain **ssl3** are listed.
      D. Change the value of all Cipher preferences containing **ecdhe** to **false**.

You can enable or disable a preference by toggling its value with a double-click on the preference name. **true** indicates that the cipher suite is enabled, **false** indicates not available.

E. Restart Firefox.

- **Update the Crypto-J toolkit files to version 6.2.2**

  i. Close your web browser (Internet Explorer 11, Microsoft Edge, or Firefox).

  ii. Stop the UCMDB server and the Data Flow Probe.

  iii. Delete the browser cache under the **C:\Users\<user>\AppData\Local\Temp\UcmdbAppletJars** folder.

  iv. Obtain the Crypto-J toolkit files (**cryptojce-6.2.2.jar**, **cryptojcommon-6.2.2.jar**, and **jcmFIPS-6.2.2.jar**).

  > **Note:** For information about Crypto-J 6.2.2 files, you may go to https://community.rsa.com/community/products/bsafe/crypto-j-62.

  v. On the UCMDB server side:

  A. Delete the files under the **<UCMDB_server_home>\runtime\jetty-cache** folder.

  B. Copy the Crypto-J toolkit files (**cryptojce-6.2.2.jar**, **cryptojcommon-6.2.2.jar**, and **jcmFIPS-6.2.2.jar**) to the following folders:

  - **<UCMDB_server_home>\bin\jre\lib\ext**
  - **<UCMDB_server_home>\deploy\ucmdb-ui\static\appletJars**
  - **<UCMDB_server_home>\deploy\ucmdb-ui\WEB-INF\lib**
  - **<UCMDB_server_home>\integrations\lib**

  vi. On the Data Flow Probe side, copy the Crypto-J toolkit files (**cryptojce-6.2.2.jar**, **cryptojcommon-6.2.2.jar**, and **jcmFIPS-6.2.2.jar**) from the **<UCMDB_server_home>\lib** directory, and place them inside the **<DataFlowProbe>\lib** folder (for example, **C:\hp\UCMDB\DataFlowProbe\lib**).

  vii. Restart the UCMDB server and the Data Flow Probe.

Troubleshooting the UCMDB Server

- **Manual steps to make a reader server FIPS ready**

  In case the **enableFipsMode** JMX method reports a failure for a reader server, you can perform several manual steps to make the reader server FIPS-ready.

  > **Note:** These steps are applicable only when the switch to FIPS mode was successful on the writer server.
  >
  > The JMX output page displayed after the **enableFipsMode** JMX method is executed contains detailed information about the status of the switch to FIPS mode on all the HA cluster servers. Only when the switch to FIPS mode was successful on the writer server, but failed on a reader server, you can follow the steps below to make the reader server FIPS ready.

  a. Stop all the servers in the HA cluster, including the writer server.

  b. Start only the writer server.

     After the first startup since FIPS was enabled, the newly generated FIPS compliant files will reside on the writer's file system. To make the reader server FIPS ready, you need to manually copy these files to the reader server.

  c. Copy the **encryption.bin** and **cmdbSuperIntegrationCredentials.bin** files from the writer server's **<*UCMDB_Server_Home*>/conf/persistence** folder and place them in the corresponding location on the reader server.

  d. Copy the **fips.conf** file from the writer server's **<*UCMDB_Server_Home*>/bin** directory and place it in the corresponding directory on the reader server.

  e. Copy the **cmdb.conf** file from the writer server's **<*UCMDB_Server_Home*>/conf** folder and place it in the corresponding directory on the reader server.

     > **Note:** If necessary, correct the database connection details in the **dal.datamodel.host.name** parameter from the **cmdb.conf** file.

  f. Start the reader server.

- **Switch to FIPS JMX output and important log files**

  When switching the UCMDB Server to FIPS mode, the JMX output result should print information about whether the switch to FIPS mode succeeded on all the servers from the HA cluster:

JMX Search JMX List Operations Index Back to MBean Reinvoke MBean (Current Server is a writer:<Writer Server Id>)

Mbean: UCMDB:service=Security Services. Method: enableFIPSMode

```
Unlimited key strength is supported on the writer server.
Encrypt and Decrypt test using the unlimited strength jurisdiction policy files has passed on the writer server.
Unlimited key strength policy resources were successfully uploaded to URM from the filesystem.
Unlimited key strength policy jars were deployed as discovery resources.

Going to check whether the reader servers are ready for Fips:
Reader server      <Reader Server Id>       is ready for enabling Fips mode.

Fips mode enabled successfully on the writer server.

The status of enabling FIPS mode on the reader servers:
Reader server:     <Reader Server Id>         FIPS mode enabled status: true
Please proceed with restarting the HA Cluster for the Fips configuration changes to take effect.
```

The relevant logs that can be checked for detailed information are:

- **security.log** - contains detailed information about the switch to FIPS mode process. The following output is present in the **security.log** after calling the **enableFIPSMode** JMX method:

```
2017-07-10 19:18:13,155  INFO   [qtp325079998-215] - Switch to FIPS mode started:
2017-07-10 19:18:13,155  INFO   [qtp325079998-215] - Starting decrypt with Legacy
Providers.
2017-07-10 19:18:13,155  INFO   [qtp325079998-215] - Triggering the Master Key Decrypt
step.
...
...
2017-07-10 19:18:14,130  INFO   [qtp325079998-215] - Perform decrypt test for the new
super integration user file.
2017-07-10 19:18:14,131  INFO   [qtp325079998-215] - Super Integration user credentials
from new file are matching the credentials from input? Result: true
2017-07-10 19:18:14,131  INFO   [qtp325079998-215] - Switch to FIPS mode validation
succeeded!
```

After calling the **enableFIPSMode** JMX method, a lot of the FIPS changes will be present in temporary files on disk. When the UCMDB Server is restarted, the security log should also print details about the switch between the temporary and current files:

```
2017-07-10 19:25:33,382  INFO   [WrapperSimpleAppMain] - Copy new conf file:
..\conf\new_cmdb.conf into old one: ..\conf\cmdb.conf
2017-07-10 19:25:33,395  INFO   [WrapperSimpleAppMain] - New conf file was deleted?
true
2017-07-10 19:25:33,432  INFO   [WrapperSimpleAppMain] - Copy new file:
..\conf\persistence\encryption.bin.new into old one: ..\conf\persistence\encryption.bin
2017-07-10 19:25:33,439  INFO   [WrapperSimpleAppMain] - Going to delete:
..\conf\persistence\encryption.bin.new
2017-07-10 19:25:33,439  INFO   [WrapperSimpleAppMain] - Copy new file:
..\conf\persistence\cmdbSuperIntegrationCredentials.bin.new into old one:
..\conf\persistence\cmdbSuperIntegrationCredentials.bin
2017-07-10 19:25:33,443  INFO   [WrapperSimpleAppMain] - Going to delete:
..\conf\persistence\cmdbSuperIntegrationCredentials.bin.new
2017-07-10 19:25:36,239  INFO   [WrapperSimpleAppMain] - Master key was loaded with
success into memory!
2017-07-10 19:28:00,666  INFO   [WrapperSimpleAppMain] - LWSSO in FIPS mode
```

```
2017-07-10 19:28:00,666  INFO   [WrapperSimpleAppMain] - Reload configuration with
filename lwsso/ucmdb_fips_mode_lwsso_conf.xml
2017-07-10 19:28:00,819  INFO   [WrapperSimpleAppMain] - LWSSO in FIPS mode
2017-07-10 19:28:00,819  INFO   [WrapperSimpleAppMain] - Reload configuration with
filename lwsso/ucmdb_fips_mode_lwsso_conf.xml
```

- **startup.log** - contains information which can be consulted to determine whether the UCMDB server has performed the switch to FIPS.

```
2017-07-10 19:25:33,450  INFO   [WrapperSimpleAppMain] -
************************************
2017-07-10 19:25:33,450  INFO   [WrapperSimpleAppMain] - *******  Starting Framework
*******
2017-07-10 19:25:33,458  INFO   [WrapperSimpleAppMain] - ***  Java Version: 1.8.0_92
2017-07-10 19:25:33,471  INFO   [WrapperSimpleAppMain] - ***  CMDB Version: 10.33.185
2017-07-10 19:25:33,471  INFO   [WrapperSimpleAppMain] - ***  Java Home:
C:\hp\UCMDB\UCMDBServer\bin\jre
2017-07-10 19:25:33,472  INFO   [WrapperSimpleAppMain] - ***  OS Name:      Windows
Server 2008 R2 6.1
2017-07-10 19:25:33,472  INFO   [WrapperSimpleAppMain] -
************************************
2017-07-10 19:25:33,472  INFO   [WrapperSimpleAppMain] - Fips mode is enabled.
2017-07-10 19:25:33,472  INFO   [WrapperSimpleAppMain] - Switching to secure providers
2017-07-10 19:25:34,280  INFO   [WrapperSimpleAppMain] - Removing the current SunJSSE
provider.
2017-07-10 19:25:34,280  INFO   [WrapperSimpleAppMain] - Adding the new SunJSSE
provider which is configured in FIPS mode.
2017-07-10 19:25:34,280  INFO   [WrapperSimpleAppMain] - Changed SunJSSE to use JSafe
for SSL.
2017-07-10 19:25:34,280  INFO   [WrapperSimpleAppMain] - Added the JSafe provider.
2017-07-10 19:25:34,300  INFO   [WrapperSimpleAppMain] - Start framework init
```

- **Decryption error**

  In case a decryption error occurs, and the UCMDB server cannot start up, you can do the following:

  a. Regenerate the **server-fips.keystore/server-fips.truststore** files.

     For detailed instructions, see Regenerate a new self-signed hpcert and sign it with the default UCMDB root certificate.

  b. Synchronize password in the database by running the following command:

```
<UCMDBServer>\bin\key-truststore.bat <FIPS or not? true for FIPS>
<keystore password> <truststore password>
```

     Example:

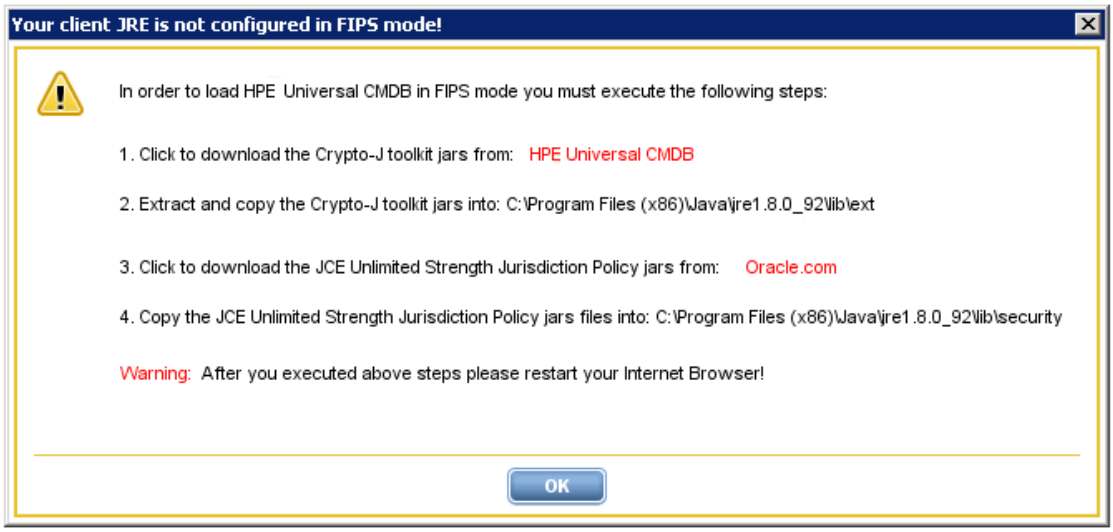
```
C:\hp\UCMDB\UCMDBServer\bin\key-truststore.bat true mykeystorepass
mytruststorepass
```

Troubleshooting the UCMDB UI

1. **Applet FIPS preliminary checks**

   After performing login in the UCMDB UI, there are basic checks done to make sure the Crypto J toolkit and the JCE Unlimited Strength Policy Files are present in the correct location in the JRE.

   Pop-up example from the UCMDB UI when the Crypto J toolkit jars and the Unlimited Strength Policy Files are missing:

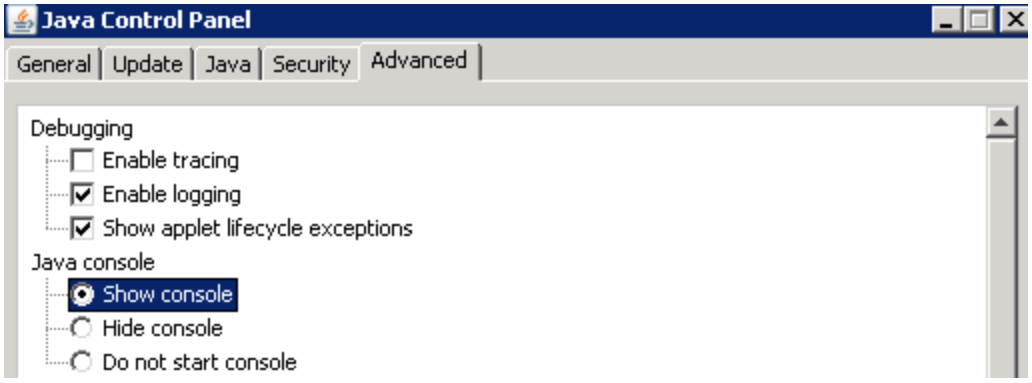


2. **Troubleshooting the SSL Communication between the UCMDB UI and the UCMDB Server**

   To investigate applet loading issues and SSL communication issues between the UCMDB UI and the UCMDB Server, HPE recommends you to enable the Java console from the Java Control Panel.

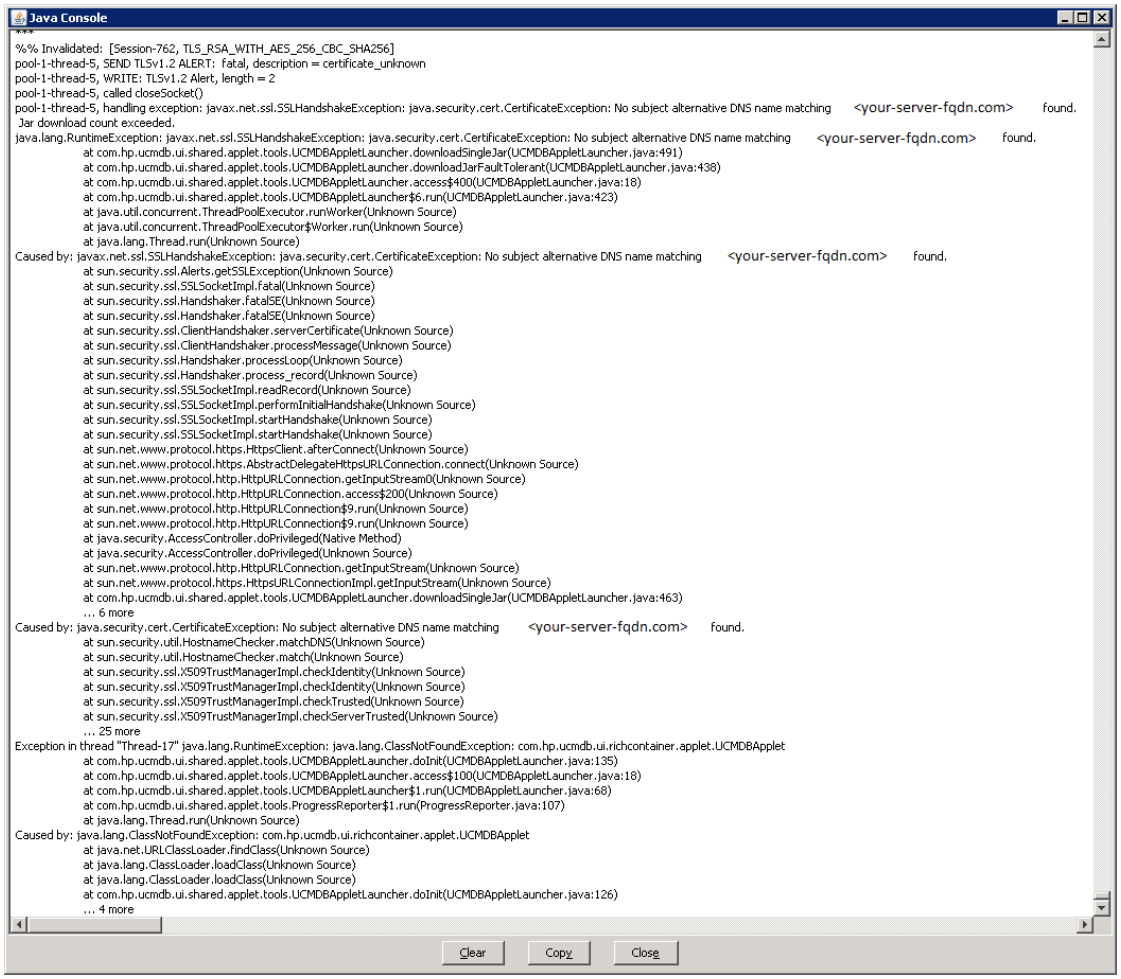
   a. In the **Advanced** tab of the Java Control Panel, under the **Java Console** category, select the **Show console** radio button.

b. Make sure that under the **Debugging** category, the **Enable logging** radio button is selected.



In addition to enabling the Java console, you should also add the `-Djavax.net.debug=ssl` parameter to the **JAVA_TOOL_OPTIONS** environment variable. (The environment variable should be present on the client machine if you performed steps in "Task 5. UCMDB UI Migration" for enabling the FIPS mode). After adding the SSL debug flag, you can inspect the output from the Java console when the UCMDB UI is loading.

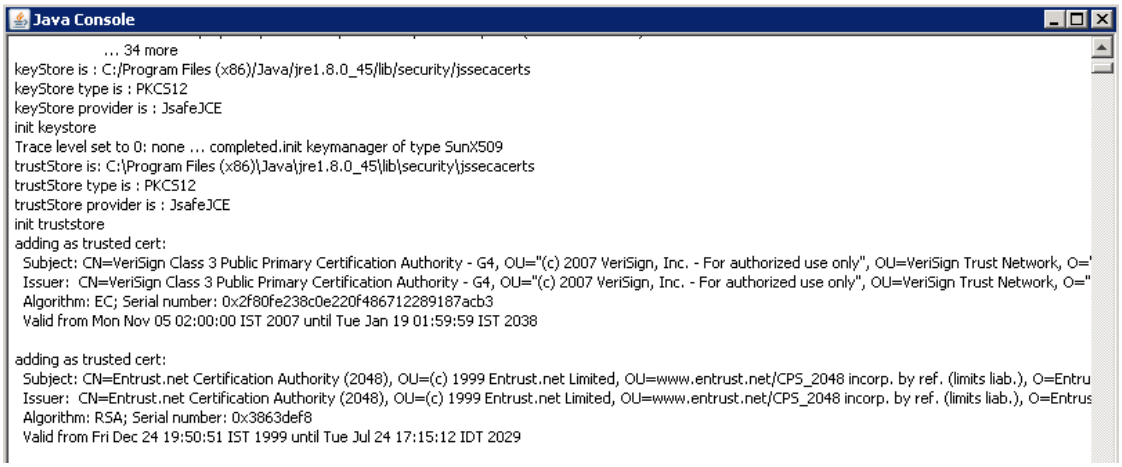
As an example on how to troubleshoot applet issues, we will use the default hpcert limitation. The default hpcert certificate from **server-fips.keystore** uses a SAN extension with DNS field set to **localhost**. This limits the access to the UCMDB UI only from the UCMDB Server Machine (localhost). That is to say, UCMDB UI must be on the same machine with UCMDB Server, and you can only use URL **https://localhost:8443/** to access the UCMDB Server, neither **https://<UCMDB_Server_Name>:8443/** nor **https://<UCMDB_Server_IP_Address>:8443/**. In case we try to access the UI with FQDN from a machine different than localhost, since the SAN extension DNS name (localhost) from the certificate does not match the URL we have used to access the UI (FQDN of the UCMDB Server), an SSL exception will be thrown in the Java Console and the loading of the UCMDB UI will stop.



```
Java Console
%% Invalidated:  [Session-762, TLS_RSA_WITH_AES_256_CBC_SHA256]
pool-1-thread-5, SEND TLSv1.2 ALERT:  fatal, description = certificate_unknown
pool-1-thread-5, WRITE: TLSv1.2 Alert, length = 2
pool-1-thread-5, called closeSocket()
pool-1-thread-5, handling exception: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching <your-server-fqdn.com> found.
 Jar download count exceeded.
java.lang.RuntimeException: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching <your-server-fqdn.com> found.
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.downloadSingleJar(UCMDBAppletLauncher.java:491)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.downloadJarFaultTolerant(UCMDBAppletLauncher.java:438)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.access$400(UCMDBAppletLauncher.java:18)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher$6.run(UCMDBAppletLauncher.java:423)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
        at java.lang.Thread.run(Unknown Source)
Caused by: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching <your-server-fqdn.com> found.
        at sun.security.ssl.Alerts.getSSLException(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.fatal(Unknown Source)
        at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
        at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
        at sun.security.ssl.ClientHandshaker.serverCertificate(Unknown Source)
        at sun.security.ssl.ClientHandshaker.processMessage(Unknown Source)
        at sun.security.ssl.Handshaker.processLoop(Unknown Source)
        at sun.security.ssl.Handshaker.process_record(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.readRecord(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)
        at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)
        at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.getInputStream0(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.access$200(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection$9.run(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection$9.run(Unknown Source)
        at java.security.AccessController.doPrivileged(Native Method)
        at java.security.AccessController.doPrivileged(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.getInputStream(Unknown Source)
        at sun.net.www.protocol.https.HttpsURLConnectionImpl.getInputStream(Unknown Source)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.downloadSingleJar(UCMDBAppletLauncher.java:463)
        ... 6 more
Caused by: java.security.cert.CertificateException: No subject alternative DNS name matching <your-server-fqdn.com> found.
        at sun.security.util.HostnameChecker.matchDNS(Unknown Source)
        at sun.security.util.HostnameChecker.match(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.checkIdentity(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.checkIdentity(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.checkTrusted(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(Unknown Source)
        ... 25 more
Exception in thread "Thread-17" java.lang.RuntimeException: java.lang.ClassNotFoundException: com.hp.ucmdb.ui.richcontainer.applet.UCMDBApplet
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.doInit(UCMDBAppletLauncher.java:135)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.access$100(UCMDBAppletLauncher.java:18)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher$1.run(UCMDBAppletLauncher.java:68)
        at com.hp.ucmdb.ui.shared.applet.tools.ProgressReporter$1.run(ProgressReporter.java:107)
        at java.lang.Thread.run(Unknown Source)
Caused by: java.lang.ClassNotFoundException: com.hp.ucmdb.ui.richcontainer.applet.UCMDBApplet
        at java.net.URLClassLoader.findClass(Unknown Source)
        at java.lang.ClassLoader.loadClass(Unknown Source)
        at java.lang.ClassLoader.loadClass(Unknown Source)
        at com.hp.ucmdb.ui.shared.applet.tools.UCMDBAppletLauncher.doInit(UCMDBAppletLauncher.java:126)
        ... 4 more
Clear   Copy   Close
```

