Universal CMDB

Software Version: Content Pack 24.00 (CP24)

Discovery and Integrations Content Guide - General Reference

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

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com/.

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

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

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

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

Contents

Chapter 1: How to Define a New Port

Edit the **portNumberToPortName.xml** file to define a new port:

1. In the Adapter Management window (**Managers > Data Flow Management > Adapter Management**), search for the `portNumberToPortName.xml` file: click the **Find resource** button and enter **portNumberToPortName.xml** in the **Name** box. Click **Find Next**, then click **Close**.

   The file is selected in the Resources pane and the file contents are displayed in the View pane.

   For details about this file, see "portNumberToPortName.xml File" on page 32.

2. Add another row to the file and make changes to the parameters:

   ```
   <portInfo portProtocol="xxx" portNumber="xxx" portName="xxx" discover="0"
   cpVersion="xx"/>
   ```

Parameter	Description
portProtocol	The network protocol used for discovery (`udp` or `tcp`).
portNumber	The port number to be discovered. This attribute may be a number or a range. Ranges may be separated by commas or dashes or both. For example: "10, 21, 45", "10-21", or "10-21, 45, 110".
portName	The name that is to be displayed for this port.
discover	**1**. This port must be discovered. **0**: This port should not be discovered.
cpVersion	Use this parameter when you want to export the **portNumberToPortName.xml** file to another UCMDB system with the Package Manager. If the **portNumberToPortName.xml** file on the other system includes ports for this application but does not include the new port you want to add, the **cpVersion** attribute ensures that the new port information is copied to the file on the other system. The **cpVersion** value must be greater than the value that appears in the root of the **portNumberToPortName.xml** file. For example, if the root **cpVersion** value is **3**: `<portList parserClassName="com.hp.ucmdb.discovery. library.communication.downloader.cfgfiles. KnownPortsConfigFile" cpVersion="3">`

Parameter	Description
	the new port entry must include a **cpVersion** value of **4**: `<portInfo portProtocol="udp" portNumber="1" portName="A1" discover="0" cpVersion="4"/>` > **Note:** If the root **cpVersion** value is missing, you can add any non-negative number to the new port entry. This parameter is also needed during Content Pack upgrade. For details, see "How to Use the cpVersion Attribute to Verify Content Update" on page 9.

Chapter 2: How to Discover IP Addresses in Universal Discovery

In Universal Discovery, IP addresses can be defined as the following two types:

- **Data center IP addresses**. These IP addresses are stable or long-term.
- **Client IP addresses**. These IP addresses are dynamic or short-term.

This task contains the following:

- How to discover Data center IP addresses

  a. Run the following ICMP jobs:

  - **Range IPs by ICMP**
  - **Class B IPs by ICMP**
  - **Class C IPs by ICMP**

  b. Run the **Range IPs by nmap** job.

  For details about these jobs, see the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Modules*.

- How to discover Client IP addresses

  a. Run the **Client Connection by SNMP** job to discover switches or routers. The IP addresses need to be defined in the Data Flow Probe range as the Client IP addresses.

  b. Run the **IP MAC Harvesting by SNMP** job to discover Client IP addresses that are cached in the triggered switch or router.

  For details about these jobs, see the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Modules*.

- How to improve performance for IP addresses related jobs

  - Adjust the following job parameters if available:
    - **bulkSize**
    - **retryDiscover**

- **threadPoolSize**
- **timeoutDiscover**

For details about these job parameters, see the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Modules*.

- Change the **Get Request Operation Type** value in the SNMP protocol from **Get-NEXT** to **Get-BULK** if possible.

  For details about this value, see the *SNMP Protocol* section of the *HPE UCMDB Discovery and Integrations Content Guide - Supported Content*.

Chapter 3: How to Use the cpVersion Attribute to Verify Content Update

The **cpVersion** attribute is included in the portNumberToPortName.xml file, and indicates in which Content Pack release a port has been discovered. For example, the following code defines that the LDAP port 389 has been discovered in Content Pack 11.00:

```
<portInfo portProtocol="tcp" portNumber="389" portName="ldap" discover="11"
cpVersion="11"/>
```

During a Content Pack upgrade, DFM uses this attribute to perform a smart merge between the existing portNumberToPortName.xml file (which may include user-defined ports) and the new file. Entries previously added by the user are not removed and entries previously deleted by the user are not added.

For details about the **portNumberToPortName.xml** file, see "portNumberToPortName.xml File" on page 32.

To verify that a Content Pack is successfully deployed:

1. Install the latest Service Pack release.
2. Start the UCMDB Server.
3. Verify that all services are running. For details, see the section about HPE Universal CMDB Services in the *HPE Universal CMDB Administration Guide*.
4. Install and deploy the latest Content Pack release. For details, refer to the Content Pack installation guide.
5. In the Adapter Management window, access the **portNumberToPortName.xml** file.
6. Verify that no user-defined ports have been deleted and that any ports deleted by the user have not been added.

Chapter 4: How to Delete Files Copied to Remote Machine

During discovery, the Data Flow Probe copies files to a remote Windows machine. For details, see "Files Copied to a Remote Machine" on page 13.

To configure DFM to delete files copied to the destination machine after discovery is finished:

1. Access the **globalSettings.xml** file: **Adapter Management > AutoDiscoveryContent > Configuration Files**.
2. Locate the **removeCopiedFiles** parameter.
   - **true**. The files are deleted.
   - **false**. The files are not deleted.
3. Save the file.

To control HPCmd behavior:

1. In the **globalSettings.xml** file, locate the **NtcmdAgentRetention** parameter.
2. Enter one of the following:
   - **0**. (The default) Unregister the service and delete the remote executable file. (**Unregister**: stop the service and remove it from the remote machine, so that it is no longer listed in the list of services.)
   - **1**. Unregister the service, but leave the executable file on the file system.
   - **2**. Leave the service running, and leave the executable file on the file system.

