



HP Universal CMDB & Configuration Manager

Software Version: 10.11 CUP6

Release Notes

Document Release Date: August 2015
Software Release Date: August 2015

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP 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

© 2002 - 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

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

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

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

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

Support

Visit the HP Software Support site at: <https://softwaresupport.hp.com>.

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

HP Software 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 HP 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 an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this website is <http://h20230.www2.hp.com/sc/solutions/index.jsp>.

Contents

HP Universal CMDB & Configuration Manager Release Notes	5
What's New	5
What's New in UCMDB 10.11 CUP6	5
What's New in UCMDB 10.11 CUP5	6
What's New in UCMDB 10.11 CUP4	7
What's New in UCMDB 10.11 CUP3	9
Installation Notes	9
HP Universal CMDB and Configuration Manager 10.11 CUP6 Files/Components	9
System Requirements	10
Install 10.11 CUP6 on the HP Universal CMDB and Configuration Manager Servers	11
HP Universal CMDB 10.11 CUP6 Manual Data Flow Probe Installation	13
HP Universal CMDB and CM 10.11 CUP6 Uninstall Procedure	13
Notes	15
Known Problems, Limitations, and Workarounds	16
Enhancements Requests	29
Enhancements Requests in 10.11 CUP6	29
Enhancements Requests in 10.11 CUP5	29
Enhancements Requests in 10.11 CUP4	31
Fixed Defects	32
Fixed Defects for UCMDB 10.11 CUP6	32
Fixed Defects for UCMDB 10.11 CUP5	36
Fixed Defects for UCMDB 10.11 CUP4	40
Fixed Defects for UCMDB 10.11 CUP3	43
Fixed Defects for UCMDB 10.11 CUP2	48
Fixed Defects for UCMDB 10.11 CUP1	50
Documentation Errata	52
Appendixes	54
Enable Secure Login for the JMX Console	54
How to Re-index the CIs of a Given CI Type	55

How to Perform a Full Reindex of All CIs	56
How to Configure Query Search Filter	56
How to Mark Sensitive Settings and Enable Storing Encrypted Data in the Database Using JMX	57
How to Set Shared Key for Encrypting or Decrypting the InfrastructureSettings.xml File Using JMX	59
Enable Mutual Certificate Authentication for SDK	60
How to Set Master Keys	63
How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification	66
1_script_delete_index.sql	68
2_script_delete_constraint.sql	69
Send Documentation Feedback	71

HP Universal CMDB & Configuration Manager Release Notes

Keep your system up to date with the most recent cumulative update package (CUP) for UCMDB 10.11. This package contains all of the UCMDB 10.11 hotfixes that have been released since the initial release of UCMDB 10.11.

What's New

What's New in UCMDB 10.11 CUP6

UCMDB 10.11 CUP6 contains the following new features and changes:

- Added user password expiration policy settings in the Infrastructure Settings Manager

To access the settings, go to **Administration > Infrastructure Settings Manager > Security Settings**.

Name	Description	Default Value
User password expires after the specified number of days	User password expires after the specified number of days	90
User password expires after the specified number of generations	User password expires after the specified number of generations	4

Note: In order for the above password expiration checks (the expiration time and repetition of passwords generation) to be validated, you must manually set the value for the **Passwords must use default policy** setting to **true** to enable the above user password expiration policy settings. The default value for the **Passwords must use default policy** setting is false.

- You can verify names of CI Types during the matching phase of the identification process for the

TenantOwner attribute by using the new JMX setting **reconciliation.tenantaware.citypes**. If, compared to the other CI, the value of the **TenantOwner** attribute is different, the verification process stops and the match is rejected.

For details, see ["How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification" on page 66](#).

- You can use the JMX console to change the master key that is used to encrypt all UCMDB keys. For detailed instructions, see ["How to Set Master Keys" on page 63](#).
- As an integration user, with tenant information set on the TQL query layout, your autocomplete reconciliation data will also have set the assigned tenant information during push flows.

What's New in UCMDB 10.11 CUP5

UCMDB 10.11 CUP5 contains the following new features and changes:

- **Enhancements implemented to server health check**
 - Added a new JMX method **exportDiscoveryProcessingStatisticsToExcel** in **UCMDB:service=Reconciliation Services**. After invoking this method, an Excel file named **DiscoveryProcessingStatistics.xlsx** in the ZIP file is generated to record discovery throughput statistics data.
 - Added a new JMX method **testConnectionToDB** in **UCMDB:service=DAL services**. Stored procedures for Oracle and MSSQL will be used when invoking the **testConnectionToDB** method.
 - Added a JMX supportability handler **Memory and Thread Count Info** to record the UCMDB memory usage and thread count in the **MemoryAndThreadInfo.html** file. The information is displayed in color: green, orange, and red. If the color is not green, it requires attention.

Note: LDAP authentication can generate many idle threads. Until these threads are closed, it can temporarily lead to a high thread number, which is causing performance potential issues.

- Added a new JMX method **reindexCiType** in **UCMDB:service=Topology Search Services**. This method selects a subset of data in a short time.

- Added a new JMX method **deactivateAllViewsTqls** in **UCMDB:service=New Views Services** to deactivate all the TQL queries that are related to views.
- Added a new setting **cmdb.search.use.query.syntax.tree** to the **setSettingValue** method to control if syntax tree is logged or not.

To enable the setting,

- a. Go to **JMX Console > UCMDB:service=Settings Services**.
- b. Locate the **setSettingValue** method.
- c. To enable logging of syntax tree, invoke the **setSettingValue** method with the following parameters:
 - **customerID:** <customer id>
 - **name:** cmdb.search.use.query.syntax.tree
 - **value:** true

What's New in UCMDB 10.11 CUP4

UCMDB 10.11 CUP4 contains the following new features and changes:

- **A lockout mechanism is now available**

The lockout mechanism allows UCMDB administrators to:

- enable or disable the lockout mechanism
- specify how many failed login attempts are allowed before a user is locked out
- specify the period of time after which the locked accounts will be automatically released
- retrieve a list of locked out users and unlock certain users

In addition, all failed login attempts will be logged, and consecutive attempts are reported to the proper security administration personnel in your organization.

The table below describes the new infrastructure settings available with the lockout mechanism (**Administration > Infrastructure Settings Manager > Security Settings**):

Name	Description	Default Value
User lockout mechanism enabled	Enable the user lockout mechanism after a number of failed login attempts.	True
User lockout timeout value (minutes)	The time value in minutes until the next login attempt can be successfully permitted in case the current user is locked out.	10
The maximum number of failed login attempts prior to a user lockout	The maximum number of failed login attempts before a user enters the timed lock out state.	3

Also in JMX, under **Security Services**, two new methods are added for unlocking users:

- **retrieveCurrentlyLockedOutUsers.** Retrieves a list of the currently locked out users and allows individual unlocking.
- **unlockUser.** Allows unlocking a certain user that is currently locked out by the login mechanism.
- Added a new API method **void setDiscoveryConfigurationXML(String xmlString, boolean includeGroup).**

Compared to the existing API method **void setDiscoveryConfigurationXML(String xmlString)**, this new method contains the **includeGroup** parameter. The **includeGroup** parameter allows you to set whether you want to update the entire device group.

For example, if you want to update IP ranges and credentials only and leave the statuses of all jobs as is, you can invoke this new method by setting the **includeGroup** parameter to **false**.

- Added multi-tenant status information into the system information to show whether the UCMDDB Server is set up as a single-tenant or multi-tenant environment.

The multi-tenant status information can be seen in two places:

- a. **Mbean: UCMDDB:service=Server Services. Method: viewSystemInformation**

When executing the JMX method **viewSystemInformation**, the result now displays an additional line:

MT: [enabled | disabled]

b. **Mbean: UCMDB:service=Supportability Services. Method: runSupportHandlersForAllCategories**

When exporting the UCMDB System Info information by executing the JMX supportability tool (JMX method **runSupportHandlersForAllCategories**), in one of the archive files created (**systemInfo.properties**), a new line is added to display the status of the multi-tenancy:

MT: [enabled | disabled]

What's New in UCMDB 10.11 CUP3

UCMDB 10.11 CUP3 contains the following change:

- A new attribute **isTopologyRequired** is added in the **<connected-ci-condition>** XML tag of the reconciliation rule of a CI type. Setting the **isTopologyRequired** attribute value to **true** overrides the UNKNOWN result with FALSE for a validation criterion when there are no connected CIs. (QCCR1H96982)

The following example shows the usage of the attribute, which is taken from the identification rule for the **sap_system** CI type:

```
<validation-criterion priority="2">
  <connected-ci-condition ciType="sap_app_server" linkType="membership"
  isTopologyRequired="true"conditionType="approveAndContradict">
    <overlap-fixed-operator number-of-matches="1"/>
  </connected-ci-condition>
</validation-criterion>
```

Installation Notes

HP Universal CMDB and Configuration Manager 10.11 CUP6 Files/Components

HP UCMDB 10.11 CUP6 is packaged in one ZIP file.

The **UCMDB_00167.zip** (for Windows) includes the following files/components:

- **HPUCMDB_Server_10.11.CUP6.exe.** The installation of the version 10.11 CUP6 HP UCMDB Server and Data Flow Probe for Windows.
- **HPCM_10.11.CUP6.exe.** The installation of version 10.11 CUP6 HP UCMDB Configuration Manager for Windows.
- **ReleaseNotes.pdf** (this file)

The **UCMDB_00168.zip** (for Linux) includes the following files/components:

- **HPUCMDB_Server_10.11.CUP6.bin.** The installation of the version 10.11 CUP6 HP UCMDB Server and Data Flow Probe for the Linux platform.
- **HPCM_10.11.CUP6.bin.** The installation of version 10.11 CUP6 HP UCMDB Configuration Manager for the Linux platform.
- **ReleaseNotes.pdf** (this file)

System Requirements

For a list of system requirements, see the **HP UCMDB Support Matrix** PDF file. Check the most previous Release Notes for any additions or changes to the matrix.

Note: If you are using an Oracle version that is prior to 10.2.0.5, you must apply the Oracle patch that fixes Oracle defect # 5866410. For details, go to the Oracle website and find the information regarding this defect number.

Note: HP provides the following recommendations for increasing the security of your overall infrastructure for informational purposes only. These are only recommendations and are not intended to be a guarantee of protection against all potential vulnerabilities and attacks. Please note that some security measures may impact the features and functionality of your overall system; so, it is recommended that every customer become aware of those impacts when implementing any changes to your environment.

Use of this HP Software Product [UCMDB CUP] may require the pre-installation of certain third-party components that are not provided by HP ("Third Party Components"). HP recommends that its customers check frequently for the most current updates to the Third Party Components, which may include fixes or patches for security vulnerabilities.

Install 10.11 CUP6 on the HP Universal CMDB and Configuration Manager Servers

CUP Installation for both HP Universal CMDB and Configuration Manager is performed through an automated procedure using the installation wizard.

You can still install the Data Flow Probes separately by upgrading the Data Flow Probes using the UCMDB user interface. For details, see "[HP Universal CMDB 10.11 CUP6 Manual Data Flow Probe Installation](#)" on [page 13](#).

Note:

- HP UCMDB 10.11 CUP6 can be installed only on top of an HP Universal CMDB version 10.11.
- HP UCMDB CM 10.11 CUP6 can be installed only on top of HP UCMDB CM 10.11.
- The UCMDB CUP version and the CM CUP version must be the same.

Pre-requisites - UCMDB Server and Data Flow Probes

1. Extract **UCMDB_00167.zip** (for Windows) or **UCMDB_00168.zip** (for Linux) to a temporary directory.
2. Stop the HP Universal CMDB 10.11 server and the HP Universal CMDB Integration Service (if running) before starting the 10.11 CUP6 installation.

Note: If you have a High Availability configuration, the CUP must be installed on all the servers in the cluster, and prior to installation, you must stop all the servers in the cluster.

3. If you have received private patches for the Data Flow Probe, you must delete them before performing the upgrade. These steps for deleting a private patch must be followed whether you are upgrading the probes during the installation wizard, or if you upgrading the probes using the UCMDB user interface after installation is complete.
 - a. Stop the Data Flow Probe.
 - b. Delete all private patches that were installed on the system prior to this CUP by deleting the following directory:

\\hp\UCMDB\DataFlowProbe\classes directory

- c. Start up the version 10.11 Data Flow Probe.

CUP Installation

You must first install the UCMDB CUP, start up the server, and then perform the Configuration Manager (CM) CUP installation.

1. For UCMDB: Double-click the file **HPUCMDB_Server_10.11.CUP6.exe** (for Windows) or **sh HPUCMDB_Server_10.11.CUP6.bin** (for Linux) to open the HP Universal CMDB Server CUP Installation Wizard.