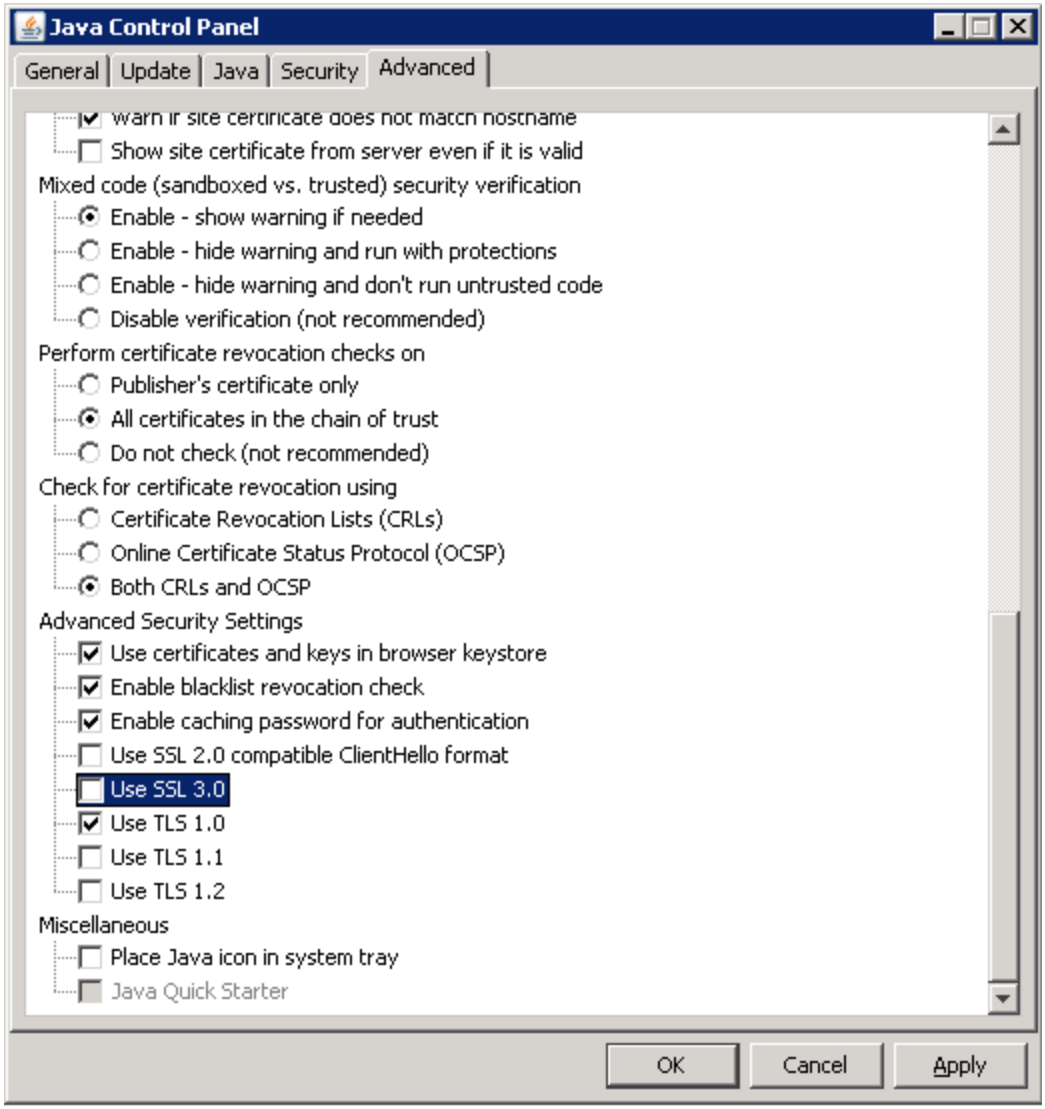
This issue should not appear if you have followed the instructions in the "4. UCMDB Server Migration" section, because a new hpcert certificate will be generated with appropriate SAN extensions (containing correct DNS names).

3. **Make sure the jssecacerts is loaded by the client JRE by checking the java console.**



4. **Customize JRE 7 to use FIPS compliant protocols**

   If you use use JRE 7 for loading the UCMDB UI, make sure only TLS protocols are checked in the Java Control Panel. You need to un-check SSL 3.0.



Troubleshooting - High Availability Mode

Upon every startup of the UCMDB server, the server sends a test message to the cluster to verify if it successfully connected to the cluster. If there is a problem with the connection, the message fails and the server is stopped to avoid the whole cluster getting stuck.

Some examples of wrong cluster encryption configuration are:

- Disabled encryption on one node when another node enabled it.
- Wrong or missing cluster.encryption.keystore

- Wrong or missing key in the keystore

If the server gets stuck because of a configuration issue, the error message is:

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - #### Server failed to connect properly
to the cluster and its service is stopped! Please fix the problem and start it
again ####
```

```
2012-09-11 17:48:23,586 [Thread-14] FATAL -       Potential problems can be: wrong
security configuration (wrong or missing cluster.encryption.keystore, wrong key,
disabled encryption in a cluster with enabled encryption)
```

Chapter 4: Troubleshooting Data Flow Management

This chapter includes:

Troubleshooting and Limitations – Data Flow Probe Setup

Data Flow Probe Setup - Troubleshooting

Problem: You cannot transfer a Data Flow Probe from one domain to another.

Reason: Once you have defined the domain of a Probe, you can change its ranges, but not the domain.

Solution: Install the Probe again:

1. (Optional) If you are going to use the same ranges for the Probe in the new domain, export the ranges before removing the Probe. For details, see Ranges Pane.
2. Remove the existing Probe from UCMDB. For details, see the **Remove Domain or Probe** button in Data Flow Probe Setup Window.
3. Install the Probe. For details, see the section about installing the Data Flow Probe in the interactive *HPE Universal CMDB Deployment Guide*.
4. During installation, make sure to give the new Probe a different name to the name given to the old Probe, or make sure you delete the reference to Probe from the original domain.

Problem: Discovery shows a disconnected status for a Probe.

Solution: Check the following on the Probe machine:

- That the Probe is running
- That there are no network problems

Solution: The probe status is **Disconnected** or **Disconnected (being restarted)**.

- Search for restart messages in the **wrapperProbeGW** logs.
- If the probe does not restart, try to take probe thread dump from the disconnected time and search for the **ProbeGW Tasks Downloader** thread.
- If there is no probe thread dump, investigate the problematic timeframe in the **wrapperProbeGw**

log. In particular:

- Check if the probe tasks confirmer has been running for more than 5 minutes.
- Check if some of the resources are being downloaded for more than 5 minutes.

Problem: The connection between the Universal CMDB server and the Probe fails due to an HTTP exception.

Solution: Ensure that none of the Probe ports are in use by another process.

Problem: A Data Flow Probe node name cannot be resolved to its IP address. If this happens, the host cannot be discovered, and the Probe does not function correctly.

Solution: Add the host machine name to the Windows HOSTS file on the Data Flow Probe machine.

Problem: After uninstalling the Data Flow Probe, mysqld.exe and associated files are not deleted.

Solution: To delete all files, restart the machine on which the Data Flow Probe was installed.

Problem: After the UCMDB Server CUP is updated, the Probe fails to start or fails to connect to server

Solution: The Probe's CUP version must be the same as UCMDB Server's CUP version. If the CUP versions are not aligned, you must update the Probe's CUP version. To do this, see How to Deploy a Data Flow Probe CUP.

In some cases, the CUP may need to be deployed manually on a Probe. For details, see How to Deploy a Data Flow Probe CUP Manually.

Problem: I want to check if my integration probe is connected, but I can't see it listed in the Data Flow Probe Setup module tree.

Reason: The Data Flow Probe Setup module displays only Data Flow Probes for discovery. Integration Probes—that is, Probes on Linux machines, and Windows Probes configured for integration only— are not displayed in the Data Flow Probe Setup module.

Workaround: To see if an integration Probe is connected, create a dummy integration point and verify that the Probe is listed among the Probes that can be selected for the integration point (in the **Data Flow Probe** field). For details, see How to Set Up an Integration Point.

Problem: Troubleshooting PostgreSQL Issues

Solution:

The table below lists the Data Flow Probe database scripts. These scripts can be modified for administration purposes, both in Windows and Linux environments.

> **Note:**
>
> - The scripts are located on the Data Flow Probe machine, in the following location:
> - **Windows: C:\hp\UCMDB\DataFlowProbe\tools\dbscripts**
> - **Linux: /opt/hp/UCMDB/DataFlowProbe/tools/dbscripts**
> - Data Flow Probe database scripts should be changed for specific administration purposes only.

Script	Description
exportPostgresql [PostgreSQL root account password]	Exports all data from the DataFlowProbe database schema to **data_flow_probe_ export.bin** in the current directory
importPostgresql [Export file name] [PostgreSQL root account password	Imports data from a file created by the **exportPostgresql** script into the DataFlowProbe schema
enable_remote_user_access	Configures the PostgreSQL Data Flow Probe account to be accessible from remote machines
remove_remote_user_access	Configures the PostgreSQL Data Flow Probe account to be accessible only from the local machine (default)
set_db_user_password [new PostgreSQL Data Flow Probe account password] [PostgreSQL root account password]	Modifies the PostgreSQL Data Flow Probe account password
set_root_password [new PostgreSQL root account password] [Current PostgreSQL root account password]	Modifies the PostgreSQL root account password

Problem: The Data Flow Probe database service cannot start.

- **Reason:** Hosts machine must not contain "**localhost**".

  Solution: On the Data Flow Probe machine, open

  - Windows: **%systemroot%\system32\drivers\etc\hosts**
  - Linux: **/etc/hosts**

  and ensure that all lines containing "**localhost**" are commented out.

- **Reason: Microsoft Visual C++ 2010 x64 Redistributable** is installed during the installation of the Probe. If for some reason this redistributable is uninstalled, PostgreSQL stops working

  Solution: Check if Microsoft Visual C++ 2010 x64 Redistributable is installed. If not, reinstall it.

Data Flow Probe Setup - Limitations

- When the Probe is running in separate mode on a machine where both the Gateways and the Manager share a same installation folder, the Data Flow Probe CUP must be installed manually. For details, see How to Deploy a Data Flow Probe CUP Manually.
- Data Flow Probe CUPs that were deployed manually can be uninstalled using manual methods only. For details, see How to Uninstall Probe CUPs Manually.
- Universal Discovery Agent may not callhome in, but not limited to, the following scenario:
  - The callhome IP address that is configured on the Universal Discovery Agent belongs to a client type range that is added to a cluster.

    > **Note:** The Universal Discovery Agent supports 1 primary and 1 secondary probe.

  - The range is a member of a probe cluster.
  - The cluster contains two or more probes.

  In this scenario, callhome may not work as expected. Contact HPE Support for assistance in configuring callhome.

Troubleshooting Probe Auto Upgrade

Troubleshooting Probe Auto Upgrade - General

- **Limitation:** If the auto upgrade fails, retry will not resolve the issue. You need to access the corresponding probe server and perform manual deployment of version 10.33 probe.
- **Known Issue:** The **C:\hp\UCMDB\temp** folder was created and used by the probe auto upgrade agent during the upgrade process. If you see this folder on your probe server, you can just ignore it, or safely remove it. It has no functional impact.
- **Check if resources are placed under the right place after UCMDB server is upgraded to version 10.33**

  a. Check if the Data Flow Probe installer is placed under the right place

     Go to the **<UCMDB_Server>\content\probe_installer** directory. This directory should contain the probe installer **UCMDB_DataFlowProbe_10.33.exe**.

  b. Check if the probe auto upgrade agent package is placed under the right place

     Go to the **<UCMDB_Server>\runtime\probe_upgrade** directory. This directory should contain the probe upgrade package **probe-patch-windows.zip**.

     If the **probe-patch-windows.zip** package does not exist,

     i. Go to **<UCMDB_Server>\content\probe_patch**.

     ii. Copy the **probe-patch-10.33-windows.zip** package to the **<UCMDB_Server>\runtime\probe_upgrade** directory.

     iii. Restart the UCMDB server. UCMDB server will then perform probe auto upgrade.

- **Probe auto upgrade log files**

  Check the probe auto upgrade log files (in the **<DataFlowProbe>\runtime\log** directory) for more details:

  - **pg_upgrade.log**. Shows the running details of the **pg_upgrade.bat** script, including the details about PostgreSQL upgrade and table splitting.
  - **probe_upgrade_conf_merge.log**. Shows the related information when probe installer merger configuration files.

- **probe_auto_upgrade.log**. In the **probeUpgradeLogs** subfolder, shows the related information when the probe auto upgrade agent upgrades a probe.

For more details about the log files, see "Data Flow Probe Log Files" on page 1.

- **XML Enricher service port conflict issue**

  Problem: The XML Enricher service may fail to start after the probe upgrade due to port conflict. In that case, the **probe_auto_upgrade.log** is placed under the **failed** folder, for example, **<UCMDB_Server>\runtime\log\probeUpgradeLogs\10.22to10.33\failed**. You can find the following message in **probe_auto_upgrade.log**:

```
2017-07-14 11:27:11 INFO  ServiceControl:106 - Starting XML Enricher service...
2017-07-14 11:27:11 INFO  ServiceControl:328 - XML EnricherStatus status:
STOPPED
2017-07-14 11:27:11 INFO  ServiceControl:381 - Waiting for execution...
2017-07-14 11:27:46 ERROR ServiceControl:394 - Problems occurred during
execution.
```

  Solution: Check **<DataFlowProbe>\runtime\logWrapperEnricher.log**, if you find "`Port already in use: 34545`", you can change the port for XMLEnricher by editing the **<DataFlowProbe>\bin\xmlenriche\WrapperEnricher.conf** file, or free the port **34545**.

Troubleshooting Probe Auto Upgrade - PostgreSQL Upgrade

- When PostgreSQL finishes upgrade, you can check the PostgreSQL version to verify if the upgrade is successful or not.

  In a more general way, you can check the **pg_upgrade.log** in the **<DataFlowProbe>\runtime\log** folder for more details.

  If PostgreSQL upgrade is completed successfully, you can find "`The new PostgreSQL will be used`" message in the **pg_upgrade.log** file, and you can also see two folders: **<DataFlowProbe>\pgsql** and **<DataFlowProbe>\pgsql.old** . The **<DataFlowProbe>\pgsql.new** folder was removed when the upgrade is completed successfully. If you manually run the script from the **<DataFlowProbe>/tools/dbscripts** folder to upgrade the database again, the log will tell you that **pgsql.new** does not exist, and running the script again has no functional impact to the PostgreSQL installation.

- In some cases the PostgreSQL upgrade may fail. Then you can find three subfolders under **<DataFlowProbe>**: **pgsql**, **pgsql.old**, and **pgsql.new**. You can also find more details in the **pg_upgrade.log** file, which displays messages that may indicate why the upgrade failed. You may

follow the solutions for different log messages.

a. **Log message:** `Folder pgsql.new doesn't exist.`

   - **Possible Cause:** Something unexpected happened when installing the probe, and the probe failed to generate the **pgsql.new** folder.

     Solution: Download PostgreSQL resources for the same version from the official PostgreSQL website and extract the resources to the **pgsql.new** folder, then rerun the **pg_upgrade.bat** script.

   - **Possible Cause:** You have already run the script more than once, and the script already deleted the **pgsql.new** folder previously.

     Solution: The PostgreSQL upgrade is completed successfully previously. Just check for the PostgreSQL version.

b. **Log message:** `The new PostgreSQL database initialization failed.`

   Possible Cause: The conditions for **initdb** were not met.

   Solution: Check if the password is correct, or there is no **data** folder in **pgsql.new**.

c. **Log message:** `The precheck of the old and new PostgreSQL failed.`

   Possible Cause: The script did not run in the local system account or has no full control of the files.

   Solution: Switch to the local system account, or add full control to the whole folder for users, then rerun the script.

d. **Log message:** `PostgreSQL upgrade failed, the old PostgreSQL will still be used.`

   Possible Cause: The conditions for **pg_upgrade.exe** were not met.

   Solution: Check the conditions for both the old PostgreSQL and the new PostgreSQL, make sure both are fine. You can manually run the following command to find more details:

```
"%DB_PATH%\pg_upgrade.exe" -b "%BASE_DIR%\pgsql\bin" -B  "%BASE_
DIR%\pgsql.new\bin" -d "%BASE_DIR%\pgsql\data" -D "%BASE_
DIR%\pgsql.new\data" -p 5436 -P 5437 -U postgres
```

e. **Log message:** `Table splitting failed, the old PostgreSQL will still be used.`

   Possible Cause: There is no **ddm_discovery_results** table in the database, or the upgrade failed when creating the **ddm_discovery_touch_results** table.

Solution: Check the log details to find out where the problems happened, then check the script **tools\dbscripts\migrateData.cmd**.

After resolving issue a ~ issue e above, you can follow the steps below to upgrade PostgreSQL manually:

a. Stop the **UCMDB_Probe_DB** service.

b. Remove the content of the **pgsql** folder and copy the content of the **pgsql.old** folder into the **pgsql** folder.

c. Give full control to the user of the **DataFlowProbe** folder, and then from the **<DataFlowProbe>/tools/dbscripts** folder run the following command:

```
pg_upgrade.bat %DB_Password%
```

d. Once the command is successful run, revert the full control you granted to the user.

> **Note:** During the upgrade, HPE does not keep the configuration files for **<DataFlowProbe>\pgsql\data\postgresql.conf**, so make sure you reconfigure it after the upgrade (if necessary).

Troubleshooting - Probe Auto Upgrade Agent

Before upgrading a probe, the probe auto upgrade agent checks the environment and the probe status.

a. **Check probe version.** Only a probe of version 10.22 or higher could be upgrade. For supported probe versions, see Supported Versions.

b. **Check probe status.** Only union mode probe in non-FIPS mode could be upgraded.

c. **Check available disk space.** At least 10 GB disk space is required to perform the probe auto upgrade.

If a probe does not satisfy the requirements, it will be restored and back on running.

> **Important:**
>
> - A probe has only one chance for auto upgrade. If the auto upgrade process fails, and the probe was not broken during the process, it would be restored and you will need to manually upgrade it.
> - The probe auto upgrade does not support to upgrade a probe started in console mode.

- **How to check if a probe has been upgraded successfully?**

  You can check the **probe_auto_upgrade.log** file (in the **C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs** folder).

  - If the probe has been upgraded successfully, you can see the following message in the log file:

    ```
    Finished probe upgrade. Probe has been upgraded to [version] [Build]. Probe
    auto upgrade agent will exit.
    ```

  - If the probe upgrade failed, there is no upgrade related error message in the **probe_auto_upgrade.log** file.

    For further information about the upgrade failure, check the following log files:

    - **probe_upgrade_conf_merge.log**
    - **pg_upgrade.log**
    - **probe_post_upgrade.log**

    For information about the probe log files, see "Data Flow Probe Log Files" on page 1.

  - **Problem:** Sometimes due to the environment, the probe installer may be in hung state and cannot finish the upgrade. If this happens, the probe auto upgrade agent will abort the probe upgrade process and restore the probe.

    Solution: You need to manually upgrade the probe.

  - **Problem:** Log shows that "`errors occurred installing probe`", and probe service, probe DB service, or XML Enricher service could not be started. It may happen when errors occur launching the probe installer.

    Solution: You need to manually upgrade the probe.

    Most likely it is caused by the missing of some properties in the configuration file. If not, you may need to check the following log files for further information:

    - **probe_upgrade_conf_merge.log**
    - **pg_upgrade.log**
    - **probe_post_upgrade.log**

Troubleshooting - Three Way Merge Function

When the probe installer is launched, it will merge the following configuration files:

- **DataFlowProbe.properties**
- **DataFlowProbeOverride.properties** (If exists)

The result is that all the custom configuration settings will be written into the **DataFlowProbeOverride.properties** file.

> **Note:** The recommended value of the **appilog.agent.probe.sendtouchResultsToServer.maxObjects** setting in **DataFlowProbe.properties** for version 10.33 is **500**. So if your value is greater than 500, it will be modified to **500**.

The following files will be replaced with the ones from your environment:

- **<DataFlowProbe>\conf\postgresql.conf**
- **<DataFlowProbe>\conf\probeMgrList.xml**
- **<DataFlowProbe>\conf\WrapperGatewayCustom.conf**
- **<DataFlowProbe>\conf\WrapperManagerCustom.conf**
- **<DataFlowProbe>\conf\security\ssl.properties**
- **<DataFlowProbe>\conf\security\HPProbeKeyStore.jks**
- **<DataFlowProbe>\conf\security\HPProbeTrustStore.jks**
- **<DataFlowProbe>\conf\enricher.properties**
- **<DataFlowProbe>\conf\EnricherServiceSettings.ini**
- **<DataFlowProbe>\bin\WrapperEnv.conf**
- **<DataFlowProbe>\bin\wrapper-platform.conf**
- **<DataFlowProbe>\bin\WrapperManager.conf**
- **<DataFlowProbe>\bin\WrapperGateway.conf**
- **<DataFlowProbe>\bin\xmlenricher\WrapperEnricher.conf**

Problem: After finishing probe auto upgrade, the probe cannot not be started, and many properties in **DataFlowProbe.properties** are empty. This happens when probe backing up configuration files failed.

Solution: You need to manually upgrade the probe. That is to say, uninstall the probe and install version 10.33 probe manually.

Troubleshooting and Limitations – Multiple CMDB Integration

Troubleshooting

When performing troubleshooting, be sure to check both CMDB server and Probe logs.

- CMDB server logs
  - fcmdb.log
  - fcmdb.adapters.log
  - error.log
  - cmdb.reconciliation.log (for population jobs)
- Probe logs
  - wrapperProbeGw.log
  - fcmdb.log
  - fcmdb.adapters.log
  - probe-infra.log

Following are some problems that you may encounter and their solutions.

- **Problem.** TQL query not active/persistent error message.

  The Query settings have been changed manually.

  Solution. Run full population to reactivate/persist the query.
- **Problem.** The number of CIs that is populated is much larger than the requested amount.

  Solution. Since the automatic completion feature for reconciliation is turned on by default, it may populate the CMDB with additional CIs or links, in order to contain sufficient information to insert the CIs into the CMDB.
- **Problem.** Changes are not populated immediately after a job is run.

  Changes may take a few minutes to be detected by the live mechanism.

  Solution. Wait a few minutes for changes to be populated by your next population job.

- **Problem.** CIs are not populated into the CMDB.

  Changes may take a few minutes to be detected by the live mechanism.

  Solution. Wait a few minutes for changes to be populated by your next population job.

  Check the CMDB reconciliation logs for more information.

- **Problem.** Deletions are not populated.

  Solution:

  - Make sure that you have selected the **Allow Delete** check box in the population job properties.
  - Check the query you are running. Deletes are not supported on federated queries, and the aging mechanism must be used.

- **Problem**. Queries that contain compound relationships fail.

  Solution. If you want to let those TQL queries run, remove subgraph and uncheck **Show full path between source and target CIs** in the query's Compound Relationship properties, then the queries can run.

- **Problem.** Authentication fails.

  Solution. Since the UCMDB 9.x /10.x adapter uses the UCMDB API for connection, set up an integration user to ensure that you provide proper credentials. For details, see "Create an Integration User" in the *HPE Universal CMDB Developer Reference Guide*.

- **Problem.** The Data Push job fails with the message “Remote UCMDB version is not supported.”

  Solution. The Data Push flow only supports pushing to UCMDB version 9.05 CUP 9 and later CUPs, or UCMDB version 10.01 and later (it does not support pushing to UCMDB version 10.00). Upgrade your remote UCMDB or alternatively, run the integration using the population flow.

Limitations

- If the TQL query for a population job (defined on the source) includes CI types or links that do not exist on the target, or links that are not valid, those types or links are ignored in the target data repository.
- Since the UCMDB 9.x/10.x adapter works with the "changes" population engine, if a population flow retrieves federated data, no removals are made in the CMDB, since the federation brings only added or updated data.

CyberArk Integration Troubleshooting and Limitations

- **Symptom:** Received an error message "`User <ApplicationID> is not defined`" when running the **checkCyberArkConn.bat** script to test connection.

  Possible Cause: The application ID is not added to the Safe in CyberArk.

  Solution: Add the applicaition ID to the Safe in CyberArk. For detailed instructions, see Create and configure an application ID.

- **Symptom:** Checking credential failed with an error message similar to the following:

  `Failed to get credential XYZ, please check the related error logs in probe side.`

  Scenarios:

  - Found the following error messages in the **WrapperProbeGw.log**:

    - ... `Failed to get credential for id 52_1_CMS - Failed quering CyberArk Password, Application ID is empty.`
    - ...`Failed to get credential for id 2_1_CMS - Failed quering attribute from CyberArk Password.`

    Possible Cause: Application ID or Classpath is not properly set.

    Solution: Set application ID and classpath properly. For detailed instructions, see Set ApplicationID and Classpath parameters manually.

  - Found the following error message in the **WrapperProbeGw.log**: `Query string not legal. Should be "safe\folder\name"`.

    Possible Cause: The format of the Reference ID is not correct.

    Solution: Update the reference ID by strictly following the reference ID format:

    <Safe_Name>\<Folder Path>\<ReferenceID>

    Where **<Safe_Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<ReferenceID>** is the name of the CyberArk account you specified or auto-generated in CyberArk.

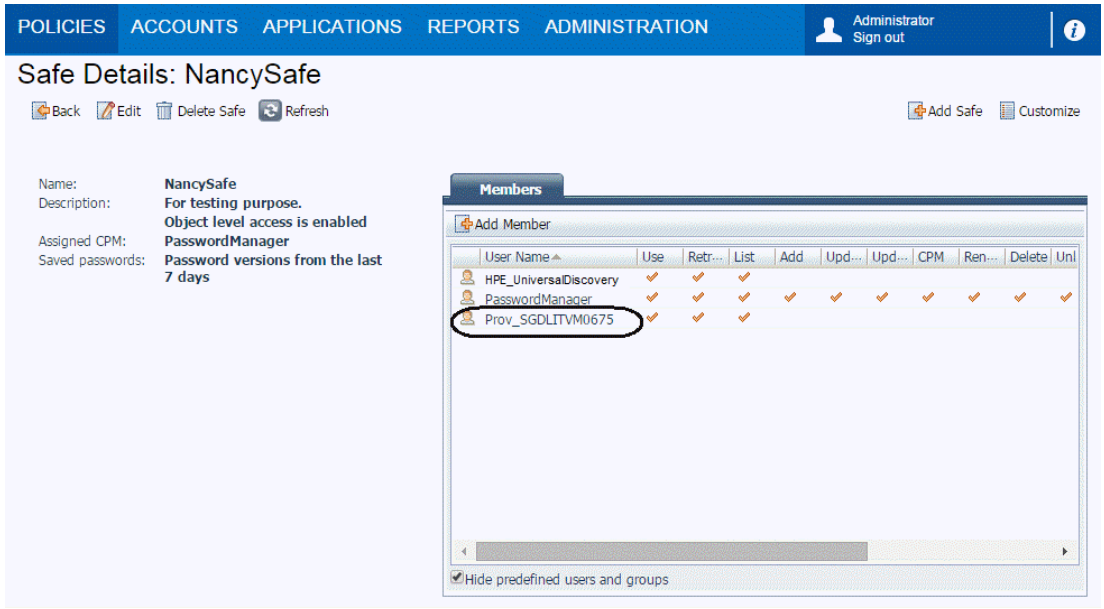
    For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

  - Found the following error message in the **WrapperProbeGw.log**:

```
Password object matching query [object=ABC;Folder=Root;Safe=XYZ] was not found
(Diagnotic Info: 9). Please check that there is a password object that answers
your query in the vault and that both the provider and the application user
have the appropriate permissions needed in order to use the password.
```

Possible Cause: The CyberArk Credential Provider user was not added as a member to the Safe.

Solution: Add the CyberArk Credential Provider user as a member to the Safe in CyberArk, as follows:



For detailed instructions, see "How to Create and Configure CyberArk Account for the Integration" on page 1.

- Found the following error message in the **WrapperProbeGw.log**: `Error: CASVL012E User Name [ApplicationID] is invalid`.

  Possible Cause: This is related to the authentication. The OS user was not properly set when creating the Application ID in CyberArk.

  Solution: If the Probe is running as a service, add **NT AUTHORITY\SYSTEM** as OS user.

  If the Probe is running as console, add the **<hostname\username>** as OS User.

- **PROBLEM:** After enabling CyberArk integration, there are no CyberArk related fields in the Protocol Parameters dialog for some protocols. Is it possible to add CyberArk credential reference to those protocols?

Solution: Yes. Apart from UDDI Registry and Universal Discovery protocols (which have no passwords at all), we can add CyberArk credential reference to these protocols with the help of JMX methods. For a list of protocols that are supported from JMX, see "Supported Protocols" on page 1. For detailed instructions, see "How to Add CyberArk Credential for Protocols from JMX" on page 1.

- **Limitation:** Probe will not be able to retrieve passwords from CyberArk if it is running on the local system account and that this account is not added as a member to the CyberArk Safe.
- **PROBLEM:** After enabling CyberArk integration and the FIPS mode, check credential for CyberArk failed on Windows platform. This is because the file path separator "\" in the conf files cannot be properly processed on Windows platform. (QCCR1H104637)

  Solution: When enabling CyberArk integration and the FIPS mode on Windows platforms, make sure you replace the file path separator "\" with "/" in the conf files.

  For example, replace the file path separator "\" in the following setting:

  ```
  wrapper.java.classpath.8=C:\Program Files
  (x86)\CyberArkApplication\PasswordSdk\JavaPasswordSDK.jar
  ```

  with "/", as shown below:

  ```
  wrapper.java.classpath.8=C:/Program Files
  (x86)/CyberArkApplication/PasswordSdk/JavaPasswordSDK.jar
  ```

- **PROBLEM:** After adding a new probe to the UCMDB server that was already switched to the FIPS mode, the automatic FIPS switch process for the new probe might fail. This is because once the newly installed probe is started, it downloads all the resources from the UCMDB server, and when the probe gets the probe upgrade package, it would schedule a restart, which blocks the automatic FIPS Switch process. (QCCR1H106595)

  Workaround: Once you find that the automatic FIPS Swtich process for a new probe failed,

  a. Copy the jar files of JCE Unlimited Strength Jurisdiction Policy Files 8 into the **%\DataFlowProbe_HOME%\bin\jre\lib\security** directory on the Data Flow Probe machine.

     For more information about how to obtain the files, see the *HPE Universal CMDB FIPS Deployment Guide*.

  b. Add the following line into the **DataFlowProbe.properties** file on the Data Flow Probe machine, and then save the file.

```
probe.fips.status=1
```

c. Restart the Data Flow Probe.

> **Note:** If the Data Flow Probe is in separate mode, you need to perform the above steps for both the Probe Manager and Probe Gateway instances.

- **PROBLEM:** When running discovery jobs or checking credentials, the following error occurs:

```
Failed to verify application authentication data: Hash XXX is unauthorized.
```

This is caused by inconsistent hash values between UCMDB and CyberArk Server.

Workaround: Check if the hash value is the same as the one you configured on the CyberArk server. If different, regenerate the hash value and then fill the new hash value in the CyberArk server. For instructions, see "How to Calculate Hash Code for JARs with Annotation" on page 1.

Universal Discovery Troubleshooting and Limitations

This section describes general troubleshooting and limitations related to working with Data Flow Management.

> **Note:**
>
> - For details on using log files to perform basic troubleshooting, see:
> - "Data Flow Probe Log Files" on page 1
> - "UCMDB Log Files" in the *HPE Universal CMDB Administration Guide*

Troubleshooting – Universal Discovery

Discovery Results Do Not Appear in the Topology Map

Problem. Data that should have been discovered during the discovery process does not appear in the topology map.

Verification. The CMDB cannot retrieve the data or build the query results. Check the Discovery Results pane. If the CIs were not created, the problem is occurring during the Discovery process.

Solution. Check the error messages in the **probeMgr-services.log** file located in **C:\hp\UCMDB\DataFlowProbe\runtime\logs**.

Triggers Running Unexpectedly in Management Zone

Problem: There are triggers running in the Management Zone that should not be running.

Reason: Running triggers continue to run in the case where a Probe cluster is bound to the Management Zone, and the Probes in the cluster are removed from the cluster while the triggers are running.

Solution: To stop the triggers running, deactivate and then reactive the Management Zone.

Job Running Triggers Not Within Probe Limit

Problem: A discovery job is running triggers that are not within its Probe limit.

Indication: Triggers are not released from a job in the following cases:

Scenario 1

1. ProbeA and ProbeB belong to Cluster1.
2. **Range IPs by ICMP** is limited to run only on Cluster1. The job runs on both Probes in Cluster1.
3. ProbeB is removed from Cluster1.
4. In the next scheduled run of **Range IPs by ICMP**, you notice that the trigger is still running on both Probes in the cluster, even though ProbeB no longer belongs to Cluster1.

Scenario 2

1. ProbeA is in Cluster1; ProbeB is under the Default Domain
2. **Range IPs by ICMP** is limited to run only on ProbeB.
3. ProbeB is added to Cluster1.
4. In the next scheduled run of **Range IPs by ICMP**, you notice that the trigger is still running on ProbeB, even though ProbeB now belongs to Cluster1.

Solution. Deactivate and then reactive the job.

Networks and IPs

Problem. Not all networks or IPs have been discovered.

Indication. Not all the networks or IPs appear in the topology map results.

Verification. The IP address range in the Data Flow Probe Setup window does not encompass the scope of the networks or IPs that should have been discovered.

Solution. Change the scope of the Discovery range:

1. Select **Data Flow Management > Data Flow Probe Setup**.
2. Select the Probe and the range.
3. Change the IP address range in the Ranges box as required.

TCP Ports

Problem. Not all TCP ports have been discovered.

Indication. Not all TCP ports appear in the topology map results.

Verification. Open the **portNumberToPortName.xml** file (**Data Flow Management > Adapter Management > DDM Infra > Configuration Files > portNumberToPortName.xml**), and search for the missing TCP ports.

Solution. Add the port numbers that should be discovered to the **portNumberToPortName.xml** file.

Discover Resources on a Windows XP Machine

Problem. Failure to discover resources on a machine running on the Windows platform.

- **Solution 1**. **Start > Settings > Control Panel > System**. In the Remote tab, verify that the following check box is selected: **Allow users to connect remotely to this computer**.
- **Solution 2**. In Windows Explorer, select **Tools > Folder Options**. In the View tab, clear the **Use simple file sharing (Recommended)** check box.

Trigger CIs for jobs in a management zone are in continuous "Progress" status

Problem. If you notice that trigger CIs for jobs in a management zone are in continuous "Progress" status, configure Data Flow Probe to ignore certain call home requests from the Universal Discovery Agent.

- **Solution**. To resolve this issue, change a parameter value as follows:
  - GlobalSettings.xml file
  - allowCallhomeInterval parameter
  - Default is 24.
  - Measured in hours that call home requests are ignored.
  - Allowable values are any integer greater than 0.

Device attributes are not populating or contain unexpected or null values

Problem. If you notice that certain devices contain unexpected values or contain no values.

- **Solution**. To resolve this issue, run the Rulebase Support Report and send to HPE Support for analysis. For more information, see *HPE Universal CMDB Modeling Guide*.

Inventory Discovery by Scanner job fails

Problem. If you notice that the Inventory Discovery by Scanner job fails.

Indication. The Communication log contains the following entry: "Step Wait XML Enricher Process execution failed.".

Solution. If BDNA Normalize integration is enabled, troubleshoot BDNA Normalize operation using its documentation or contact BDNA support.

Data push troubleshooting

- **How to get a view of the integrations**

  To get a view of the integrations, run the following command :