Chapter 5: How to Run HPCmd from Windows Server 2008, 2008 R2, 2012, and 2012 R2 Machines

Perform the following to ensure that HPCmd functions properly when the Probe is installed on a Windows Server 2008, 2008 R2, 2012, or 2012 R2 machine:

1. Stop the Probe.
2. Open the standard Windows Registry Editor application by running the **regedit** executable.
3. In the Registry Editor navigate to the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
4. Under this key there should be a **REG_DWORD** parameter **SCMApiConnectionParam**
   a. If this is missing, add a new **REG_DWORD** parameter **SCMApiConnectionParam** and set its value to 0x80000000.
   b. If this value is already available in the registry, combine it with the 0x80000000 mask (using bitwise OR). For example, if there was a value 0x1 in there, you need to set this value to 0x80000001.

   > **Note:** To run HPCmd from a Windows 2008 machine **with UAC enabled**, also perform the following additional steps. **Do not perform these steps for a Windows Server 2008 R2, 2012, or 2012 R2 machine.**
5. Locate the **wrapper.exe** file, in the **hp\UCMDB\DataFlowProbe\bin** directory.
6. Right-click the **wrapper.exe** file, and select **Properties**.
7. In the **Compatibility** tab:
   a. Select **Compatibility mode**.
   b. Select **Run this program in compatibility for**: **Windows XP (Service Pack 2)**.
   c. Select **Run this program as administrator**.
8. Start the Probe.

> **Note:** HPCmd uses DCOM protocol for connecting to remote machines. The DCOM protocol requires that the following ports are open: **135**, **137**, **138,** and **139**. In addition it uses arbitrary ports

> between **1024** and **65535**, but there are ways to restrict the port range used by WMI/DCOM/RPC. For information about configuring DCOM to work with firewalls, see http://support.microsoft.com/kb/154596/en-us.

Chapter 6: Files Copied to a Remote Machine

During discovery, Data Flow Probe copies files to a remote Windows machine to enable discovery of the machine's components. The files are copied to the **%SystemRoot%\system32\drivers\etc** folder on the remote machine.

> **Note:**
>
> - Data Flow Management runs **HPCmdSvc.exe** to connect to and retrieve the Shell on the remote machine.
> - When the **wmic** command is launched on the remote Windows machine, by the **Host Connection by Shell** or **Host Resources by Shell** or **Host Applications by Shell** jobs, an empty **TempWmicBatchFile.bat** file is created.

The following files are copied:

File	Content Pack Version	Description
adsutil.vbs	All	The Visual Basic script used for discovery of Microsoft IIS applications. DFM copies this script to the remote machine to discover IIS. **Relevant DFM Job:** IIS Applications by NTCMD or UDA
diskinfo.exe	All	The executable that enables the retrieval of disk information when it is not available to be retrieved by **wmic**. DFM discovers default disk information with the **wmic** query. However, if the **wmic** query fails to execute, DFM copies the **diskinfo.exe** file to the remote machine. This failure can occur if, for example **wmic.exe** is not included in the PATH system variable or is completely absent on the remote machine, as is the case on Windows 2000. **Relevant DFM Job:** Host Resources by Shell

File	Content Pack Version	Description
Exchange_Server_2007_Discovery.ps1	CP4	The PowerShell script for MS Exchange 2007 discovery. DFM uses a PowerShell scenario to discover Microsoft Exchange 2007 by NTCMD. This file, therefore, must be copied to the remote machine. **Relevant DFM Jobs:** • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA
GetFileModificationDate.vbs	CP5	The Visual Basic script for retrieving the file modification date (disregarding locale). The most common use case is when DFM must retrieve the last modification date of a configuration file of a discovered application. **Relevant DFM Jobs:** • Apache Tomcat by Shell • File Monitor by Shell • IIS Applications by NTCMD or UDA • JEE Weblogic by Shell • JEE WebSphere by Shell or JMX • JEE WebSphere by Shell • SAP System by Shell • Service Guard Cluster Topology by TTY • Siebel Application Server Configuration • Software Element CF by Shell • Veritas Cluster by Shell • Web Server by Shell
getfilever.vbs	All	The Visual Basic script used to identify the version of the running software. The script retrieves the executable or DLL file version on Windows machines. This script is used by Shell-based application signatures plug-ins to retrieve the version of a particular software on the remote machine. **Relevant DFM Job:** Host Applications by Shell

File	Content Pack Version	Description
junction.exe	CP5	This executable file, part of the Sysinternals Suite (http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx), enables the creation of a junction point. DFM uses this file if the **linkd.exe** and **mklink.exe** tools are absent on the remote machine. When DFM runs discovery on a Windows x64 machine, DFM needs to bypass the Windows redirect feature running on that machine. DFM does this by creating a link to the **%SystemRoot%\System32** folder with either the **linkd.exe** or **mklink.exe** tool. However, if these tools are missing on the remote machine, DFM transfers **junction.exe** to the remote machine. DFM is then able to launch the 64-bit version of the system executable files. (Without this 64-bit version, DFM would be locked into an isolated 32-bit world.) This junction point is automatically removed once discovery is complete. **Relevant DFM Jobs:** • Host Resources by Shell • Host Applications by Shell • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA
meminfo.exe	All	The executable that enables the retrieval of memory information. DFM discovers memory information with the **wmic** query. However, if the **wmic** query fails to execute, DFM copies the **meminfo.exe** file to the remote machine. This failure can occur if, for example, **wmic.exe** is not included in the PATH system variable or is completely absent on the remote machine, as is the case on Windows 2000. **Relevant DFM Job:** Host Applications by Shell
reg_mam.exe	All	The copy of the Microsoft reg.exe file that enables querying the registry. If DFM does not discover a native reg.exe file, this executable is copied to the remote Windows machine. This situation occurs with some previous Windows versions (for example, Windows 2000) where the tool is not included by default but can still function there correctly. **Relevant DFM Job:** Host Applications by Shell

Chapter 7: Content Pack Configuration Files

The Content Pack contains configuration files which enable you to configure commonly used parameters such as command timeouts, usage of some utilities, application signatures, and so on.