For Configuration Manager: Double click the file **HPCM_10.11.CUP6.exe** (for Windows) or **sh HPCM_10.11.CUP6.bin** (for Linux) to open the HP Universal CMDB Configuration Manager CUP Installation Wizard.

2. While running the wizard:
 - In the Choose Install Folder screen, select the installation directory in which UCMDB/CM is already installed.
 - For UCMDB, in the Install Data Flow Probe CUP screen, select the following option:
 - **Automatically update Data Flow Probe with the new CUP version** to automatically update during this installation all the Data Flow Probes reporting to this UCMDB.
 - **Update the Data Flow Probe manually** to update the Data Flow Probes reporting to this UCMDB using the UCMDB user interface after completing the installation of this CUP on the UCMDB server. For details, see "[HP Universal CMDB 10.11 CUP6 Manual Data Flow Probe Installation](#)" on the next page.
 - In the Required Actions screen, follow the instruction to ensure that the server is down.
3. Once the installation wizard for UCMDB is completed, start up the version 10.11 server per the instructions in the Deployment Guide for version 10.11. Go back to step 1 to install the CM CUP.

Once the CM CUP installation is completed, start up Configuration Manager version 10.11 per the instructions in the Deployment Guide for version 10.11.

HP Universal CMDB 10.11 CUP6 Manual Data Flow Probe Installation

Linux: Always required.

Windows: Applicable only when **Update the Data Flow Probes manually** is selected in the CUP installation wizard.

To install the Data Flow Probe CUP upgrade using the UCMDB user interface, follow these steps.

Note: All Data Flow Probes that are associated with the UCMDB are upgraded.

1. If you have received private patches for the Data Flow Probe, perform the steps in the section ["Pre-requisites - UCMDB Server and Data Flow Probes"](#) on page 11.
2. In UCMDB, go to **Data Flow Management > Data Flow Probe Setup**, and click **Deploy Probe Upgrade**.
3. In the Deploy Probe Upgrade dialog box, navigate to the **<SERVER_HOME>\content\probe_patch\probe-patch-10.11.CUP6-windows/linux.zip** and click **OK**.
4. **Linux only:**
 - a. Stop the Data Flow Probe.
 - b. Extract the upgrade package by running the following file:

```
/opt/hp/UCMDB/DataFlowProbe/tools/upgrade/extractUpgradePackage.sh
```
 - c. Restart the Data Flow Probe.

HP Universal CMDB and CM 10.11 CUP6 Uninstall Procedure

When performing the uninstall procedure, this procedure must be performed for both the UCMDB Server and the Data Flow probes, as well as Configuration Manager.

1. Stop the HP Universal CMDB and Configuration Manager servers, and all running Data Flow Probes before uninstalling the version CUP.

2. For UCMDB:

- Windows: Go to **<CMDB installation folder>\UninstallerCup** and double-click **Uninstall HP Universal CMDB Server CUP**. After the CUP is successfully uninstalled, go to **<CMDB installation folder>\runtime** and delete the **jsp** and **jetty-cache** folders.
- Linux: Go to **<CMDB installation folder>/UninstallerCup** and run **Uninstall HP Universal CMDB Server CUP**. After the CUP is successfully uninstalled, go to **<CMDB installation folder>/runtime** and delete the **jsp** and **jetty-cache** folders.

Note: The uninstaller verifies the status of the UCMDB settings and if any settings are marked sensitive and encrypted (as part of the sensitive settings work), it pops out a warning message asking you to follow the instructions in the UCMDB document to roll back all sensitive settings.

If you see such a warning message, manually decrypt those encrypted settings by invoking the **markSettingAsNonsensitive** JMX method before proceeding with the uninstall procedure.

Only proceed with the uninstall procedure when the result returned by the **listSensitiveSettings** JMX method is empty.

For detailed instructions, see ["How to Mark Sensitive Settings and Enable Storing Encrypted Data in the Database Using JMX"](#) on page 57.

Before proceeding with the uninstaller, make sure the master key is restored to default in case you have changed the master key for the cluster. For instructions, see ["How to Set Master Keys"](#) on page 63.

3. For Configuration Manager:

- Windows: Go to **Start** menu > **Programs** > **HP Universal CMDB Configuration Manager 10.11** and double click **Uninstall HP Universal CMDB Configuration Manager 10.11 CUP6**.
- Linux: Go to **<CM installation folder>/_sp_installation/** and run **HPCM_10.11_CUP6-Uninstall**.

4. Uninstall all existing Probes as follows:

- a. **Windows:Start > All Programs > HP UCMDB > Uninstall Data Flow Probe.**

Linux:<Probe_Home> > UninstallerData > Run the Uninstall_Discovery_Probe script.

- b. Start the server.
 - c. Undeploy the **probeUpdate** package.
5. Reinstall the Probes with the same configuration, that is, use the same Probe IDs, domain names, and server names as for the previous Probe installations. Remember that the Probe ID is case sensitive.

Note: After performing an upgrade and installing the new Data Flow Probe, all the Discovery jobs that were active before the upgrade are automatically run.

Notes

- When upgrading the Data Flow Probe:
 - In a multi-customer environment, if the Data Flow Probe is not automatically upgraded to the latest CUP version, use the manual upgrade procedure to upgrade the Probe manually. For details on the manual upgrade procedure, see "How to Deploy a Data Flow Probe CUP Manually" in the *HP Universal CMDB Data Flow Management Guide*.
 - The automatic upgrade is not available for Data Flow Probes running on Linux. Use the manual upgrade procedure to upgrade the Probe manually.
 - The Data Flow Probe upgrade is only available for upgrades between CUP versions. When performing an upgrade to a major or minor release, you must reinstall the Probe.
 - When operating the Data Flow Probe Manager and the Data Flow Probe Gateway on separate machines (that is, separate mode), use the manual upgrade procedure to upgrade the Probe manually. For details on the manual upgrade procedure, see "How to Deploy a Data Flow Probe CUP Manually" in the *HP Universal CMDB Data Flow Management Guide*.
- If you encounter an error when installing the CUP under Linux on the **/tmp** directory because the **/tmp** directory is configured not to run executables, set the IATEMPDIR environment variable to a location with sufficient permissions and disk space. The IATEMPDIR variable is recognized by InstallAnywhere.

Known Problems, Limitations, and Workarounds

The following problems and limitations are known to exist in CMS 10.11 CUP1 (or later software, as indicated). The problems are categorized by the affected product area. If a problem has an assigned internal tracking number, that tracking number is provided (in parentheses) at the end of the problem descriptions.

- [Universal CMDB - General](#)
- [Universal CMDB - Platform](#)
- [Universal CMDB - Topology](#)
- [Universal CMDB - UI](#)
- [Configuration Manager](#)
- [Integration](#)
- [Universal Discovery](#)

Universal CMDB - General

PROBLEM: UCMDB server experiences performance degradation after deploying 10.11 CUP3 or CUP4, because all discovery jobs send a full result set to the UCMDB server. (QCCR1H99640)

Workaround: The UCMDB Probe normally caches data. Some CUPs require a database schema change and the cache needs to be cleaned to ensure there are no unexpected issues. The probe will re-build the cache during the next discovery cycle. However since the probe no longer has the prior history, all newly discovered results are sent to the UCMDB Server for reconciliation. This causes the additional load on the server.

If you are concerned about the impact of extra load on the server, you can take one or more of the following actions:

- Inform users to expect a system slowdown
- Schedule the CUP installation on weekend

- Schedule the discovery jobs to run on weekend after the CUP installation
 - Spread out the normal discovery over a longer period of time by adjusting the discovery job schedule
-

PROBLEM: When a CUP is applied, if users modified the **C:\hp\UCMDB\UCMDBServer\bin\wrapper.conf** file previously, the changes will be reverted. (QCCR1H99649)

Workaround: During the CUP installation, a backup copy of the **wrapper.conf** file is stored in the **\UCMDB\UCMDBServer\UninstallerCUP\backup_HP Universal CMDB Server CUP\bin** directory. To restore all custom changes made to the **wrapper.conf** file after the CUP installation, before starting the UCMDB server, place the backup copy back to the **C:\hp\UCMDB\UCMDBServer\bin** folder.

PROBLEM: A probe randomly gets stuck during discovery due to insufficient connections. (QCCR1H99653)

Workaround: To resolve the insufficient connections issue,

1. Stop the concerning probe and the UCMDB_Probe_DB service.
 2. Locate the **max_connections** setting in the **C:\hp\UCMDB\DataFlowProbe\pgsql\data\postgresql.conf** file, and increase its value to **150**.
 3. Locate the **appilog.agent.probe.maxConnection** setting in the **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** file, and increase its value to **40**.
 4. Restart the probe and the UCMDB_Probe_DB service.
-

LIMITATION: 10.11 CUP3 (or later CUP on top of version 10.11) supports CP15. CP15 can be downloaded at <https://hpln.hp.com/node/11274/contentfiles/?dir=22815>.

However, the following adapters in CP15 cannot work with 10.11 CUP3 or a later CUP (they can only work properly with 10.20):

- ASM adapters
- Top-Down Discovery adapters
- AM Generic Adapter
- Service Manager Enhanced Adapter

10.11 CUP3 can work with UDC 0.91. UDC 0.91 can be downloaded at <https://hpln.hp.com/node/11/otherfiles/?dir=15055>.

Workaround: None.

LIMITATION: 10.11 CUP4 or later CUP does not contain the latest MindTerm jar file (**mindterm-4.1.5.jar**).

Workaround: If you want to upgrade your MindTerm from version 4.0beta6 to 4.1.5, go to the following location and download the hotfix: <https://patch-hub.corp.hp.com/crypt-web/protected/viewContent.do?patchId=QCCR1H90627>.

PROBLEM: If the Enrichment rule is active, the calculation is triggered by attribute changes. Then the Enrichment rule will take into consideration only the changed values and constants when concatenating multiple attributes and constants. (QCCR1H97897)

Workaround: To calculate all attributes, make sure that the Enrichment rule is NOT active and use the scheduler to calculate at certain intervals.

PROBLEM: (High Availability environment only) Changes made to Global Settings in HA take effect for all nodes in cluster only after restarting each node. (QCCR1H98141)

Workaround: In order for all changes in Global Settings that require the server's restart to take effect, you must restart all nodes from the cluster (one by one or with the **restartCluster** JMX method).

PROBLEM: Properties of any CI under the CIT **running_software** could not be viewed. This issue is caused by the fact that a certain custom attribute with the default constraint or index cannot be deleted. The issue is reproducible only on MSSQL when a new attribute is deleted. (QCCR1H95512)

Workaround: To delete the problematic attribute from the database, perform the following steps:

1. Stop the UCMDB server.
2. Back up the UCMDB database. Make sure that the database is backed up appropriately and UCMDB starts with the database backup.
3. Run the following scripts to delete the attribute from all tables: **1_script_delete_index.sql** and **2_script_delete_constraint.sql** (See "[Appendixes](#)" on page 54).

The scripts must be run by Database Administrator in CMDB Database. Set the column name or attribute name to be deleted in the scripts (SET @column_name = 'Column Name').

- If the attribute has an index property, first run **1_script_delete_index.sql** and then run **2_script_delete_constraint.sql**.
- If the attribute has no index property, simply run **2_script_delete_constraint.sql**.

Note: These scripts will be useless if the same attribute is defined for more classes (more CI Types). For one CI Type, the attribute can be deleted from all related types (from all the children). If you are not clear which CI Types include the attribute, run the SQL statement that is described in the following step e to verify.

4. Save the output generated on MSSQL in a text file.
5. Run the following SQL statement to check whether any columns are left. Replace the **Column Name** value with your column name or attribute name that you want to delete.

```
use 'CMDB DB NAME'  
  
SELECT  
    df.name constraint_name ,  
    t.name table_name  
FROM sys.default_constraints df  
INNER JOIN sys.tables t ON df.parent_object_id = t.object_id  
INNER JOIN sys.columns c ON df.parent_object_id = c.object_id AND df.parent_  
column_id = c.column_id  
WHERE c.name = 'Column Name'
```

6. Start UCMDB.
7. Run **rebuildModelDBSchemaAndViews** and **rebuildModelViews** from UCMDB JMX Console under **UCMDB:service=DAL services** for the CI type whose attribute is deleted. Check for any errors in dal logs.
8. Check the CI properties from IT Universe Manager.

Note: This issue also occurs when certain custom attributes are deleted. A permanent fix will be available in the next UCMDB version (QCCR1H91560).