  ```
  SELECT ds.datastore as integration_point_name ,COUNT(*) as nbr_of_records
  ,ds.ds_id FROM SYNC_ID_MAP as ID, SYNC_DATASTORE as DS where id.ds_id =
  ds.ds_id group by ds.datastore,ds.ds_id
  ```

- **Clear a given datastore by invoking the removeIdMappingsOfDataStore JMX method**

  To clear a given datastore, you can invoke the **UCMDB:service=FCMDB Synchronizer Services > removeIdMappingsOfDataStore** JMX method.

  > **Caution:** Make sure you do it only when necessary.

  For SM adapters, invoking the **removeIdMappingsOfDataStore** JMX method will resend all CIs, and then create duplicates.

  However, in general it is useful for AM adapter and Generic Adapter, when there is assumption that the data push is corrupted.

Limitations – Universal Discovery

- When Discovery is installed on a non-English operating system, names of modules, Management Zones, and jobs are limited to English characters (a-z; A-Z).
- When naming entities in Data Flow Management , you can use the following characters:
  - **Modules:** `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), space ( ), and forward slash (/).
  - **Management Zones:** `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), and space ( ).
  - **Jobs:** `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), and space ( ).
  - Names can be a maximum length of 50 chars and MUST NOT start with a digit.

- When entering IP addresses, use only digits and asterisks (*)
- Each Content Pack installation overrides all out-of-the-box resources with the contents of that Content Pack. This means that any changes you made to these resources are lost. This applies to the following resources: Queries, Views, Enrichments, Reports, Discovery Jython scripts, Discovery adapters, Discovery jobs, Discovery resources, Discovery configuration files, Discovery modules, CI Types, and Relationships. (Attributes added to CI Types and Relationships are not overridden).

Inventory Discovery Troubleshooting

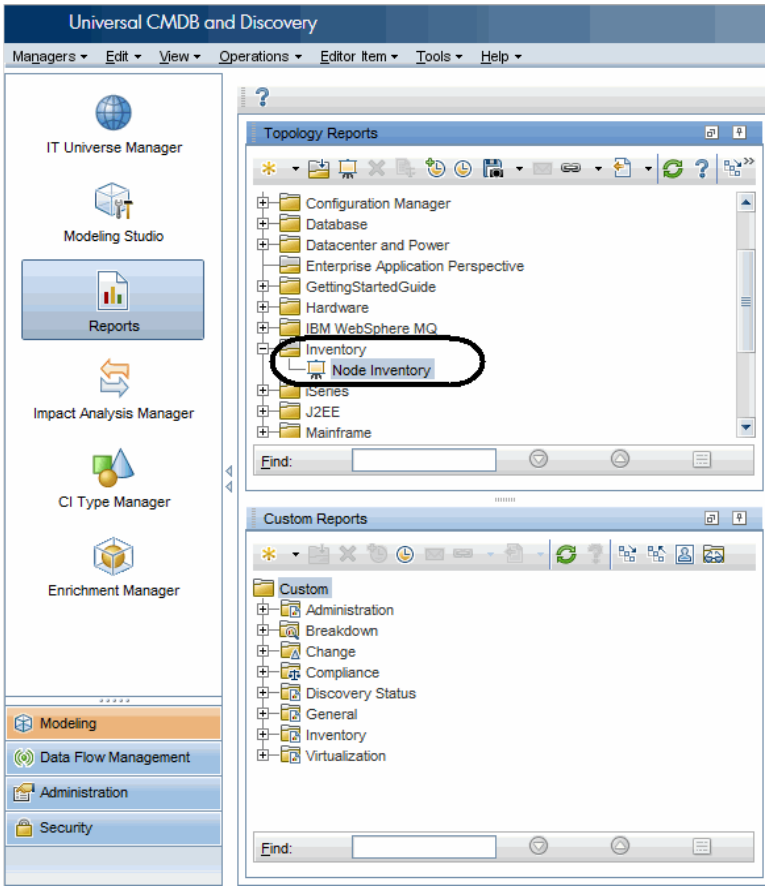
This chapter includes:

How to view all information related to a device in a centralized view?

Question: How can I view all relevant information to a device in a centralized view?

To view all information related to a device in a centralized view,

1. Select **Modeling > Reports**.
2. In the Topology Reports pane, expand **Inventory > Node Inventory**.



3. Double-click **Node Inventory** or right-click it and select **Open Report**.

   The Node Inventory report opens in the right pane.

4. Do either of the following to view device details:

   - Select a specific CI in the right pane and drill down to view more details. Or,
   - Export the report to PDF, so that you can view all details in grid view. To do so,

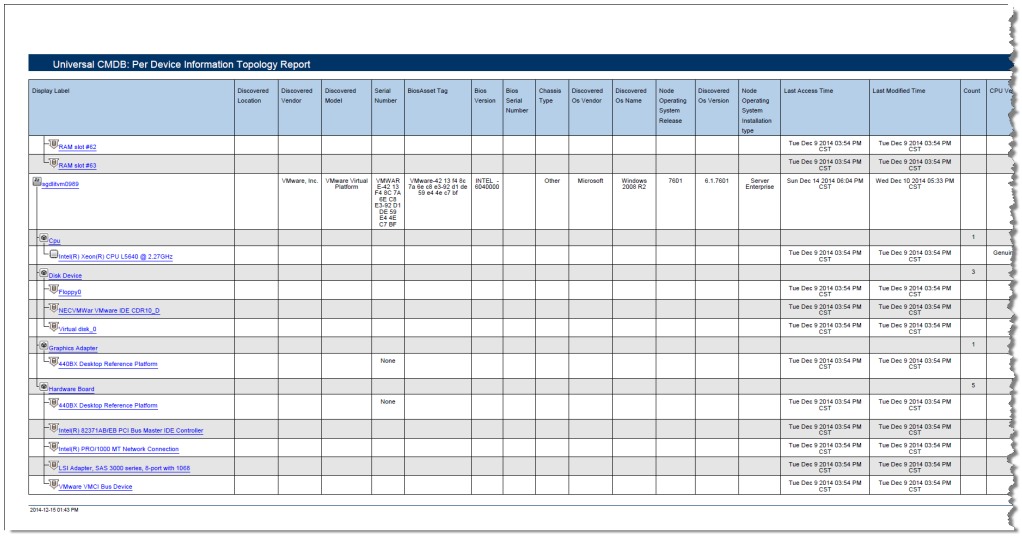
     i. Right-click **Node Inventory**, select **Export Report > Export to PDF** from the context menu.

     ii. In the Export dialog box, specify file location and file name for the target PDF file.

     iii. Click **Export**.

     iv. Click **Yes** when prompted whether you want to open the PDF file now.

The exported PDF file opens, displaying all details in grid view.



Universal CMDB: Per Device Information Topology Report

Display Label	Discovered Location	Discovered Vendor	Discovered Model	Serial Number	BiosAsset Tag	Bios Version	Bios Serial Number	Chassis Type	Discovered Os Vendor	Discovered Os Name	Node Operating System Release	Discovered Os Version	Node Operating System Installation type	Last Access Time	Last Modified Time	Count	CPU Ve
RAM slot #62														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
RAM slot #63														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
sgdlvm0989		VMware, Inc.	VMware Virtual Platform	VMWARE-42 13 f4 7a 6b 7f 4E C3 E3-92 01 DE 59 E4 4E C7 BF	VMware-42 13 f4 8c 7a 6e c8 e3-92 d1 de 59 e4 4e c7 bf	INTEL - 6040000		Other	Microsoft	Windows 2008 R2	7601	6.1.7601	Server Enterprise	Sun Dec 14 2014 06:04 PM CST	Wed Dec 10 2014 05:33 PM CST		
CPU																1	
Intel(R) Xeon(R) CPU L5640 @ 2.27GHz														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		Genuin
Disk Device																3	
Floppy0														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
HECVMWar VMware IDE CDR10_D														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Virtual disk_0														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Graphics Adapter																1	
440BX Desktop Reference Platform				None										Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Hardware Board																5	
440BX Desktop Reference Platform				None										Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Intel(R) 82371AB/EB PCI Bus Master IDE Controller														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
Intel(R) PRO/1000 MT Network Connection														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
LSI Adapter, SAS 3000 series, 8-port with 1068														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
VMware VMCI Bus Device														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		

2014-12-15 01:43 PM

For more information about the topology report, see the *HPE Universal CMDB Modeling Guide*.

How to troubleshoot network availability and latency issue related to a device?

Question: How should I troubleshoot network availability and latency issue related to a device?

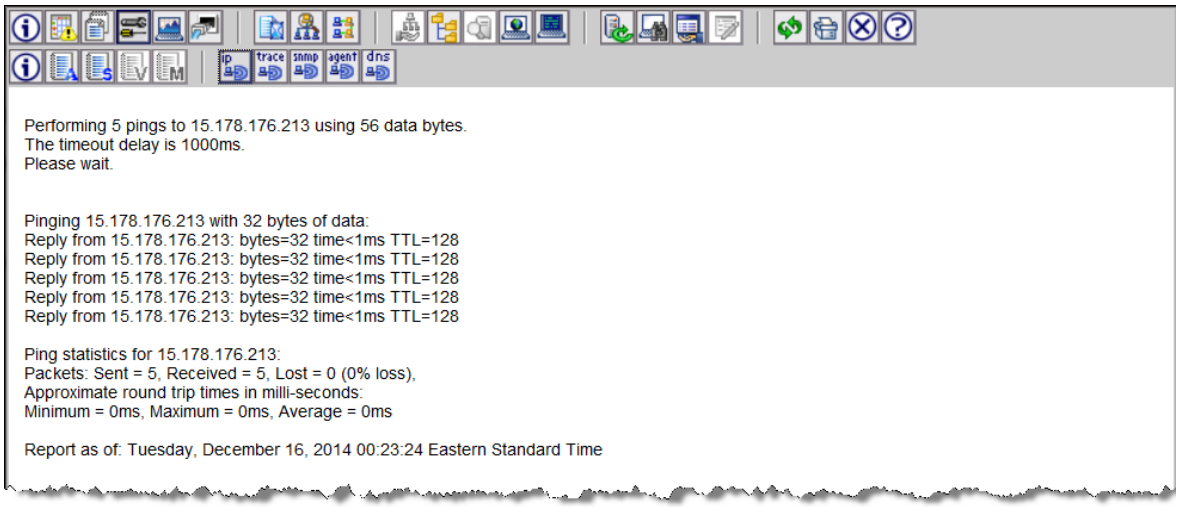
You can troubleshoot network availability and latency issue related to a device in the following ways:

- IP Ping and Agent Ping
- SNMP Ping
- Tracert and DNS Query

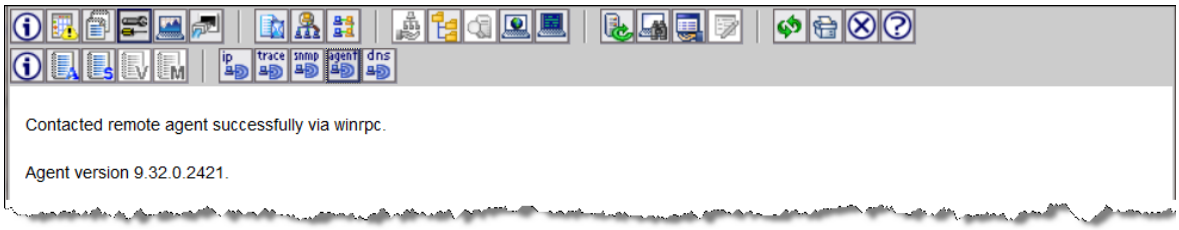
IP Ping and Agent Ping

In DDMi, you can use IP ping and agent ping.

Result of the IP ping looks similar to the following:



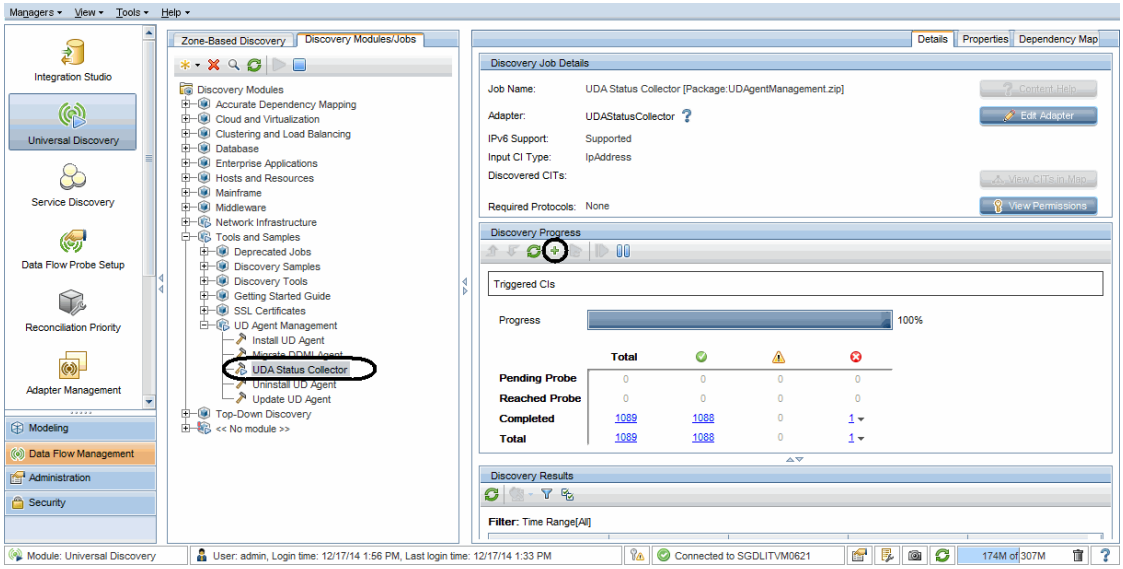
Result of the agent ping looks similar to the following:



In UD, you can use also use IP ping and agent ping via the UDA Status Collector job.

To use IP ping and agent ping

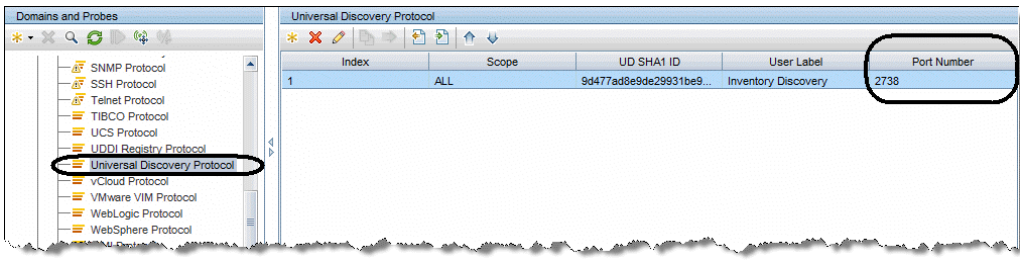
1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > UDA Status Collector**.
3. If the UDA Status Collector job is not activated, right-click **UDA Status Collector**, and select **Activate**.



4. In the Discovery Progress pane, click the **Add CI** button.

5. In the Choose CIs to Add dialog box, select the IP address of your interest, and click the **Add** button.

   The UDA Status Collector job will ping using IP and agent port to check.

> **Note:** Agent port can be found in the **Port Number** parameter value of the Universal Discovery Protocol credential. This is a default parameter in the protocol, and is applied to all agent connections using this protocol.
>
> To view the agent port,
>
> a. In the Data Flow Management module, go to **Data Flow Probe Setup**.
>
> b. In the Domains and Probes tree, select a domain of your interest and expand the **Credentials** node, and then select **Universal Discovery Protocol**.
>
> c. In the Universal Discovery Protocol credentials displayed in the right pane, check the value for the **Port Number** column.
>
> 
>

6. Click the **Close** button to exit the Choose CIs to Add dialog box.

To view the IP ping and agent ping result

1. Access the JMX console on the Data Flow Probe machine by launching the Web browser and enter the following address:

   https://localhost:8453/

   You may have to log in with the user name **sysadmin** and password.

2. Locate the **exportUdaStatus** operation to invoke.

   On the MBean View page, select **type=JobsInformation**. Locate the **exportUdaStatus** operation.

3. Provide a folder name in the **Value** field.

4. Click **Invoke** to run the operation.

The UDA status is exported to a CVS file.

5. Open the exported CSV file to view details of the result from the UDA Status Collector job.

   The CSV file shows status details similar to the following:

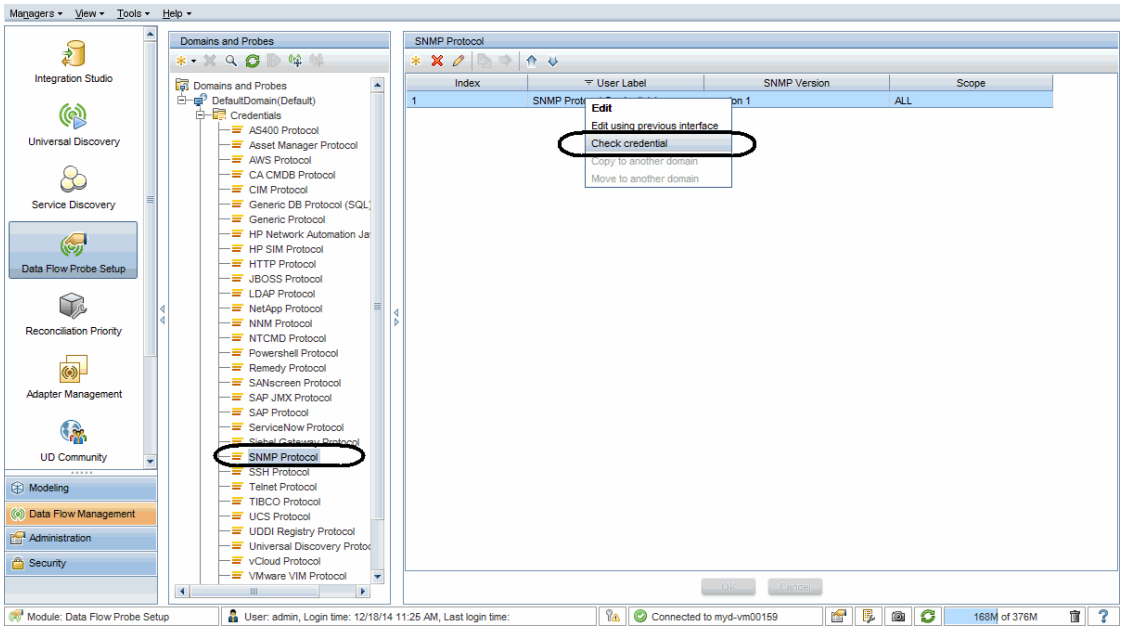
ipaddress	computerName	alive	portAlive	isDDMI	isWin	osType	agentVersion	UDUniqueId	isNative
16.60.169.33	myd-vm11101.hpswlabs.adapps.hp.com	TRUE	TRUE	FALSE	FALSE	Linux	v10.20.000 build:346	73a911c4-b0fa-4e10-2047-b270e5a0cb18	TRUE

SNMP Ping

To run SNMP ping in UDI,

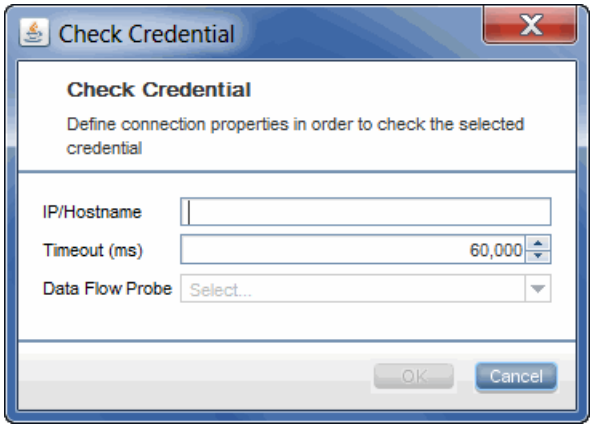
1. In the Data Flow Management module, go to **Data Flow Probe Setup**.
2. In the Domains and Probes tree, expand the **Credentials** node, and select **SNMP Protocol**.

   All SNMP credentials are displayed in the right pane.
3. Right-click the SNMP credential you want to use to run SNMP ping, and select **Check credential** from the pop-up menu.



4. In the Check Credential dialog box, specify the host name or IP address (in IPv4/IPv6 format) of the remote machine on which you want the protocol to run SNMP ping, specify a connection

timeout (in milliseconds), and select the probe to use.



5. Click **OK**.

   The result returns soon.

Tracert and DNS Query

Currently UD does not have such functionalities as DDMi did.

How to check the key indexes of the discovery history information for a discovered device?

Question: For a discovered device, how should I check the key indexes of the discovery history information? For example, when was the device first discovered? When was it last seen?

To answer this question, let's take a look at the information available from DDMi first:

DDMi Parameter	Value
First discovered:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:20:45 Eastern Standard Time
Added to map:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:48:51 Eastern Standard Time

DDMi Parameter	Value
Last seen:	2 minutes 1 second ago at: Monday, December 15, 2014 21:06:55 Eastern Standard Time in ping or poll by DDM Inventory
Last moved:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:50:47 Eastern Standard Time
Agent last contacted:	1 day 17 hours 7 minutes ago at: Sunday, December 14, 2014 04:01:01 Eastern Standard Time
Agent upgrade time:	2 weeks 6 days 1 hour ago at: Tuesday, November 25, 2014 19:56:04 Eastern Standard Time
Scanner model last updated:	2 weeks 6 days 0 hours ago at: Tuesday, November 25, 2014 20:12:35 Eastern Standard Time