This section includes:

globalSettings.xml File

The following table describes the parameters in the **globalSettings.xml** configuration file (**Data Flow Management > Adapter Management > Resources > Packages > AutoDiscoveryContent > Configuration Files**):

Parameter	Description
AdditionalClasspath	Additional path that enables to run different patterns (that is, database patterns); all paths should be relative to the **$PROBE_INSTALL/root/lib/collectors/probeManager/discoveryResources/** folder and should be semicolon separated **Example:** **<property name="AdditionalClasspath"> db/oracle/.;db/mssqlserver/.</property>** means that following paths will be included in the classpath: • **$PROBE_INSTALL/root/lib/collectors/probeManager/discoveryResources/db/oracle/** • **$PROBE_INSTALL/root/lib/collectors/probeManager/discoveryResources/db/mssqlserver/**
allowCaliperOnHPUX	Indicates whether to allow the execution of caliper on HP-UX. This setting will be used in the **WebSphere_By_Shell** adapter, to get the full command line when the **ps** command fails to do so. **Default:** false

Parameter	Description
allowCallhome	Indicates whether to allow to call home. **Default:** true
allowCallhomeInterval	The time interval in hours that is allowed between two call home requests from the same host. **Default:** 24
allowDataCenterCallhome	Indicates whether to allow Data Center IP addresses to call home. **Default:** true
allowGettingCredential SecuredAttribute	Indicates whether Jython scripts are allowed to get credentials secured data (true) or not (false). If this setting is set to false, then Jython scripts are not allowed to retrieve sensitive credentials data (like passwords that are stored on the server side). **Default:** true
allowPFilesOnSunOS	Indicates whether to allow the execution of pfiles on Solaris. **Default:** false **Caution:** Setting this parameter to true may cause problems for some processes on some Solaris systems.
allowPFilesOnHPUX	Indicates whether to allow the execution of pfiles on HP-UX. **Default:** false **Caution:** Setting this parameter to true may cause problems for some processes on some HP-UX systems.
autoTruncateDbEncoding	Indicates the encoding used by the CMDB underlying database. This property is used for calculating the number of characters that should be sent after truncation. **Default:** UTF8
autoTruncatePercentage	If the value of the attribute (with the DDM_ AUTOTRUNCATE qualifier) exceeds the size limit multiplied by this parameter it will be truncated to the specified part of the defined size. **Default:** 100 percent

Parameter	Description
clearCommandLineFor Processes	Clears the Command line for these processes. This option is used to ensure that no private or confidential data is stored in CMDB. **Default:** srvrmgr.exe, srvrmgr, xCmd.exe, HPcmd.exe, ssonsvr.exe **Syntax exceptions:** Process names are case insensitive and should be split by commas.
consoleCommands	The comma-separated list of commands globally available for all PowerShell connections. The commands specified in this list will be executed using CMD interpreter (cmd /c "command")
datacenter callhome	If the management zone is set to Data Center and this parameter is enabled, Data Flow Probe ignores call home messages from Universal Discovery Agent. **Default:** Enabled
dbQueryTimeout	The timeout (in seconds) for all SQL queries. Indicates how long to wait for query results. The timeout applies only if the value is greater than zero (0). **Default:** 100 seconds **Note:** Some JDBC drivers cannot support this setting.
ddmagentCiphers	The algorithm used by the UD Agent to encrypt or decrypt the data transferred to or from client machines.
ddmagentPrefix	The prefix used by the UD Agent.
ddmagentProtocol	The protocol used by the Probe to communicate with UD Agent.
ddmagentEnableDownloadResume	Specifies whether the resumable download is enabled or not. **true.** The resumable download functionality is available. **false.** The resumable download functionality is not available.
ddmagentDefaultBlockLen	The default chunk size (in bytes) used to upload/download files to/from the UD Agent.
ddmagentResumableFileSuffix	The file extension used for parts of the resumable transfer file.
ddmagentDefaultResumeBlockLen	The default chunk size (in bytes) for resumable file transfer.

Parameter	Description
ddmagentEnableUploadResume	Specifies whether the resumable upload is enabled or not. **true.** The resumable upload functionality is available. **false.** The resumable upload functionality is not available.
defaultSapClients	When this parameter is defined, you do not need to specify the SAP Client Number parameter in the SAP ABAP protocol. Instead, you can create one or more comma-separated credentials for multiple SAP systems with different supported clients. **Example:** `<property name= "defaultSapClients"> 800,500,200,300 </property>` **Default:** 800
desktopOperatingSystems **serverOperatingSystems**	These two parameters are used to determine if the host's operating system is of type Desktop or Server. If the host's operating system name contains a value from one of these lists, its **host_isdesktop** is set accordingly. Otherwise the value of **host_isdesktop** attribute is left empty.
discovereAllListenPorts	Related to application signatures configuration.