Universal CMDB - Platform

PROBLEM: (UCMDB 10.11 CUP3 or earlier) The Writer server becomes unresponsive which schedules a restart of the entire HA infrastructure. This impacts the load balancing URL, causing all probes to disconnect. This is caused by the existing Garbage Collector algorithm used in UCMDB. (QCCR1H100145)

Workaround: The problem can be resolved by improving the performance of the Garbage Collector by using G1 algorithm for the Garbage Collector. For enterprise environments where you have more than

16 GB of RAM allocated just for UCMDB (see the **wrapper.java.maxmemory** property value in the **..\UCMDB\UCMDBServer\bin\wrapper-platform.conf** file), check and make sure you add the following settings to the **wrapper-custom.conf** file if they are not present:

```
#Enable the following parameters for JVM G1 garbage collector in enterprise environments
wrapper.java.additional.54=-XX:+ParallelRefProcEnabled
wrapper.java.additional.55=-XX:G1HeapRegionSize=32
wrapper.java.additional.56=-XX:InitiatingHeapOccupancyPercent=70
```

Universal CMDB - Topology

PROBLEM: The priority for TQL queries under the pattern-based model are changed from medium on UCMDB 9.05 to inactive on UCMDB 10.xx. The performance may be affected if the TQL queries under the pattern-based model are set to low or medium priority on UCMDB 10.xx. In this case, you can see that the locked gates and calculation for scheduled pattern-based model can take a couple of hours. (QCCR1H95041)

Workaround: None.

PROBLEM: The View result in **Browse Views** is not consistent with the result in the **Modeling Studio**, when creating a New Pattern View with the attribute condition **NOT Node Is Virtual Equal "True"**. (QCCR1H100696).

Workaround: To avoid this issue, create a New Pattern View and define the following attribute conditions in the **Query Node Properties** window: **Node Is Virtual Equal "False" AND Node Is Virtual Is null**.

Universal CMDB - UI

PROBLEM: InfrastructureService models are working with the following types of custom key attributes used for identification (without the **Name** attribute): boolean, date number, double number, float number, integer, list of integers, list of strings, long number, string.

However, the following types of attributes are not supported: bytes, xml, some custom lists (such as lists of dates).

Workaround: None.

PROBLEM: When a TQL is used by both a pattern-based model (PBM) and a view, the PBM becomes inconsistent with the TQL if the TQL is updated from the view. This issue is caused by the fact that Package Manager Resource Selector becomes inaccessible while a new package is being created or an existing package is open. The following error message is displayed in the logs:

"Caused by: java.lang.IllegalStateException: EnrichmentBusinessViewDefinition *ModelName* is not synchronized with its pattern. Element number 12 does not exist in pattern graph."

ModelName and 12 in the error message could be different values. (QCCR1H95551)

Workaround: Pattern-based models must be created or edited only from the model instead of from the TQL. The same TQL cannot be used both by the model and the view.

To fix a corrupted PBM, use one of the following two ways:

- Delete the model and then recreate it
 - a. Log in to UCMDB JMX Console and URM Services.
 - b. Run method **listResources** for Resources of type: **Topology_ENRICHMENT_BUSINESS_VIEW**.
 - c. Locate the EnrichmentBusinessView that is mentioned in the error message and delete it. Then the model is deleted.
 - d. Recreate the model from Modeling Studio using the same TQL.
- Edit the unsynchronized resources of the problematic model
 - a. Log in to UCMDB JMX Console and URM Services.
 - b. Run method **listResources** for Resources of type: **Topology_ENRICHMENT_BUSINESS_VIEW** and **Topology_TQL**.
 - c. Retrieve the xml definition of the **Topology_ENRICHMENT_BUSINESS_VIEW** and **Topology_TQL** of the problematic model.
 - d. Open the EnrichmentBusinessView and locate the ID that is mentioned in the error message.

```
<CmdbProperty>
  <Key>nodeNumberEnd2</Key>
  <Type>integer</Type>
  <Value>12</Value>
</CmdbProperty>
```

- e. Do one of the following:

- Change the missing ID in the `EnrichmentBusinessView` with an existing one from the **Topology_TQL** definition and save the resource.
- Add the missing ID in the **Topology_TQL** definition by replacing an existing one and then save the resource.

Here is an example:

```
<tql:node class="node" name="Node" id="19">
  <tql:where>
    <tql:data-stores>
      <tql:data-store>UCMDB</tql:data-store>
    </tql:data-stores>
  </tql:where>
</tql:node>
```

If you do not have id 12 in the tql, you can change it in the following way:

```
<tql:node class="node" name="Node" id="12">
```

PROBLEM: Before the installation of 10.11 CUP2 (fixed QCCR1H92519), a CIT may have gotten corrupted and no instances of it could be created. This issue is caused by newly-created classes that contain attribute qualifiers on **root_iconproperties**. The following error message is displayed in the log:

"[ErrorCode [404] Attribute [{0}] contains calculated attribute qualifier without items in it.{root_iconproperties}]. Attribute [root_iconproperties] contains calculated attribute qualifier without items in it."

Workaround: After installing this CUP, this issue no longer happens. But if a CIT is corrupted, it must be manually edited in the XML. To do so,

1. Export all class models using `jmx exportClassModelToXml` from Class Model Services.
2. Locate the `<Attribute-Qualifier name="CALCULATED_ATTRIBUTE" is-factory="false" />` line in the **root_iconproperties Attribute-Override** section as follows.

```
<Attribute-Override is-partially-override="true" name="root_iconproperties"
is-factory="true">
  <Attribute-Qualifiers>
    <Attribute-Qualifier name="APPLICATIVE_ATTRIBUTE" is-factory="true"
origin="basic-deployment" version="10" />
    <Attribute-Qualifier name="CALCULATED_ATTRIBUTE" is-factory="false" />
```

3. Note down the CITs whose definitions contain the above problematic line.

4. Log in to the UCMDB UI and go to **Modeling > CI Type Manager**.
 5. Locate the CITs that you noted down and export them to XML.
 6. Open the XML file and delete the **<Attribute-Qualifier name="CALCULATED_ATTRIBUTE" is-factory="false"/>** line.
 7. Save the resource and restart the server.
-

Configuration Manager

LIMITATION: JMX remote access on Configuration Manager is not secure enough. (QCCR1H98135)

Workaround: To secure the JMX remote access on Configuration Manager, do the following on the Configuration Manager machine:

1. Stop the Windows CM service.
 2. Open a command prompt console as an Administrator.
 3. Navigate to the **<CM_Install_Home>\tomcat\bin** folder.
 4. Run the following command:

```
tomcat7w.exe //ES//HPUCMDBCM1010server0
```
 5. In the window that pops up, go to the **Java** tab and locate the **Java Options** textbox.
 6. In this textbox, remove the following three entries that refer to jmxremote:

```
-Dcom.sun.management.jmxremote.authenticate=false  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.port=39600
```
 7. Click **OK**.
 8. Start the Windows Configuration Manager service.
-

Integrations


PROBLEM: Reconciliation causes BSM EUM model problems.

Workaround: After installing the CUP, manually redeploy the UCMDDB 9.x integration adapter package located in the **C:\hp\UCMDDB\UCMDDBServer\content\adapters** directory. (QCCR1H96944)

If the package is not redeployed, the integration adapter still works, but the reconciliation issue fixed in QCCR1H92320 will re-occur.

LIMITATION: You cannot create one integration point for both data push and population. (QCCR1H97157)

Workaround: To create an integration point for both data push and population, do the following:

1. Update the value for **Object Root** from **managed_object** to **root**.
 - a. Log in to UCMDDB with an administrator account and go to **Administration > Infrastructure Settings Manager**.
 - b. From the **Filter by column** drop-down list, click **Name**, type **Object Root** in the text box and double-click the **Object Root** entry that is displayed.
 - c. In the Properties dialog box, go to the **Current Value** field, change **managed_object** to **root**, and then click **Save**.
 - d. Log out of UCMDDB and log in to UCMDDB again for the change to take effect.
2. Add the **discoverypattern_mdr_type** attribute to **Auto Discovery Pattern definition**.
 - a. Go to **Modeling > CI Type Manager > CI Types** pane > **Root** tree > **Data > Object > Configuration**, and click **Auto Discovery Pattern definition**.
 - b. In the right pane, click the **Attributes** tab and click the **Add**  button.
 - c. In the Add Attribute dialog box, type **discoverypattern_mdr_type** in the **Attribute Name** and **Display Name** fields, and click **OK**.
3. If you already create an integration point, delete it and create it again.
4. Open Adapter Source Editor and save.
 - a. Go to **Data Flow Management > Adapter Management > Resources** pane, select the adapter that is related to your integration point.

- b. Right-click the adapter, select **Edit adapter source**.
- c. In the Adapter Source Editor dialog box, click **Save**.

PROBLEM: When you create an NNMI integration point in the CP13 environment, and then upgrade CP13 to CP15, an error is returned while running the integration job. (QCCR1H98191)

Workaround: To fix this issue, you must recreate the NNMI integration point in the CP15 environment.

PROBLEM: The integration between UCMDDB 10.01 and OMi 10 does not work. This issue is caused by the OMi's and UCMDDB's tenant name mismatch. (QCCR1H101056)

Workaround: To solve this issue, OMi must use the same default tenant name as UCMDDB. To change the default tenant in OMi, perform the following steps:

1. Add a new tenant named **System Default Tenant** (go to the RTSM's JMX Console > **Tenant Management Services** > **addTenant** method)
2. Set the newly created tenant (**System Default Tenant**) as default (in the RTSM's JMX console > **Tenant Management Services** > **setTenantAsDefault** method)
3. Delete the old tenant (**DEFAULT_TENANT**) (in the RTSM's JMX console > **Tenant Management Services** > **deleteTenant** method)

To avoid the re-occurrence of this issue in the future, for the new OMi releases, rename the default tenant from **DEFAULT_TENANT** to **System Default Tenant**. This will ensure OOTB interoperability with UCMDDB.

Universal Discovery

LIMITATION: When probes are in Separate Mode, connecting to the UCMDDB server may fail after changing the default credential for basic authentication.

Workaround: You need to update the default credentials for basic authentication manually. To do so,

1. Open the JMX Console of the UCMDDB Server side, enter **changeBasicAuthenticationCredential** in the quick search field and click the link that appears.

- Specify the **userName** and **password** that you want. For example:

changeBasicAuthenticationCredential

Change basic authentication credential.

Name	Type	Value	Description
customerId	int	<input type="text" value="1"/>	Customer Id
userName	java.lang.String	<input type="text" value="test"/>	new user name for basic authentication.
password	java.lang.String	<input type="text" value="123456"/>	new password for basic authentication.

Invoke

Note: Password must contain at least six characters.

- Click **Invoke**.
- Encrypt the password by using the JMX Console of the probe side as follows:
 - Open the JMX Console of the probe side, enter **getEncryptedKeyPassword** in the quick search field and click the link that appears.
 - Enter the password that you specified.

getEncryptedKeyPassword

Encrypt a password for use with Keystore/Truststore properties file

Name	Type	Value	Description
Key Password	java.lang.String	<input type="text" value="123456"/>	

Invoke

- Click **Invoke** and then the encrypted password is generated.
- Copy the encrypted password.
 - Edit the **DataFlowProbe.properties** file as follows:

```
appilog.agent.Probe.BasicAuth.User = <the user name that you specified>  
appilog.agent.Probe.BasicAuth.Pwd = <the encrypted password that you just  
copied>
```

7. Save the change and then restart the probe.

PROBLEM: When the **appilog.collectors.storeDomainScopeDocument** property in the **<UCMDB_HOME>\DataFlowProbe\conf\DataFlowProbe.properties** file is set to **false**, jobs which run in the remote process mode may fail, because the remote process cannot read the probe memory, thus having no access to the **domainScopeDocument** file stored in the memory. When the setting is false, the file is only stored in the probe memory. (QCCR1H93459, QCCR1H96126)

Workaround: If some jobs run in the remote process mode, make sure that you set the value of the **appilog.collectors.storeDomainScopeDocument** property in the **DataFlowProbe.properties** file to **true**.

LIMITATION: When using PostgreSQL as your database on the Windows platform, the UCMDB_Probe_DB service is not starting as a non-system user. This is a third-party product limitation, because PostgreSQL is able to "irrevocably give up administrative rights at startup". For details, see [this PostgreSQL wiki page](#). (QCCR1H96208)

Workaround: In order for the UCMDB_Probe_DB service to start properly, you may configure the **Log On** options for the UCMDB_Probe_DB service as follows:

1. Locate the **UCMDB_Probe_DB** service in the Services window.
2. Right-click **UCMDB_Probe_DB** and select **Properties**.
3. In the UCMDB_Probe_DB Properties window, go to the **Log On** tab, and do either of the following:
 - Select the **Local System account** option.