Device last modeled as an unmanaged device:	3 hours 12 minutes 6 seconds ago at: Monday, December 15, 2014 17:56:50 Eastern Standard Time
Device last replied to ICMP during modeling:	2 weeks 3 days 21 hours ago at: Thursday, November 27, 2014 23:12:44 Eastern Standard Time
Mean break diagnosis time:	2 minutes (major alarm)
Agent platform:	Windows (x86)
Agent port number:	2738
Agent version:	10.20.000.346
AUM agent upgrade state:	No AUM agent
Workflow type:	Agent
Scanner version:	9.32.000.2421
Scanner configuration:	<default_delta>
Scan file location:	https://15.155.155.155/nm/scans/QASERVER1_005056B81459.xsf
Scan type:	HP Discovery and Dependency Mapping Inventory
Scan CRC:	295532891
Scan modification time:	2014-11-25 22:47:26
Mean device modeler update run time:	4 minutes 52 seconds
Recent device modeler update run times:	4 minutes 48 seconds, 4 minutes 17 seconds, 6 minutes 32 seconds, 3 minutes 53 seconds
Rulebase id:	266305

In Universal Discovery, you can find similar attributes for most of DDMi parameters as shown in the table below:

DDMi Parameter	Corresponding Attributes in UD
First discovered:	**Create Time** attribute (of the **node** CI)
Added to map:	N/A
Last seen:	**Last Access Time** attribute (of the **node** CI)
Last moved:	N/A
Agent last contacted:	**Last Access Time** attribute (of the **UDA** CI Type)
Agent upgrade time:	**LastModifiedTime** attribute (of the **UDA** CI Type)
Scanner model last updated:	**LastModifiedTime** attribute (of the **InventoryScanner** CI Type)
Device last modeled as an unmanaged device:	N/A
Device last replied to ICMP during modeling:	N/A
Mean break diagnosis time:	N/A
Agent platform:	**Platform** attribute (of the **UDA** CI Type)
Agent port number:	**Application Listening Port Number** attribute (of the **UDA** CI Type)
Agent version:	**Version** attribute (of the **UDA** CI Type)
AUM agent upgrade state:	N/A
Workflow type:	N/A
Scanner version:	**Version** attribute (of the **InventoryScanner** CI Type)
Scanner configuration:	**ScannerConfiguration** attribute (of the **InventoryScanner** CI Type)
Scan file location:	**ProcessedScanFilePath** attribute (of the **InventoryScanner** CI Type)
Scan type:	**Scan Type** attribute (of the **InventoryScanner** CI Type)
Scan CRC:	N/A
Scan modification time:	**Last Access Time** or **Scan File Last Downloaded Time** attribute (of the **InventoryScanner** CI Type)

DDMi Parameter	Corresponding Attributes in UD
Mean device modeler update run time:	N/A
Recent device modeler update run times:	**Scan Duration** attribute (of the **InventoryScanner** CI Type)
Rulebase id:	N/A

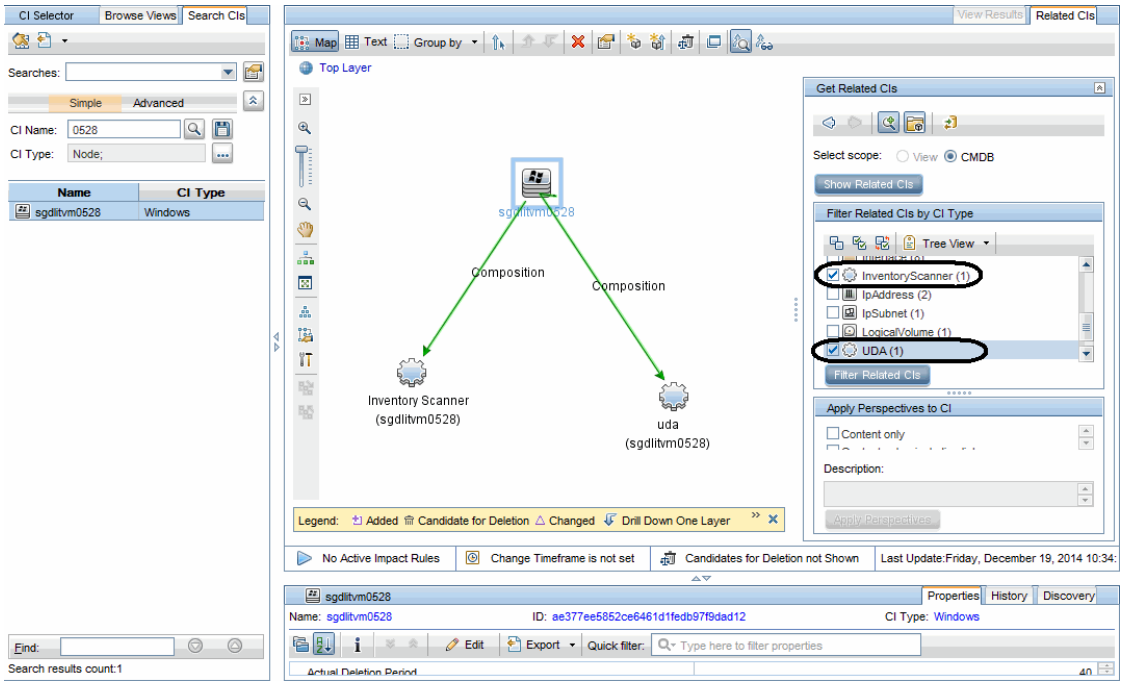
> **Note:** "N/A" indicates that there is no corresponding attribute in UD now.

To check similar information in UD,

1. In UCMDB, go to **Modeling > IT Universal Manager**.
2. In the CI Selector pane, go to the **Search CIs** tab.
3. In the Simple search mode, search for a CI of Node CI type.
   a. In the **CI Name** field, enter a keyword to search, for example, **0528**.
   b. For the **CI Type** field, click , locate and select the **Node** CI type.
   c. Click .
4. Click the node CI in the search result list.

   The node CI map displays in the Related CIs pane.
5. In the Filter Related CIs by CI Type sub-pane, locate and select **Inventory Scanner**and **UDA** CI types, then click **Filter Related CIs**.

   The Related CIs map refreshes.



6. Click the **uda** or **Inventory Scanner** CI icon in the map.

   In the CI Details pane below the map, check attributes that correspond to DDMi parameters.

   The highlighted **uda** attributes in the screenshot below correspond to similar DDMi parameters.

uda (sgdlitvm0528) | Properties | History | Discovery

Name: uda (sgdlitvm0528) ID: b4d11b46f879822f59d86b66dfc3a98c CI Type: UDA

Edit | Export | Quick filter: Type here to filter properties

Actual Deletion Period	40
Allow CI Update	True
Application Category	
Application Installed Path	
Application IP	16.187.190.28
Application IP Routing Domain	DefaultDomain
Application IP Type	IPv4
Application Listening Port Number	2738
Application Timeout	
Application Username	
Application Version Description	
Architecture	amd64
classification	
Container name	(sgdlitvm0528)
Create Time	Thu Dec 18 2014 03:08 PM GMT+08:00
Created By	UCMDBDiscovery: Host Connection by Shell
Deletion Candidate Period	20
Description	
DiscoveredProductName	uda
Display Label	uda (sgdlitvm0528)
Edition	
Enable Aging	True
Global Id	b4d11b46f879822f59d86b66dfc3a98c
Is Candidate For Deletion	False
Last Access Time	Thu Dec 18 2014 11:57 PM GMT+08:00
LastModifiedTime	Thu Dec 18 2014 11:57 PM GMT+08:00
layer	software
Name	
Note	
Origin	
Platform	windows
ProductName	
Reference to the OS credentials dictionary entry	NA
StartupTime	
Updated By	Enrichment: Enrichment's rule: SoftwareElementDisplayLabel...
User Label	
Vendor	
Version	v10.20.000 build:364

The highlighted **Inventory Scanner** CI attributes in the screenshot below correspond to similar DDMi parameters.

Inventory Scanner (sgdlitvm0528) | Properties | History | Discovery

Name: Inventory Scanner (sgdlitvm0528) ID: 00601fdc3845ee3a50e5b148618e8be3 CI Type: InventoryScanner

Edit | Export | Quick filter: Type here to filter properties

Actual Deletion Period	40
Allow CI Update	True
Application Category	
Application Installed Path	
Application IP	
Application IP Routing Domain	
Application IP Type	IPv4
Application Listening Port Number	
Application Timeout	
Application Username	
Application Version Description	
classification	
Container name	(sgdlitvm0528)
Create Time	Thu Dec 18 2014 03:51 PM GMT+08:00
Created By	UCMDBDiscovery: Inventory Discovery by Scanner
Deletion Candidate Period	20
Description	Hardware-only Inventory Scanner
DiscoveredProductName	Inventory Scanner
Display Label	Inventory Scanner (sgdlitvm0528)
Edition	
Enable Aging	True
FilesProcessed	0
FilesRecognized	0
FilesTotal	0
Global Id	00601fdc3845ee3a50e5b148618e8be3
Is Candidate For Deletion	False
Last Access Time	Thu Dec 18 2014 11:57 PM GMT+08:00
LastModifiedTime	Thu Dec 18 2014 11:57 PM GMT+08:00
layer	software
Name	
Note	
Origin	
ProcessedScanFilePath	C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher\Scans\pr...
ProcessedScanFileProbe	DataFlowProbe
ProductName	
root_iconproperties	
Scan File Last Downloaded Time	Thu Dec 18 2014 03:49 PM GMT+08:00
ScanDuration	1
ScannerCommandLine	-cfg:scan.cxz -l:local.xsf -appliance
ScannerConfiguration	_hwonly.cxz
* ScannerType	WINDOWS_X64
StartupTime	Thu Dec 18 2014 10:13 AM GMT+08:00
Updated By	Enrichment: Enrichment's rule: SoftwareElementDisplayLabel...
Upgrade Date	Thu Dec 18 2014 03:43 PM GMT+08:00
User Label	
Vendor	
Version	10.20.000 build 364

How to check device related logs for a discovered device?

Question: For a discovered device, where should I check the device related logs? Such as agent deployment log, scanner deployment log, virtualization log, and so on.

The following sections provide details about checking device related log in Universal Discovery.

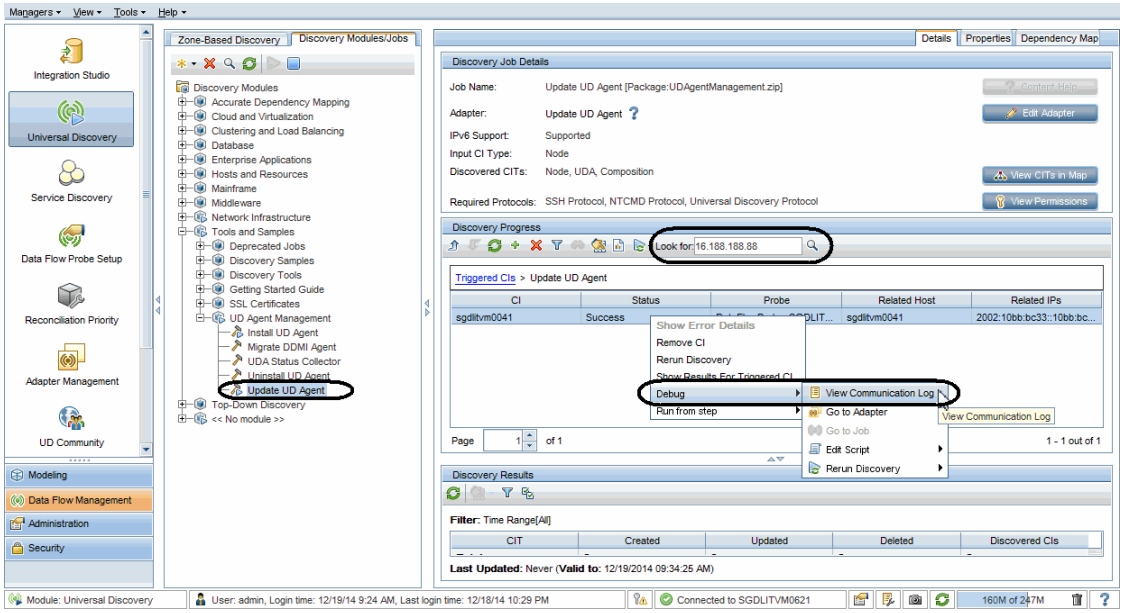
- Agent deployment log
- Scanner deployment log
- Virtualization log

Agent deployment log

The agent related action record (the Install UD Agent job and the Update UD Agent job) can be found in the Communication Log.

To view communication log for agent related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Install UD Agent** (or **Update UD Agent**).
3. Right-click **Install UD Agent** (or **Update UD Agent**), select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target agent and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.



7. In the communication log that opens,
   - search **Step [Install Agent]** as keyword to locate the log entry where probe starts the agent installation
   - search **Step [Check Agent Installed]** as keyword to locate the log entry that indicates whether the agent is installed

Scanner deployment log

The Inventory Discovery by Scanner job related action record (the Install UD Agent job and the Update UD Agent job) can be found in the Communication Log.

To view communication log for scanner deployment related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**).
3. Right-click **Inventory Discovery by Scanner**), select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.

4. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
5. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.
7. In the communication log that opens,
   - search **Step [Run Scanner]** as keyword to locate the log entry where the probe starts running the scanner
   - search **Step [Download Scan File]** as keyword to locate the log entry that indicates the probe starts downloading the scan file

Virtualization log

This log is not frequently used in DDMI. However, in UD, the Communication Log for the following jobs can provide you detailed logs about virtualization environments:

- VMware ESX Connection by VIM job
- VMware vCenter Connection by VIM job

How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors?

Question: For a discovered device, to identify any potential discovery errors, how should I invoke discovery job relevant to the device manually, and check the progress/on-going status of the discovery?

In DDMi, if you find any error in the discovery result, you can run the DDMi jobs in an ad-hoc way. In UD, similar jobs are available to provide similar functionalities.

The table below describes DDMi jobs and the corresponding UD jobs that can be run in an ad-hoc way:

DDMi Job	UD Job
Deploy Agent	Install UD Agent
Upgrade Agent	Update UD Agent
Run Scanner	Run Scanner
Retrieve Scan File	Download Scan File
Uninstall Agent	Uninstall UD Agent
Run Agentless Scanner	Run Agentless Scanner
Enrich XML	Parse Enriched Scan File
Run Rulebase	The normalization functionality is included the Rerun Discovery option for each job
Run VMware Discovery	VMware discovery jobs

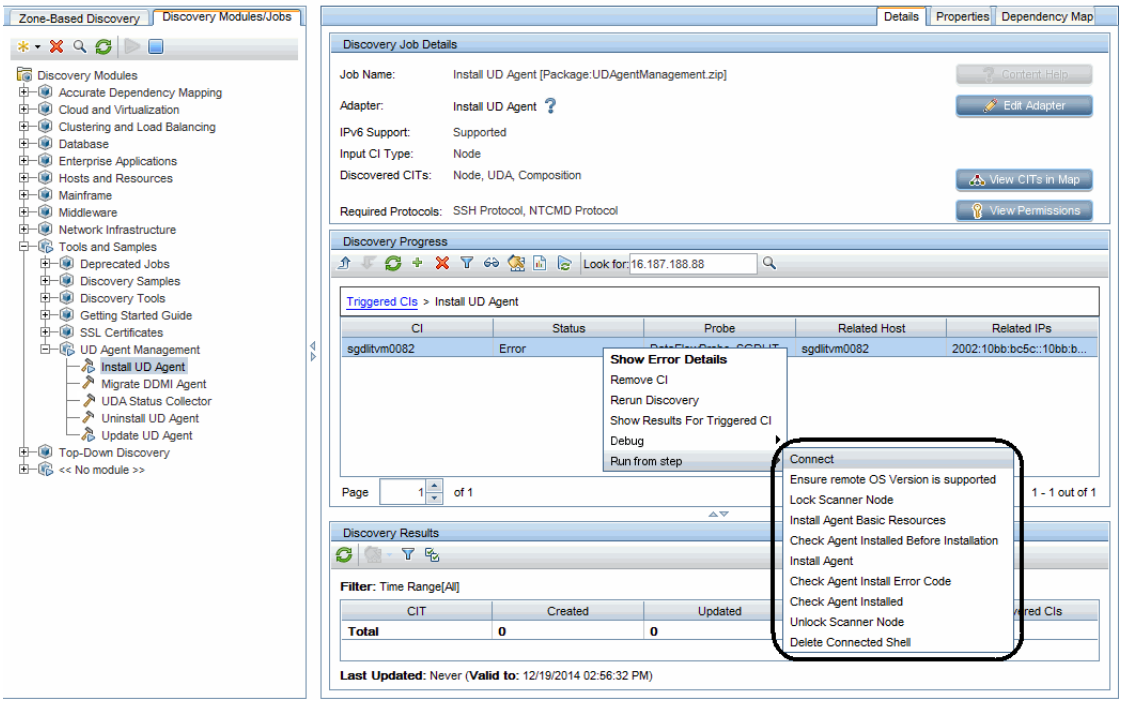
For details, click the UD job of your interest in the table above.

Install UD Agent

To invoke discovery job relevant to the device manually,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Install UD Agent**.
3. Right-click **Install UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an**

action>.



To check the progress/on-going status of the discovery job,