Parameter	Description
discoveredStorageTypes	Describes storage types which have to be reported to UCMDB. Options are split by commas. Available options are: • FixedDisk • NetworkDisk • CompactDisk • RemovableDisk • FloppyDisk • VirtualMemory • FlashMemory • RamDisk • Ram • No Root Directory • Other • UNKNOWN
enableJeeEnhancedTopology	Indicates whether to enable the reporting of the improved JEE topology. **Default:** false
enableNormalizationRuleLabel	Specifies whether the label format for output values in the normalization rule is enabled or not. If you want to display values in the label format instead of the default format that contains underscores for the normalized fields, do the following: 1. Add **<property name="enableNormalizationRuleLabel">true</property>** in the **globalSettings.xml** file if it does not exist. 2. Restart the probe. **Default:** false

Parameter	Description
enableSSHSharedHomeDir	Setting this parameter to **true** enables Inventory Discovery via SSH to be able to use a user account that has the shared home directory. For example, the home directory is mounted via NFS or Samba, so that the same directory is used when the user logs into different computers. In order for this feature to work correctly, Universal Discovery Agent cannot be installed to run under a user account that has the home directory that is shared (for example, mounted via NFS or Samba). If it is already installed, uninstall it. For more information, see the *How to Completely Uninstall the Universal Discovery Agent* section in the *Data Flow Management Guide*. To enable this feature, set this parameter value to **true**. The default value is **false**. **Caution:** Enabling and then disabling this feature may cause unpredictable behavior. **Note:** • Do not install Universal Discovery Agent to run under a user account that has the shared home directory (for example, mounted via NFS or Samba) after you enable this feature. • In UCMDB, you may unexpectedly see newly-created empty Node CIs. You can delete them, or wait for the aging mechanism to delete them (usually after 40 days). • The software utilization information cannot be reported by the Inventory Discovery by Scanner job when using the SSH protocol.
fs_discovery_method	The file system discovery method. Valid values are **perl** and **lsawk**. • **perl** (default)**.** Run Perl scripts to discover file systems. If Perl is not installed on the target host, the **lsawk** discovery method is used as a fallback mechanism. • **lsawk.** Run **ls** + **awk** commands to discover file system.

Parameter	Description
IgnoreClassAttributes	Ignores the attributes in the discovery result processing. **Format:** node.name, node.description Data Flow Probe will not validate the node attribute name and description. The probe will not report these attributes to UCMDB. **Default:** node.misc_info
ignoreLocalizedVirtualInterfaces PatternList	Lists patterns for localized Windows Virtual interface description that must not take part in the Host Key creation process. **Format:** Comma-separated list of strings, no additional white-spaces allowed.
ignoreVmwareInterfaces	Indicates whether to ignore the VMware MAC address. • **When there is a Physical MAC** (default)**.** The VMware MAC address is used only if the pattern cannot find any physical MAC address. • **Always.** Always ignore VMware MAC address.

Parameter	Description

jdbcDrivers	This section enumerates driver classes used to connect to a dedicated Database server. Names of sub-keys must be the same as used in credentials (sqlprotocol_dbtype attribute of protocol).
	
	Change them if drivers other than OOTB JDBC drivers are used.
	
	Default values for OOTB-installation:
	
	`<property name="jdbcDrivers:>`
	`<oracle>`
	`oracle.jdbc.OracleDriver`
	`</oracle>`
	`<oracleSSL>`
	`oracle.jdbc.OracleDriver`
	`</oracleSSL>`
	`<MicrosoftSQLServer>`
	`net.sourceforge.`
	`jtds.jdbc.Driver`
	`</MicrosoftSQLServer>`
	`<MicrosoftSQLServer> net.sourceforge.jtds.`
	`jdbc.Driver`
	`</MicrosoftSQLServerNTLM>`
	`<MicrosoftSQLServerNTLMv2>`
	`net.sourceforge.jtds.jdbc.Driver`
	`</MicrosoftSQLServerNTLMv2>`
	`<Sybase>`
	`com.sybase.jdbc.SybDriver`
	`</Sybase>`
	`<db2>`
	`com.ibm.db2.jcc.DB2Driver`
	`</db2>`
	`<mysql>`
	`com.mysql.jdbc.Driver`
	`</mysql>`
	`</property>`

Parameter	Description
jdbcPreUrls	This section enumerates URL templates used to connect to dedicated the database server. Names of sub-keys must be the same as those used in credentials (sqlprotocol_dbtype attribute of protocol). Change them if drivers other than OOTB JDBC drivers are used. Values depend on used drivers and should be taken from driver documentation. **Note:** The ampersand symbol (&) must be escaped according to the XML standard (&). **Default values for OOTB-installation:** <property name="jdbcPreUrls"> <oracle>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS= (PROTOCOL=tcp) (HOST=%%ipaddress%%)(PORT=%%protocol_port%%)) (CONNECT_DATA=(%%connect_data%%=%%sqlprotocol_ dbsid%%))) </oracle> <oracleSSL>jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps) (HOST=%%ipaddress%%)(PORT=%%protocol_port%%)) (CONNECT_DATA=(%%connect_data%%=%%sqlprotocol_ dbsid%%))) </oracleSSL> <MicrosoftSQLServer> jdbc:jtds:sqlserver:// %%ipaddress%%:%%protocol_port%%; instanceName=%%sqlprotocol_dbname%%; loginTimeout=%%protocol_timeout%%; logging=false;ssl=request </MicrosoftSQLServer> <MicrosoftSQLServerNTLM> jdbc:jtds: sqlserver://%%ipaddress%%: %%protocol_port%%;instanceName= %%sqlprotocol_dbname%%;domain= %%sqlprotocol_windomain%%; loginTimeout= %%protocol_timeout%%;logging=false </MicrosoftSQLServerNTLM>