Note: This is the recommended option, because the SYSTEM account can access all necessary folders according to the default settings on Windows.

- Select **This account**, and specify the account name and password.

Note: This option is NOT recommended. Even if you specify an administrator account, it will be treated as a common user account by PostgreSQL, because PostgreSQL is able to "irrevocably give up administrative rights at startup".

If you really need to specify a different account, make sure that the USERS group on your Windows platform has:

- **Read** and **Write** access to the **C:/hp/UCMDB/DataFlowProbe/pgsql** folder.
- **Read** access to the files in system library (for example, the **C:/Windows/System32** folder) that PostgreSQL needs to access.

For the list of files that PostgreSQL needs to access, see PostgreSQL documentation.

4. Click **OK**.

PROBLEM: After deleting some customized protocols, adding or editing credentials or ranges may fail with the "Can not find class protocol" error. (QCCR1H96595)

Workaround: Before you add or edit credentials or ranges, do the following:

1. Re-add the deleted protocol.
2. Go to **Data Flow Management > Data Flow Probe Setup > Domains and Probes** pane > **Domains and Probes** root node > a domain > **Credentials**, locate the protocol that you just re-added.
3. Delete all credentials under this protocol, and click **OK** to save the change.
4. Delete the customized protocol again.

PROBLEM: No password is required when running **clearprobedata.bat** to clear the data on the Data Flow Probe. (QCCR1H93320)

Workaround: None.

PROBLEM: The **WebSphere to Web Server Dependency** job is causing `OutOfMemoryError` on the probe side. (QCCR1H97711)

Workaround: The probe requires at least 4G memory to run the **WebSphere to Web Server Dependency** job. Therefore, allocate at least 4G memory for the probe.

PROBLEM: Data Flow Probes cannot be upgraded to the latest CUP successfully on the Linux platform. (QCCR1H102387)

Workaround: To resolve the issue,

1. Copy **/opt/hp/UCMDB/UCMDBServer/content/probe_patch/probe-patch-`<version>`-linux.zip** (for example, **probe-patch-10.11.CUP6-linux.zip**) to the following folder:

/opt/hp/UCMDB/DataFlowProbe/runtime/upgrade

2. Extract the upgrade package by running the following file:

/opt/hp/UCMDB/DataFlowProbe/tools/upgrade/extractUpgradePackage.sh

3. Restart the Data Flow Probe.
-

Enhancements Requests

Enhancements Requests in 10.11 CUP6

Here is a list of the enhancement requests that were implemented in the CUP6 release.

Global ID	Problem	Solution
QCCR1H99728	In the High Availability (HA) environment, the reader server cannot be logged in to if the writer server is busy.	You can now log in to the reader server even if the writer is blocked.
QCCR1H101710	Currently it is hard to reproduce complex reconciliation issues. It will help greatly if we can record the exact bulk and CMDB data that is being processed and reproduce the issue on any environment.	Implemented the enhancement by adding a new property reconciliation.dump.bulks to the setSettingValue JMX method in the UCMDB:service=Settings Services category. By setting the reconciliation.dump.bulks property to true , you can dump CMDB and bulk containers to files in the <UCMDB_Server_Home>\runtime\log\bulkDumps directory.

Enhancements Requests in 10.11 CUP5

Here is a list of the enhancement requests that were implemented in the CUP5 release.

Global ID	Problem	Solution
QCCR1H83305	Invoking the full reindex method in the JMX console takes hours.	Implemented an enhancement by adding a new JMX method reindexCiType in UCMDB:service=Topology Search Services . This method selects a subset of data in a short time.
QCCR1H90820	Package manager should take resource dependencies into account when creating packages.	Enhanced the Create Custom Package Wizard by adding the Automatically export dependencies of the checked resources check box to the Resource Selection page of the wizard. Selecting this check box allows you to automatically export dependencies of the checked resources when creating a package.
QCCR1H91311	UCMDB Browser returns undesired results after conducting a search related to a specific time period.	Implemented an enhancement so that the search results are filtered based on finding and ignoring query matches.
QCCR1H95577	Users request to remove the “[]” characters from the Concatenated List column in reports.	Implemented an enhancement so that the “[]” characters are no longer added automatically to the string representation of a Java ArrayList object. Now the Concatenated List column in reports does not contain the “[]” characters.
QCCR1H96022	Users request to improve the troubleshooting of the discovery.	Added a new permission to allow users to view the discovery status and errors.
QCCR1H98825 QCCR1H98833 QCCR1H98834	Users request for a server health check dashboard.	Implemented server health check enhancements. For details, see "Enhancements implemented to server health check " on page 6.
QCCR1H98835	The Jetty monitoring mechanism should be enhanced so that each UCMDB instance checks whether Jetty is accessible. When the Jetty Server is stuck, the UCMDB server cluster should respond	Enhanced the Jetty monitoring mechanism so that each UCMDB instance checks whether Jetty is accessible. The writer will not update its timestamp if the Jetty Server is not responding. The UCMDB instance only updates its timestamp in the High Availability environment if Jetty is accessible to new connections.

Global ID	Problem	Solution
	accordingly.	In case Jetty is stuck, this will force another UCMDDB to become a writer.
QCCR1H98837	Push back of global IDs works for population flows, but not for push flows.	Push back of global IDs for push flows is now working, with similar behavior like that for population flows.
QCCR1H99006	More logs are needed to debug adapter states.	Added more logs on the debug level for Push engine states.
QCCR1H99103	When using Integration Adapter 10.x, the Push creates CIs in a wrong Tenant because the tenant information is not pushed because of the integration user's default tenant assignment.	Improved the design of the tenant assignment. Now tenant information is also pushed to the other UCMDDB.
QCCR1H99448	The Is Candidate for Deletion status can be synchronized with the population flow. Integration users request for the same capability for the Push flow.	Implemented an enhancement so that the Is Candidate for Deletion status can be synchronized with the Push flow as well.
QCCR1H99600	A JMX method is needed to deactivate all the TQLs that are related to views.	Added a new JMX method deactivateAllViewsTqls in UCMDDB:service=New Views Services to deactivate all the TQLs that are related to views.

Enhancements Requests in 10.11 CUP4

Here is a list of the enhancement requests that were implemented in the CUP4 release.

Global ID	Problem	Solution
QCCR1H98666	Pattern Based Models (PBMs) that are created based on existing Instance Base Models (IBMs) in an environment (for example,	Enhanced the Package Manager to provide the capability of exporting all the resources of a Pattern Based Model that is created based on an Instance Base Model, including the business enrichment, TQL, and model CI. Now Pattern Based Models that are

Global ID	Problem	Solution
	development) are not available in the Package Manager for exporting to other environments.	created based on existing Instance Based Models are available in the Package Manager for selection when exporting a package.

Fixed Defects

Fixed Defects for UCMDB 10.11 CUP6

Here is a list of the defects fixed in the CUP6 release.

Global ID	Problem	Solution
QCCR1H93682	After users sort the CI type by its name or number in the Show Results For Triggered CI dialog box and then double-click a CI type, the original CI type shows in the Discovered CIs dialog box that opens.	After users sort the CI type by its name or number in the Show Results For Triggered CI dialog box and then double-click a CI type, the correct CI type shows in the Discovered CIs dialog box that opens.
QCCR1H99016	When logging in to the UCMDB UI in the authorized state and using the advanced conditional search, the authorized CIs that satisfy the search condition are not found and displayed.	Fixed the issue by applying a code change. Now the advanced CI conditional search works properly.
QCCR1H99244	When configuring HP SIM credential, the integration point has no reference to the credentials being used. The HP SIM Protocol entry has no reference to the HP SIM application server, only to the database.	Fixed the issue by applying a code change. Now the MSSQL_NTLMV2 type connection is available when configuring HP SIM credential. Note: This fix requires CP15 Update 3 to work.
QCCR1H99439	When the Changed CIs filter is on, some changes that are related to CIs	Fixed the issue by applying a code change. When the Changed CIs filter is on, all CI

Global ID	Problem	Solution
	are not displayed.	changes appear.
QCCR1H99647	Information on the verification or validation criterion results is not present in the logs.	Implemented logging for showing the result of each verification and validation criterion. However, you need to set the cmdb.reconciliation.datain.multiplematch log to the TRACE level in order to enable this implementation.
QCCR1H99918	The integration between Service Manager and UCMDB that is based upon Connect-IT creates CIs of the Infrastructure Element CI type with the qualifier Abstract Class . This means that no CIs of this type may be created. This results in errors with the UCMDB to BSM integration.	Fixed the issue by applying a code change, so that no update type change is allowed when Abstract Class is the type to update to.
QCCR1H99940 QCCR1H100476	In certain circumstances, database deadlock occurs in log files when multiple threads try to update records in different orders.	Fixed the issue by using row locks so that no deadlock occurs.
QCCR1H100343	No email is received even if a Scheduler job was created with success for the Compare Archives Report, the Compare CIs Report, or the Compare Snapshot Report. This was caused by an older version of the UI apache.poi jar file.	Fixed the issue by upgrading the UI apache.poi jar to a later version.
QCCR1H100531	There are many triggers that are stuck in the PARKING state for a long time.	Added one new column Last invocation to indicate the job execution status. The original column shows the workflow status.
QCCR1H100629	Currently the documentation lacks full re-index required steps.	Added documentation about how to perform a full re-index of all CIs. For details, see "How to Perform a Full Reindex of All CIs" on page 56 .
QCCR1H100791	After UCMDB CUP5 is deployed, the	Fixed the issue by applying a code change

Global ID	Problem	Solution
	out-of-the-box XML PushAdapter export crashes. Integration crashes with the NullPointerException error.	so that null value check will be performed to avoid NullPointerException.
QCCR1H100800	Data Flow Probe connects to the UCMDB server using the close HTTP connections.	Data Flow Probe connects to the UCMDB server using the keep-alive HTTP connections and the number of connections can be controlled.
QCCR1H100808	When running the Migrate DDMI Agent job to upgrade some DDMI agents to UD, the communication log says that is a successful connection; however, no CI is created for performing Inventory Discovery.	Fixed the issue by applying a code change. When the probe detects the node that is a dummy node and out-of-scope, the probe will not add the license tag to it.
QCCR1H100919	The Authorized state of Customer ID 100001 appears with the failed status on the UCMDB server's status page. The ping_url is down, causing no probes to connect to the writer. This issue is reproducible when multiple states are present in UCMDB.	Fixed the issue by applying a code change. Now the UCMDB server is started without failure.
QCCR1H100940	<p>Universal Discovery Control Panel is not opening. There is no error in the UI. Nothing happens when users try to open it. Only the NullPointerException is found in the client logs.</p> <p>The root cause is that when initializing the Universal Discovery Control Panel, all activities and their data (for example, templates being used) need to be loaded. If users happen to delete a template that is being used by some activities, NullPointerException will be raised during the control panel initialization.</p>	Now if a template is deleted by users accidentally, activities that are created with this template are corrupted. When loading the control panel, activities are checked, and missing templates are handled, so the control panel still works, and users will see a warning message when accessing a corrupted activity.

Global ID	Problem	Solution
QCCR1H100980	<p>Some jobs are scheduled to send reports in Excel format via email to a few users. The SMTP server setting seems okay but there is always an error with one of the scheduled jobs: <code>javax.mail.MessagingException: SMTP server host is empty.</code></p> <p>It turns out that the Alternate SMTP server setting was left empty. If sending the email with the SMTP server fails, the Alternate SMTP server setting will be used.</p>	<p>The following note should be added to the <i>How to Configure the UCMDB Mail Server</i> section in the <i>HP Universal CMDB Administration Guide</i> to indicate that why the Alternate SMTP server and Alternate SMTP server port fields should not be left empty:</p> <div data-bbox="889 594 1370 890" style="background-color: #f0f0f0; padding: 10px;"> <p>Note: It is recommended to set both the SMTP server and alternate SMTP server. In case the SMTP server is not available, an alternative SMTP server will be used by the UCMDB server when sending emails.</p> </div>
QCCR1H101120	<p>The following error message is returned by the Oracle Database by SQL job: "Failed to collect data from Oracle server".</p>	<p>Fixed the issue by applying a code change. Now the Oracle Database by SQL job works properly.</p>
QCCR1H101223	<p>The Data Flow Probe status appears disconnected (stopped) in the UCMDB UI for a long time. However, the Probe service is up, and the Probe is reporting data and connecting to UCMDB.</p>	<p>Now UCMDB sets the Data Flow Probe status correctly.</p>
QCCR1H101252	<p>The UCMDB servers experiences the performance issue. The UCMDB GUI becomes unresponsive from time to time.</p>	<p>Fixed the issue by increasing the default value for jetty.maxThreads to 300.</p>
QCCR1H101581	<p>Universal Discovery 10.20 sets incorrect values in the hwHostOS field for HP-UX by including hwOSHostHPUXType into the value.</p>	<p>Fixed the issue by removing the inclusion of hwOSHostHPUXType in the hwHostOS field.</p> <div data-bbox="889 1675 1370 1801" style="background-color: #f0f0f0; padding: 10px;"> <p>Note: This fix requires CP15 Update 3 to work.</p> </div>
QCCR1H101843	<p>The corrupted CALCULATED_</p>	<p>Fixed the issue by applying a code change.</p>

Global ID	Problem	Solution
	ATTRIBUTE line in the class definition prevents the CI type icon change.	Now the CALCULATED_ATTRIBUTE qualifier is added when creating a new CIT.
QCCR1H102018	The displayName attribute is not updated if this setting is selected to be used for LDAP users.	The LDAP display name is now used and updated for users.
QCCR1H102098	The UCMDB Integration Service cannot be started due to "connection failure to the database" if users have changed the master key on the UCMDB server side.	Fixed the issue by applying a code change. Now UCMDB Integration Service can load the updated master key properly so that it can connect to the database.
QCCR8D38423	When loading factory contents into RTSM at the first startup, some packages fails to be loaded, with the result of some missing content.	Fixed the issue by changing the order in which the deployers are run. Packages can be deployed without errors now.
QCCR1H102081	Encryption for Oracle ASO does not work.	Fixed the issue by adding the following lines in the sqlnet.ora file: SQLNET.ENCRYPTION_SERVER = required SQLNET.CRYPTO_CHECKSUM_SERVER = required This forced the use of encryption on connection between the UCMDB server and database.