1. Modify the adapter's configuration to make sure that the communication log is always created.

   In this case, modify the Install UD Agent adapter's configuration.

   a. In the Data Flow Management module, go to **Adapter Management**.

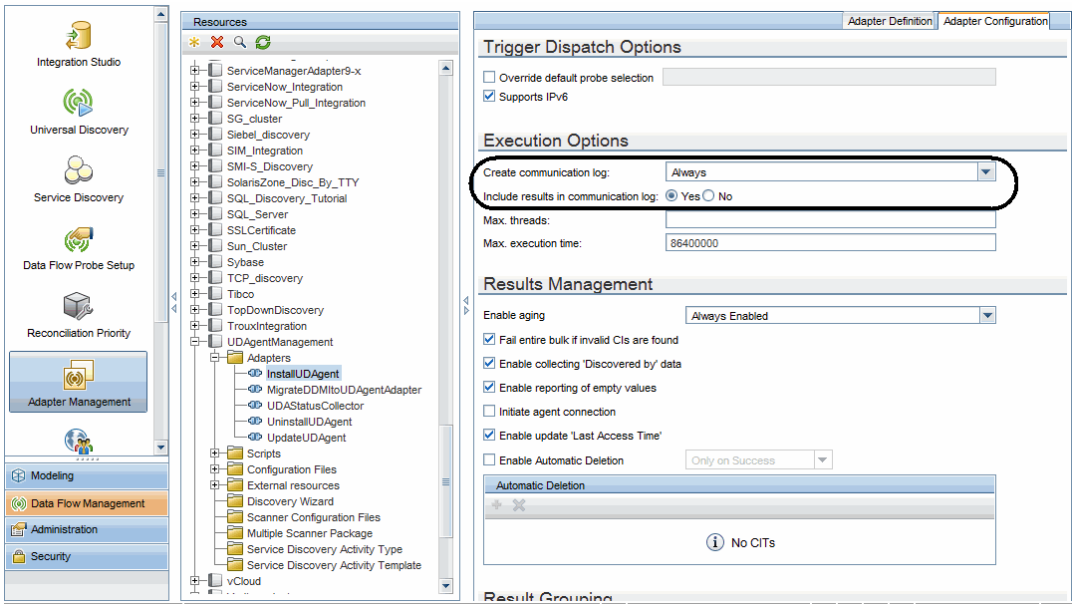
   b. In the Resources pane, expand **UDAgentManagment > Adapters > InstallUDAgent**.

   c. In the right pane, click the **Adapter Configuration** tab.

   d. In the Execution Options section, set the following:

      - **Create communication log**: **Always**

- **Include results in communication log**: **Yes**



2. Return to the Universal Discovery window, right-click the returned entry, from the context menu, select **Debug > View Communication Log**

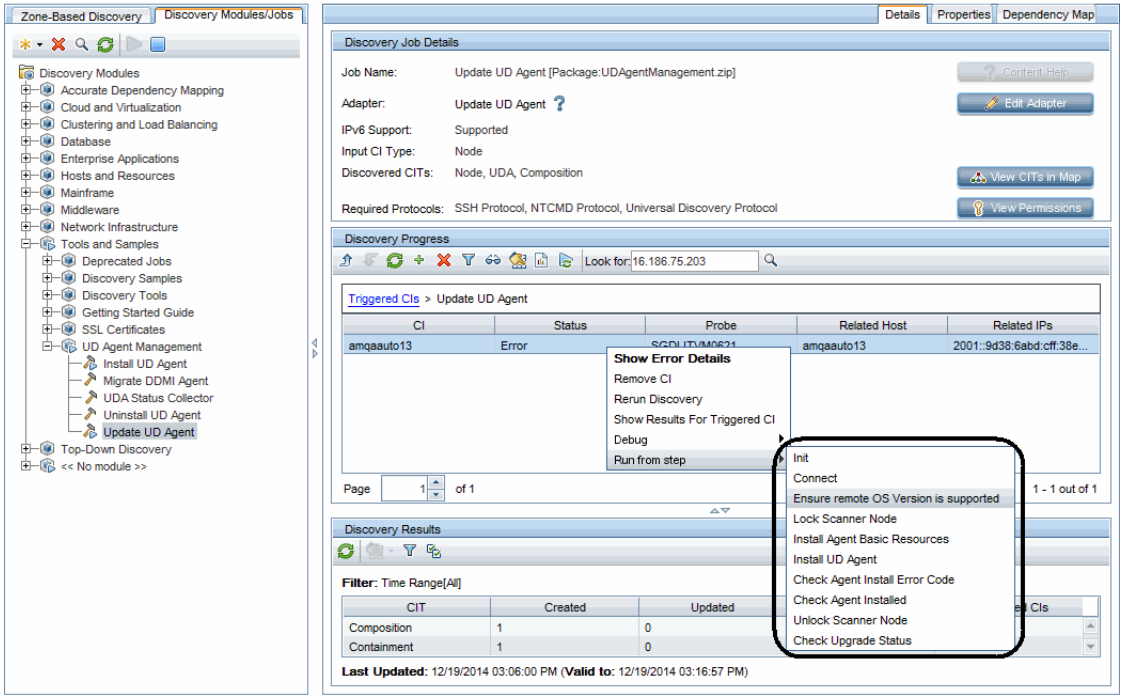
   For details, see "How to check device related logs for a discovered device?" on page 123.

Update UD Agent

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Update UD Agent**.

3. Right-click **Update UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



7. To check the progress/on-going status of the discovery job,
   a. Modify the Update UD Agent adapter's configuration to make sure that the communication log is always created.

      For detailed instructions, see "To check the progress/on-going status of the discovery job," on page 127.

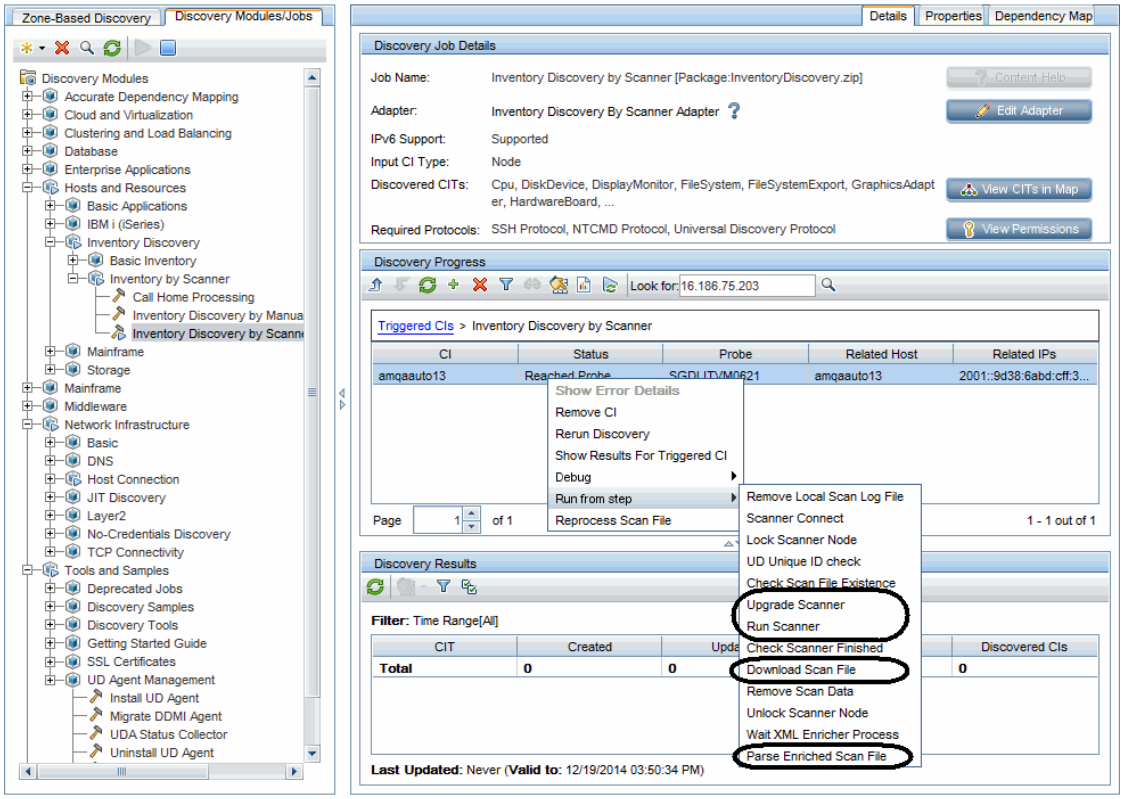
   b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

      For details, see "How to check device related logs for a discovered device?" on page 123.

Upgrade Scanner / Run Scanner / Download Scan File / Parse Enriched Scan File / Run Agentless Scanner

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
3. Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
5. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



Note: To **Run Agentless Scanner**, before selecting a **Run from step** option, set Universal Discovery Protocol scope to **Probes: Disabled**.

To do so,

a. In the Data Flow Management module, go to **Data Flow Probe Setup**.

b. Expand **Domains and Probes > DefaultDomain(Default) > Credentials > Universal Discovery Protocol**.

c. In the right Universal Discovery Protocol pane, right-click a protocol and select **Edit**.

d. In the Universal Discovery Protocol Parameters dialog box, click the **Edit** Edit... button for the Network Scope field.

e. In the Scope Definition dialog box, click the **Edit** Edit button for the Selected Probes section.

f. In the Selected Probes dialog box, clear the check box for **All Data Flow Probes** and click **OK** three times to exit.

g. Repeat step c through step f for other protocols.

h. Click **OK** to save the changes.

7. To check the progress/on-going status of the discovery job,

   a. Modify the Inventory Discovery by Scanner adapter's configuration to make sure that the communication log is always created.

      For detailed instructions, see "To check the progress/on-going status of the discovery job," on page 127.

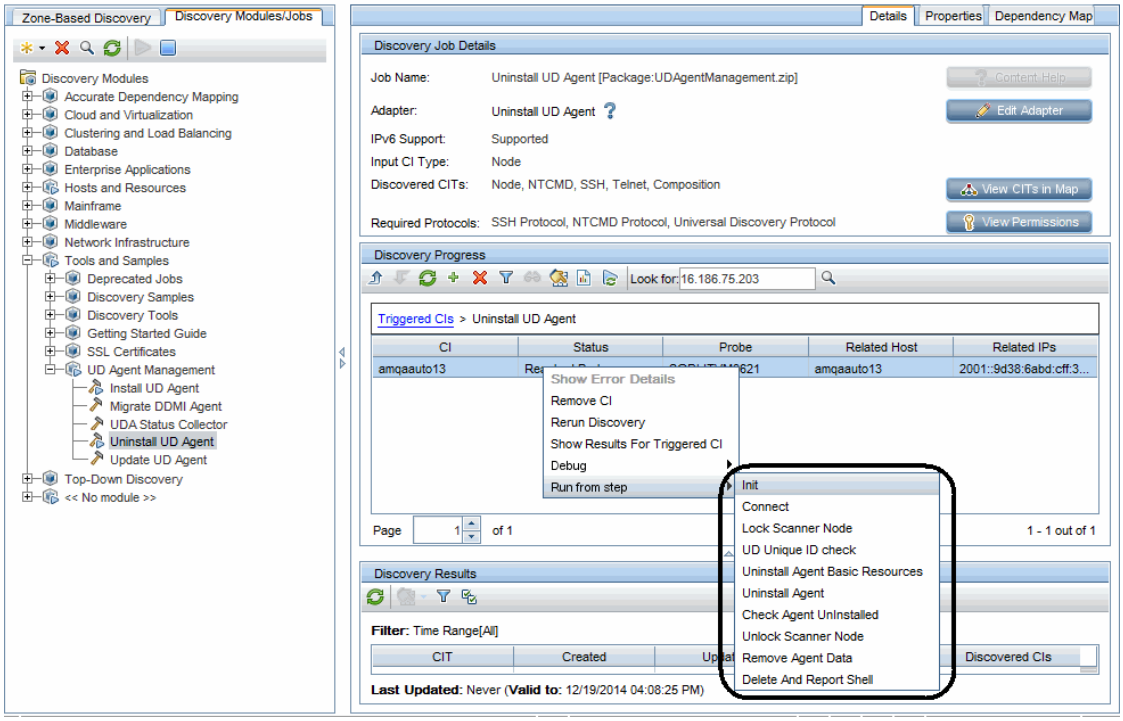
   b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

      For details, see "How to check device related logs for a discovered device?" on page 123.

Uninstall Agent

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Uninstall UD Agent**.
3. Right-click **Uninstall UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



7. To check the progress/on-going status of the discovery job,

   a. Modify the Uninstall UD Agent adapter's configuration to make sure that the communication log is always created.

      For detailed instructions, see "To check the progress/on-going status of the discovery job," on page 127.

   b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

      For details, see "How to check device related logs for a discovered device?" on page 123.

Rerun Discovery

The Run Rulebase feature is implemented in UD normalization, which covers all jobs.

To invoke the normalization manually, in the Discovery Progress pane, right-click the CI entry returned from your search and select **Rerun Discovery** from the context menu, which will perform the normalization.

> **Note:** Normalization cannot be invoked alone in UD. By selecting **Rerun Discovery**, you can invoke the normalization, but would also trigger other operations included in the discovery job in addition to the normalization.

To check the progress/on-going status of the discovery job,

1. Modify the concerning adapter's configuration to make sure that the communication log is always created.

   For detailed instructions, see "To check the progress/on-going status of the discovery job," on page 127.

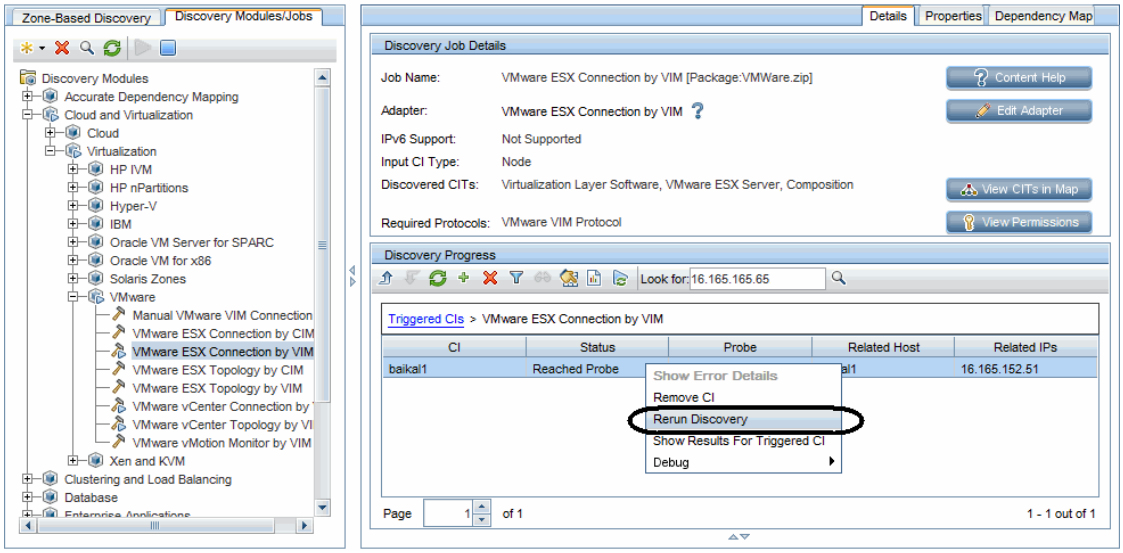
2. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

   For details, see "How to check device related logs for a discovered device?" on page 123.

VMware Discovery Jobs

To invoke the VMware discovery job manually,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Cloud and Virtualization > VMware > <select a job>**.
3. Right-click the selected job, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and select **Rerun Discovery** from the context menu.



7. To check the progress/on-going status of the discovery job,

   a. Modify the concerning adapter's configuration to make sure that the communication log is always created.

      For detailed instructions, see "To check the progress/on-going status of the discovery job," on page 127.

   b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

      For details, see "How to check device related logs for a discovered device?" on page 123.

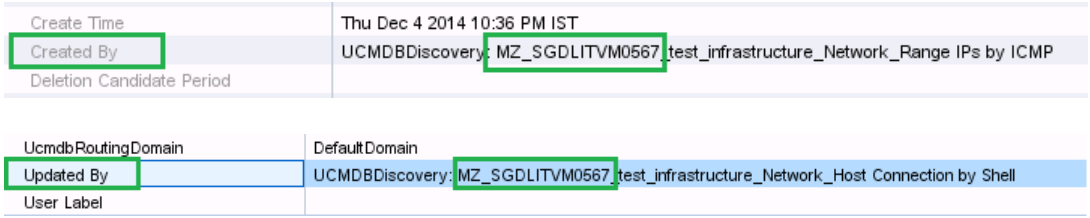
How to check which pattern (management zone) is used in the discovery for a discovered device?

Question: For a discovered device, how should I check which pattern (management zone) is used in the discovery?

In UD, there are two ways to check the management zone used:

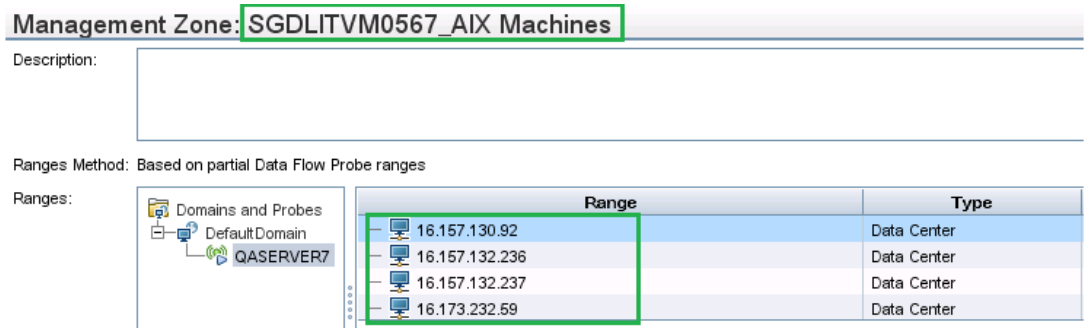
- **From IT Universe Manager**
  a. In the Modeling module, go to **IT Universe Manager**.
  b. On the Search CIs tab, enter the IP address for a discovered device in the **CI Name** field, select **Managed Object** for the **CI Type** field, and click .
  c. Click the returned entry on the Search CIs tab. CI details are displayed in the right pane.
  d. Go to the **Properties** tab for the CI and check the value for the following attributes:
     - Created By
     - Updated By

     For example,



- **From the Management Zone Description**
  a. In the Data Flow Management module, go to **Universal Discovery > Zone-Based Discovery**.
  b. From the Management Zones tree, select a management zone. The Management Zone description displays in the right pane.

     For example



How to check detailed discovery settings used in the discovery for a discovered device?

Question: For a discovered device, how should I check the detailed discovery settings (such as job parameters and scan settings) used in the discovery?

In UD, there are two ways to check detailed settings used in the discovery:

- **From UI** (the Properties tab and the Edit Inventory Discovery Activity dialog box)
  - Run jobs in **Discovery Modules/Jobs**

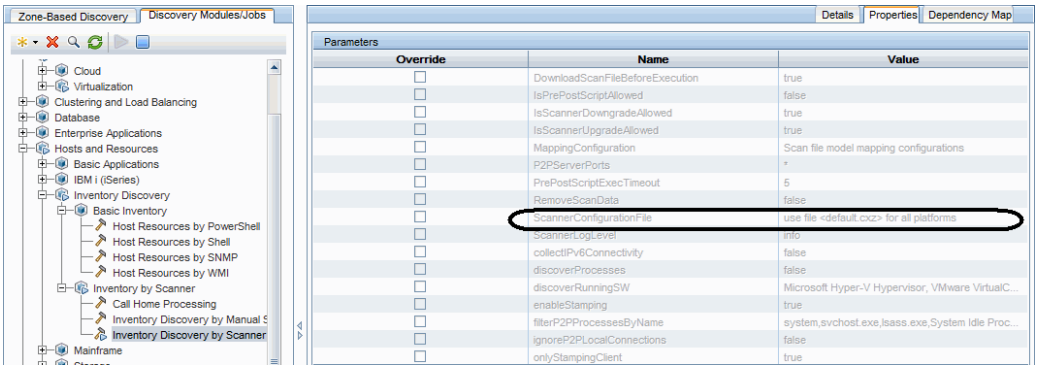
    The Properties tab of the Inventory Discovery by Scanner job displays all parameters and scanner settings of the job

    i. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.

    ii. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**).

    iii. In the pane, go to the **Properties** tab.

    All parameters and scanner settings of the job are displayed.



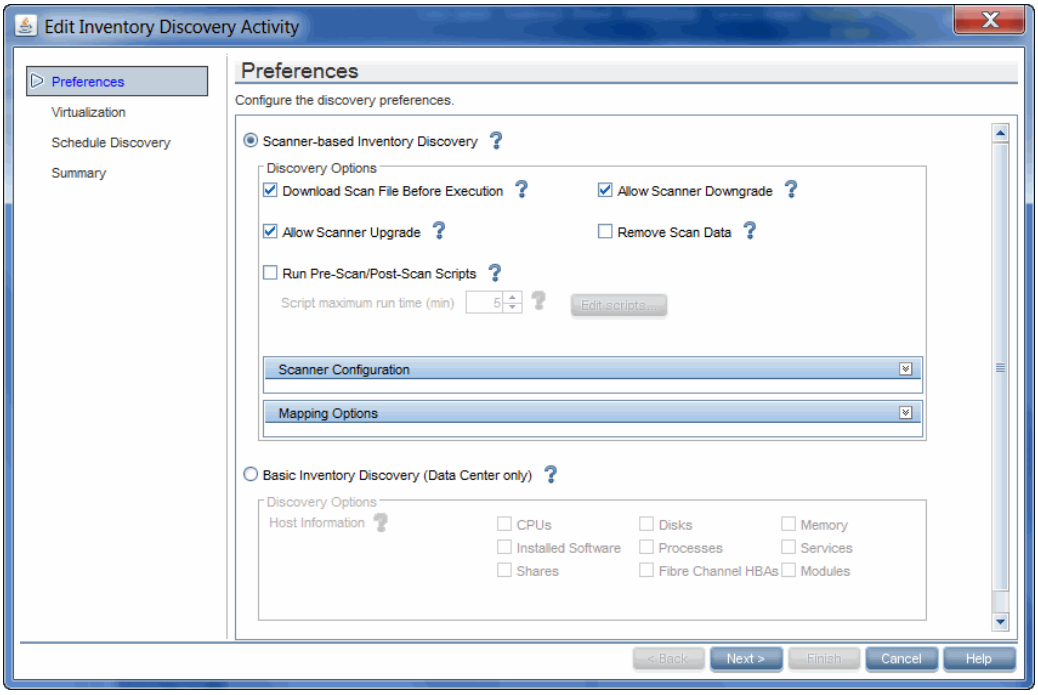
  - Run jobs in **Zone-Based Discovery**

    i. In the **Data Flow Management module, go to Universal Discovery > Zone-Based Discovery**.

    ii. From the Management Zones tree, select a management zone.

    iii. Right-click a discovery job and select **Edit** from the context menu.

The Edit Discovery Activity dialog box opens.



You can find the discovery job parameters and scanner settings in this dialog box.

- From the **Communication Log**

  a. Modify the configuration of the adapter for the Inventory Discovery by Scanner job to make sure that the communication log is always created.

     i. In the Data Flow Management module, go to **Adapter Management**.

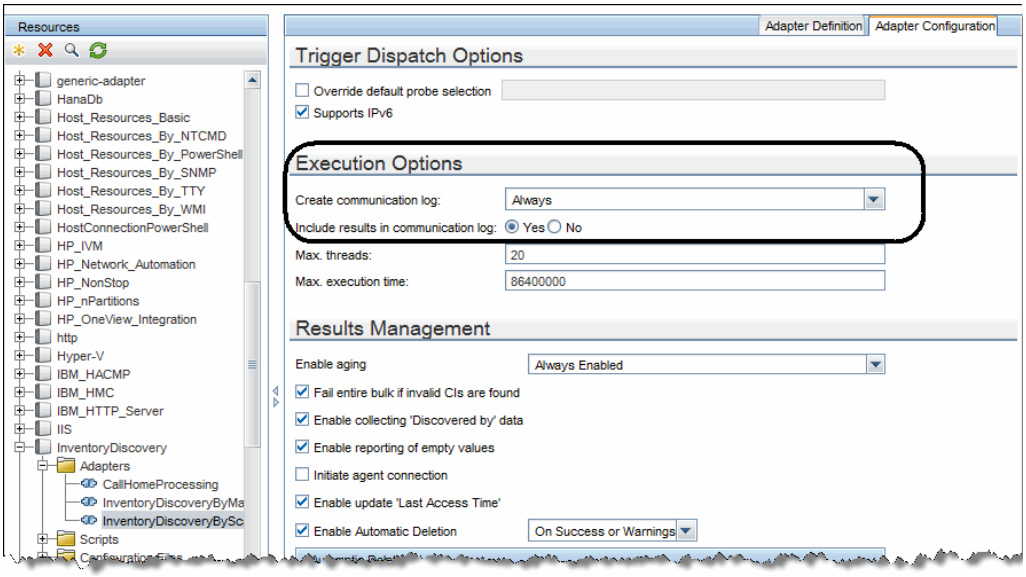
     ii. In the Resources pane, expand **InventoryDiscovery> Adapters > InventoryDiscoveryByScanner**.

     iii. In the right pane, click the **Adapter Configuration** tab.

     iv. In the Execution Options section, set the following:

     - **Create communication log**: **Always**

- **Include results in communication log**: **Yes**



b. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.

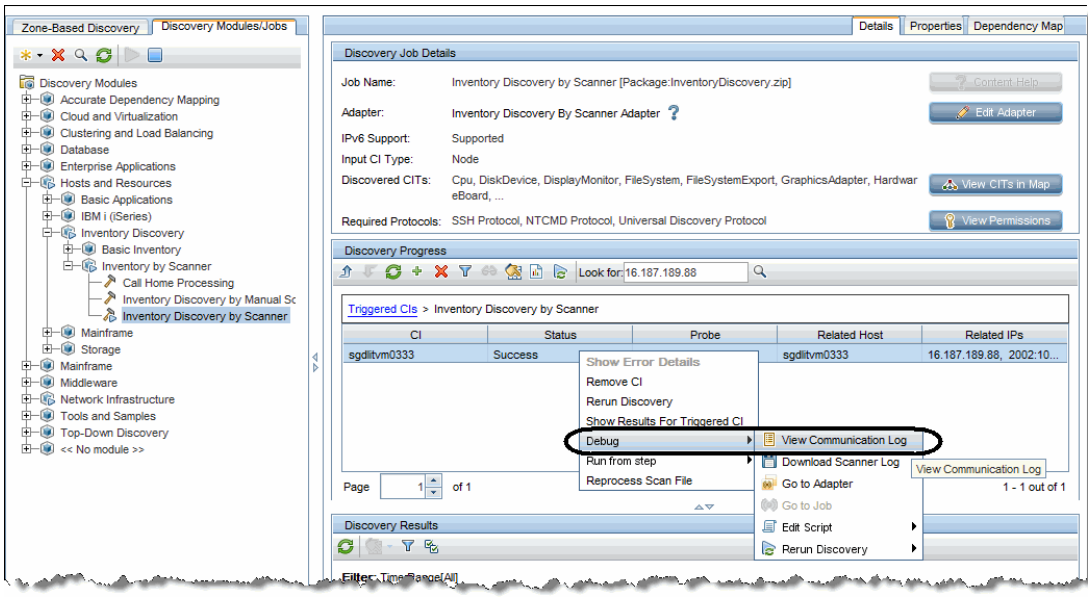
c. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.

d. (Optional) Right-click **Inventory Discovery by Scanner**), select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.

e. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.

f. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .

g. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.



h. In the log that opens, search keywords to check details:

- To locate where the job parameters start in the log, search **<params>**.
- To locate where the job parameters end in the log, search **</params>**.
- To locate where the scanner configuration file is used in the log, search **Config file to be used:**.

How to check the SNMP credentials used in the discovery for a discovered device?

Question: For a discovered device, how should I check the SNMP credentials used in the discovery?

To check the SNMP credentials used in the discovery, you can search the Communication Log of the Host Connection by SNMP job.

To view communication log for agent related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Network Infrastructure > Host Connection > Host**

Connection by SNMP.

3. (Optional) Right-click **Host Connection by SNMP**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.
7. In the log that opens, search **<CONNECT start** as keyword to locate the entry in the log that indicates starting from when the device is connected.

   For example:

```
<CONNECT start="08:05:20" duration="4" CMD="client_connect" RESULT="success"
type="snmp" credentialsId="7_1_CMS">
    <ClientProperties>
        <prop name="protocol_index" value="1" />
        <prop name="protocol_timeout" value="3000" />
        <prop name="credentialsId" value="7_1_CMS" />
        <prop name="cm_credential_id" value="7_1_CMS" />
        <prop name="snmpprotocol_version" value="version 2c" />
        <prop name="protocol_type" value="snmpprotocol" />
        <prop name="snmpprotocol_postfix" value="" />
        <prop name="port" value="161" />
        <prop name="protocol_netaddress" value="DEFAULT" />
        <prop name="ip_address" value="16.187.190.19" />
        <prop name="snmpprotocol_privalg" value="3DES" />
        <prop name="snmpprotocol_authalg" value="MD5" />
        <prop name="protocol_port" value="161" />
        <prop name="snmpprotocol_retry" value="2" />
        <prop name="snmpprotocol_snmpmethod" value="getnext" />
        <prop name="user_label" value="SNMP Protocol Credential 1" />
        <prop name="snmpprotocol_authmethod" value="noAuthNoPriv" />
        <prop name="retry" value="2" />
        <prop name="protocol_username" value="" />
        <prop name="protocol_in_use" value="false" />
    </ClientProperties>
</CONNECT>
```

   This log example indicates that the device is connected successfully by SNMP and the credential ID is **7_1_CMS**.

   The log information between the **<ClientProperties>** and **</ClientProperties>** tags are the details of the SNMP credential used in the discovery. Among these properties information, to find

out the credential name, you can check the value for the **user_label** attribute (highlighted above) of the SNMP credential that you defined in the SNMP protocol.

> **Note:** The SNMP community strings you defined in the protocol are encrypted in UD, therefore they are not visible in the log.

Chapter 5: Troubleshooting Configuration Manager

This chapter includes:

Troubleshooting and Limitations – Content Management

Problem. Changes in CIs in UCMDB are not reflected in Configuration Manager.

Solution. Configuration Manager runs an offline asynchronous analysis process. The process may not yet have processed the latest changes in UCMDB. To resolve this, try one of the following:

- Wait a few minutes. The default interval between analysis process executions is 10 minutes. This value is configurable in under **Administration > Settings**.
- Execute a JMX call to run the offline analysis calculation on the relevant view.
- Navigate to **Policies**. Click the **Recalculate Policy Analysis** button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

Problem. When you click the **Launch UCMDB** button, the UCMDB login page appears.

Solution. In order to access UCMDB without logging in again, you need to enable single sign-on. For details, see the section about enabling LW-SSO between Configuration Manager and UCMDB in the *HPE Universal CMDB Deployment Guide*. Additionally, ensure that the Configuration Manager user logged on is defined in the UCMDB user management system.

Problem. The **Matching Rules** tab does not appear in Universal CMDB when you navigate to **Managers > Modeling > CI Type Manager**, and select **CI Types** from the list box in the CI Types pane.

Solution. Navigate to **Managers > Administration > Infrastructure Settings** in Universal CMDB and set **Enable Configuration Manager Matching Rules** as `True`. After you log out and then log in again, the Matching Rules tab appears in the CI Type Manager.

Troubleshooting and Limitations – Federating Data to UCMDB

- Federation only works with CIs in the actual state. Therefore:
  - Policy compliance is federated only for CIs in the actual state.
  - The authorization status for CIs that were deleted from the actual state is not shown.
- The maximum number of CIs that can be federated is configurable. To change this number, edit the value of the Max Num To Federate setting in the Infrastructure Settings Manager in UCMDB. For details about changing settings, see "Infrastructure Settings Manager" in the *HPE Universal CMDB Administration Guide*. The recommended number of CIs is no more than 20,000, if large views have been enabled in Configuration Manager. For details about enabling support for large views, see the section about large capacity planning in the interactive *HPE Universal CMDB Deployment Guide*.
- If the test connection fails, click **Details** and check the first error in the stack trace for more information.
- Since a CI can be managed in multiple views, the same policy may be applied to the same CI in multiple views and may receive different similarity results, since the similarity group may be different in different views.

Troubleshooting – Explore Views

- **Problem**. Buttons for creating RFCs are disabled.

  Possible reasons:

  - The Change Management integration has been disabled for the activated configuration.
  - The Change Management integration has been defined, saved, and activated, but the user did not log in to Configuration Manager again.

  Solution. Do the following:

a. Navigate to **Administration > Integrations > Change Management**. To configure the integration, select the check box and provide the details for the Service Manager configuration.

b. Save and activate the configuration.

c. Log out and then log in again to see the changes take effect.

- **Problem.** RFC creation fails.
  - **Reason 1:** Incorrect credentials were defined for the integration user under **Administration > Integrations > Change Management > Service Manager**.

    Solution 1: In Service Manager, verify that the integration user exists. If required, update the password (for details, see the Service Manager documentation).

  - **Reason 2:** The user does not have the proper credentials to invoke a call to the Service Manager web-service.

    Solution 2: Enable the ability to execute the SOAP API for this integration user (for details, see the Service Manager documentation).

  - **Reason 3:** The UNL file for this integration has not been loaded into Service Manager.

    Solution 3: To detect if the UNL file has been uploaded, call the following Service Manager URL:

    <host>:<port example:13080>/sm/7/ucmdcm.wsdl

    If the call returns an XML file, then a web-service is on, meaning that the UNL file has been uploaded. If not, follow the directions in Import a UNL File into Service Manager.

  - **Reason 4:** An RFC has been created with at least one of the following mismatches:
    - The service does not exist in Service Manager.
    - One or more of the selected CIs does not exist in Service Manager.
    - The category value does not match a valid value in Service Manager.
    - The risk assessment value does not match a valid value in Service Manager.
    - The impact value does not match a valid value in Service Manager.
    - The urgency value does not match a valid value in Service Manager.

    Solution 4: Change the values for each of the possible mismatches listed above under **Administration > Application Management > RFC > RFC Creation**, so they match with the corresponding values in Service Manager. Save and activate the configuration for the settings to take effect.

  - **Problem.** Configuration Manager doesn't display RFCs.

> **Tip:** As a first step in identifying whether the problem is in UCMDB or Service Manager, you can execute a TQL query in UCMDB that fetches all RFCs from Service Manager. If RFCs are expected but do not appear in the query's results, it means that there is an issue with the integration between UCMDB and Service Manager.
>
> To execute this TQL query: log in to UCMDB and navigate to **Modeling > Modeling Studio > Resources** tab (select Queries as the Resource Type) **> Configuration Manager > Configuration Manager – Do not modify > Generate RFC Queries** and execute **amber_rfc_by_id**.

- **Reason 1:** The integration point between UCMDB and Service Manager is either not correctly configured or does not exist.

  Solution 1: See the UCMDB documentation for details on how to set up the integration between UCMDB and Service Manager.

- **Reason 2:** An RFC change phase value in the Configuration Manager settings does not match the RFC phase definition in Service Manager.

  Solution 2: Change the value for the RFC Change Phase field in the Configuration Manager settings to a valid value (as defined in Service Manager). Navigate to **Administration > Application Management > RFC > Fetch RFCs Criteria > RFC Filters** to change the settings. Note that the Change Phases field can contain multiple comma-separated values. Save and activate the configuration for the settings to take effect.

- **Reason 3:** The RFC does not meet the time window condition defined in the Configuration Manager settings for fetching RFCs.

  Solution 3: Make sure that the RFC meets the time window condition in the Configuration Manager settings, or change the condition so that the RFC matches the time window. Save and activate the configuration for the settings to take effect.

- **Reason 4:** The date and time format between the integration user used by Configuration Manager for this integration has a different format than the corresponding user in Service Manager.

  Solution 4: Make sure that the time format is defined identically for both user instances. In Configuration Manager, the Date Format definition is found under **Administration > Integrations > Change Management > Service Manager > Date Format**.

Troubleshooting – Review/Authorize

- **Problem**. Buttons for creating RFCs are disabled.

  Possible reasons:

  - The Change Management integration has been disabled for the activated configuration.
  - The Change Management integration has been defined, saved, and activated, but the user did not log in to Configuration Manager again.

  Solution. Do the following:

  a. Navigate to **Administration > Integrations > Change Management**. To configure the integration, select the check box and provide the details for the Service Manager configuration.

  b. Save and activate the configuration.

  c. Log out and then log in again to see the changes take effect.

- **Problem.** RFC creation fails.

  - **Reason 1:** Incorrect credentials were defined for the integration user under **Administration > Integrations > Change Management > Service Manager**.

    Solution 1: In Service Manager, verify that the integration user exists. If required, update the password (for details, see the Service Manager documentation).

  - **Reason 2:** The user does not have the proper credentials to invoke a call to the Service Manager web-service.

    Solution 2: Enable the ability to execute the SOAP API for this integration user (for details, see the Service Manager documentation).

  - **Reason 3:** The UNL file for this integration has not been loaded into Service Manager.

    Solution 3: To detect if the UNL file has been uploaded, call the following Service Manager URL:

    <host>:<port example:13080>/sm/7/ucmdcm.wsdl

    If the call returns an XML file, then a web-service is on, meaning that the UNL file has been uploaded. If not, follow the directions in Import a UNL File into Service Manager.

  - **Reason 4:** An RFC has been created with at least one of the following mismatches:

    - The service does not exist in Service Manager.
    - One or more of the selected CIs does not exist in Service Manager.

- The category value does not match a valid value in Service Manager.
- The risk assessment value does not match a valid value in Service Manager.
- The impact value does not match a valid value in Service Manager.
- The urgency value does not match a valid value in Service Manager.

Solution 4: Change the values for each of the possible mismatches listed above under **Administration > Application Management > RFC > RFC Creation**, so they match with the corresponding values in Service Manager. Save and activate the configuration for the settings to take effect.

- **Problem.** Configuration Manager doesn't display RFCs.

> **Tip:** As a first step in identifying whether the problem is in UCMDB or Service Manager, you can execute a TQL query in UCMDB that fetches all RFCs from Service Manager. If RFCs are expected but do not appear in the query's results, it means that there is an issue with the integration between UCMDB and Service Manager.
>
> To execute this TQL query: log in to UCMDB and navigate to **Modeling > Modeling Studio > Resources** tab (select Queries as the Resource Type) **> Configuration Manager > Configuration Manager – Do not modify > Generate RFC Queries** and execute **amber_rfc_by_id**.

- **Reason 1:** The integration point between UCMDB and Service Manager is either not correctly configured or does not exist.

  Solution 1: See the UCMDB documentation for details on how to set up the integration between UCMDB and Service Manager.

- **Reason 2:** An RFC change phase value in the Configuration Manager settings does not match the RFC phase definition in Service Manager.

  Solution 2: Change the value for the RFC Change Phase field in the Configuration Manager settings to a valid value (as defined in Service Manager). Navigate to **Administration > Application Management > RFC > Fetch RFCs Criteria > RFC Filters** to change the settings. Note that the Change Phases field can contain multiple comma-separated values. Save and activate the configuration for the settings to take effect.

- **Reason 3:** The RFC does not meet the time window condition defined in the Configuration Manager settings for fetching RFCs.

  Solution 3: Make sure that the RFC meets the time window condition in the Configuration Manager settings, or change the condition so that the RFC matches the time window. Save and activate the configuration for the settings to take effect.

- **Reason 4:** The date and time format between the integration user used by Configuration Manager for this integration has a different format than the corresponding user in Service Manager.

  Solution 4: Make sure that the time format is defined identically for both user instances. In Configuration Manager, the Date Format definition is found under **Administration > Integrations > Change Management > Service Manager > Date Format**.

Troubleshooting and Limitations – Views

The following limitations are applicable when working with managed views in Configuration Manager:

- Views that contain federated TQL queries cannot be selected for addition to the managed views list.
- If a view contains a node with a date restriction, you will see updated data for this view only if it is configured to be updated once per day (not each time the view is updated). To see updated data for such a view, use the JMX console to manually refresh the view.

Troubleshooting and Limitations – Policies

The following limitation is applicable when working with policies:

Condition TQL queries must not include attribute conditions on unmanaged attributes.

Chapter 6: Troubleshooting Automated Service Modeling

This chapter includes:

Automated Service Modeling (ASM) Troubleshooting

This chapter introduces the general troubleshooting guidelines for problems that may occur during the Service Modeling process.

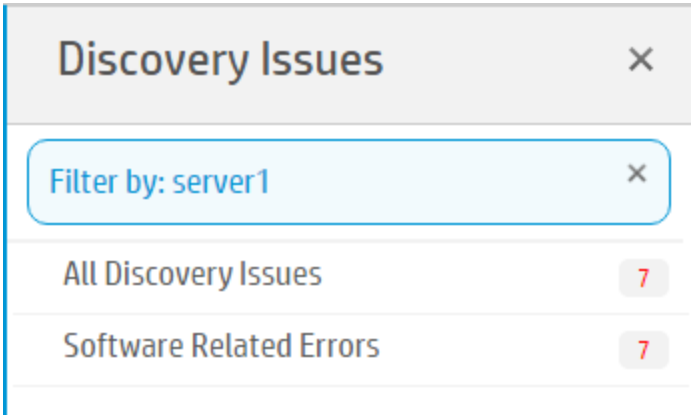
When an error occurs with a particular CI in the topology map, an error icon appears on the CI.

The following steps demonstrate the basic troubleshooting procedure for such an error:

1. View the error message in the UCDMB Browser.

   a. Click the error icon on the CI.

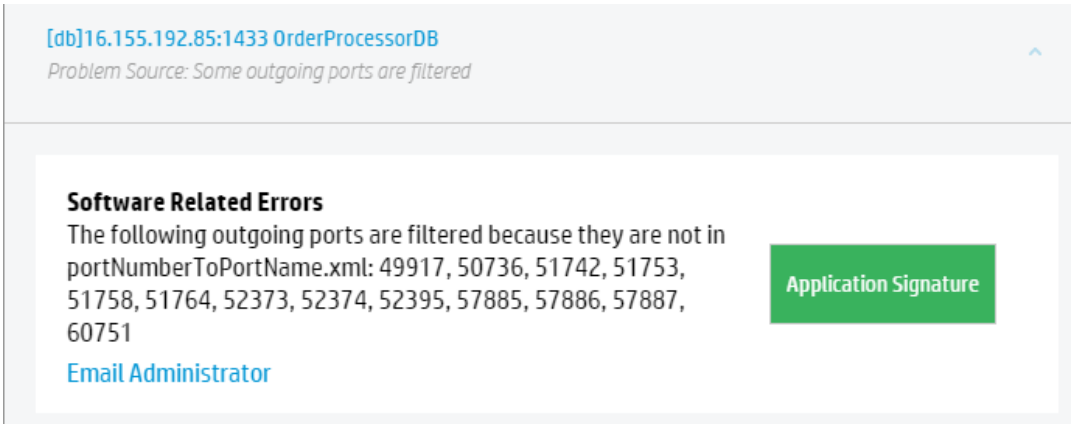
      The **Discovery Issues** pane appears and lists all the related discovery issues.



b. Click one of the categories.

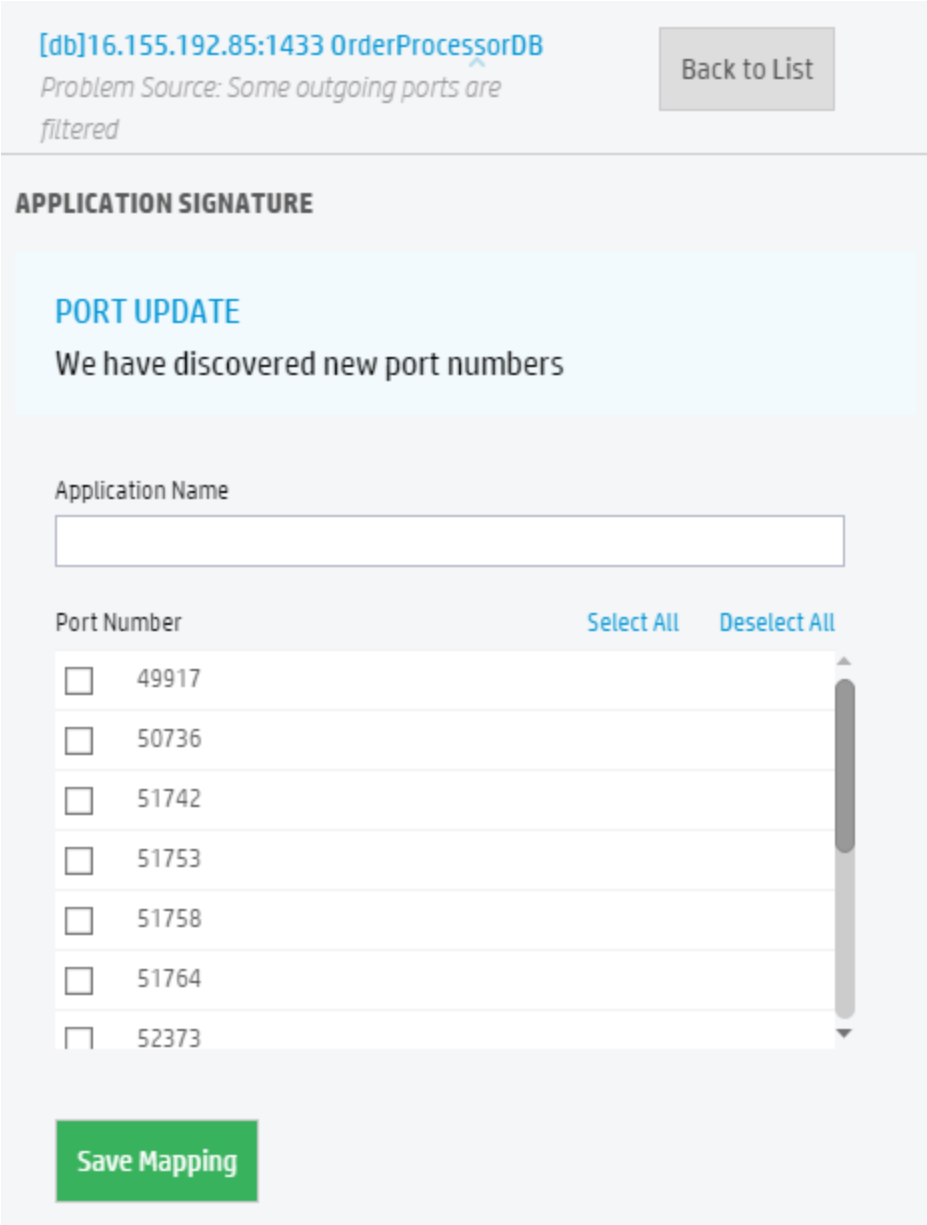
   A list of errors of the category appears.

c. Click an error to see the detailed error message.



2. Perform one of the following tasks when appropriate.

   - For some errors under **Software Related Errors**, you can directly provide some missing information from the UCMDB Browser. As in the above example, if you click the **Application Signature** button, you will be able to add the missing port numbers.



- Search the error message in this chapter, and try the suggested solutions.

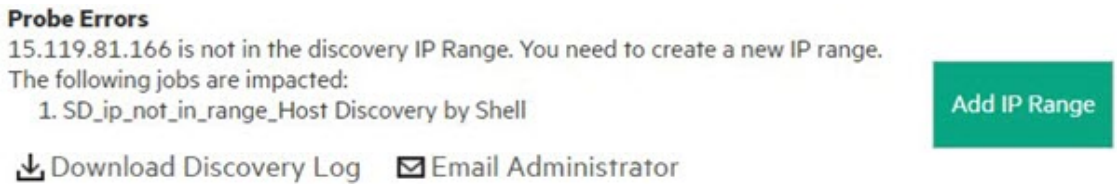
3. Rerun the Service Modeling task.

Host Discovery by Shell Job

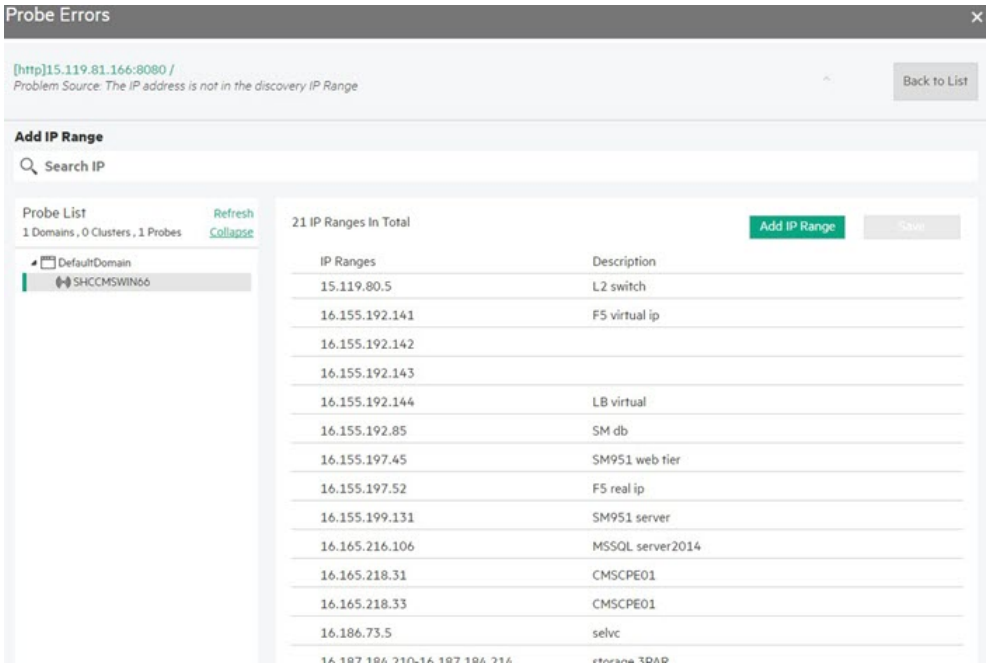
This chapter describes the error messages you may receive from the Host Discovery by Shell job and provides suggested solutions.

Error Message: The IP address is not in the discovery IP Range

Error Category: Probe Errors



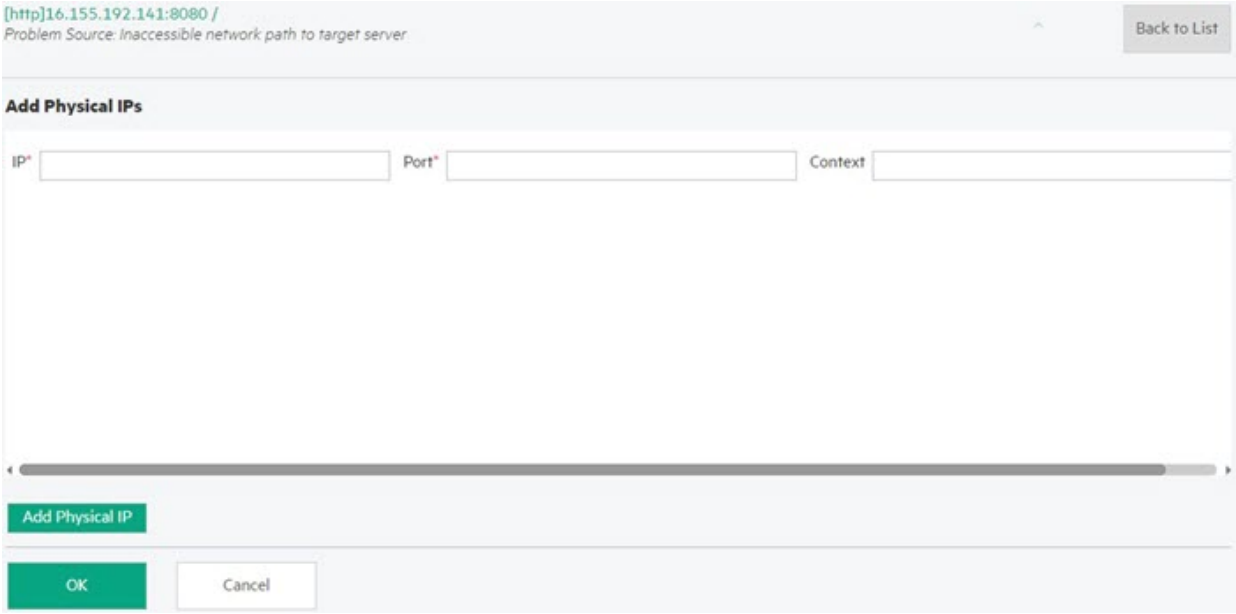
Solution: Add the IP address or range to the **Ranges** setting of the probe. For more information about how to do this, see "Add an IP Range to the Ranges Setting" on page 157.



Error Message: Inaccessible network path to target server. Perhaps it is a virtual IP address.

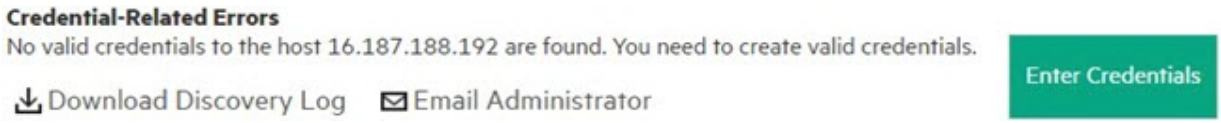
Error Category: Connection Errors

Solution: Add physical IPs as entry points of next hop

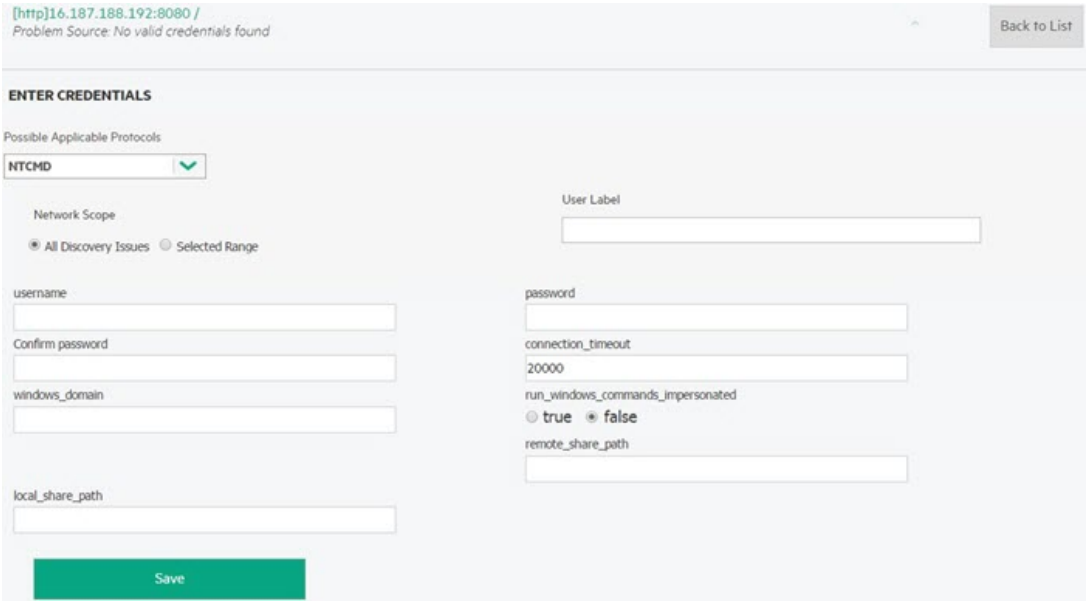


Error Message: Need credential to the host

Error Category: Credential-related Errors



Solution: Add the valid credentials. For more information about how to do this, see "Add or Edit Credentials" on page 157.



Error Message: Connection timeout

Error Category: Timeout Errors

Timeout Errors
SSH: Timeout trying to connect to the remote agent. Try increasing the timeout value.

Download Discovery Log Email Administrator

Solution:

- Increase the timeout value in protocol settings.
- For Windows machines, wait for a few minutes and then try again.

Error Message: The discovery job did not find any process listening on port: *<port_number>*

Error Category: Software Related Errors

Solution:

- Check if the configured account has sufficient privileges to run relevant commands. Specifically,
  - `ps -e`
  - `netstat -nap`
  - `lsof`

  Elevate privilege for UNIX credentials.
- Verify if the service is still accessible.
- Check if **lsof** is installed on the target machine if it runs UNIX.

Error Message: No application signature matches the process *<process_info>* listening on port *<port_number>*

Error Category: Software Related Errors

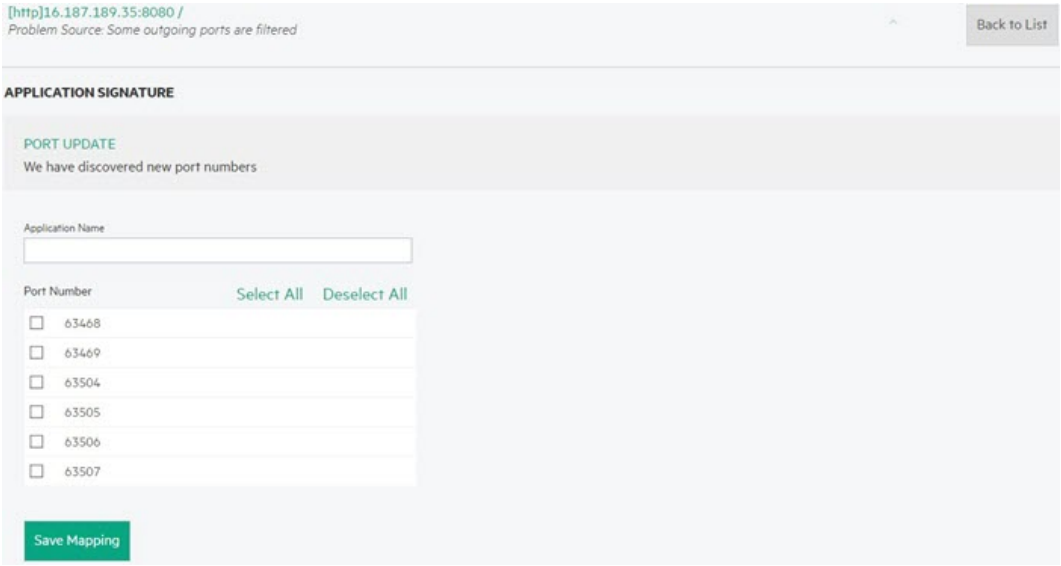
Solution: Add the signature for the application. For more information about how to do this, see "Add or Edit Application Signatures" on page 158.

Error Message: The following outgoing ports are filtered because they are not in **portNumberToPortName.xml**

Error Category: Software Related Errors

Solution: Add the port number to **portNumberToPortName.xml**.

To do this, click the **Application Signature** button in the error message and then follow the instructions. Alternatively, you can directly modify the **portNumberToPortName.xml** file to add the port number.



Error Message: Failed to resolve host name to IP

Error Category: IP-related Errors

Solution: Check DNS server configuration.

Error Message: Need sudo permission

Error Category: Software Related Errors

Solution: Elevate privilege for UNIX credentials to run the relevant command.

Error Message: No lsof installed on the host

Error Category: Software Related Errors

Solution: Install lsof on the target machine.

Error Message: The host is a Solaris local zone

Error Category: Software Related Errors

Solution: None for this release. Currently Solaris local zone is not supported by ASM.

References

This chapter provides instructions for some of the solutions mentioned earlier.

Add an IP Range to the Ranges Setting

1. Go to **Data Flow Probe Setup** > **Domains and Probes** pane > **Domains and Probes** root node > a domain > **Data Flow Probes** > a Data Flow Probe.
2. In the **Ranges** pane, click **New Range** .
3. Provide the necessary information on the **New Ranges** dialog box, and then click **OK**.

Discover Load Balancers

1. Run the Host Connection by SNMP job.
2. Run one of the following jobs depending on the type of the load balancer:
   - F5 BIG-IP LTM by SNMP
   - Alteon application switch by SNMP
   - Cisco CSS by SNMP

Add or Edit Credentials

1. Go to **Data Flow Probe Setup** > **Domains and Probes** pane > **Domains and Probes** root node > a domain > Credentials > a protocol.
2. In the right pane, perform one of the following actions to add or edit an entry:

- To add a new connection detail, click **Create new connection details for selected protocol type** .
- To edit an existing credential, select the entry and then click **Edit connection details for selected protocol type** .

3. Provide the information on the dialog box that pops up, and then click **OK**.

Edit the portNumberToPortName.xml File

1. Go to **Data Flow Management > Adapter Management**.
2. Click the **Search** button , and then search for **portNumberToPortName.xml**.
3. Edit the **portNumberToPortName.xml** file, and then click **Save**.

Add or Edit Application Signatures

1. Go to **Data Flow Management > Adapter Management**.
2. In the Resources pane, select **Host_Resources_By_TTY > Adapters > TTY_HR_All**.
3. In the **Adapter Definition** tab > **Global Configuration Files** section, select **applicationsSignature.xml** and then click **Edit** .

Chapter 7: Troubleshooting Development

This chapter includes:

Troubleshooting Migration from Jython Version 2.1 to 2.5.3

Universal Discovery now uses Jython version 2.5.3. All out-of-the-box scripts have been properly migrated. If you developed your own Jython scripts prior to this upgrade for use by Discovery, you may run into the following issues and have to make the fixes indicated.

> **Note:** You must be an experienced Jython developer to make these changes.

String Formatting

- **Error message:** `TypeError: int argument required`
- **Possible cause:** Using string formatting to decimal integer from string variable containing integer data.
- **Problematic Jython 2.1 code:**