Parameter	Description
jdbcPreUrls continued	<MicrosoftSQLServerNTLMv2>jdbc:jtds:sqlserver://%%ipaddress%%:%%protocol_port%%;instanceName=%%sqlprotocol_dbname%%;domain=%%sqlprotocol_windomain%%;loginTimeout=%%protocol_timeout%%;logging=false;ssl=request;useNTLMv2=true</MicrosoftSQLServerNTLMv2> <Sybase> jdbc:sybase:Tds:%%ipaddress%%:%%protocol_port%%?DatabaseName=%%sqlprotocol_dbname%% </Sybase> <db2> jdbc:db2://%%ipaddress%%:%%protocol_port%%/%%sqlprotocol_dbname%% </db2> <mysql> jdbc:mysql://%%ipaddress%%:%%protocol_port%%/%%sqlprotocol_dbname%%</mysql> <parameters> <parameter type="oracle" name="connect_data"> <value>SERVICE_NAME</value> <value>SID</value> </parameter> <fallbackExceptionList> <error type="oracle">.*ORA\-12514.*</error> <error type="oracle">.*ORA\-27101.*</error> </fallbackExceptionList> </parameters> </property> Each <parameter> element has a name attribute and one or more <value> tags. Each <parameter> can be used in the Oracle URL template by using the format "%%[parameter name]%%" (for example, %%connect_data%%). If a <parameter> has more than one <value> tag, then the parsing engine generates all permutations of the possible values in the template string, and the client tries to connect to the database server by each of these permutations. Since during connection errors can occur, the <fallbackExceptionList> element specifies which errors should be ignored if they occur. If the engine ignores such an error, then it tries to connect using another permutation of values in the template string. If an error occurs that is not specified by <fallbackExceptionList>, the engine does not try another permutation and the job fails with the error message that was caught.

Parameter	Description
loadExternalDTD	Used to configure file_mon_utils to prevent downloading DTD files while validating the XML. **Default:** false
maxExecutionRecords	Specifies maximal number of execution records that can be in the communication log. This parameter should be used when the discovery process discovers a lot of data. The parameter can be overridden on an adapter level. In this case, add the parameter to the adapter with desired record limit (see Probe documentation). **Default:** -1 means unlimited
maximumConnectionsPerSecond	Enables limiting the number of new connections per second created by the Probe to other machines. • **0.** Unlimited number of connections allowed. • **> 0.** The maximum number of connections. If this limit is reached, any job trying to create a new connection will wait for a period of time that is determined in the "timeToSleepWhenMaximumConnectionsLimitReached" parameter below. **Default:** 0 (unlimited)
maxStoreSentResults	Specifies maximal number of sent results that can be stored in the communication log. This parameter can be changed if there are too many results stored in the communication log. If this value is greater than 0, the log will store the corresponding number of results for deleted results AND updated results, meaning that the results set will contain double the value of **maxStoreSentResults.** **Default:** -1 means unlimited
maxPingIPv6CountPerRange	Specifies the maximum IPv6 count of per range for Ping Sweep. **Default:** 1000000
multipleDB2Instances	Indicates whether multiple DB2 instances are installed on the same server. **Default:** true
multipleUpdateIgnoreTypes	Used by UCMDB. The Probe does not generate a **Multiple updates in bulk** warning for enumerated CI types.

Parameter	Description

notRecordedMethods	Specifies a list of methods that are not to be recorded in the communication log.
	To remove a method from being recorded in the communication log, copy its name from the communication log and add it here.
	Example:
	`<property name="notRecordedMethods">`
	`<method>getLastCommandOutputBytes</method>`
	`</property>`

NtcmdAgentRetention	NTCMD agent retention mode. Specifies how to handle a remote NTCMD service and its executable file when closing the connection. • **0** (default)**.** Unregister the service and delete the remote executable file. • **1.** Unregister the service but keep the executable file on the file system. • **2.** Leave the service running, keep the executable file.
NtcmdSessionUseProcessBuilder	This parameter is for **NtcmdSessionAgent** and should be always be **true**. This parameter tells how to create a new process. • **true.** The new process will be created by ProcessBuilder (new API from Java 5.0) • **false.** The new process will be created by Runtime.exec (old API, from Java 1.4.2). Set to false only in case of backward compatibility problems.
objectSendAmountThreshold	When the number of discovered objects exceeds this threshold, the objects are immediately sent to the server. Requires using the sendObject(s) API in jython scripts. **Default:** 2000 objects
objectSendTimeThreshold	When more than the specified time (in seconds) has passed since the previous object report, the objects are immediately sent to the server. Requires using the 0sendObject(s) API in jython scripts. **Default**: 300 seconds

Parameter	Description
pingClientTypeIp	(Only for the **Inventory Discovery by Scanner** job) Indicates whether to allow to ping Client IP addresses. **Default:** false
pingHostName	(Only for the **Inventory Discovery by Scanner** job) Indicates whether to allow to ping host names. **Default:** false
portExpirationTime	The expiration time (in seconds) of the TCP/UDP port entry in the Probe's database. **Default:** 60 seconds
powershellConnectionIdleTimeout	Defines the maximum idle time (in milliseconds) for the powershellconnector.exe process. The timer resets its state after each command execution. **Default:** 3600000 milliseconds (1h)
processExpirationTime	The expiration time (in seconds) of the Process entry in the Probe database. **Default:** 60 seconds
protocolConnectionOrder	The protocol connection order for the **Host Connection by Shell** job. **Default:** ssh, telnet, ntadmin
remoteProcessTimeout	After being launched, the remote process should connect with the Probe within the defined time (in milliseconds), otherwise the following error is produced: **Failed to connect to remote process**. **Default:** 300000 milliseconds (5 minutes)
removeCopiedFiles	In some cases DFM copies scripts and third-party utilities on a client machine. The **removeCopiedFiles** parameter defines whether these files should (true) or should not (false) be deleted after discovery is finished.
reportSapAppServerDatabase	Indicates whether to report SAP Application Server databases that are based on the configuration file content. Only affects the **Host Applications by Shell**, and **SAP ABAP Topology by SAP JCO** jobs. **Default:** false