Fixed Defects for UCMDB 10.11 CUP5

Here is a list of the defects fixed in the CUP5 release.

Global ID	Problem	Solution
QCCR1H95545	Data Flow Probe randomly stops, and does not send results back to the server.	Fixed the issue by resolving the deadlock for DB connection, now Data Flow Probe runs discovery successfully.

Global ID	Problem	Solution
QCCR1H95747	The Add Parameter button under Modeling > CI Type Manager >Attached Menu tab > Menu Item Method pane > New Method option is not working in UCMDB 10.11.	Fixed the issue by applying a code change, now the Add Parameter button works properly.
QCCR1H98611	The SCCM population job fails with the "ClassCastException" error.	Fixed the issue by correcting logic to use proper child type, now the SCCM population job runs successfully.
QCCR1H98947	The reader server restarts in the High Availability environment because the writer server sends the revisions in an incorrect order. The log shows the following error message: "Server had to be restarted because of a missing revision."	Fixed the issue by creating an ordered queue to place the revisions in the expected order.
QCCR1H98963	The SSH credential is changed after being saved and reopened in the UCMDB UI.	Fixed the issue by applying a code change. The SSH credentials now can be saved successfully.
QCCR1H99025	When creating a package using the Create Custom Package Wizard , not all Pattern Based Models appear under Resource Selection page > Model tree > Service Models for exporting to other environments, because a simple PBM is translated into a PBM over an Instance-Based Model (IBM) after saving the model.	Fixed the issue by applying a code change. Now all Pattern Based Models can be exported properly.
QCCR1H99152	No documentation about the binary data is found in the communication logs, which causes users to think that the scan files fail to parse the communication logs.	<p>Added the following note to the documentation:</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: CDATA mechanism is used to store information retrieved from user environment in the communication logs. When scan files get some</p> </div>

Global ID	Problem	Solution
		<p>characters or XML segments that cannot be parsed by the CDATA mechanism, the information will be saved in binary format for further troubleshooting purpose. HP Software Support will decode the binary data in the communication logs to perform troubleshooting.</p>
QCCR1H99331	<p>UCMDB to UCMDB Push creates duplicated CIs. Identifier criteria take the calculated ID into consideration when identifying objects. Because global_id is changing during the push, the calculated ID is also changing and it creates duplicated data.</p>	<p>Fixed the issue by adding a special setting reconciliation.calculated.id.attribute to take the calculated ID into consideration. By default, this setting is set to false. If the setting is not present, it is also treated as false by default.</p>
QCCR1H99425	<p>The VMware vCenter Topology by VIM job fails with the following error message: "Failed to connect to remote process: details: Software caused connection abort: socket write error".</p>	<p>Fixed the issue to avoid the socket error when running the VMware vCenter Topology by VIM job.</p>
QCCR1H99559	<p>When adding a CI to a job that is currently stopped by using IT Universe Manager, the probe limit changes to disabled and the job does not start. This is a regression that occurs in the 10.11 CUP3, because this issue does not exist in the 10.11 CUP2.</p>	<p>Fixed the issue by rolling back the change made in 10.11 CUP3. Now CIs can be added to a job that is currently stopped by using IT Universe Manager as in the 10.11 CUP2.</p>
QCCR1H99736	<p>The following error message occurs when the Long type attributes are used in the reconciliation rule: "There is no temp table for cmdb type [CmdbLongType]".</p>	<p>Fixed the issue by applying a code change. Now the Long type attributes can be used in the reconciliation rule.</p>
QCCR1H100030	<p>When discovering Cisco devices by the Host Connection by SNMP job, thousands of the</p>	<p>Fixed the issue by modifying the attribute comparison code to</p>

Global ID	Problem	Solution
	following warning messages are returned: "Normalization rule output conflict for CI {0}" ".	avoid the normalization rule conflict error.
QCCR1H100066	The reader server restarts in the High Availability environment because of the following error on the writer server: "java.util.ConcurrentModificationException".	Fixed the issue by applying a code change. Now the reader server works properly in the High Availability environment.
QCCR1H100132	A very long dispatch queue is seen on the Universal Discovery server and almost no new jobs are scheduled. The dispatch queue should be reduced to zero till new jobs get activated if you restart the server.	Added logs to show the time that is spent on each step of the dispatch for analysis purposes.
QCCR1H100144	The reader server in the High Availability environment restarts because of the JGroups cluster recreation.	Fixed the issue by changing the JGroups configuration.
QCCR1H100146	When deleting the search folder, the reindex method fails with the following error message: "No such core: customer1". This is caused by the solr.xml file being changed twice after server restart, which resulted in creation of two instances of the core container.	Fixed the issue by applying a code change, so that the solr.xml file is created at server startup, instead of being changed twice after server restart.
QCCR1H100269	All Tenant IDs coming from the automatic deletion process are returned as the System Default Tenant although a specific tenant is set on the Data Flow Probe.	Fixed the issue by applying a code change. Now the automatic deletion process sends the proper Tenant ID to the server.
QCCR1H99123	When Solr Search is enabled, the Disruptor keeps growing and reaches a high memory consumption.	Fixed the performance issue by decreasing the size of the Disruptor ring buffer from 16 * 1024 to 1024. Now JVM heap usage is normal.
QCCR1H99154	Long full Garbage Collector shows in wrapper.log and JVM hangs or restart because Solr logging is causing big objects	Fixed the issue by adding a new setting cmdb.search.use.query.syntax.tree to control if syntax

Global ID	Problem	Solution
	on the heap.	tree is logged or not. For more details, see the What's New section.

Fixed Defects for UCMDB 10.11 CUP4

Here is a list of the defects fixed in the CUP4 release.

Global ID	Problem	Solution
QCCR1H95235	After changing the SAP Server icons in CI Type Manager, the changes do not appear in the CI Type tree or anywhere else.	Now SAP Server icons in CI Type Manager can be changed and the changes appear as expected.
QCCR1H95558	After upgrading from 10.01 CUP4 to 10.01 CUP10, discovery probes in non-union mode cannot run discovery jobs.	Now discovery probes in non-union mode can run discovery jobs.
QCCR1H97566	Many triggers for several discovery jobs fail randomly with the "Java.lang.NullPointerException" error.	Fixed the issue by a code change so that discovery jobs can successfully run.
QCCR1H97715	The Server database returns the time-out error when processing the result.	Fixed the issue by modifying the batch chunk from 10000 to 200 so that the chunk can be processed in a short time.
QCCR1H97925	Call Home returned incorrect tenant owner ID for some CIs.	Call Home can return the correct tenant owner ID for CIs.
QCCR1H97950	When using Java API setDiscoveryConfigurationXML to update Probe IP address ranges, all jobs are restarted because setDiscoveryConfigurationXML contains the following parameter that enables or disables all jobs in the group: <pre><DiscoveryGroup</pre>	Fixed the issue by adding a new method void setDiscoveryConfigurationXML (String xmlString, boolean includeGroup) . If you want to update IP address ranges and credentials only, you can use this new method by setting the includeGroup parameter to false . For more details, see the What's New section.

Global ID	Problem	Solution
	<pre data-bbox="428 296 862 411">name="Network"> <IsEnabled>True </IsEnabled></pre>	
QCCR1H98037	The values of normalized fields are not in a user-friendly format.	Fixed the issue by unifying the result content when Data Flow Probe sends the result to UCMDB.
QCCR1H98051	When multiples roles are assigned to a user, the user's permission level is set to the role with the minimum permissions. This is the desired behavior, but it is not explained in full details, thus causing confusion.	<p data-bbox="889 590 1385 663">The HP Universal CMDB Administration Guide is updated as follows:</p> <p data-bbox="889 695 1385 1104">For CIT Menu Items, you select a CIT from the tree and then select specific actions from the Available Actions pane and move them to the Selected Actions pane. You can also right-click a CIT and select the actions from the pop-up dialog box. If no permissions are assigned for any CIT, all the menu items are permitted by default (in accordance with the permissions granted in the General Actions tab).</p> <p data-bbox="889 1136 1385 1209">The following important note is added to clarify the desired behavior:</p> <div data-bbox="894 1230 1370 1839" style="background-color: #f0f0f0; padding: 10px;"> <p data-bbox="911 1262 1354 1829">Note: The above principle remains valid when there are multiple roles with menu items permissions/general actions. Both the menu items permissions and the general actions are accumulated. If there are NO menu items permissions accumulated from all the user's roles, all the menu items are permitted by default (in accordance with the permissions granted by accumulating all the General Actions from all the user's roles). In the opposite way, if there are menu items permissions accumulated</p> </div>

Global ID	Problem	Solution
		<p>from all the user’s roles, they will be taken into account and the UI will enforce them, even in the case when a role with no CIT Menu Items is aggregated with a role with CIT Menu Items.</p>
QCCR1H98095	Browser search stops working because of changes in the snapshot CI type instances.	Browser search works as expected.
QCCR1H98116	The following error message is returned in the management zone: "Failed to initialize CM client (sleep interrupted)".	Now credentials can be fetched from the Confidential Manager Client.
QCCR1H98117	Many unsent results exist on probes.	Fixed the issue by reducing the unsent results on probes.
QCCR1H98290	Custom jobs are stuck with zero working threads, for example, no triggers on one probe are running.	Custom jobs now can run as expected.
QCCR1H98458	The “NullPointerException” error is thrown in processing discovery results.	Fixed the issue to avoid processing null objects.
QCCR1H98485	Identification by key attributes is not working for certain types of attributes (for example, long) when you create an InfrastructureService model.	<p>Now InfrastructureService models are working with the following types of custom key attributes used for identification (without the Name attribute): boolean, date number, double number, float number, integer, list of integers, list of strings, long number, string.</p> <p>However, the following types of attributes are not supported: bytes, xml, some custom lists (such as lists of dates).</p>
QCCR1H98737	When a Full Synchronization is	After a Full Synchronization, a differential

Global ID	Problem	Solution
	completed, running a differential synchronization with NNMi pull integration sends Layer 2 Connection CIs without the required reconciliation information.	synchronization can be run as expected.
QCCR1H99001	After you upgrade to 10.11 CUP3, the Normalization rule does not work.	The Normalization rule works as expected.


Fixed Defects for UCMDB 10.11 CUP3

Here is a list of the defects fixed in the CUP3 release.