```
variable = "43"
print "%d" % variable
```

- **Correct Jython 2.5.3 code:**

```
variable = "43"
print "%s" % variable
```

or

```
variable = "43"
print "%d" % int(variable)
```

Checking String Type

The code below may not work correctly if input contains unicode strings:

- **Problematic Jython 2.1 code:** `isinstance(unicodeStringVariable,'')`
- **Correct Jython 2.5.3 code:** `isinstance(unicodeStringVariable,basestring)`

  The comparison should be done with `basestring` to test whether an object is an instance of `str` or unicode.

Non-ASCII character in file

- **Error Message:**
  `SyntaxError: Non-ASCII character in file 'x', , but no encoding declared; see http://www.python.org/peps/pep-0263.html for details`
- **Correct Jython 2.5.3 code:** (add this to the first line in the file)

  ```
  # coding: utf-8
  ```

Import sub-packages

- **Error message:**
  `AttributeError: 'module' object has no attribute 'sub_package_name'`
- **Possible cause:** A sub-package is imported without explicitly specifying the name of sub-package in the import statement.
- **Problematic Jython 2.1 code:**

  ```
  import a
  print dir(a.b)
  ```

  The sub-package is not explicitly imported.
- **Correct Jython 2.5.3 code:**

  ```
  import a.b
  ```

  or

  ```
  from a import b
  ```

Iterator Changes

Starting from Jython 2.2, the **__iter__** method is used to loop over a collection in the scope of a **for-in** block. The iterator should implement the **next** method, returning an appropriate element or throw the **StopIteration** error if it reached the end of the collection. If the **__iter__** method is not implemented, the **getitem** method is used instead.

Raising Exceptions

- **Jython 2.1 method for raising exceptions is obsolete:**
  ```
  raise Exception, 'Failed getting contents of file'
  ```
- **Recommended Jython 2.5.3 method for raising exceptions:**
  ```
  raise Exception('Failed getting contents of file')
  ```

Troubleshooting and Limitations – Developing Generic Database Adapters

This section describes troubleshooting and limitations for the generic database adapter.

General Limitations

- When you update an adapter package, use Notepad++, UltraEdit, or some other third-party text editor rather than Notepad (any version) from Microsoft Corporation to edit the template files. This prevents the use of special symbols, which cause the deployment of the prepared package to fail.
- In most of the cases, after making a change, it is needed to reload the adapter on the probe side, otherwise the adapter will not function properly

  a. Log in to the probe JMX console: **https://localhost:8453/**

  b. Locate the **adapters** bean, and reload adapter with the integration point name.

  If the adapter is not reloaded after each change, issues may occor (wrong error messages, query failures, and so on).

JPA Limitations

- All tables must have a primary key column.
- CMDB class attribute names must follow the JavaBeans naming convention (for example, names must start with lower case letters).
- Two CIs that are connected with one relationship in the class model must have direct association in the database (for example, if `node` is connected to `ticket` there must be a foreign key or linkage table that connects them).
- Several tables that are mapped to the same CIT must share the same primary key table.

Functional Limitations

- You cannot create a manual relationship between the CMDB and federated CITs. To be able to define virtual relationships, a special relationship logic must be defined (it can be based on properties of the federated class).
- Federated CITs cannot be trigger CITs in an impact rule, but they can be included in an impact analysis TQL query.
- A federated CIT can be part of an enrichment TQL, but cannot be used as the node on which enrichment is performed (you cannot add, update, or delete the federated CIT).
- Using a class qualifier in a condition is not supported.
- Subgraphs are not supported.
- Compound relationships are not supported.
- The external CI CMDB`id` is composed from its primary key and not its key attributes.
- A column of type `bytes` cannot be used as a primary key column in Microsoft SQL Server.
- TQL query calculation fails if attribute conditions that are defined on a federated node have not had their names mapped in the **orm.xml** file.

Troubleshooting - Build an Adapter Package

The procedure for building a new push adapter requires complete and correct re-naming and replacing. Any error will likely affect the adapter. The package must be unzipped and re-zipped correctly to act as a UCMDB package. Refer to the out-of-the-box packages as examples. Common errors include:

- Including another directory on top of the package directories in the ZIP file.

  Solution: ZIP the package in the same directory as the package directories such as **discoveryResources**, **adapterCode**, etc. Do not include another directory level on top of this in the ZIP file.

- Omitting a critical re-name of a directory, a file, or a string in a file.

  Solution: Following the instructions in this section very carefully.

- Misspelling a critical re-name of a directory, a file, or string in a file.

  Solution: Do not change your naming convention in mid-stream once you begin the re-naming procedure. If you realize that you need to change the name, start over completely rather than trying to retroactively correcting the name, as there is a high risk of error. Also, use search and replace rather than manually replacing strings to reduce risk of errors.

- Deploying adapters with the same file names as other adapters, especially in the **discoveryResources** and **adapterCode** directories.

  Solution: You may be using a UCMDB version with a known issue that prevents mappings files from having the same name as any other adapter in the same UCMDB environment. If you attempt to deploy a package with duplicates names, the package deployment will fail. This problem may occur even if these files are in different directories. Further, this problem can occur regardless of whether the duplicates are within the package or with other previously deployed packages.

At this point you can create a new push adapter job in the Integration Studio using the new adapter you just deployed.

Chapter 8: Troubleshooting Hardening

This chapter includes:

Troubleshooting and Limitations - Data Flow Credentials Management

If you change the default domain name on the UCMDB server, you must first verify that the Data Flow Probe is not running. After the default domain name is applied, you must execute the **DataFlowProbe\tools\clearProbeData.bat** script on the Data Flow Probe side.

> **Note:** Execution of the **clearProbeData.bat** script will cause a discovery cycle on the Probe side once the Probe is up.

Troubleshooting and Limitations - LW-SSO Authentication

This section describes known issues and limitations when working with LW-SSO authentication.

Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

  Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

- **Multi-domain logout functionality when using Internet Explorer 7.** Multi-domain logout functionality may fail under the following conditions:
  - The browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

  In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

  As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application.**

  If a domain is defined in the LW-SSO configuration:
  - The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.**companydomain**.com/WebApp.

    > **Note:** The length of the FQDN cannot be longer than the value of the **Maximum domain extension length** setting in the Infrastructure Settings Manager. The default value is 8.

  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.
  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

  If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. In this case, a LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.

- **Multi-Domain Support.**
  - Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window,

except when both applications are in the same domain.

- The first cross domain link using **HTTP POST** is not supported.

  Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET.**

- LW-SSO Token size:

  The size of information that LW-SSO can transfer from one application in one domain to another application in another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

- Linking from Protected (HTTPS) to non-protected (HTTP) in a multi-domain scenario:

  Multi domain functionality does not work when linking from a protected (HTTPS) to a non-protected (HTTP) page. This is a browser limitation where the referrer header is not sent when linking from a protected to a non-protected resource. For an example, see: `http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`

- Third-Party cookie behavior in Internet Explorer:

  Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences (P3P) Project," meaning that cookies coming from a Third Party domain are blocked by default in the Internet security zone. Session cookies are also considered Third Party cookies by IE, and therefore are blocked, causing LW-SSO to stop working. For details, see: `http://support.microsoft.com/kb/323752/en-us`.

  To solve this issue, add the launched application (or a DNS domain subset as *.mydomain.com) to the Intranet/Trusted zone on your computer (in Microsoft Internet Explorer, select **Menu > Tools > Internet Options > Security > Local intranet > Sites > Advanced)**, which causes the cookies to be accepted.

  > **Caution:** The LW-SSO session cookie is only one of the cookies used by the Third Party application that is blocked.

- **SAML2 token**

  - Logout functionality is not supported when the SAML2 token is used.

    Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.

  - **The SAML2 token's expiration is not reflected in the application's session management.**

    Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.

- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.
- **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

  It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the **common\classes** Tomcat folder.
- **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.
- **Demo mode.** In Demo mode, LW-SSO supports links from one application to another but does not support typing a URL into a browser window, due to an HTTP referrer header absence in this case.

Chapter 9: Troubleshooting Modeling

This chapter includes:

Troubleshooting and Limitations – Topology Query Language

This section describes troubleshooting and limitations for Topology Query Language.

- When creating resources, such as TQL queries, views, and Impact rules, make sure that there are no spaces at the end of the resource name.
- In a multi-tenancy environment, TQL query names cannot contain an **@** character.
- When importing a resource (for example, TQL query, view) in a multi-tenancy environment in Modeling Studio, for the import to work, the TQL query used for the creation of the view needs to have as consumer or owner tenant, the tenant associated with the user that performs the import. The user who performs the import of a view has to have at lest view permission on the TQL query used.

  The instructions below are an example for your reference:

  a. Create a tenant.

  b. Create a role with the following permissions: All permissions on view and folder, and permissions to access Modeling Studio.

  c. Create a user with the above role in the context of tenant from step a.

  d. Go to **Modeling Studio > Resources > View**, assign the tenant created in step a for the desired folder as owner tenant. (Meaning that the views are assigned to the tenant associated with the user who will perform the import.)

  e. Log in as the new user.

  f. In Modeling Studio, import a new view.
- If an error occurs while working with views in the Modeling managers, when adding CIs to the CMDB, or when updating existing CIs, and the error log indicates that objects are missing in the

database, do the following:

a. Perform a DB backup.

b. Access the JMX console and run the following methods under **service=DAL services**:

- **rebuildModelViews**
- **rebuildModelDBSchemaAndViews**

> **Caution:** Invoking the above JMX method could drop the following: attributes, tables, indexes. Random usage is prohibited.

- If the login takes a long time when navigating to the Modeling modules, go to Infrastructure Settings Manager and set the value of the **mam.gui.automation.flow.mapping.enabled** setting to false. This disables the Automation Flow functionality but improves the login time for the Modeling modules.
- For TQL queries to be valid, they must comply with certain restrictions.

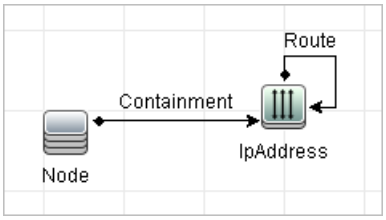
  This section includes the following topics:

  - "Understanding Validation Restrictions" below
  - "Impact Analysis TQL Query Validation" on the next page
  - "Enrichment TQL Query Validation" on page 171

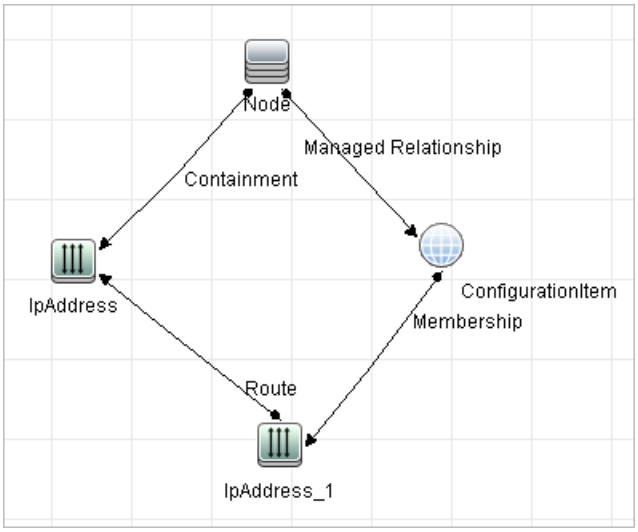
Understanding Validation Restrictions

For Impact Analysis, Discovery, and Enrichment TQL query types to be valid, they must comply with the following restrictions:

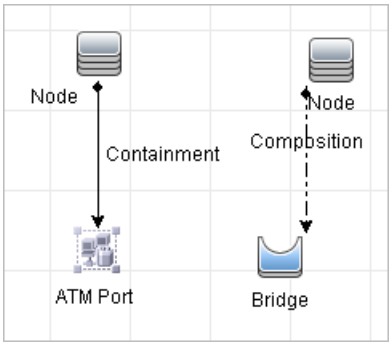
- **Unique Names.** TQL query elements must have unique names.
- **Self Relationships**. A TQL query must not contain self relationships, that is, a relationship must not lead from a query node to itself, as the following example illustrates:



- **Cyclic Graph**. The TQL query structure cannot be a closed circle, as shown in the following example:



- **Separate Query Nodes and Groups**. All the TQL query nodes must be linked to one another, that is, the TQL query cannot contain separate query nodes or groups, as the following example illustrates:

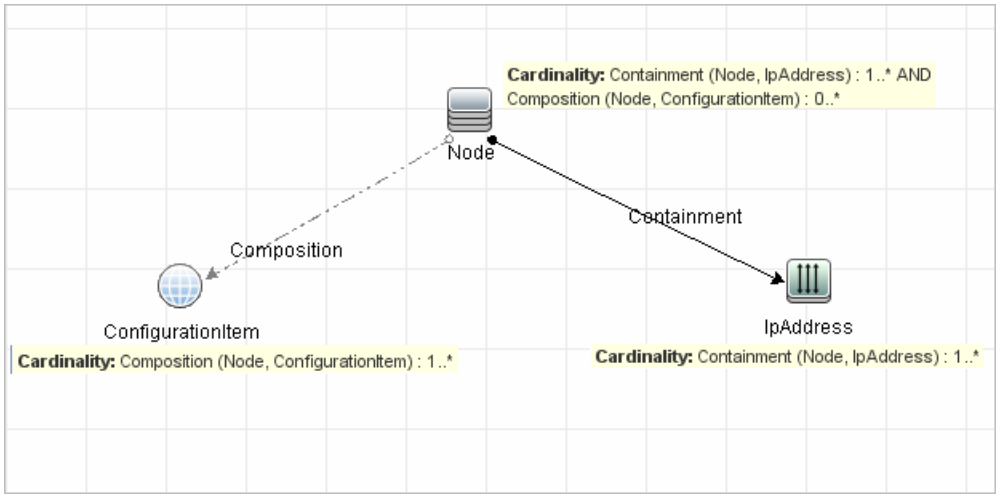


Impact Analysis TQL Query Validation

Impact Analysis TQL queries must also comply with the following restrictions:

- **Number of query nodes**. An Impact Analysis TQL query must consist of at least two query nodes.
- **Trigger and affected query nodes must be connected**. There must be a path of relationships from the triggered query node to the affected query nodes.
- **Selecting query nodes to function as Impact Analysis triggers**. When selecting query nodes to function as Impact Analysis triggers, the query nodes must comply with the following restrictions:

- You can select more than one query node as a trigger. However, you cannot define a query node both as affected and as a trigger.
- If a query node has a relationship whose minimum limit is 0 (meaning that one of its ends does not necessarily have a query node linked to it), the query node that is linked to its other end cannot be a root cause query node (because it may or may not exist in the TQL query). For details about minimum limits, see "Cardinality Tab". For example, **Configuration Item** cannot be either a root cause or affected query node because it is connected to the query node with a **Min** limit of `0`.



> **Note:** A query node that is hidden cannot be a root cause or an affected query node.

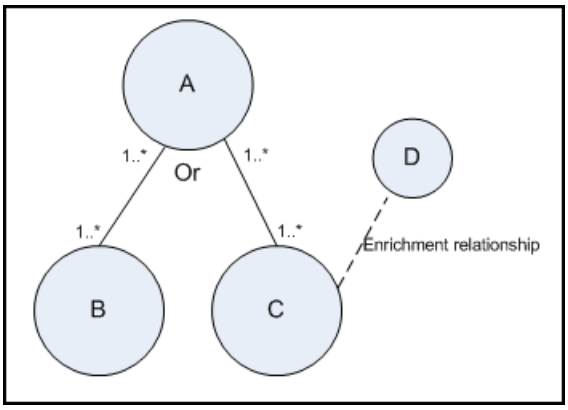
- **The connection between trigger and affected query nodes**. The trigger query node and affected query nodes you define must be connected by a path of relationships from the triggered query node to the affected query nodes.

Enrichment TQL Query Validation

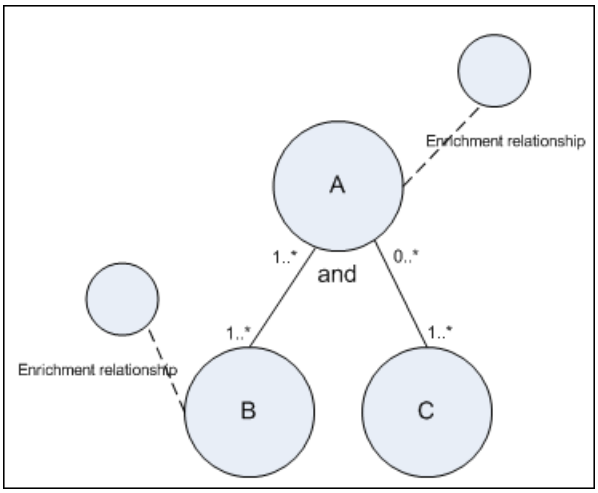
Enrichment TQL queries must comply with the following restriction:

- **Required elements**. You cannot perform Enrichment on a non-required query node, that is, a query node that does not necessarily appear in the TQL query results.

  Example 1. In this example, the TQL query results can be either **A** and **B** or **A** and **C**. Therefore, you cannot add an Enrichment query node to query nodes **B** or **C** because they are not required elements. You can add an Enrichment query node to query node **A** because it always appears in the TQL query results. For details on how to add Enrichment query nodes and relationships, see Add Enrichment Query Nodes and Relationships to an Enrichment TQL Query.



Example 2. In this example, both **A** and **B** are required elements that always appear in the TQL query results. Only **C** is not a required element because it has a cardinality of 0. Therefore, you cannot add an Enrichment query node to it.



Troubleshooting and Limitations – CI Selector

This section describes troubleshooting and limitations for the CI Selector.

Unavailable Views and CIs

The View list in the CI Selector may not display all views in the CMDB, or it may not display the contents of a view, for any of the following reasons:

- The View list includes only the views for which you have the necessary permissions. Similarly, Search mode is only available if you have the **Allow Search** general action permission. To set

permissions, select **Managers > Administration** > **Roles Manager**. For more information, see Roles Manager in the *HPE Universal CMDB Administration Guide*.

- Views that are currently inactive appear in red in the View list, but they cannot be selected. In IT Universe Manager, inactive views appear in faded text.
- Out-of-the-box views for which you do not have a license may appear in the View list, but these views do not contain CIs. For information on the out-of-the-box views, see Predefined Folders and Views.

> **Note:** After deleting one or more query nodes from a TQL query, it can take time for changes to be updated to the view; meanwhile, the removed CIs appear in the view. If you select one of these CIs before it is updated, an error message is displayed. Click the **Refresh** button to update the view.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on CMS Troubleshooting Guide (Universal CMDB 10.33)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to cms-doc@hpe.com.

We appreciate your feedback!