Parameter	Description
reportPhysicalSerialNumbers	Indicates whether to report physical serial numbers from **hwsmbiosPhysicalAttributeSerialNumber** of scan files. **Default:** false
ResultProcessIsLenient	When setting to **true**, the discovery result processing is lenient, which is not recommended: • If a reported string attribute has a too large value, the string is automatically truncated according to the CMDB Class Model definition. • If the OSH attribute is invalid (type/nonexisting attribute/missing ID attribute), only the invalid OSH is dropped, rather than entire bulk (default). **Default:** false
setBiosUuidToMicrosoftStandart	Indicates whether the BIOS UUID value for Windows operating systems should be reported in Microsoft style (some bytes order reversed) instead of the original BIOS value. Affects Host Connection jobs. • **false** (default)**.** Converts to original BIOS stored value • **true.** Converts to Microsoft standard. **Note:** Setting this parameter to **true** may result in conflicts with the BIOS UUID value discovered by VMware jobs or some integrations.
shellGlobalBandwidthLimit	The maximum bandwidth (in kilobits per second) to upload and download files to and from the discovery node **Note:** If no value or 0 is assigned, all of the available bandwidth is used.
shellGlobalCommandTimeout	Global timeout (in milliseconds) for all Shell client commands. Indicates how long to wait for a command's result. **Default:** 15000 milliseconds
siebelCommandTimeout	The amount of time to wait for the Siebel command's result. **Default:** 3 minutes (180000 ms)

Parameter	Description
snmpGlobalRequestTimeout	This is the time, in milliseconds, after which a request using SNMP will timeout. **Default:** 3,000 milliseconds **Note:** This value is global for all SNMP requests. If you want to override the SNMP request timeout for a specific query (where you know the query takes more time than the default timeout), provide the timeout value as a second parameter to the executeQuery method on the SNMP client: **snmpClient.executeQuery(SNMP_QUERY_STRING, QUERY_TIMEOUT_IN_MILLISECONDS).**

snmpTestQueries	Defines the default SNMP test query for SNMP Agent. Can be overridden for specific devices.
	Default:
	`<property name="snmpTestQueries">`
	`<query>`
	`1.3.6.1.2.1.1.1,1.3.6.1.2.1.1.2,`
	`string</query>`
	`</property>`

ssh-log-level	The SSH log level. **Levels:** 1-7, where 7 is the most detailed defect level.
tcpExpirationTime	The expiration time (in hours) of TCP connection entry in probe database. **Default:** 24 hours
timeToSleepWhenMaximumConnectionsLimitReached	Determines how long (in milliseconds) a job needs to wait until a new connection can be created, assuming the maximum connections limit has been reached. (See "maximumConnectionsPerSecond" above.) **Default:** 1000 milliseconds (1 second) **Note:** If **maximumConnectionsPerSecond = 0** this property is ignored.

Parameter	Description
tnsnamesFilePaths	Paths to search the **tnsnames.ora** file (including **tnsnames.ora** itself, comma separated) **Example:** <property name="tnsnamesFilePaths"> c:\temp\tnsnames.ora </property>
useIntermediateFileForWmic	Usage of an intermediate temporary file for data transfer by wmic command. **Default:** false
useJinteropOnWindows	This property is used on Windows machines. • **true.** The Probe uses JInterop for WMI discovery. • **false** (default)**.** The Probe uses WMIdll native code.
useMultiThreadForEventHub	Indicates whether to use multiple threads in Event Hub. **Default:** true
useNtcmdModifiedMarkers	• **true.** The Probe uses markers with counters in NTCMD agents' infrastructure. • **false** (default)**.** The Probe uses old NTCMD behavior - without markers with counters.
useWinexeOnLinux	This setting is used on non-Windows machines. • **true.** The Probe uses local winexe executable for NTCMD Windows discovery. • **false** (default)**.** The Probe uses Windows remote Proxy.

portNumberToPortName.xml File

The **portNumberToPortName.xml** file is used by DFM as a dictionary to create IpServiceEndpoint CIs by mapping port numbers to meaningful port names. When a port is discovered, the Probe extracts the port number, searches in the **portNumberToPortName.xml** file for the port name that corresponds to this port number, and creates the IpServiceEndpoint CI with that name. If the port name does not appear in this file, the Probe uses the port number as the port name.

You can specify different names for same port number for different IP ranges. In this case, the same port discovered for IPs contained in different ranges will have different port names.

> **Note:** The **portNumber** attribute may be a number or a range. Ranges may be separated by commas or dashes or both. For example: "10, 21, 45", "10-21", or "10-21, 45, 110". You may use x as a wildcard in any position in a number. For example “5xx00” includes ports 50000, 50100, 50200, …51000, 51100, 51200, …59900.

For details on adding new ports to be discovered, see "How to Define a New Port" on page 5.

Chapter 8: Additional Protocol Information

This section includes:

Extended Shell Interface

UCMDB 10.00 extended the Shell Interface to remove limitations when uploading files to, and downloading files from, Windows machines. This increased functionality applies to the NTCMD and SSH protocols, and UD Agents.

When uploading or downloading files to or from Windows machines, you can set the parameter **setBandwidthLimit**, to restrict network bandwidth consumption.

You can set this parameter in **globalSettings.xml**:

The property is **shellGlobalBandwidthLimit**. For shell objects that support file downloading and uploading, it sets a limit, in kilobits per second, on the amount of bandwidth consumed by the download or upload operation. The value must be a positive integer. The default is 0, meaning no limit. For example:

```
<property name="shellGlobalBandwidthLimit">0</property>
```

The speed can be overwritten at adapter level or at job level; for example, when installing or updating UD Agents.

How to Create an SSH Connection Based on Public/Private Keys Pair

To create a Secure Shell (SSH) connection based on a public/private keys pair, perform the following steps:

1. Open the Mindterm console (on the probe machine) and from the command line run following command:

   ```
   C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\java.exe -jar
   C:\hp\UCMDB\DataFlowProbe\content\lib\Mindterm.jar
   ```

2. In the Mindterm console, go to **File > Create Keypair** and assign the following values:
   - **Key type/format:** choose DSA or RSA
   - **Key length:**
     - **If Key type/format = DSA:** choose 1024
     - **If Key type/format = RSA:** choose one of the following: 768, 1024, 1536, 2048, 4096, 8192, 16384 or 32768
   - **Identity file:** assign a name (the default name is **identity)**
   - **Password:** for no password, do not enter anything

   > **Caution:** The **OpenSSH .pub format** option must be selected.