Global ID	Summary
QCCR1H88798	Fixed an issue that occurred when global_id was not updated if UCMDB was not configured as a global_id generator.
QCCR1H90278	Added the functionality to re-run a job with commlog enabled.
QCCR1H91007	Fixed an issue that occurred when trying to populate some links from Service Manager to UCMDB and errors were returned.
QCCR1H91923	Fixed an issue that occurred when resources were not updated in UCMDB during the content pack deployment because of double file extensions.
QCCR1H92224	Fixed an issue that occurred when the input parameters for the content validator of a job was not available.
QCCR1H92742	Fixed an issue that occurred when the AM integration failed with an error.
QCCR1H92925	Fixed an issue that occurred when the change report did not work correctly if selecting the LastMonth option as the parameter.
QCCR1H93378	Fixed an issue that occurred when all triggers were added to the job with Probe Limit disabled.
QCCR1H94507	Fixed an issue that occurred when the getProbeFromHost() method did not check whether an IP address was configured in the management zone range before using this IP address's probe name.
QCCR1H94686	Fixed an issue that occurred when editing a service tree failed with the following

Global ID	Summary
	error: "Pattern existing ci tq1 has identical names for its (Node or Link) Elements".
QCCR1H94855	Fixed an issue that occurred when the ORA-01400 and ORA-30926 errors were returned on probe logs.
QCCR1H94956	Fixed an issue that occurred when the probe did not properly run from a restart.
QCCR1H95112	Fixed an issue that occurred when errors were returned by the Viewer on the Windows 2012 probe.
QCCR1H95195	Fixed an issue that occurred when the scheduler in the Integration Studio could not support a long repetition period.
QCCR1H95277	Fixed an issue that occurred when the discovery task took several hours to be dispatched to the probe.
QCCR1H95322	Fixed an issue that occurred when the data was not displayed in the CI Type Manager if a particular CI type had two attributes with the same name.
QCCR1H95544	Fixed an issue that occurred when software that was registered by Package Rules could not be identified in UCMDB.
QCCR1H95599	Fixed an issue that occurred when the external policies results were invisible in Configuration Manager.
QCCR1H95638	Fixed an issue that occurred when UCMDB incorrectly assigned Universal Discovery full licenses to incomplete Node CIs with no operating system that were not in the probe scope.
QCCR1H95665	Fixed an issue that occurred when many "java.lang.NullPointerException" errors occurred in the probe-error.log.
QCCR1H95698	Fixed an issue that occurred when the "java.sql.BatchUpdateException" errors constantly occurred in the probe-error.log.
QCCR1H95813	Fixed an issue that occurred when a relationship could not be individually deleted from the IT Universe Manager.
QCCR1H95852	Fixed an issue that occurred when the "Cannot invoke trigger" error was returned.
QCCR1H95915	Fixed an issue that occurred when UNIX nodes were incorrectly merged.
QCCR1H96037	Fixed an issue that occurred when user.zsai was incorrectly imported into the UCMDB Software Library using Import SAI file .

Global ID	Summary
QCCR1H96176	Fixed an issue that occurred when the scheduler in the Integration Studio could not support Week for the Interval repetition.
QCCR1H96216	Fixed an issue that occurred when UCMDB Server encountered the <code>OutOfMemoryError</code> in Java heap in processing the discovery results of the Host Resources by Shell and Host Applications by Shell jobs.
QCCR1H96241	Fixed an issue that occurred when an error was returned while running loggrabber.bat .
QCCR1H96242	Fixed an issue that occurred when the "java.lang.RuntimeException: Could not find domain" error was returned.
QCCR1H96251	Fixed an issue that occurred when the authorization failed with errors.
QCCR1H96267	Fixed an issue that occurred when the Host Applications by Shell job failed on the UCMDB Server caused by the "java.lang.NullPointerException" error.
QCCR1H96324	Fixed an issue that occurred when the discovery status in the management zone did not update.
QCCR1H96336	<p>Added the capability to control, when LDAP authentication is enabled, whether non-interactive flows are verified against the LDAP Server or not. By default, when LDAP authentication is enabled, all the authentication flows, whether interactive (manual user login) or non-interactive (authentication of integrations, Web Services, API's) are checked in the LDAP repository.</p> <p>A new setting enable.ldap.authentication.in.non.interactive.flow is added to control whether the non-interactive flows should be verified against the LDAP Server or not. By default, it is set on true. When setting to false, the non-interactive flows will be verified only against the local UCMDB user repository.</p>
QCCR1H96349	Fixed an issue that occurred when not all Trigger CIs were dispatched to the probes correctly.
QCCR1H96397	<p>Added the Enable the use of the pfiles command check box to allow you to enable or disable the use of pfiles command in TCP/IP connectivity detection in scanner on the Solaris and HP-UX platforms.</p> <p>To enable the use of pfiles command in TCP/IP connectivity detection on the Solaris or HP-UX platform when you generate scanners,</p> <ol style="list-style-type: none"> 1. Go to Data Flow Management > Adapter Management > Resources >

Global ID	Summary
	<p>InventoryDiscovery > Scanner Configuration Files > <Select a configuration file (.cxz) file>.</p> <ol style="list-style-type: none"> 2. In the right pane, click . 3. In the Scanner Generate (Manual Deployment Mode) dialog box that opens, provide necessary information and go to the Scanner Options page. 4. Go to the Miscellaneous tab, and select the Enable the use of the pfiles command check box for the TCP/IP connectivity options section. By default this setting is not selected.
QCCR1H96504	Fixed an issue that occurred when generating a CI Change report took too much time.
QCCR1H96577	Improved the UCMDB Browser search performance. Folding rules are configurable through a new setting cmdb.search.enriching.use.folding.rules for search enriching.
QCCR1H96626	Improved the UCMDB Browser search performance. Enriching no longer runs for a large amount of CIs.
QCCR1H96659	Improved the return messages for an integration point job that operates on a busy Data Flow Probe.
QCCR1H96660	<p>Fixed an issue that occurred when the push adapter did not check credentials.</p> <p>Note: You must manually redeploy the push adapter.</p>
QCCR1H96685	Fixed an issue that occurred when discovery jobs could not be saved under existing discovery modules after upgrading to 10.11 CUP2.
QCCR1H96688	Fixed an issue that occurred when the Enable aging attribute of CIs that were created by the Import from Excel adapter was true though this attribute was set to false.
QCCR1H96783	Fixed an issue that occurred when the push to DB integration was triggered at each server restart.
QCCR1H96842	Fixed an issue that occurred when the UCMDB to UCMDB push adapter returned an error message.
QCCR1H96845	Fixed an issue that occurred when ExternalImpl threw "NullPointerException" errors

Global ID	Summary
	for attributes of type DATE and BYTES.
QCCR1H96907	Fixed an issue that occurred when the Generic Database Adapter did not automatically delete CIs or links.
QCCR1H96982	<p>Fixed an issue that caused an incorrect merging of the sap_system CIs in rare cases when the associated node could not be identified and inserted into UCMDB.</p> <p>As a result, a new attribute isTopologyRequired is added in the <connected-ci-condition> XML tag of the reconciliation rule of a CI type. For details, see the Notes section.</p>
QCCR1H97031	Fixed the null pointer exception issue that occurred when processing the NNMI integration data.
QCCR1H97099	Fixed an issue that occurred when the Number of Changes report failed on database selection with the following error: "Failed to load report".
QCCR1H97103	Fixed an issue that occurred when about 1000 CIs that were in the results of the trigger query disappeared in the triggered CIs list.
QCCR1H97157	<p>Fixed an issue that occurred when the Management Data Repositories (MDR) licenses were counted by integration points. A new mechanism is provided to allow users to create one integration point for both data push and population.</p> <p>For instructions about creating one integration for both data push and population, see the Notes section.</p> <div data-bbox="428 1285 1370 1415" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: Deployment of the Universal Discovery Content Pack 15.00 is required for this defect fix to work.</p> </div>
QCCR1H97168	Fixed an issue that occurred when the following error was returned: "Can't add to DataContainer because its size larger than the fuse 200000 which defined by reconciliation.internal.data.container.size.fuse".
QCCR1H97197	Fixed an issue that occurred when the "collection error -1(-1)" error occurred in the Analysis Workbench after performing a software teaching and using the "Unload Scan File" function.
QCCR1H97273	Fixed an issue that occurred when new errors were returned after applying the ORA30926_classes.zip hotfix.

Global ID	Summary
QCCR1H97374	Added procedure on how to disable the HTTP TRACE or TRACK methods on the probe.
QCCR1H97512	Fixed an issue that occurred when the UCMDB-NNMi integration failed with reconciliation errors on Non-SNMP nodes.
QCCR1H97779	<p>Fixed an inconsistency issue that occurred at minor upgrade from UCMDB 10.01 to UCMDB 10.1x. The links were not migrated correctly from the ROOT table to the ROOT_LINK table during the minor upgrade procedure.</p> <p>If you plan to upgrade from UCMDB 10.01 to UCMDB 10.1x, it is recommended that you proceed with upgrading directly to UCMDB 10.11 CUP3. That is to say, after UCMDB 10.11 is installed, do NOT start the UCMDB server yet. Only after UCMDB 10.11 CUP3 is applied, start the UCMDB Server, which will then trigger the minor upgrade.</p>
QCCR1H97790	Fixed an issue that occurred when the recognition engine incorrectly reported applications after importing a new user SAI file in the Software Library in UCMDB.
QCCR1H97871	Fixed an issue that occurred when the last use date for the discovered software was incorrect.
QCCR1H97888	Fixed an issue that occurred when the NNMi sync took a long time to insert data into UCMDB.
QCCR1H97904	<p>Fixed an issue that occurred when false restarts of UCMDB writer server happened occasionally.</p> <p>Important: Before starting the UCMDB server, open the \UCMDBServer\bin\wrapper.conf file, locate the following settings and modify their values as indicated below:</p> <pre> wrapper.cpu.timeout=60 wrapper.ping.timeout=320 wrapper.ping.interval=30 wrapper.stop.timeout=320 wrapper.shutdown.timeout=320 wrapper.jvm_exit.timeout=320 </pre>
QCCR1H97941	Fixed an issue that occurred when Infrastructure Service instances could not be created without a name value.

Fixed Defects for UCMDB 10.11 CUP2

Here is a list of the defects fixed in the CUP2 release.

Global ID	Summary
QCCR1C20050	Added support for reporting multiple installations of the same software version.
QCCR1H92474	Fixed an issue that occurred when the MSSQL Server Connection by SQL job failed to discover while using the NTLM authentication.
QCCR1H94134	Fixed an issue that occurred when trigger CIs for jobs under the management zone were in the status of Progress . The UI status of the trigger CI did not update and even continued for several days.
QCCR1H94525	Fixed an issue that occurred when a misleading message indicating that all the CIs were touched was returned when using the touch window.
QCCR1H94615	Fixed an issue that occurred when the Host Applications by shell job reported a node CI without any properties except one IP address.
QCCR1H94693	Fixed an issue that occurred when the upgrade from 9.05 to 10.10 failed because of the missing of the server_side attribute for the adapter_config class.
QCCR1H94792	Added the time value for the date cells in exported Microsoft Excel reports.
QCCR1H94815	Fixed an issue that occurred when the XML Enrichment service could not start on any probes with the timezone of GMT +9:30 because of the incorrect WrapperEnricherLicense.conf.
QCCR1H94832	Fixed an issue that occurred when discovery jobs stopped triggering all available CIs after the upgrade from 10.10 to 10.11.
QCCR1H94901	Fixed an issue that occurred when the Merge Clustered Software job did not properly merge the duplicated database instances that fit the trigger TQL.
QCCR1H95016	Fixed an issue that occurred when the Inventory Discovery by Scanner job did not display the correct trigger count.
QCCR1H95063	Fixed an issue that occurred when the Layer2 Topology Import job from NNMi failed with the following error "ORA-12899: value too large for column "UCMDB10"."DDM_TEMP_MAPPINGS"."TEMPID" (actual: 53, maximum: 43)".
QCCR1H95112	Fixed an issue that occurred when Viewer did not work and errors were returned on Windows 2012 probe.
QCCR1H95146	Fixed an issue that occurred when UCMDDB on postgresql could not modify the CIT attribute size.
QCCR1H95157	Fixed an issue that occurred when the disconnected 9.05 probes from UCMDDB could

Global ID	Summary
	not be removed.
QCCR1H95182	Fixed an issue that occurred when the Package Manager resource selection took a long time to populate on UI.
QCCR1H95201	Fixed an issue that occurred when the custom adapter and script were deleted from Adapter Management > Resources > Packages > <<No Package>> .
QCCR1H95216	Fixed an issue that occurred when a newly-installed probe or LWP could not connect the UCMDB server with basic authentication enabled.
QCCR1H95223	Fixed an issue that occurred when the topology reporting by SiteScope integrated with BSM failed without any alerts.
QCCR1H95264	Added Application-Name to Manifest of GUI jars.
QCCR1H95284	Fixed an issue that occurred when the following warning message in the WrapperProbeGw.log file was returned while running the Inventory Discovery by Scanner job: "Can not execute the script. The reason is forceDontExecute=false or the script file contains mainfunction=false".
QCCR1H95347	Fixed an issue that occurred when searching in UCMDB Browser froze the server.
QCCR1H95470	Fixed an issue that occurred when the Push IDs into NNMi adapter produced the following errors in RemoteProcesses.log: "The ucldb_wrapper.jar module, which is not valid, caused null"and "java.lang.ExceptionInInitializerError".
QCCR1H95472	Fixed an issue that occurred when manually deployed scanners could not be created.
QCCR1H95545	Fixed an issue that occurred when a Data Flow Probe randomly stopped discovering and sending results to the server.
Configuration Manager Fixed Defects	
QCCR1H95306	Fixed an issue that occurred when the current version of the view did not match the last authorized version.
QCCR1H95599	Fixed an issue that occurred when the external policies results were invisible in Configuration Manager.