3. Click **Generate** and move your mouse to generate public/private keys.
4. Once the pair is generated, go to **C:\Users\<username>\AppData\Roaming\MindTerm**. This directory contains generated public/private keys pair. The public key has the **.pub** extension.
5. Copy the contents of **.pub** file to the remote Linux/Unix machine you want to connect to as follows:
   a. Connect to the Linux/Unix remote machine and locate the **~/.ssh/authorized_keys** file (if the file does not exist, create it).
   b. Open the file for editing as follows:

      ```
      vi ~/.ssh/authorized_keys
      ```

   c. Append the contents of the **.pub** file to the **authorized_keys** file.
   d. Add <username>@<probe IP> to the end of the contents of the **.pub** file. For example, if the contents of the **.pub** file are:

      ```
      ssh-dss AAAAB3N.....<snippet>.....r2LnQrqhncpJyL1s0id76j6wA==
      ```

      and the probe's IP is 16.59.56.255 and the username to connect with is **root**, you would append the following to the contents of the **~/.ssh/authorized_keys** file:

      ```
      ssh-dss AAAAB3N.....<snippet>.....r2LnQrqhncpJyL1s0id76j6wA==
      ```

```
root@16.59.56.255
```

e. Save the **~/.ssh/authorized_keys** file and close it.

6. Open the UCMDB and go to **Data Flow Management > Data Flow Probe Setup > Credentials > SSH Protocol**.
7. Add a new SSH protocol with the following parameters:
   - **Authentication Method:** publickey
   - **User Name:** root
   - **Key File Path:** C:\\Users\\<username>\\AppData\\Roaming\\MindTerm\\<identity file>, where <identity file> is the name you entered in step 2.
   - **Password:** if you provided a password during creation of the public/private keys pair, you must enter the same password here.

How to Enable Support for the AES256-CBC and AES256-CTR Encryption Ciphers

To enable support for the AES256-CBC and AES256-CTR encryption ciphers, perform the following steps:

1. Stop the UCMDB server and Data Flow Probe service.
2. Download the **UnlimitedJCEPolicyJDK7.zip** file from http://www.oracle.com/technetwork/java/embedded/embedded-se/downloads/jce-7-download-432124.html.
3. Extract the ZIP package.
4. Copy the **local_policy.jar** and **US_export_policy.jar** files to the **<DataFlowProbe installation folder>\bin\jre\lib\security** directory to replace the old ones.
5. Start the UCMDB server and Data Flow Probe service.

Chapter 9: Event Based Discovery

Background

In UCMDB, the regular Universal Discovery jobs are scheduled to run, such as once a day or once a week. During the discovery interval, UCMDB cannot detect what have been changed in remote nodes. For the traditional IT infrastructure, this kind of discovery is good enough to reflect the topology of the data center.

In recent years, the Cloud is becoming quite popular among the IT world. Amazon Web Services, OpenStack, VMware vCloud, Cloud Foundry, and Docker are rapidly adopted by many companies. One of common characters of these technologies is that changes happen easily and frequently. However, the regular Universal Discovery cannot accurately handle such changes in real time. For example:

- No clues of the existence of nodes. One virtual machine is created for testing at 9:00, and then it is terminated at 16:00 after the testing. Its administrator is not even aware of its existence because most of regular discovery jobs are scheduled to run at midnight.
- Topology in UCMDB cannot reflect the current status of the Cloud environment. The typical aging time in UCMDB is more than one month. In traditional data centers, nodes are rarely changed. Generally, regular discovery jobs do not delete CI. Therefore, the topology in UCMDB is consistent with the actual environment in most time. However, in the Cloud environment, nodes are created and deleted at any time. After a while, many nodes that are deleted in the Cloud environment still exist in UCMDB. These nodes become a kind of "noise" before they are aged.

Overview

In order to adjust to the Cloud environment, the event based discovery is introduced. This discovery is based on the event that is sent out from Cloud providers in real time. The event based discovery uses a framework called Event Hub to capture such events and report them into UCMDB. Thus, the topology in UCMDB can reflect the actual environment as much as possible.

So far, the following event based discoveries for Cloud environments are introduced:

- Cloud Foundry Event Discovery
- OpenStack Event Discovery
- VMware vCloud Event Discovery
- Docker Swarm Event Discovery

For details about these event based discoveries, see the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Modules*.

Discovery Mechanism

This section describes the discovery mechanism for the event based discovery.

Event Hub

Event Hub is a new framework designed for the event based discovery. It includes the following:

- Event Source. Collects events from event providers and puts them in Event Queue.
- Event Filter. Filters events to only allow specific events to pass through.
- Event Handler. Handles events and reports them as CIs to UCMDB.

When Event Source starts, it continuously listens to or fetches events from event providers. After events arrive, the events are buffered in a memory queue. Meanwhile, there is a thread pool that is waiting for new events to pull them from the queue. After a new event is pulled, a thread uses Event Filter to filter the event. Then, the filtered event is passed to Event Handler. In Event Handler, one typical handler parses the event and constructs the CI topology to report to UCMDB.

Continuously running jobs

One important difference between an event based discovery job and a regular job is that the event based discovery job runs continuously until the job is manually deactivated or terminated by Data Flow Probe due to exceeding the maximum execution time.

In UCMDB 10.22, the maximum execution time of jobs is 2147483647 milliseconds (about 24.86 days). Thus, the job needs to be rerun after the timeout. This is a limitation. In UCMDB 10.30, if the maximum execution time of jobs is set to 0 (zero), the job will not reach the time limit.

Event providers

So far, the following Event Source providers are implemented:

- Cloud Foundry
- OpenStack
- VMwarevCloud
- Docker Swarm

Limitation

Limitation. In UCMDB 10.30 and earlier versions, using multiple threads in the event-based discovery may cause the missing of events.

Workaround. It is recommended to upgrade UCMDB to 10.31 or a later version. For UCMDB 10.30 and earlier versions, setting **useMultiThreadForEventHub** to **false** in **globalsetting.xml**; however, this operation may affect the performance of event-base discovery jobs. For details about this setting, see "globalSettings.xml File" on page 16.

Chapter 10: **PrimaryDNSName** Logic

Previously, the **DNS Resolver** job sets the **PrimaryDNSName** (**primary_dns_name**) of a Node to the resolved DNS name of the smallest IP address integer equivalent among all IP addresses contained by a given Node. If either the backup network or cluster virtual IP addresses have a numerically smaller address than the address of the Node, that address incorrectly updates the **PrimaryDNSName** of the Node.

In order to solve this issue, the **PrimaryDNSName** logic is changed as follows:

For a full DNS name (for example, **host1.cms.chn.hpe.com**),

- If the short name (that is, **host1** in the example) of the full DNS name is NOT equal to the host name, the full DNS name will NOT be considered as the **PrimaryDNSName**.
- If the short name (that is, **host1** in the example) of the full DNS name is equal to the host name, the full DNS name will be one candidate of the **PrimaryDNSName**.

  For each candidate,

  a. Covert its related IP address to the integer equivalent, and then retrieve the smallest one.

  b. Take the DNS name of the smallest IP address integer equivalent as the **PrimaryDNSName**.

For example:

- Node 1 has three IP addresses: A, B, C; the host name is **host1**.
- IP address A is resolved as **host1.cms.chn.hpe.com**.
- IP address B is resolved as **host2.cms.chn.hpe.com** (That is possible, in the cluster environment, some cluster IP addresses can be resolved as cluster names).
- IP address C is resolved as **host1.chn.hpe.com**.
- IP address B is the smallest IP address integer equivalent.

Previously, the **DNS Resolver** job takes **host2.cms.chn.hpe.com** as the **PrimaryDNSName** regardless of the fact that **host2 !=host1**, because IP address B is the smallest IP address integer equivalent.

Currently, **host2.cms.chn.hpe.com** is no longer considered as the **PrimaryDNSName**. Both **host1.cms.chn.hpe.com** and **host1.chn.hpe.com** are candidates of the **PrimaryDNSName**. For these candidates, covert their related IP addresses to the integer equivalents. If A > C, **host1.cms.chn.hpe.com** is the **PrimaryDNSName**.

Chapter 11: Supported UNIX Shells

UCMDB supports use of the following UNIX shells:

- bash
- csh
- ksh
- tcsh

Chapter 12: Troubleshooting and Limitations

This section describes general troubleshooting and limitations related to performing discovery using Universal Discovery.

- **Problem**: Cannot Connect to Windows Vista/2008-R2 Machines with UAC Enabled

  Reason: Starting from Windows Vista, Microsoft has changed the security mechanism by introducing the UAC (User Account Control) technology. This change causes problems with HPCmd connecting to remote Windows Vista/2008-R2 machines when using the local administrator account.

  Solution: The following procedure enables HPCmd connection to remote Windows Vista/2008-R2 machines with UAC enabled.

  a. Verify the HPCmd connection

     i. Log on to the Probe machine.

     ii. Locate the **HPCmd.bat** file in hp\UCMDB\DataFlowProbe\tools directory.

     iii. Open **cmd.com** in the same directory.

     iv. At the command prompt, invoke following command:

     ```
     HPCmd.bat \\<problematic machine name or ip>
     /USER:<domain>\<username> /PWD:<password>
     ```

  b. If the HPCmd connection is not successful, check accessibility to the shared folder, admin$.

     Ensure that the Probe machine can access the shared folder, **admin$**, on the remote machine.

     i. Log on to the Probe machine.

     ii. Select **Start > Run**, and enter `\\<remote machine>\admin$ address`.

     iii. If there is no access to **admin$**:

     - Log on to the remote machine.
     - Select **Start > Run**, and enter `regedit`.
     - Locate the following registry subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
LanmanServer\Parameters
```

- Click **Parameters**.
- If the **AutoShareServer** registry entry does not exist, in the **Edit** menu, select **New > DWORD (32-bit) Value.** Enter **AutoShareServer**, and click **OK**.
- Select **AutoShareServer**. In the **Edit** menu, select **Modify**, and in the **Value** box, type `1`.
- Exit the Registry Editor, and restart the computer.
- Select **Start > Run**, and enter `net start srvnet`.

iv. When access to **admin$** is successful, try to verify the HPCmd connection again as described in "Verify the HPCmd connection" on the previous page.

c. If the verification still fails, connect to Windows Vista/2008-R2 machines with UAC enabled.

i. On Windows Vista/2008-R2 machines, local administrators do not have full privileges when connected remotely.

Use one of the following options to overcome this problem:

- Connect using domain administrator credentials.
- Enable local administrators to have full privileges by modifying the registry on remote machine as follows:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
Value	LocalAccountTokenFilterPolicy should be set to 1. If this value is not available, create a new DWORD value and set it to 1.

ii. Restart the machine.

- **Problem:** The file transfer does not work when communicating with the remote Linux/UNIX/Mac OS X machines, as the result operations like Scanner-based Inventory Discovery or deployment of Universal Discovery agents fail.

  Solution:

  a. Make sure the SSH agent is configured to allow file transfer via the SCP/SFTP protocols.

  b. Make sure that the logon process for the user that is used for the SSH protocol does not have a banner that requires manual user input during the logon process.

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 Discovery and Integrations Content Guide - General Reference (Universal CMDB Content Pack 24.00 (CP24))

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to cms-doc@hpe.com.

We appreciate your feedback!