Fixed Defects for UCMDB 10.11 CUP1

Here is a list of the defects fixed in the CUP1 release.

Global ID	Summary
QCCR1H84172	Windows Server 2012 is supported for Data Flow Probe and Universal Discovery.
QCCR1H89618	Fixed an issue that occurred when UCMDB Configuration Manager login is case sensitive.
QCCR1H91624	Fixed an issue that occurred when a trigger was dispatched to the wrong Data Flow Probe.
QCCR1H93238	Fixed an issue that IP addresses CIs discovered by member probes of clusters cannot be dispatched on host connection jobs.
QCCR1H93287	Fixed an issue that occurred when Universal Discovery Agent application is not populated to UCMDB.
QCCR1H93297	Fixed an issue that occurred when the SCCM adapter was configured to use the temp table.
QCCR1H93418	Fixed an issue that occurred when modifying the output node for a pattern-based model and an error was returned.
QCCR1H93480	Fixed an issue that occurred when executing UCMDB API Web Service "updateProbeScope".
QCCR1H93712	Fixed an issue that occurred when some scan files are moved to scans\Failed\error folder with error : String index out of range: -1.
QCCR1H93725	Added support for Oracle12c.
QCCR1H93798	Fixed an issue that occurred when new packages were not created.
QCCR1H93805	Fixed an issue that occurred when a user with no permissions attempts to login to UCMDB.
QCCR1H93836	Fixed an issue that occurred when WebSEAL passed the PD session cookie to the backend during a WebSEAL integration. A new setting is added which caused the browser cookies to be read at applet start time. The setting name is mam.web.should.read.web.browser.cookies.
QCCR1H93940	Fixed an issue that occurred when the UcmdbService calculateImpact() method is not able to cope with global Ids.
QCCR1H93980	Fixed an issue that occurred when a processing error was returned because of a List System Type definition.

Global ID	Summary
QCCR1H93982	Fixed an issue that occurred when an "Access Denied" error was returned while logging in to Configuration Manager after an upgrade.
QCCR1H94051	Fixed an issue that occurred when Pattern-Based models with ENUM Attributes revert values back to default values.
QCCR1H94162	Fixed an issue that occurred when the Rerun discovery button did not rerun discovery and the following error message was returned: "maximum number of expressions in a list is 1000".
QCCR1H94313	Fixed an issue that occurred when SQL error messages were returned in the Data Flow Probe: "ddm_gw_task_results_pkey index violation".
QCCR1H94350	Fixed an issue that occurred when Class B/C IPs by ICMP jobs failed with error "java.lang.NumberFormatException: For input string..".

Documentation Errata

The following items are listed incorrectly in the documentation.

HP Universal CMDB Administration Guide

Important note about a user's CIT Menu Items permissions when both custom and Out Of Box roles are assigned to the user

Location: *HP Universal CMDB Administration Guide*, version 10.10, page 188

Error: When multiples roles are assigned to a user, the user's permission level is set to the role with the minimum permissions. This is the desired behavior, but it is not explained in full details, thus causing confusion. (QCCR1H98051)

Correction: Under the current bullet as follows,

- For **CIT Menu Items**, you select a CIT from the tree and then select specific actions from the Available Actions pane and move them to the Selected Actions pane. You can also right-click a CIT and select the actions from the pop-up dialog box. If no permissions are assigned for any CIT, all the menu items are permitted by default (in accordance with the permissions granted in the General Actions tab).

The following important note shall be added to clarify the desired behavior:

Note: The above principle remains valid when there are multiple roles with menu items permissions/general actions. Both the menu items permissions and the general actions are accumulated. If there are NO menu items permissions accumulated from all the user's roles, all the menu items are permitted by default (in accordance with the permissions granted by accumulating all the General Actions from all the user's roles). In the opposite way, if there are menu items permissions accumulated from all the user's roles, they will be taken into account and the UI will enforce them, even in the case when a role with no CIT Menu Items is aggregated with a role with CIT Menu Items.

HP UCMDB Discovery and Integrations Content Guide - Supported Content

The description for the Command List column in the SSH Protocol section is missing a dot

Location: *HP UCMDB Discovery and Integrations Content Guide - Supported Content*, page 54 (CP14); page 54 (CP15) (QCCR1H92999)

Error: The description for the Command List column in the *SSH Protocol* section of *Chapter 7: Supported Protocols* is missing a dot.

Correction: The line "For example, entering *uname would select all of the following expressions:" should be changed to "For example, entering **.***uname would select all of the following expressions:"

HP Universal CMDB Developer Reference Guide, HP Universal CMDB Data Flow Management Guide

No documentation about the binary data found in communication logs

Location: *HP Universal CMDB Developer Reference Guide*, 10.20, pages 66~67; *HP Universal CMDB Data Flow Management Guide*, 10.20, page 256 (QCCR1H99152)

Error: There is no documentation about the binary data found in the communication logs, which is leading users to think that the scan files fail to parse the communication logs.

Correction: Add the following note to the two guides:

Note: CDATA mechanism is used to store information retrieved from user environment in the communication logs. When scan files get some characters or XML segments that cannot be parsed by the CDATA mechanism, the information will be saved in binary format for further

troubleshooting purpose. HP Software Support will decode the binary data in the communication logs to perform troubleshooting.

Appendixes

This appendix includes:

Enable Secure Login for the JMX Console	54
How to Re-index the CIs of a Given CI Type	55
How to Perform a Full Reindex of All CIs	56
How to Configure Query Search Filter	56
How to Mark Sensitive Settings and Enable Storing Encrypted Data in the Database Using JMX	57
How to Set Shared Key for Encrypting or Decrypting the InfrastructureSettings.xml File Using JMX	59
Enable Mutual Certificate Authentication for SDK	60
How to Set Master Keys	63
How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification	66
1_script_delete_index.sql	68
2_script_delete_constraint.sql	69

Enable Secure Login for the JMX Console

To enable secure login for the JMX console,

1. Access the UCMDDB JMX console: Launch a Web browser and enter the following address:
http://<UCMDDB machine name or IP address>:8080/jmx-console. You must log in with a user name and password (default is sysadmin/sysadmin).
2. Locate **UCMDDB:service=Ports Management Services** and click the link to open the Operations page.
3. Locate the **mapComponentToConnectors** operation.

4. To enable secure login for the JMX console, invoke the **mapComponentToConnectors** method with the following parameters:
 - **componentName**: jmx-console
 - **isHTTPS**: true
 - All other flags: false
5. Restart the server.
6. Log in to the JMX console using **https://** and port **8443** (default) or the one for https if it was changed.

For example, **https://mymachine:8443**.

Note: HP also recommends you setting a strong password for the **sysadmin** user and any other user that can access the JMX console.

How to Re-index the CIs of a Given CI Type

You can re-index the CIs of a given CI type from the CMDB model database for search purposes. To do this, follow these steps:

1. Go to **JMX Console > UCMDDB:service=Topology Search Services > reindexCiType**.
2. In the **ciType** field, enter the CI Type that you want to re-index.
3. Select one of the following options for the **includeSubtypes** option:
 - **True**: Re-index all the subtypes of the specified CI Type.
 - **False**: Do not re-index the subtypes of the specified CI Type.
4. Click **Invoke**.

To check the status and progress of the re-indexing operation, use the **printStatusReport** JMX method. This method can display the information such as overall status, progress, and number of indexed entries.

Note:

- In a multi-UCMDB environment, the **reindexCiType** method triggers the re-indexing operation on all nodes in the cluster.
- During the execution of the re-index operation, search operations are allowed and will return results based on what is already indexed.

How to Perform a Full Reindex of All CIs

Perform a Full Reindex of All CIs

Use either of the following approaches to perform a full reindex of all CIs available for search in the UCMDB Browser:

- Go to **JMX Console > UCMDB:service=Topology Search Services** and invoke the **reindex()** method.

This method removes all CIs information stored inside the SOLR index files without removing any internal SOLR files.

Note: You can also invoke the **reindexCiType()** method to re-index all the CIs of a given CI type from the CMDB model database. For more information, refer to the *HP Universal CMDB JMX Reference Guide*.

- Stop the UCMDB server, delete the **<UCMDB_Server_Home>/search** folder, and then start the UCMDB server.

The deletion of the folder forces a full reindex for all UCMDB customers and reverts the SOLR configuration to the out of the box values. This process removes all internal SOLR files and hence takes longer time than the previous one.

How to Configure Query Search Filter

By default, the search algorithm filters out the queries that are too general. If you want to turn off the filter, follow these steps:

1. Go to **JMX Console** > **UCMDB:service=Settings Services** > **setGlobalSettingValue**.
2. In the **name** field, enter **cmdb.search.filter.queries**.
3. In the **value** field, enter **false**.

Note: Enter **true** if you want to turn on the filter.

4. Click **Invoke**.

How to Mark Sensitive Settings and Enable Storing Encrypted Data in the Database Using JMX

UCMDB administrators can mark sensitive settings and enabling storing encrypted values for the sensitive settings in the database by using the following JMX methods added in the **UCMDB:service=Settings Services** category:

- **listSensitiveSettings** - Returns the list of settings that are marked as sensitive.
- **markSettingAsSensitive** - Marks a setting as sensitive. Usually sensitive settings contain confidential data. If a setting is marked as sensitive, its data will be encrypted when stored in the database.

Note: A setting can be marked as sensitive only when its value has been changed. If a setting does not have a value or if the value is out of the box, then the setting cannot be marked as sensitive.

- **markSettingAsNonsensitive** - Marks a setting as non-sensitive. Non-sensitive settings will have the value stored in plain text in database. This method is also used to decrypt the sensitive settings you encrypted using the **markSettingAsSensitive** method.

To mark a setting as sensitive,

1. On the UCMDBRTSM server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.
2. Click **UCMDB:service=Settings Services** to open the JMX MBEAN View page.

3. Click the **markSettingAsSensitive** method.
4. Enter the name of the setting you would like to mark as sensitive.
5. Click **Invoke**.

To mark a setting as non-sensitive,

1. On the UCMDVRTSM server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.
2. Click **UCMDB:service=Settings Services** to open the JMX MBEAN View page.
3. Click the **markSettingAsNonsensitive** method.
4. Enter the name of the setting you would like to mark as non-sensitive.
5. Click **Invoke**.

To view a list of sensitive settings,

1. On the UCMDVRTSM server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.
2. Click **UCMDB:service=Settings Services** to open the JMX MBEAN View page.
3. Click the **listSensitiveSettings** method.
4. Click **Invoke**.

A list of settings that are marked as sensitive is returned.

Note: The following existing settings are already encrypted in the database and cannot be marked as sensitive:

- **ha.cluster.authentication.keystore.password**
- **ha.cluster.authentication.shared.secret**
- **ha.cluster.message.encryption.keystore.password**

- **ssl.server.keystore.password**
- **ssl.server.truststore.password**

After upgrading to version 10.11 CUP6, two new OOTB settings introduced in version 10.11 CUP6 are marked as sensitive by default:

- **java.naming.ldap.search.password**
- **jetty.connections.http.probe.basicAuthentication.defaultPassword**

How to Set Shared Key for Encrypting or Decrypting the InfrastructureSettings.xml File Using JMX

UCMDB administrators can set a shared key for encrypting or decrypting the **InfrastructureSettings.xml** file on the UCMDB Server side or the Data Flow Probe/Integration Service side by using the **setSharedKey** JMX method.

Once you have set a shared key on the server side, make sure you set the same shared key on the Data Flow Probe/Integration Service side as well. This ensures that the Data Flow Probe/Integration Service can properly decrypt the **InfrastructureSettings.xml** file.

To set a shared key on the UCMDB Server side,

1. On the UCMDBRTSM server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.
2. Click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.
3. Click the **setSharedKey** method.
4. Enter a new value in the **Value** field for the shared key.
5. Click **Invoke**.

To set a shared key on the Data Flow Probe/Integration Service side,

1. Access the Data Flow Probe/Integration Service JMX console: Launch a Web browser and enter the

following address: **http://<Probe or integration service machine name or IP address>:1977**. If you are running the Data Flow Probe/Integration Service locally, enter **http://localhost:1977**.

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

2. Locate the **Probe_<Probe Name> type=MainProbe** service and click the link to open the JMX MBEAN View page.
3. Click the **setSharedKey** method.
4. In the **Value** field, enter the same value you provided on the UCMDB Server side for the shared key.
5. Click **Invoke**.

Note: If the Data Flow Probe is running in separate mode, make sure you set the shared key on both probeManager and probeGateway.

Enable Mutual Certificate Authentication for SDK

This mode uses SSL and enables both server authentication by the UCMDB and client authentication by the UCMDB-API client. Both the server and the UCMDB-API client send their certificates to the other entity for authentication.

Note:

- The following method of enabling SSL on the SDK with mutual authentication is the most secure of the methods and is therefore the recommended communication mode.
- The keystore used for client SDK must be in Java Keystore (JKS) format. The Java Cryptography Extension KeyStore (JCEKS) or other formats are not supported.
- The keystore used for SDK must contain only one key-pair and nothing else in it. The password for this key-pair must be the same as the one for keystore.

1. Harden the UCMDB-API client connector in UCMDB:
 - a. Access the UCMDB JMX console: Launch a Web browser and enter the following address: **http://<UCMDB machine name or IP address>:8080/jmx-console**. You may have to log in with a user name and password (default is sysadmin/sysadmin).

- b. Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.
- c. Locate the **PortsDetails** operation and click **Invoke**. Make a note of the HTTPS with client authentication port number. The default is 8444 and it should be enabled.
- d. Return to the Operations page.
- e. To map the ucldb-api connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:
 - **componentName**: ucldb-api
 - **isHTTPSWithClientAuth**: true
 - All other flags: false

The following message is displayed:

Operation succeeded. Component ucldb-api is now mapped to: HTTPS_CLIENT_AUTH ports.

- f. Return to the Operations page.
2. Repeat [step 1](#) for the **ping** component.
 3. Make sure the JRE that runs the UCMDB-API client has a keystore containing a client certificate.
 4. Export the UCMDB-API client certificate from its keystore.
 5. Import the exported UCMDB-API client certificate to the UCMDB Server Truststore.
 - a. On the UCMDB machine, copy the created UCMDB-API client certificate file to the following directory on UCMDB:

C:\HP\UCMDB\UCMDBServer\conf\security

- b. Run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <exported  
UCMDB-api client certificate> - alias ucldb-api
```

- c. Enter the UCMDB Server Truststore password (default **hpass**).

- d. When asked, **Trust this certificate?**, press **y** and then **Enter**.
 - e. Make sure the output **Certificate** was added to the keystore.
6. Export the UCMDB server certificate from the server keystore.
 - a. On the UCMDB machine, run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert  
-keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore  
-file C:\HP\UCMDB\conf\security\server.cert
```

- b. Enter the UCMDB Server Truststore password (default **hpass**).
 - c. Verify that the certificate is created in the following directory:
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
7. Import the exported UCMDB certificate to the JRE of the UCMDB-API client truststore.
 8. The certificate used by the API Client must contain in it's Common Name (CN) field the name of a user that's present in UCMDB.

This user **MUST** have an **EMPTY** password and all required permissions for SDK access.

To set an empty password to an existing UCMDB user,

- a. Go to **JMX Console > UCMDB:service=URM Services > listResourceTypes**.
 - b. Click **Auth_USER**.
 - c. Click your user and wait for the XML to load.
 - d. In the XML, replace the password with **s39t30*tfoZXg30xd/nvJGL5is8=**.
 - e. Click **Save resource**.
9. Restart the UCMDB Server and the UCMDB-API client.
 10. To connect from the UCMDB-API client to UCMDB-API server, use the following code:

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider  
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
```

```
(default:8444>));  
UcldbService ucldbService = provider.connect  
(provider.createCertificateCredentials(<TheClientKeystore.  
e.g: "c:\\client.keystore">, <KeystorePassword>),  
provider.createClientContext(<ClientIdentification>));
```

How to Set Master Keys

You can use the JMX console to change the master key that is used to encrypt all UCMDB keys.

Change the master key for a cluster

This method assumes that your UCMDB environment is deployed in a high-availability setup.

Caution:

- This method involves a restart of the entire cluster, so plan accordingly. It is recommended to change the master key of the cluster when there is little or no load on the servers. For example, you should avoid using this method during data-in operations.
- Do not change any settings in the time period between changing the master key and restarting the server. Not following this instruction may result in a failure to start the server.
- Machines that are not up or that will be added later to the cluster will need to be configured manually. Until they are configured, at most they can run as reader machines; trying to run them as writer machines will fail.

1. Back up the **c:\hp\UCMDB\UCMDBServer\conf\cmdb.conf** file and the values for the following settings:
 - ha.cluster.authentication.keystore.password
 - ha.cluster.authentication.shared.secret
 - ha.cluster.message.encryption.keystore.password
 - ssl.server.keystore.password
 - ssl.server.truststore.password
2. Make sure all the servers in the cluster are up and running.

3. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **http://localhost:8080/jmx-console**.

Note: If a load balancer is present, you must bypass it and not log on to the writer machine through a load balancer.

4. Do one of the following:
 - Search for **changeMasterKeyForCluster**.
 - Click **UCMDB:service=Security Services > changeMasterKeyForCluster**.
5. Enter and confirm the master key, and click **Invoke**. The master key will be changed first on the writer machine and then on all reader machines.
6. Restart all the machines in the cluster. You can use the JMX method **High Availability Services > restartCluster** to do this.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

Change the master key for a new machine in a cluster

If at least one of the following settings was changed, use Method A; otherwise, use Method B:

- ha.cluster.authentication.keystore.password
- ha.cluster.authentication.shared.secret
- ha.cluster.message.encryption.keystore.password
- ssl.server.keystore.password
- ssl.server.truststore.password

Method A

This method assumes that you already have properly configured a master key for the writer machine that is up and running in the cluster. If not, follow the instructions in ["Change the master key for a cluster" on the previous page](#).

1. Copy the **c:\hp\UCMDB\UCMDBServer\bin\wrapper.conf** file from the writer machine to the same location on the new (reader) machine.
2. Restart the server.

Method B

1. Back up the **c:\hp\UCMDB\UCMDBServer\conf\cmdb.conf** file.
2. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **http://localhost:8080/jmx-console**.
3. Do one of the following:
 - Search for **changeMasterKey**.
 - Click **UCMDB:service=Security Services > changeMasterKey**.
4. Enter and confirm the master key, and click **Invoke**.
5. Restart the machine.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

Revert the master key for a cluster to its default value

This procedure resets the master key for an entire cluster.

1. Make sure all the servers in the cluster are up and running.
2. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **http://localhost:8080/jmx-console**.

Note: If a load balancer is present, you must bypass it and not log on to the writer machine through a load balancer.

3. Do one of the following:

- Search for **restoreMasterKeyForCluster**.
 - Click **UCMDB:service=Security Services > restoreMasterKeyForCluster**.
4. Click **Invoke**. The master key will be changed first on the writer machine and then on all reader machines.
 5. Restart all the machines in the cluster. You can use the JMX method **High Availability Services > restartCluster** to do this.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

Revert the master key for a machine that was down when master key was reverted for whole cluster

1. Back up the **c:\hp\UCMDB\UCMDBServer\conf\cmdb.conf** file.
2. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **http://localhost:8080/jmx-console**.
3. Do one of the following:
 - Search for **restoreMasterKey**.
 - Click **UCMDB:service=Security Services > restoreMasterKey**.
4. Click **Invoke**.
5. Restart the machine.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification

You can dynamically add a verification criterion based on the **TenantOwner** attribute during the

matching phase of the identification process for CIs by using the new JMX setting **reconciliation.tenantaware.citypes**. If, compared to the other CI, there is a different value among the CI attribute values defined in this setting, the verification process stops and the match is rejected.

The following example explains how this setting works:

- If you have two node CIs:
 - Node1 with **TenantOwner=t1** and **name=n**
 - Node2 with **TenantOwner=t2** and **name=n**
 - **reconciliation.tenantaware.citypes** set to **node**

This scenario will result in the two nodes not matching.

- If Node1 does not have **TenantOwner** set, the default Tenant will be provided.

To enable the `reconciliation.tenantaware.citypes` setting for specific CITs (separated by comma) that are identified based on identification rules,

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the **name** field, enter **reconciliation.tenantaware.citypes**.
3. In the **value** field, enter names of the CITs, separated by comma.

Note: To disable this setting, leave the **value** field empty.

4. Click **Invoke**.

Note: If you add a node CIT, UNIX for example, you do not have to add it since it is inherited by identification rule. Only if you change the UNIX CIT identification rule, you need to add it explicitly.

To enable the `reconciliation.tenantaware.citypes` setting for all the CITs that are identified based on identification rules,

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the **name** field, enter **reconciliation.tenantaware.citypes**.

3. In the **value** field, enter *****.
4. Click **Invoke**.

To enable **TenantOwner** attribute verification for CITs that are identified by key attributes,

1. Add the **ID_ATTRIBUTE** qualifier for the **TenantOwner** attribute on the **managed_object** CIT.

Note: The **TenantOwner** attribute will be inherited to all the child classes. Make sure that a child class does not override it.

- a. Go to the **JMX console > UCMDB:service=URM Services**
- b. Invoke the **listResourceTypes** method.
- c. On the returned page, click **CM_CLASS**, then click **managed_object**.
- d. In the Resource XML box, add the following attribute qualifier to the **TenantOwner** attribute and click **Save resource**:

```
<Attribute-Qualifier name="ID_ATTRIBUTE" is-factory="false"
version="15">
  <Data-Items/>
</Attribute-Qualifier>
```

2. Reload the class model from persistency (go to the **JMX console > UCMDB:service=Class Model Services**, and invoke the **reloadClassModelFromPersistency** method).
3. Go to **JMX console > UCMDB:service=Model Services**, invoke the **recalculateID** method with **classname** field empty.

This may take a while as it updates the calculated IDs for all instances of the classes with key attributes identification.

1_script_delete_index.sql

The **1_script_delete_index.sql** script is as follows:

```
use 'CMDB Database'
```

```
declare
    @column_name nvarchar(255),
    @index_name nvarchar(255),
    @table_name nvarchar(255),
    @sql_str nvarchar(4000) = ''

SET @column_name = 'COLUMN_NAME'

DECLARE ColumnCursor CURSOR FOR
SELECT
    ind.name as index_name,
    t.name as table_name
FROM sys.indexes ind
INNER JOIN sys.index_columns ic
    ON ind.object_id = ic.object_id
    AND ind.index_id = ic.index_id
INNER JOIN sys.columns col
    ON ic.object_id = col.object_id
    AND ic.column_id = col.column_id
INNER JOIN sys.tables t
    ON ind.object_id = t.object_id
WHERE col.name = @column_name

OPEN ColumnCursor

FETCH NEXT FROM ColumnCursor INTO @index_name, @table_name
WHILE @@FETCH_STATUS = 0
BEGIN
    -- drop index
    set @sql_str = 'DROP INDEX ' + @index_name + ' ON ' + @table_name

    print @sql_str
    exec sp_executesql @sql_str

    FETCH NEXT FROM ColumnCursor INTO @index_name, @table_name
END
CLOSE ColumnCursor
DEALLOCATE ColumnCursor
```

2_script_delete_constraint.sql

The **2_script_delete_constraint.sql** script is as follows:

```
use 'CMDB Database'

declare
    @column_name nvarchar(255),
```

```
@constraint_name nvarchar(255),
@table_name nvarchar(255),
@sql_str nvarchar(4000) = ''

SET @column_name = 'COLUMN_NAME'

DECLARE ColumnCursor CURSOR FOR
SELECT
    df.name constraint_name ,
    t.name table_name
FROM sys.default_constraints df
INNER JOIN sys.tables t ON df.parent_object_id = t.object_id
INNER JOIN sys.columns c ON df.parent_object_id = c.object_id AND df.parent_column_
id = c.column_id
WHERE c.name = @column_name

OPEN ColumnCursor

FETCH NEXT FROM ColumnCursor INTO @constraint_name, @table_name
WHILE @@FETCH_STATUS = 0
BEGIN
    -- drop constraint
    set @sql_str = 'ALTER TABLE ' + @table_name + ' DROP CONSTRAINT ' + @constraint_
name
    print @sql_str
    exec sp_executesql @sql_str
    --drop column
    set @sql_str = 'ALTER TABLE ' + @table_name + ' DROP COLUMN ' + @column_name
    print @sql_str
    exec sp_executesql @sql_str

FETCH NEXT FROM ColumnCursor INTO @constraint_name, @table_name
END
CLOSE ColumnCursor
DEALLOCATE ColumnCursor
```

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 Release Notes (Universal CMDB & Configuration Manager 10.11 CUP6)

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@hp.com.

We appreciate your feedback!